COMODO
Creating Trust Online®

COMODO ONE
MSP

Comodo Dome Shield

Software Version 2.0

Administrator Guide

Guide Version 2.0.113018

Table of Contents

1   Introduction to Comodo Dome Shield

Comodo Dome Shield 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. Dome Shield also features advanced reporting, custom B/W lists and a granular policy manager which allows you to create location-specific filtering policies.

Features

- Default rules which provide blanket protection from malware, botnets and high risk sites for networked, roaming and mobile devices
- Website categories make it easy to create a custom filtering policy
- Create your own domain blacklists and whitelists.
- Fast import of networks and roaming devices. Local resolvers can encrypt and forward DNS queries from endpoints to Dome Shield DNS servers
- Advanced reporting grants full visibility of events on your Dome Shield perimeter
- Easy to setup. Just set your DNS servers to Dome Shield

Guide Structure

This guide is intended to take you through the configuration and use of Dome Shield and is broken down into the following main sections:

- **Introduction**
    - **Purchase a License**
    - **Login to Dome Shield**
    - **Setup Options Explained**
        - **Tutorial to Add Networks to Dome Shield**
        - **Tutorial to Add Roaming Endpoints to Dome Shield**
        - **Tutorial to Add Mobile Devices**
        - **Tutorial to Deploy Shield Virtual Appliances**
        - **Setup Wizard - Add Networks**

1.1   Purchase a License

Two license types are available for Dome Shield:

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

Click here to compare packages.

The are two ways to enroll for Dome Shield:

- **Stand-alone customers** (Enterprise licenses only) - Sign-up for a free license at **https://www.comodo.com/cdomeshield/freelicense/**
- **Comodo One customers** (Enterprise and MSP licenses) - Dome Shield is automatically activated in your account
    - US customers - **https://us.one.comodo.com/**
    - Other countries - **https://one.comodo.com/**

Dome Shield Stand-alone Customers:

Note – Applies to customers that purchased an Enterprise license via **https://www.comodo.com/cdomeshield/freelicense/**

- **Get a Gold license**
- **Get a Platinum license**

COMODO
Creating Trust Online®

Sign up for a Gold (free) license

- Visit **https://www.comodo.com/cdomeshield/freelicense/**

- **'Enterprise' licenses** - Single business licenses.
  - Login at **https://shield.dome.comodo.com/login**
- Note 1 – 'Individual' licenses are no longer offered. All existing individual licenses have been updated to enterprise license types.
- Note 2 – If you get an MSP license instead then you must access Shield via the Comodo One portal at **https://one.comodo.com**
- Click 'Enterprise' (orange button) to open the order form:

- Existing customers - If you already have a Comodo account, select 'Existing Comodo User' and enter your user name and password.

- New customers - Create a new account by selecting 'New Comodo User'

- Select the number of user-devices you want to protect from the employees drop-down

- Read and agree to the the end-user license agreement then click 'Continue'.

You will be taken to the order confirmation page:

- You will receive a confirmation email which contains a summary of your order.
- You will also receive an account activation email. Click the link in this mail to activate your account
- Follow the instructions on the page to get started with Dome Shield

To purchase a Platinum package

- Visit **https://www.comodo.com/cdomeshield/freelicense/**

- Click 'Learn More' > 'Compare Packages'

- Click 'Buy Now' in the 'Dome Shield Platinum for Enterprises' tile

- Existing customers - If you sflready have a Comodo account, select 'Existing Comodo User' and enter your user name and password.

- New customers - Create a new account by selecting 'New Comodo User'

- Select the number of user-devices you want to protect

- Provide your payment details.

- Read and agree to the the end-user license agreement then click 'Continue'. Complete the order process.

- We will send order confirmation and license emails to your registered address.

Comodo One Customers

- US customers - **https://us.one.comodo.com/**
- Other countries - **https://one.comodo.com/**

A Dome Shield Gold license is automatically activated in your account when you sign-up for a C1 account.

To upgrade to a Platinum license

- Login to your C1 account at **https://one.comodo.com/** or **https://us.one.comodo.com/**

- Click 'Management' > 'Applications'

- Select 'Dome Shield' then click the 'Subscriptions' tab

- Click 'Add New Subscription'
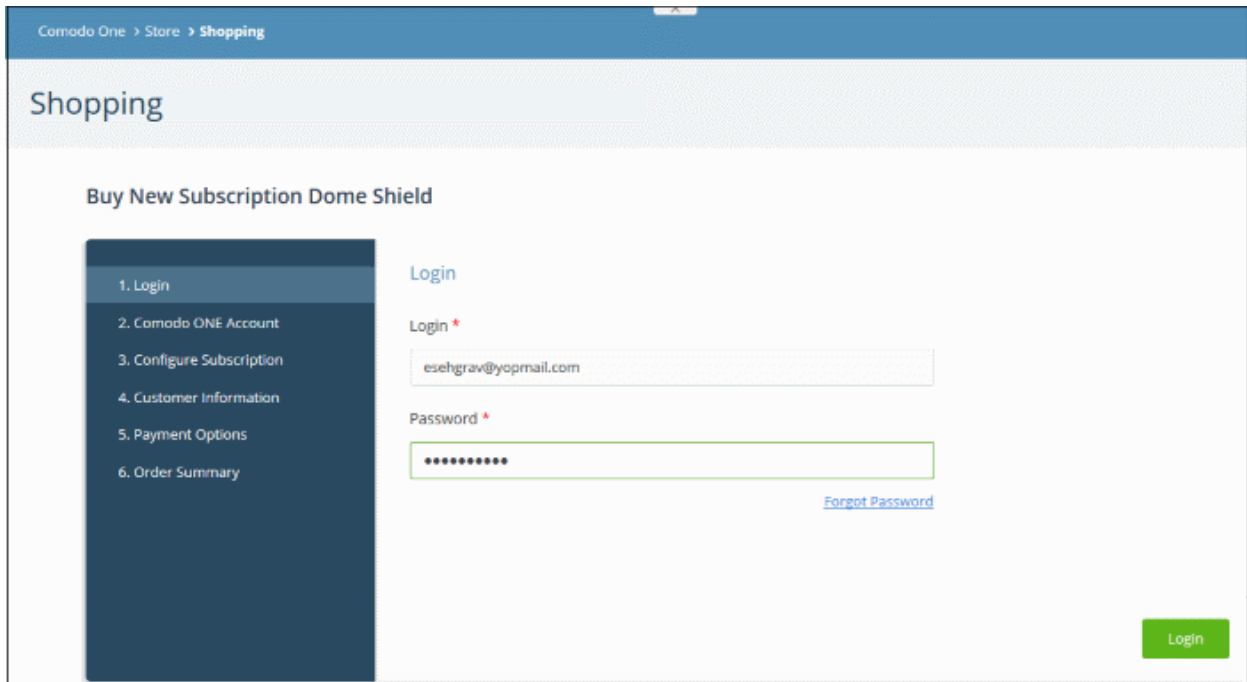
- The account username will be pre-populated.
- Enter your Comodo password and click 'Login'
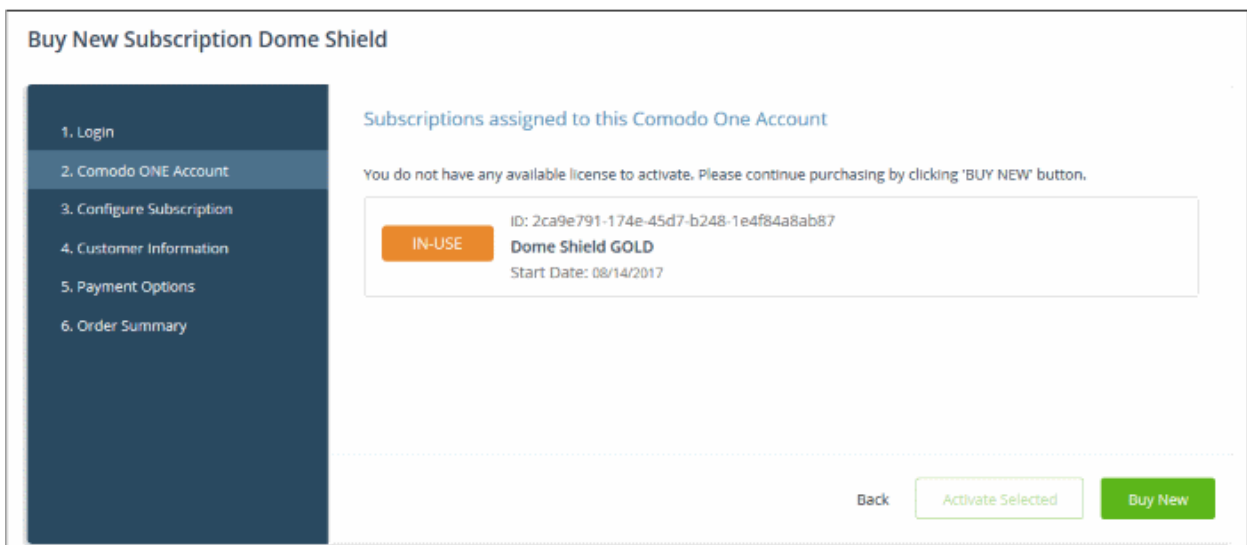
- **Activate Selected** – Platinum licenses bought via your Comodo Accounts Manager (CAM) account can be activated for use in Comodo One.
- **Buy New** – Purchase a new Platinum license.
- Select the number of users you require and the term of the license:

COMODO
Creating Trust Online®

Buy New Subscription Dome Shield

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

Configure Subscription

Amount of Users   1000   Users

1	100	250	500	1000	2500	5000	10000	25000	10000000
	$29.38 per user	$25.78 per user	$21.02 per user	$16.20 per user	$14.98 per user	$14.40 per user	$18.82 per user	$13.18 per user	$12.60 per user

Select Period

1 month   3 months   6 months   **1 year**   2 years   3 years

$14.98 per 1000 users for 1 year = $14,980.00

$14,980.00

Back   Next

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

Buy New Subscription Dome Shield

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

Customer Information

Company Name

Great MSP

Company Website

Phone Number *

12345678

Street Address *

Street 1

Street Address 2

Street 2

City *

Chennai

Country *

India

State or Province

Postal Code *

600042

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 terms and conditions and click 'Next'
- Complete your payment details

- Click 'Next' to place your order.

Compare Dome Shield Packages

Dome Shield – 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	✘	✔	✔
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 Dome Shield Portal are *not* included in the 300 K limit.
  - Once 300 K limit is reached:
    - All existing policies will continue to function as before.
    - You can edit existing rules and policies
    - You cannot add new rules, policies or objects. Objects = networks, roaming agents and mobile agents.
  - The request count is reset to zero at the beginning of each month. At this point you can add new objects, policies and rules.
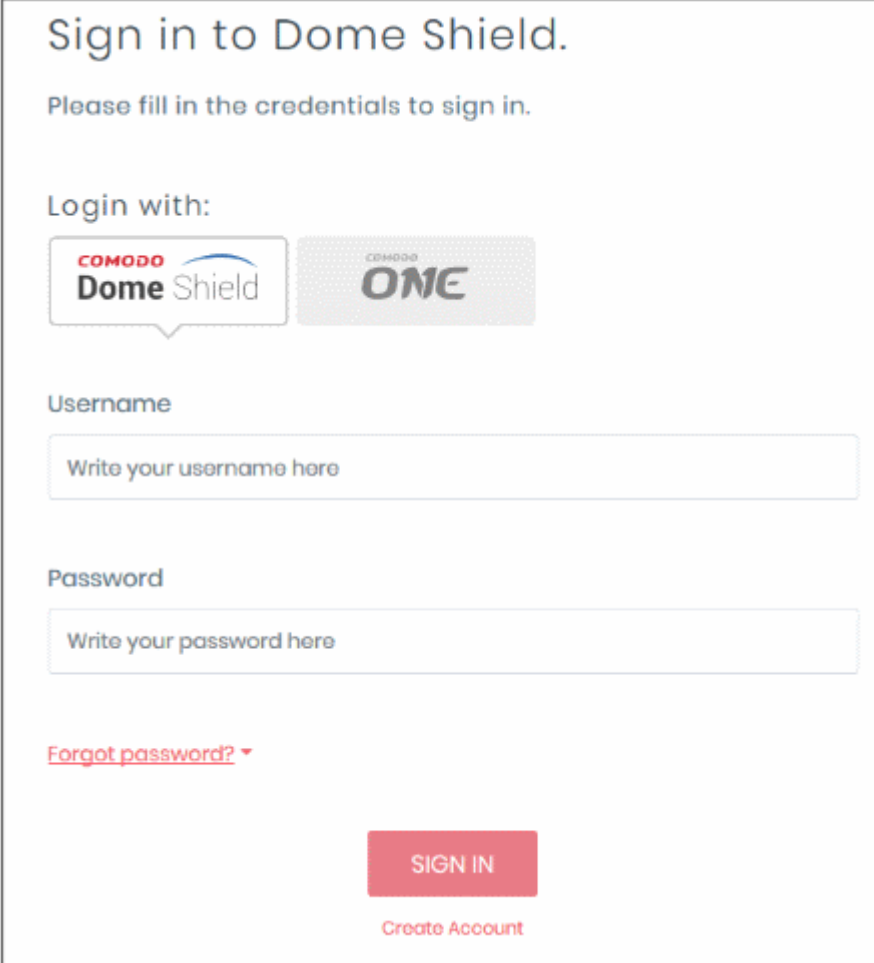
Click here for more information about Shield license package details.

1.2   Login to Dome Shield

Login to Dome Shield

Stand-alone Dome Shield portal

- Note – Applies to enterprise customers that purchased a license from the Dome website at **https://cdome.comodo.com/**
- Login at **https://shield.dome.comodo.com/login** and select 'Dome Shield'
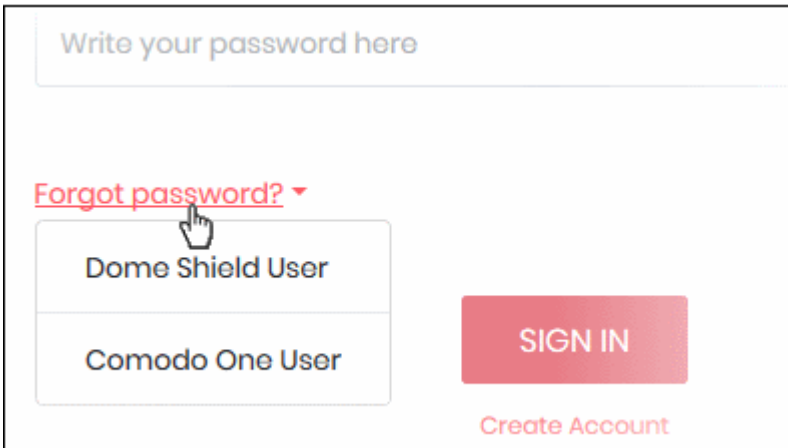
- Username and password are case sensitive. Make sure you use the correct case.
- Click 'Forgot password?' if you can't remember your password. Select 'Dome Shield User' account type:

- You will be taken to **https://accounts.comodo.com/account/forget_password**. to reset your password.

Comodo One Portal

- Login to your C1 account:

- US customers - **https://us.one.comodo.com/app/login**
  - Other countries - **https://one.comodo.com/app/login**
- Username and password are case sensitive. Please make sure that you use the correct case.
- Click 'Forgot password?' if you can't remember your password. A mail will be sent to your registered email address with a link to reset it.
- Click 'Applications' > 'Dome Shield' to open the Shield interface.
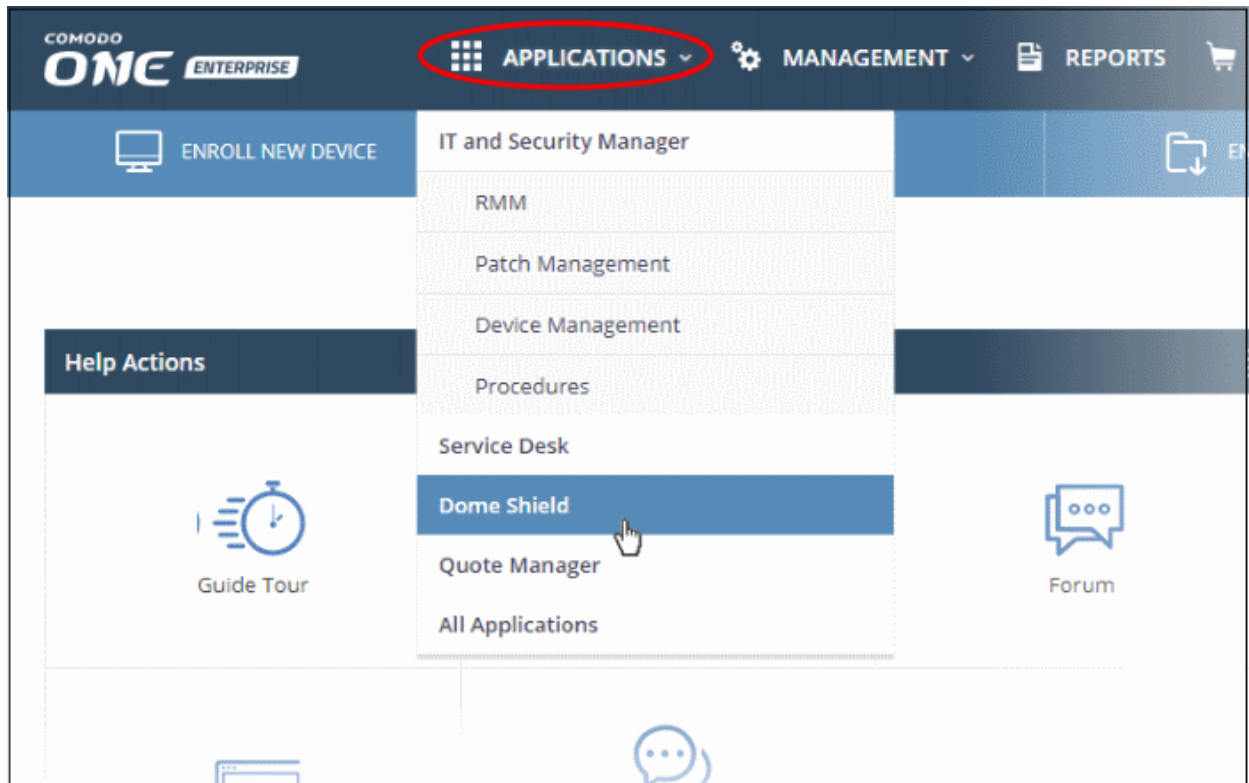
1.3 Setup Options Explained

There are three alternative ways you can setup Dome Shield 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**.
   - Follow the steps in the tutorials to setup Dome Shield

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 Dome Shield
   - The resolver will forward public DNS queries from your endpoints to Dome 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 Dome Shield

- Login to Dome Shield
- Click 'How-to' at the top-right to open the tutorial menu:
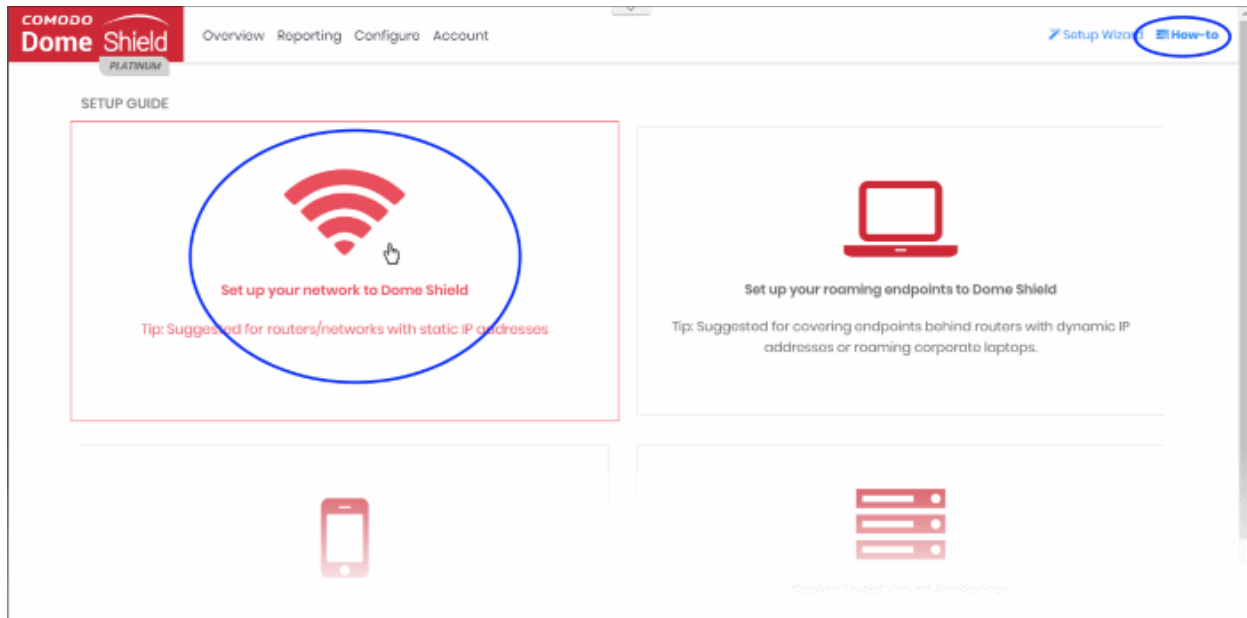
- Click the network icon on the left to open the network setup guide:
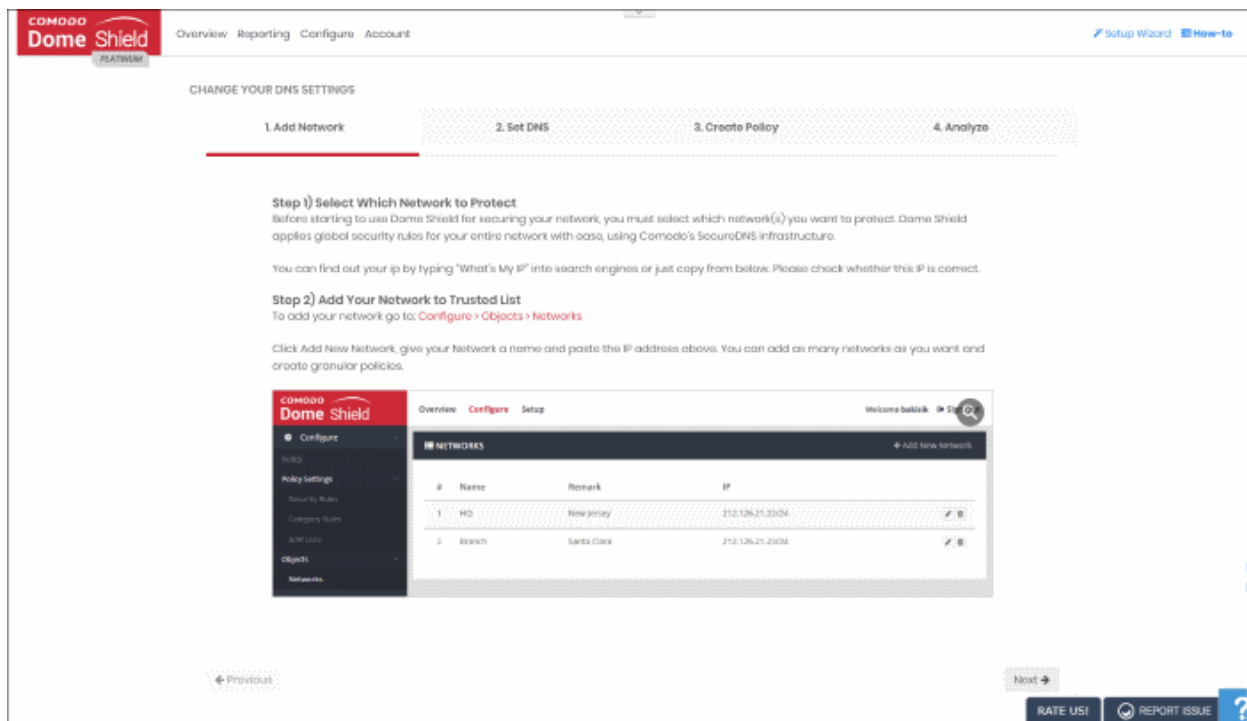
There are four main steps in the tutorial:

- **Add Network** - Import your network to Dome Shield.
- **Set DNS** - Set your DNS server, router or firewall to use the Dome Shield DNS service.
- **Create Policy** – Create content filtering rules and domain black/whitelists.

- **Analyze** - View traffic trends on your network.

1.3.2   Tutorial to Add Roaming Endpoints to Dome Shield

- Login to Dome Shield

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

- Click the laptop icon to open the guide:
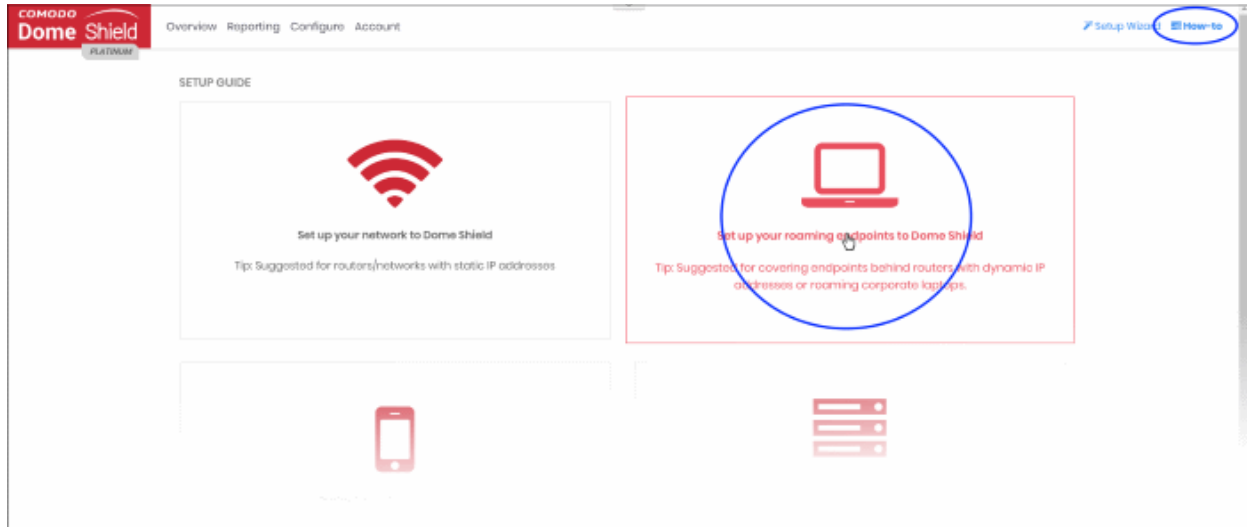
- Click the device icon to open the roaming endpoints setup guide:
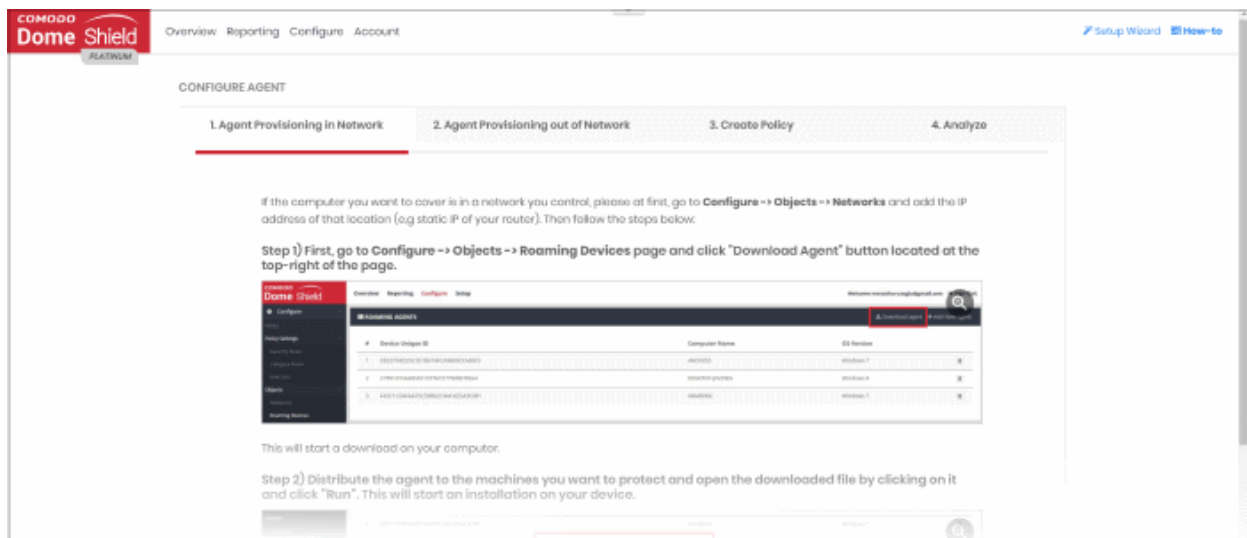
There are four main steps covered in the tutorial:

- **Agent Provisioning in Network** - Enroll devices inside your network

- **Agent Provisioning out of Network** - Enroll devices outside your network

- **Create Policy** - Create content filtering rules and domain black/whitelists.

- **Analyze** - View traffic trends on your network.

1.3.3 Tutorial to Add Mobile Devices

- Login to Dome Shield
- Click 'How-to' at top-right to open the tutorial menu:
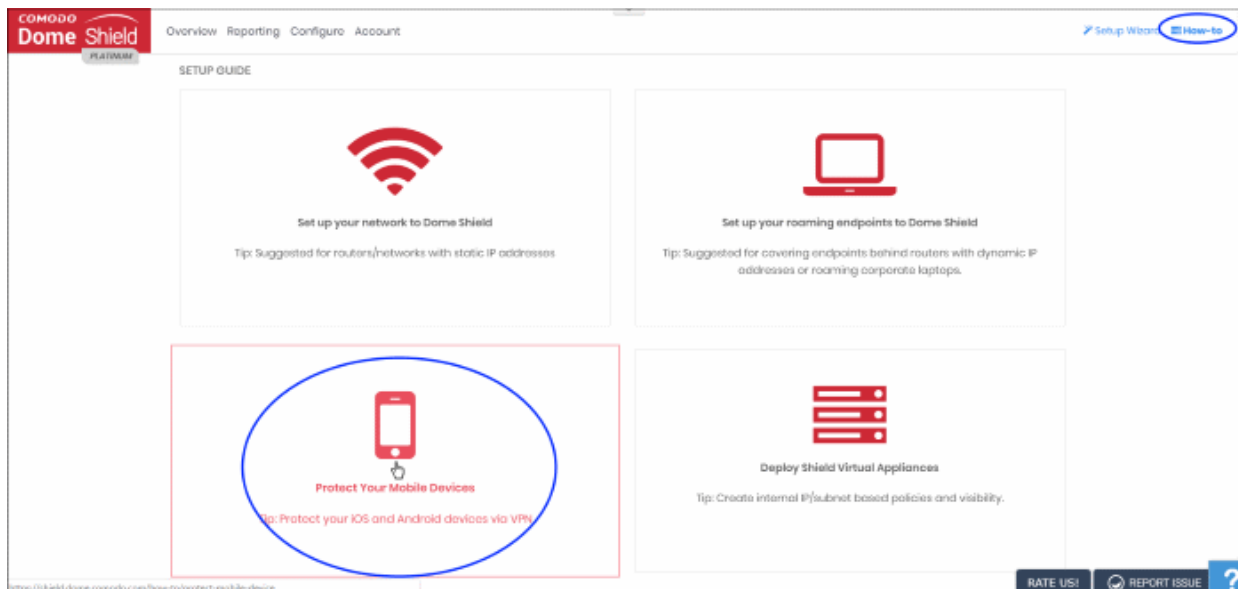
- Click the mobile device icon to open the setup guide:
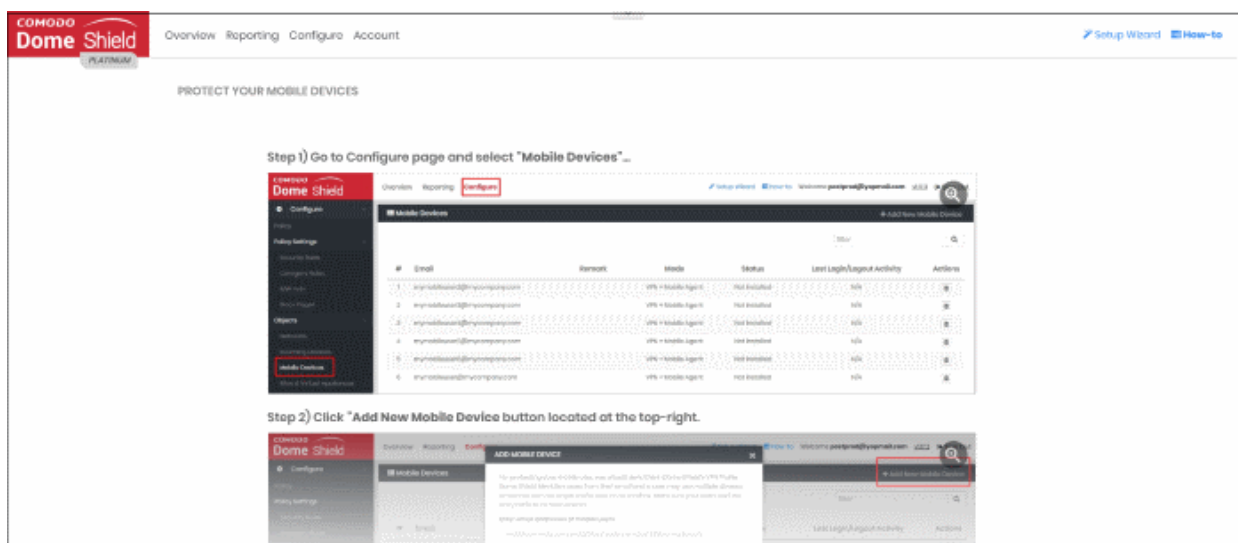
The tutorial explains how to add mobile devices to Shield.

- See '**Add Mobile Devices to Dome Shield**' for more information.

1.3.4   Tutorial to Deploy Shield Virtual Appliances

- Login to Dome Shield
- Click 'How-to' at the top-right to open the tutorial menu:
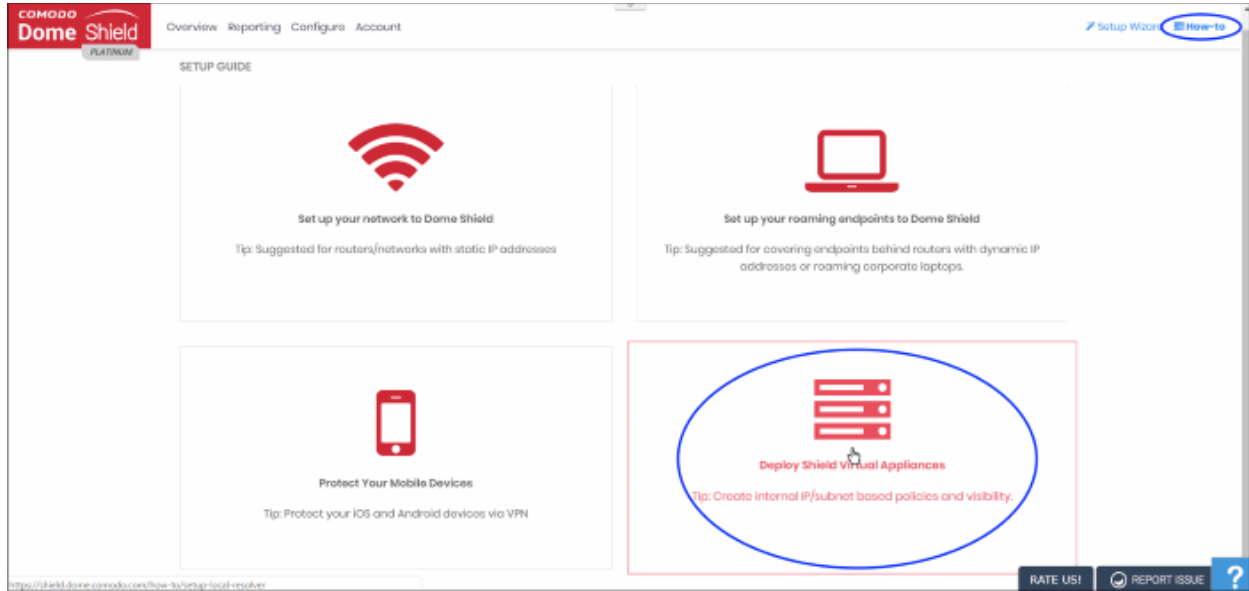
- Click the appliances icon to open the 'Shield Virtual Appliances' setup guide:
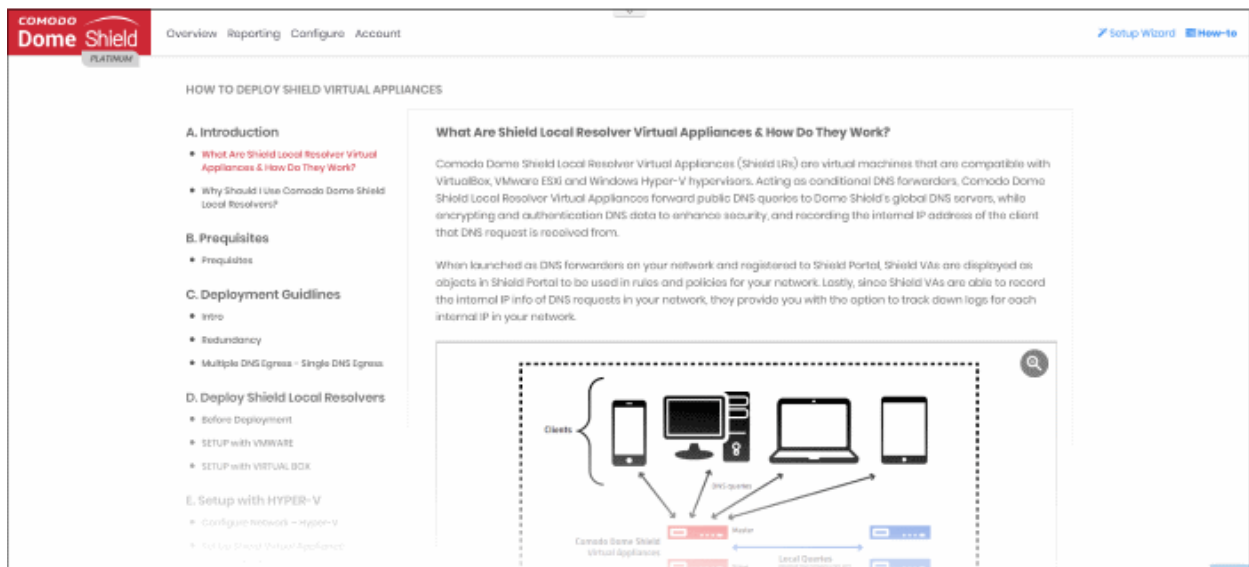
The instructions explain how Shield local resolvers work and how to setup virtual appliances.

- See '**Setup Local Resolver Virtual Machines and Import Sites**' if you need more help.

1.3.5   Setup Wizard - Add Networks

- The setup wizard lets you quickly enroll your networks to Dome Shield protection.

- If you have not yet added any networks then the wizard will start automatically after logging in.

- You can also start the wizard at any time by clicking the 'Setup Wizard' link at top-right:
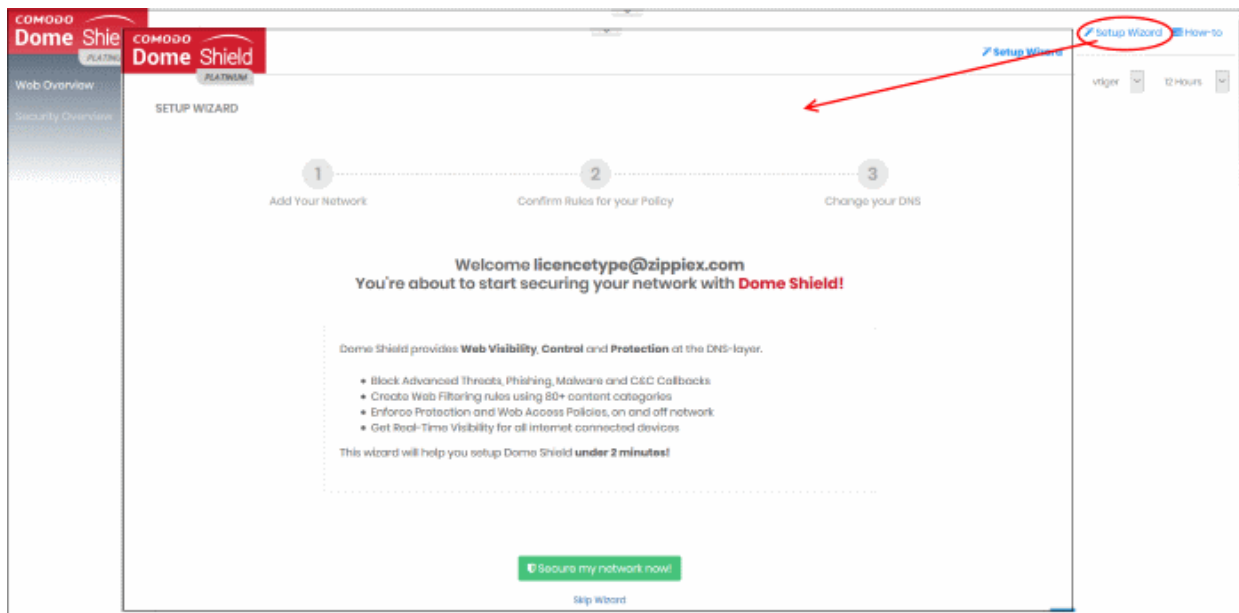
- Click 'Secure my network now!'

Step 1 - **Add your IP Address**

- **IP Address / FQDN**
    - The IP address or fully qualified domain name of your network. Enter the address in CIDR

(Classless Inter-Domain Routing) notation.

- Dome Shield can accept network prefixes from /24 to /32.

- By default, this field shows the public IP of the network from which you are connecting to Dome Shield. This network is automatically activated after initial enrollment.

  You can also add the IP address of a different network that you want to protect.

- Note 1 – Any IP address you add here will be automatically activated for protection. Make sure you have access to change the network's DNS settings to Dome Shield, as explained in step 3.

- Note 2 – Shield also supports dynamic IP addresses. You need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint. See '**Manually Add Networks to Dome Shield**' for more information.

- Select Company - This applies only to MSP accounts.

- 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.
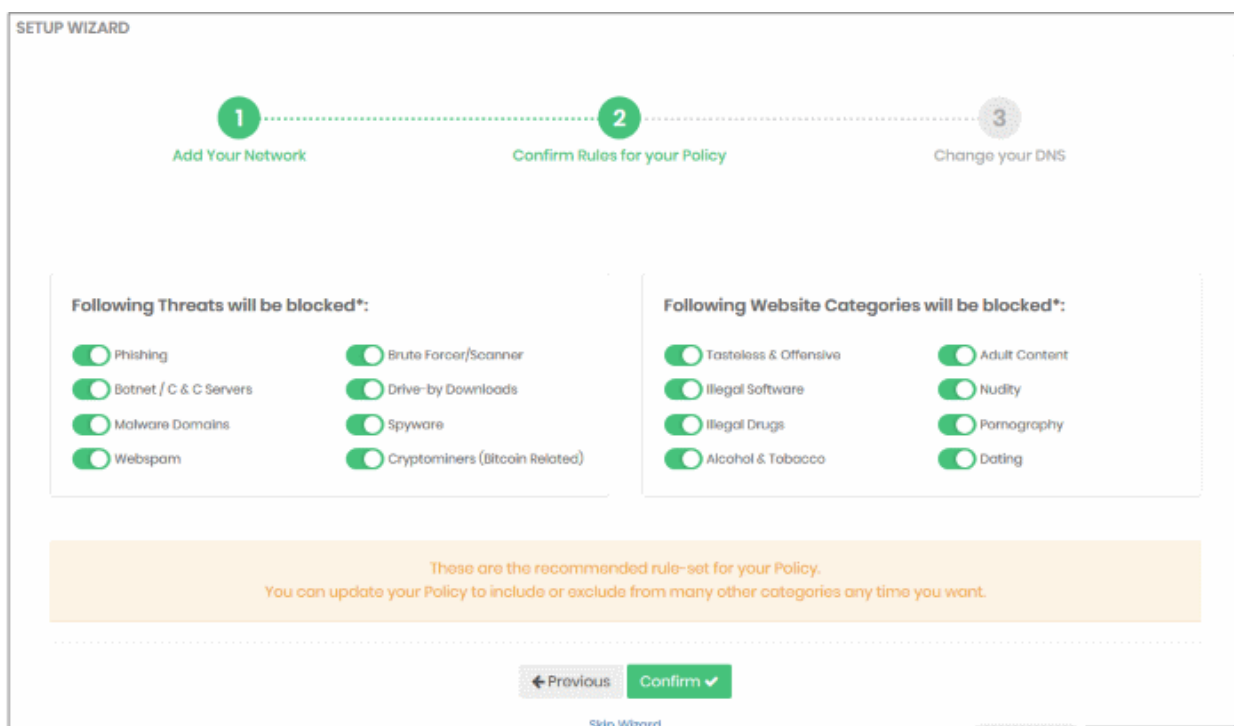
- All rules are enabled by default. You can enable / disable rules here as required.

- 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 Dome Shield addresses:

  - Preferred DNS server - 8.26.56.10

  - Alternate DNS server - 8.20.247.10

- Click 'Yes, My DNS is set to Shield' after configuring the DNS settings.
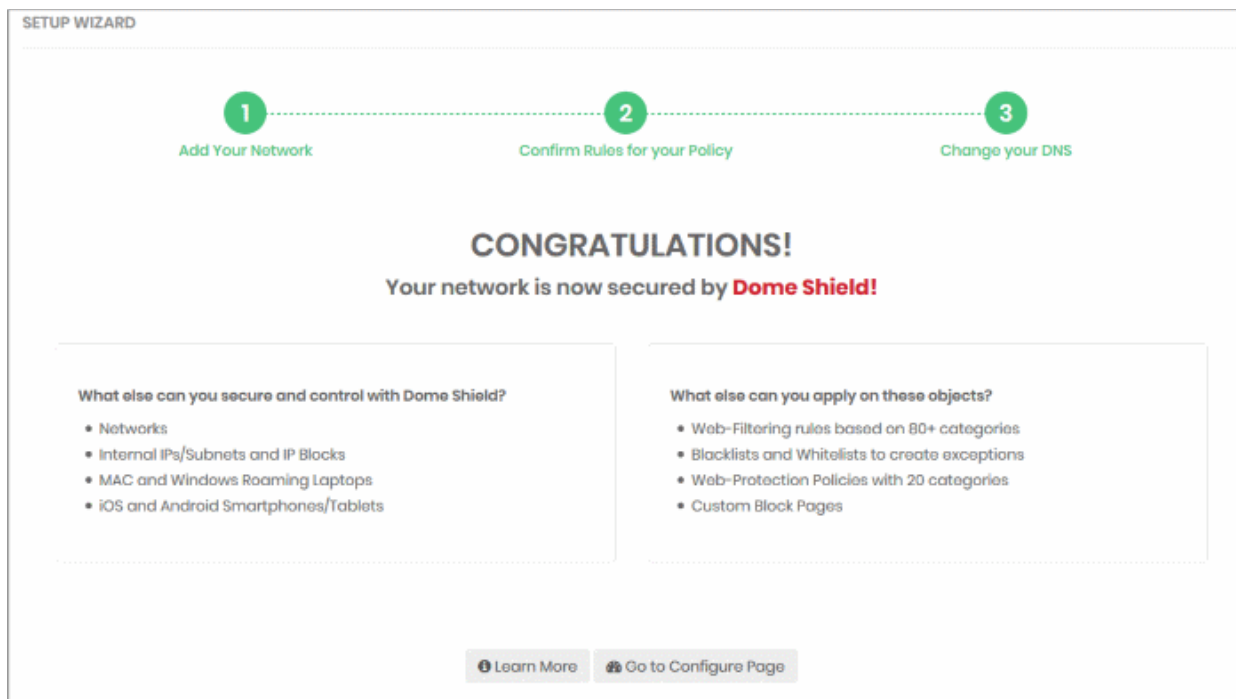
That's it. You have now added a network to Dome Shield.

- Click 'Configure' > 'Objects' > 'Networks' in the Dome interface to see all networks that you have added.

- The specified static IP address for your network will automatically become active.

- Note – To support dynamic IP addresses, you need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint. See '**Manually Add Networks to Dome Shield**' for more information.

Next, see:

- **Policies** - See '**Manage Shield Rules**' and '**Apply Policies to Networks Roaming and Mobile Devices**'

- **Adding networks, roaming and mobile devices** - See ' **Add Networks, Roaming Endpoints and Mobile Devices to Dome Shield**'

- **Dashboard** - See '**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 Dome Shield.

- The resolver is deployed as a virtual machine on your network and will forward public DNS queries to Dome Shield global DNS servers.

- Once deployed, the network will be automatically imported to Dome Shield.

- The resolver import method offers some key advantages 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 Dome Shield logs and reports, which gives you insight into the browsing patterns of your endpoints.

- 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. The endpoint DNS settings just need to be pointed 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 (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 Dome Shield 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:

The local resolver VA can be setup using virtual machine applications like VMWare, VirtualBox or Hyper-V manager.

The virtual appliance should be configured with the following minimum hardware configuration:

- One virtual CPU
- 1024 MB of RAM
- 7 GB of disk space

> **Important Note**: If you believe you will have a high-traffic site, we recommend you to use 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 from the overall network.

The rest of this section explains the step-by-step installation process of the LR VA's

Setup the Local Resolver(s)

- **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 Dome Shield
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Download Component' at the top-right
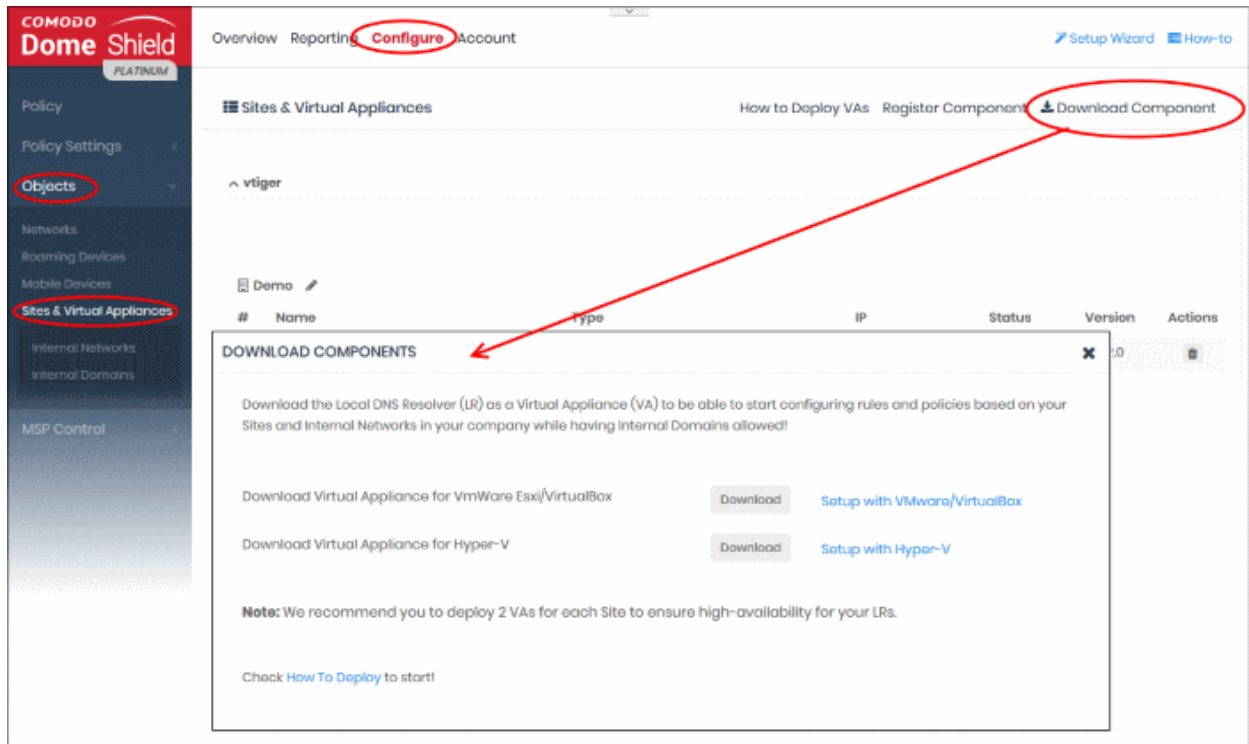
The resolver VA can be setup on virtual machine applications like VMWare, VirtualBox and Hyper - V.

