COMODO
Creating Trust Online®

COMODO ONE
MSP

Comodo Dome Shield

Software Version 1.17

Administrator Guide

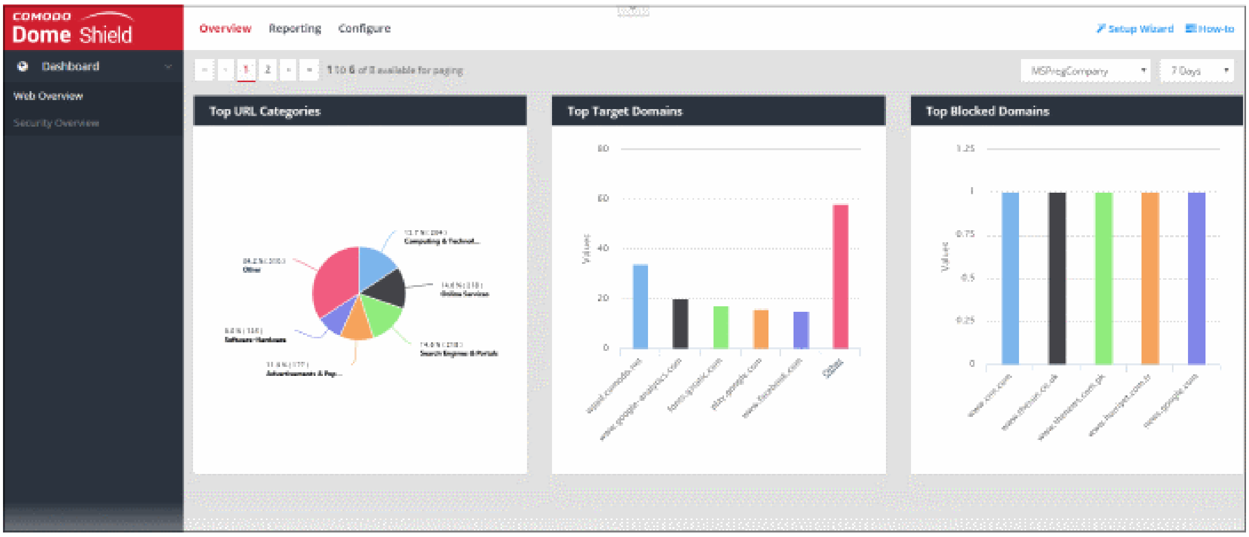
Guide Version 1.17.072718

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

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 and Login to Dome Shield
  - Setup Options Explained
    - Tutorial to Add Networks to Dome Shield
    - Tutorial to Add Roaming Endpoints to Dome Shield
    - Setup Wizard - Add Networks and Install Roaming Agent
    - Setup Local Resolver Virtual Machines and Import Sites
- The Admin Console
- The Dashboard
  - Web Overview
  - Security Overview
  - View Logs

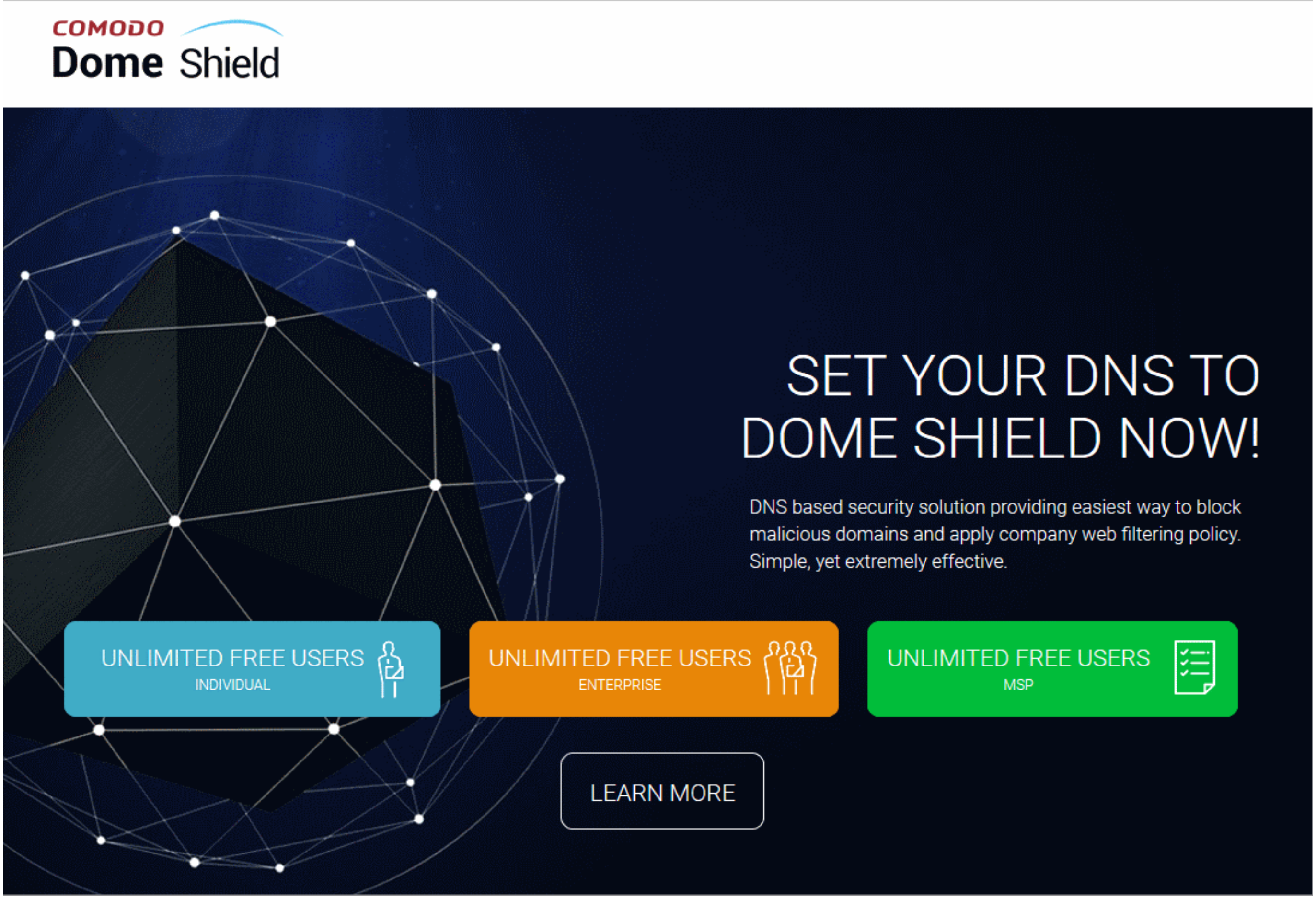
1.1 Purchase a License and Login to Dome Shield

The are two ways to enroll for Dome Shield:

- Stand-alone customers - Sign-up for a free subscription at https://www.comodo.com/cdomeshield/freelicense/
- Comodo One customers - 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:

- Visit https://www.comodo.com/cdomeshield/freelicense/ and choose a license type:

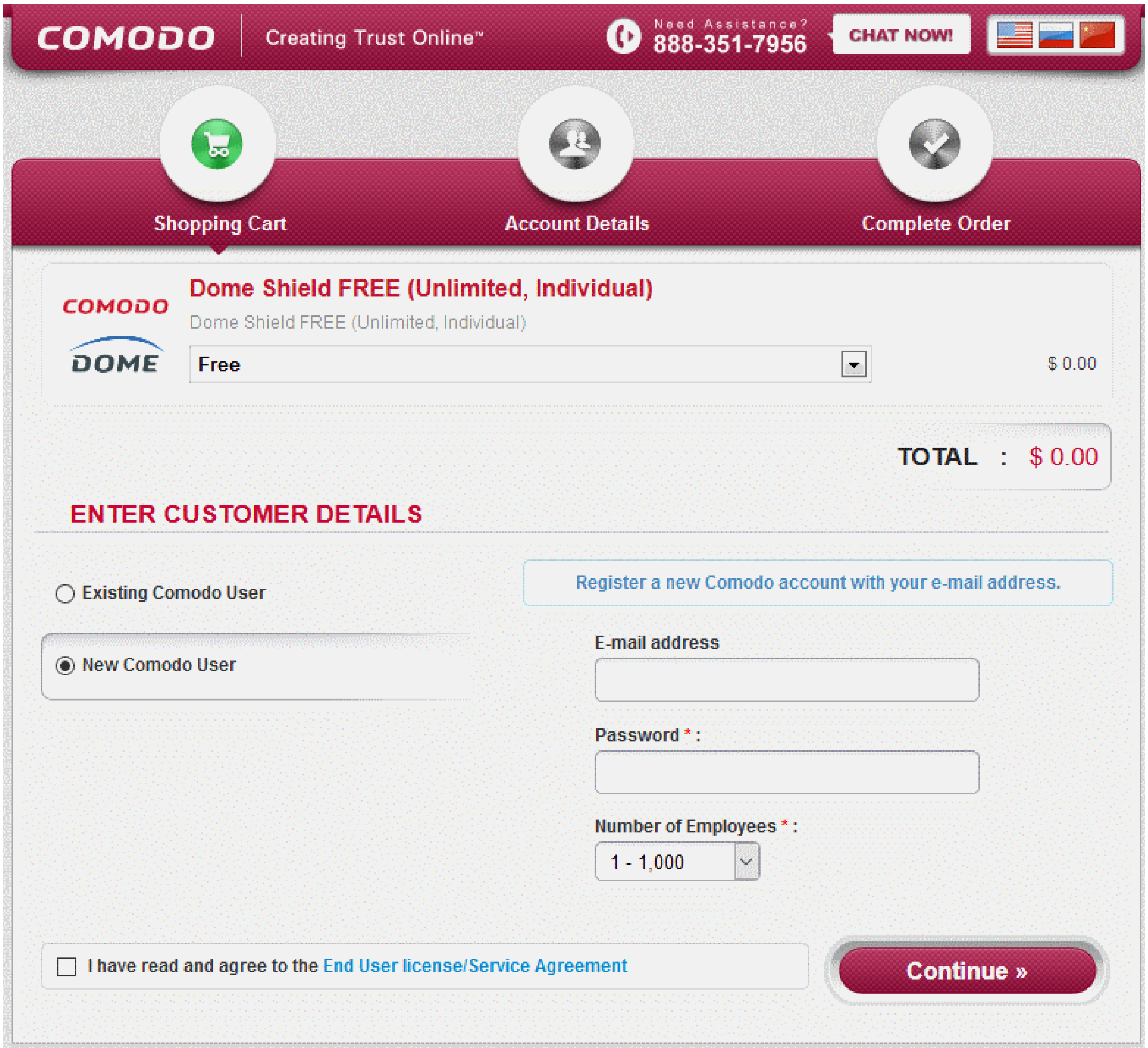

COMODO Dome Shield

SET YOUR DNS TO DOME SHIELD NOW!

DNS based security solution providing easiest way to block malicious domains and apply company web filtering policy. Simple, yet extremely effective.

- **'Individual' and 'Enterprise' licenses -** Single business licenses.
  - Login at https://one.comodo.com/app/login or https://us.one.comodo.com/app/login to manage Dome Shield via the Comodo One console. You'll also get access to Comodo range's of free security and management products, including ITSM, Service Desk, cWatch, Quote Manager and CRM.
  - Login at https://shield.dome.comodo.com/login if you only want to use Dome as a stand-alone product.
- **'MSP' licenses -** Implement and manage Dome security on your client/customer networks.
  - Login at https://one.comodo.com/app/login or https://us.one.comodo.com/app/login
  - Any customers you add to Comodo One are automatically imported into Dome Shield.
  - See https://help.comodo.com/topic-289-1-716-8483-Manage-Companies.html for help to manage customers in Comodo One.

After choosing a license type you will be taken to the order placement page:



Dome Shield FREE (Unlimited, Individual)

Dome Shield FREE (Unlimited, Individual)

Free $ 0.00

TOTAL : $ 0.00

ENTER CUSTOMER DETAILS

○ Existing Comodo User

● New Comodo User

Register a new Comodo account with your e-mail address.

E-mail address

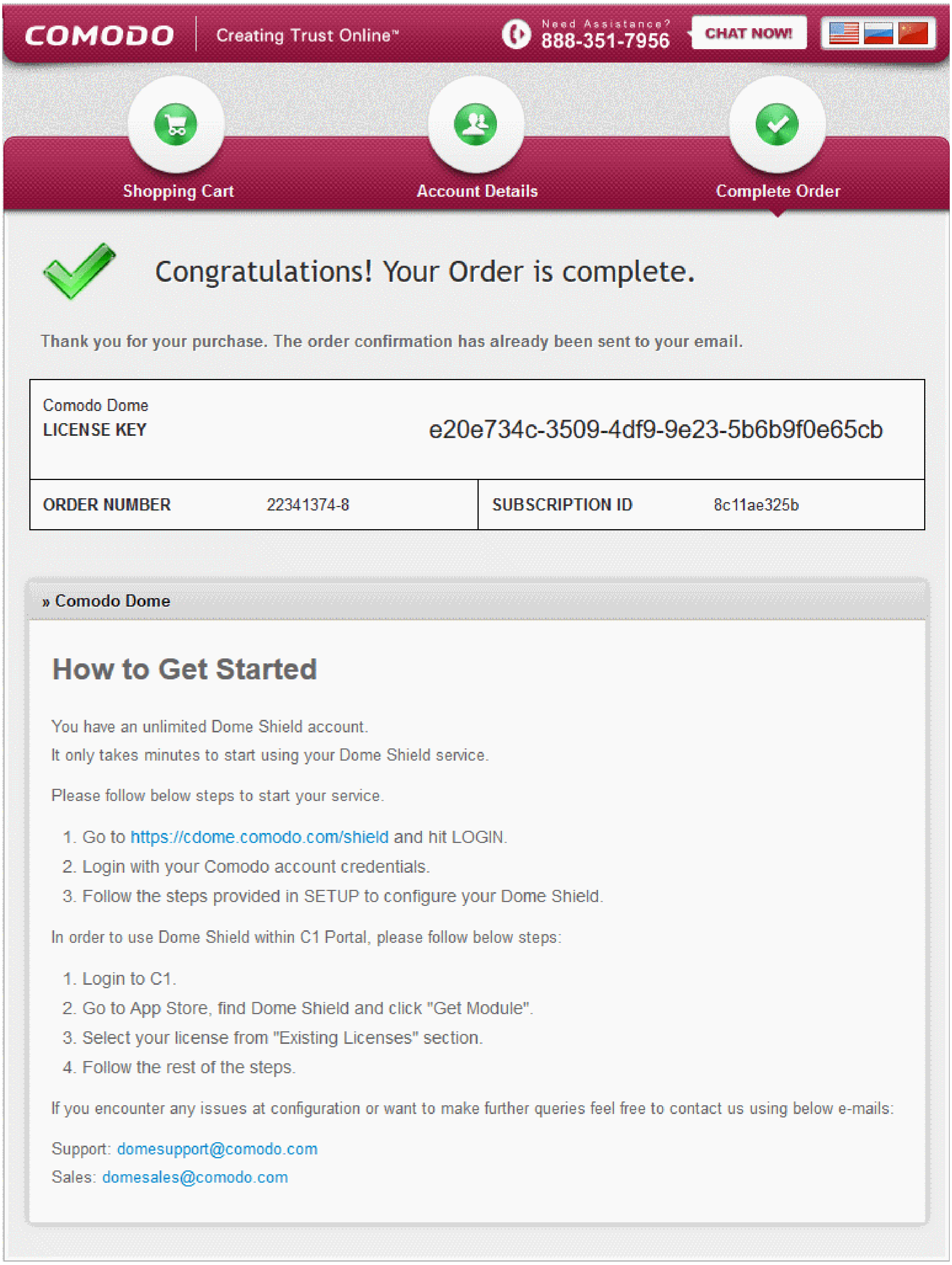
Password * :

Number of Employees * : 1 - 1,000

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

- 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' then enter your contact email address and a password.
- 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:



Congratulations! Your Order is complete.

Thank you for your purchase. The order confirmation has already been sent to your email.

Comodo Dome LICENSE KEY	e20e734c-3509-4df9-9e23-5b6b9f0e65cb		
ORDER NUMBER	22341374-8	SUBSCRIPTION ID	8c11ae325b

» Comodo Dome

How to Get Started

You have an unlimited Dome Shield account.
It only takes minutes to start using your Dome Shield service.

Please follow below steps to start your service.

1. Go to https://cdome.comodo.com/shield and hit LOGIN.
2. Login with your Comodo account credentials.
3. Follow the steps provided in SETUP to configure your Dome Shield.

In order to use Dome Shield within C1 Portal, please follow below steps:

1. Login to C1.
2. Go to App Store, find Dome Shield and click "Get Module".
3. Select your license from "Existing Licenses" section.
4. Follow the rest of the steps.

If you encounter any issues at configuration or want to make further queries feel free to contact us using below e-mails:

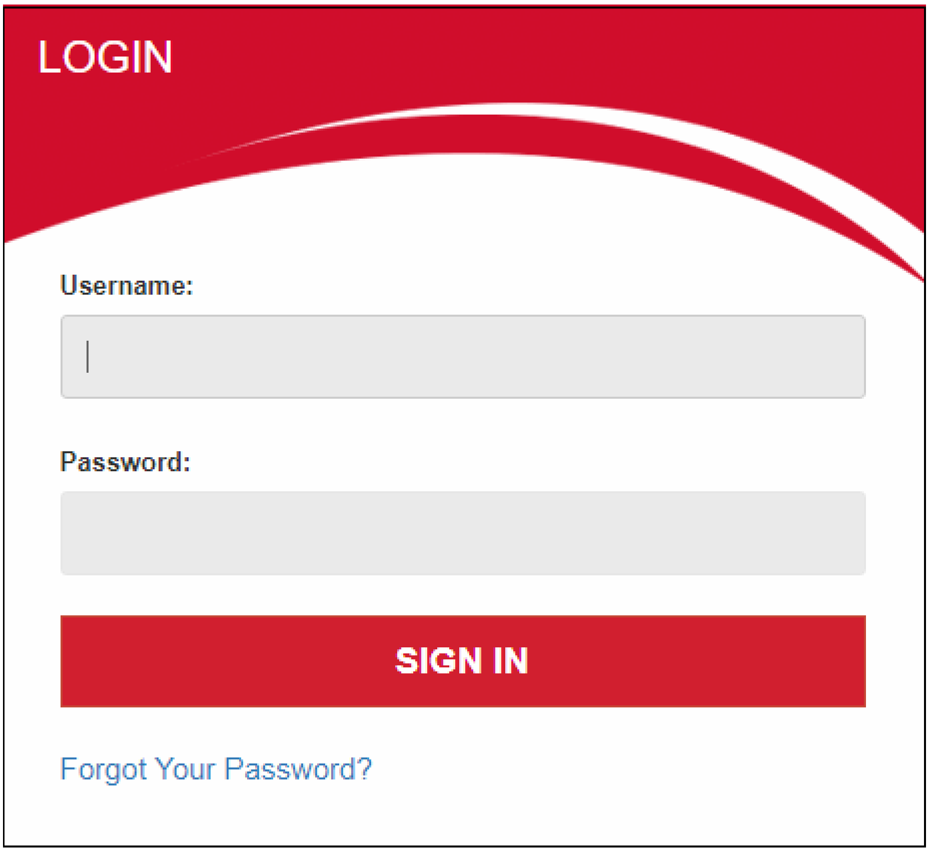
Support: domesupport@comodo.com
Sales: domesales@comodo.com

- 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

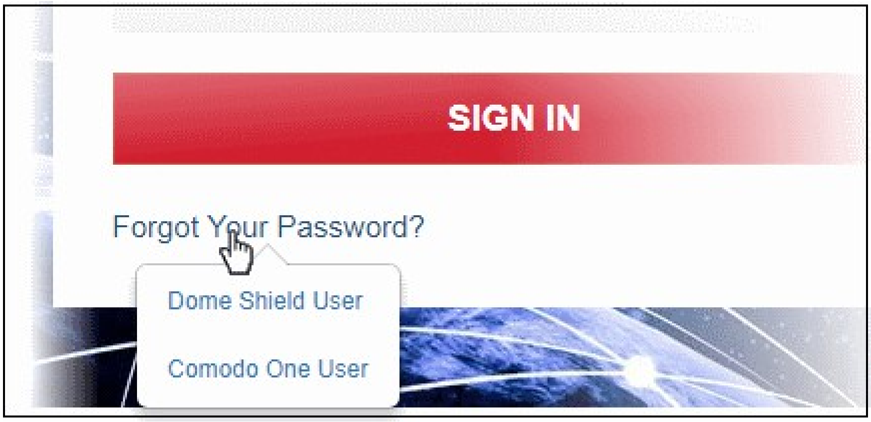
Login to Dome Shield

Stand-alone Dome Shield portal

- Login at https://shield.dome.comodo.com/login



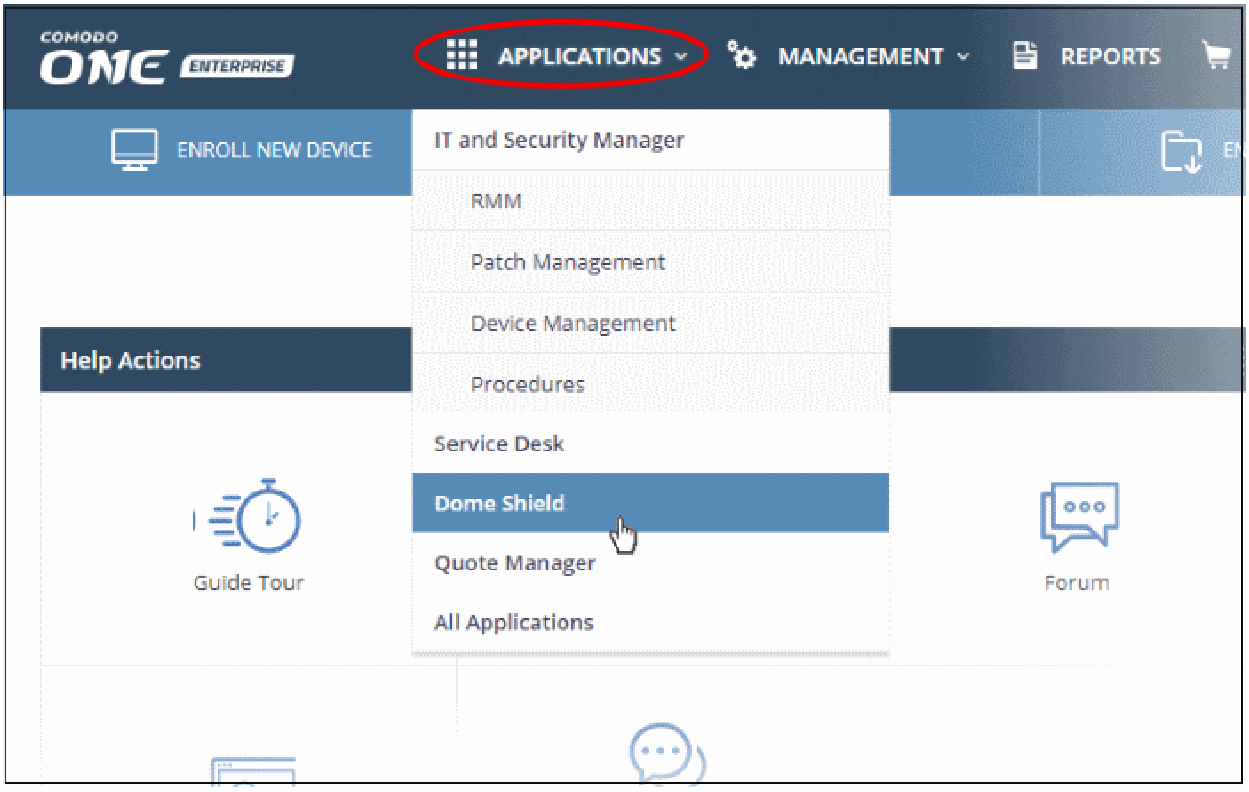
  - Username and password are case sensitive. Make sure you use the correct case.
  - Click 'Forgot password?' if you can't remember your password. Select 'Dome Shield User' account type:



  - 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 Dome Shield interface.