- Click the 'Download' button beside the VM application you want to use
- The setup package will be downloaded in .zip format
- The package contains an OVA or HYPER-V file depending on the VM application 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 Dome 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'
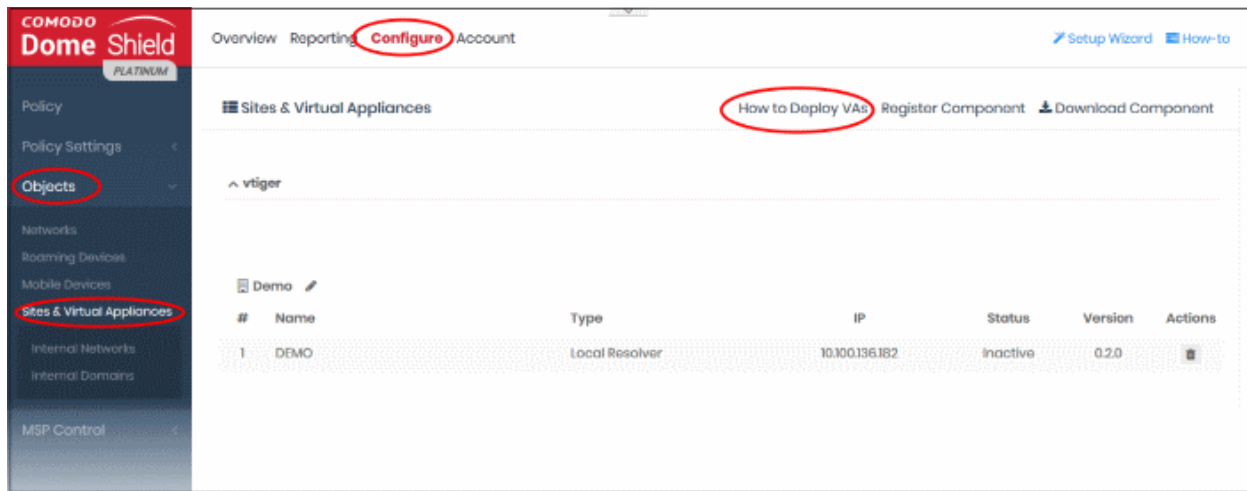
The instructions page explains how to install the VA on VMWare, VirtualBox and Hyper-V:
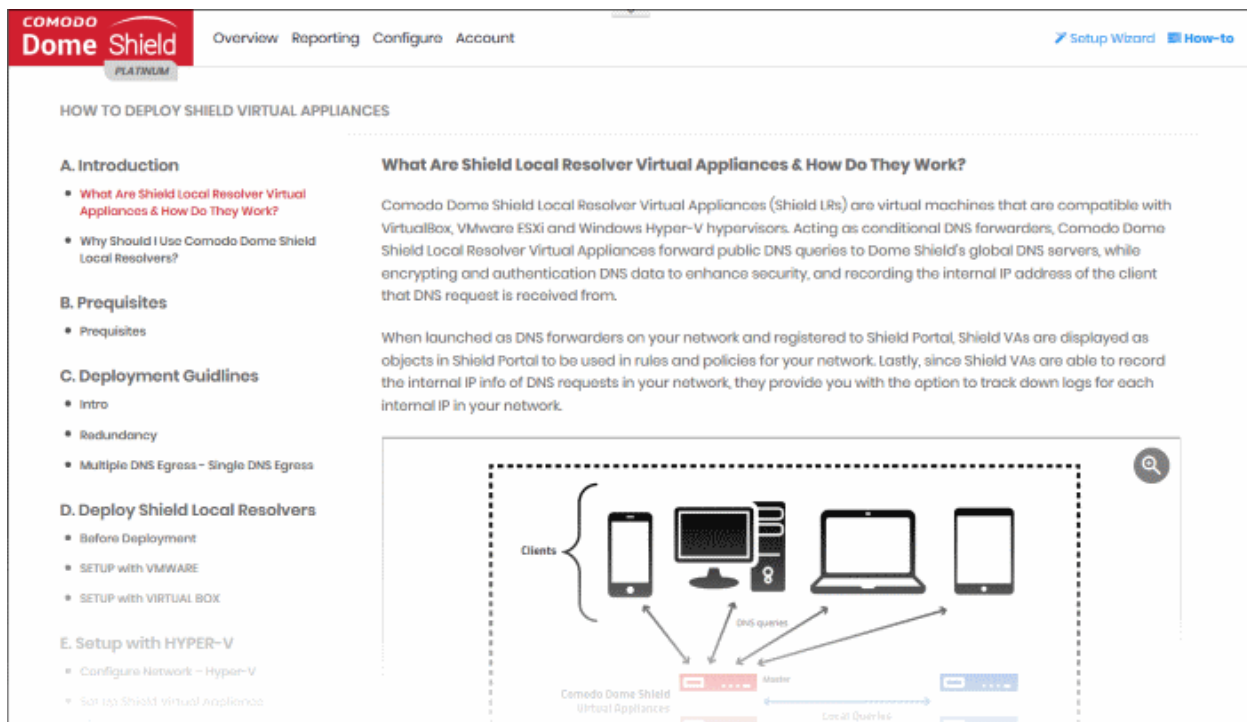
Configure the Local Resolver

• Start up the VA once installation is complete.
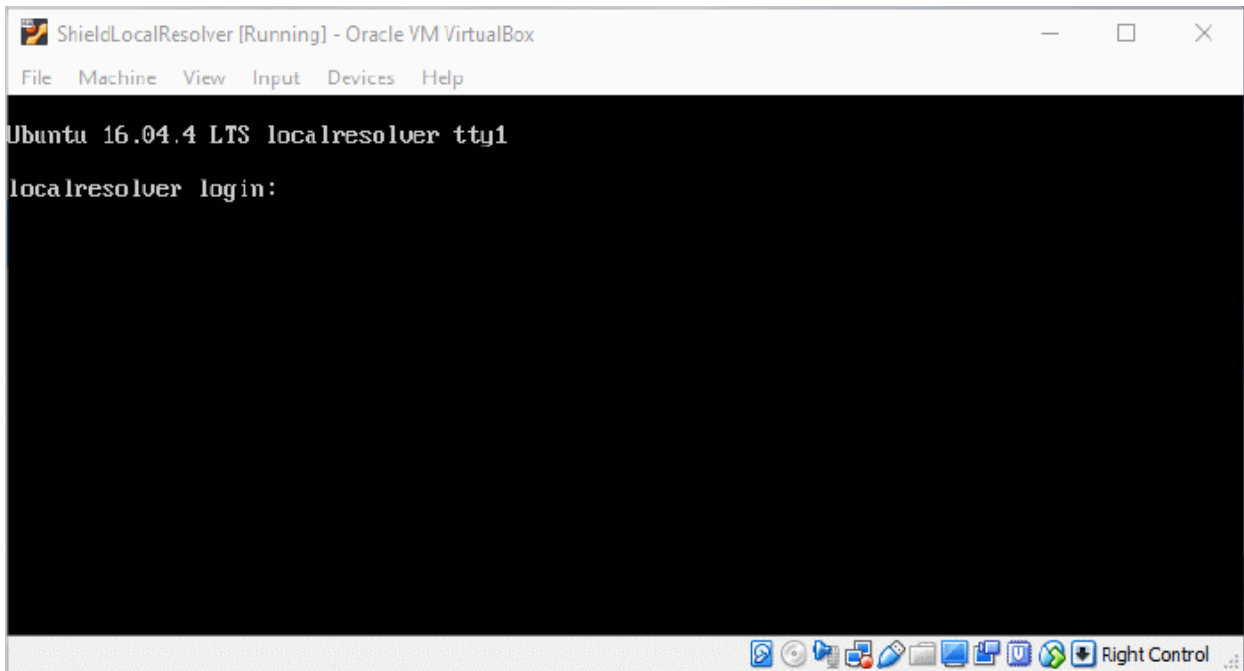
- Login to the appliance with the username and password in credentials.txt. This file is in the VA package you downloaded.
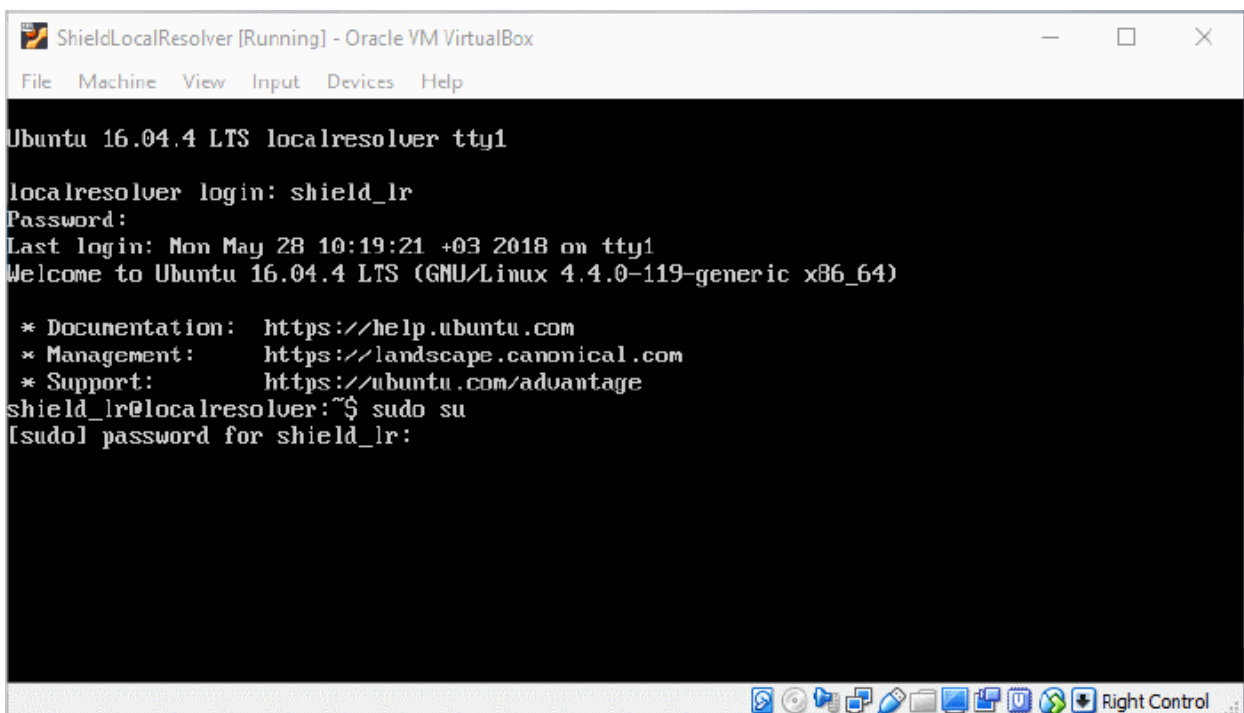
- Run the 'sudo su' command and enter the root password contained in the 'credentials.txt'. This will give you root access.

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

The LR configuration screen will open.
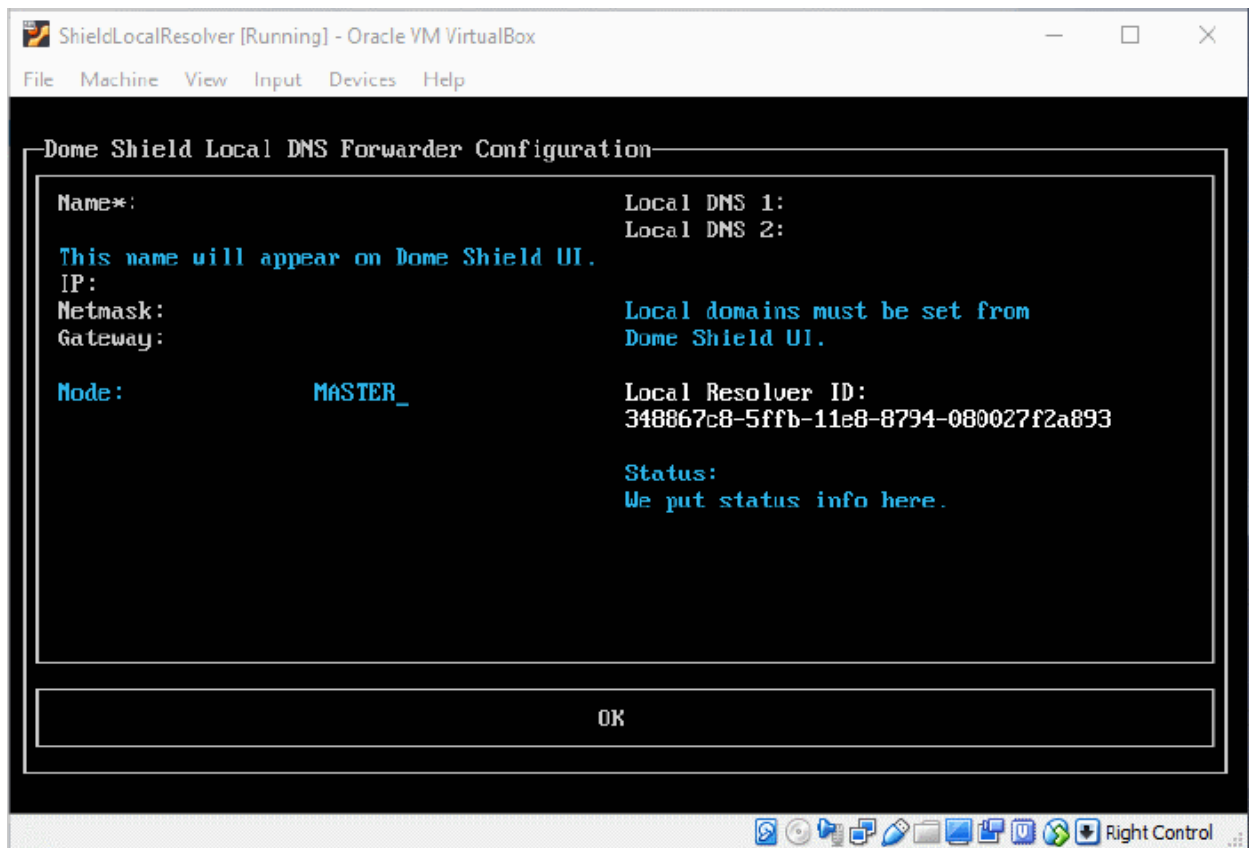
LR Configuration Screen	
Form Element	**Description**
Name	Type a label to identify the master VA. This name will appear in the Dome Shield interface after registration.
IP	Assign an IP address to the local resolver.
Netmask	Enter the LR netmask
Gateway	Enter the IP address of the network gateway.
Mode	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 Dome Shield. 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 will be saved.
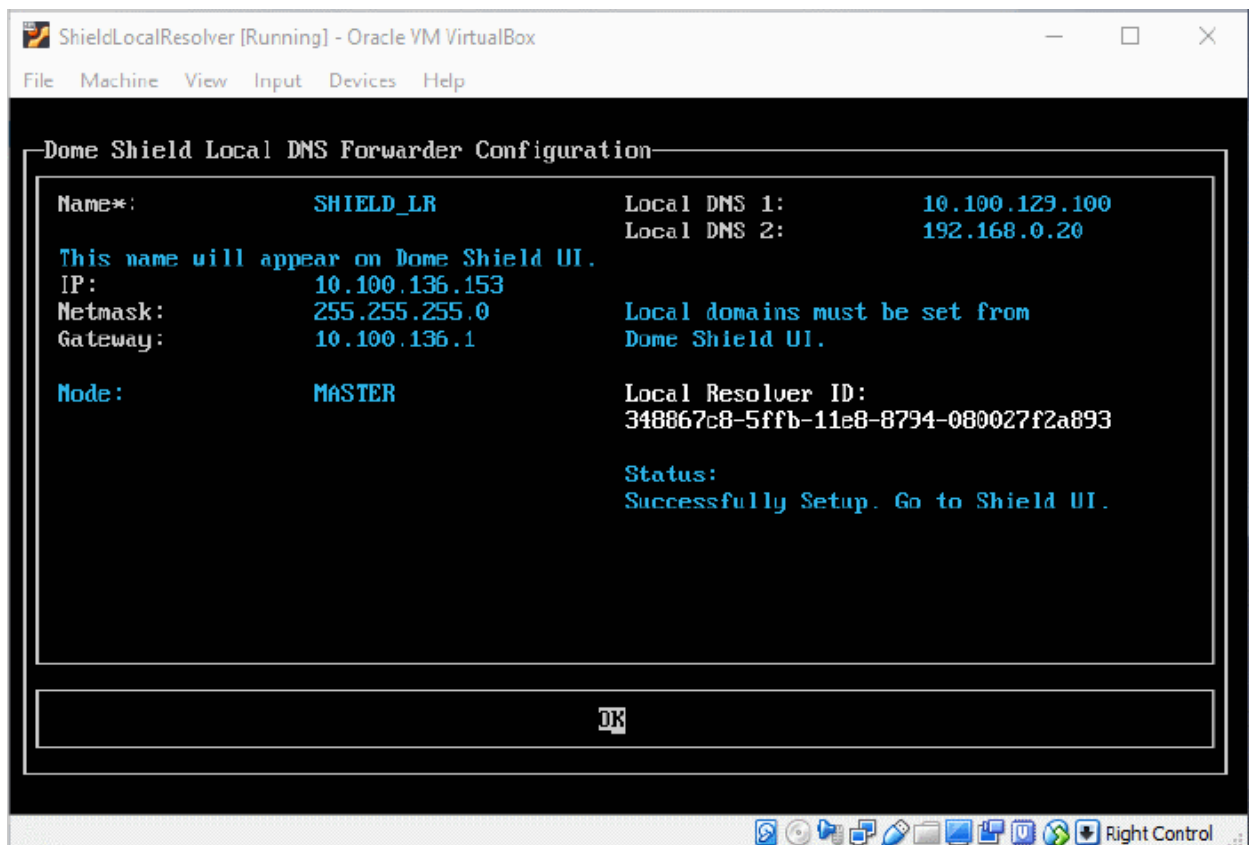
The next step is to register the LR with Dome Shield.

Step 3 - Register the Master VA

- Login to Dome Shield
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Register Component'
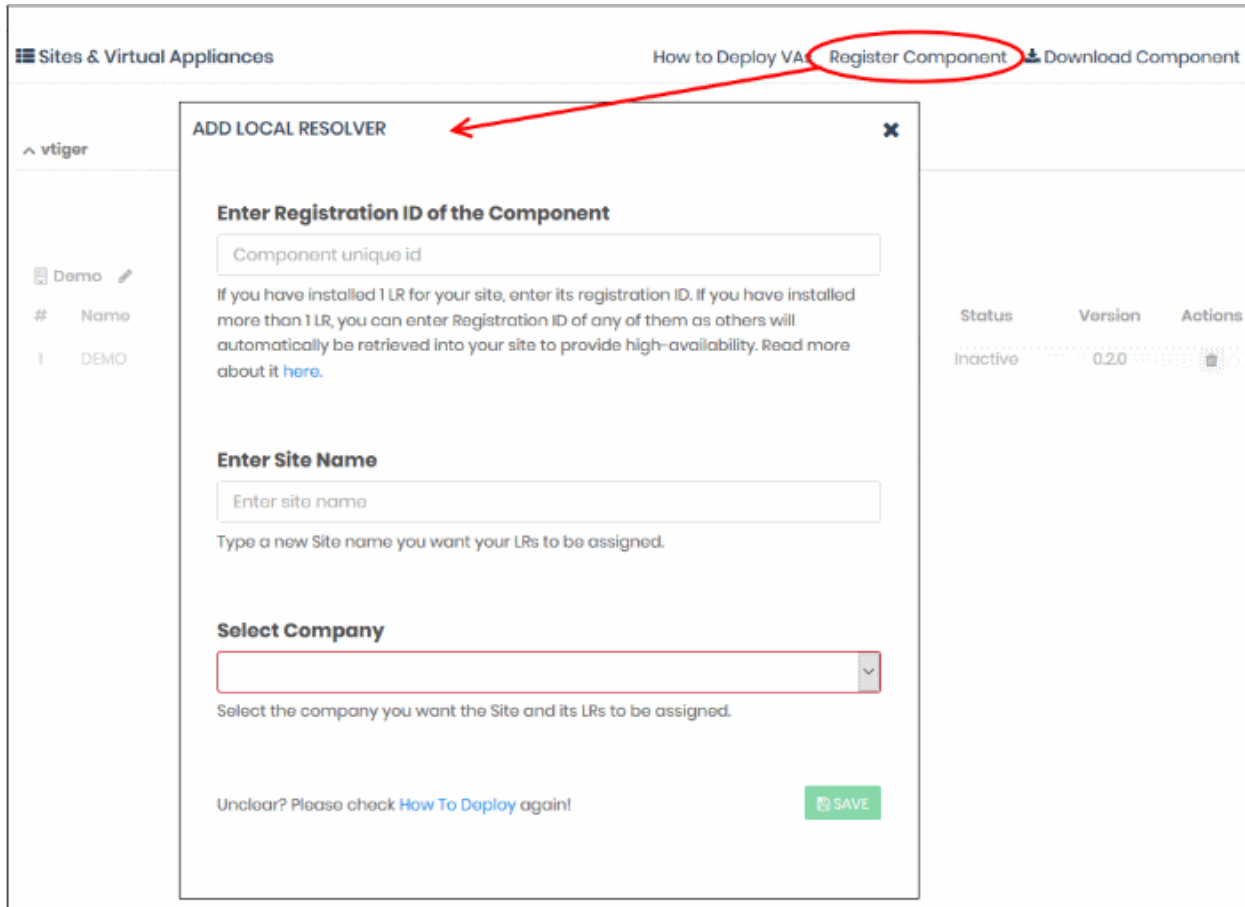
The 'Add Local Resolver' dialog will appear.

'Add Local Resolver' dialog - Table of Parameters	
Form Element	**Description**
Enter Registration ID of the Component	The local resolver ID 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 Dome Shield interface.
Select Company	Only available for MSP customers. • Choose the customer company 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:
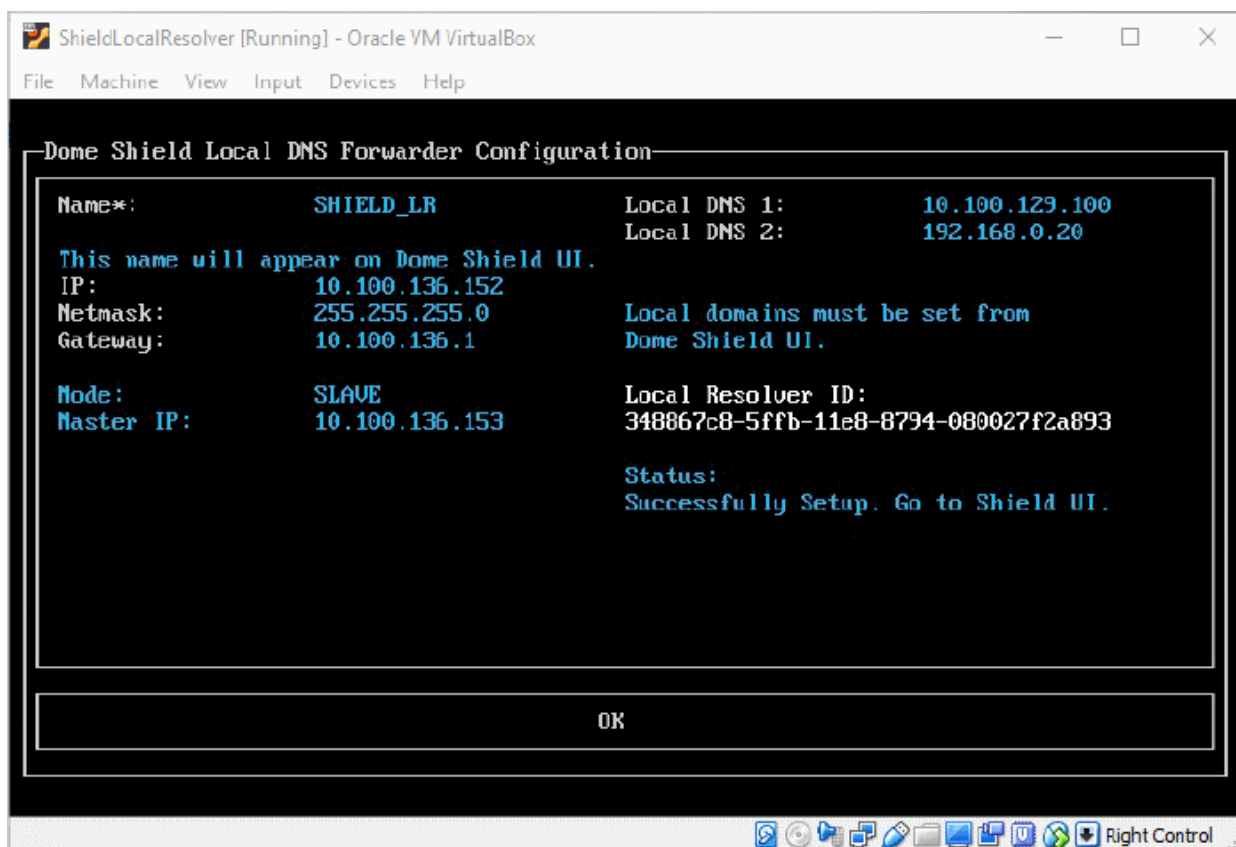
| LR Configuration Screen - Table of Parameters	
Form Element	**Description**
Name	Type a label to identify the slave VA.
IP	Assign an IP address to the local resolver.
Netmask	Enter the LR netmask
Gateway	Enter the IP address of the network gateway.
Mode	Select 'Slave'
Master IP	Appears after choosing '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 Dome Shield. 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 will be saved. The Local Resolver will be automatically registered as 'Slave' to the pre-registered 'Master' LR.

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 mobile/roaming devices, create security policies, analyze statistics 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.
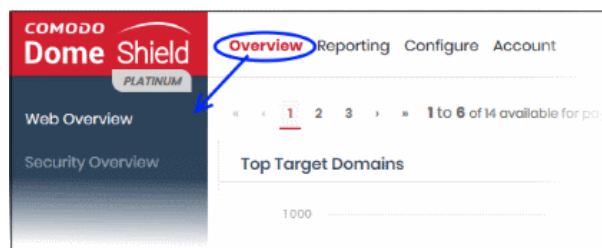
Reporting - View reports on threats detected on your assets, security trends, web browsing trends and more. You can choose from a range of pre-configured reports or create a custom report.

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

See '**Reports**' for more details.

Configure - Add networks and individual endpoints to Dome Shield 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, Roaming and Mobile Devices**' for more details.

- **Security Rules** - Create and manage rules to block websites which host specific types of threat. 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.

- **Networks** - Add and manage protected networks. See '**Add Networks to Dome Shield**' for more details.

- **Roaming Devices** - Add and protect roaming devices outside your network. See '**Add Roaming Endpoints to Dome Shield**' for more information.

- **Mobile Devices** - Add and protect Android and iOS devices. See '**Add Mobile Devices to Dome Shield**' for more details.

- **Sites & Virtual Appliances** - Add networks by configuring local resolver virtual machines. See **Import Sites to Dome Shield by Deploying Local Resolver Virtual Appliances** for more details.

  - **Internal Networks** - Add single internal IPs or 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
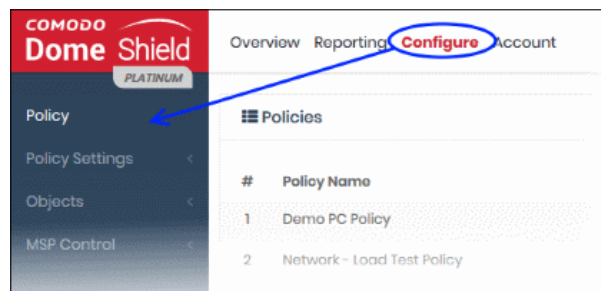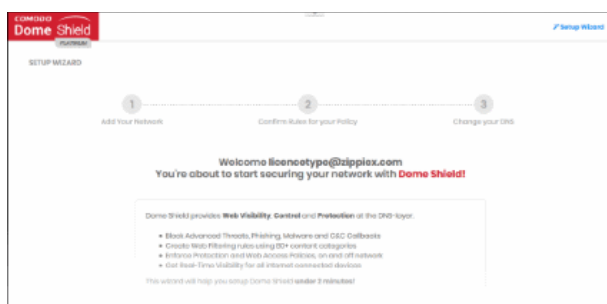
available for MSPs only. See '**View Protection Details by Customer**' for more information.
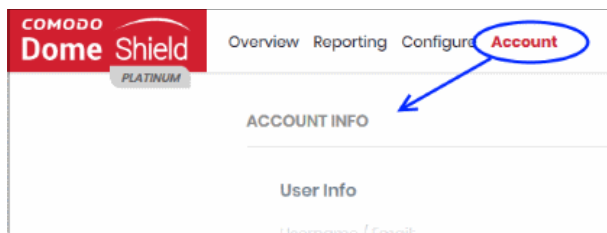
Account – View your account details and keep track of DNS requests. See '**View Account Details**' for more information.

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.

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 Shield 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 Shield to your friends. Also provide your valuable suggestions to improve the product.
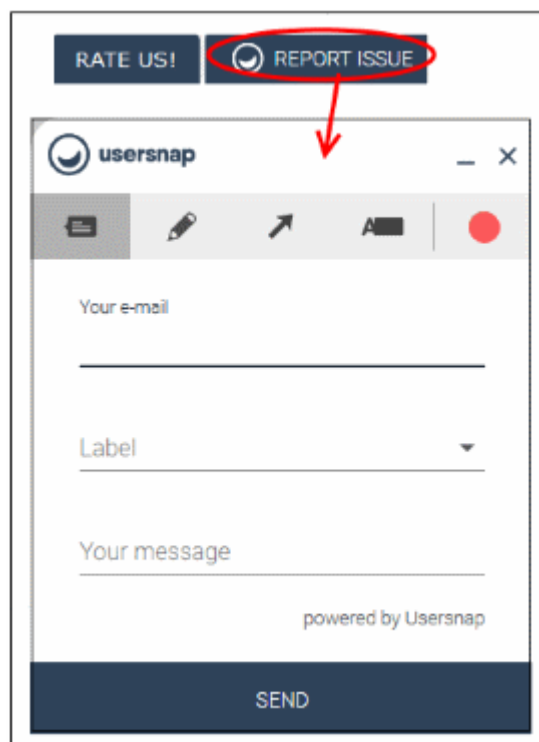
3   The Dashboard

- Click 'Overview' in the top-menu to open the dashboards.

The dashboard is an 'at-a-glance' summary of your security posture under Dome Shield. Using a range of statistics and charts, the dashboard shows vital information about your policy deployment and allows you to drill-down to further areas of interest. Charts include overall web browsing trends, roaming devices, overall security trends, top URL categories, top visited domains and top blocked domains.

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.
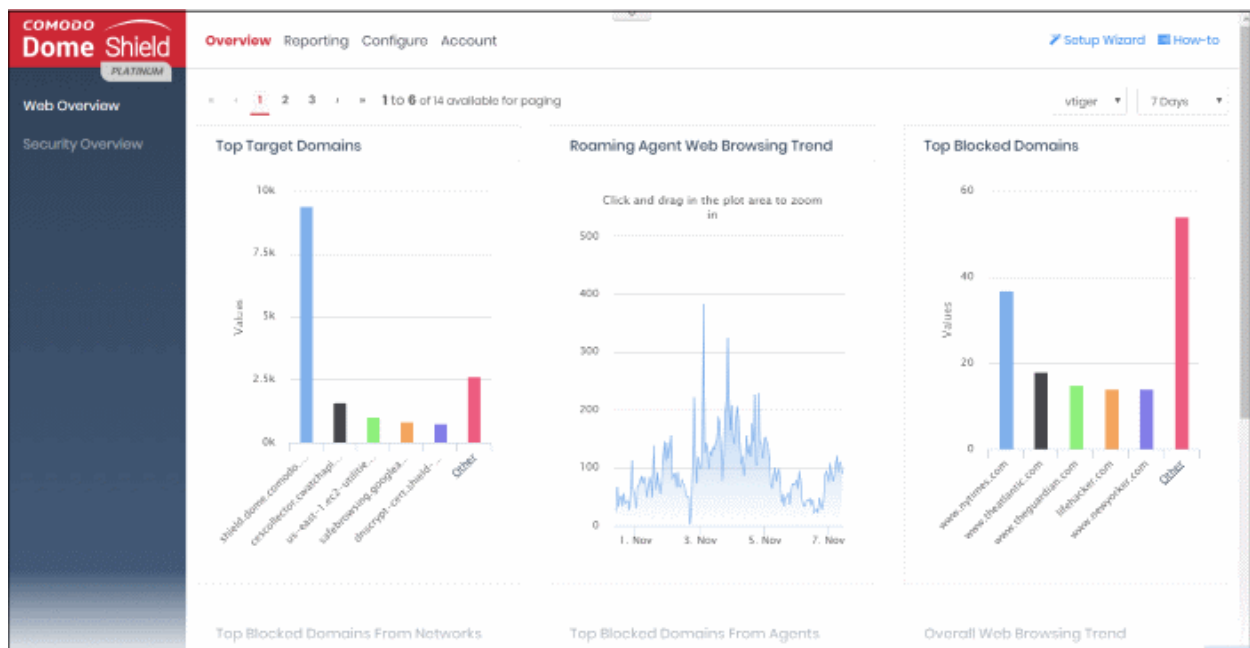
MSP customers can view statistics for particular customers. Possible data ranges are from the last 12 hours to the previous 7 days.
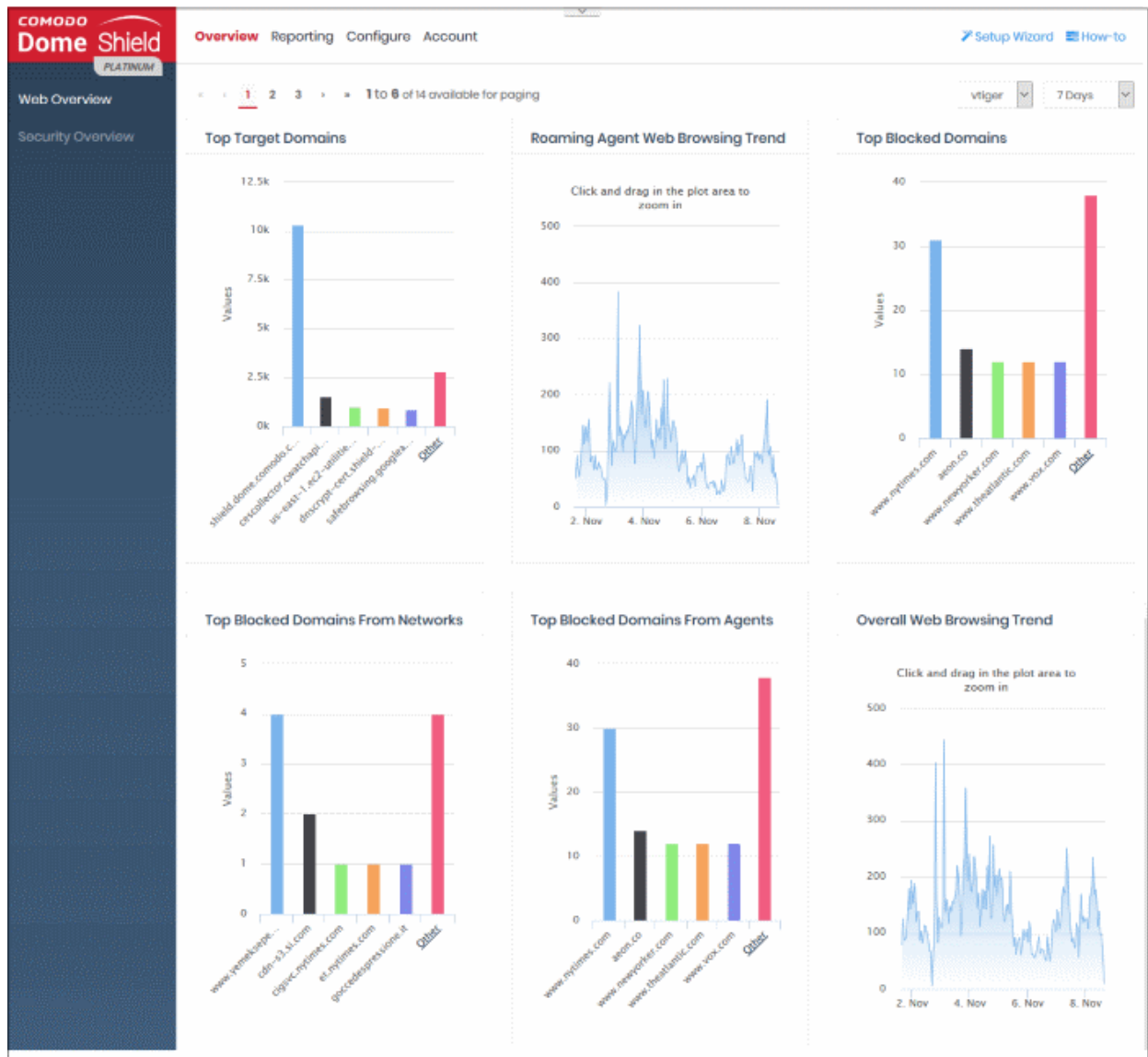
The following sections explain more about:

- **Web Overview**
- **Security Overview**
- **Viewing Logs from Dashboard**

3.1 Web Overview

The 'Web Overview' contains data on browsing activity and domains blocked on 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**

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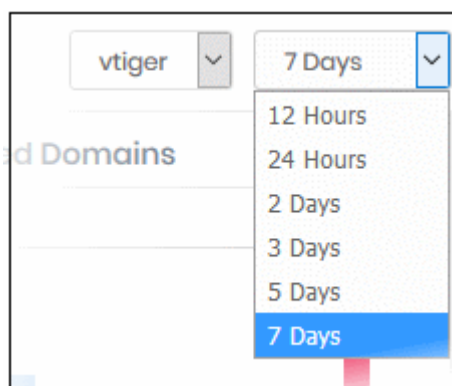
Top Target Domains

Shows the websites which were most often visited by users in enrolled networks. Results are displayed for the top 10 domains.

- The X-axis displays the name of the domain. The Y-axis displays the number of requests from endpoints in your network(s) or roaming devices.
- Place your mouse cursor over a bar to view further details.
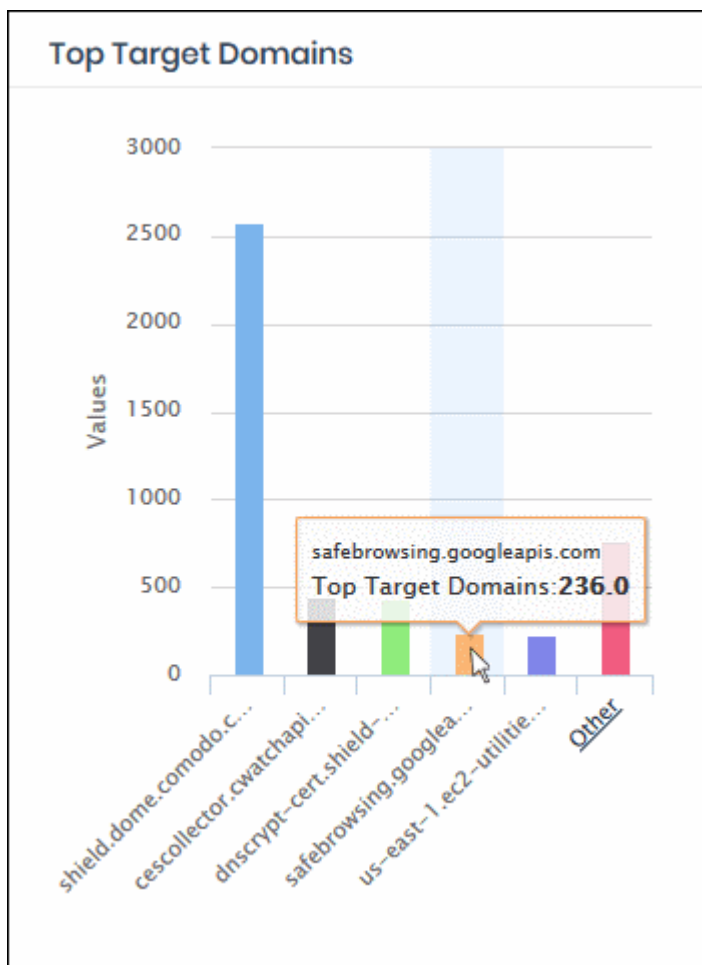
• By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.
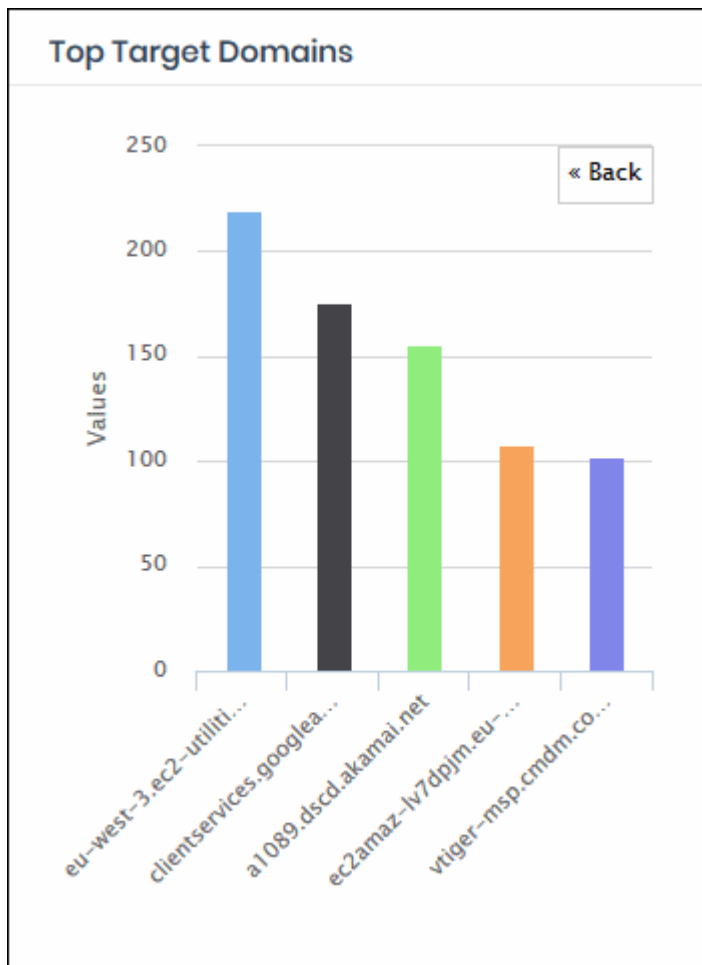
- Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See '**View Logs**' for more details.

Roaming Agent Web Browsing Trend

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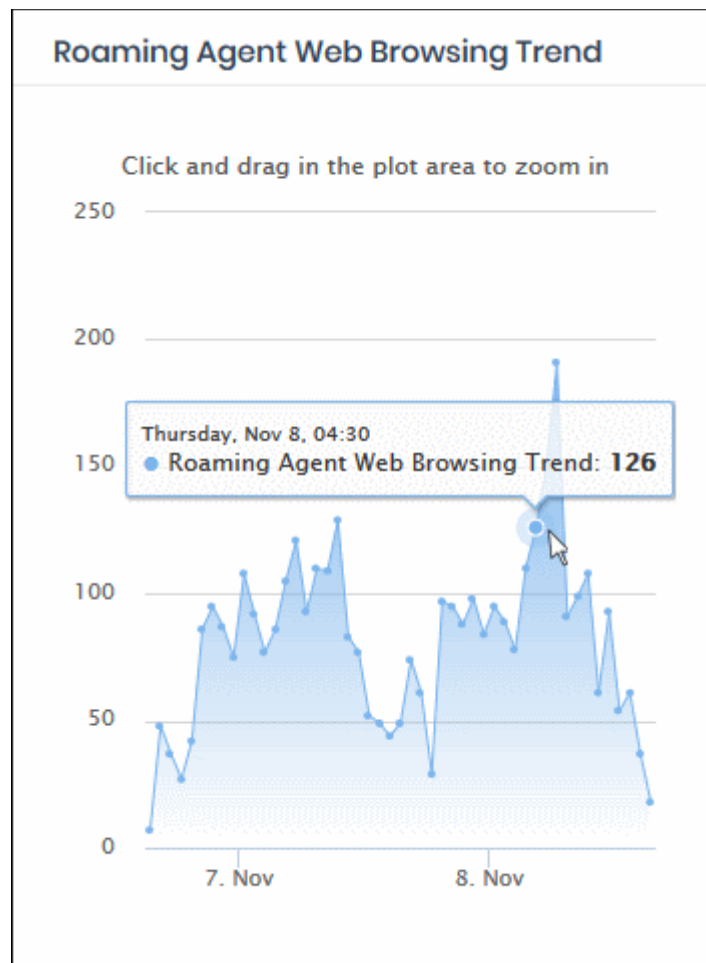
- Click and drag on the chart to zoom into a particular time period.
  - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See '**View Logs**' for more details.

Top Blocked Domains

Shows those websites that were most often blocked by your security policies. The results are displayed for the top 10 blocked domains.

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

- By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.
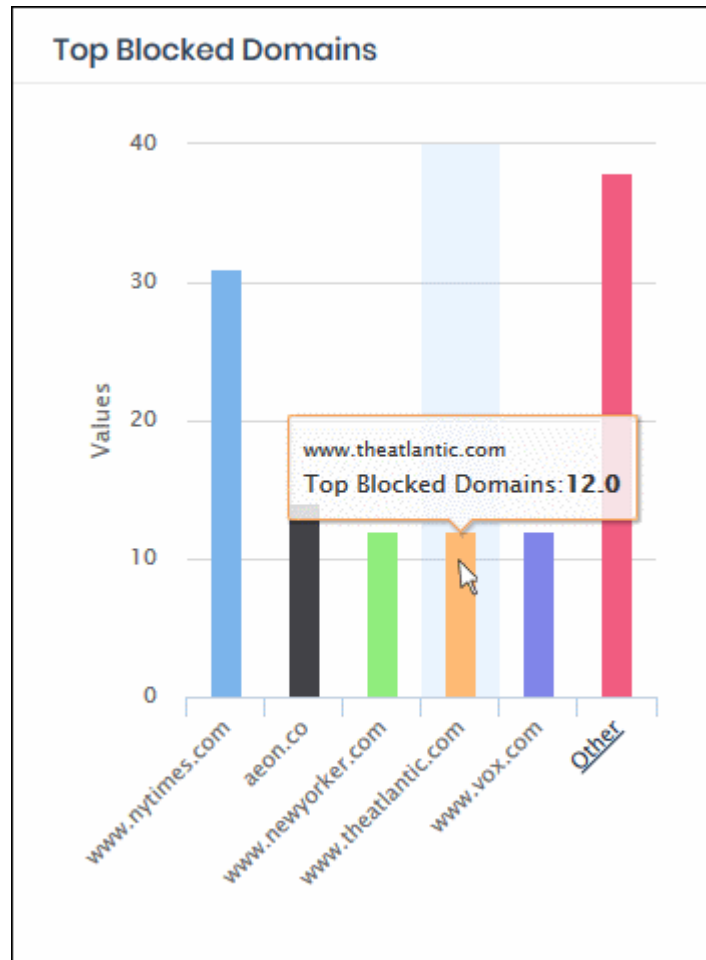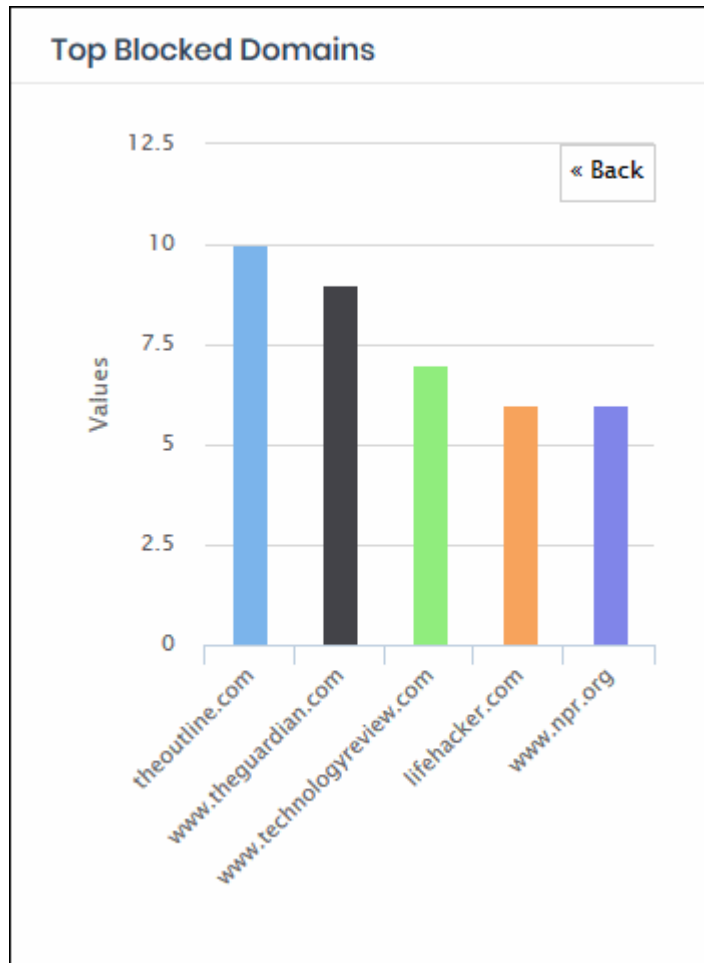
- Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See '**View Logs**' for more details.

Top Blocked Domains from Networks

Shows the websites that were most often blocked for endpoints in your networks. Results are displayed for the top 10 domains.