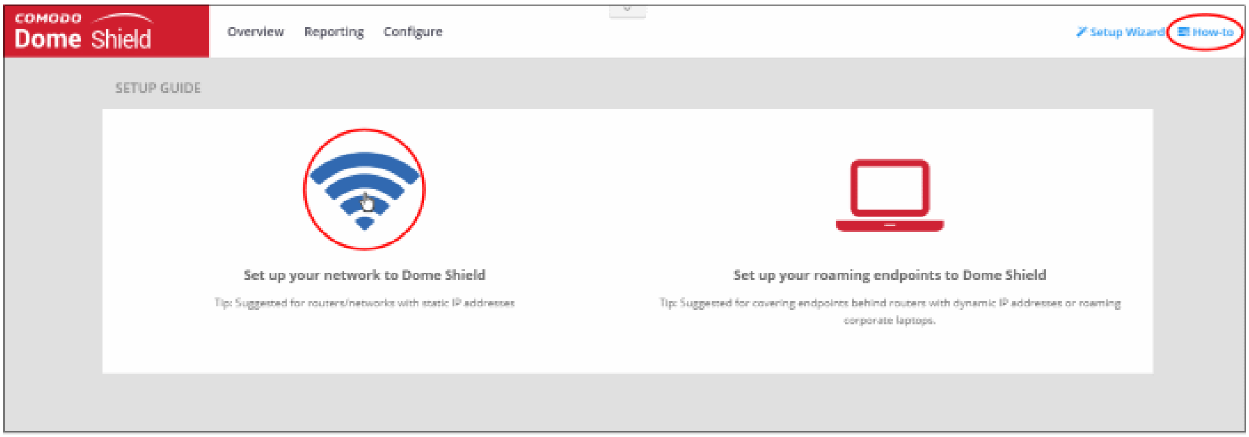
1.2 Setup Options Explained

There are three alternative ways you can setup Dome Shield protection:

1. Use the setup wizard
    - Click 'Setup Wizard' at the top-right of the interface to start the wizard
    - Follow the steps to add your networks and enroll mobile devices
    - Click **here for help** with the wizard
2. Set up protection manually
    - Click 'How-to' at the top-right of the interface
    - There are two tutorials - **adding networks** and **adding roaming endpoints**
    - Follow the steps in the tutorials to setup Dome Shield
3. Install local resolvers to automatically import networks
    - You install a local resolver (LR) as a virtual appliance on the network
    - Once deployed, the network will be automatically imported to Dome Shield
    - The resolver will forward public DNS queries from network endpoints to Dome Shield DNS servers
    - The resolver method offers some key advantages over the 'direct' methods
    - **Click here** for help to setup the local resolvers

1.2.1 Tutorial to Add Networks to Dome Shield

- Login to Dome Shield
- Click 'How-to' at the top-right to open the tutorials pages:



SETUP GUIDE

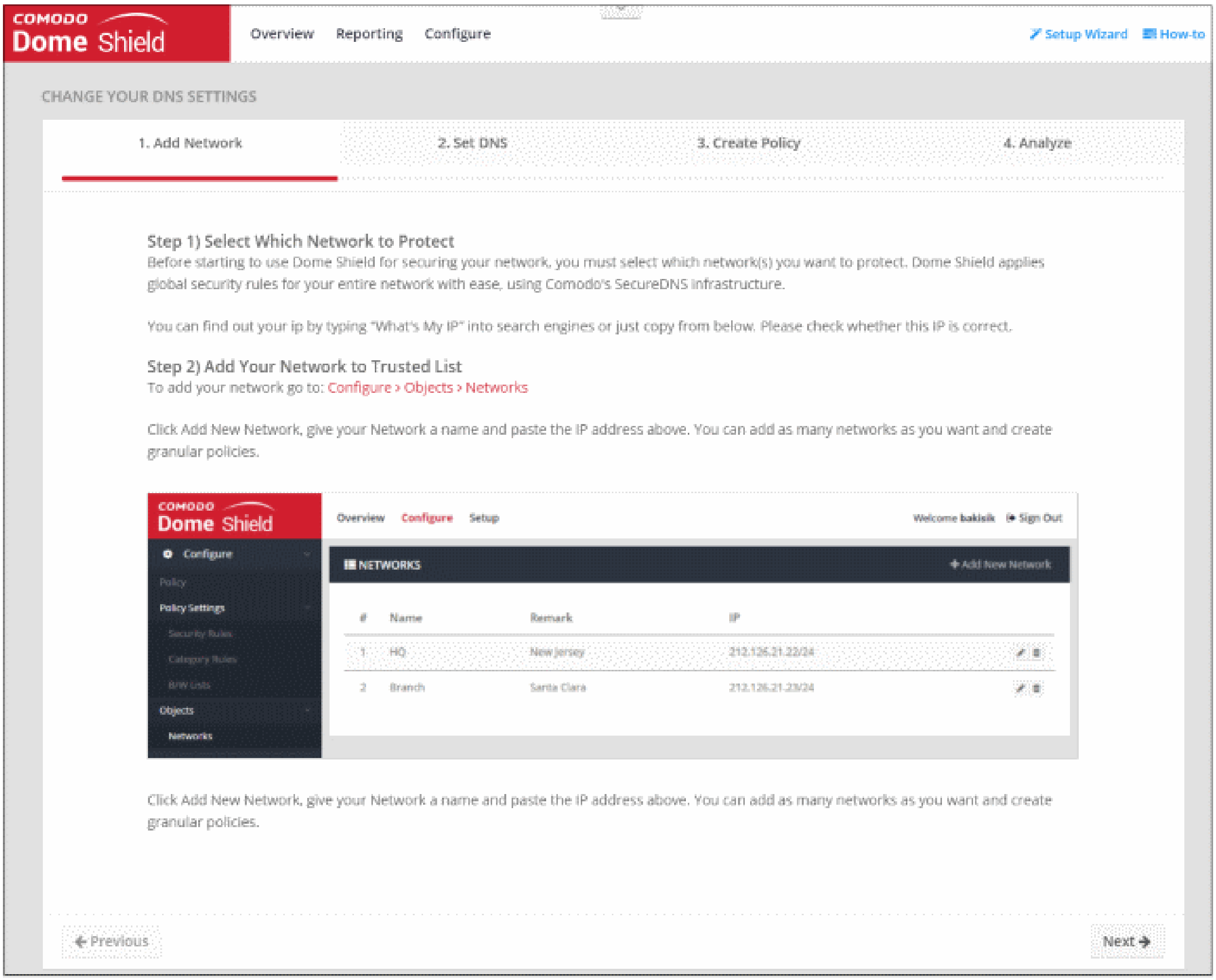
Set up your network to Dome Shield

Tip: Suggested for routers/networks with static IP addresses

Set up your roaming endpoints to Dome Shield

Tip: Suggested for covering endpoints behind routers with dynamic IP addresses or roaming corporate laptops.

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



CHANGE YOUR DNS SETTINGS

1. Add Network | 2. Set DNS | 3. Create Policy | 4. Analyze

Step 1) Select Which Network to Protect

Before starting to use Dome Shield for securing your network, you must select which network(s) you want to protect. Dome Shield applies global security rules for your entire network with ease, using Comodo's SecureDNS infrastructure.

You can find out your ip by typing "What's My IP" into search engines or just copy from below. Please check whether this IP is correct.

Step 2) Add Your Network to Trusted List

To add your network go to: Configure › Objects › Networks

Click Add New Network, give your Network a name and paste the IP address above. You can add as many networks as you want and create granular policies.

#	Name	Remark	IP
1	HQ	New Jersey	212.126.21.22/24
2	Branch	Santa Clara	212.126.21.23/24

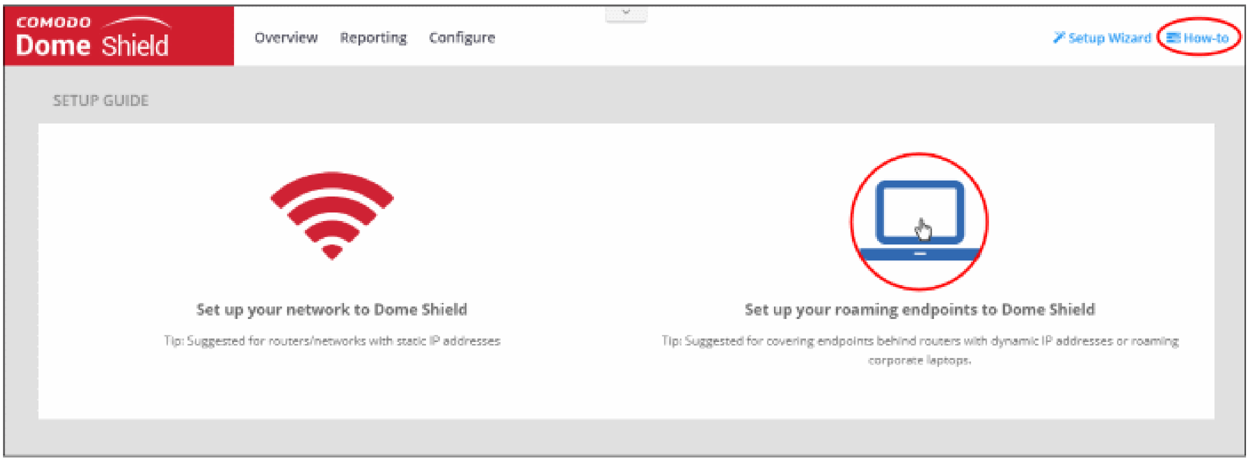
Click Add New Network, give your Network a name and paste the IP address above. You can add as many networks as you want and create granular policies.

There are four main steps covered in the tutorial:

- **Add Network** - Enroll your network to Dome Shield.
- **Set DNS** - Set up your DNS server, router or firewall to use Dome Shield DNS service.
- **Create Policy** - Create rules and domain black/whitelists and apply them to policies. This allows you to selectively allow or block internet traffic to your network endpoints.
- **Analyze** - View traffic trends on your network using widgets on the dashboard or by viewing logs.

1.2.2 Tutorial to Add Roaming Endpoints to Dome Shield

- Login to Dome Shield
- Click 'How-to' at the top-right to open the tutorials pages:



SETUP GUIDE

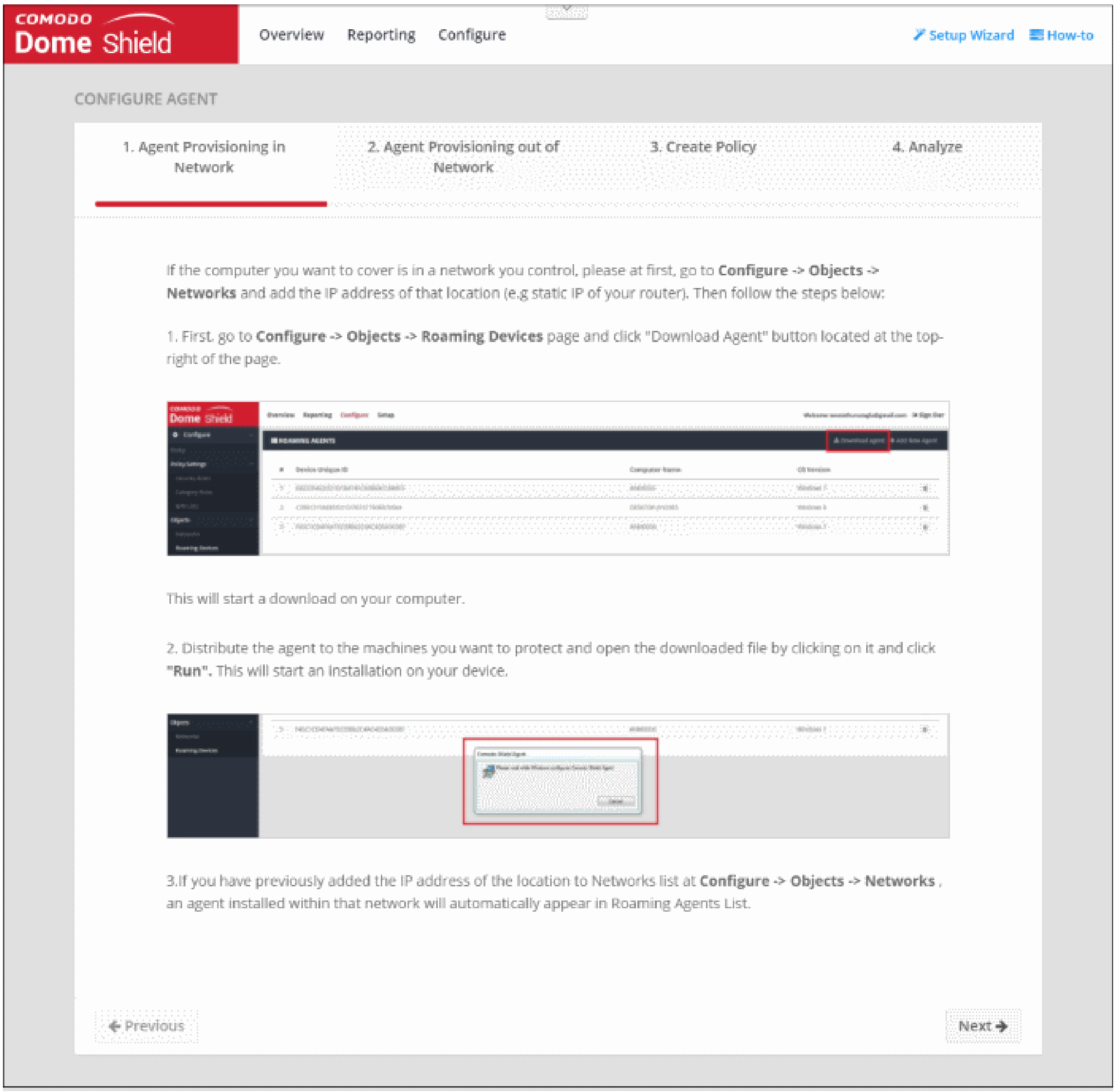
Set up your network to Dome Shield

Tip: Suggested for routers/networks with static IP addresses

Set up your roaming endpoints to Dome Shield

Tip: Suggested for covering endpoints behind routers with dynamic IP addresses or roaming corporate laptops.