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

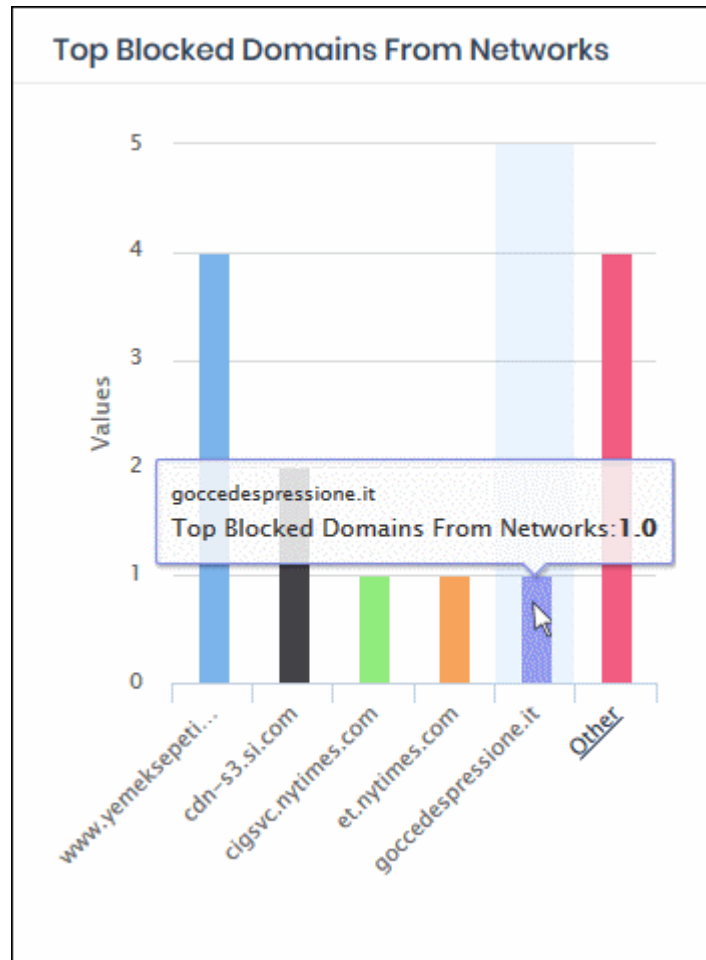• By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.

- 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.
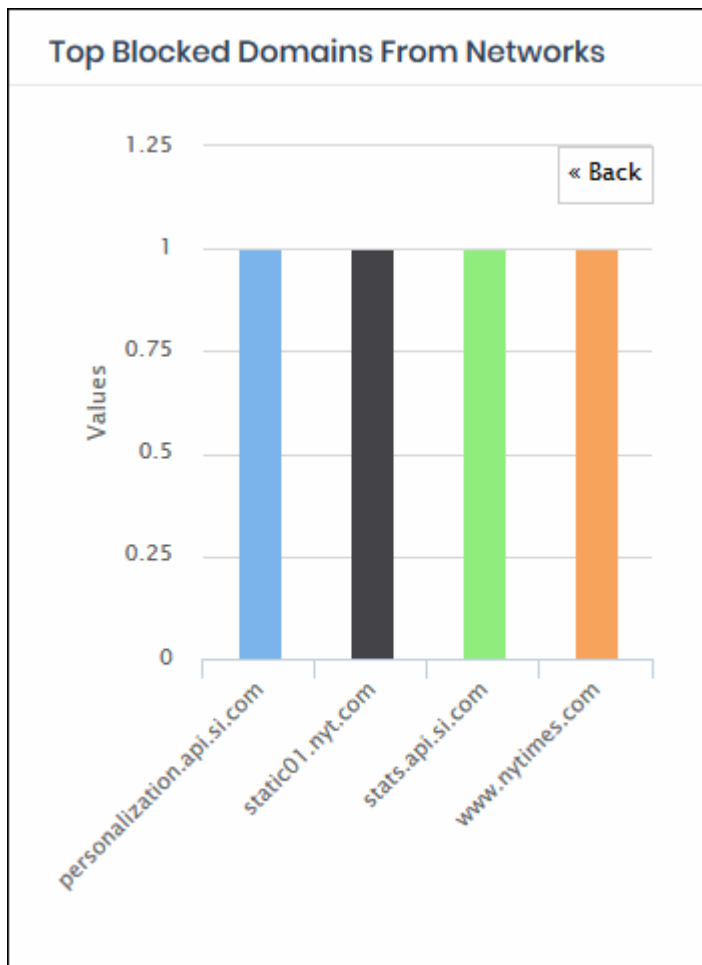
Top Blocked Domains from Agents

Shows the websites that were most often blocked for your roaming devices. Results are displayed for the top 10 domains.

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

- By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.
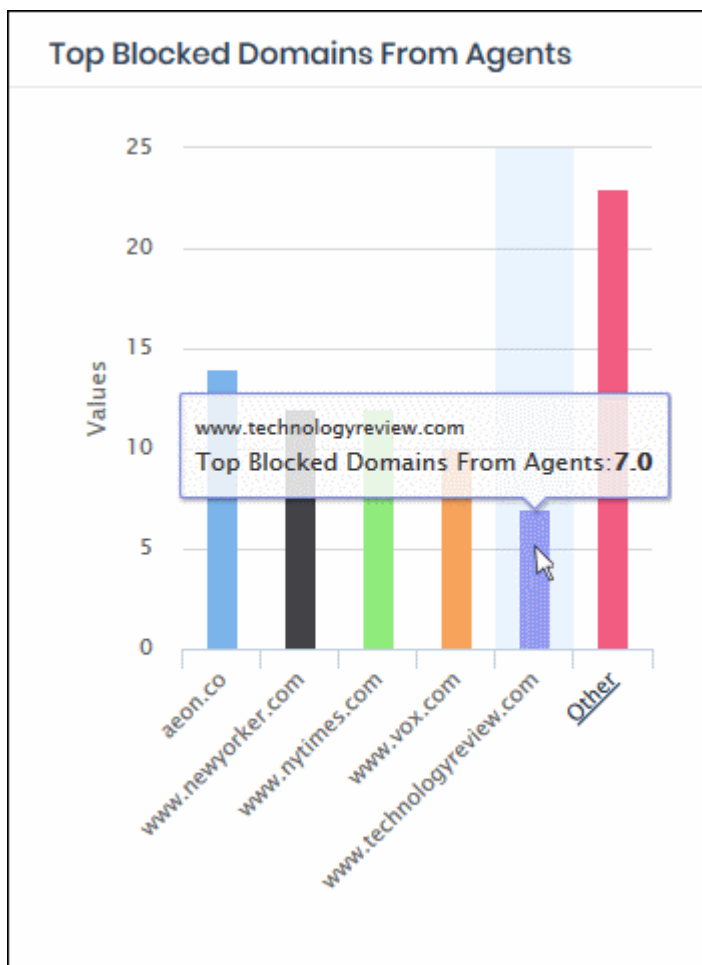
- Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See '**View Logs**' for more details.
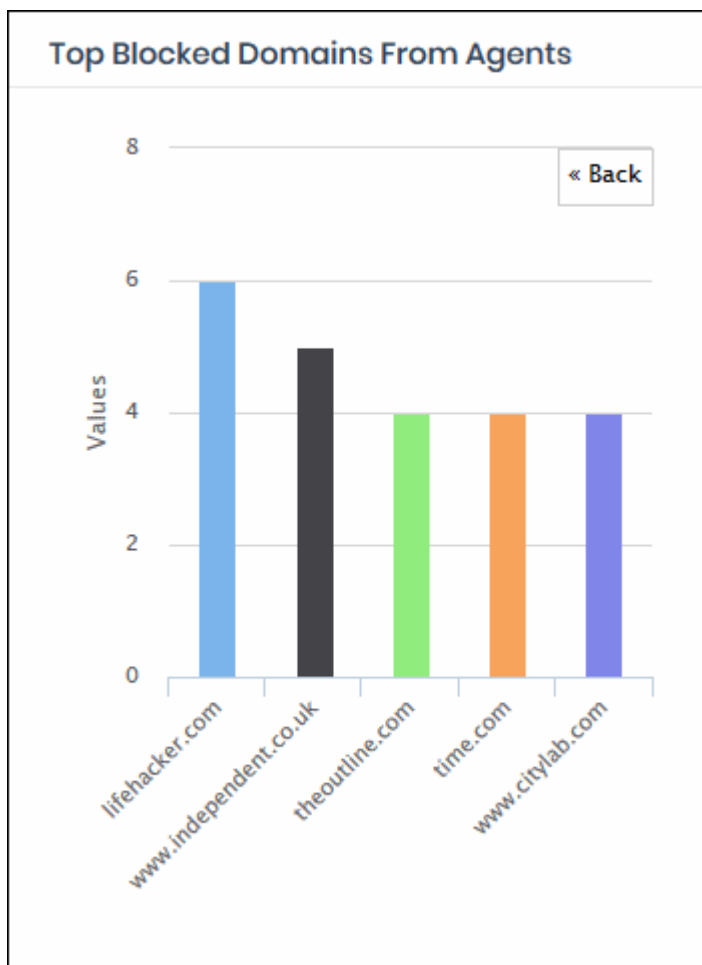
Overall Web Browsing Trend

Shows the number of domain access requests from all protected network(s) 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.
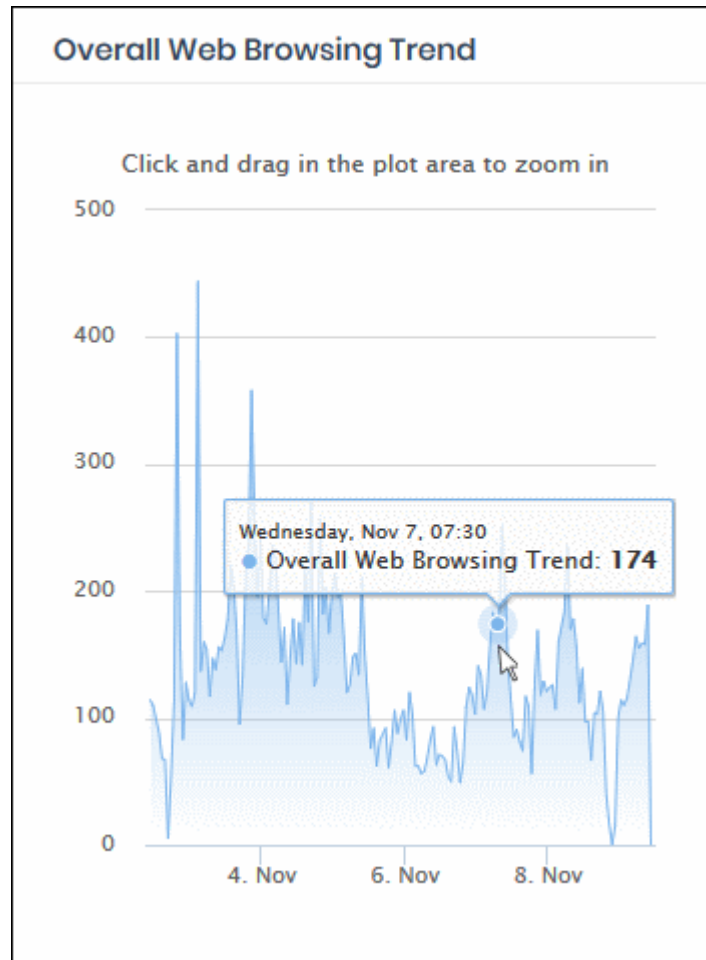
- Click and drag on the chart to zoom into a particular time period.
  - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See '**View Logs**' for more details.

Overall Security Trend

Shows the number of harmful sites blocked on your network(s) and endpoints based on security rules 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.
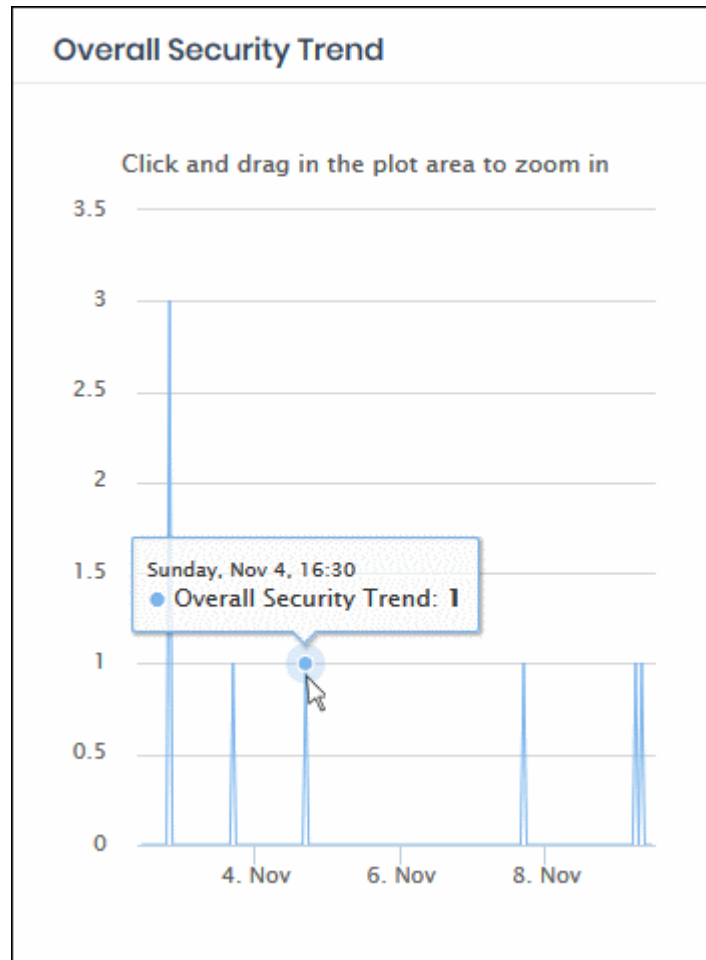
- Click and drag on the chart to zoom into a particular time period.
  - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See '**View Logs**' for more details.

Top 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..

Comodo **Dome Shield** - Admin Guide
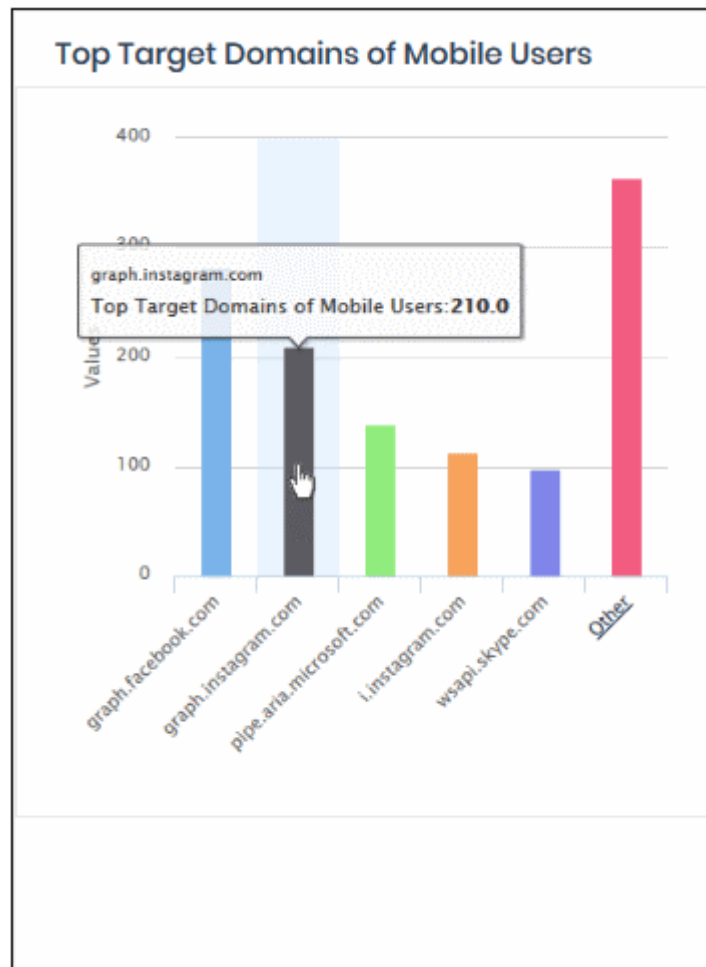
COMODO
Creating Trust Online®
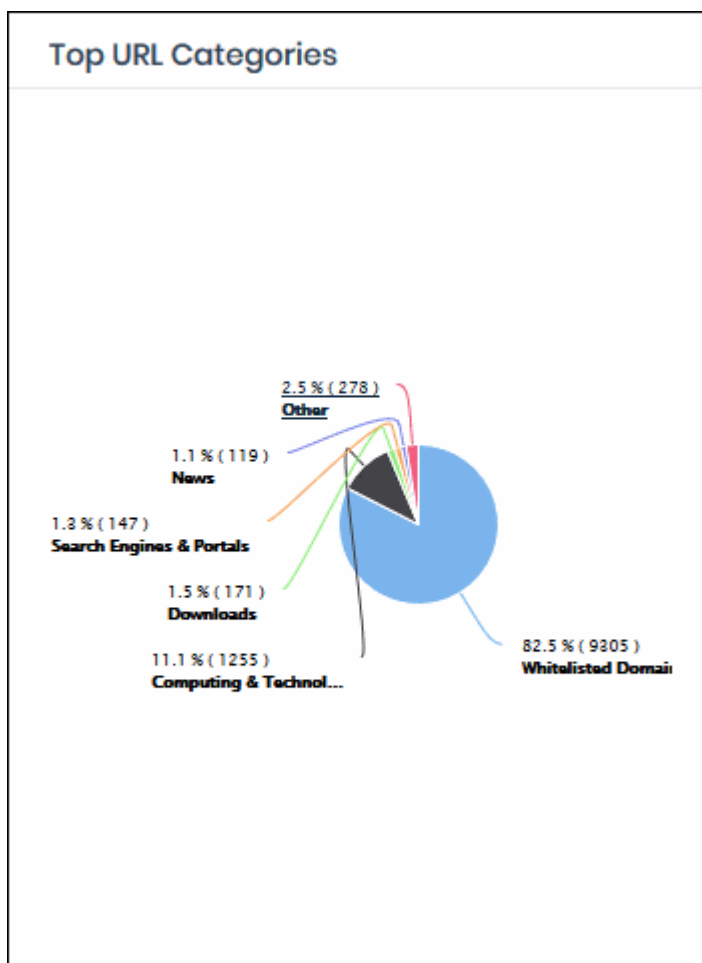
Top Target Domains of Mobile Users

Shows websites which were most often visited by mobile users in your organization. Results are available for the top 10 domains.

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

Comodo Dome Shield - Admin Guide | © 2018 Comodo Security Solutions Inc. | All rights reserved.   48

- By default, the chart shows the top five domains. Click 'Other' on the right to view the next five domains.
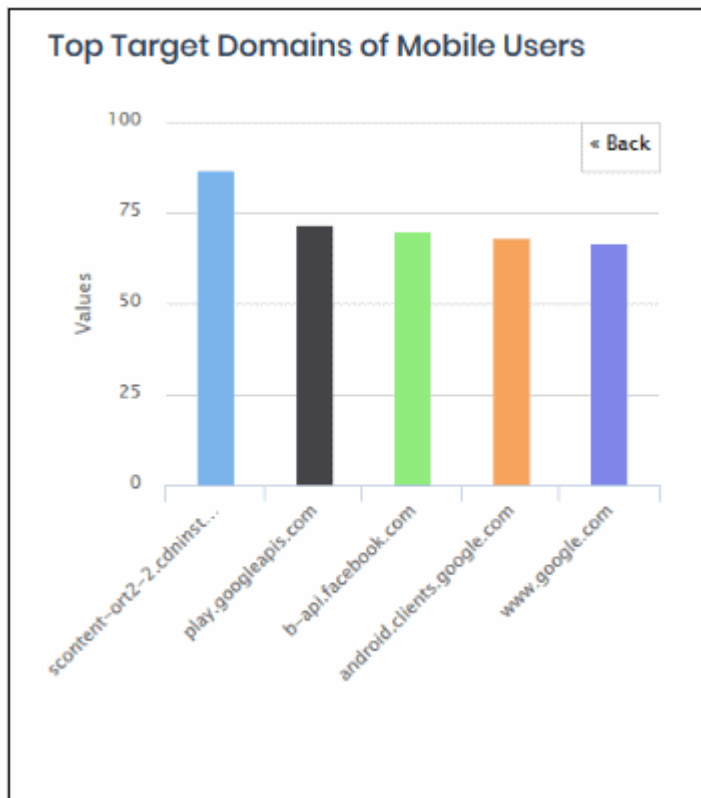
- Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See '**View Logs**' for more details.

Web Traffic of Mobile Users

Displays 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.
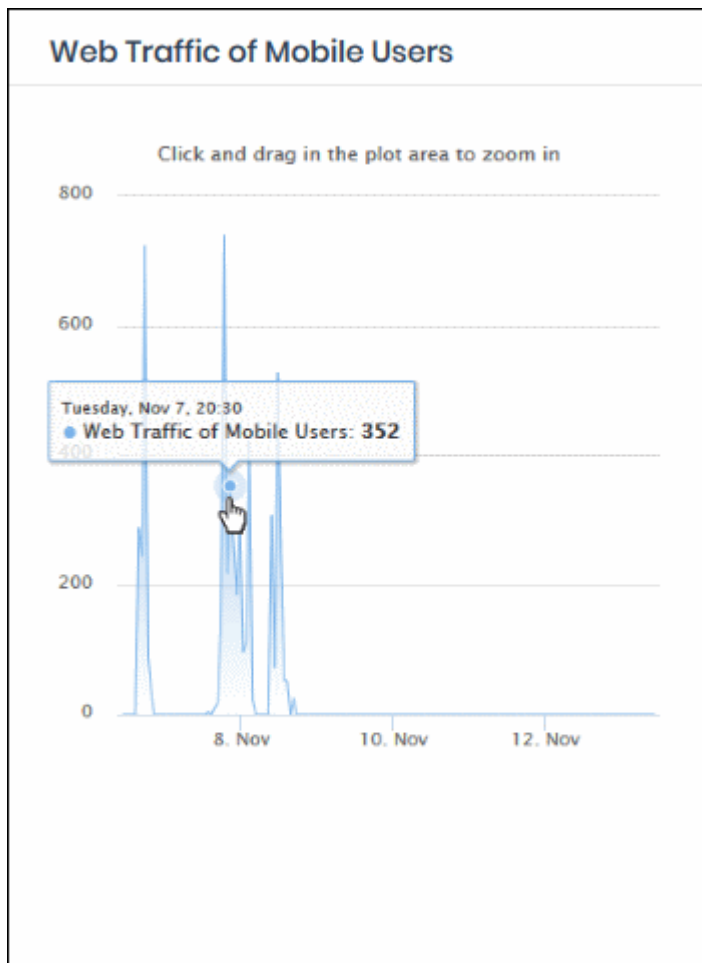
- Click and drag on the chart to zoom into a particular time period.

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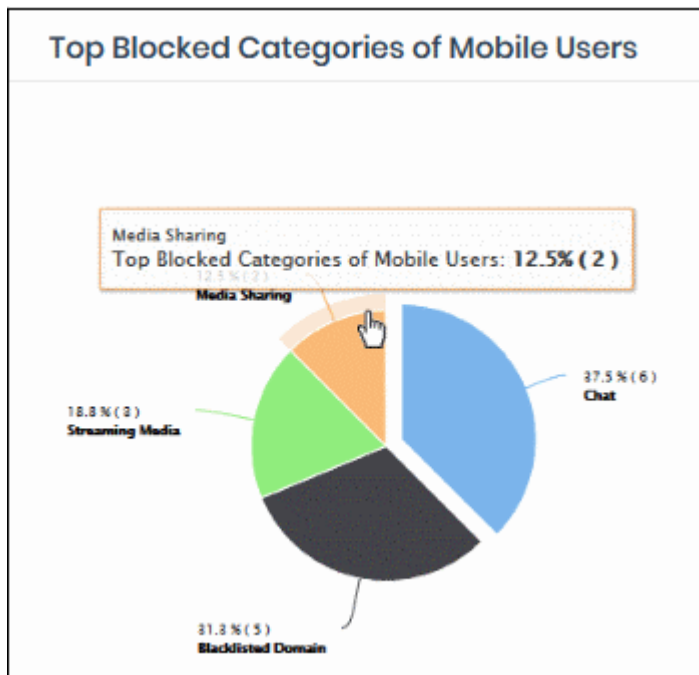
- Click on a sector to see a log of blocked categories for mobile users. See '**View Logs**' for more on this.

**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.
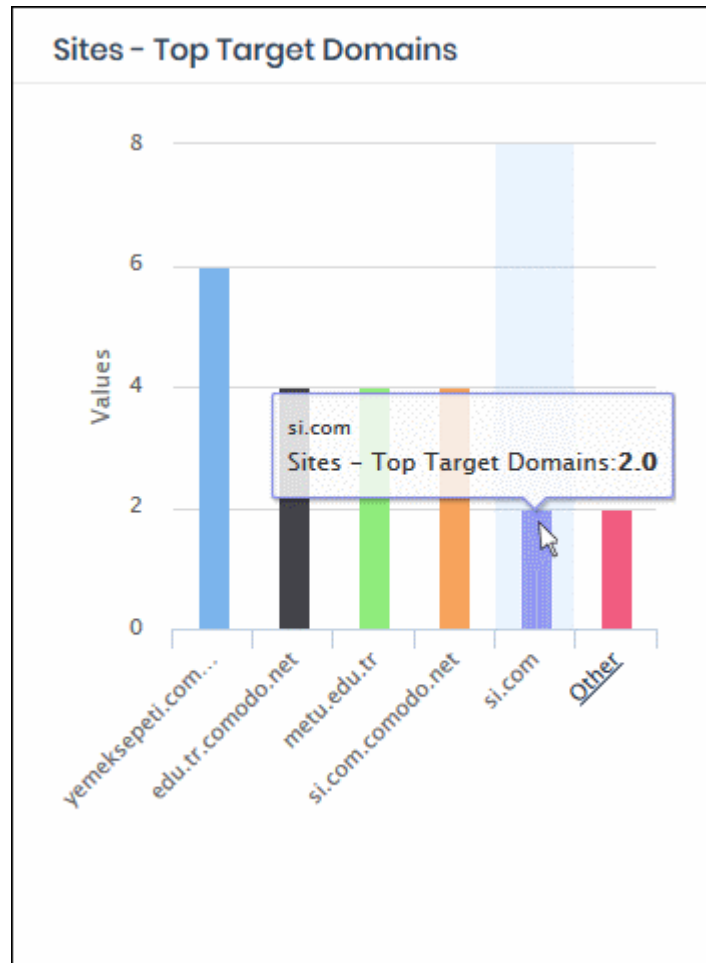
- By default, the chart shows top five domains. Click 'Other' on the right to view the next five domains.
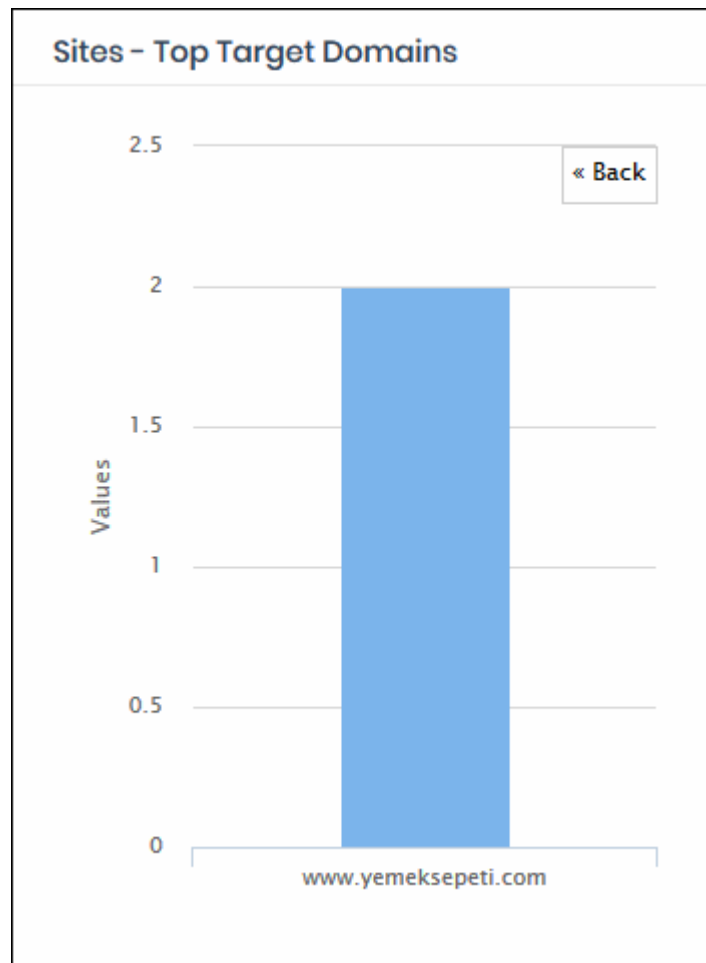
- Click 'Back' to return to the original view.
- Click on a chart bar to view domain request logs. See '**View Logs**' for more details.

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.
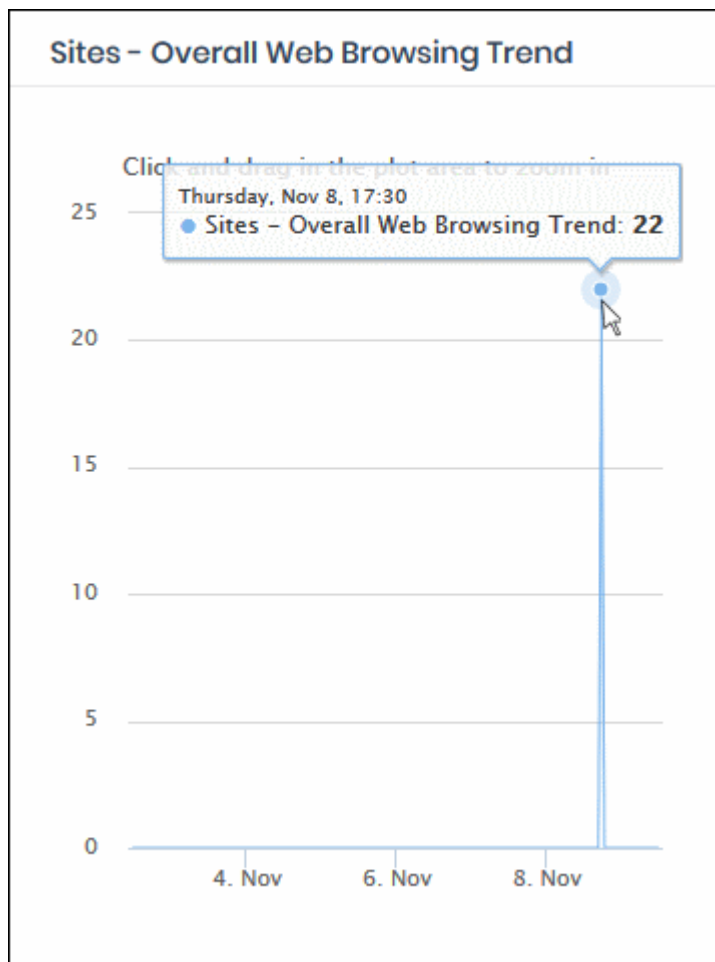
• Click and drag on the chart to zoom into a particular time period.

    • 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 blacklisted domains that were most often blocked by category rules in imported network sites.

• Place your mouse cursor over a sector to view further details.
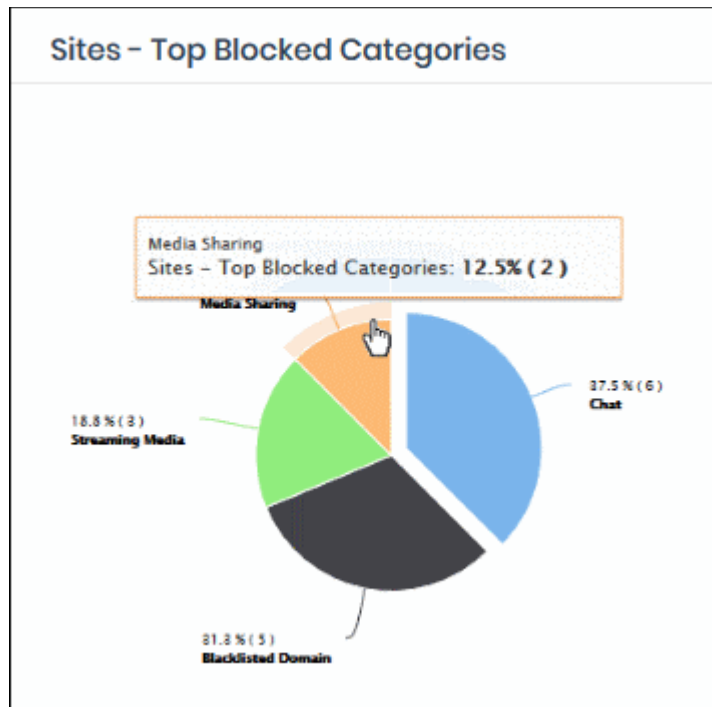
- Click on a sector to see a log of blocked categories. See '**View Logs**' for more on this.

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 'Security Overview' dashboard contains the following tiles:

- **Roaming Agent Security Incidents**
- **Overall Advanced Threats**
- **Roaming Agent Advanced Threats**

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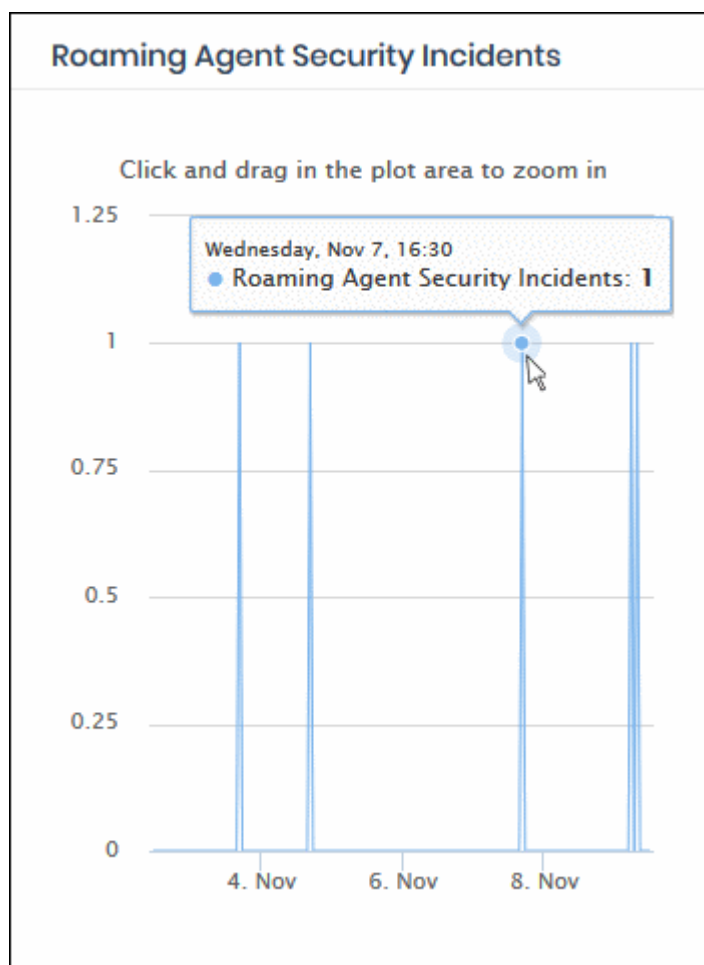
- Click and drag on the chart to zoom into a particular time period.
    - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See '**View Logs**' for more details.
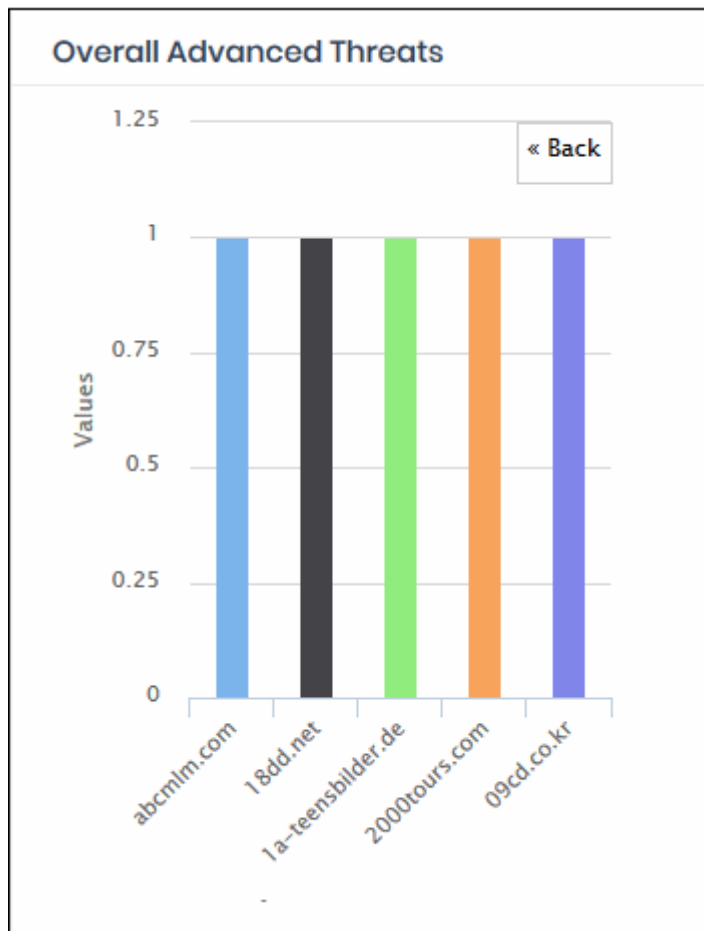
Overall Advanced Threats

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

- The X-axis displays the name of the domain. The Y-axis displays the number of requests from endpoints in your network(s) or roaming devices.
- Place your mouse cursor over a bar to view further details.
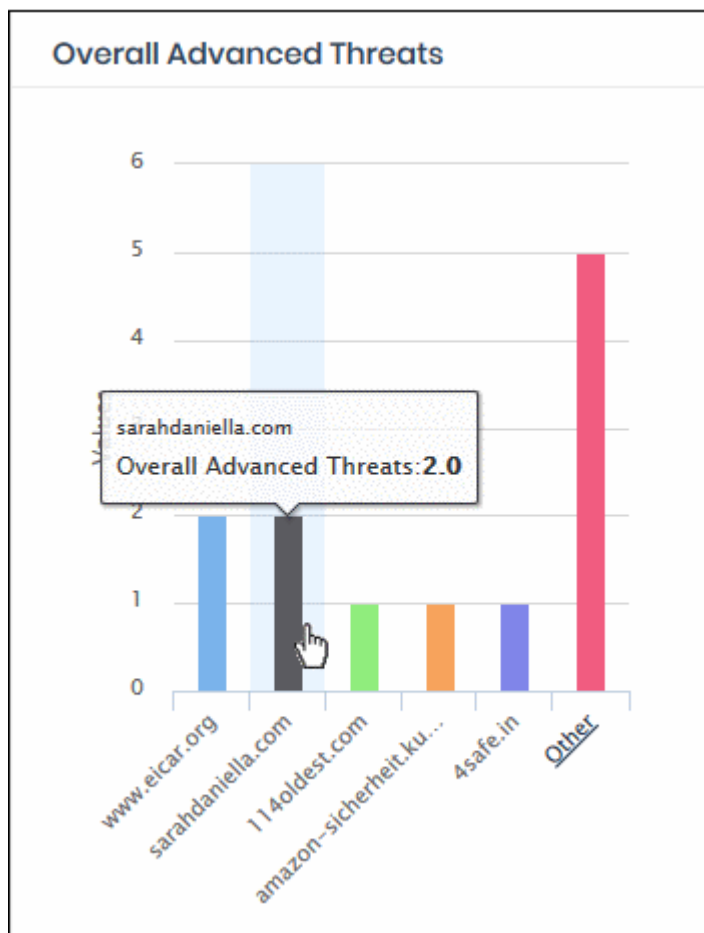
- By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.

- 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.

Roaming Agent Advanced Threats

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

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

- By default, the chart shows top five domains. Click 'Other' at the right end to view the next five domains.
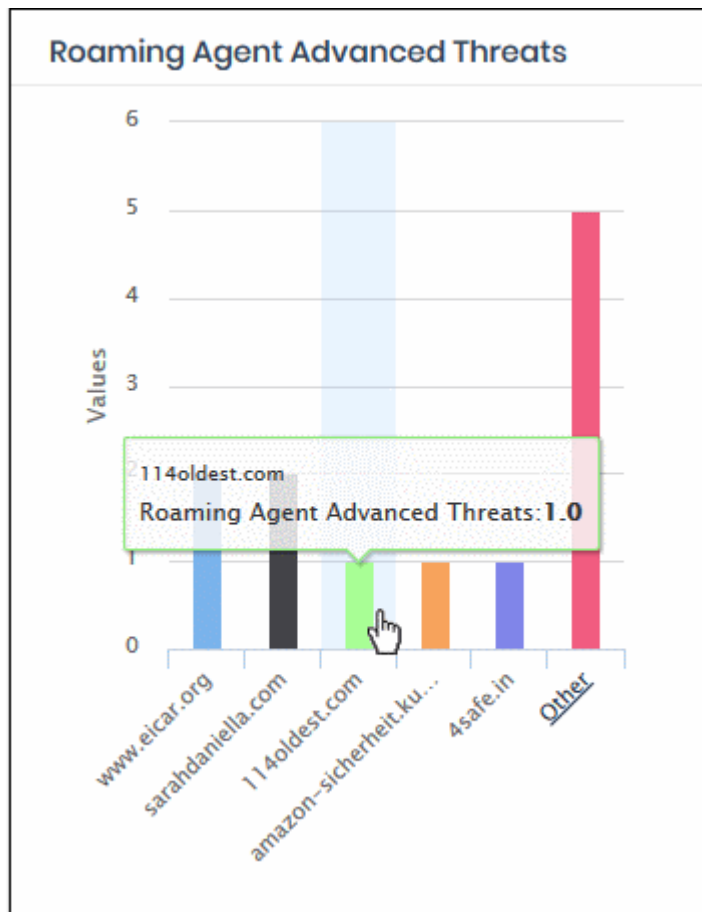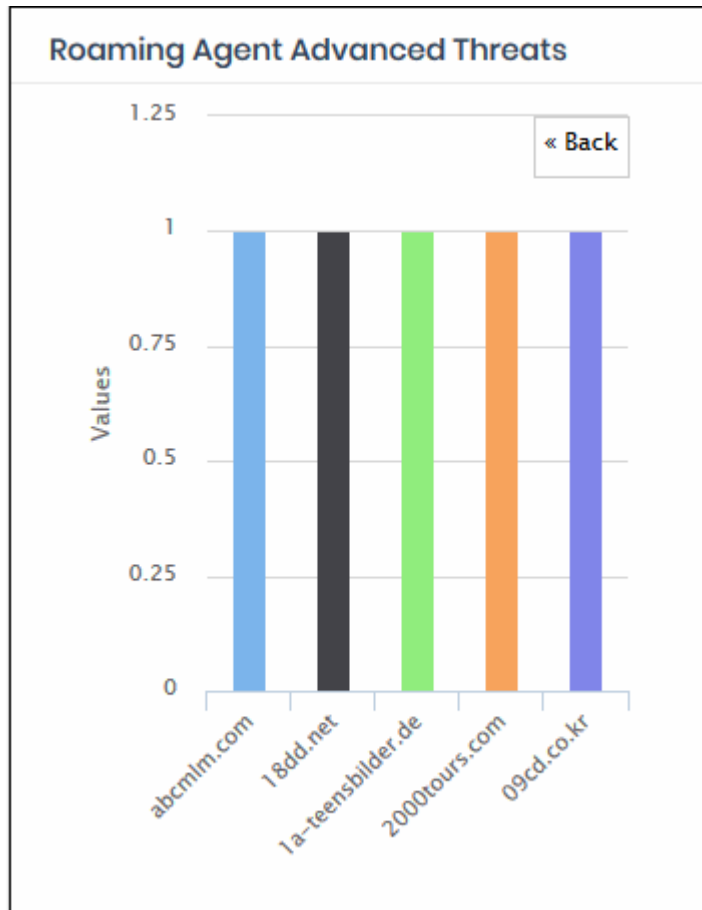
- Click 'Back' to return to the original view.

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

Overall Security Incidents

Shows the number of incidents in which harmful sites were blocked on your enrolled network(s) and 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.
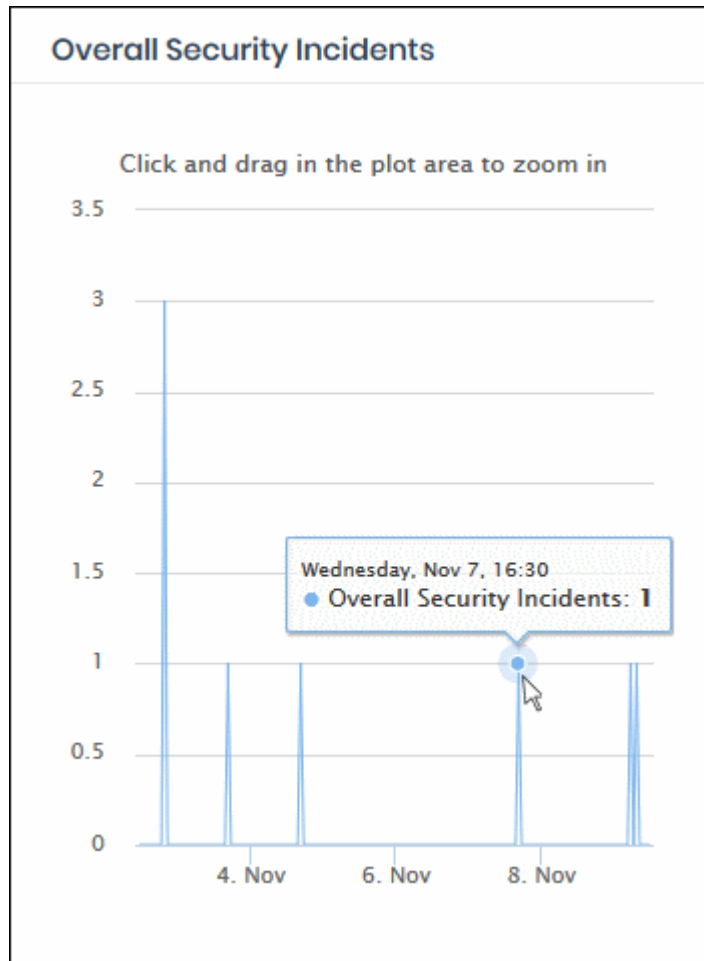
- Click and drag on the chart to zoom into a particular time period.
    - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See '**View Logs**' for more details.

Most Blocked Mobile Threats

Web categories and blacklisted domains most often blocked to mobile users by security rules in 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.
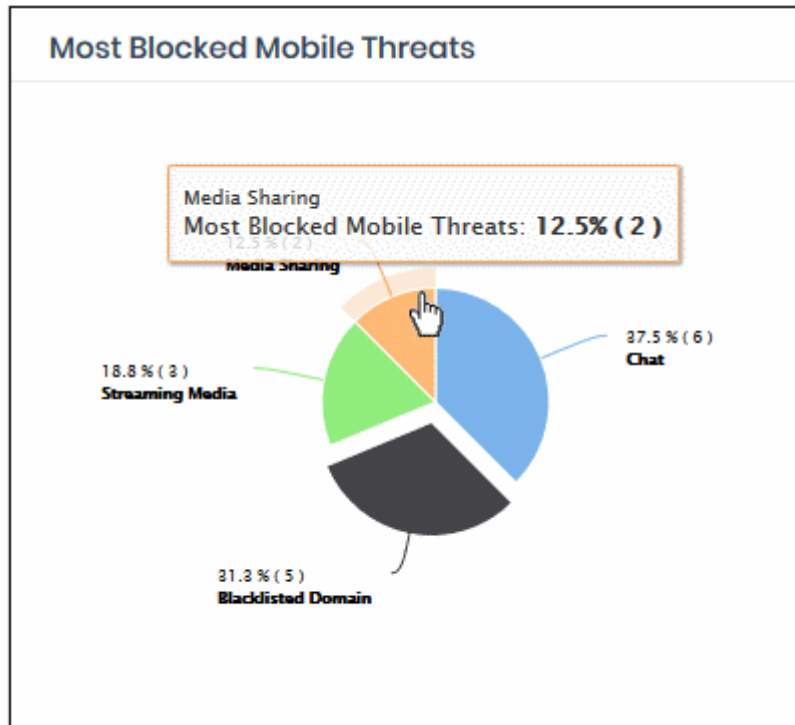
- Click on a sector to see a log of most blocked categories for mobile users. See '**View Logs**' for more on this.

Sites - Most Blocked Threats

Web categories and blacklisted domains 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, spy-ware and drive-by-downloads.

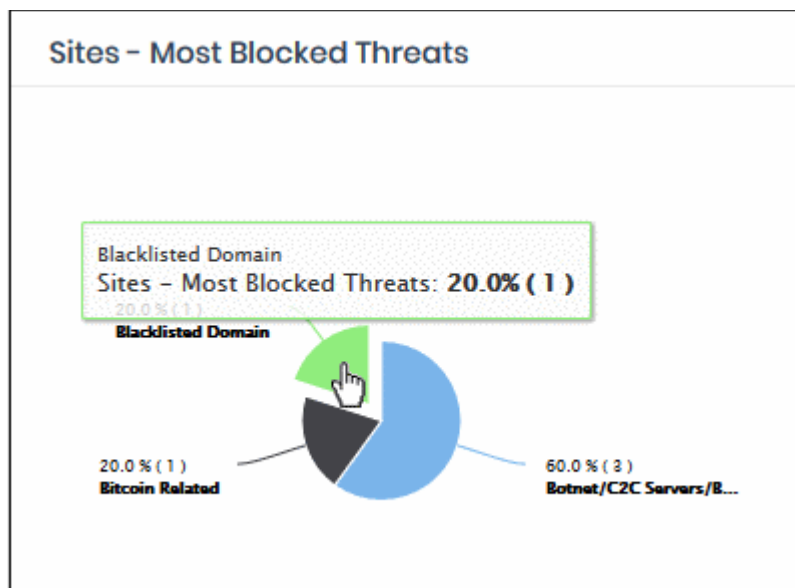- Place your mouse cursor over a sector to view further details.

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

3.3　　View Logs

- You can view logs by clicking on a data item in a dashboard chart. For example, click a specific bar in a bar-chart or a specific point in 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.

To 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:

- The panel on the left allows you to filter by time period and by other parameters.

- The right of the window lists 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 Dome Shield. Can be 'Allowed' or 'Blocked'.
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 Dome Shield.
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:

Choose Time Interval

From	To
2017-08-04 15:30	2017-08-04 16:30

- 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
2017-08-04 15:30	2017-08-04 16:30

Filter Type

Network ✓

- 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

Category ✓

Network	10.108.51.160	🗑
Destination	18xn.com	🗑
Category	Malware	🗑

Q Search

- Click the trash can icon beside a filter to remove it
- To reset the view, delete all filters and click the 'Search' button again.
- Click 'Export as CSV' to download the logs in .csv format.

The following types of logs are available:

Chart Type	Logs Displayed
Web Overview 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 **Security Overview**	• Click on a bar to view the logs of access requests made for the that domain 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.

Roaming Agent Security Incidents Overall Security Incidents	
Web Overview Roaming Agent Web Browsing Trend Overall Security Trend Web Traffic of Mobile Users Sites - Overall Web Browsing Trend **Security Overview** Overall Advanced Threats Roaming Agent Advanced Threats Most Blocked Mobile Threats Sites - Most Blocked Threats	• Click on a point the graph to view the logs of web browsing activities in that period of time 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 was allowed or denied and the reason for the action taken.
Web Overview Top URL Categories Top Blocked Categories of Mobile Users Sites - Top Blocked Categories	• Click on a sector to view logs of access history of domains in that category 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 was allowed or denied and the reason for the action taken.

4 Add Networks, Roaming Endpoints and Mobile Devices to Dome Shield

• Click 'Configure' in the Dome Shield top-menu:
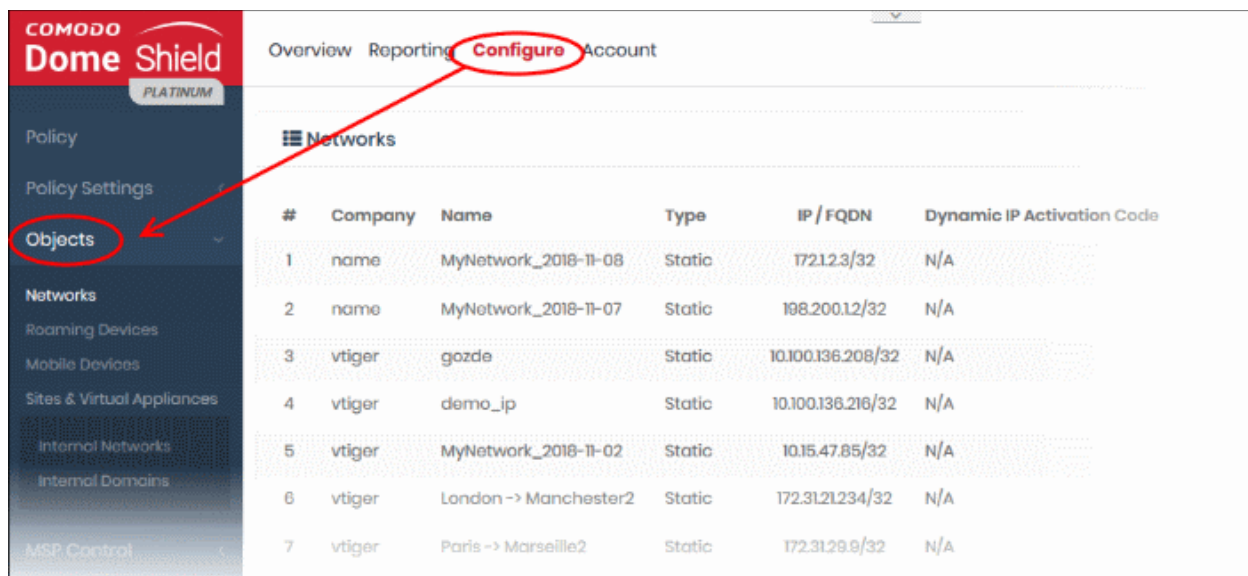
• **Objects** - Manually add networks, roaming and mobile devices to Dome Shield.
   • Alternatively, you can automatically import networks by deploying local resolvers. Click 'Sites and

---

Virtual Appliances' to get started with this method.

- Note. The public IP of the network from which you are connecting will be automatically added during enrollment. This network will become active immediately.

- **Policy Settings** - Configure and apply web protection policies to your added networks/endpoints.

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

See the following sections for help to add networks:

- **Manually Add Networks to Dome Shield**

- **Add Roaming Endpoints to Dome Shield**

- **Add Mobile Devices to Dome Shield**

- **Manage Imported Sites and Local Resolver Virtual Appliances**

4.1   Manually Add Networks to Dome Shield

- Click 'Configure' > 'Objects' > 'Networks' to add, edit and manage protected networks.

- The IP of the network from which you are connecting was automatically added during enrollment. This network is already active.

- Any additional IPs that 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 Dome Shield policies with any address changes in a dynamic network. The agent should be installed on an endpoint in your target network. After you add a network which uses dynamic IPs, Dome Shield 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 Shield 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 Dome Shield. See **Add Networks with Dynamic IP addresses** for more details.
Agents Behavior	Indicates whether the roaming agent is active or not when the roaming device is inside the enrolled network.
Status	Can be 'Active' or 'Pending'. Active networks are available for Dome 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**
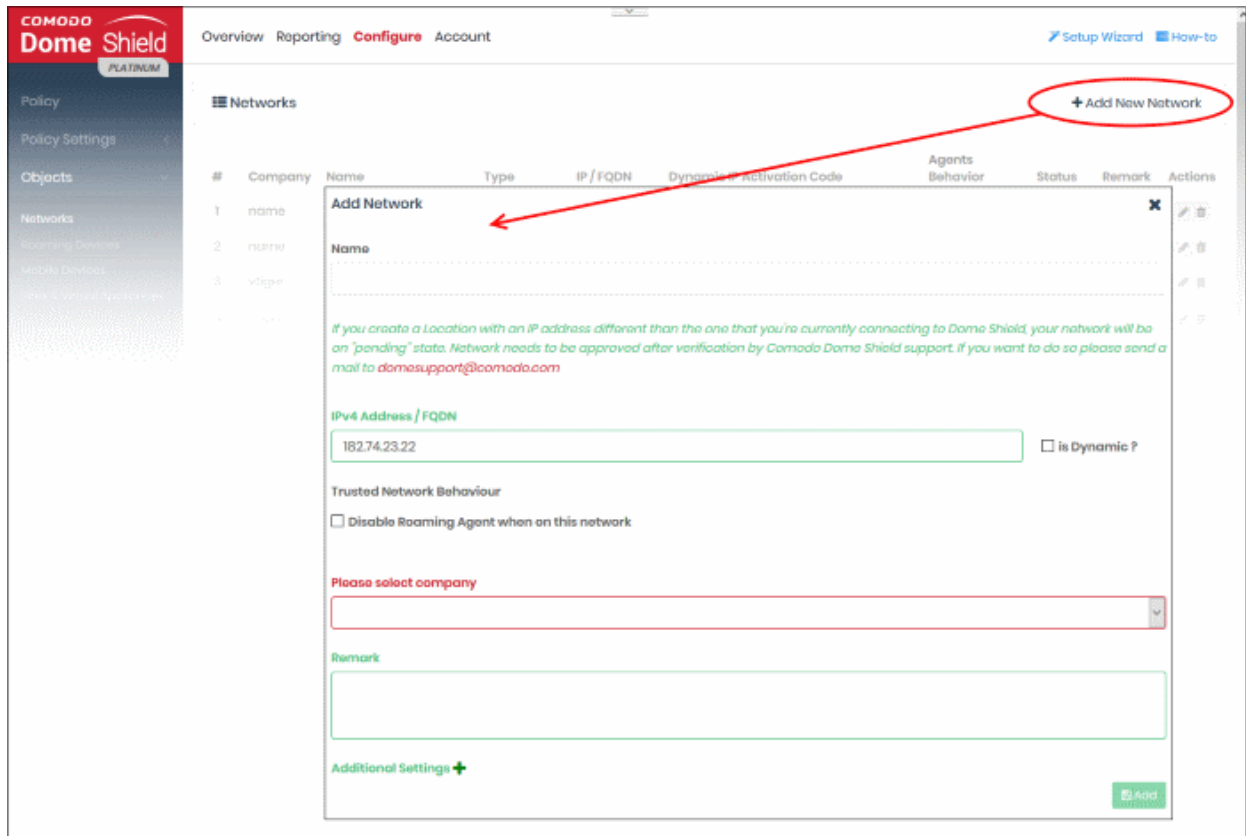- **Edit the details of a network**
- **Delete a network**

Add New Networks

You can add both networks with static IP address(es) and Dynamic Address(es).

- **Add Networks with Static IP Address(es)** - 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 Address(es)** - Download the IP Updater agent from the network setup wizard and install it on a network endpoint. The software will keep Dome Shield and your policies updated with the address of the network. An activation code is generated for each agent which is needed to connect the network to Dome Shield. See **Add Networks with Dynamic IP addresses** for more details.

Add Networks with Static IP Address(es)

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

Add Networks - Form Parameters	
Field	**Description**
Name	Enter an appropriate name for the network
IP Address / FQDN	The IP address or Fully qualified domain name of your network. • Enter the IP address of the network in CIDR (Classless Inter-Domain Routing) notation. • Dome Shield can accept network prefixes from /24 to /32. **Note**: By default, this field will show the public IP address of the network from which you are connecting to Dome Shield. This will automatically become active after initial enrollment. Any new IP address that you add here will remain in pending status until approved by Comodo. Dynamic - Select if you are enrolling a network with dynamic IP addresses. See **Add Networks with Dynamic IP addresses** for more details.
Trusted Network Behavior	Disable Roaming Agent when on this network - applies to roaming devices. • If selected, the Shield agent on devices will be disabled when they are inside the network. The network policy will apply to the roaming device. • If not selected, the roaming device's policy will remain active.
Select Company	Applies to MSPs only. Select the company for which you want to enroll the network.
Remark	Enter any notes about the network being added.

Additional Settings - These settings apply only to roaming devices which have the Dome agent installed.	
	• A roaming device cannot connect to internal hosts when inside the office network. This is because Shield 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 automatically be deployed to your device's host file.
	• See '**Add Roaming Endpoints to Dome Shield**' for more details about how to install Shield agents onto devices and connect to Dome Shield.
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 will be added and displayed in the list.

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

- Change your DNS addresses to following Dome Shield addresses:

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

Please note no rules will be applied to the newly enrolled networks by default. You have to apply a policy to this network according to your requirements. See '**Apply Policies to Networks, Roaming and Mobile Devices**' for advice on how to deploy web protection rules to networks.

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

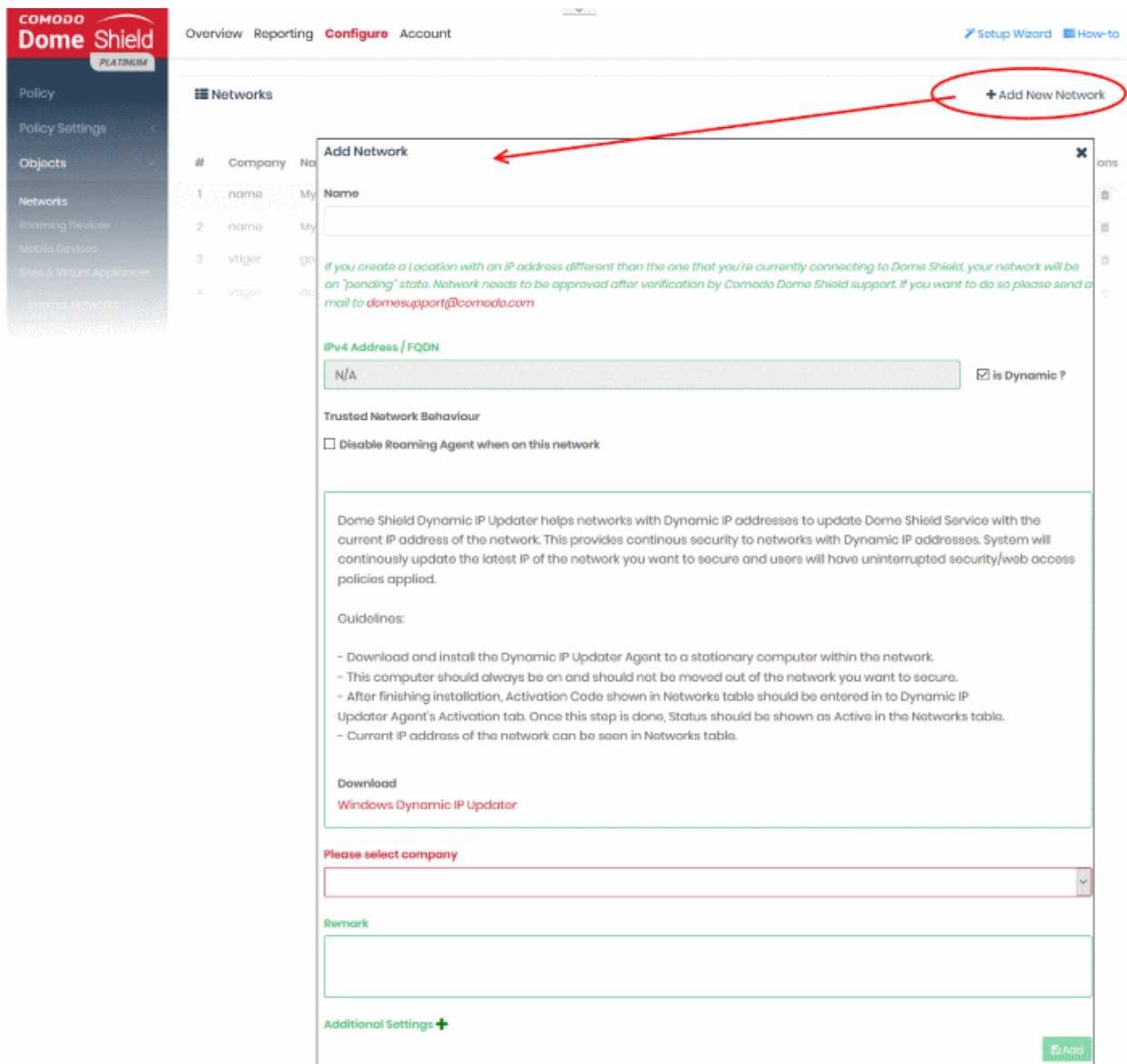| **Important Note**: |
|---|
| •   Admins also need to manually add entries for all internal domains to the host files of endpoints that are inside the network(s). This is because Shield DNS cannot resolve internal domains. |
| •   For roaming endpoints with the Shield agent, internal domains can be 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 Address(es)

Adding new networks with dynamic IP addresses involves two steps:

- **Step 1 - Install the Dome Shield IP Update agent to an endpoint in the network**
- **Step 2 - Activate the agent**

Step 1 - Install the Dome Shield IP Updater agent on an endpoint in the network

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

Add Networks - Form Parameters	
Field	**Description**
Name	Enter an appropriate name 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 guidance on enrolling networks with dynamic IP addresses.. • Click the 'Windows Dynamic IP Updater' link under Download in the message box and save the agent setup file.
Trusted Network Behavior	Disable Roaming Agent when on this network - applies to roaming devices. • If selected, the Shield agent on devices will be disabled when they are inside the network. The network policy will apply to the roaming device.

	• If not selected, the roaming device's policy will remain active.
Select Company	Applies to MSPs only. Select the company for which you want to enroll the network.
Remark	Enter a description for the network being added.

Additional Settings - These settings apply only to roaming devices which have the Dome agent installed.		
	• A roaming device cannot connect to internal hosts when inside the office network. This is because Shield 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 automatically be deployed to your device's host file.	
	• See '**Add Roaming Endpoints to Dome Shield**' for more details about how to install Shield agents onto devices and connect to Dome Shield.	
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 will be added with the status 'Pending'. Also, an 'Activation code' will be 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 Dome Shield. |
|---|

- • 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 will be displayed:
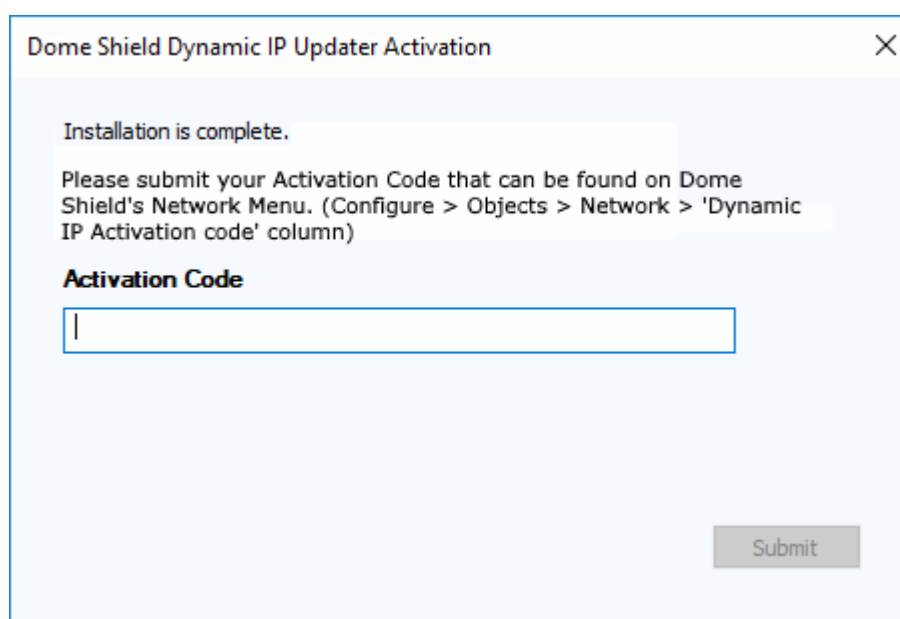
- Click 'Configure' > 'Objects' > 'Networks' in the Dome Shield interface to view the activation code:
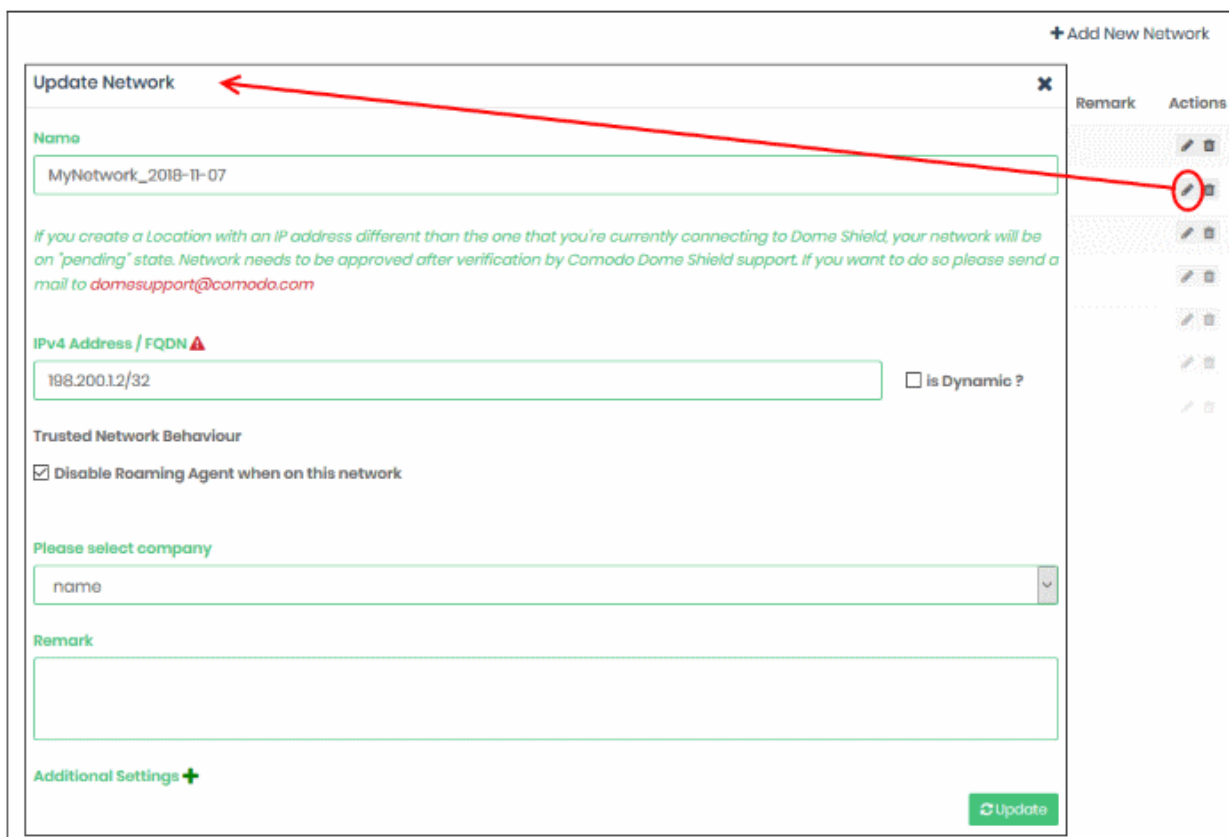

- Enter code in the IP updater activation dialog.
- Click 'Submit'

After successful activation, the network will be added and displayed in the list. Please note no rules will be applied to the newly enrolled networks by default. You can apply network specific policy according to your requirements. See '**Apply Policies to Networks, Roaming and 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.
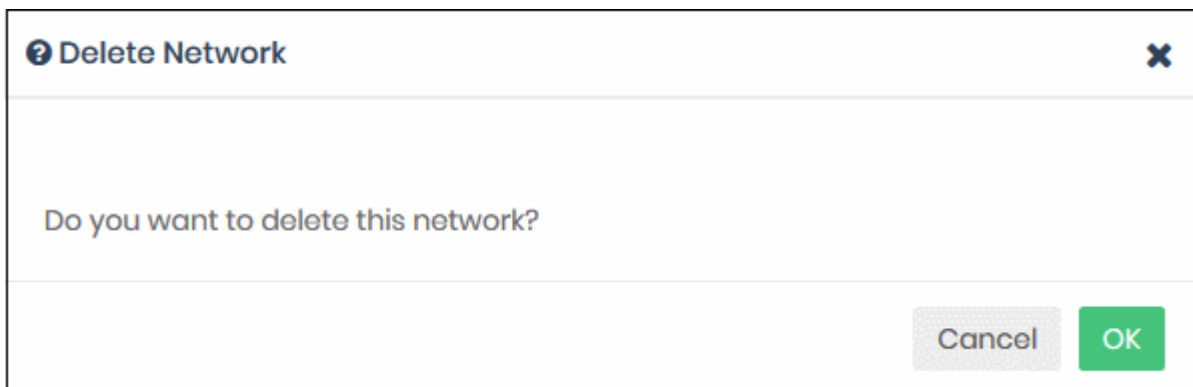
- Click the 'Update' button

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 will be displayed.

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

4.2   Add Roaming Endpoints to Dome Shield

- You can protect Windows and Mac devices outside your network by installing the Shield 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 (formerly ITSM).
- Once installed, you can deploy policies to the devices as required.
- Roaming devices will not be able to connect to internal domains unless configured appropriately in the 'Network' interface.

See '**Additional Settings**' for more about configuring internal DNS and hosts file.

- Click 'Configure' > 'Objects' > 'Roaming Devices' to view all enrolled roaming devices:
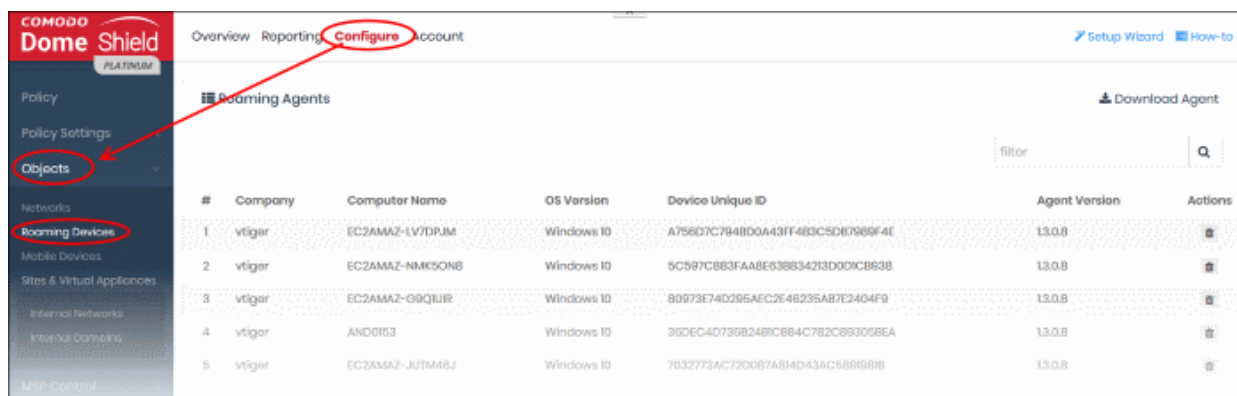
Roaming Agents - Table of Column Descriptions	
Column Header	Description
Company	Applies to MSPs only. The name of the company to which the roaming device is enrolled.

Computer Name	The name of the endpoint.
OS Version	Windows OS version used by the endpoint.
Device Unique ID	A unique ID generated by the shield agent for the device.
Agent Version	Version number of the Shield roaming agent deployed on the endpoint
Actions	Controls for removing endpoints

Search and Filtering options:

- Use the search box at top-right to search by company name, computer name, OS version, Device Unique ID. Matching results will be automatically displayed.

The interface allows you to:

- **Add new roaming devices**
- **Delete a device**

Add new Roaming Device(s)

- 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 (formerly ITSM)** - You can remotely install the agent on managed Windows endpoints from the Endpoint Manager console.

Click 'Download Agent' to get the installation package.

To add new devices

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at the top-right:
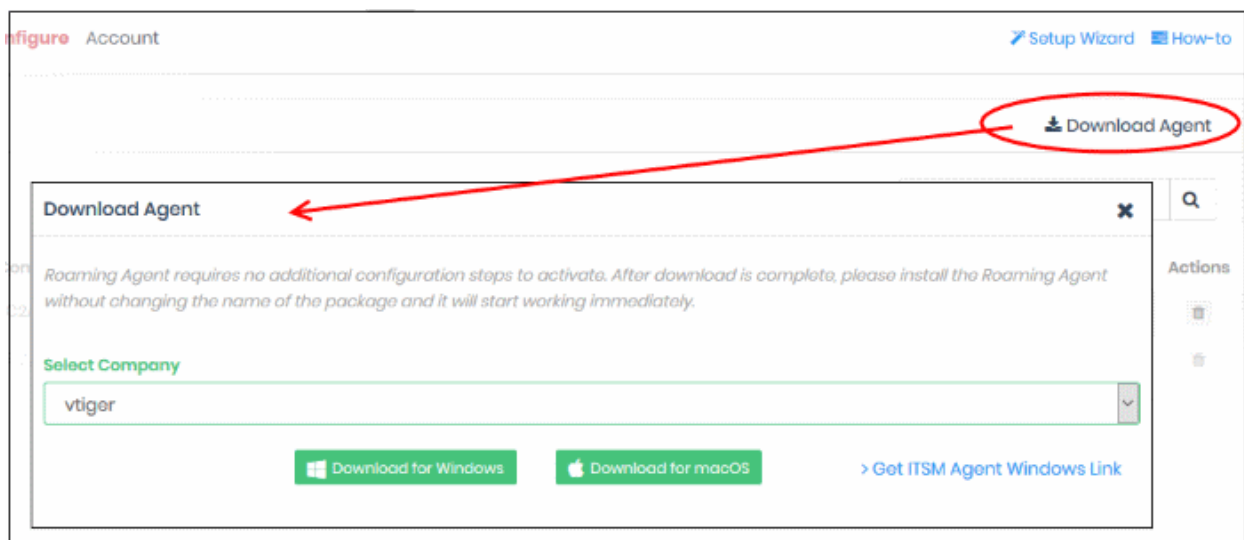
Choose your download options in the 'Download Agent' dialog:

- **Select Company** - Applies to MSPs only. Select the company for which you want to enroll devices.
- **Download for Windows** - Download the agent installation package for Windows devices. See **Enroll Windows devices** for more details.

- **Download for mac OS** - Download 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 (formerly ITSM)** for more details.
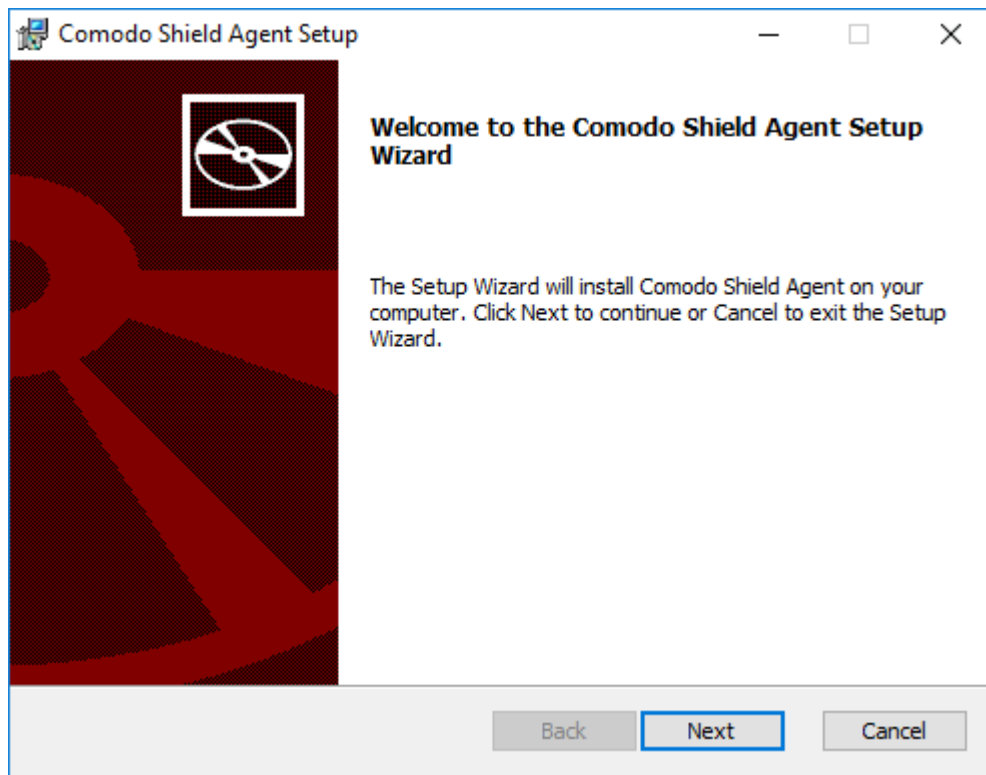
Enroll Windows devices

- 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 will start.

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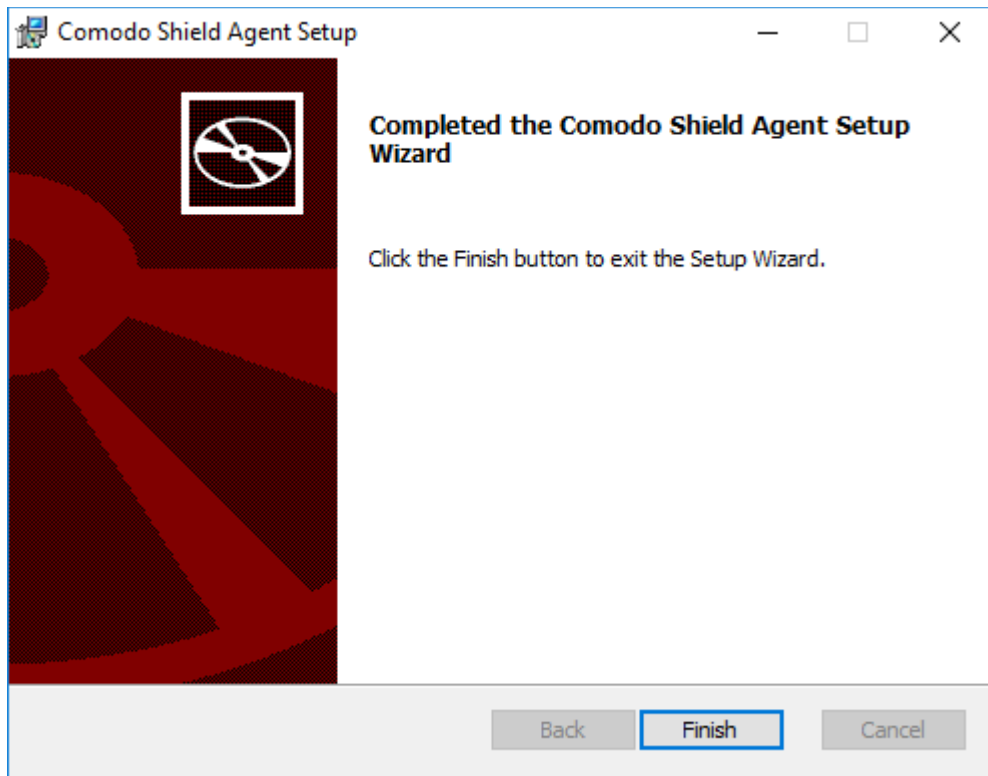
- Click 'Finish'

That's it. The device will be added and will be displayed 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, Roaming and Mobile Devices**' for advice on how to configure and deploy security policies to roaming devices.

Enroll Mac OS devices

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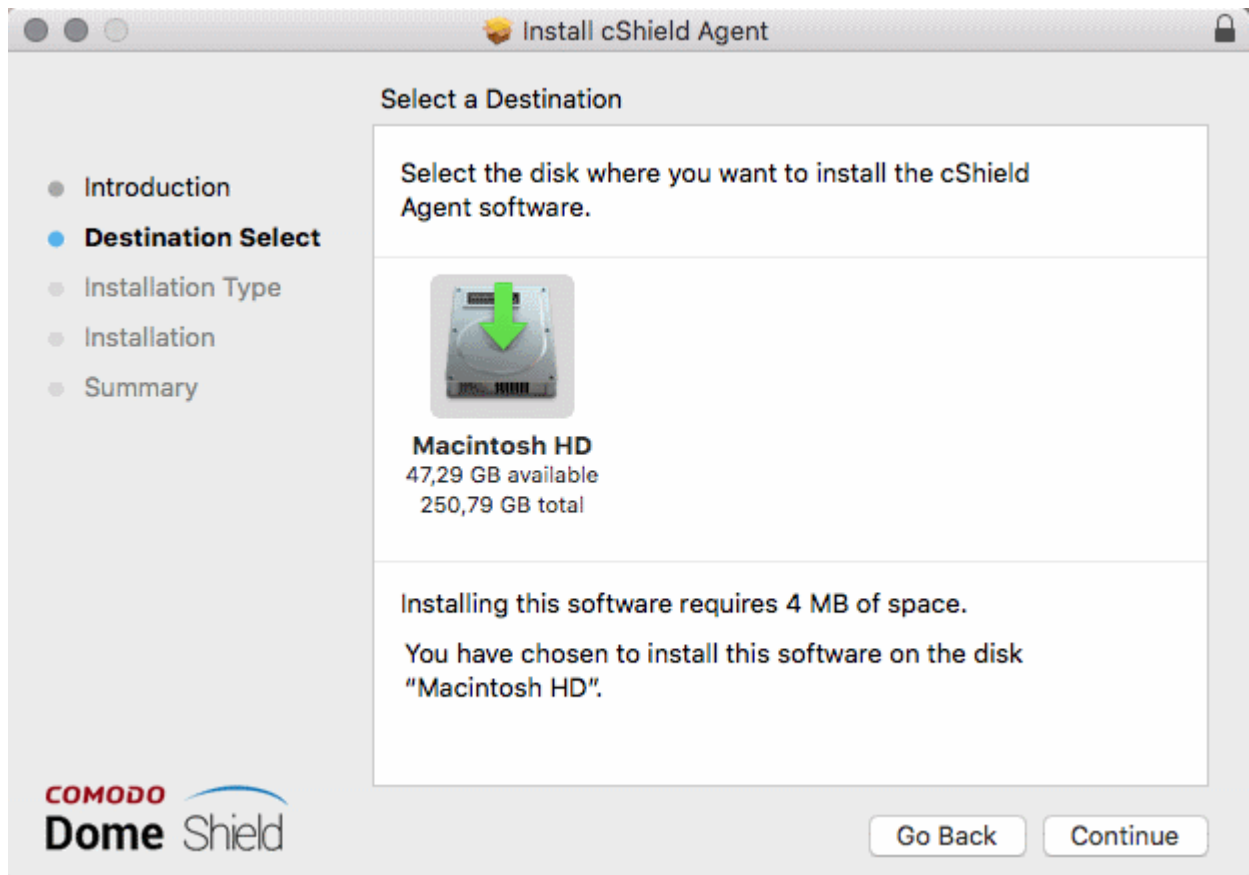
Next, install the agent on the device(s).

- Double-click the package file to start the installation wizard.
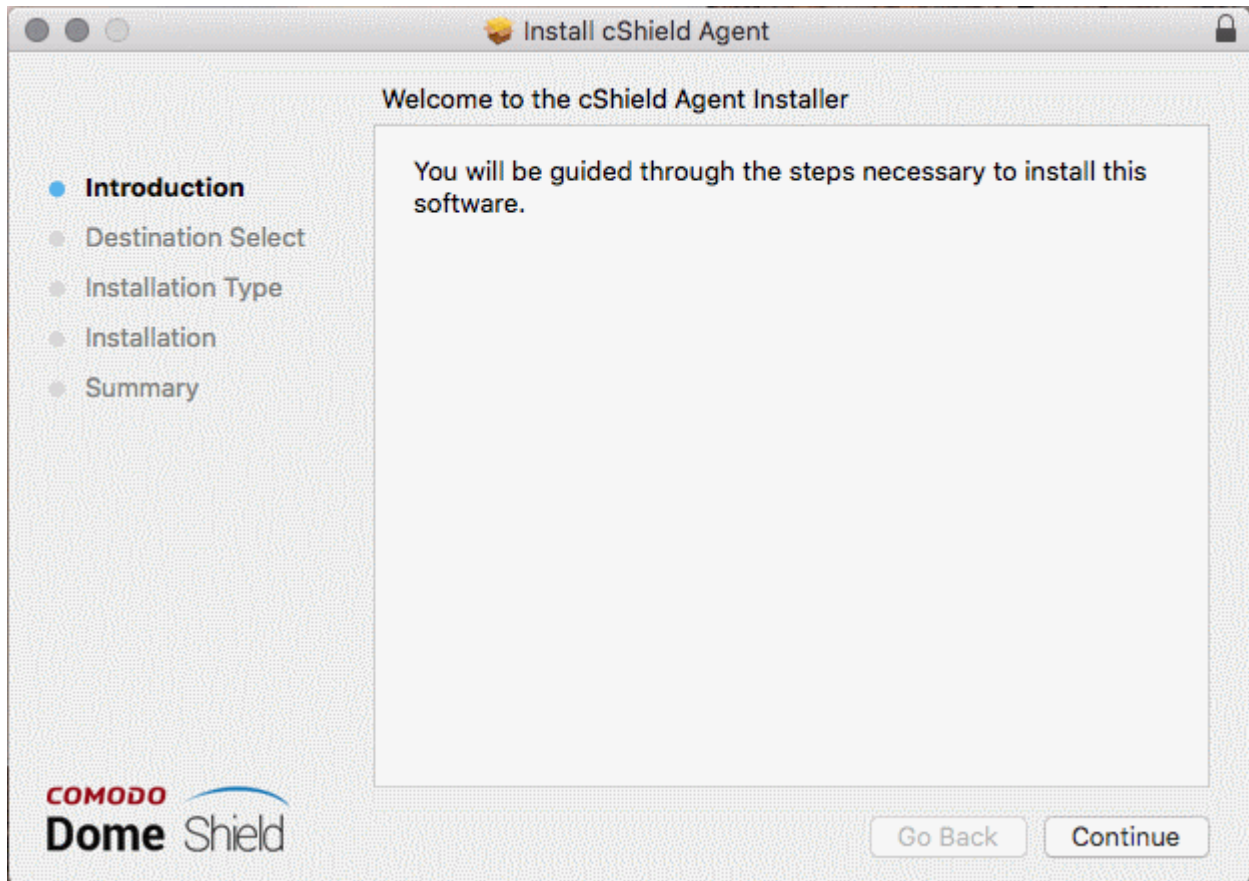
- Click 'Continue'

The next step allows you to choose the location at which the agent is to be installed.

- 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'.
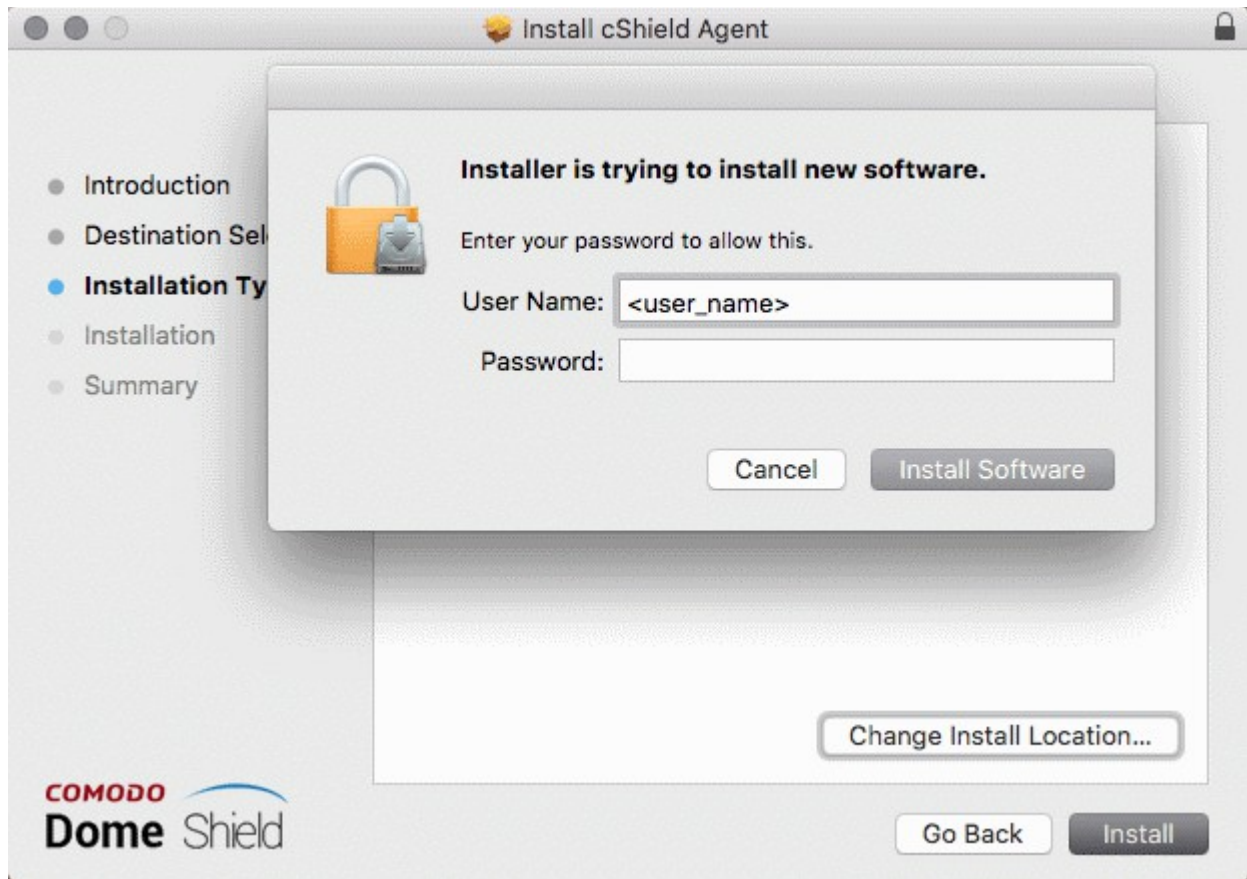
The next step allows you to choose the installation type and start the installation.
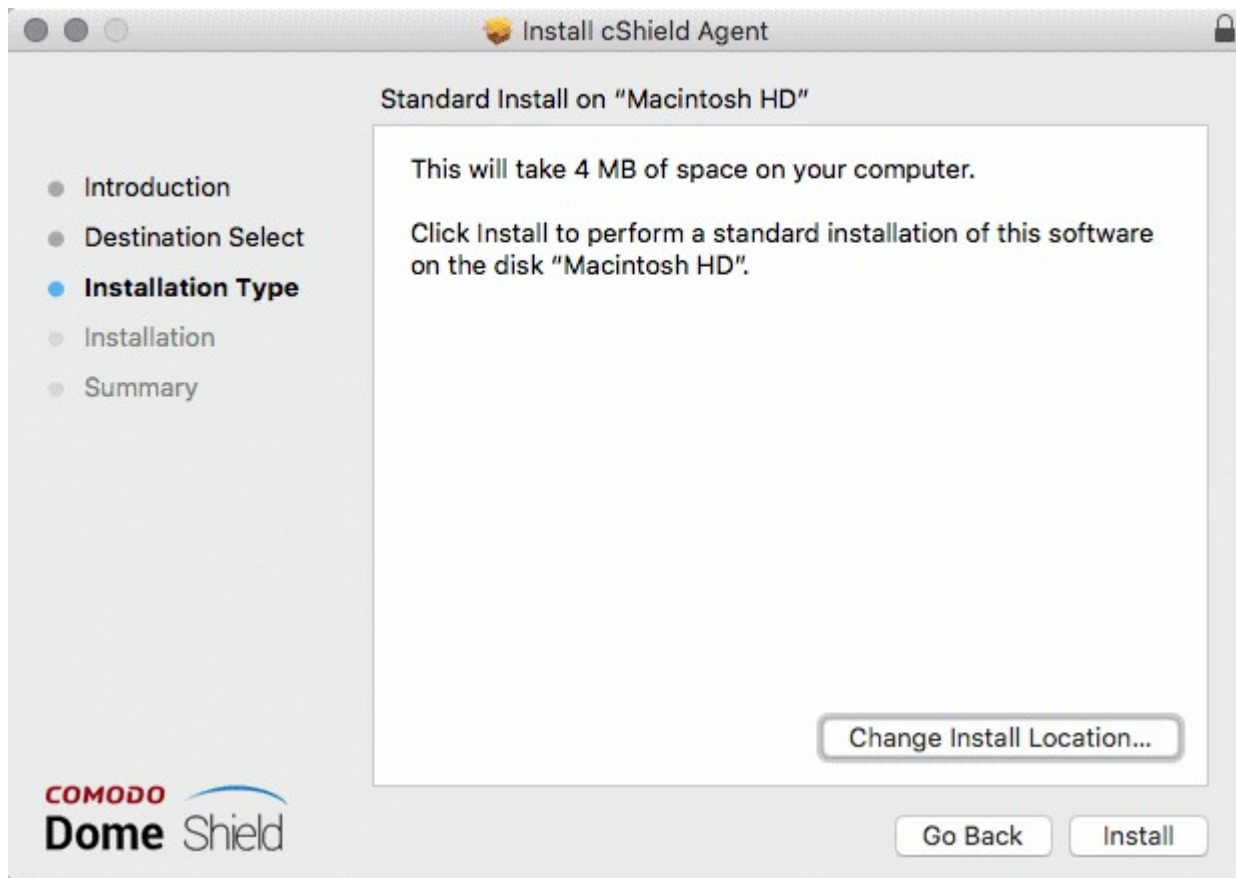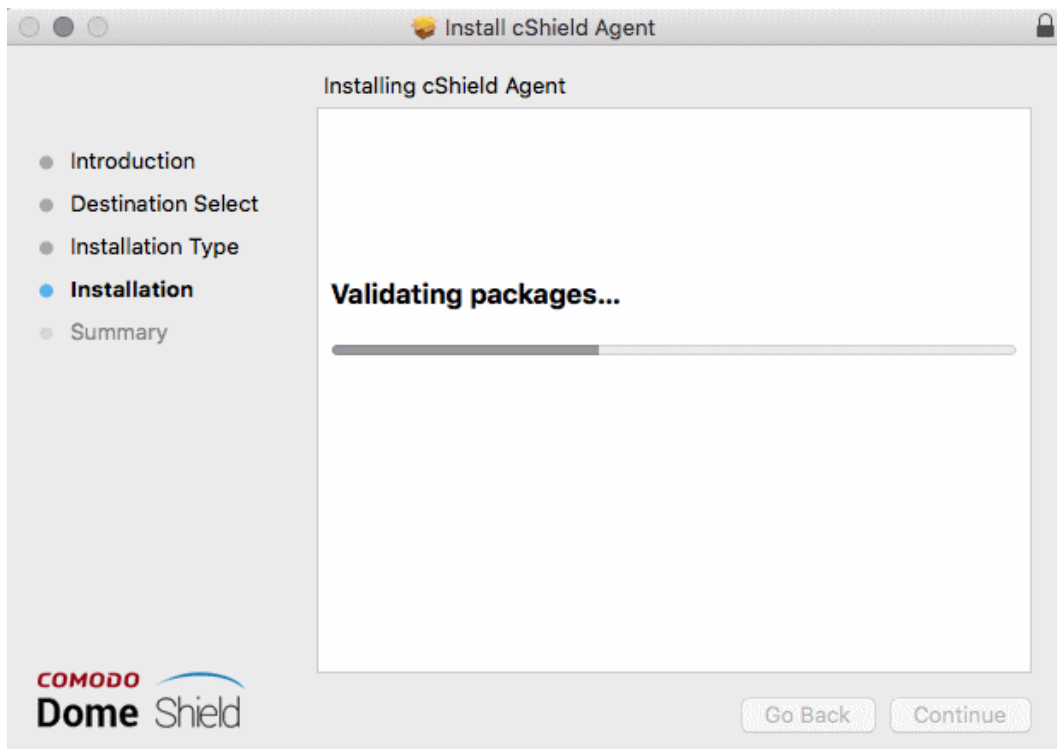

- Click 'Install'

The installation requires your user account to continue.
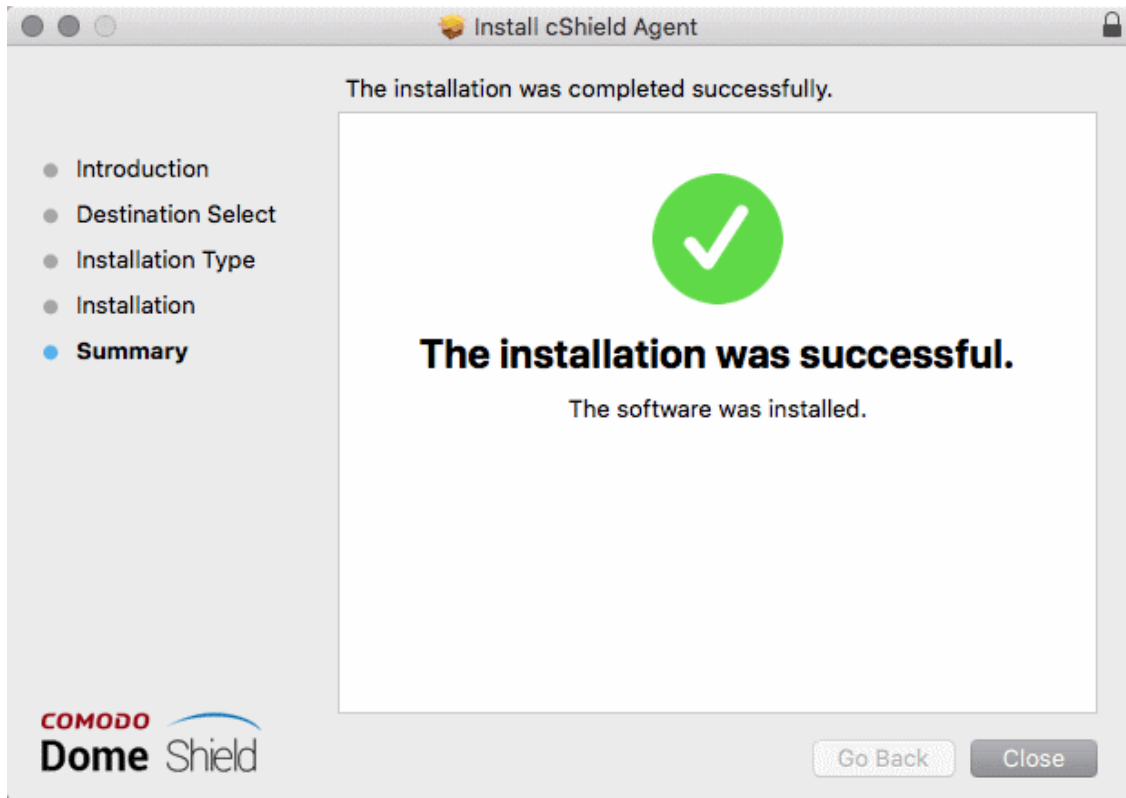
- Enter your device user name and password in the respective fields and click 'Install Software'
- The installation will begin:

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

-

Once installed, the agent will start communicating with the Dome Shield server. The device will be 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, Roaming and Mobile Devices**' for advice on how to configure and deploy security policies to roaming devices.