- Click the device icon to open the roaming endpoints setup guide:



CONFIGURE AGENT

If the computer you want to cover is in a network you control, please at first, go to **Configure -> Objects -> Networks** and add the IP address of that location (e.g static IP of your router). Then follow the steps below:

1. First, go to **Configure -> Objects -> Roaming Devices** page and click "Download Agent" button located at the top-right of the page.

This will start a download on your computer.

2. Distribute the agent to the machines you want to protect and open the downloaded file by clicking on it and click **"Run".** This will start an installation on your device.

3.If you have previously added the IP address of the location to Networks list at **Configure -> Objects -> Networks** , an agent installed within that network will automatically appear in Roaming Agents List.

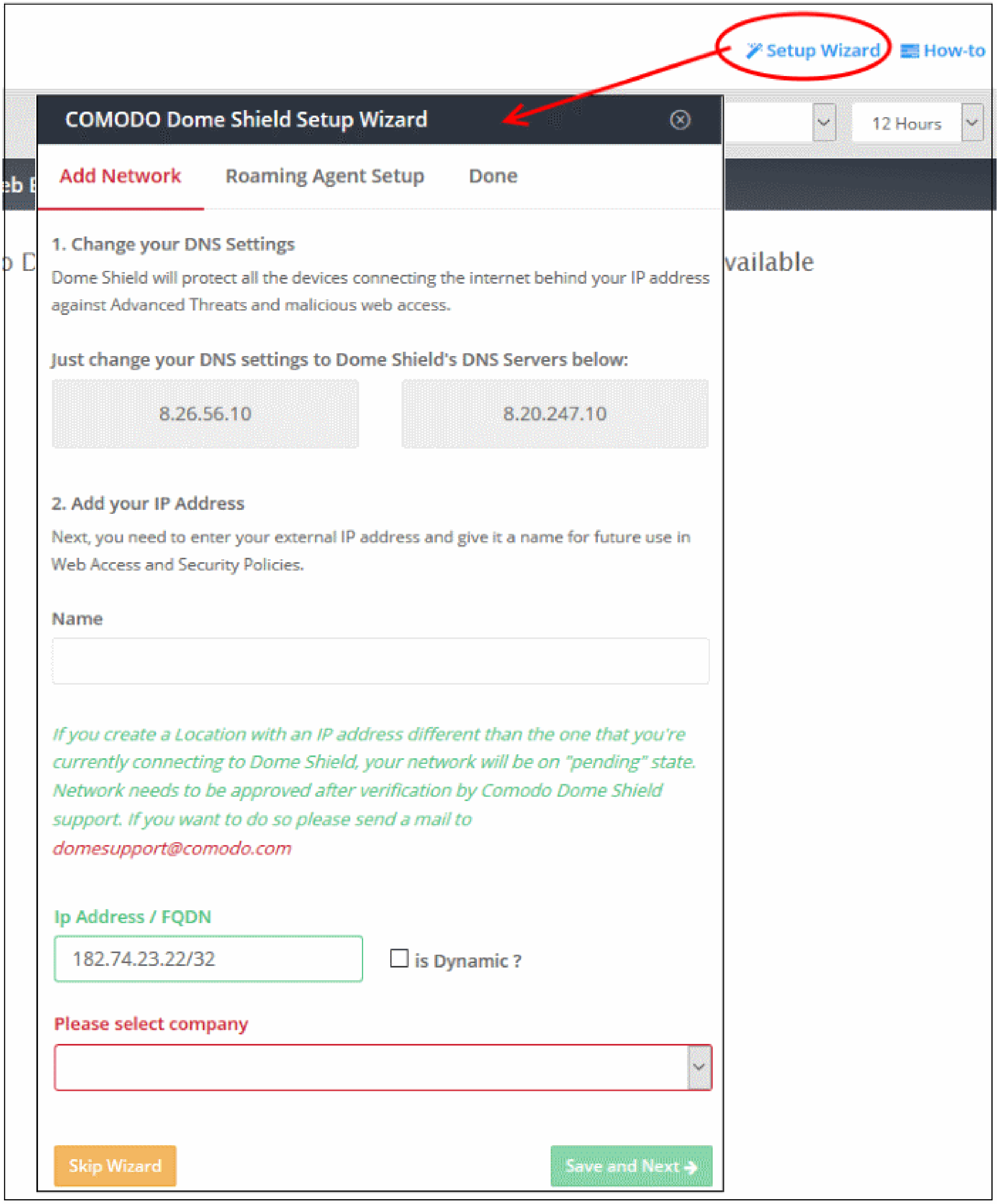
There are four main steps covered in the tutorial:

- Agent Provisioning in Network - Enroll devices inside your network

- **Agent Provisioning out of Network** - Enroll devices outside your network
- **Create Policy** - Create rules and domain black/whitelists and apply them to policies. This allows you to selectively allow or block internet traffic to your network endpoints.
- **Analyze** - View traffic trends on protected devices using widgets on the dashboard or by viewing logs.

1.2.3 Setup Wizard - Add Networks and Install Roaming Agent

- The setup wizard lets you quickly enroll your networks and roaming devices 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:



COMODO Dome Shield Setup Wizard

Add Network | Roaming Agent Setup | Done

1. Change your DNS Settings

Dome Shield will protect all the devices connecting the internet behind your IP address against Advanced Threats and malicious web access.

Just change your DNS settings to Dome Shield's DNS Servers below:

8.26.56.10 | 8.20.247.10

2. Add your IP Address

Next, you need to enter your external IP address and give it a name for future use in Web Access and Security Policies.

Name

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

Ip Address / FQDN: 182.74.23.22/32 ☐ is Dynamic ?

Please select company

Skip Wizard | Save and Next

Add Networks

Step 1 - 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

Step 2 - Add your IP Address

- Name - Enter an appropriate name for the network
- IP Address / FQDN
    - Static IP Address - The IP address or fully qualified domain name of your network. By default, this field will show the public IP address of the network from which you are connecting to Dome Shield. This network will automatically become active after initial enrollment.

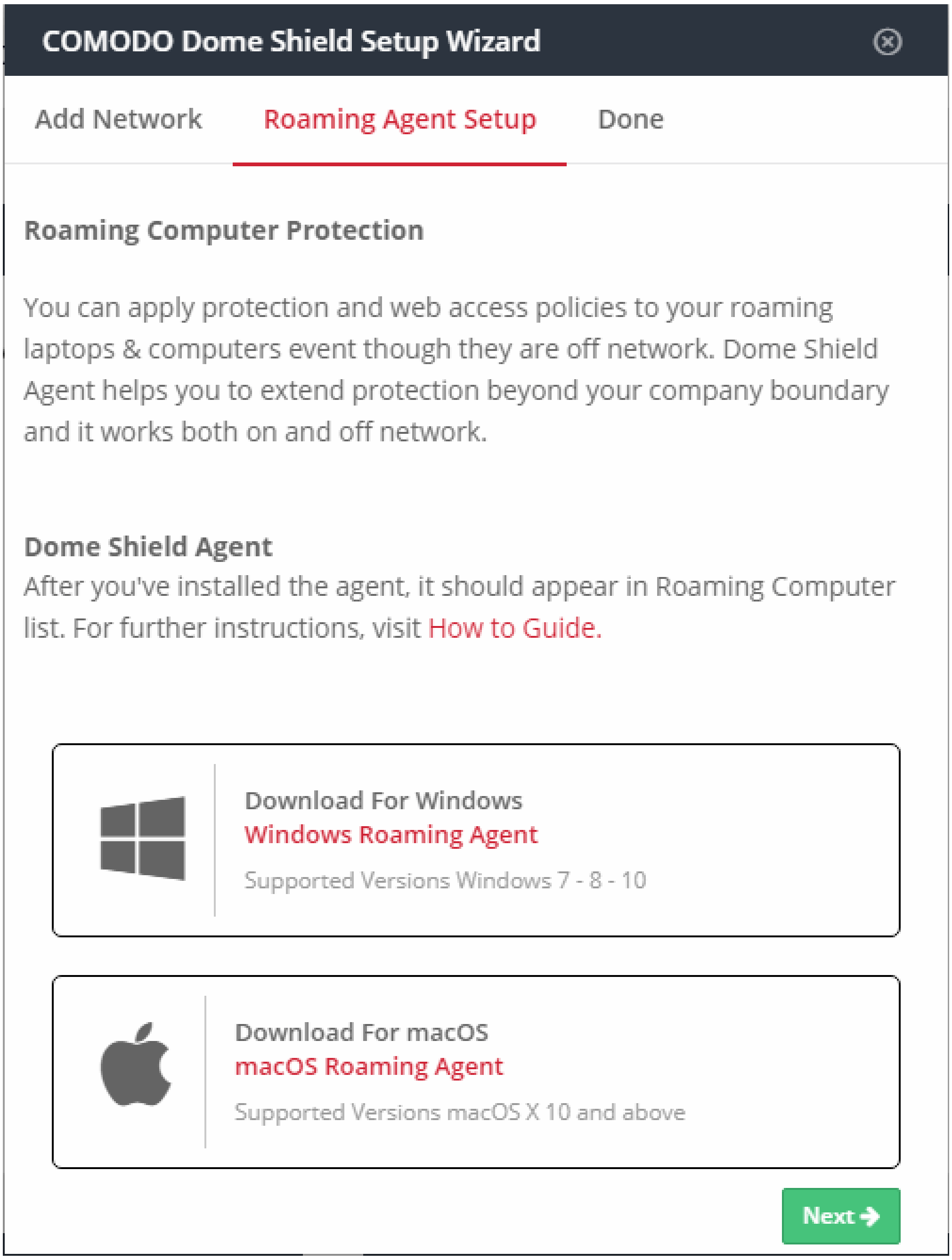
      You can also add the IP address of another network you want to enroll to Dome Shield.

        - Enter the IP address of the network in CIDR (Classless Inter-Domain Routing) notation.
        - Dome Shield can accept network prefixes from /24 to /32.

      The network needs to be approved by Comodo to complete the enrollment process. It will remain in 'Pending' status until approved.
    - Dynamic IP Address -
        - Select 'Is Dynamic' if you have a dynamic IP. Download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint.
        - This 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 'Activate the Dome Shield IP Updater Agent' for more details.
- Select Company - This applies only to MSP accounts only.
- Click 'Save and Next'. See Roaming Agent Setup for next step.

Roaming Agent Setup

- You need to install the roaming agent on all devices outside the network if you want them to be protected by Dome Shield.
- This dialog displays shows help about adding protection to roaming devices and allows you to download the roaming agent.



COMODO Dome Shield Setup Wizard

Roaming Computer Protection

You can apply protection and web access policies to your roaming laptops & computers event though they are off network. Dome Shield Agent helps you to extend protection beyond your company boundary and it works both on and off network.

Dome Shield Agent

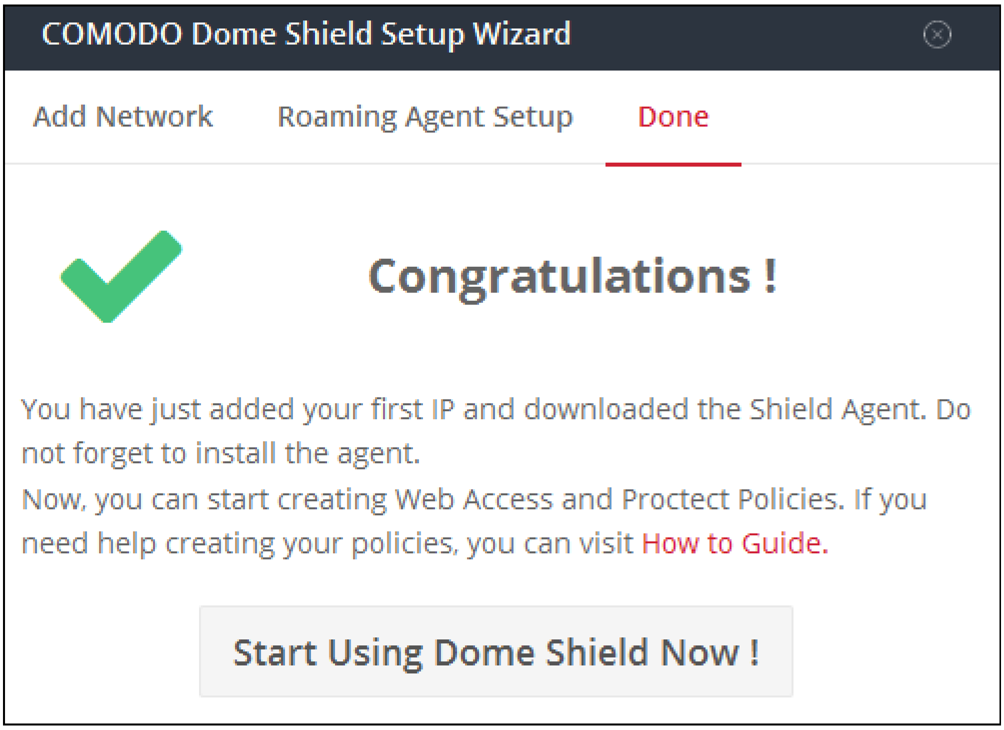
After you've installed the agent, it should appear in Roaming Computer list. For further instructions, visit How to Guide.