Import Windows Devices from Endpoint Manager (formerly ITSM)

- Click 'Get ITSM Agent Windows Link':
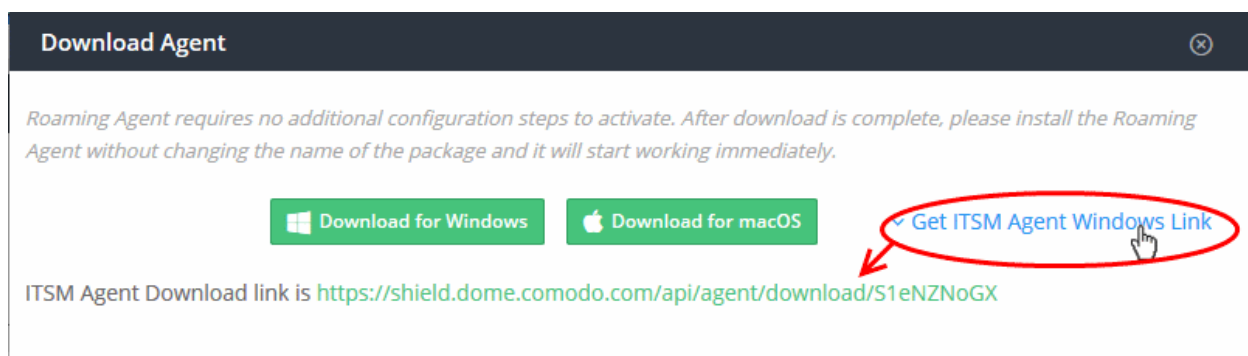
- Use this link as the 'Package URL' to install the agent on managed endpoints.

Process in brief:

- Login to Endpoint Manager
- Click 'Devices' > 'Device List' > 'Device Management' tab
- Select the Windows 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.

Delete a Roaming Device

Web protection policies will no longer apply if you remove a roaming device.

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

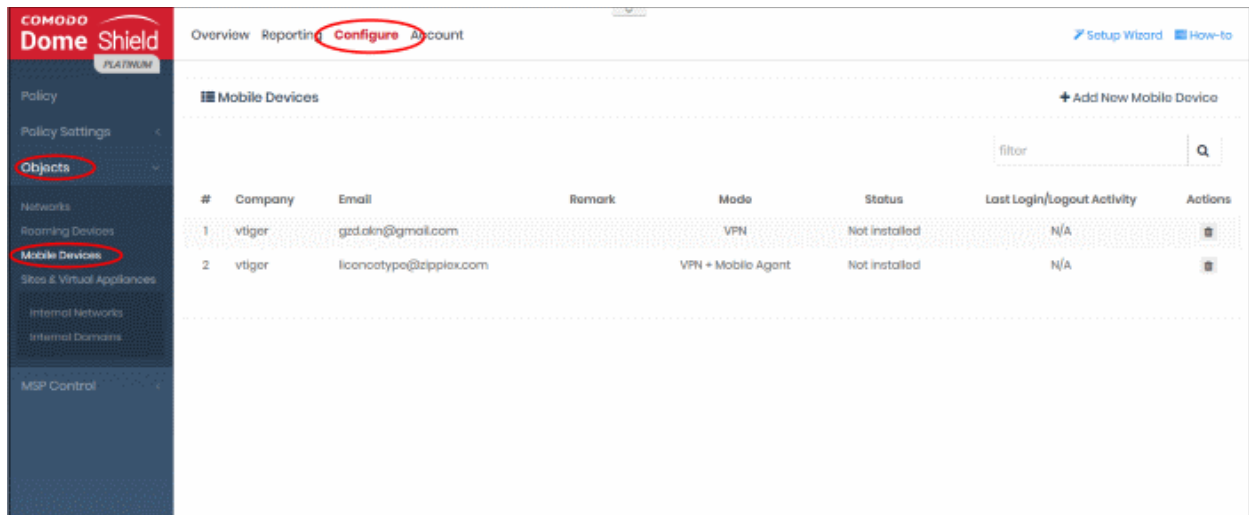A confirmation dialog will be displayed.
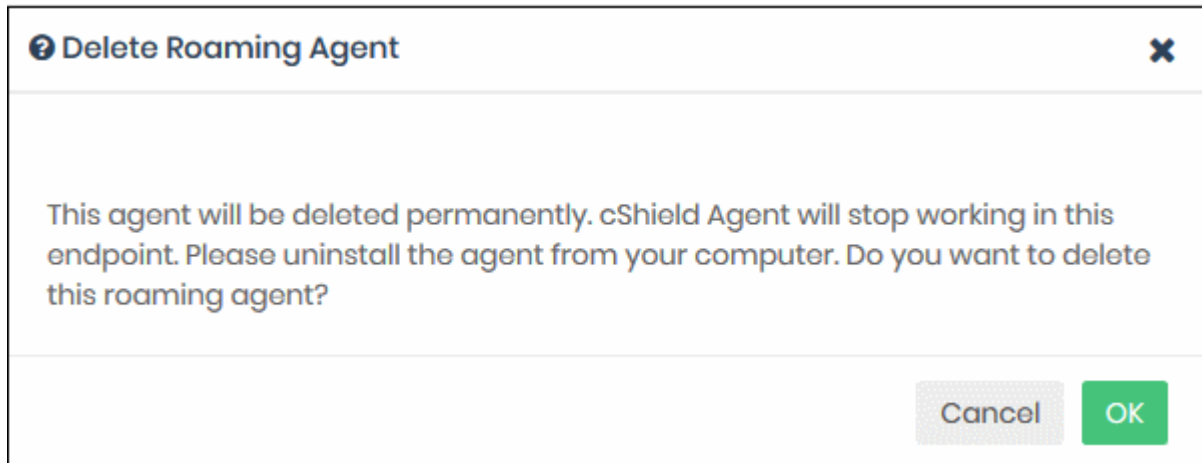
- Click 'OK' to confirm device removal

4.3   Add Mobile Devices to Dome Shield

Click 'Configure' > 'Objects' > 'Mobile Devices' to view this interface.

- Dome Shield can protect iOS and Android devices using its VPN service.
- You need to install the Dome mobile app VPN profile OR on each mobile device.
  - Dome Shield App - The Dome Shield app includes a VPN client and profile.
  - VPN Profile - Requires you to install the StrongSwan VPN tool.
- 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 polces to mobile devices as required.
- Click 'Configure' > 'Objects' > 'Mobile Devices' to view all enrolled mobile devices:

Mobile device interface - column headers	
Company	The name of the company to which the mobile device is enrolled. Applies to MSPs only.
Email	The address to which the enrollment invitation is sent.
Remark	Comments about the account.
Mode	Indicates whether 'VPN Profile' or 'VPN + Mobile Agent' is installed on the device.
Status	The state of the mobile device's connection to Shield. • Installed, Active - Shield profile is installed and the user is connected. • Installed, Not Active - Shield profile is installed and user is not connected • Not installed - The enrollment mail was sent to the user but the Shield profile / mobile app is not yet installed
Last Login/Logout Activity	User login information. • Login - Indicates the device is connected to Shield • Logout - Indicates the device is disconnected from Shield.
Actions	Controls for removing endpoints

Add a mobile device

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

• Click 'Add New Mobile Device' at top-right:
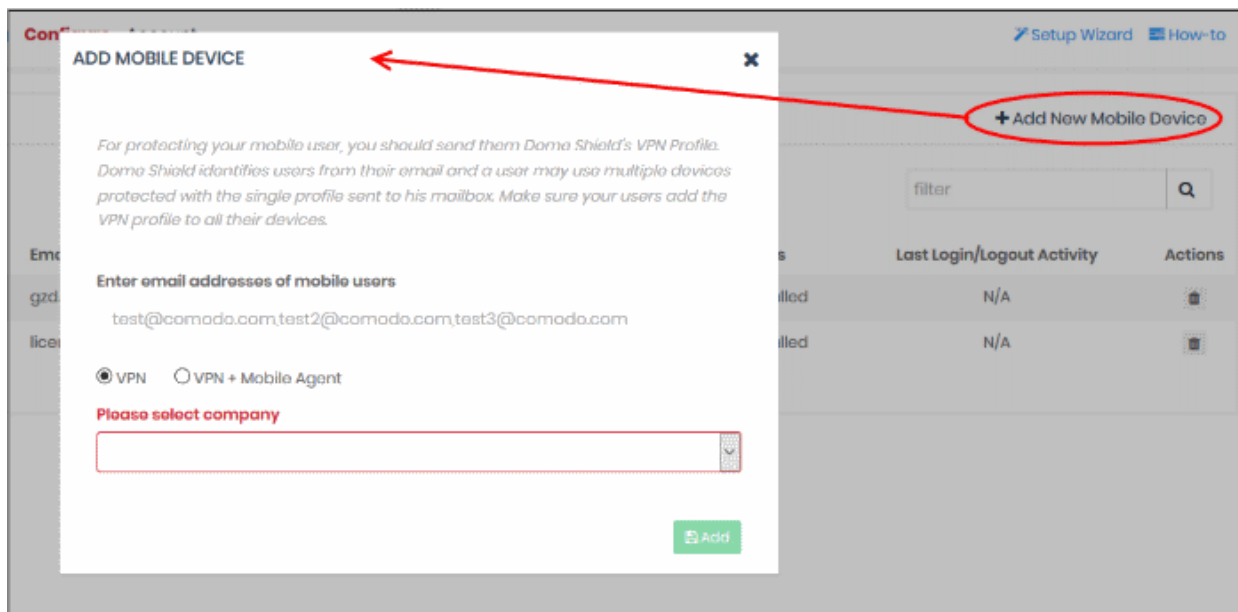
- **Enter the email addresses of mobile users** - You can enter multiple email addresses. Please note - each device requires a unique email address. You cannot use the same email address on different devices.

- **VPN and VPN + Mobile Agent**

    - **VPN + Mobile Agent** – This is the Shield mobile app. If you select this, the user need not install any third party VPN client. **Click here** to see instructions for this option.

    - **VPN** - If you select this, the user has to install the StrongSwan VPN app). This applies to Android devices only, and is not required for iOS devices. **Click here** to see instructions for this option.

VPN

- Select Company - applies to MSPs only. Select the company to which the mobile devices should be enrolled.

- Click 'Add'

Shield will send device enrollment emails to all users that you added.

The user is initially added to the list with a device status of 'Not installed':

- 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.

Instructions for iOS

- Tap the attachment 'iOS_VPN_Profile' in the mail

- Install the profile as shown below:
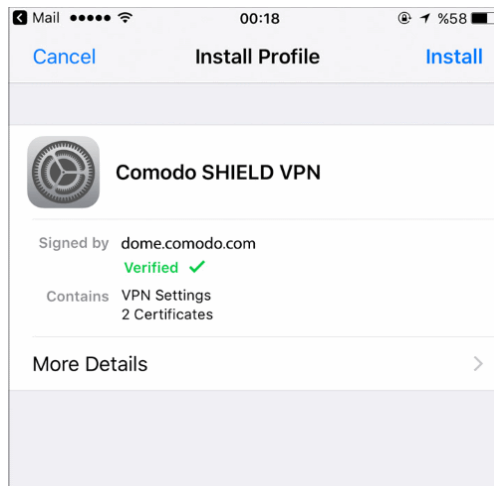
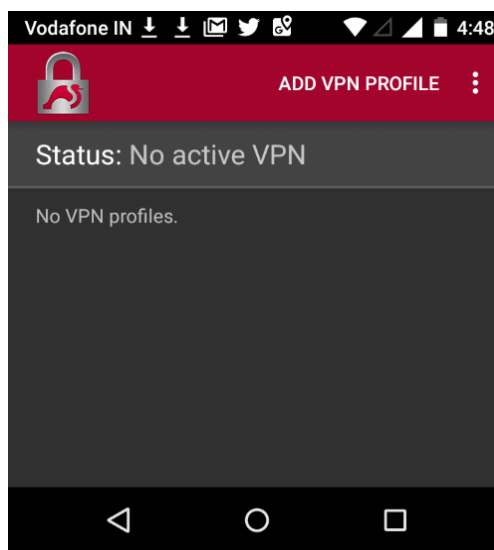That's it. The VPN profile is installed on the device.

- 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.
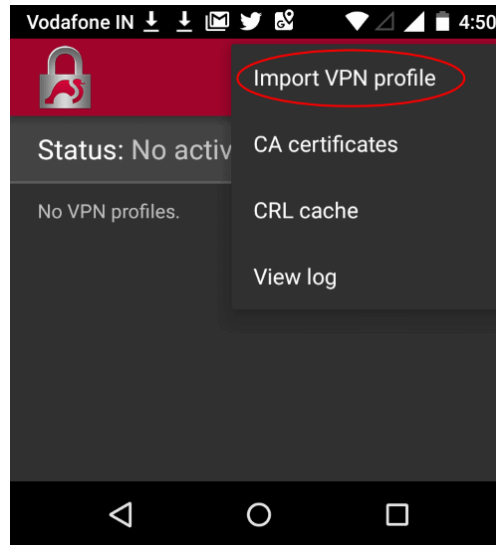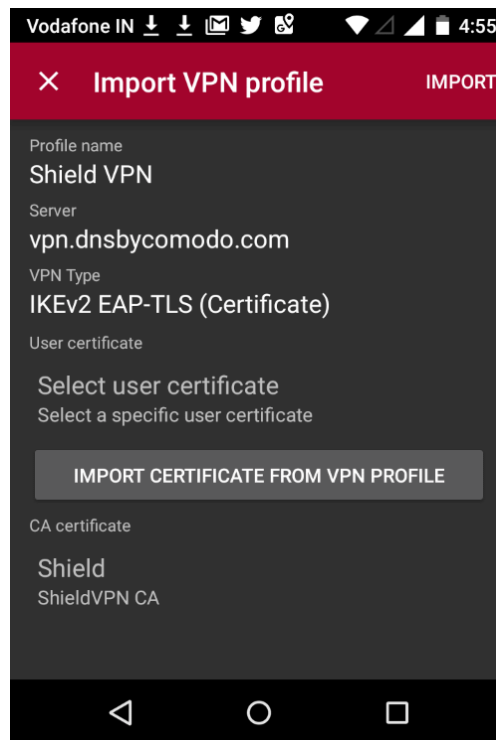
Once connected, the VPN icon will appear on the navigation bar:
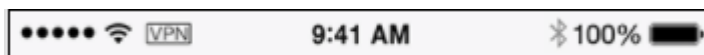
Instructions for Android

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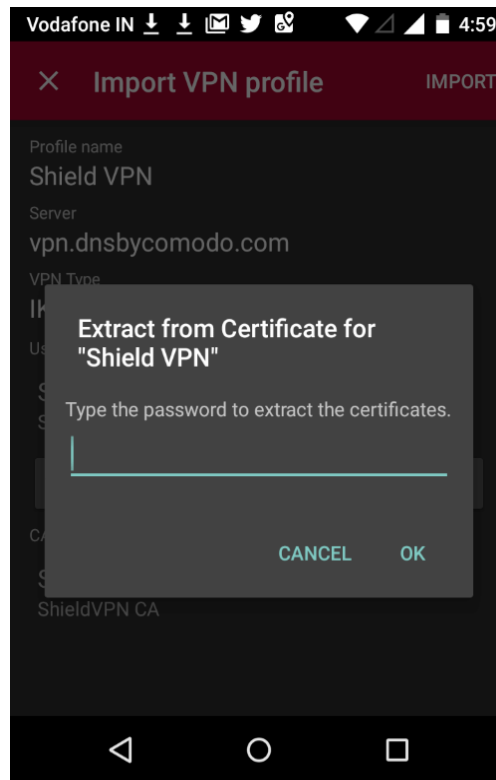
- Open StrongSwan VPN app:

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

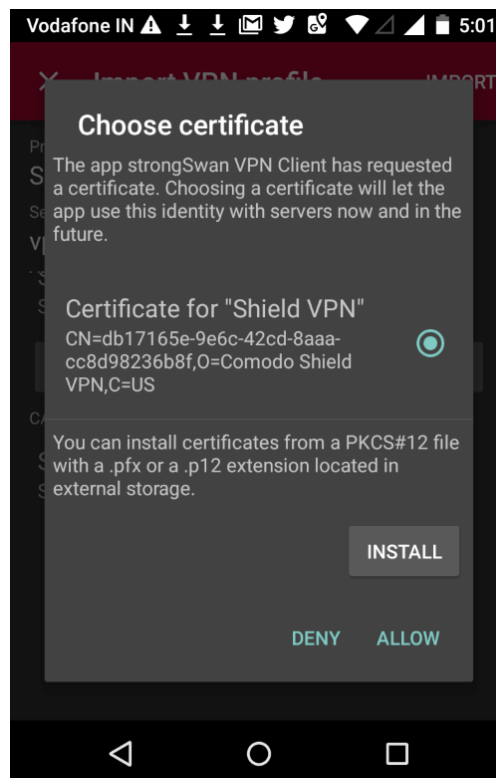
- Choose 'Android_VPN_Profile' from the downloaded location
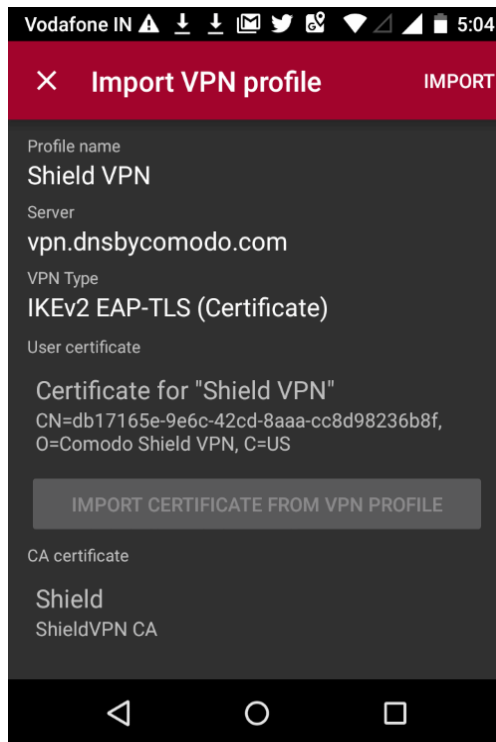

- Select 'Import Certificate from VPN Profile'

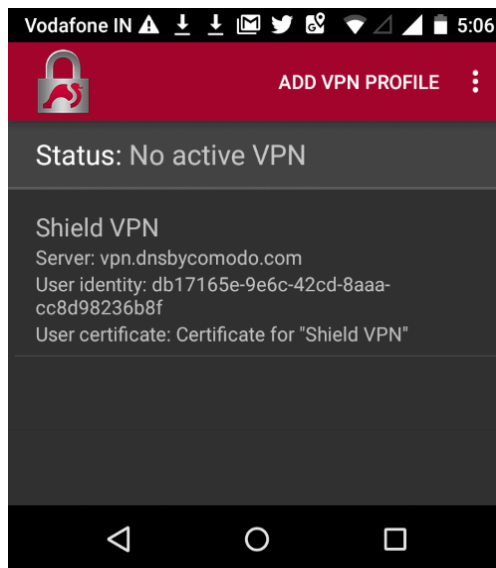- Enter the password in the email and select 'OK'

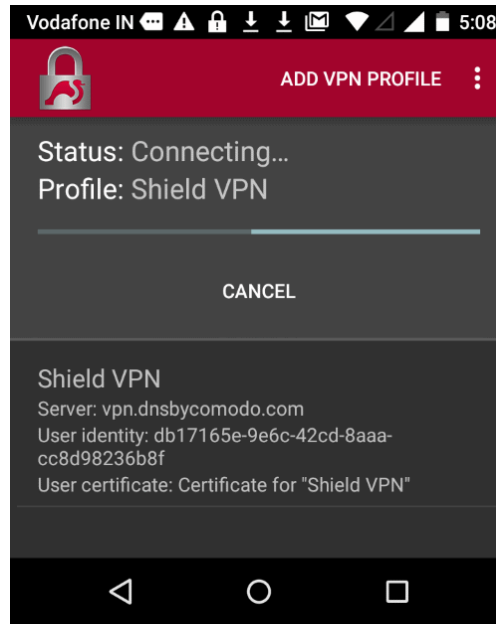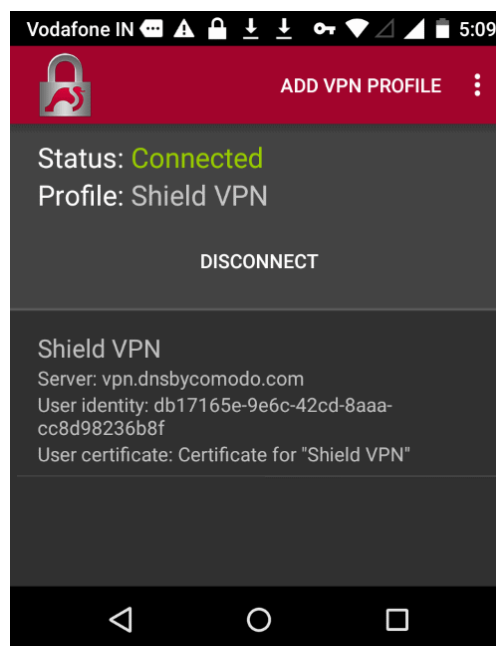- Tap 'Allow' instead of 'Install'

- Select 'Import' at the top-right

- Open the profile you just imported to start the connection to Dome Shield:
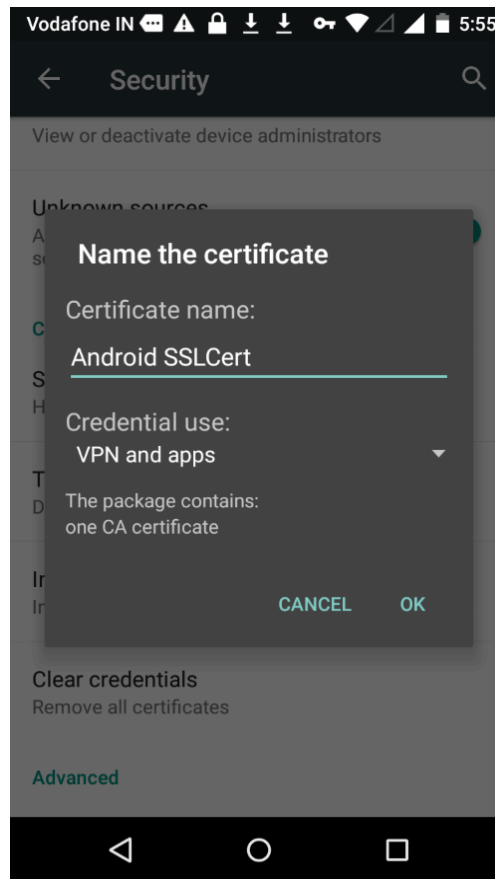
You will see the following screen when connected:

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:

- No rules are applied to mobile devices by default.

- You can apply device specific policy according to your requirements. See '**Manage Shield Rules**' and '**Apply Policies to Networks, Roaming and Mobile Devices**' for help to configure and deploy security policies to mobile devices.

Shield Mobile Device App

- Select 'VPN + Mobile Agent' in the 'Add Mobile Device' dialog

---

- Select Company - applies to MSPs only. Select the company to which the mobile devices should be enrolled.

- Click 'Add'

- Shield will send device enrollment emails 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 their device. The email contains clear instructions how to install the Shield app on Android and iOS devices:
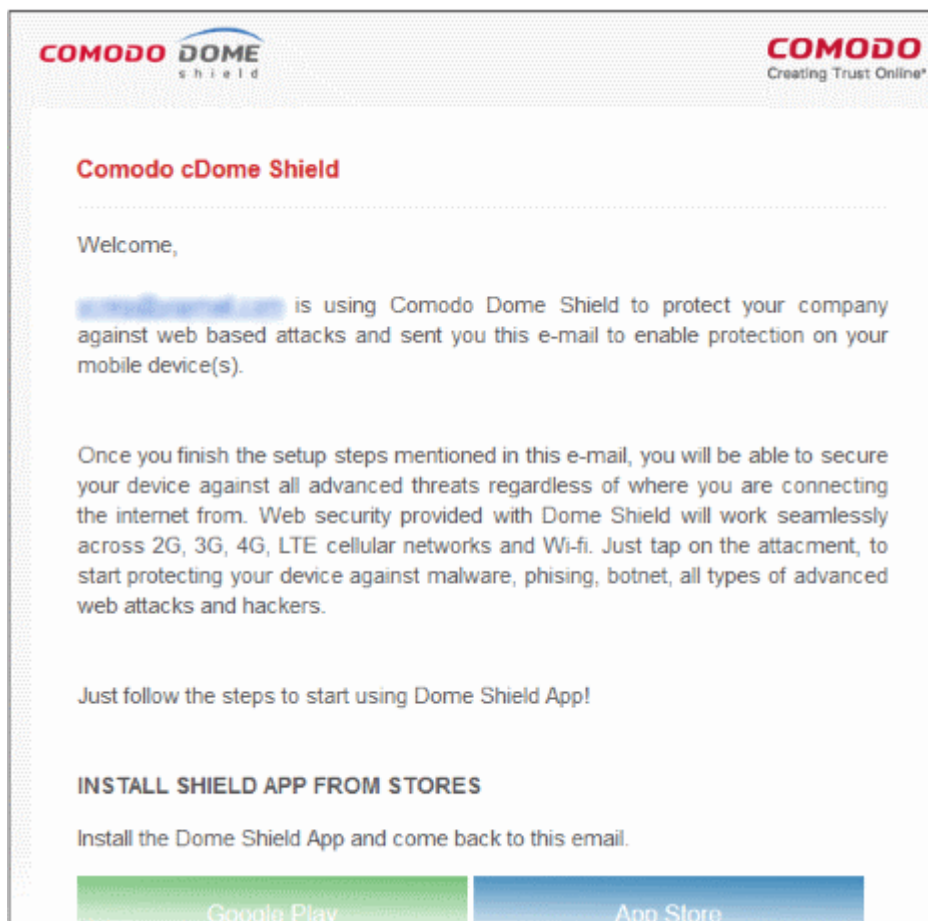
Instructions for iOS

- 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 and tap the 'Shield' button
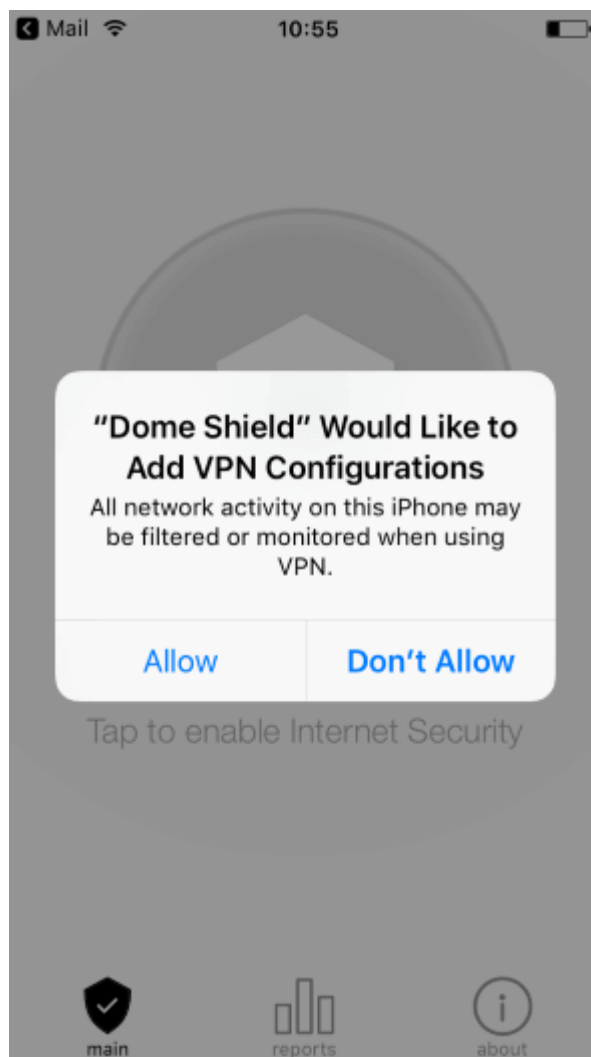
- Select 'Allow'
- Provide the device password if requested:

That's it. The iOS device is successfully enrolled to Dome Shield.
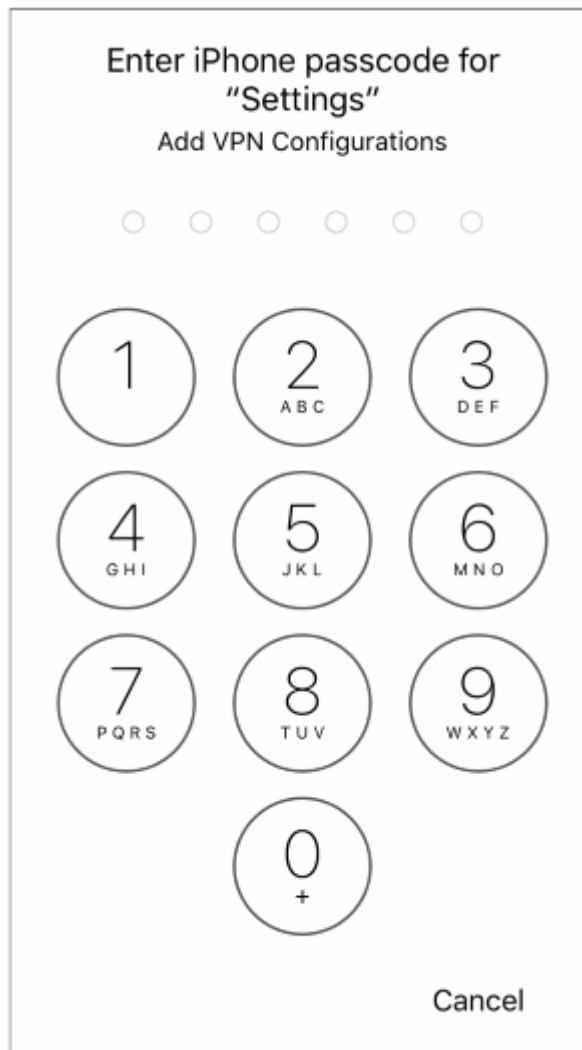
> • You also need to trust the SSL certificates in iOS in order to view HTTPS pages over the VPN.
>
> • Go to 'Settings' > 'General' > 'About' > 'Certificate Trust Settings' and enable full trust for root certificates.

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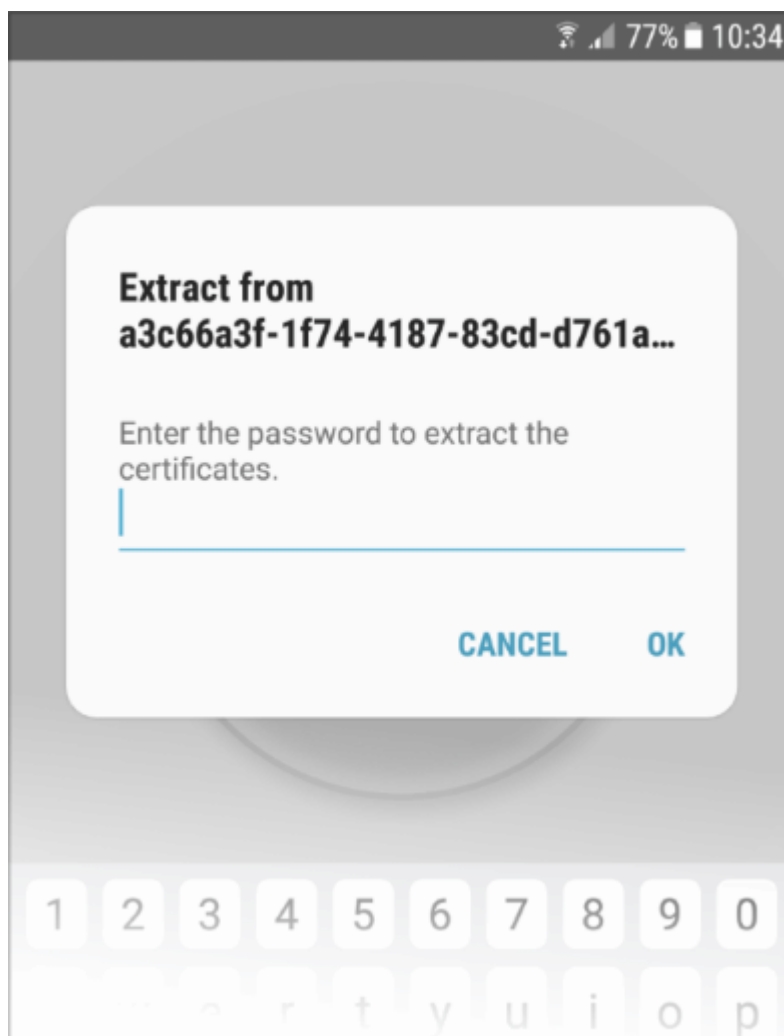
- Long press in the password field and select 'Paste'
- Select 'OK'

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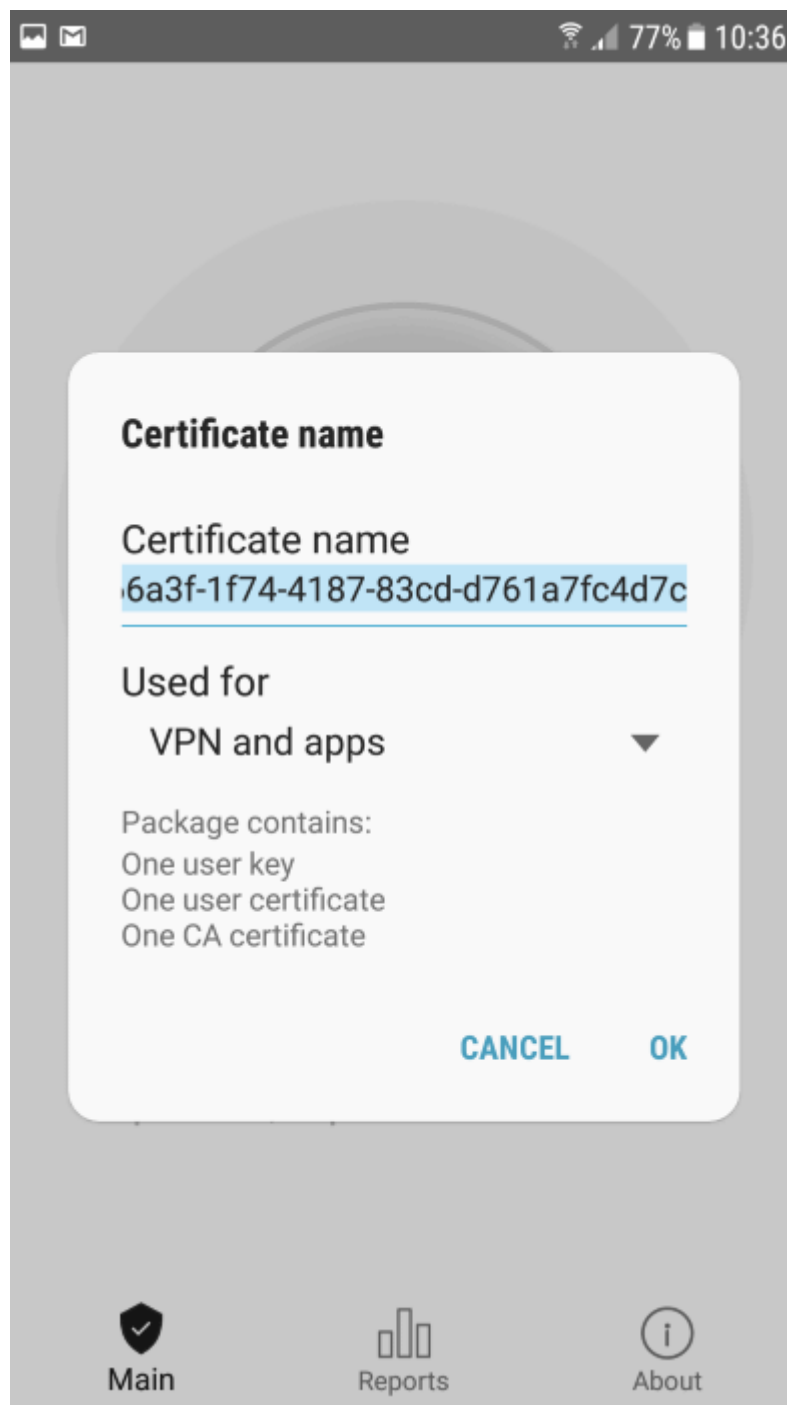
- Touch 'OK'

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 Dome Shield:

Important Note:

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

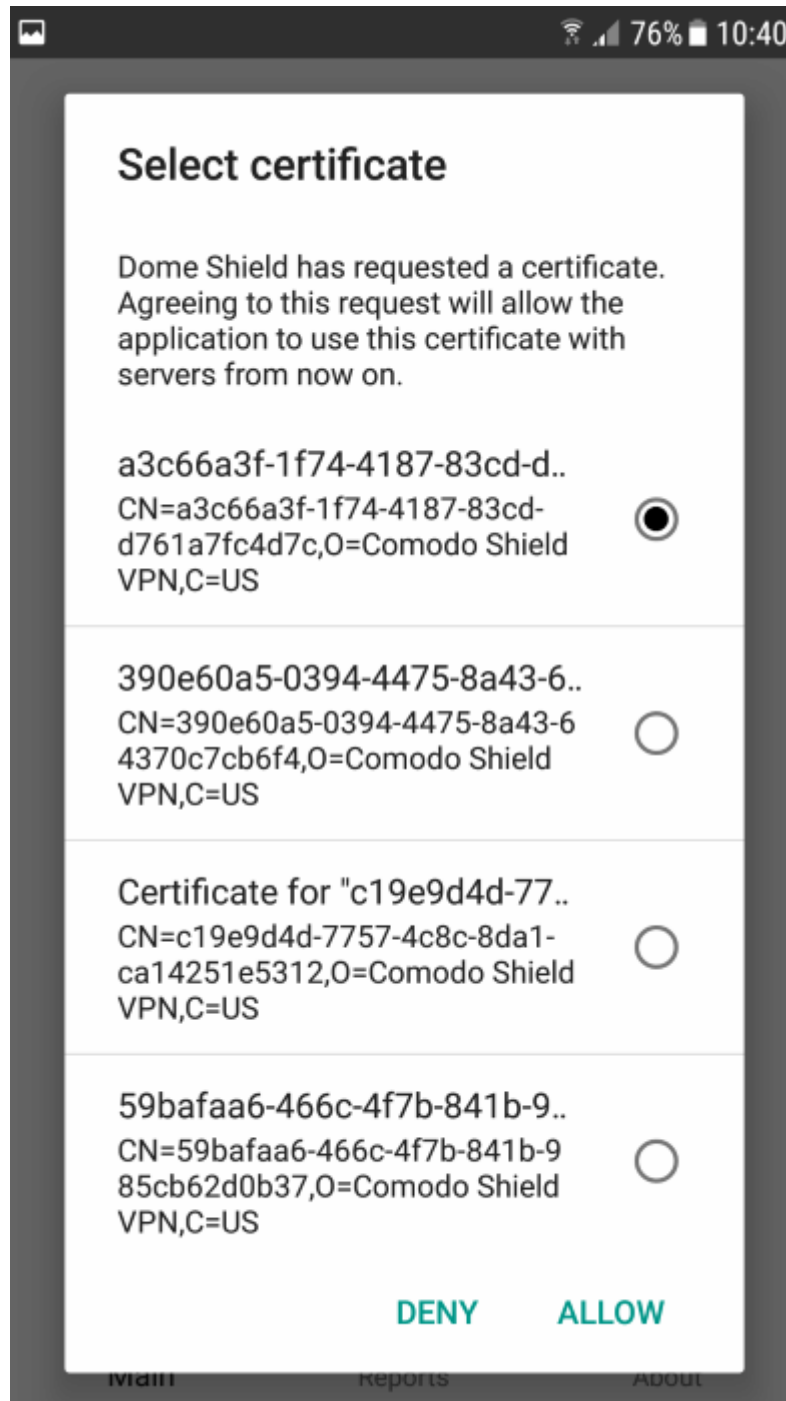- Go to 'Settings' > 'Security'

- Select 'Install from SD card'

- Select 'AndroidSSLCert.pem'

- Enter 'AndroidSSLCert' in the 'Name the certificate' screen.

- Hit 'OK' when finished

The Shield 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 Shield icon

The Shield app will open:

- Main – Select the icon to connect to Shield / disconnect from Shield.
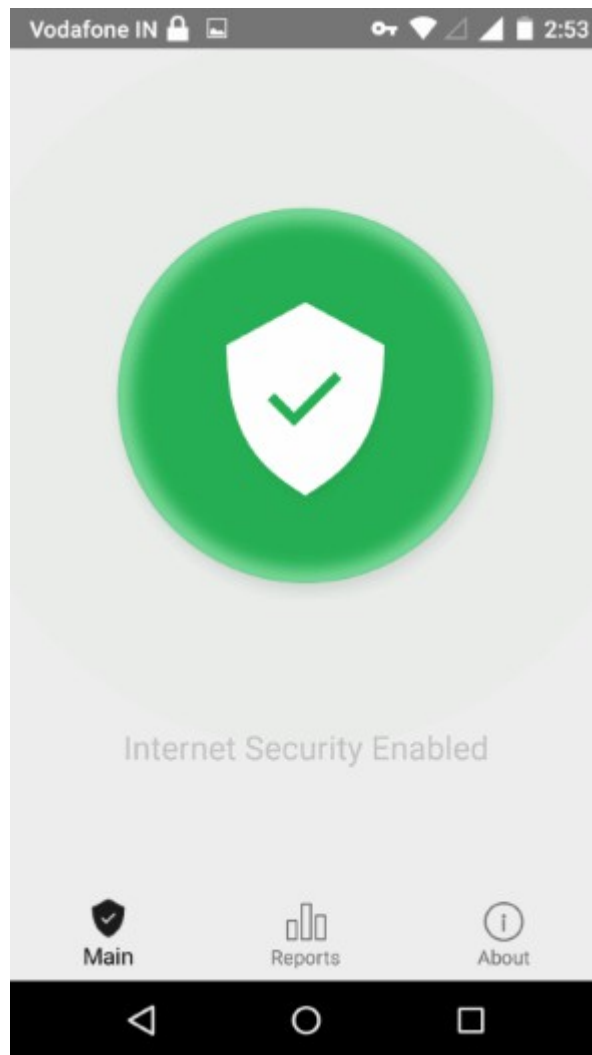
- Reports - View reports for:

    - Overall Web Browsing Trend
    - Top Target Domains
    - Top Blocked Domains
    - Overall Advanced Threats
    - Top URL Categories
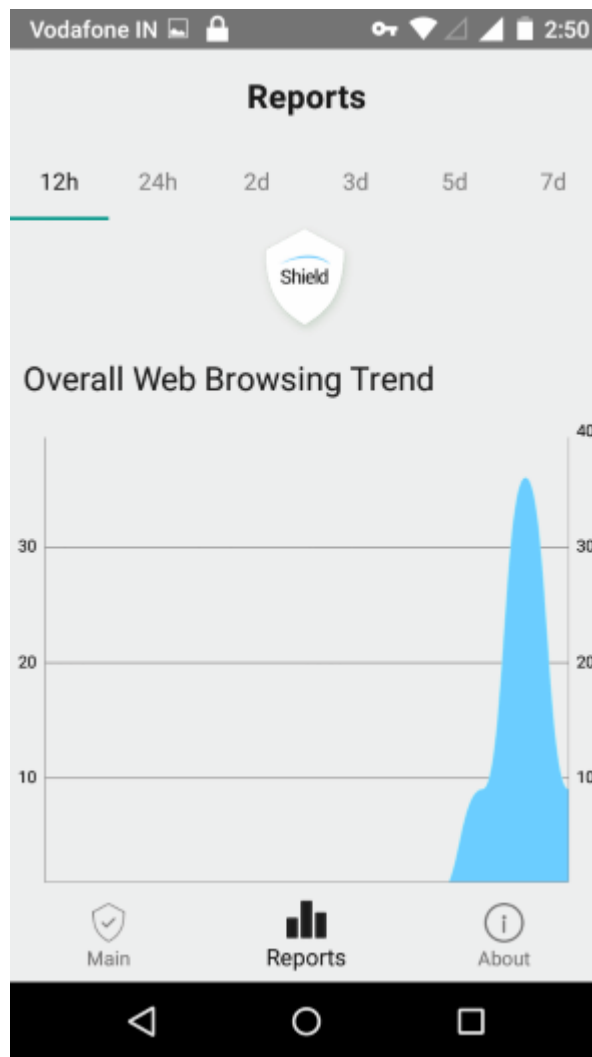
- About - Detailed information about Dome Shield
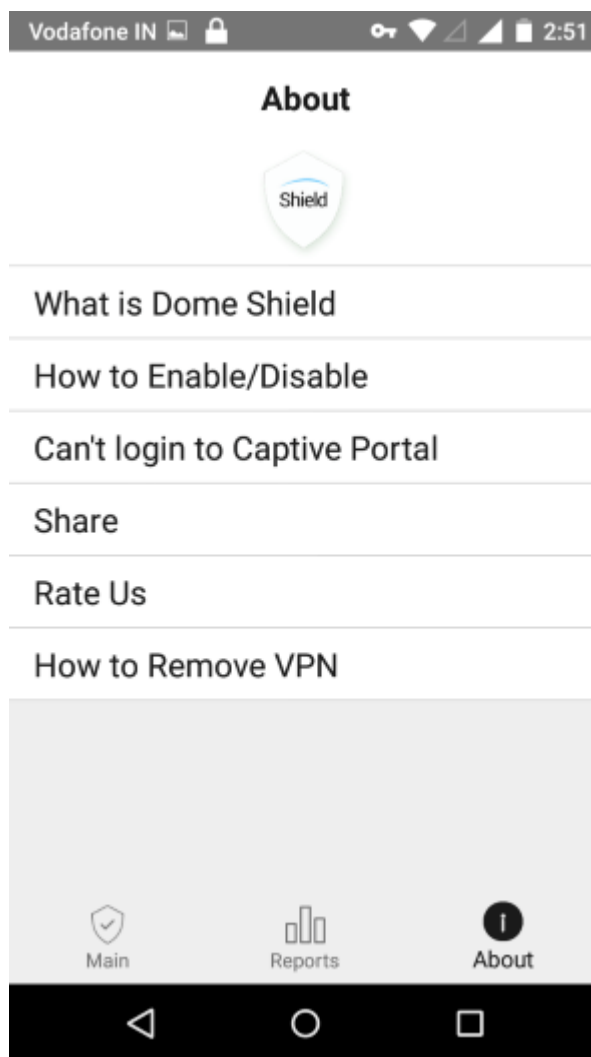
- What is Dome Shield - Brief description about the product
- How to Enable / Disable - Instructions how to connect / disconnect to Shield
- Can't login to Captive Portal - Troubleshooting instructions
- Share - Send the app location details to your friends
- Rate Us - Rate the Shield app
- How to Remove VPN - Instructions how to remove the Shield 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.
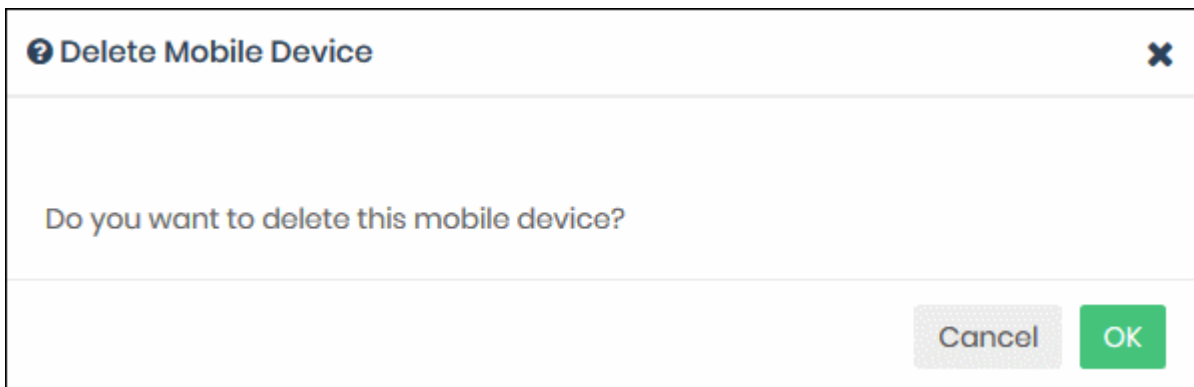
- Click 'OK' to confirm removal of the device from the list.

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 Dome Shield
- 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.

To manage imported sites

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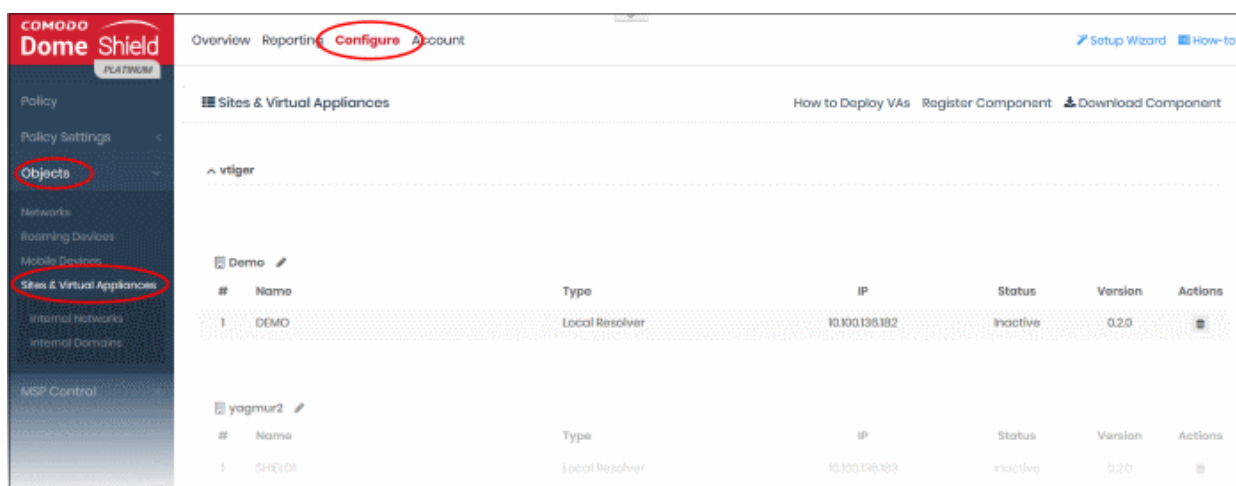
- The links on the right side of the title bar let you download and register the VA's:
  - **How to Deploy VAs** - Opens guides which explain how to deploy the local resolver VA's.
  - **Register Component** - Register a virtual appliance that you have already deployed, and import the network on which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

To edit the name of a site

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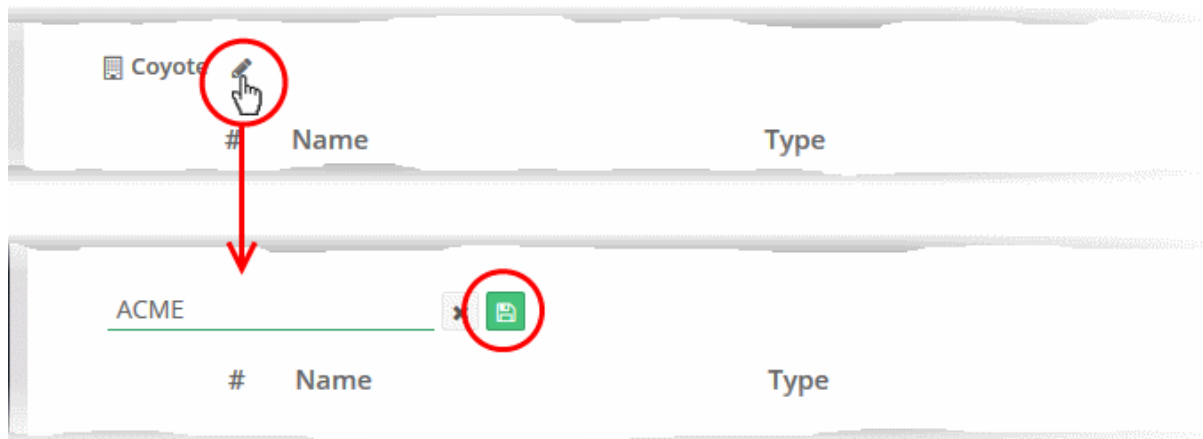
- Click the 'Save' icon

To remove a virtual appliance

- Click the trashcan icon in the row of the appliance

A confirmation dialog will be displayed.

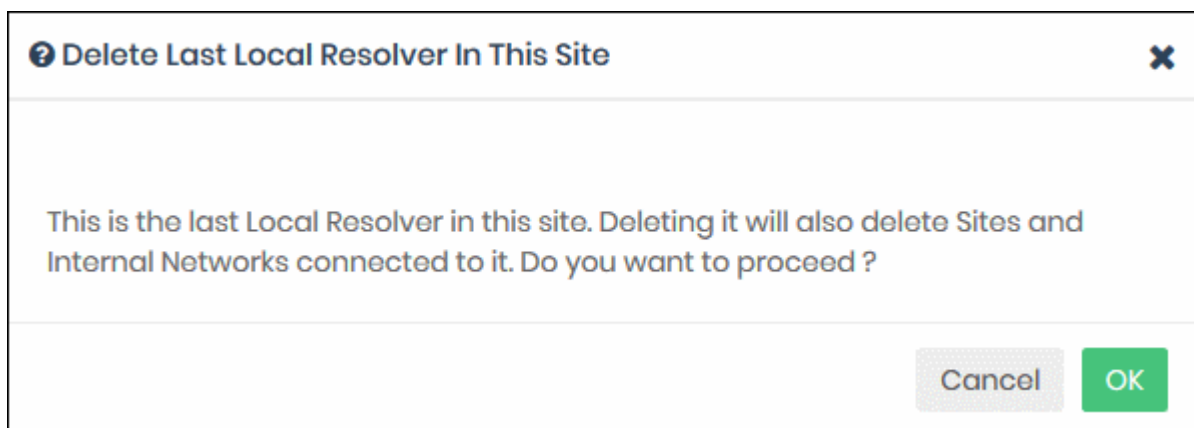- Click 'OK' to confirm removal of the appliance.

The appliance will be deleted from Dome Shield.

- Web protection policies are no longer applied to endpoints.

- The site will also be 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** for more details

- 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** for more details.

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. Dome Shield will apply the site policy to the individual objects and ignore any individual policies for those objects.

To manage Internal Networks

- Click 'Configure' > 'Objects' > 'Internal Networks'
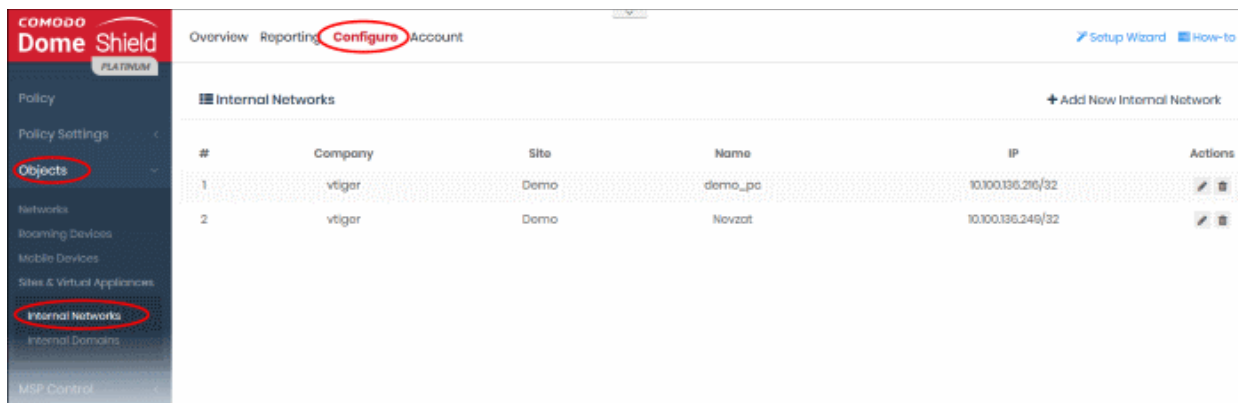
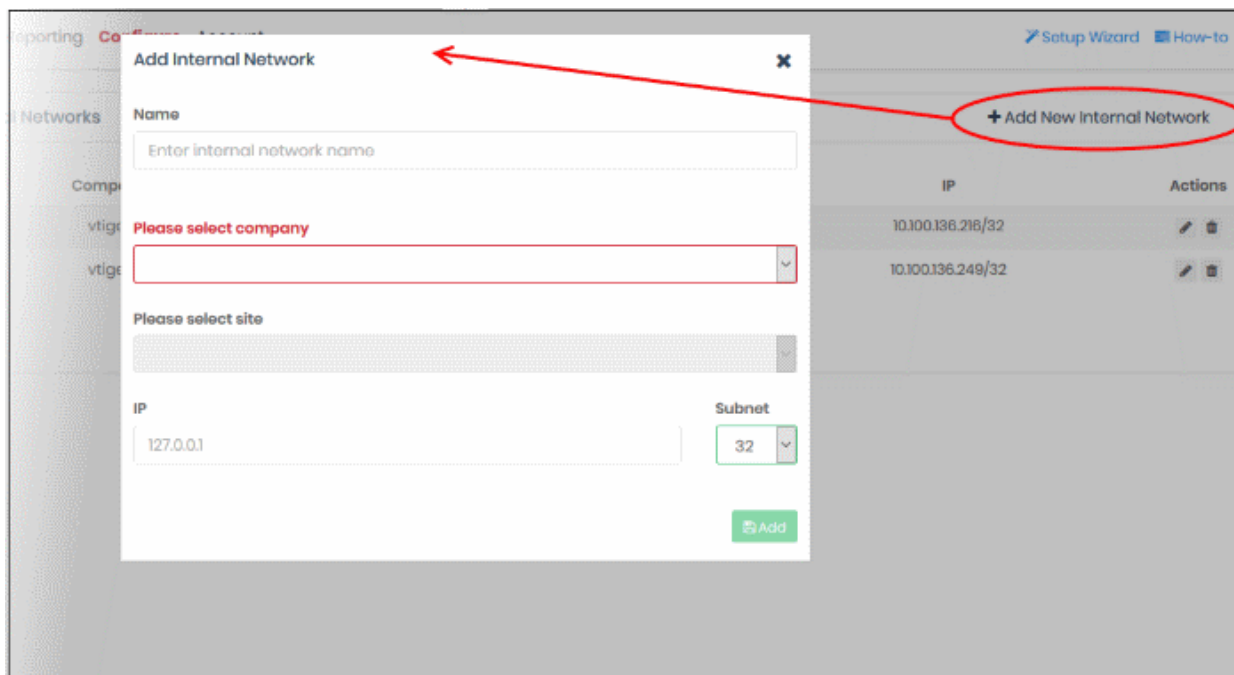| Internal Networks - Column Descriptions	
Column Header	**Description**
Company	MSPs only. Name of the organization to which the network site belongs.
Site	The network to which the endpoints or the sub-net belongs.
Name	The label of the endpoint or sub-net.
IP	The address of the endpoint or sub-net.
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'

Comodo Dome Shield - Admin Guide | © 2018 Comodo Security Solutions Inc. | All rights reserved. 106

| '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. • 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. • Enter the start IP address of the internal network block. • Select the network prefix from the 'Subnet' drop-down. • Dome Shield 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 will be 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, Roaming and Mobile Devices** for more details.

Edit Internal Network Objects

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

To edit an internal network object

• Click 'Configure' > 'Objects' > 'Internal Networks'.

• Click the pencil icon beside the internal network object to be edited.
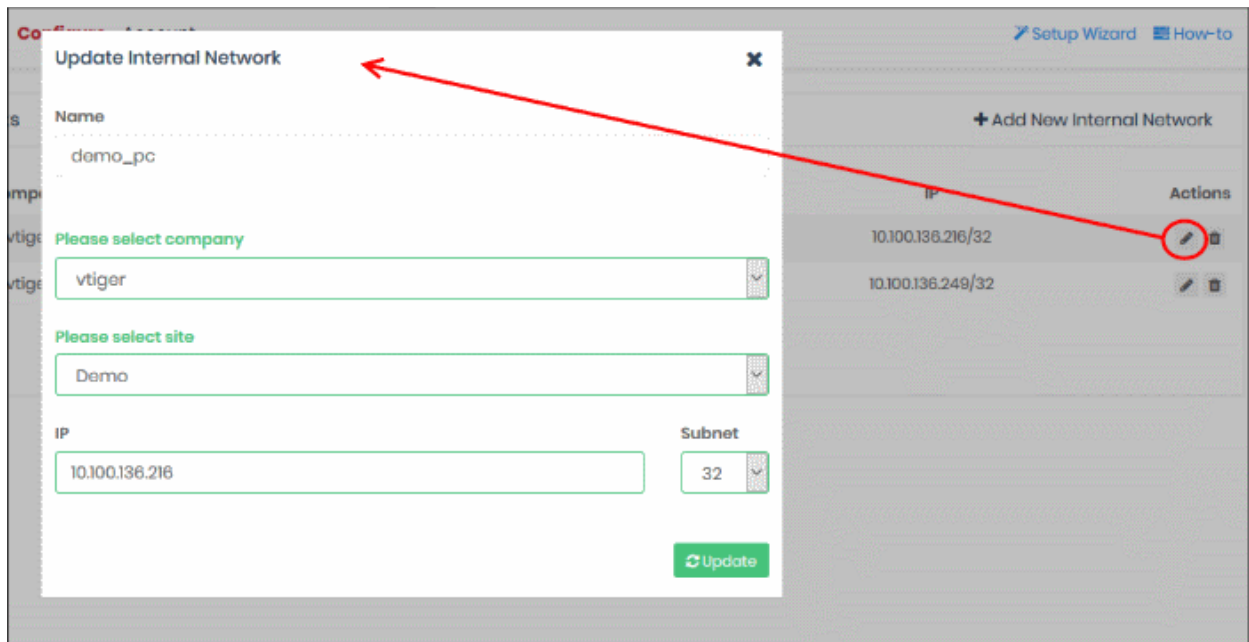
The 'Update Internal Network' dialog will open.

- 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 the explanation **above** for more details

- Click 'Update' to save your changes

The policy in effect on the internal network object will now be applied only to the endpoints covered by the new IP address range.
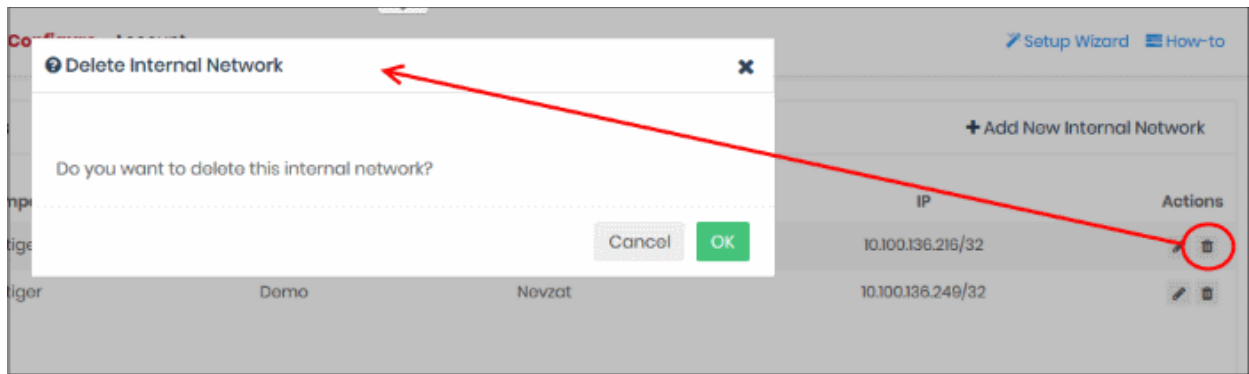
Remove Internal Network Objects

The internal network objects that are no longer needed to be applied with the specific policy can be removed from the Internal Networks list.

Once removed:

- If a policy exists for the parent site to which the internal network object is a member of, the same policy will be applied to the endpoints covered by the internal network

- If no policy is applied to the parent site, the default security policy will be applied to the endpoints covered by the internal network

To 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 Dome's public DNS servers, saving your bandwidth.

To manage internal domains in imported sites

- Click 'Configure' > 'Objects' > 'Internal Domains'
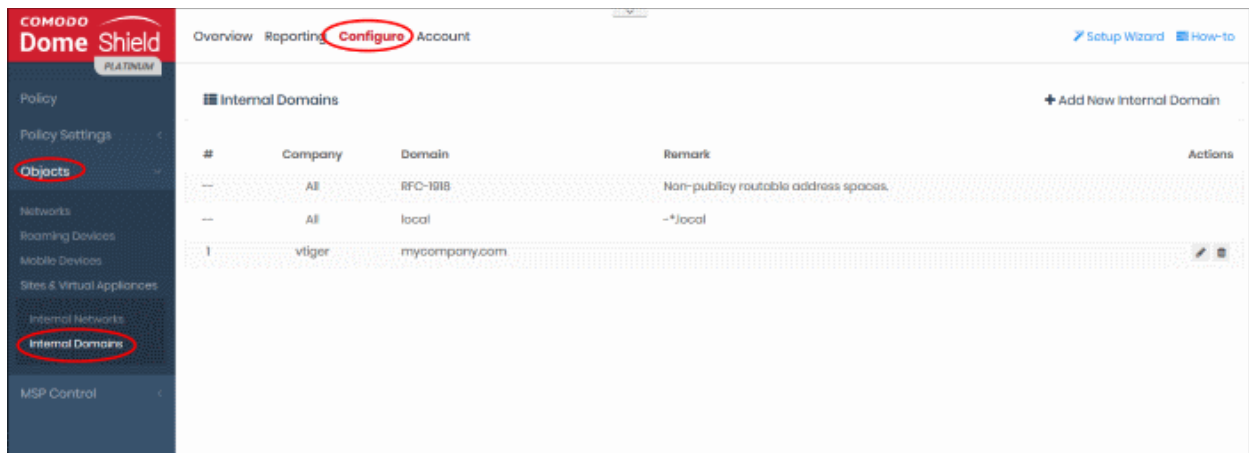
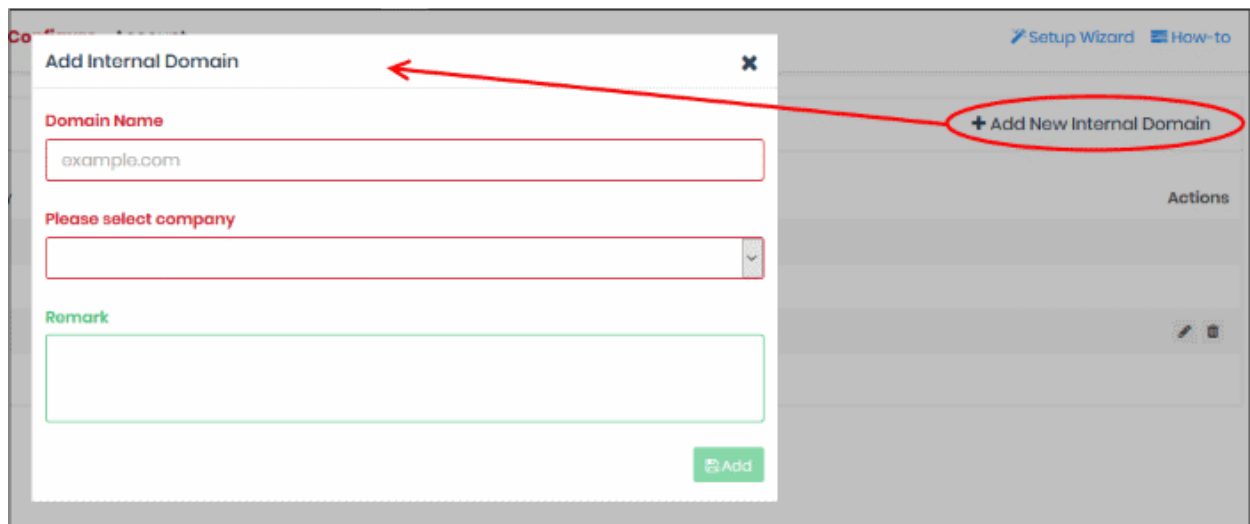| Internal Domains - Column Descriptions	
Column Header	**Description**
Company	MSPs only. Name of the organization to which the internal domain belongs.
Domain	The name of the internal domain.
Remark	A short description of the internal domain.
Actions	Edit or remove the internal domain.

The list contains two default items, including non-publicly routable address spaces and the local domains in the networks.

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	The registered name of the internal domain. • Enter the full domain name (without https://, http://, or www) • Prefix the domain with a wildcard character to include all sub-domains. Wildcard character = *. For example: *.internaldomain.com
Please select company	MSP customers only. • 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'.

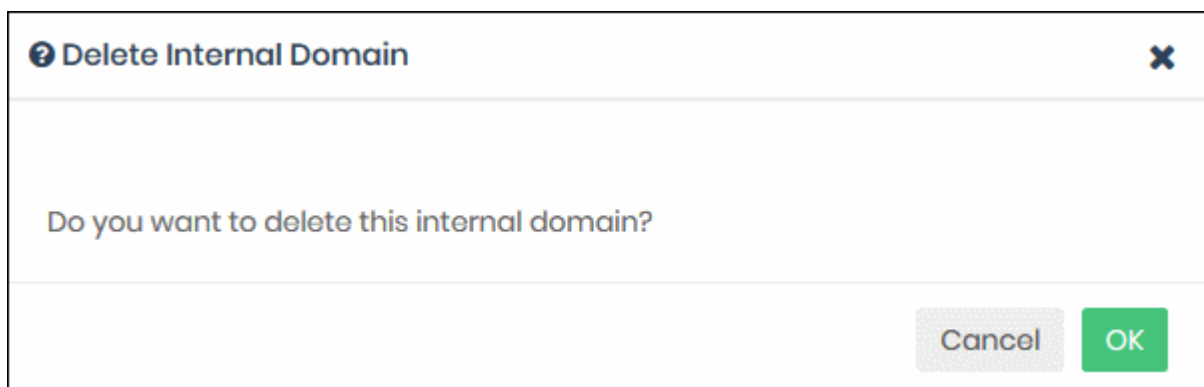The internal domain will be added to the list.

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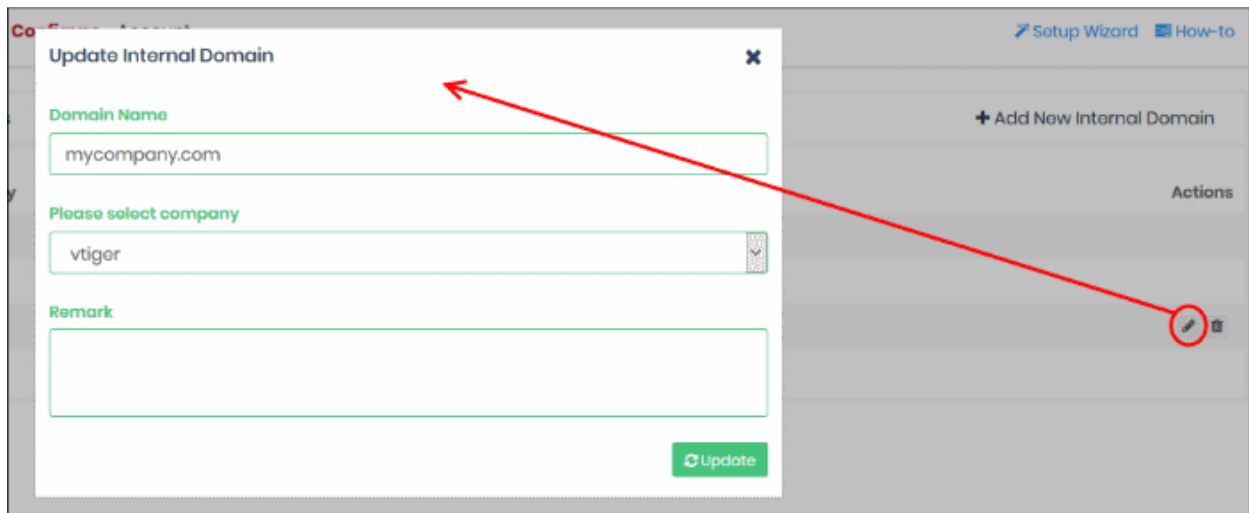
- Click 'Update' to save your changes.
- Configuration is similar to the 'Add Internal Domain' process
- You can edit the company and internal domain name. See the explanation **above** for more details

Remove Internal Domains

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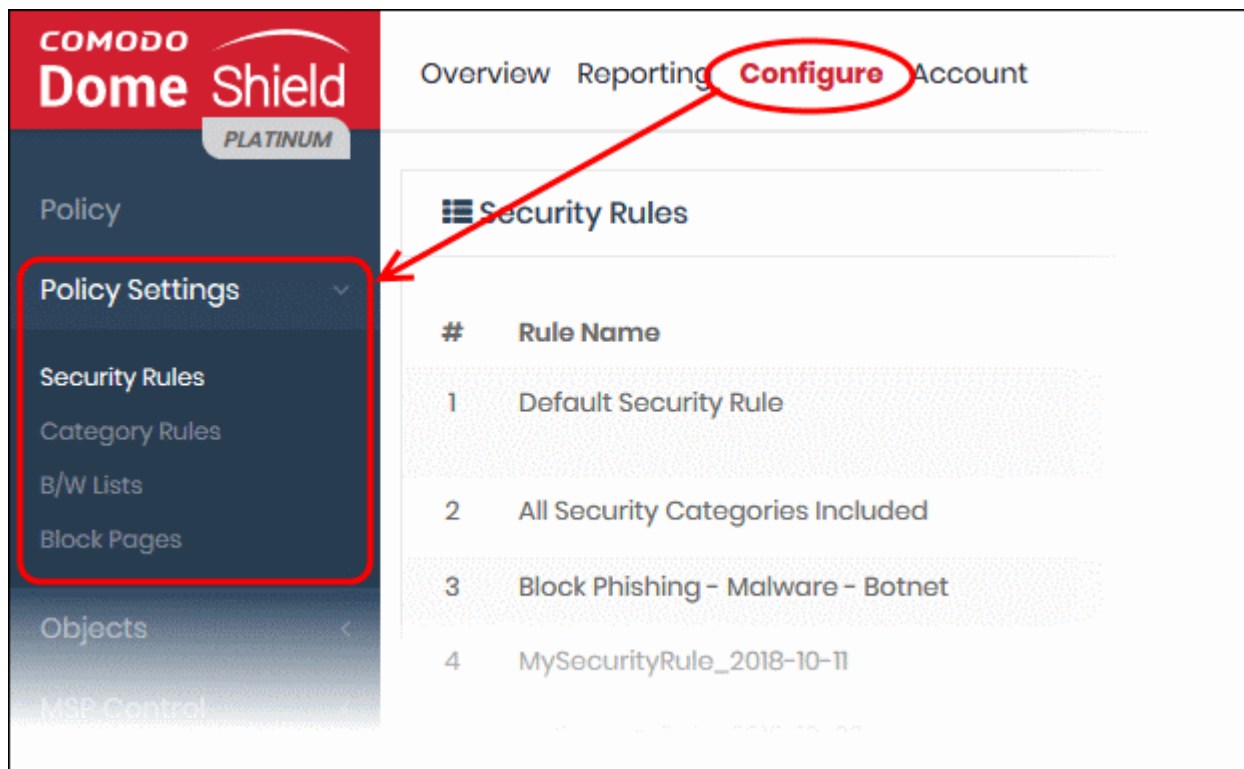- Click the trash can icon beside the internal domain to be removed.

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

5 Manage Shield Rules

The 'Policy Settings' area lets you create and manage security rules which can be added to your security 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 that 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. You can create custom block page messages and have the option to redirect users to a different URL.

- Black and whitelists over-rule any 'Security' or 'Category' rules, allowing you to create exceptions in your policy.

- 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**

5.1 Manage Security Rules

- Comodo operates a huge database of harmful websites categorized by threat type. Dome Shield 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	• P2P Nodes	• PUA Domains
• Botnet/c2c Servers/Bot Infected Sources	• Fake AV	• Remote Access Services
• Phishing	• Blackhole/Sinkhole Systems	• Self Signed SSL Sites
• Spyware	• VPN Servers	• Domains with no MX records
• Webspam	• Mobile Threats	• Spam Sources
• Drive-by Downloads	• Known DDoS Sources	• Brute Forcer/Scanner
• Tor Nodes	• Bitcoin Related	

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

- Dome Shield 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.

- Click 'Configure' > 'Policy Settings' > 'Security Rules' to open the 'Security Rules' area:

Security rules interface - Column descriptions	
Rule Name	The name of the rule
Remark	Comments provided for the rule
Actions	Controls to edit / delete the rule

The interface lets you:
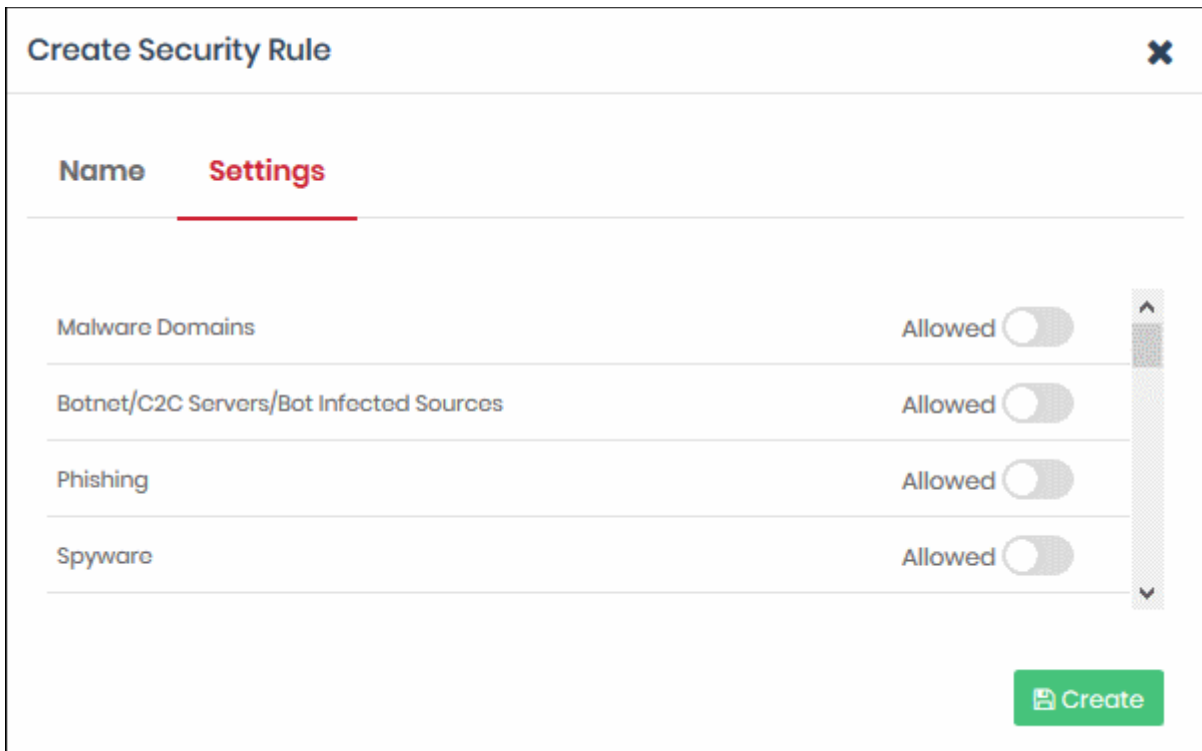
- **Create a new security rule**
- **Edit a security rule**
- **Delete a security rule**

Creating a new security rule

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

- Click ' + Create Security Rule' at the 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' if you want to save your rule at this point.
      OR

    - Click 'Settings' to configure the security categories that you want to allow/block:

COMODO
Creating Trust Online®

- 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:
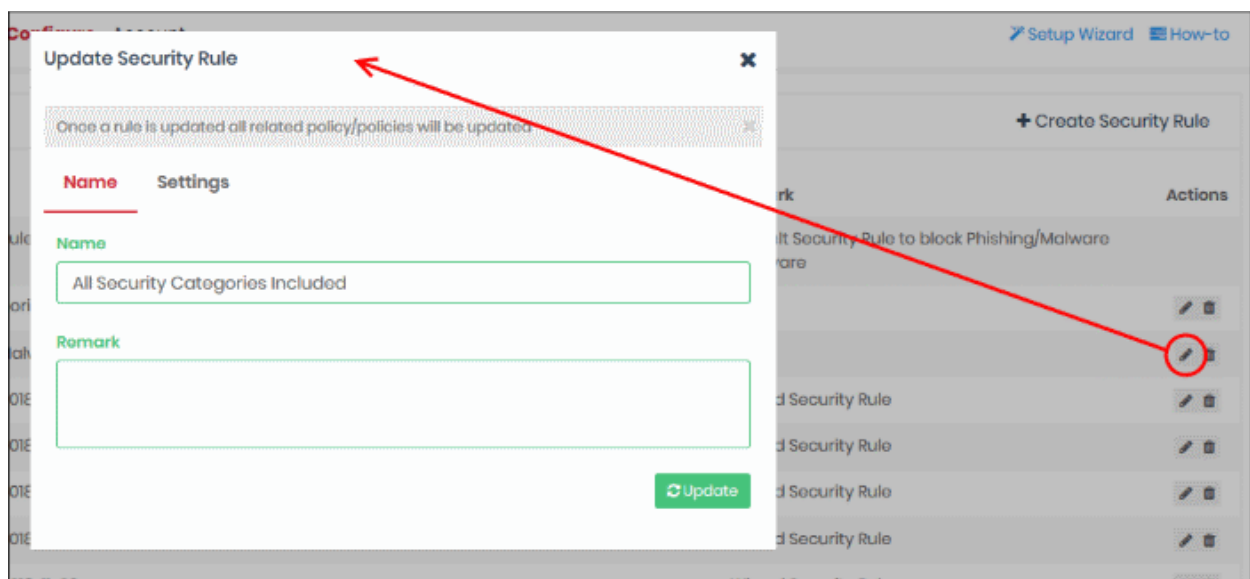

The 'Update Security Rule' dialog will appear. The dialog is similar to the 'Create Security Rule' dialog explained **above**.

- Modify the name, description and/or category settings per your requirements.

- Click the 'Update' button

Any policies containing the rule will be 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 [trash icon] beside a rule to delete it.

A confirmation dialog will be displayed:
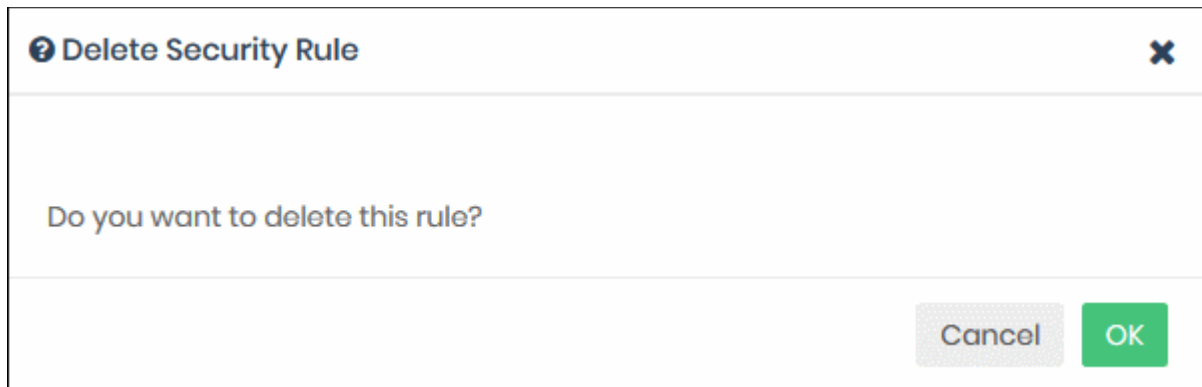
- Click 'OK' to confirm rule deletion.

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.

  - Security rules focus on harmful categories like phishing and malware. Category rules let you apply policy to sites falling under a broader range of topics.

- 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.

- Click 'Configure' > 'Policy Settings' > 'Category Rules' to open the category rules area:
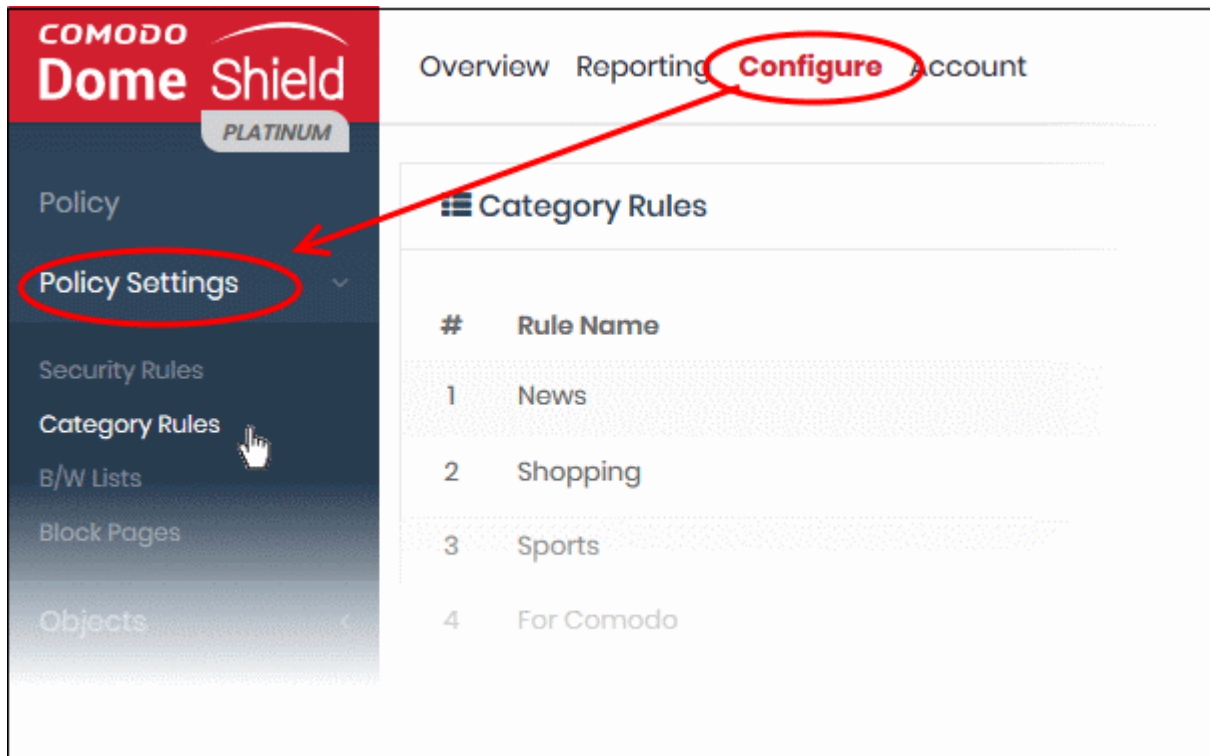
Category Rules - Table of Column Descriptions	
Column Header	**Description**
Rule Name	The label of the rule
Remark	Comments provided for the rule
Actions	Edit / delete the rule

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
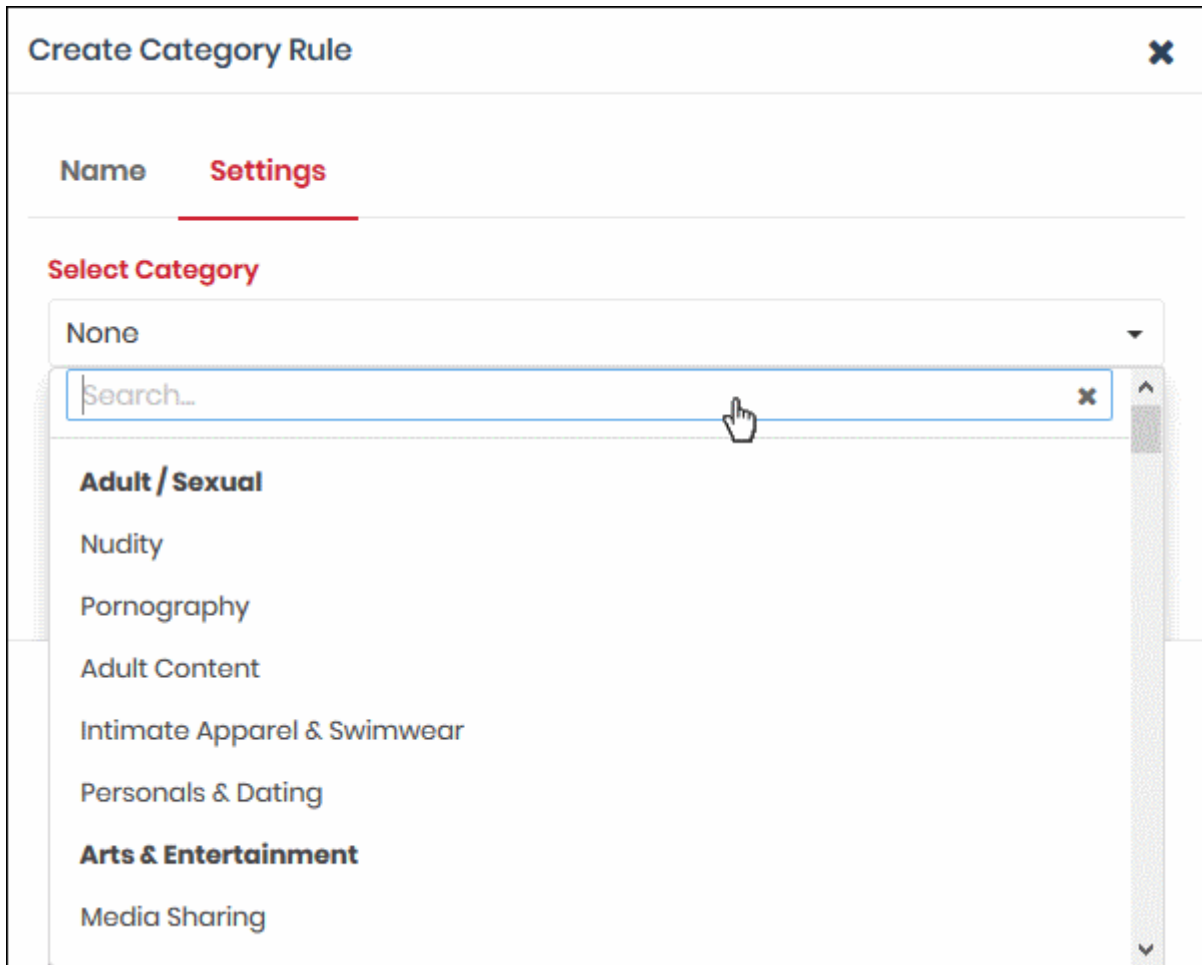
- Enter an appropriate name for the category rule in the 'Name' field.
- Enter a description of the rule in the 'Remark' field, if required.
- Click 'Settings' or 'Next' to choose which categories you want to block/allow:

COMODO
Creating Trust Online®
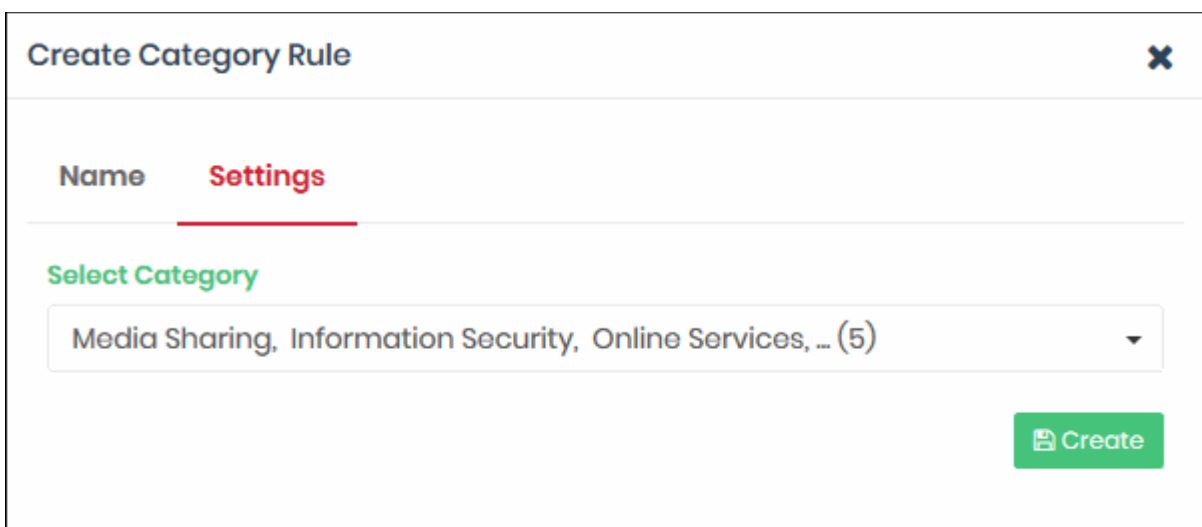
- Use the 'Select Category' drop-down to choose the types of website you wish to block.

- 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 will be displayed at the end of the list:

- Click the 'Create' button at the bottom of the dialog when done.

The website category rule will be 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:
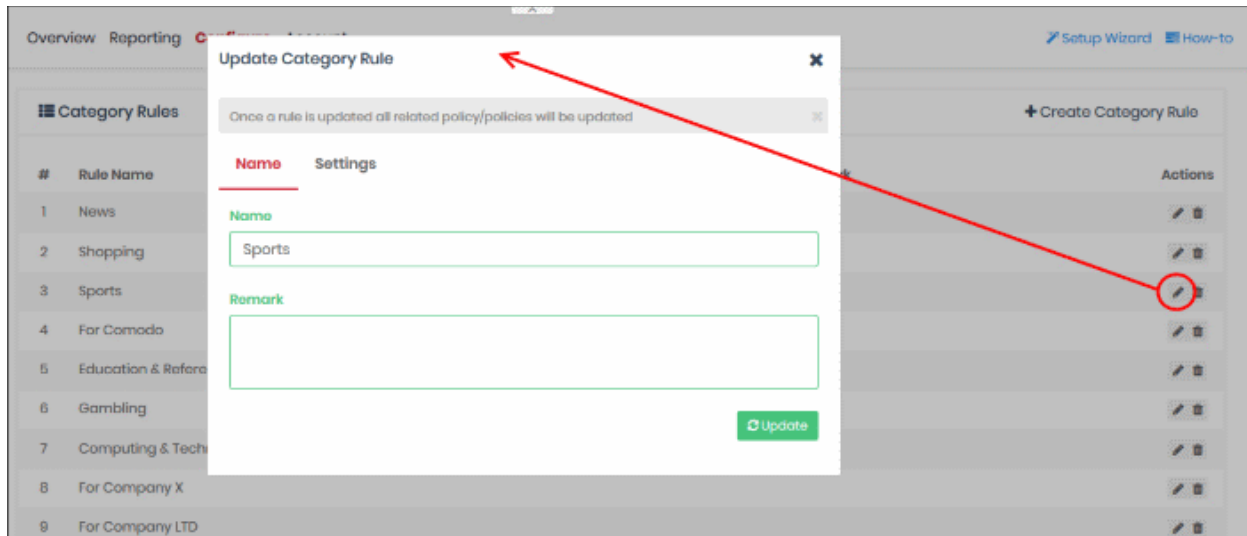
The 'Update Category Rule' dialog will appear. The dialog is similar to 'Create Category Rule' dialog explained **above**.

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

Any policies which use this rule will be 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.

A confirmation dialog will be displayed.

- Click 'OK' to confirm removal of the rule from the list

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.

- Black and whitelists over-rule category and security rules. 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' when configuring 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:
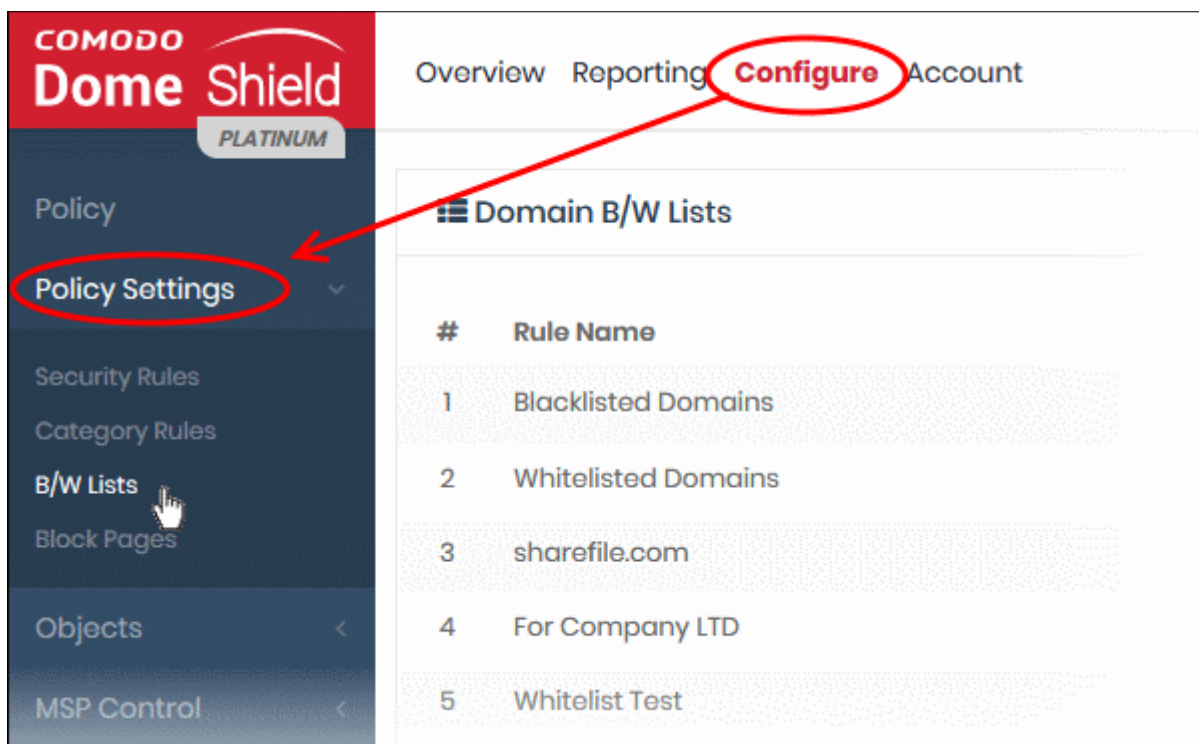
The list of B/W list rules will be displayed.

Domain B/W Lists - Table of Column Descriptions	
Column Header	**Description**
Rule Name	The name of the domain B/W list
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
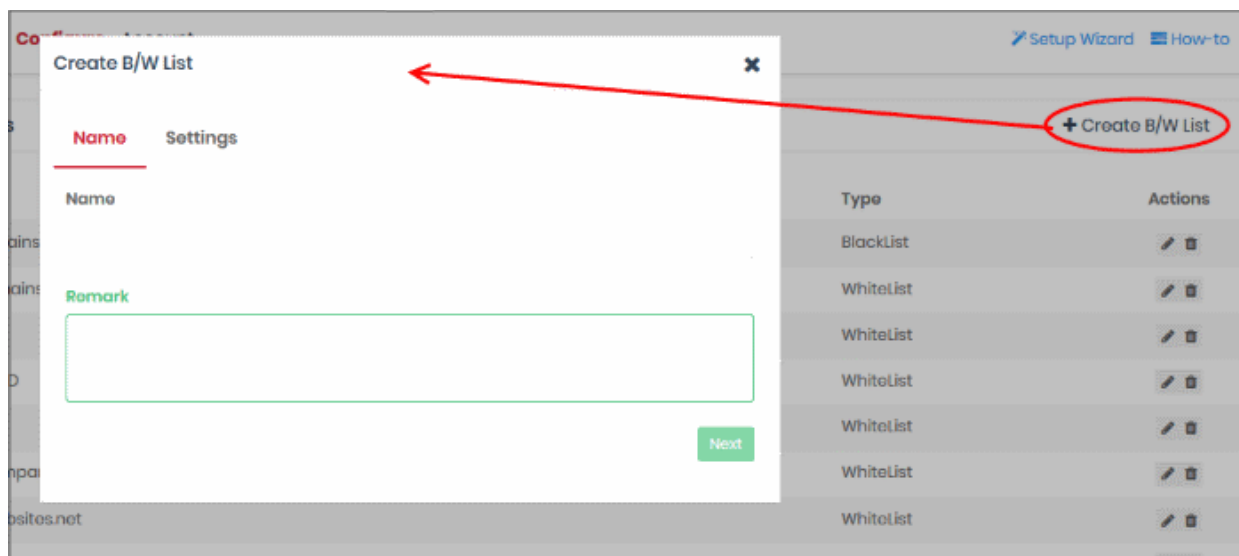
- Enter an appropriate name for the list in the 'Name' field.

- Enter a short description for the B/W list in the 'Remark' field, if required.

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

- Select Whitelist' or 'Blacklist' as required and enter the domain name without the 'http://' or 'https://' prefix.
- Click the '+' button to add the domain to the rule. Repeat the process to add more domain names.

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

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

Editing a domain blacklist / whitelist

- To update a B/W list, click the edit ✏ button beside the rule
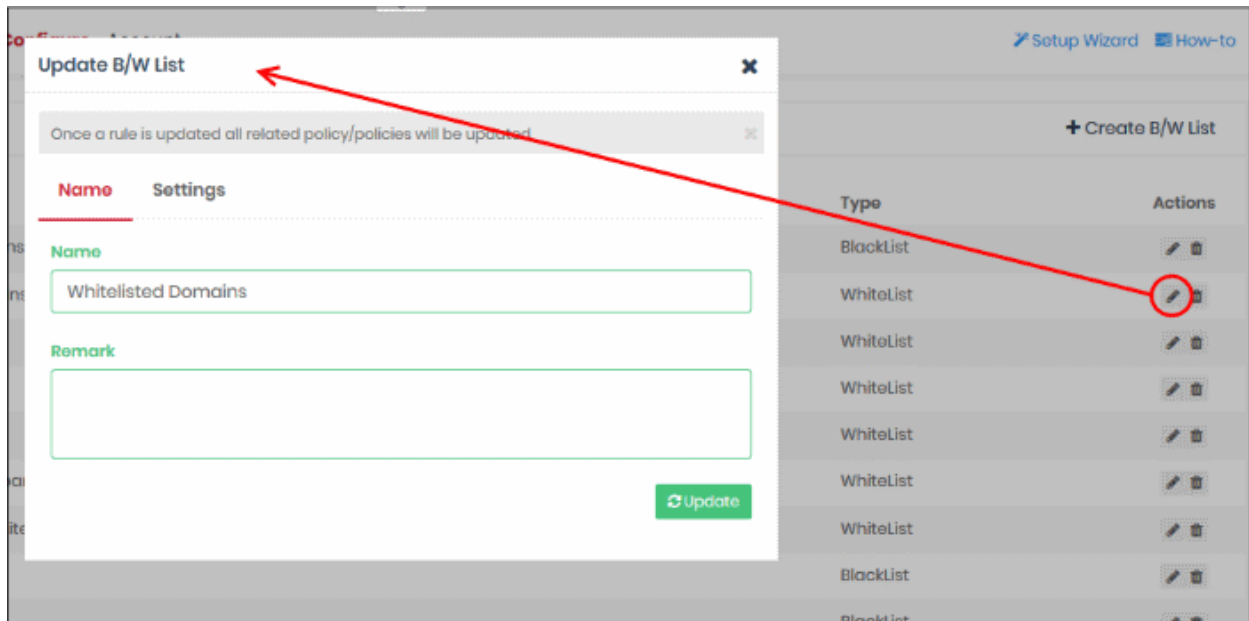
The 'Update B/W List' dialog will appear. The dialog is similar to 'Create B/W List' dialog explained **above**.