Download For Windows
Windows Roaming Agent
Supported Versions Windows 7 - 8 - 10

Download For macOS
macOS Roaming Agent
Supported Versions macOS X 10 and above

- **Download for Windows -** Agent for Windows roaming devices.
- **Download for mac OS -** Agent for Mac OS roaming devices.
- The agents should be installed on all roaming devices you wish to protect with Dome Shield. The agent will connect to your account and the endpoint will appear in the Dome Shield management interface. See Add Roaming Endpoints to Dome Shield for more details.

- Click 'Next'.



COMODO Dome Shield Setup Wizard

Congratulations !

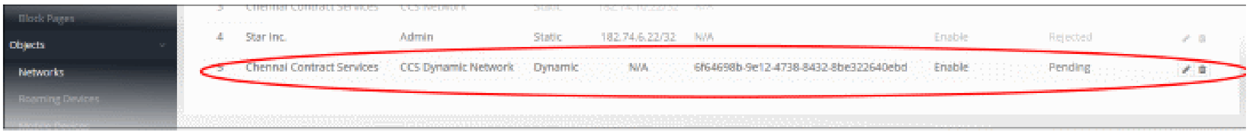
You have just added your first IP and downloaded the Shield Agent. Do not forget to install the agent.

Now, you can start creating Web Access and Proctect Policies. If you need help creating your policies, you can visit How to Guide.

- Click ⓧ to close the dialog.

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.
- If you specified a static IP address for your network then it will automatically become active. Any new IP address that you add here will remain in pending status until approved by Comodo.
- If you specified a dynamic IP address then your network will be added to Dome with the status 'Pending'.
  - You need to install the IP updater software on an endpoint in your network.
  - During installation, enter the activation code shown in the 'Networks' interface to register your network with Dome Shield.
  - See the next section, 'Activate the Dome Shield IP Updater Agent', for help with this.



3	Chennai Contract Services	CCS Network	Static	182.74.10.22/32	N/A			
4	Star Inc.	Admin	Static	182.74.6.22/32	N/A	Enable	Rejected	
5	Chennai Contract Services	CCS Dynamic Network	Dynamic	N/A	6f64698b-9e12-4738-8432-8be322640ebd	Enable	Pending	

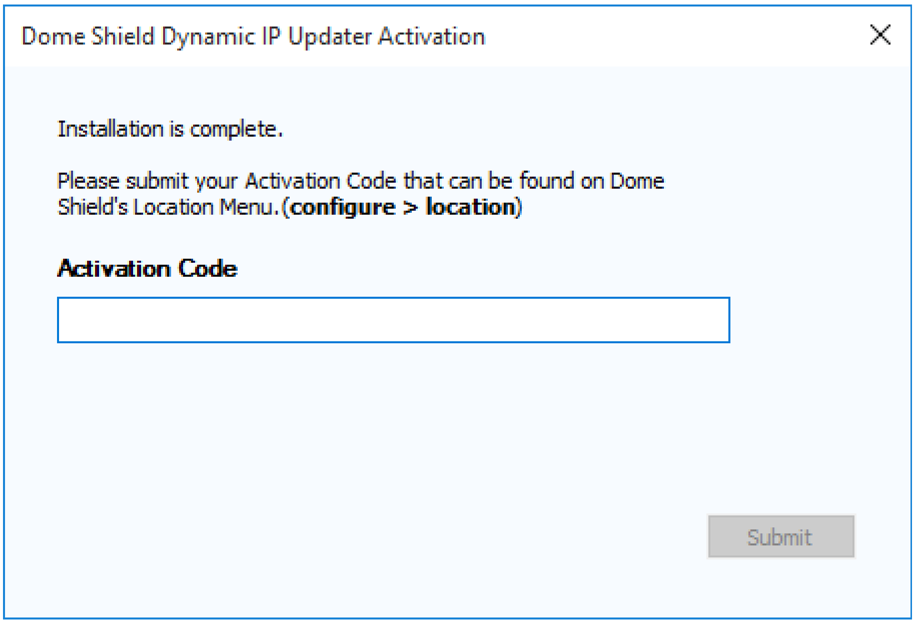
Activate the Dome Shield IP Updater Agent

This section applies to customers who use dynamic IP addresses.

- Download the IP updater agent as described in the previous step and install it on an endpoint in your 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.

- To complete setup you will need to enter the activation code of the network:



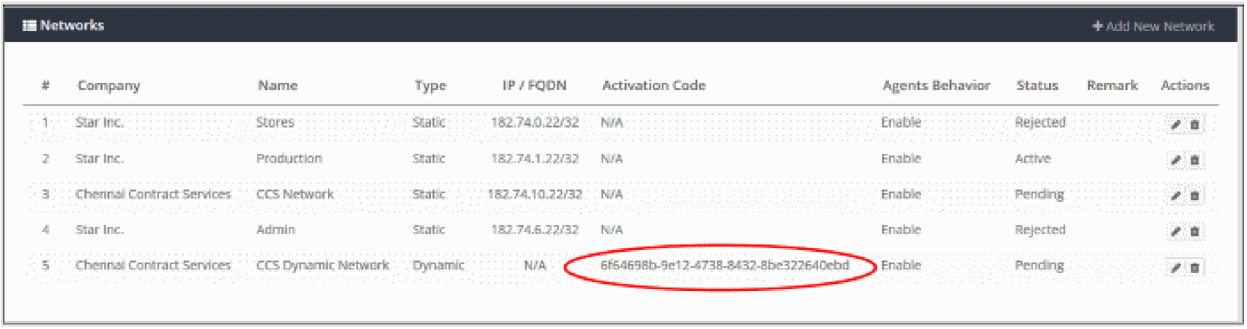
Dome Shield Dynamic IP Updater Activation

Installation is complete.

Please submit your Activation Code that can be found on Dome Shield's Location Menu.(**configure > location**)

Activation Code

- To find the code, login to Dome Shield and click 'Configure' > 'Objects' > 'Networks':



Networks

#	Company	Name	Type	IP / FQDN	Activation Code	Agents Behavior	Status	Remark	Actions
1	Star Inc.	Stores	Static	182.74.0.22/32	N/A	Enable	Rejected		
2	Star Inc.	Production	Static	182.74.1.22/32	N/A	Enable	Active		
3	Chennai Contract Services	CCS Network	Static	182.74.10.22/32	N/A	Enable	Pending		
4	Star Inc.	Admin	Static	182.74.6.22/32	N/A	Enable	Rejected		
5	Chennai Contract Services	CCS Dynamic Network	Dynamic	N/A	6f64698b-9e12-4738-8432-8be322640ebd	Enable	Pending		

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

On successful activation the network will be added and displayed in the list. You can apply network specific policy according to your requirements.

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'

1.2.4 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 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, giving 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 LR virtual appliance can be setup using virtual machine applications/tools 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 of yours. A high-traffic site is one that receives more than 500 DNS queries per second from the overall network.

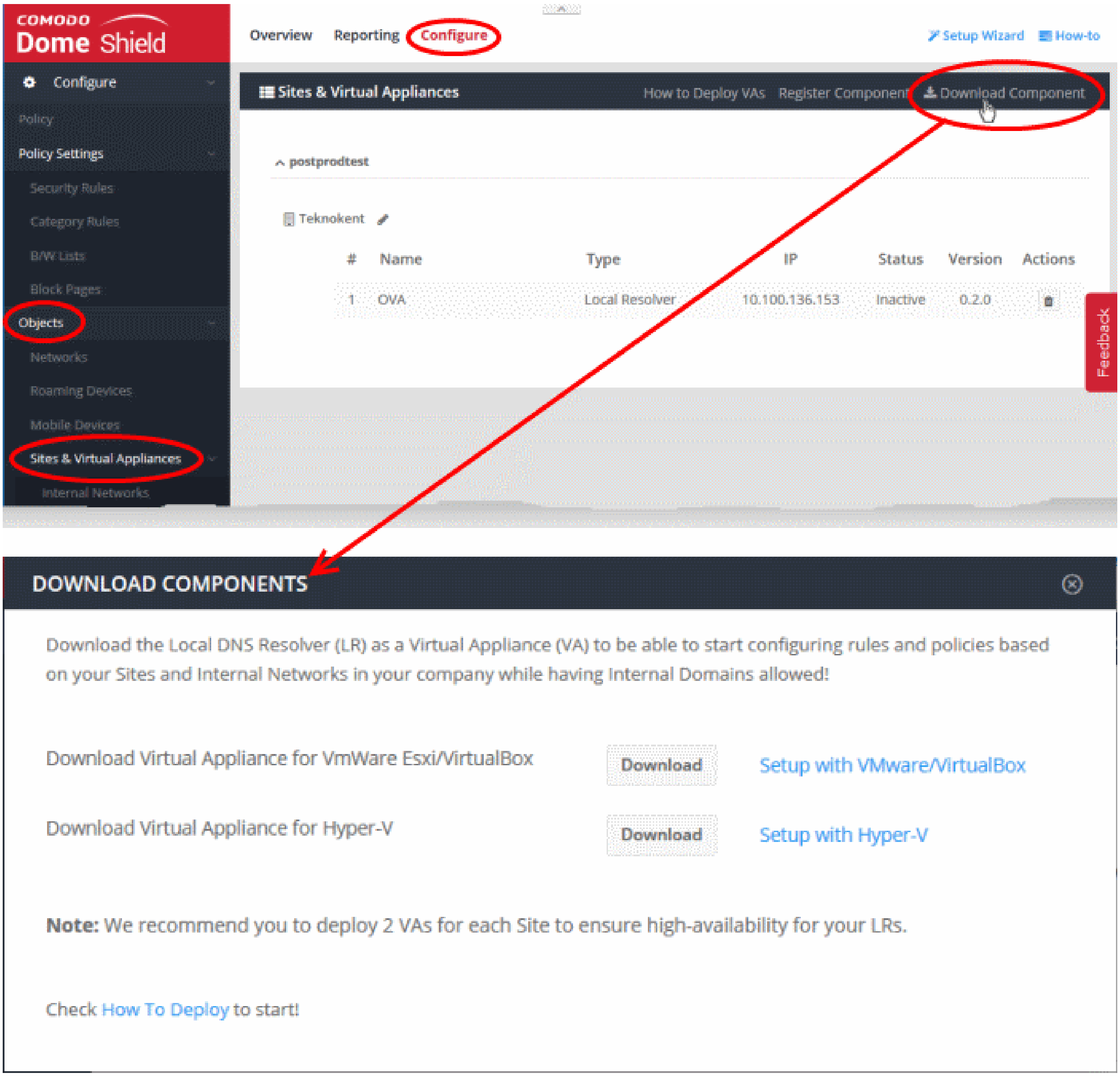
The rest of this section explains the step-by-step installation process of the LR VA's

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 DomeShield
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Download Component' on the top right



#	Name	Type	IP	Status	Version	Actions
1	OVA	Local Resolver	10.100.136.153	Inactive	0.2.0	

DOWNLOAD COMPONENTS

Download the Local DNS Resolver (LR) as a Virtual Appliance (VA) to be able to start configuring rules and policies based on your Sites and Internal Networks in your company while having Internal Domains allowed!

Download Virtual Appliance for VmWare Esxi/VirtualBox — Download — Setup with VMware/VirtualBox

Download Virtual Appliance for Hyper-V — Download — Setup with Hyper-V

Note: We recommend you to deploy 2 VAs for each Site to ensure high-availability for your LRs.

Check How To Deploy to start!

The LR VA can be setup on virtual machine applications like VMWare, VirtualBox and Hyper - V.