- 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.

Deleting 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.

A confirmation dialog will be displayed.

- Click 'OK' to confirm removal of the rule from 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.

- 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 rule violations
  - Display custom block messages with your custom banners
  - Redirect users to a specific web-page
- You need to install the Dome Shield SSL certificate on all protected endpoints. This so the block page displays correctly over HTTPS connections.
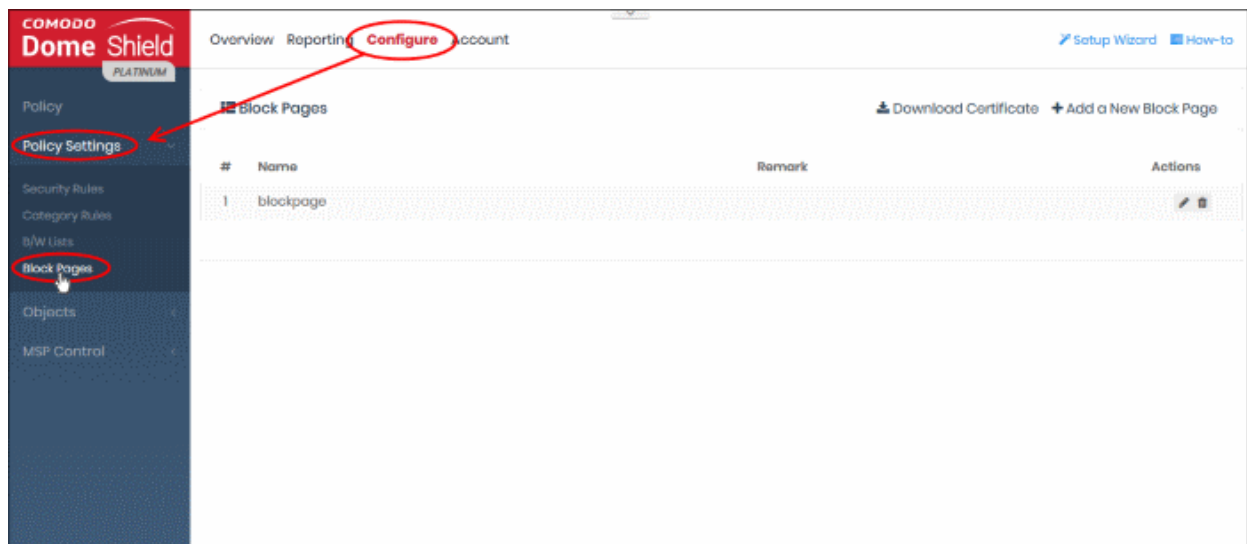

Block Pages - Table of Column Descriptions	
Column Header	**Description**
Name	Label of the block page
Remark	Comments provided for the page. The name and remark should identify the purpose of the page.
Actions	Controls to edit / delete the block page

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
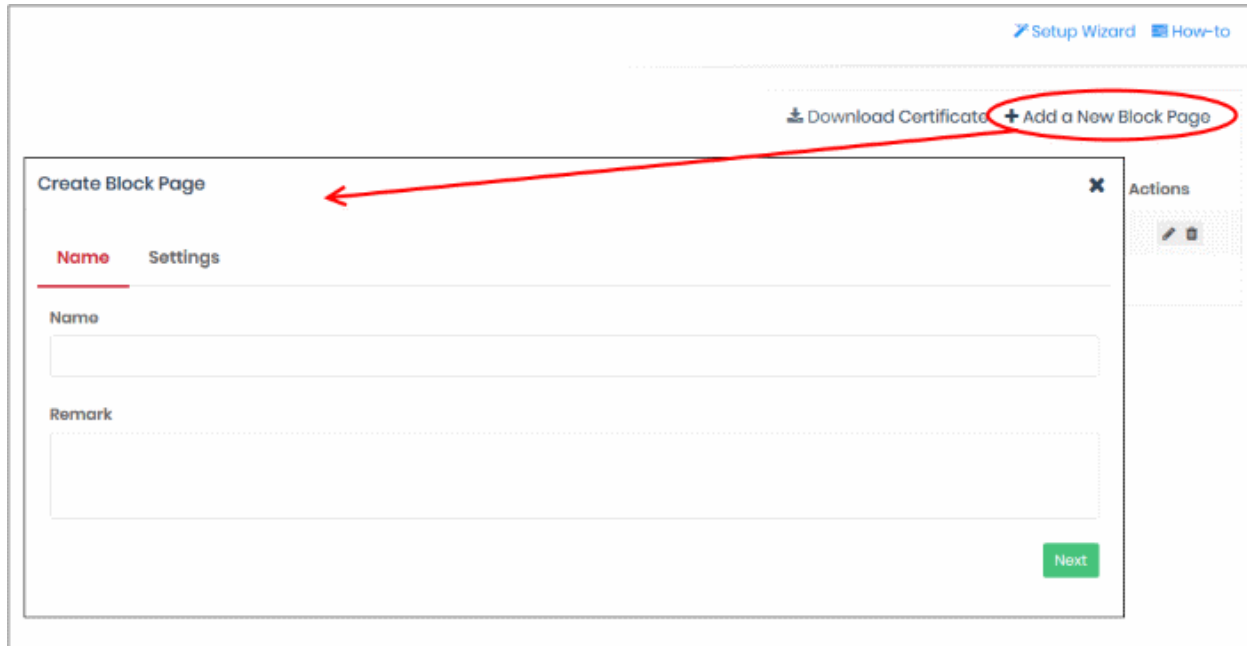
- Name - Enter a descriptive label for the block page
- Remark - Type internal notes/comments about the page if required. Text you enter here will not be shown in the block page itself.
- Click 'Next' or 'Settings' to configure the block page
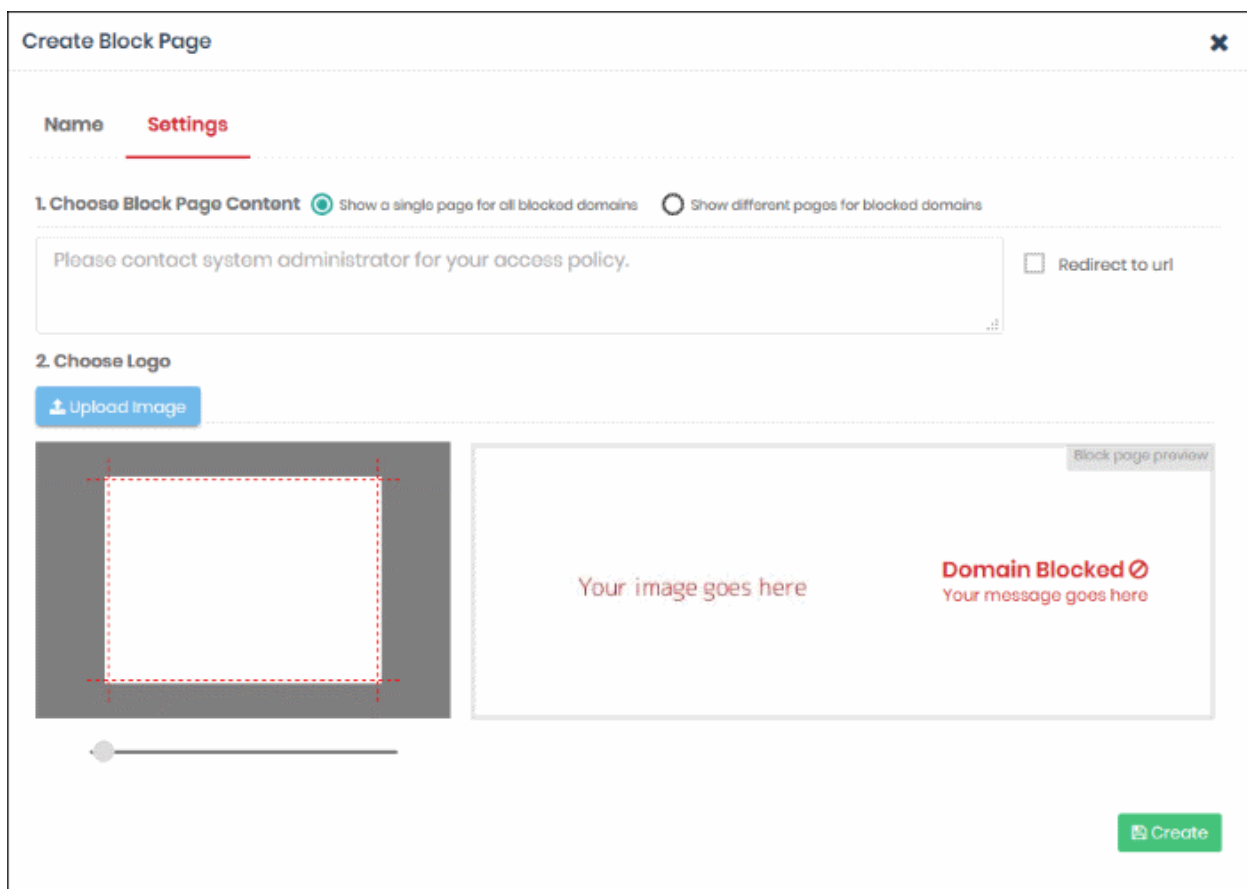
You now need to create your block page content and upload your logo:

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** - A single block page or redirect page is shown regardless of which type of rule is violated.
- **Show different pages for blocked domains** - Show specific block pages if 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 specific URL instead. Please specify the full URL if you use this option. For example, https://www.example.com/security-redirect-page.php .
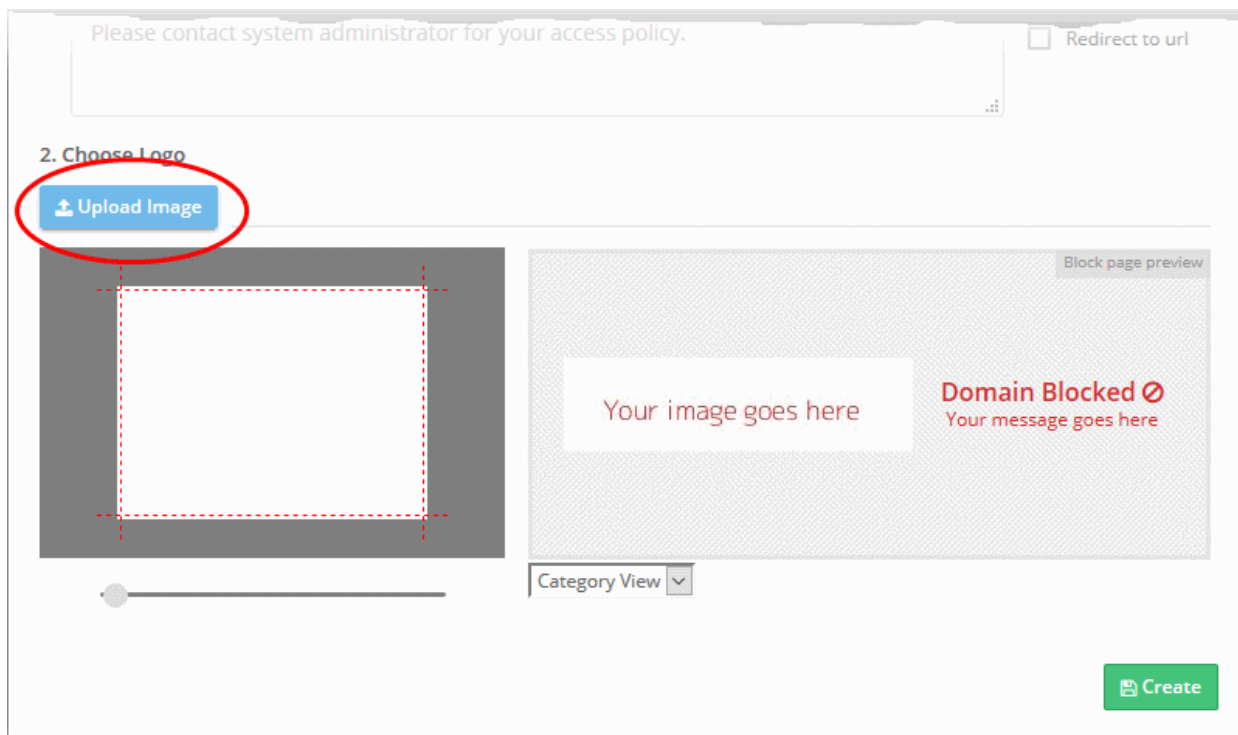
Step 2 - Upload Your Logo

- The interface shows the Dome Shield logo on the block page by default.
- You can change this to your own company logo by uploading a suitable .png or .svg file
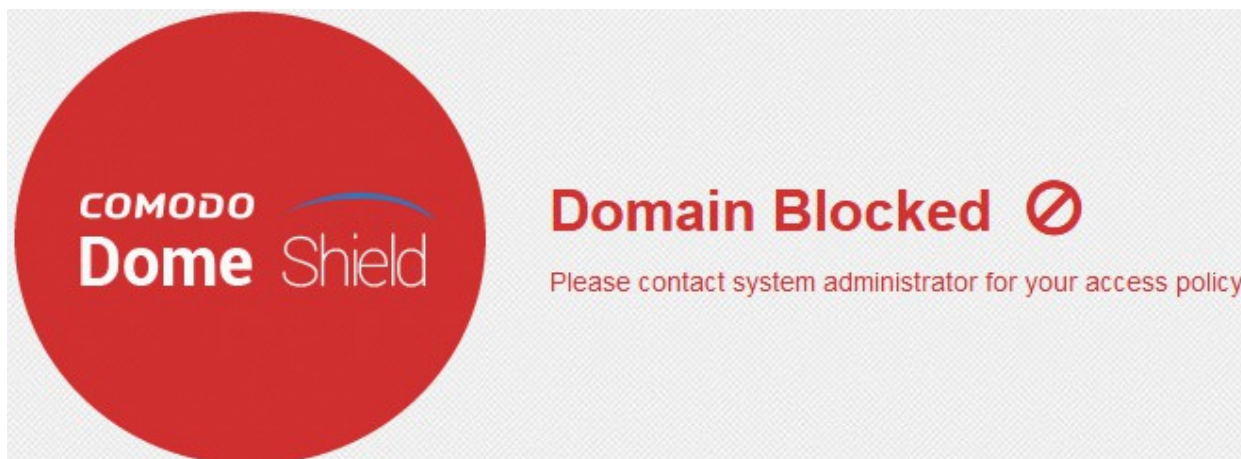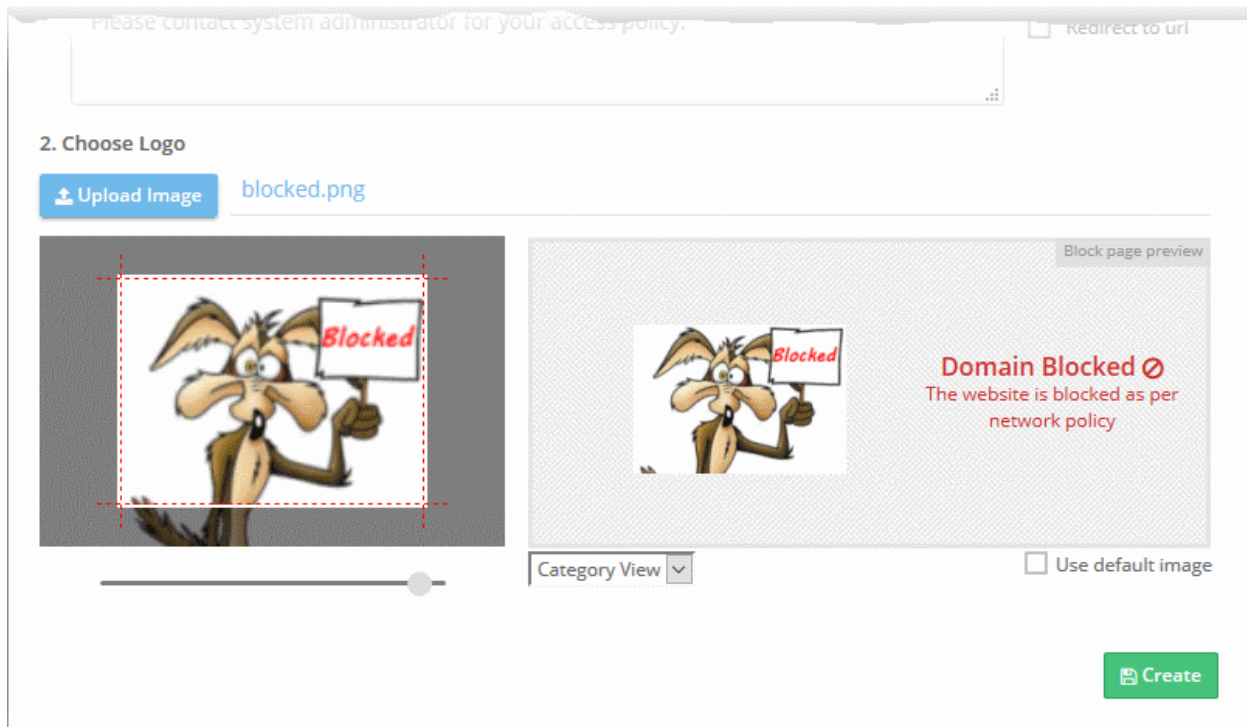
- Click 'Upload Image' under 'Choose Logo'. Browse to the location of your image and click 'Open'

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

Your image will appear 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 will appear 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 Dome Shield logo is shown as the block page.

- Click 'Create'

The new block page will be 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 Dome Shield.

- You can avoid these errors by installing the Dome SSL certificate on all protected endpoints.

Download and install the certificate

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

- Click 'Download Certificate' at top-right
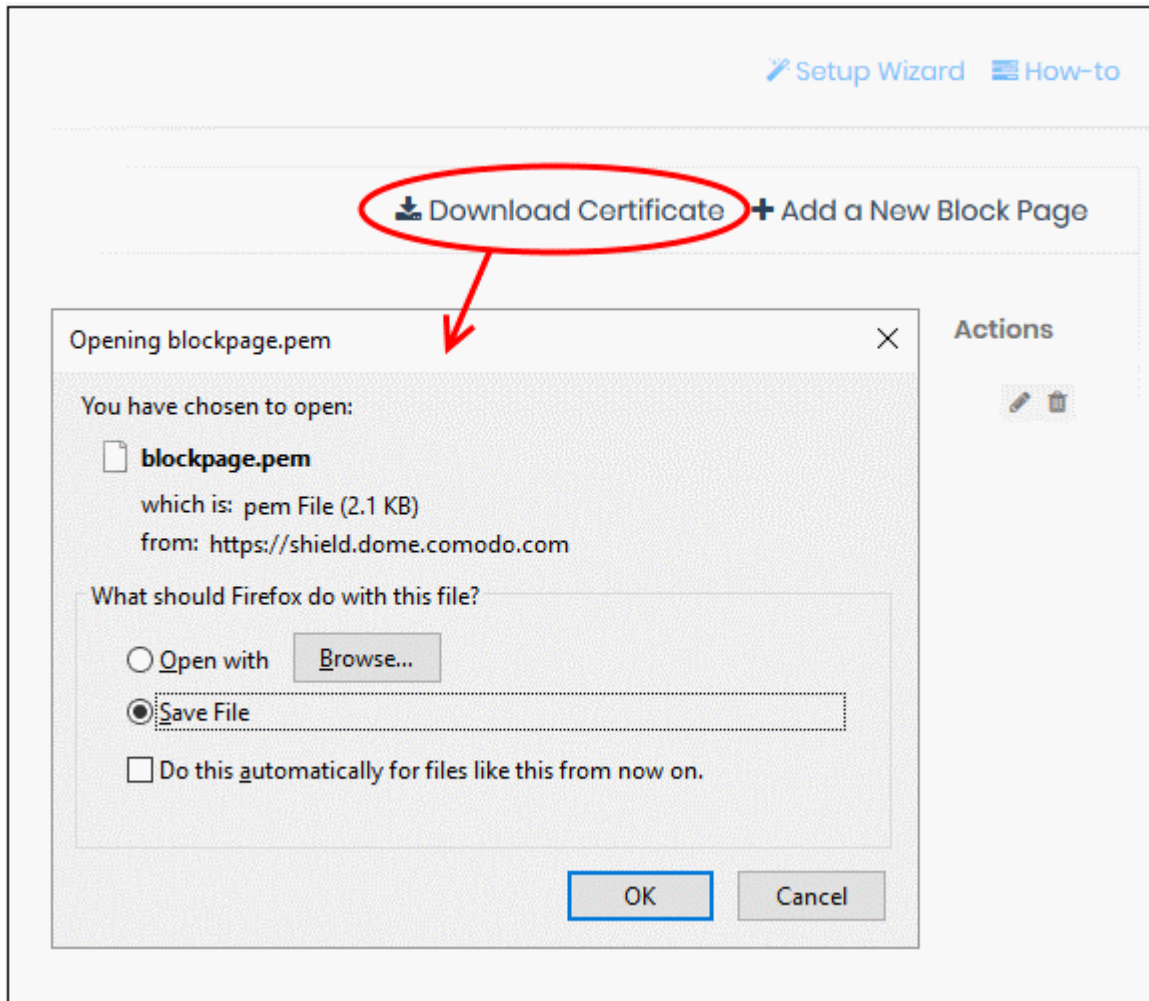
The certificate will be downloaded in .pem format.

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 certifcate store**

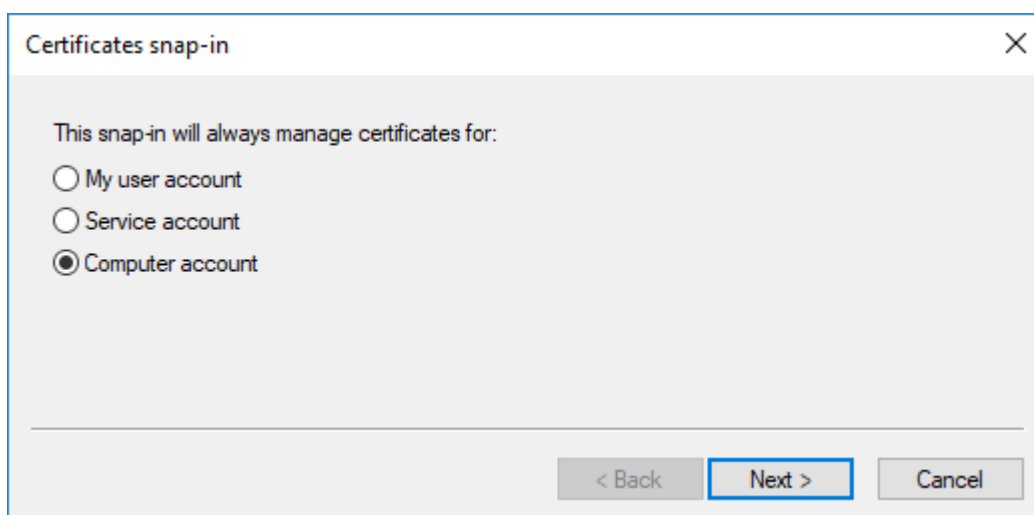**Step 1 - Add 'Certificates' snap-in to Microsoft Management Console (MMC)**

- Open the 'Run' dialog (Win' key + 'R')
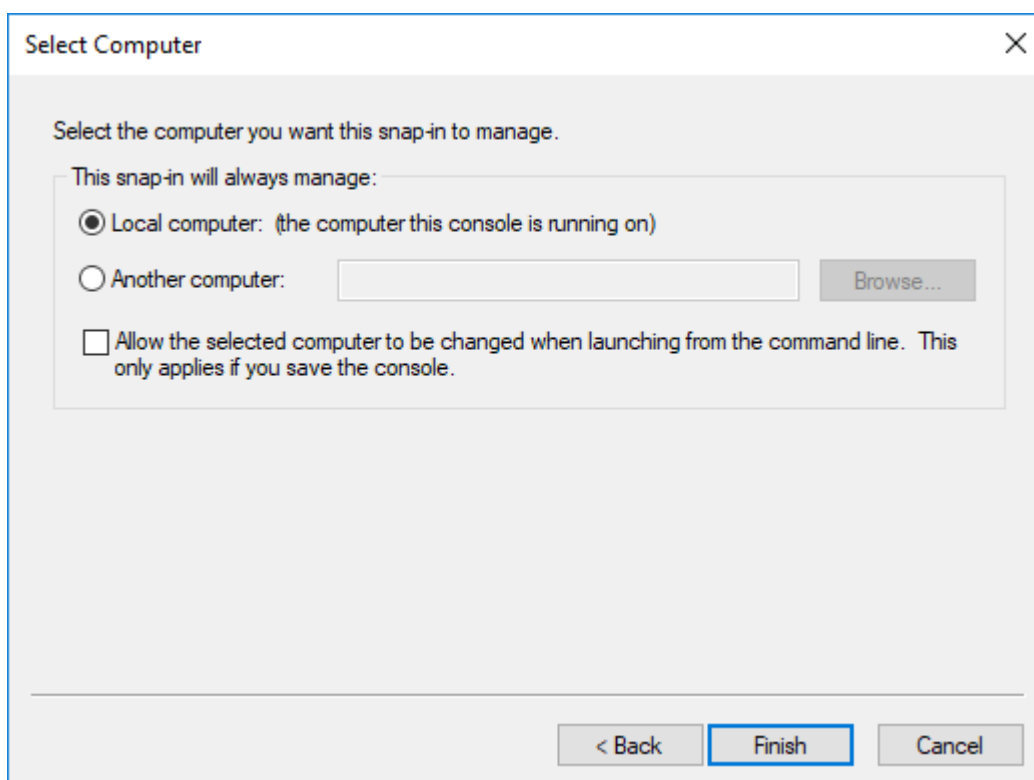- Type 'mmc' in the 'Run' dialog:
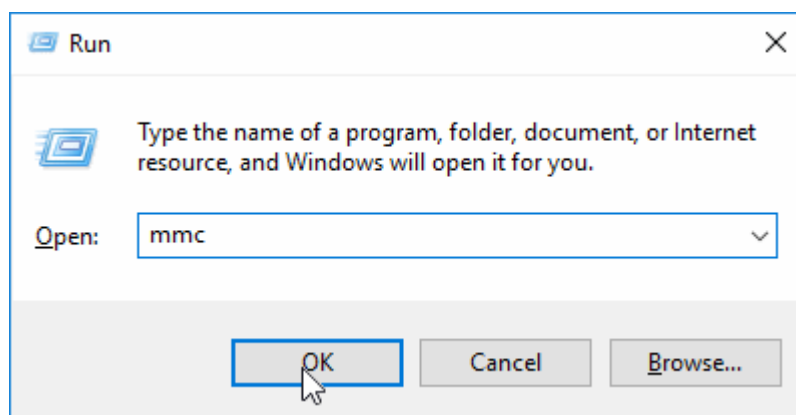
- Click 'File' > 'Add/Remove snap-in' in the console interface

- Select 'Certificates' in the list on the left. Click 'Add' to move it to the list of selected snap-ins.
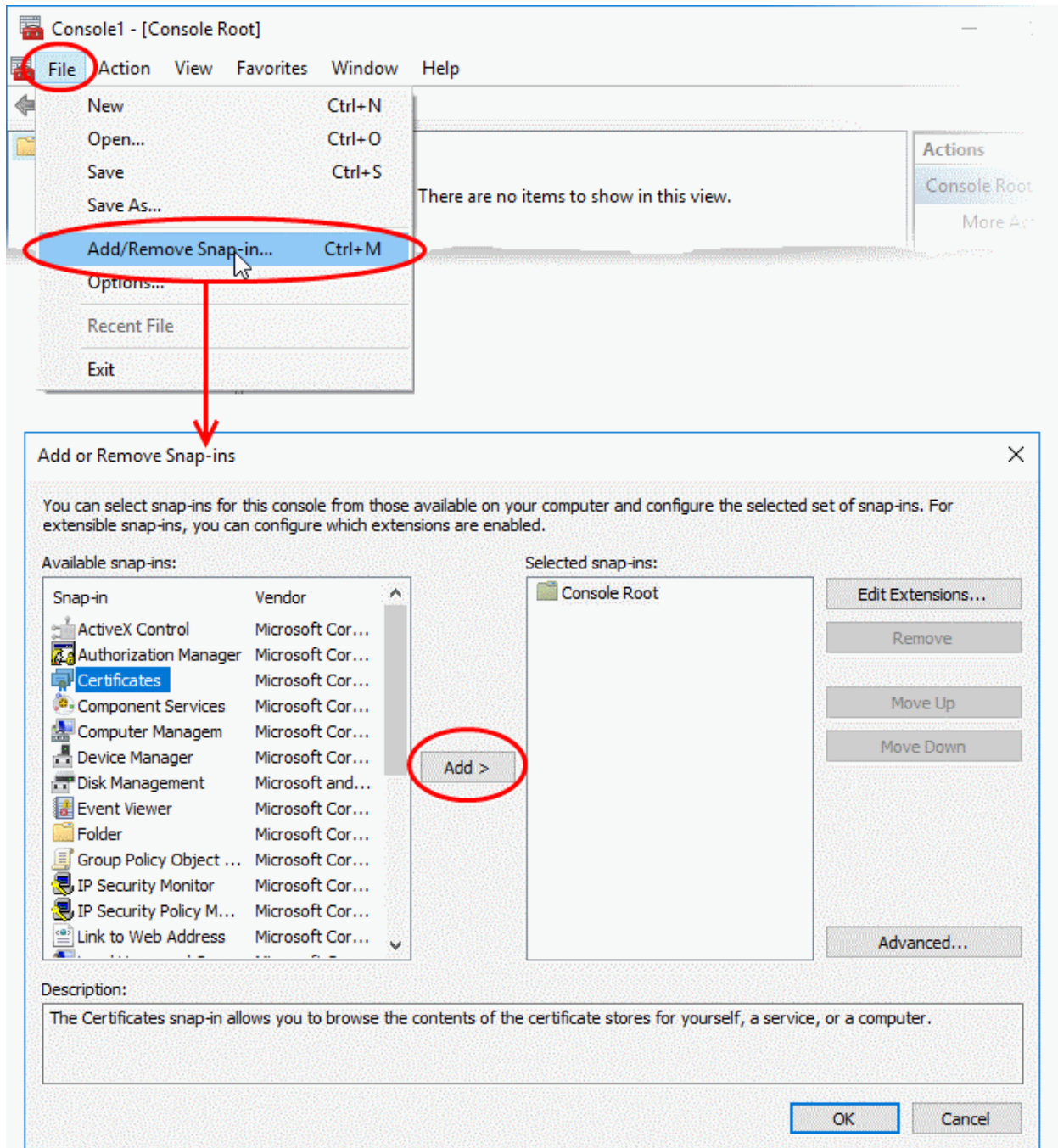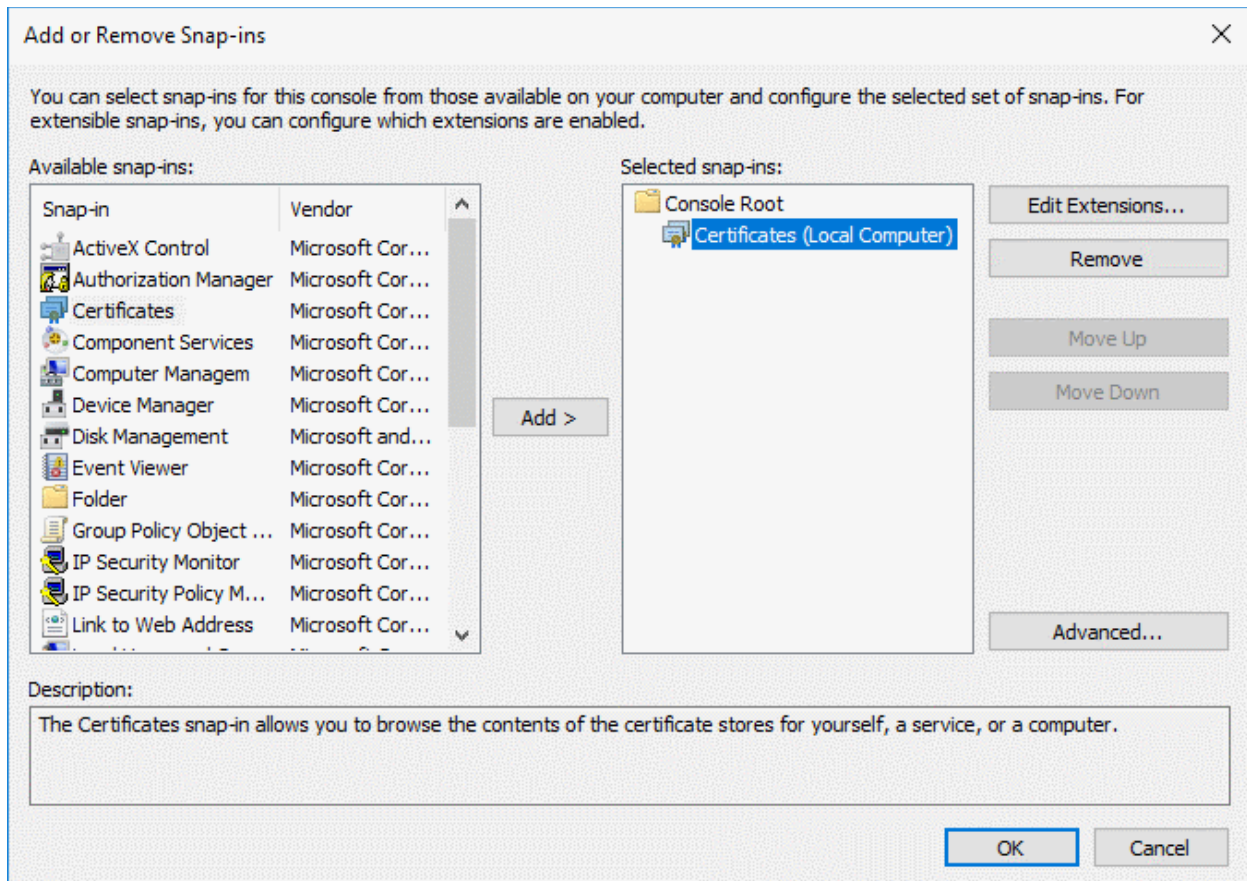

- You will be asked to select the computer and account to which the snap-in should be added:

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

- 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
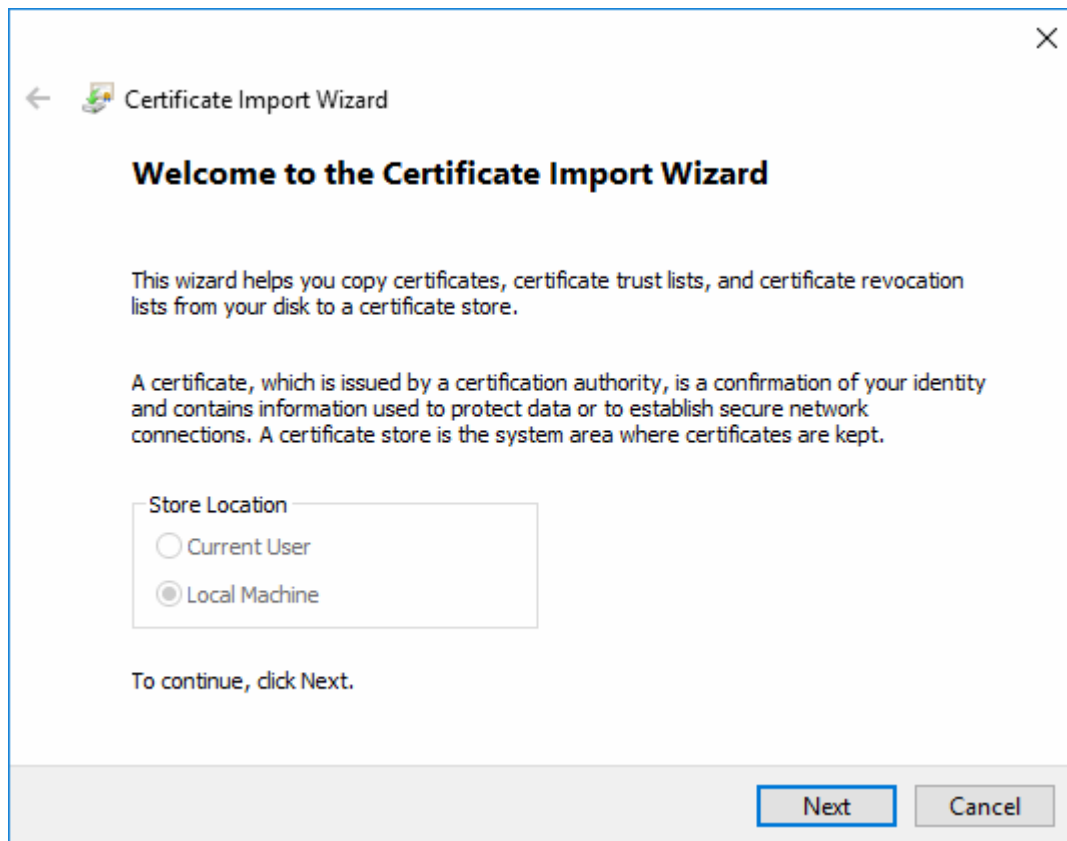
- Expand the 'Certificates (Local Computer)' tree on the left of the MMC console
- Select 'Trusted Root Certification Authorities' :
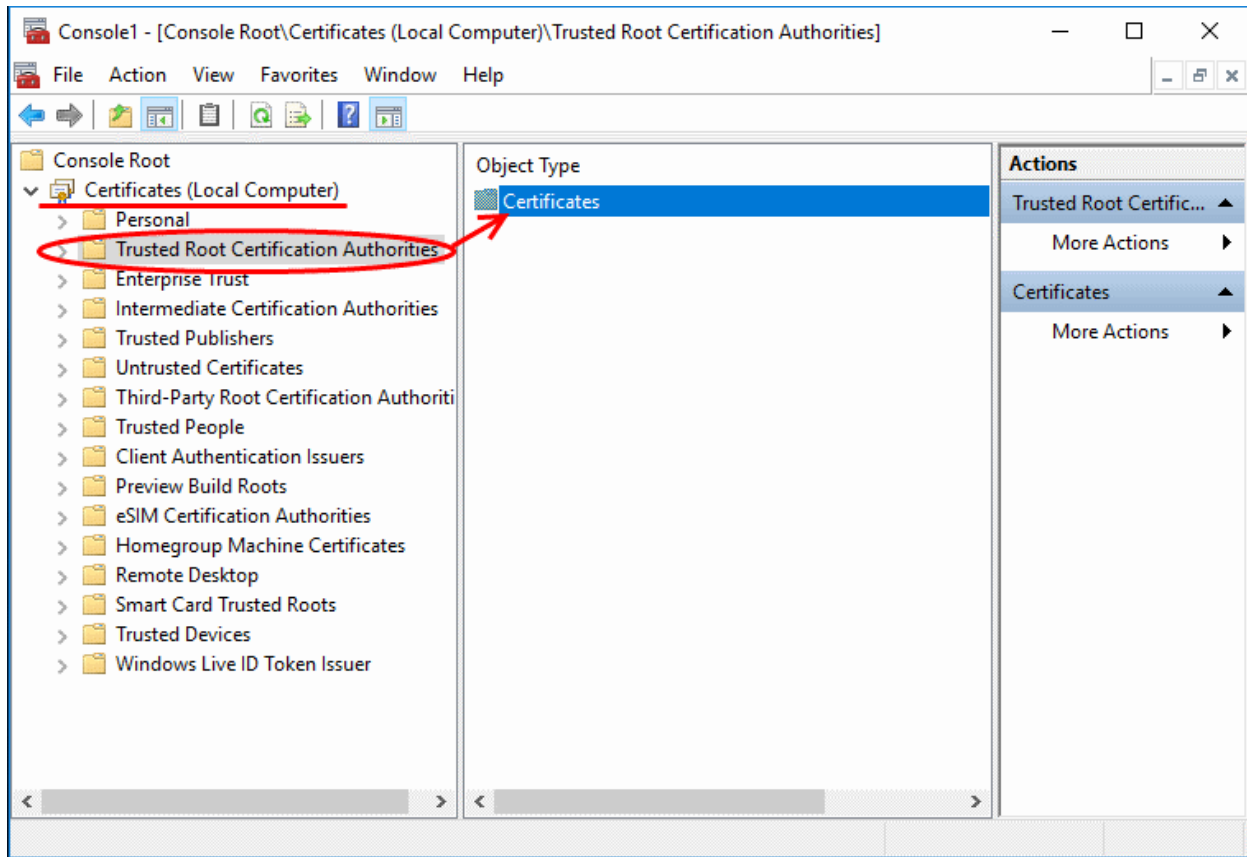
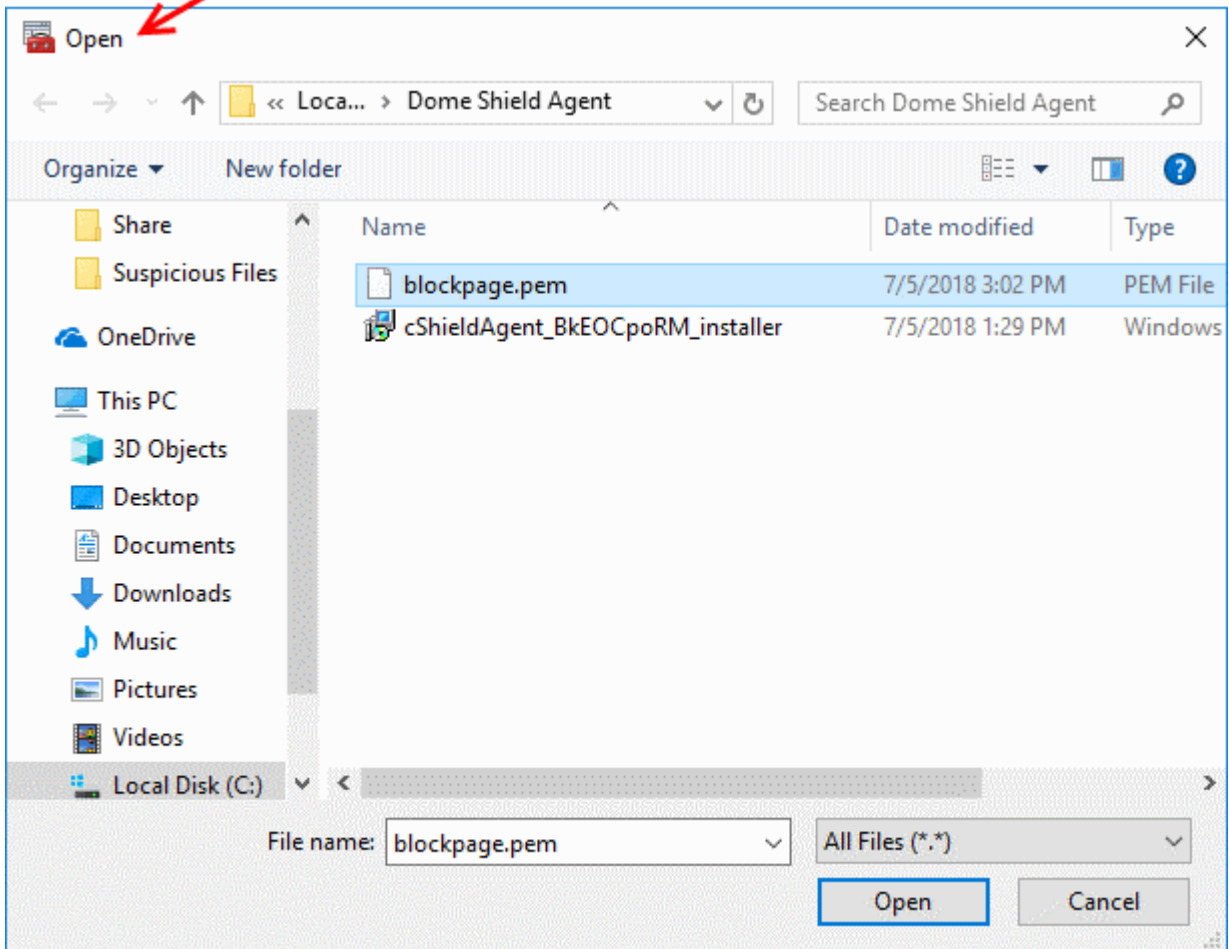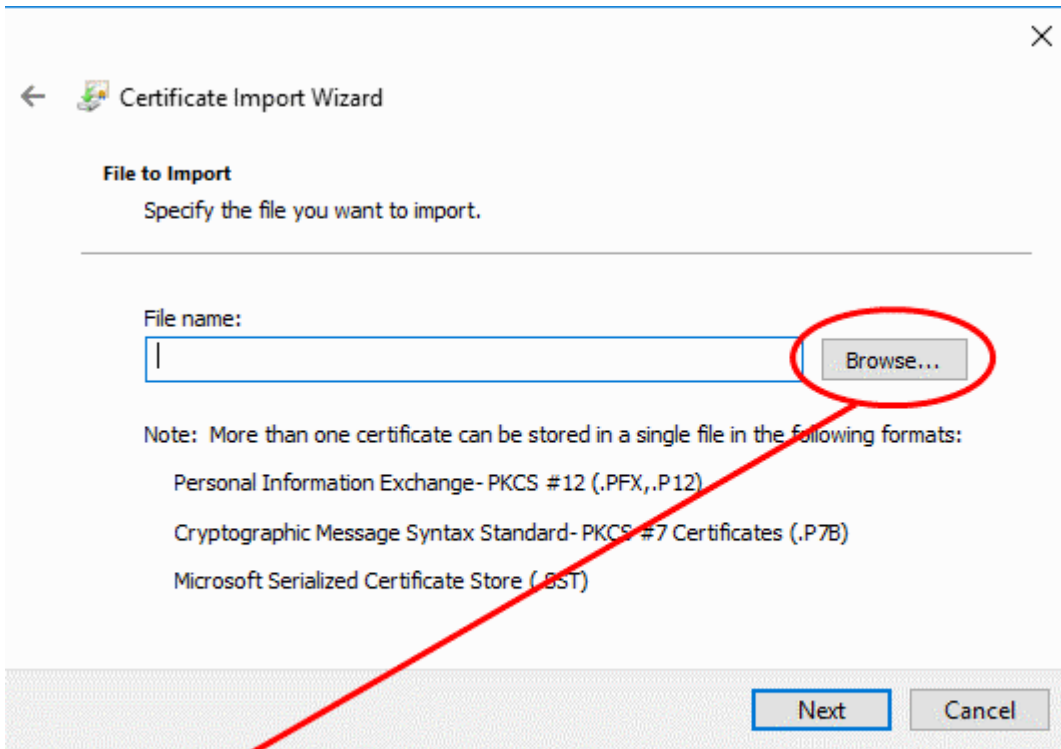• Click 'More Actions' > 'All Tasks' > 'Import', on the right:

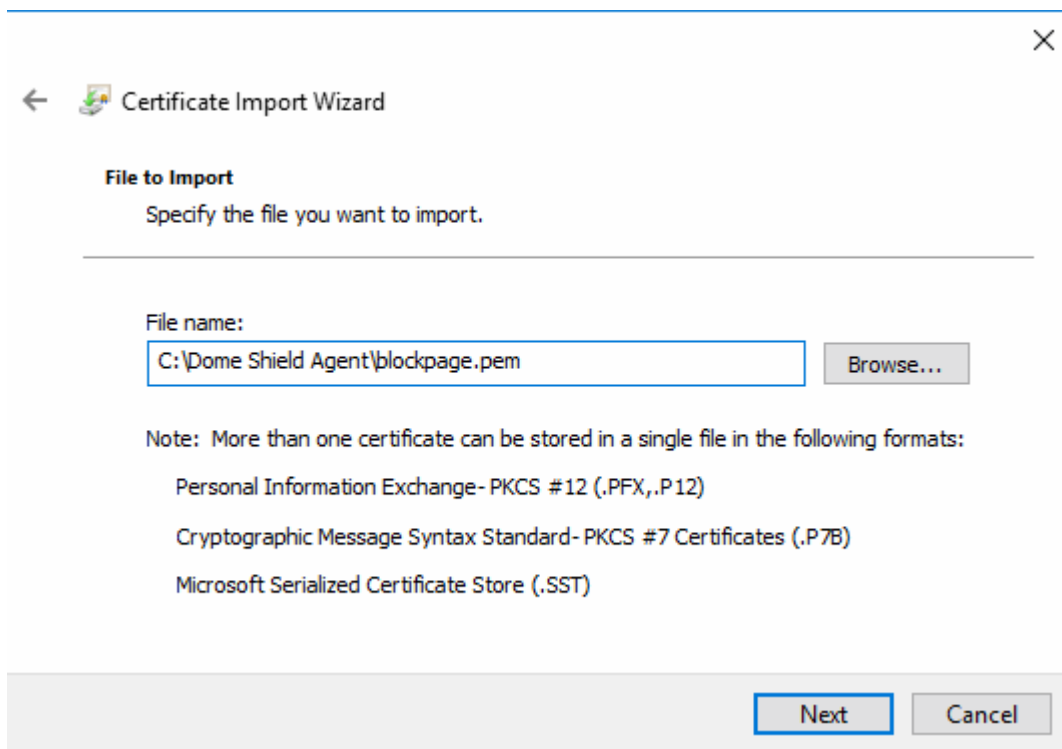The certificate import wizard will start:

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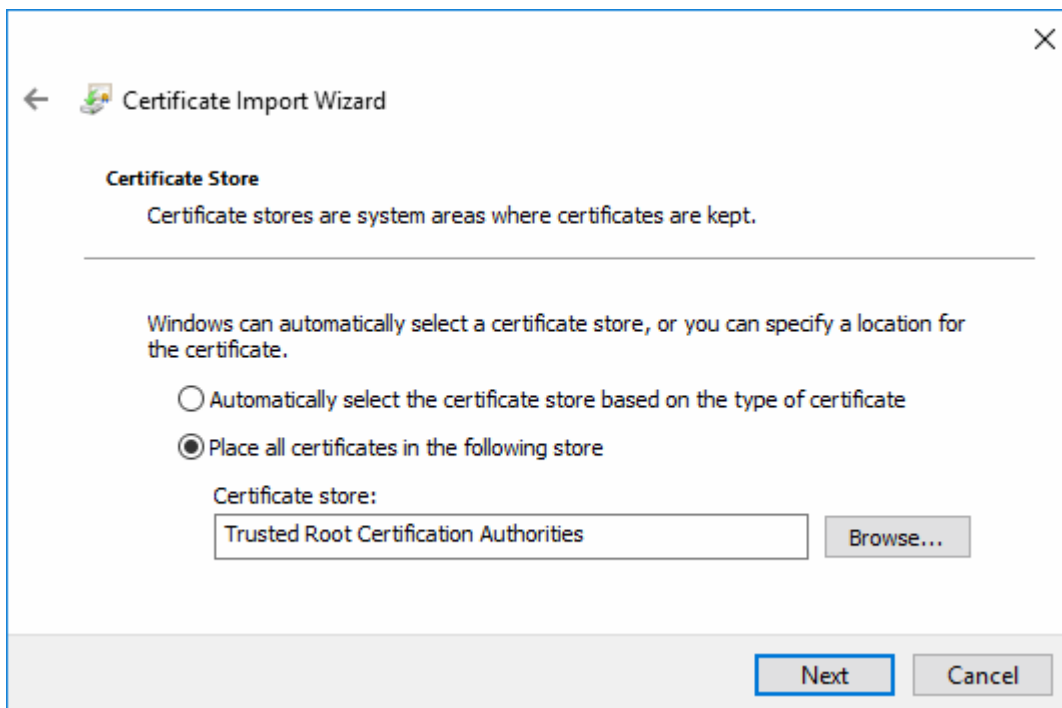- Click 'Browse', navigate to the location of the certificate and select 'blockpage.pem':

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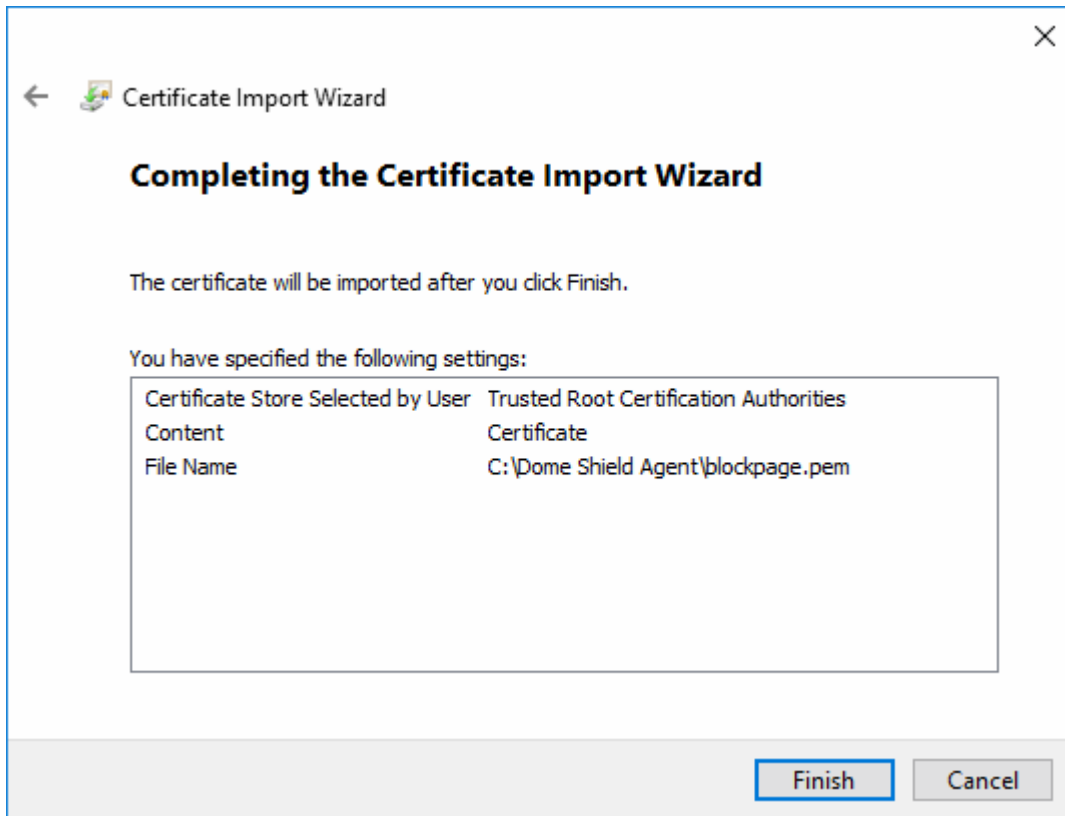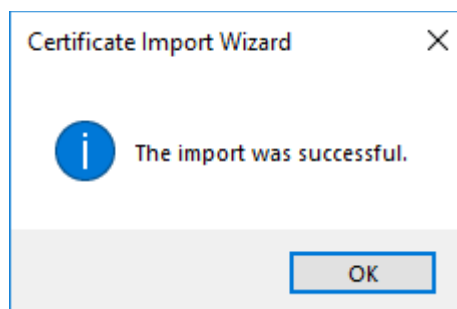
- Click 'Open'

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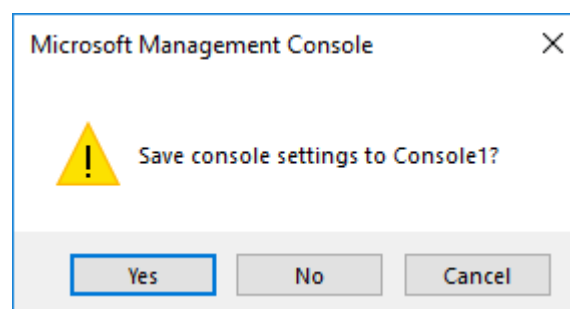

- Confirm that the 'Trusted Root Certification Authorities' store is pre-selected and click 'Next'

- 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 browser users

- Firefox uses its own certificate store instead of the Windows store (which is used by Chrome and Internet Explorer/Edge).