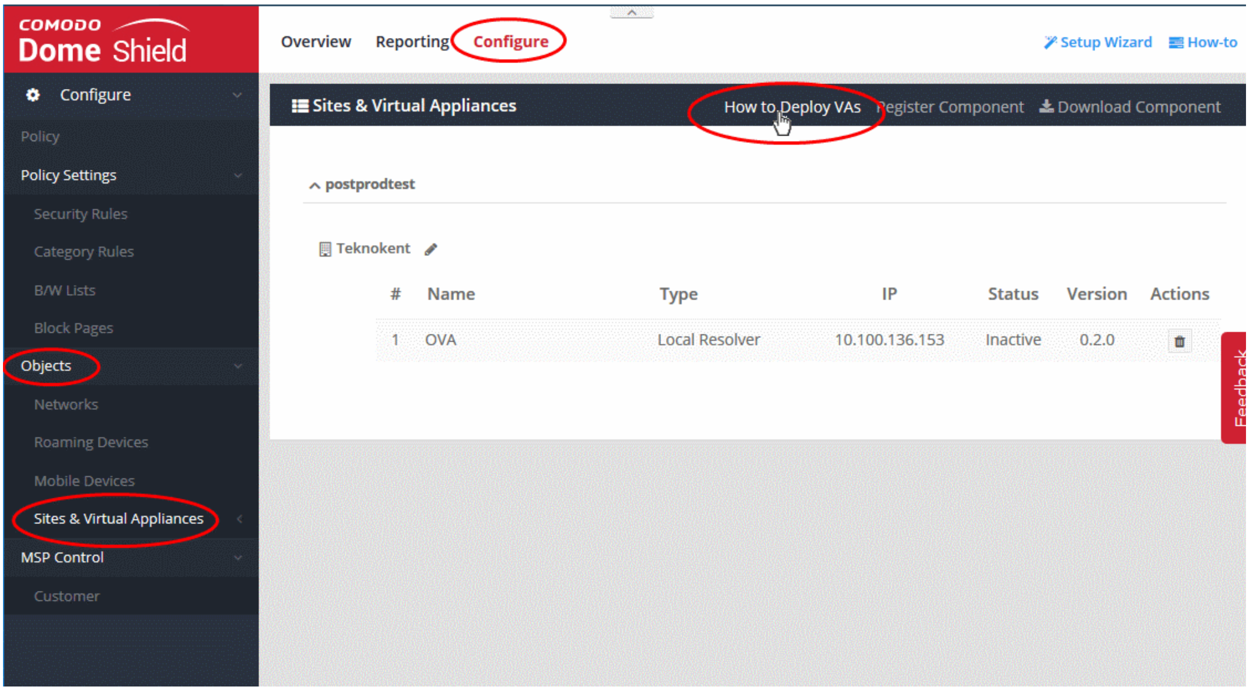
- Click the 'Download' button beside the virtual machine application you want to use
- The setup package will be downloaded in .zip format
- The package contains an OVA or HYPER-V file depending on the VM application you chose and a text file with login credentials for accessing the configuration UI of the appliance.

Step 2 - Setup the Master Virtual appliance

- Distribute the package to the server(s)/host(s) on which the appliance is to be setup.
- Extract the package.
- Install the virtual appliance.

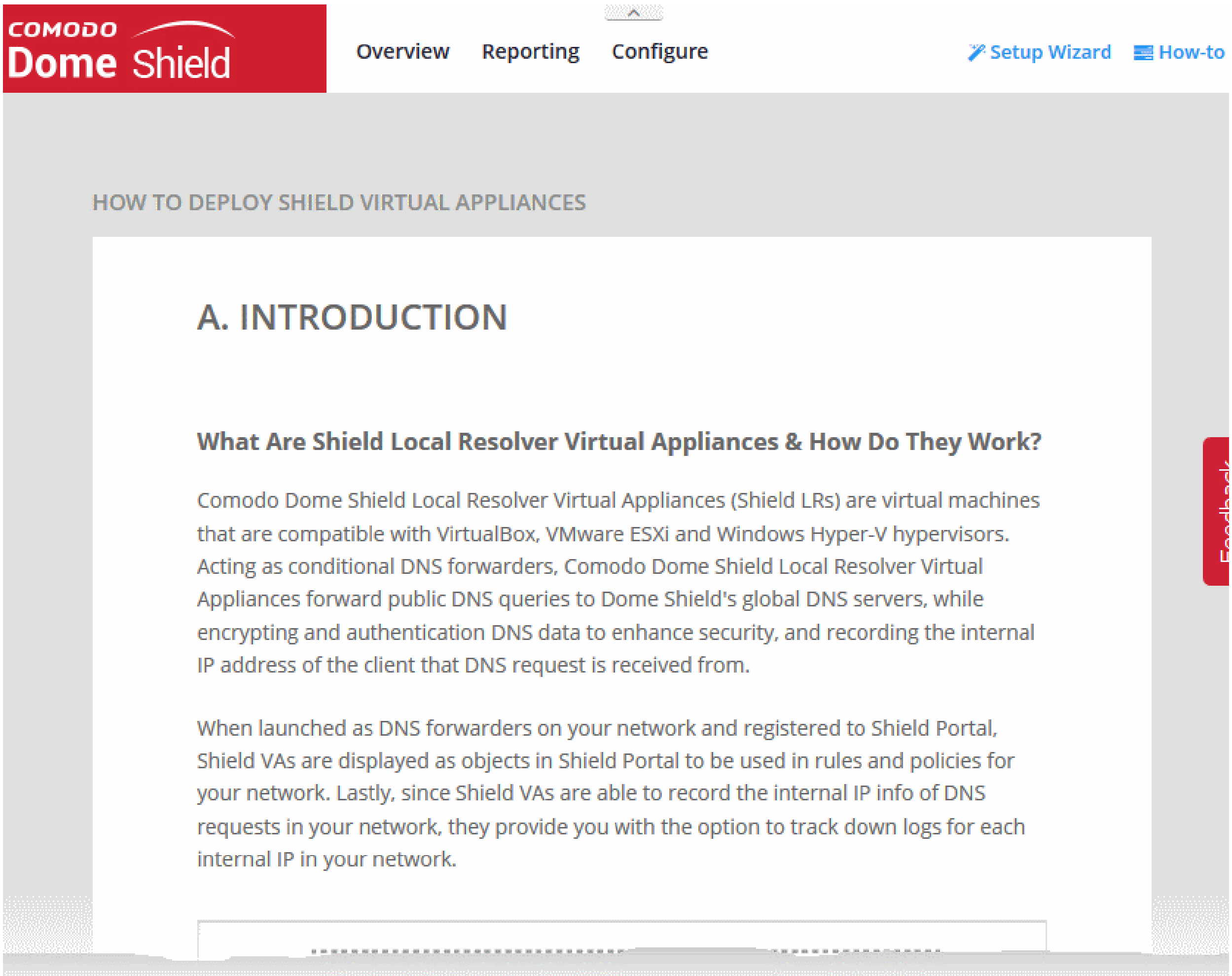
The Dome Shield interface contains tutorials to help you on installation of the virtual appliance on VMWare, VirtualBox and Hyper-V.

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



#	Name	Type	IP	Status	Version	Actions
1	OVA	Local Resolver	10.100.136.153	Inactive	0.2.0	🗑

The 'How to Deploy Shield Virtual Appliances' page will open with detailed instructions on installing the VA on VMWare, VirtualBox and Hyper-V.



HOW TO DEPLOY SHIELD VIRTUAL APPLIANCES

A. INTRODUCTION

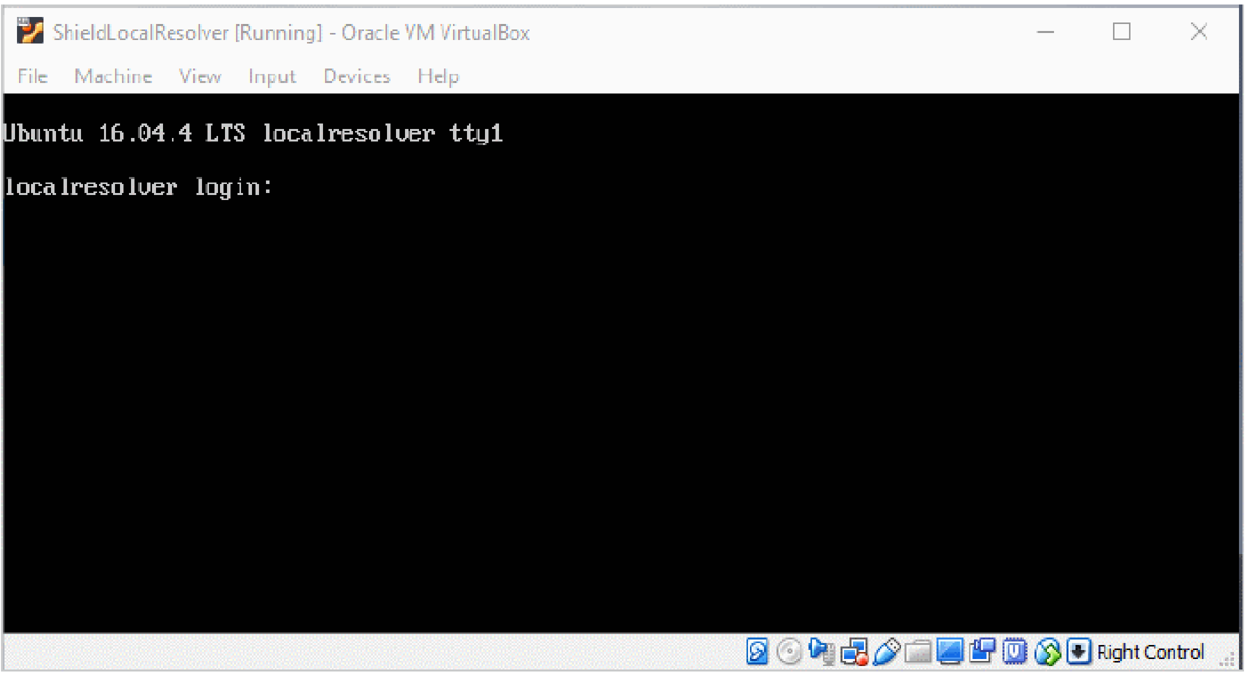
What Are Shield Local Resolver Virtual Appliances & How Do They Work?

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

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

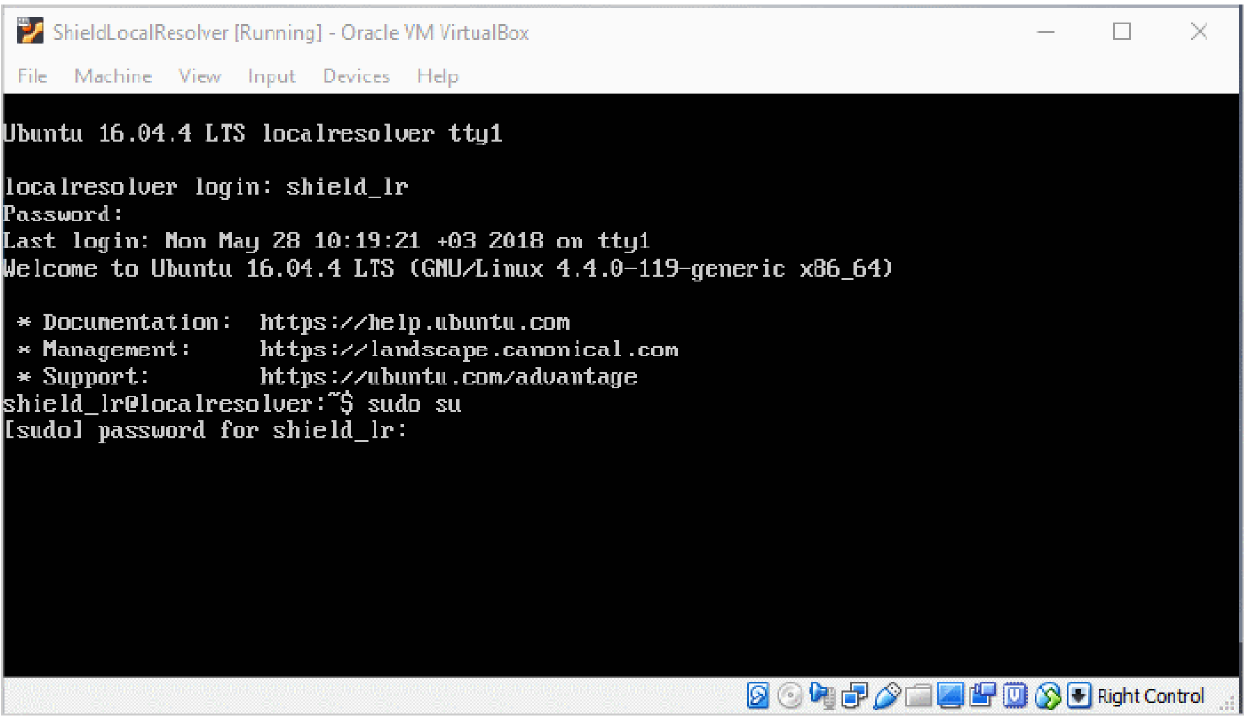
Configure the Local Resolver

- After the completion of installation, start-up the VA


ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Control

```
Ubuntu 16.04.4 LTS localresolver tty1

localresolver login:
```

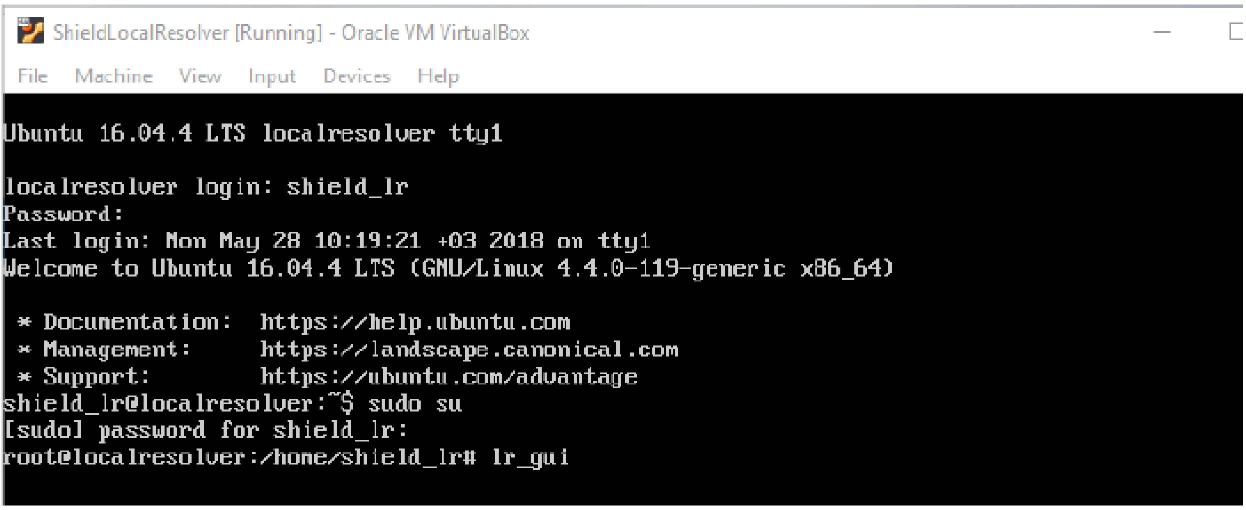
- Login to the appliance using the Username and Password contained in the credentials.txt file, the came with the setup package.


ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Control

```
Ubuntu 16.04.4 LTS localresolver tty1

localresolver login: shield_lr
Password:
Last login: Mon May 28 10:19:21 +03 2018 on tty1
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
shield_lr@localresolver:~$ sudo su
[sudo] password for shield_lr:
```

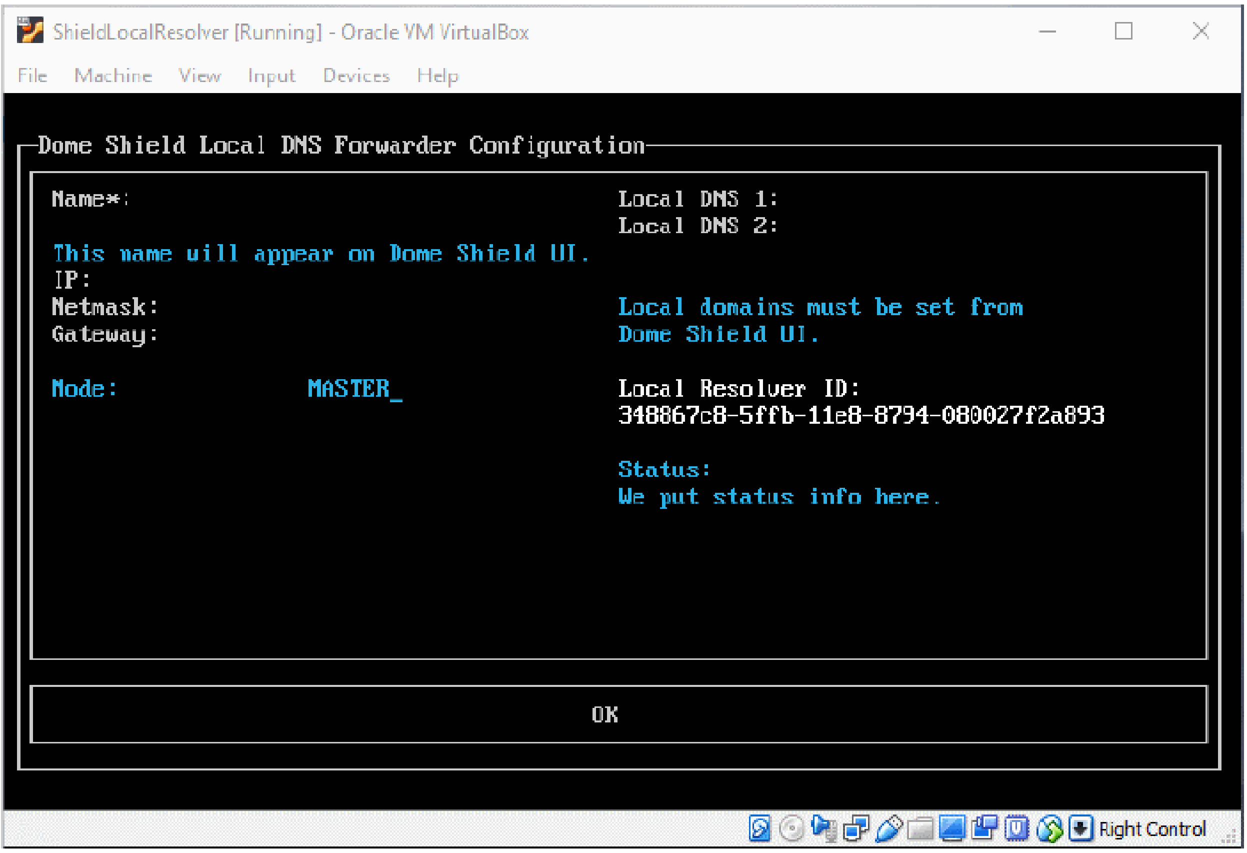
- Run the 'sudo su' command and enter the root password contained in the 'credentials.txt' file to gain the root access

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


ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
Ubuntu 16.04.4 LTS localresolver tty1

localresolver login: shield_lr
Password:
Last login: Mon May 28 10:19:21 +03 2018 on tty1
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
shield_lr@localresolver:~$ sudo su
[sudo] password for shield_lr:
root@localresolver:/home/shield_lr# lr_gui
```

The LR Configuration screen will open.


ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Control

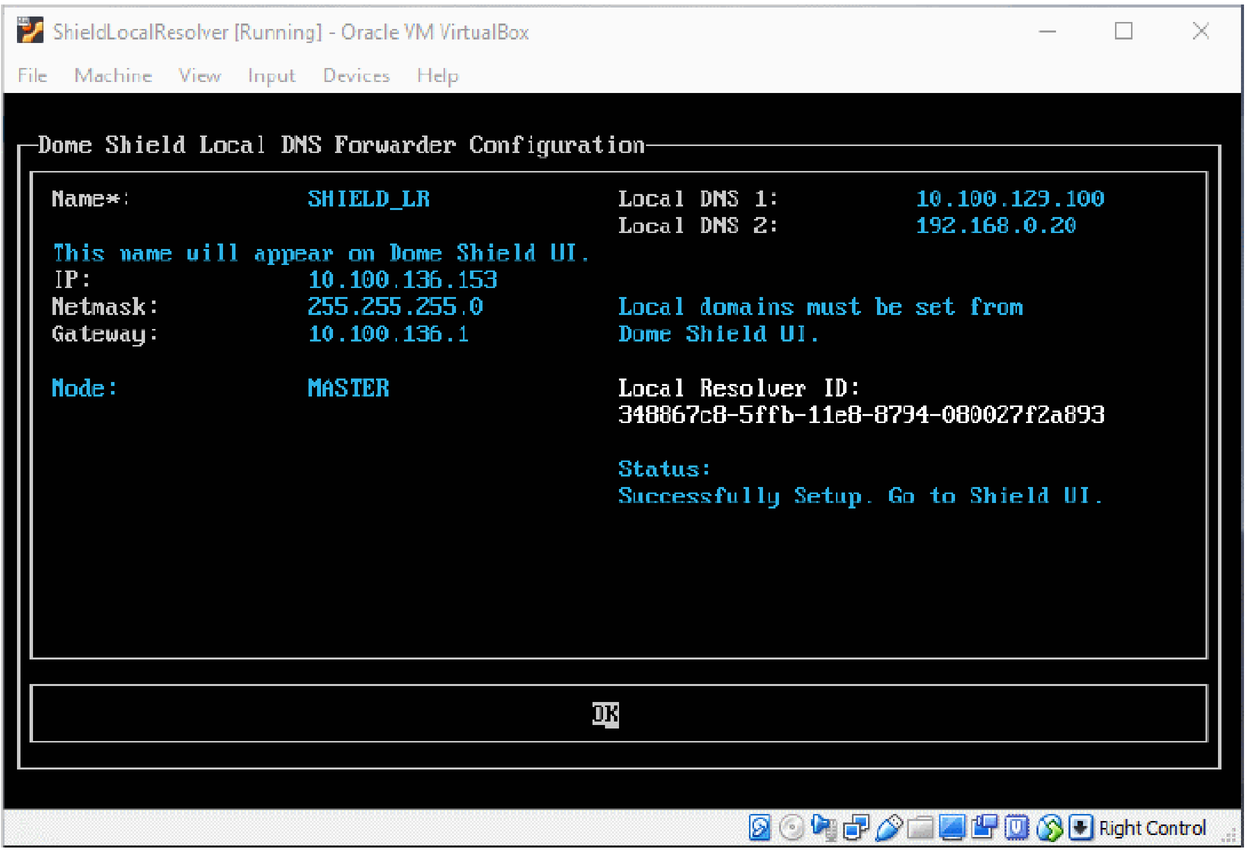
```
Dome Shield Local DNS Forwarder Configuration

 Name*:                                    Local DNS 1:
                                           Local DNS 2:
 This name will appear on Dome Shield UI.
 IP:
 Netmask:                                  Local domains must be set from
 Gateway:                                  Dome Shield UI.

 Mode:              MASTER_                Local Resolver ID:
                                           348867c8-5ffb-11e8-8794-080027f2a893

                                           Status:
                                           We put status info here.

                                   OK
```

LR Configuration Screen - Table of Parameters	
Form Element	**Description**
Name	Enter a label for identifying the Master LR VA. This name will appear in the Dome Shield interface after registration.
IP	Enter an IP address to be assigned to the LR VA.
Netmask	Enter the netmask for the VA
Gateway	Enter the IP address of the Gateway of the network
Mode	Select 'Master' if this is the first resolver being setup on the network.

Local DNS 1 and Local DNS 2	Enter the IP addresses of the primary and secondary DNS servers in the network.
Local Resolver ID	Note down the ID string displayed in this field. This ID has to be entered for registering the LS and importing the network into Dome Shield. See Step 3 - Register the Master VA for more details.
Status	Indicates the current status of the LR VA.

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

Your configuration will be saved.

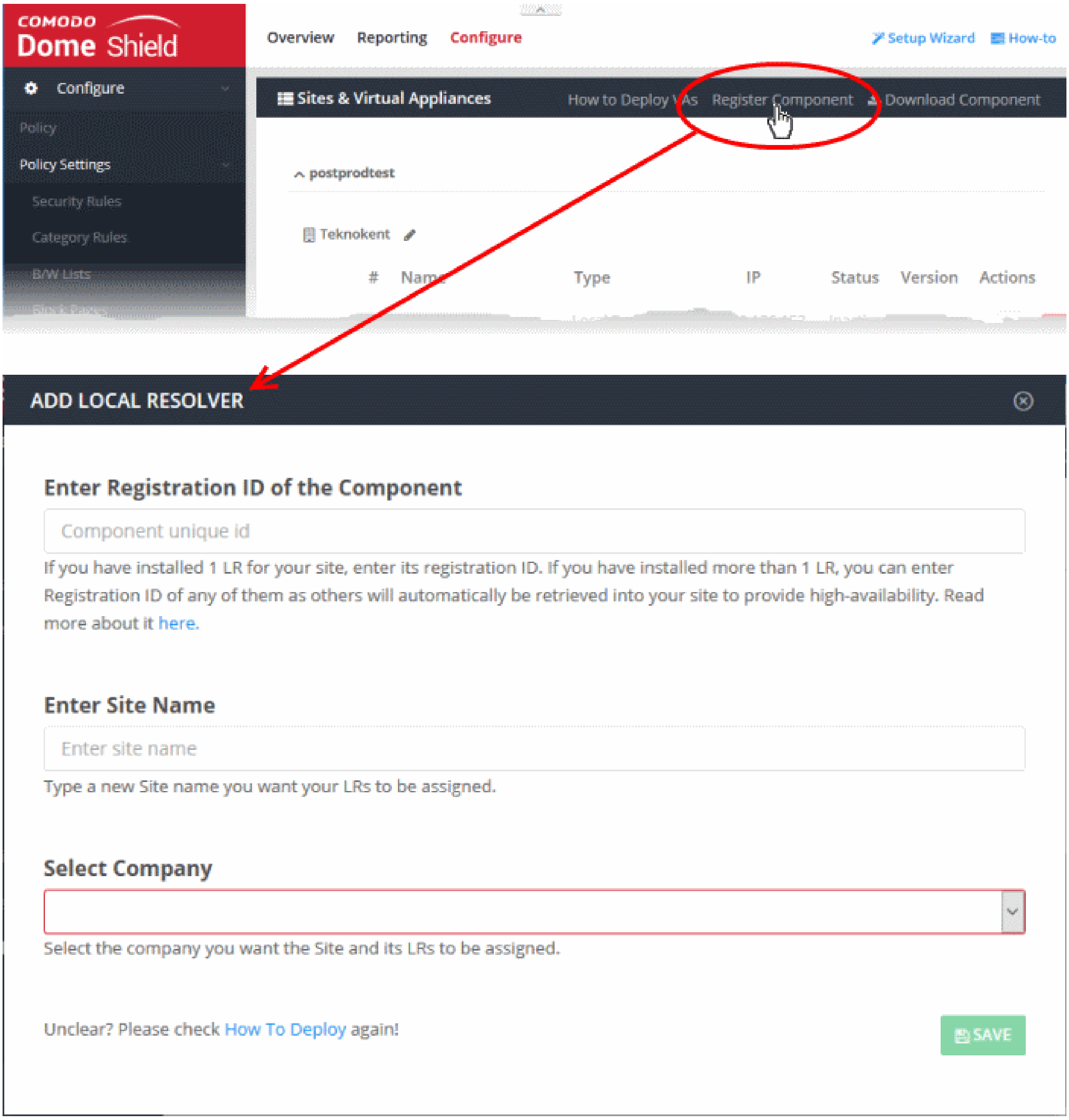

ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Control

```
Dome Shield Local DNS Forwarder Configuration

Name*:              SHIELD_LR                 Local DNS 1:          10.100.129.100
                                              Local DNS 2:          192.168.0.20
This name will appear on Dome Shield UI.
IP:                 10.100.136.153
Netmask:            255.255.255.0             Local domains must be set from
Gateway:            10.100.136.1              Dome Shield UI.