- 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'
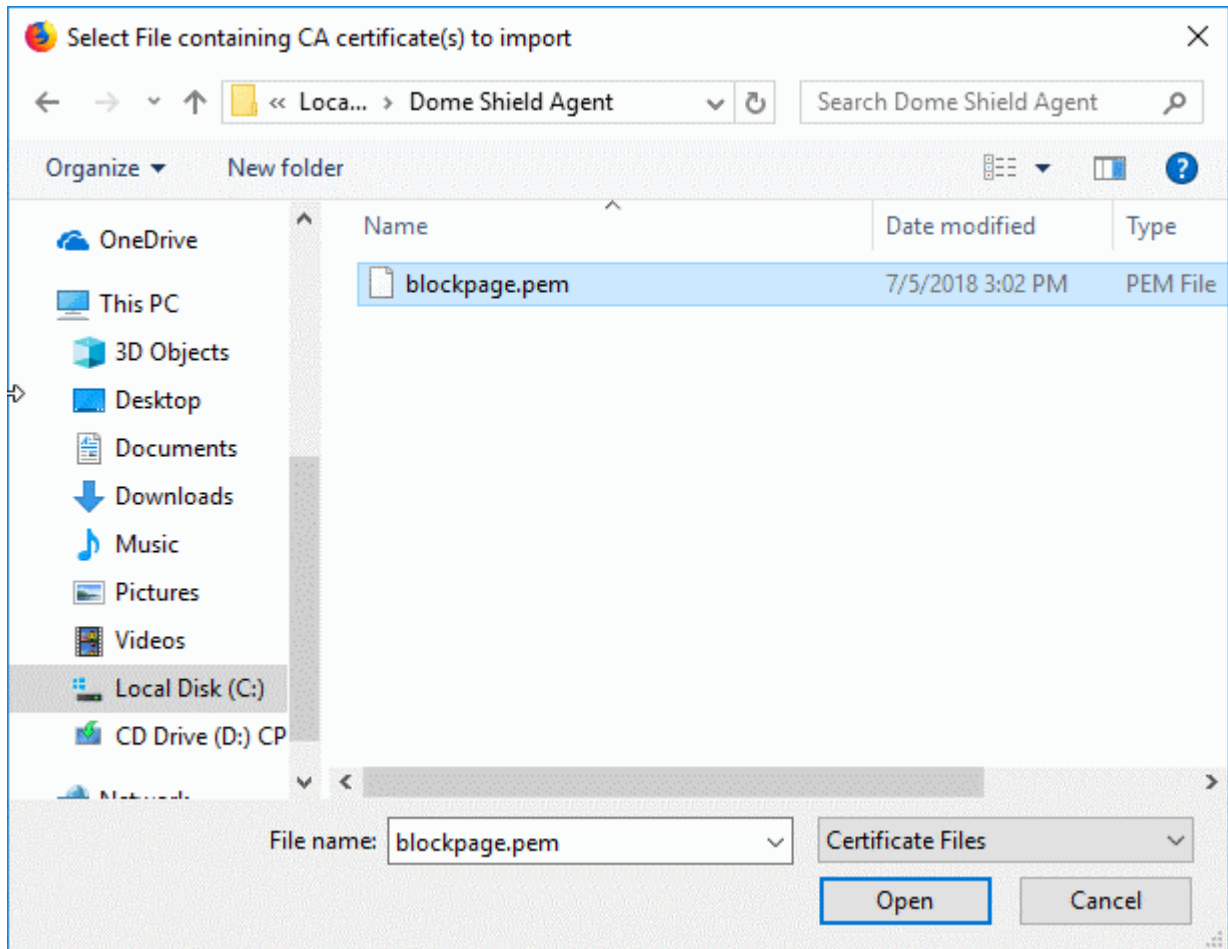
- Browse to and select 'blockpage.pem' then click 'Open'.
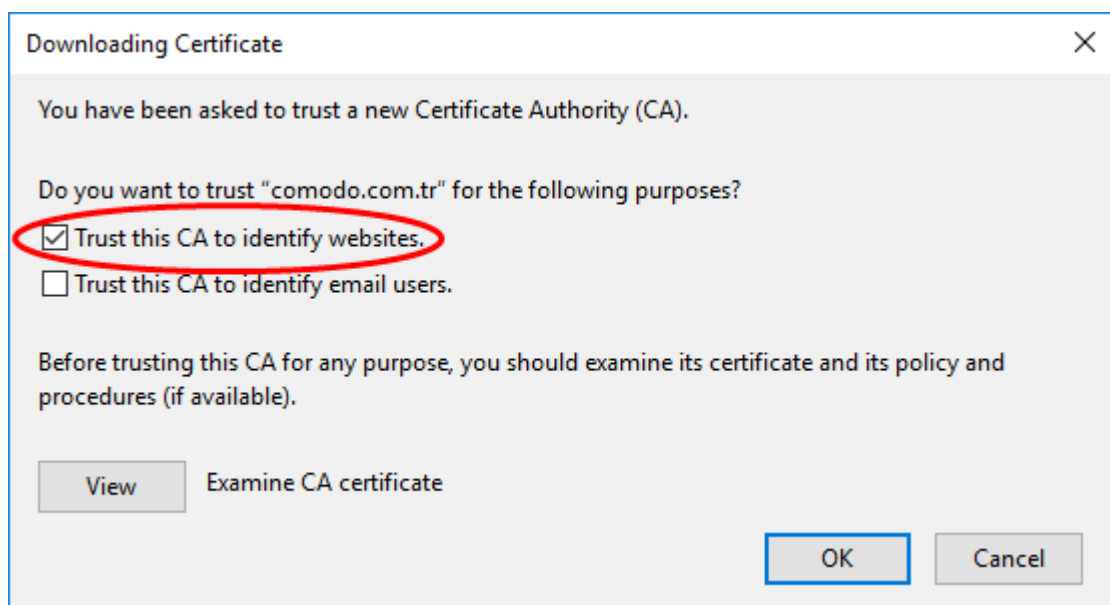
- Select 'Trust this CA to identify websites' and click 'OK'

The certificate will be imported to the Firefox store:
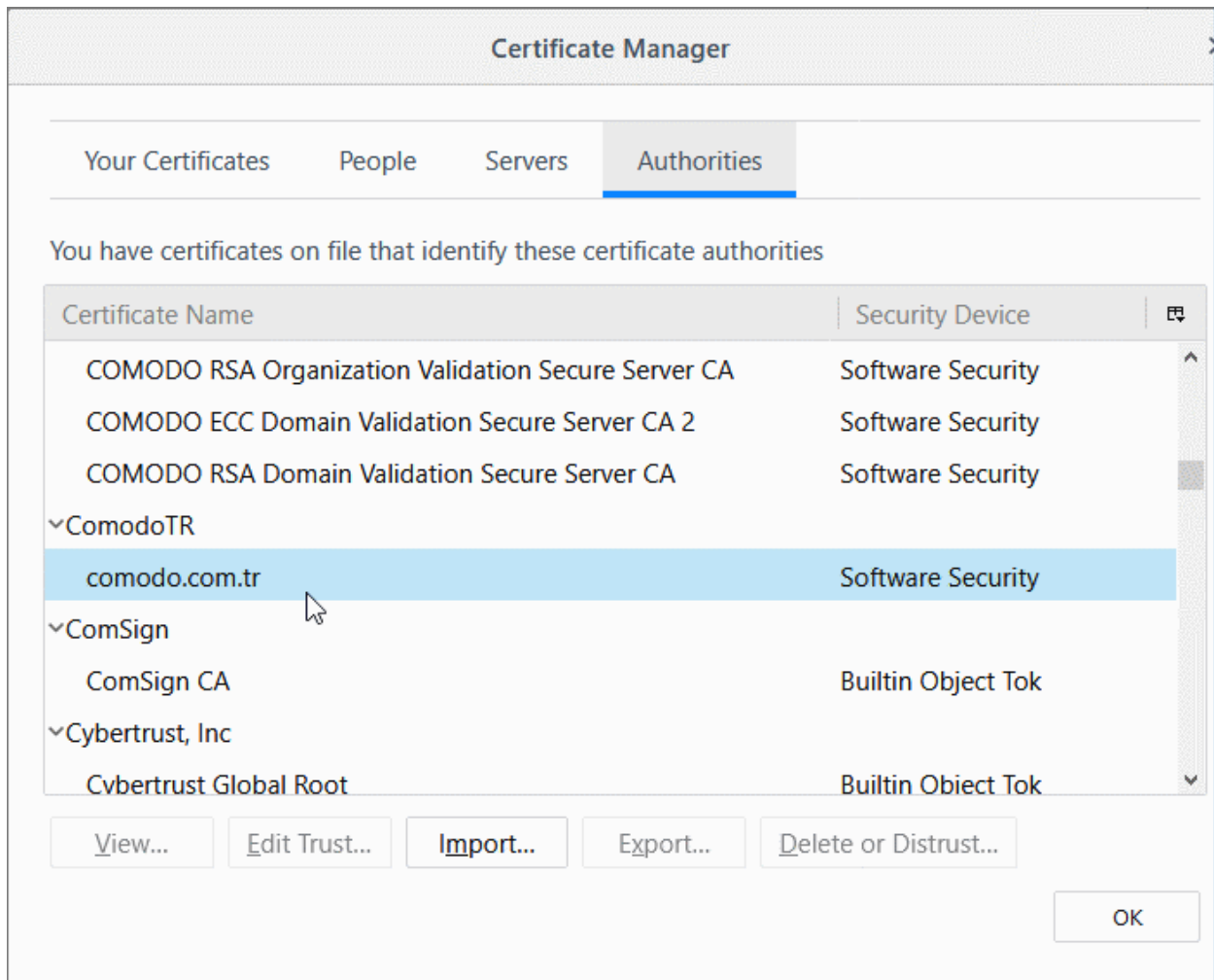
- Click 'OK' to save your changes.

Edit a Block Page

- To update a block page, click the edit ✏ button beside the page in the list
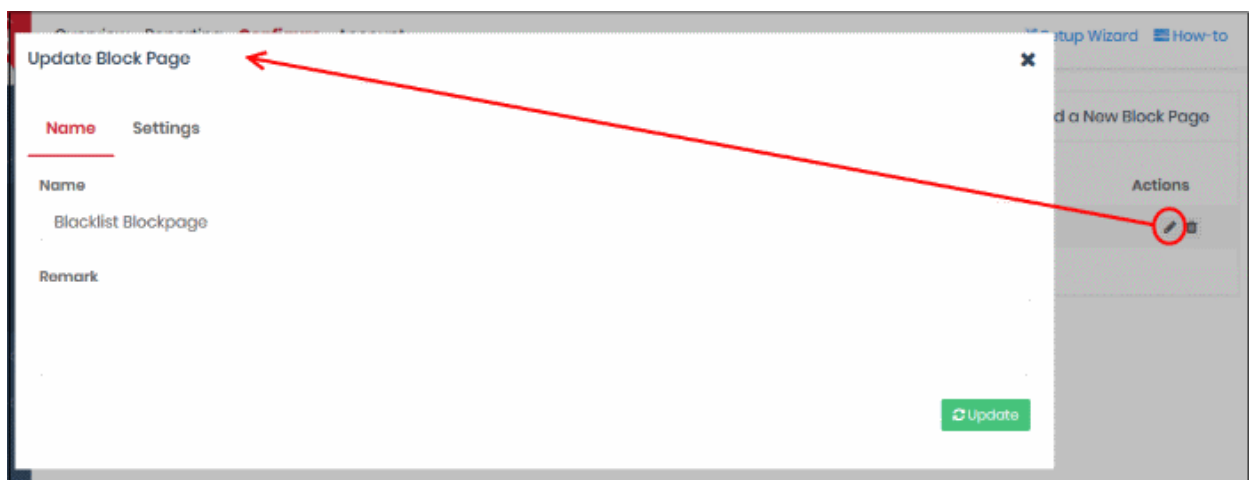
The 'Update Block Page' dialog will appear. The dialog is similar to 'Create Block Page' dialog explained **above**.

- 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:
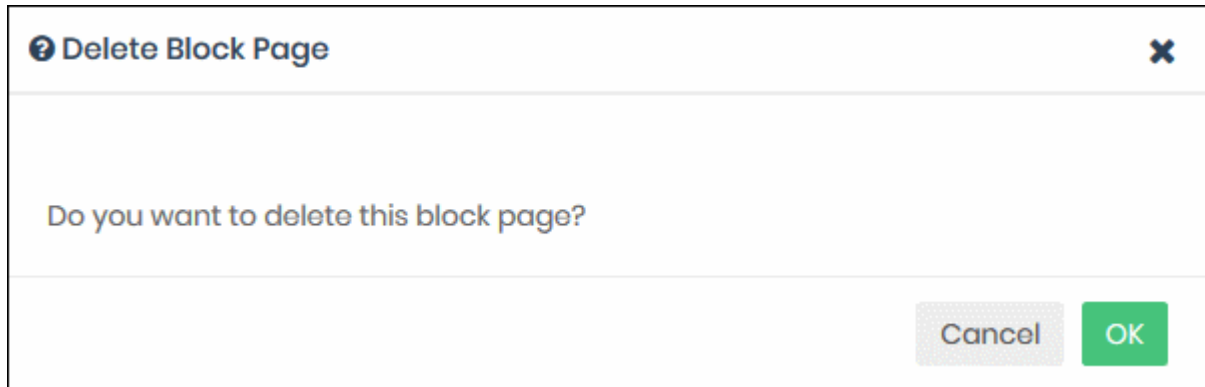
6   Apply Policies to Networks and Roaming/Mobile Devices

- Click 'Configure' > 'Policy' to open the 'Policies' screen
- A 'Policy' in Dome Shield is a security profile containing 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 created at least one rule before you can create a policy. See '**Manage Shield 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
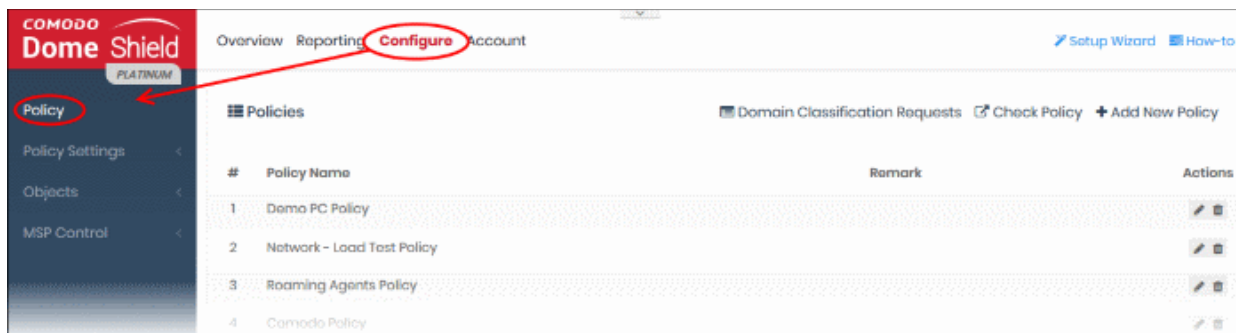
- The links on the right of the title bar let you:

  - **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**
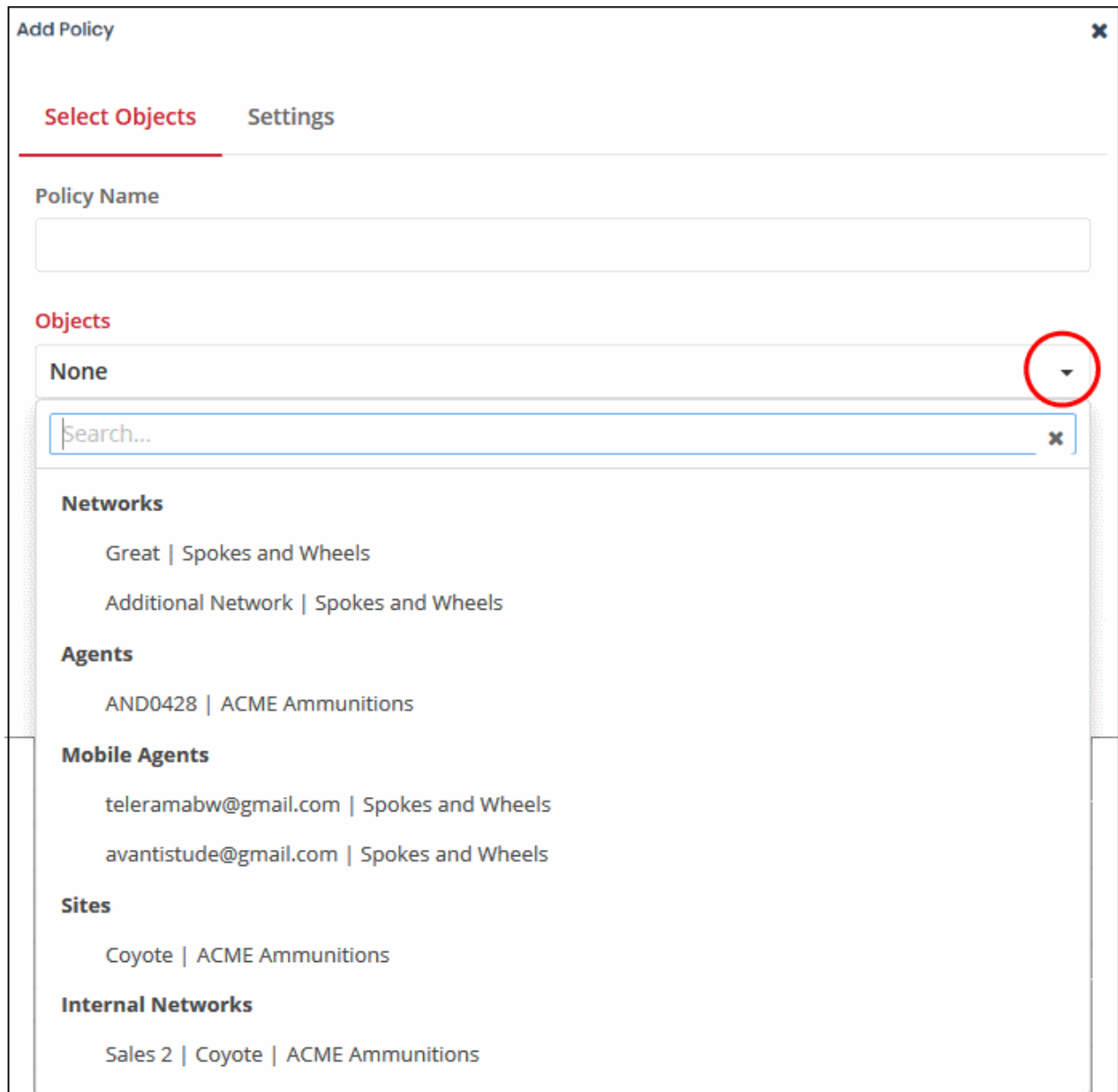
Create a new policy

- Click 'Configure' > 'Policy'

- Click '+ Add New Policy'
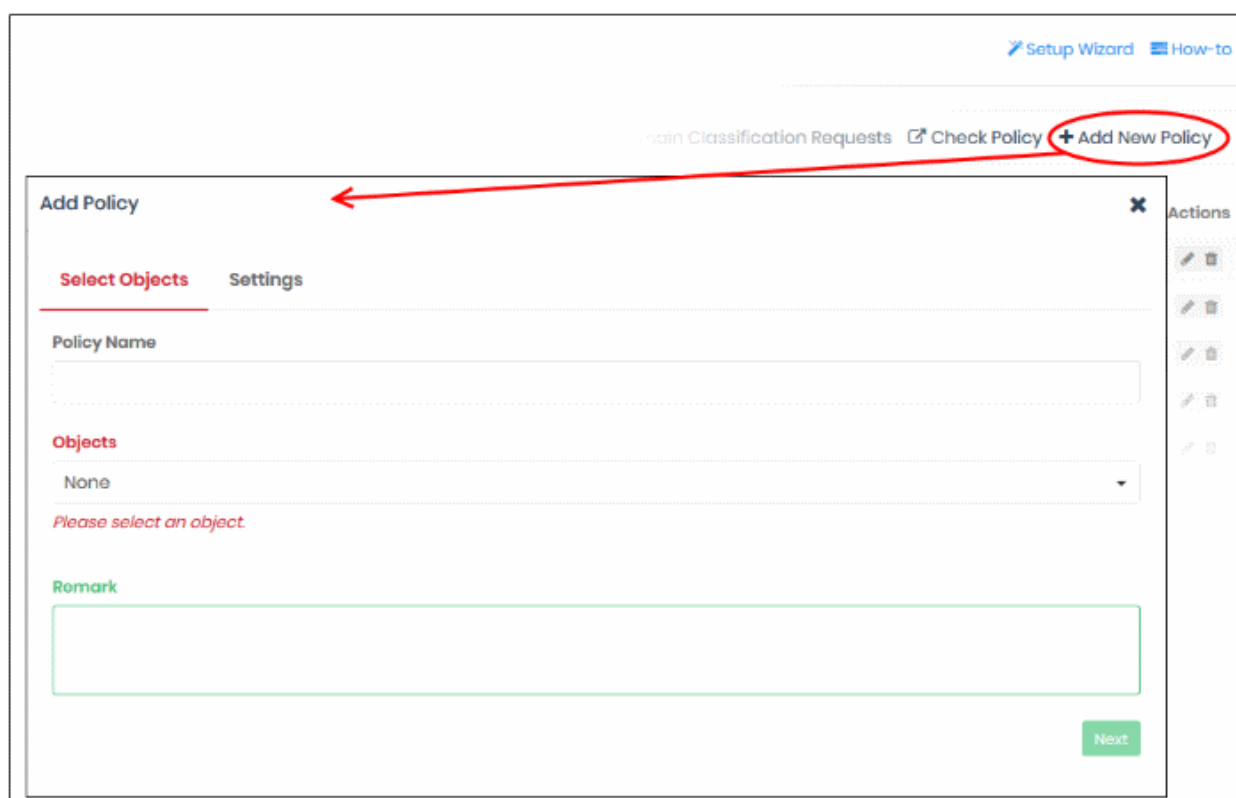
- Policy Name – Enter a label for the policy
- Objects - Select the items to which the policy should be applied. This can be a network, device, site or internal network.
  - Note - The objects drop-down only shows networks, devices and sites that do not yet have a policy.

- **Networks** - List of manually added networks
- **Agents** - List of roaming Windows and Mac OS devices enrolled by installing the Dome Shield 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.

- Enter a description for the policy in the 'Remark' field (optional)

- Click 'Next' or 'Settings' to configure the policy:

- **Only B/W Mode** - If enabled, only you will only be able to add blacklist or white-list rules to this policy. You will not be able to add security or category rules to the policy. By default, this setting is disabled.
  - Use the switch to enable or disable 'Only B/W Mode'
- **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.
  - Use the switch to enable or disable 'Block All Mode'
- **Security Rule** - Select a 'Security 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.
- **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.

Example policy settings are shown in the following screenshot:

- Click 'Add' to save your policy.

The policy will be 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:
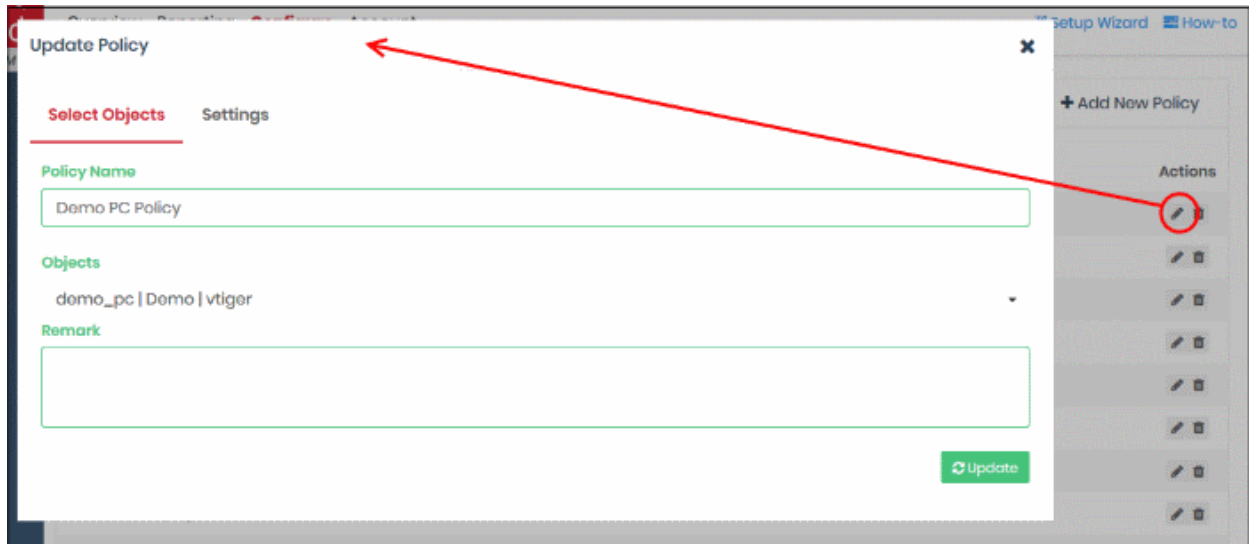
The 'Update Policy' dialog will open. The dialog is similar to the 'Add Policy' dialog explained **above**.

- Modify the name, description and/or settings as required.

- Click the 'Update' button

The updated policy will be applied to the network/roaming device/mobile device.

Test whether your policy works

The 'Policies' interface lets you check whether your applied rules are functioning correctly on your networks or roaming devices.

To do this:

- Login to Dome Shield 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
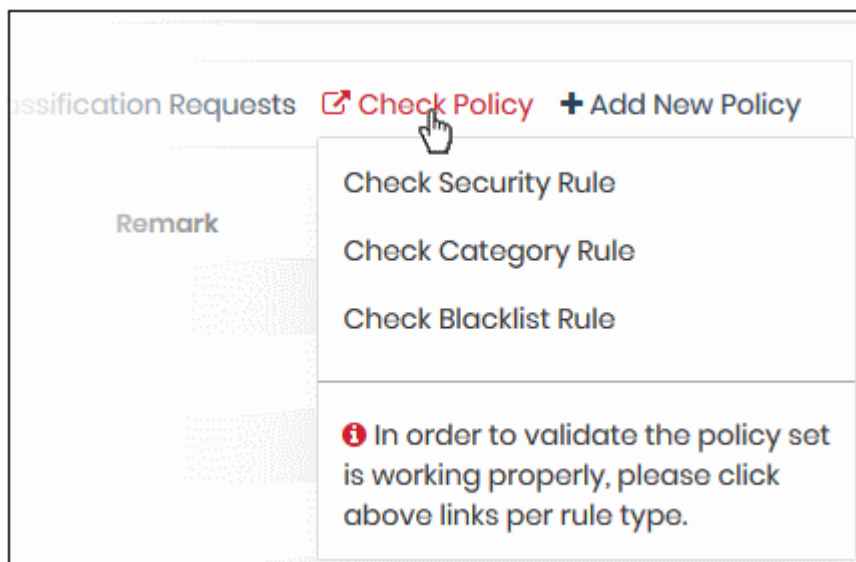
- To check whether security rules are applied by the policy, choose 'Check Security Rule'
- To check whether category rules are applied by the policy, choose 'Check Category Rule'
- To check whether blacklist rules are applied by the policy, choose 'Check Blacklist Rule'

You will see the following message if the selected type of rule is active:
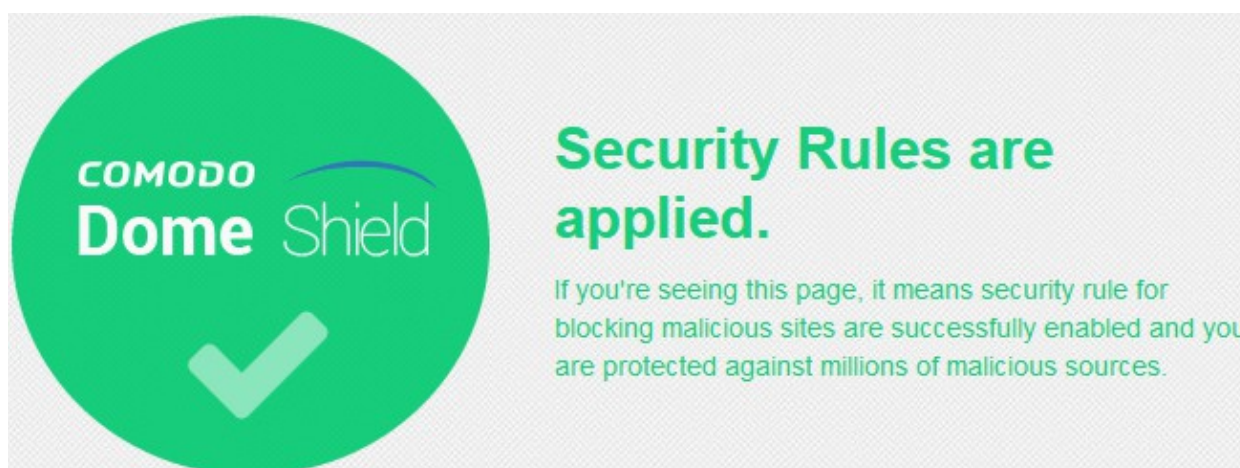
You will see the following message if the selected type of rule is not active:

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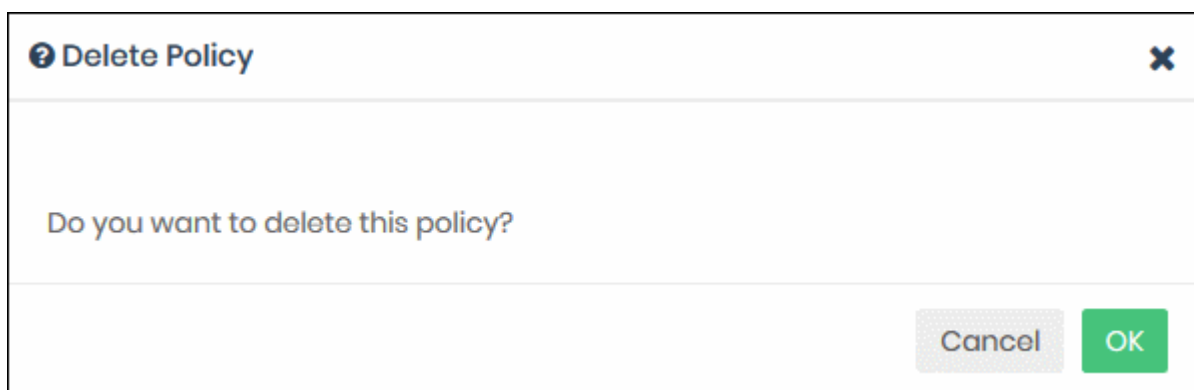
- Click 'OK' to confirm removal of the policy from the list.

The policy will be removed from the networks/endpoints on which it was active.

7   Domain Classification Requests

- Dome Shield leverages a massive database of known websites which are classified into various categories.
- These website categories can be added to a 'Category Rule'.
- The category rules are then added to a policy to stop devices/networks accessing sites in the categories.

Domain classification tools:

- You can suggest that a new domain is added to a particular category. For example, you may chance upon a gambling site which is not yet recognized by the filter.
- You can also suggest a different category for a domain if you feel it has been categorized inaccurately.

Your submission will be analyzed by Comodo and the site assigned to a category accordingly. The status of your request can be viewed in the same interface.

You can also blacklist/whitelist a domain you submitted. This is automatically applied to all your policies.

To view the 'Domain Classification Requests' interface

- Click 'Configure' > 'Policy'
- Click 'Domain Classification Requests' on the title bar
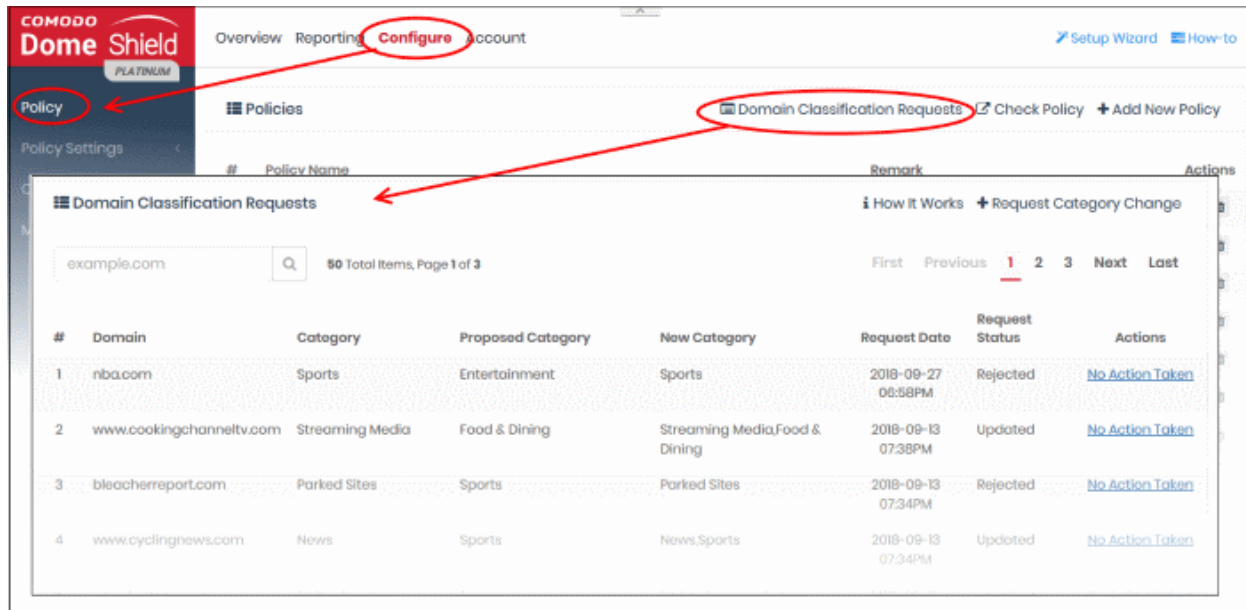
The interface shows a list of all previous requests.

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 is under analysis or has been processed.
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 feel a website should be placed into pre-defined dome shield category.
- After you specify a domain name, Dome Shield will first check whether it has already been registered to a category. If so, then Dome will show you its category.
- If you feel the domain should be classified under a different category, please specify the new category and submit the request.

To create a domain classification request

- Click 'Configure' > 'Domain Classification Requests'
- Click 'Request Category Change'
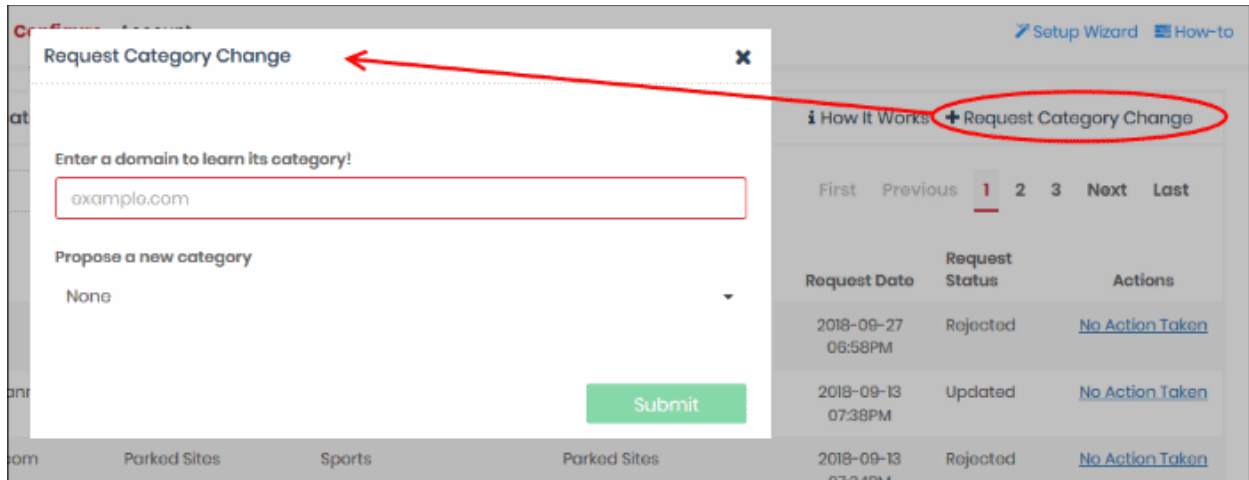
- Enter the name of the domain. Dome shield will search whether the domain has been registered.

Pre-registered Domain

- If the domain is already classified, its current category will be shown as follows:
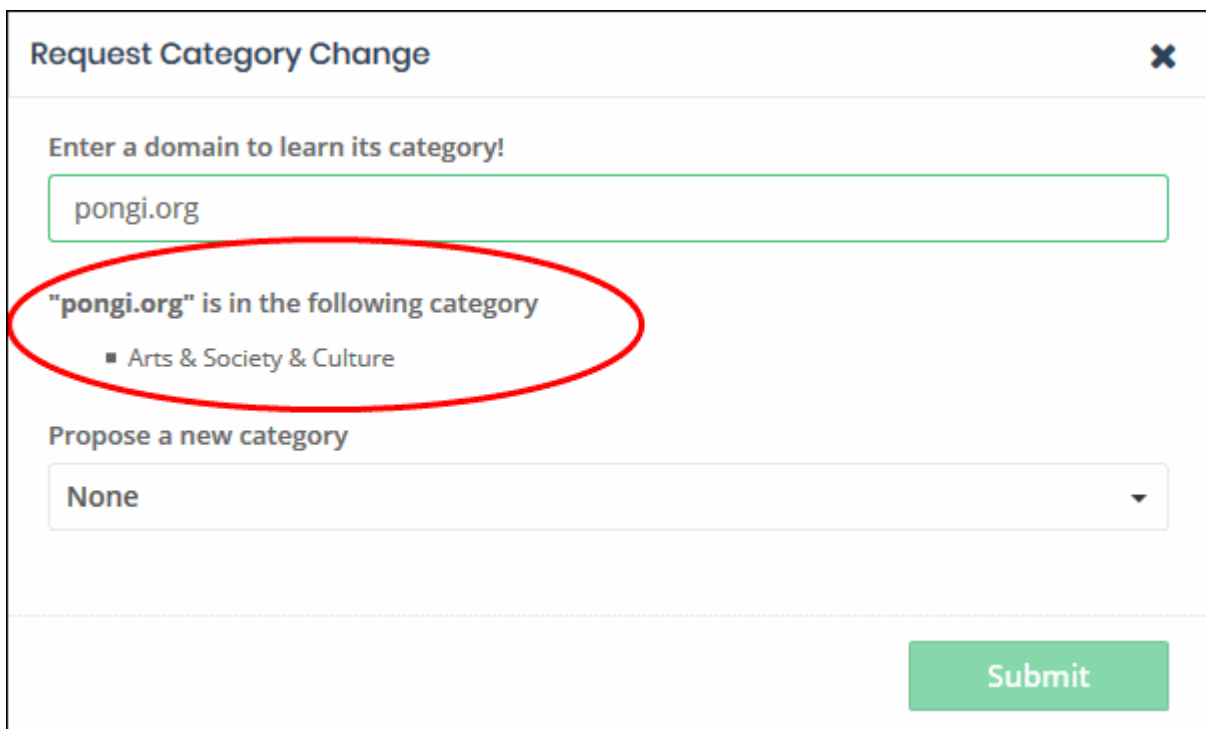
- If you wish to suggest a new category, select it from the 'Propose a new category' drop-down and click 'Submit'
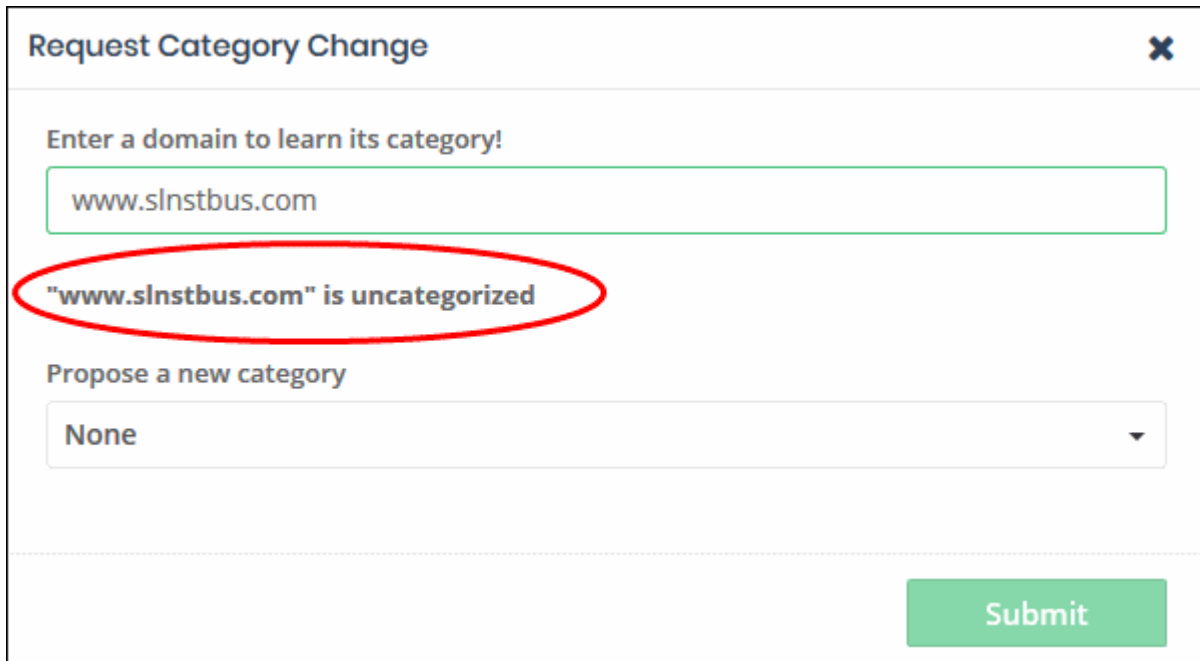
Comodo will analyze the request and, if successful, your site will be assigned the proposed category within 48 hours.

New Domain

• If the domain is new and not yet been classified, it will be shown as 'Uncategorized'.

- Select the category to be assigned to the domain from the 'Propose a new category' drop-down and click 'Submit'

Your request will be added. Dedicated staff at Comodo will analyze the domain. if found appropriate, your request will be accepted and the domain will be assigned the proposed category within 48 hours..

- If your request is accepted, the domain will be blocked or allowed depending on whether the new category is allowed or blocked in the 'Category Rules' included in the respective policies.

- If your request is rejected, the domain will be allowed or blocked depending on whether it is included in any of whitelists/blacklists included in the policies.

- You can also individually whitelist/blacklist domains that added to the Domain Classification Requests. See the following section '**Whitelist/Blacklist a Domain**' for more details.

Whitelist/Blacklist a Domain

The options in the 'Actions' column allow you to add a domain to whitelist or blacklist. It will be added to your policies and the domain will be allowed or blocked on the protected network(s), roaming and mobile device(s).

To blacklist/whitelist a domain from the 'Domain Classification Requests' interface

- Click the 'Actions' link in the row of the domain
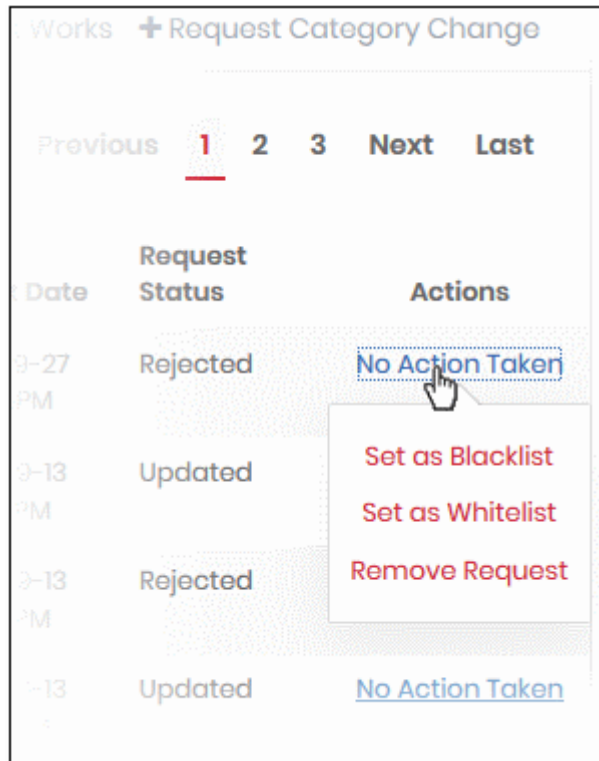
- Select the option from the drop-down

  - Set as Blacklist - The domain will be added to the global blacklist and applied to all your policies. It will be blocked on all protected networks, roaming and mobile devices.

  - Set as Whitelist - The domain will be added to the global whitelist and applied to all your policies. It will be allowed on all protected networks, roaming and mobile devices.

  - Remove Request - The request will be withdrawn and deleted from the list. The domain will also be removed from blacklist or whitelist, if you have already set one.

- If you request is accepted, the domain will be removed from the global whitelist/blacklist and from your policies. It will be allowed or blocked depending on the whether the assigned category is allowed or blocked in the category rules applied to policies.

- If your request is rejected, the domain will stay with the blacklist/whitelist status as set by you.

- If you remove a request, the domain will also be removed from the global whitelist or blacklist.

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:

Customer - Table of Column Descriptions	
Column Header	**Description**
Customer	The name of the MSP's customer
# of Networks	Number of networks enrolled for the customer
# of Roaming Devices	Number of out-of-network Windows devices enrolled for the customer. Install the Dome Shield roaming agent to enroll a roaming device.
# of Mobile Devices	Number of Android and iOS mobile devices enrolled for the customer
# of Sites	Number of networks (aka 'sites') which were automatically imported by installing the local resolver on a customer network.
# of Local Resolver	Number of local resolver virtual appliances registered for the customer

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

COMODO
Creating Trust Online®

9   Reports

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

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

- There are four types of reports, 'Web Activity', 'Security', 'Mobile Activity' and 'Site Activity' reports.
- 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 Threat**
- **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**

See '**The Dashboard**' to find out more about these reports.

10 View Account Details

The 'Account Info' page shows user information, total DNS requests for the month and license details.

- Click 'Account' at the top 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 – Type of account - MSP or Enterprise

- Joining Date – Date you subscribed to Dome Shield

Total DNS Requests

- This shows the number of requests to Dome Shield 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 Dome Shield Portal are *not* included in the 300 K limit.

Licenses

- License Type – Shield 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

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**