Mode:               MASTER                    Local Resolver ID:
                                              348867c8-5ffb-11e8-8794-080027f2a893

                                              Status:
                                              Successfully Setup. Go to Shield UI.

                                  OK
```

The next step is to register the LR to Dome Shield.

Step 3 - Register the Master VA

- Login to Dome Shield
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Register Component'



Enter Registration ID of the Component

Component unique id

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

Enter Site Name

Enter site name

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

Select Company

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

Unclear? Please check How To Deploy again!

SAVE

The 'Add Local Resolver' dialog will appear.

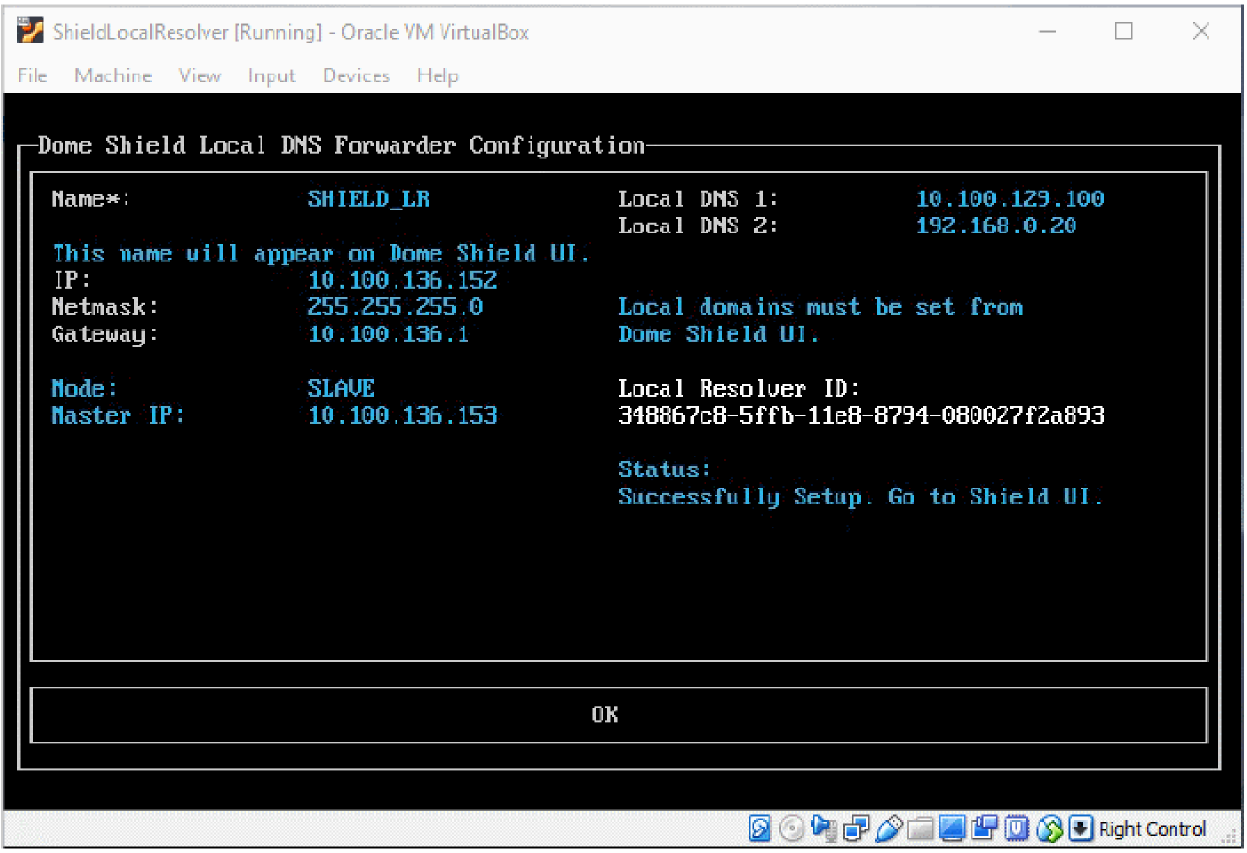
'Add Local Resolver' dialog - Table of Parameters	
Form Element	**Description**
Enter Registration ID of the Component	The unique identifier string generated for the LR VA. Enter the ID displayed in the LR configuration screen. See Configure the Local Resolver in Step 2 - Setup the Master Virtual appliance for more details.
Enter Site Name	The label of the network to be imported. The network will be identified with the same in Dome Shield.
Select Company	This field will be available only for MSP customers. • Choose the customer company for which the imported network has to be enrolled, from the drop-down.

- Click 'Save' to register the Local Solver

The local resolver will be added to the list in the 'Sites & Virtual Appliances' and the network will be auto-imported. You can apply policy to the whole network, or define internal network segments by adding internal network addresses to apply different policies. 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 ans setup the VA as slave LR.



```
Dome Shield Local DNS Forwarder Configuration

Name*:               SHIELD_LR                  Local DNS 1:          10.100.129.100
                                                Local DNS 2:          192.168.0.20
This name will appear on Dome Shield UI.
IP:                  10.100.136.152
Netmask:             255.255.255.0              Local domains must be set from
Gateway:             10.100.136.1               Dome Shield UI.

Mode:                SLAVE                      Local Resolver ID:
Master IP:           10.100.136.153             348867c8-5ffb-11e8-8794-080027f2a893

                                                Status:
                                                Successfully Setup. Go to Shield UI.

                                      OK
```

LR Configuration Screen - Table of Parameters	
Form Element	**Description**
Name	Enter a label for identifying the Slave LR VA.
IP	Enter an IP address to be assigned to the LR VA.
Netmask	Enter the netmask for the VA
Gateway	Enter the IP address of the Gateway of the network
Mode	Select 'Slave'
Master IP	Appears on selecting the 'Slave' mode. Enter the IP address of the Master Local Resolver Virtual Appliance.
Local DNS 1 and Local DNS 2	Enter the IP addresses of the primary and secondary DNS servers in the network.
Local Resolver ID	Note down the ID string displayed in this field. This ID has to be entered for registering

	the LS and importing the network into Dome Shield. See Step 3 - Register the Master VA for more details.
Status	Indicates the current status of the LR VA.

- 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.

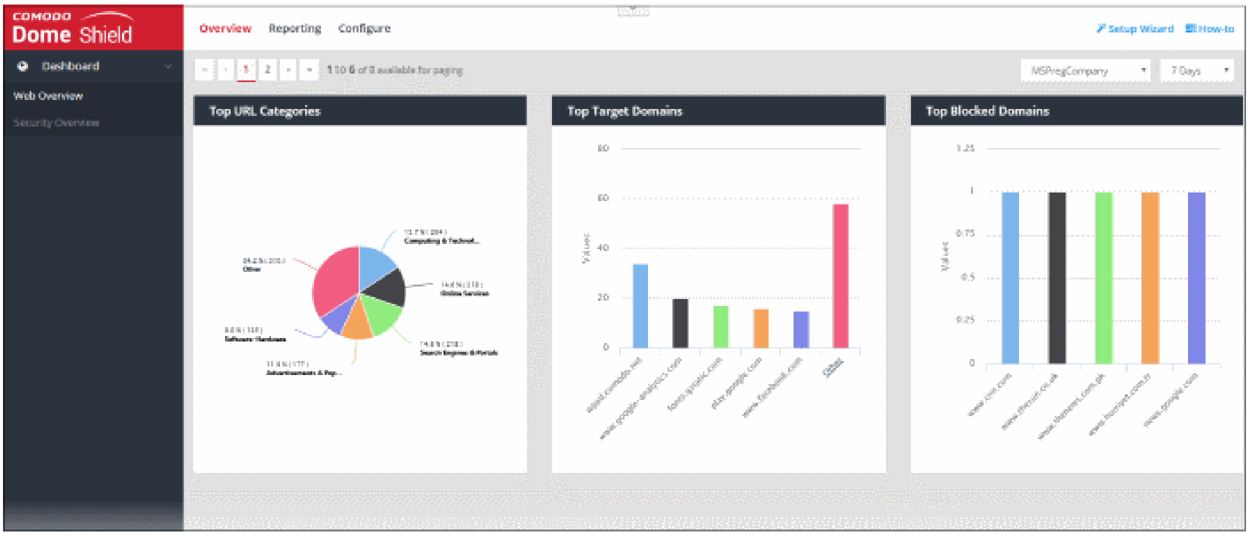
Step 5 - Configure DNS Settings in the endpoints to point to the Local Resolvers

The next step is to configure your network endpoints' DNS settings to forward queries to the Local Resolver VA's.

- Preferred DNS server - IP address assigned to the Master LR VA
- Alternate DNS server - IP address assigned to the Slave LR VA

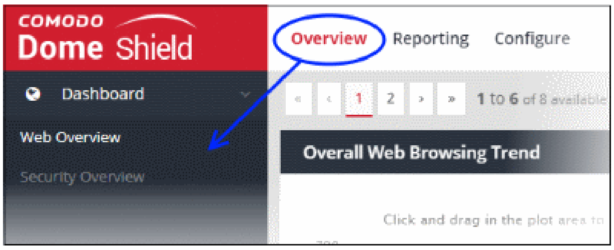
2 The Admin Console

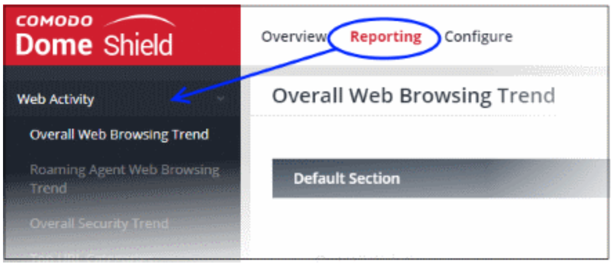
The admin console contains statistics and charts about your protected environment and is the springboard from which you can launch tasks and configure the service. From here, you can add networks and mobile/roaming devices, create security policies, analyze statistics and more.



The items in the left-hand menu will change depending on whether you select 'Overview', 'Reporting' or 'Configure' in the top-menu.

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.

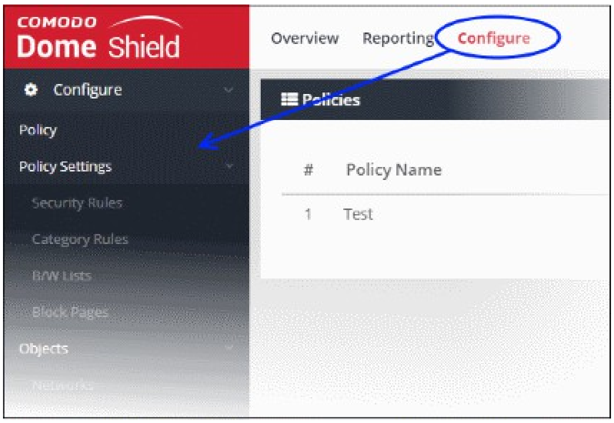




Reporting - View reports on threats detected on your assets, security trends, web browsing trends and more. You can choose from a range of pre-configured reports or create a custom report.

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

See 'Reports' for more details.

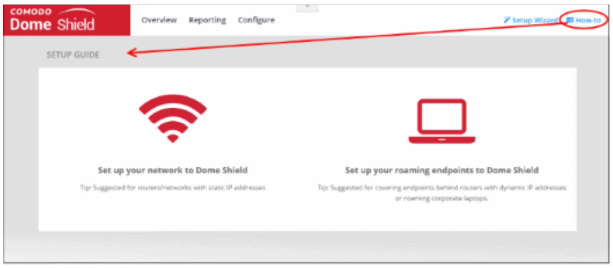


Configure - Add networks and individual endpoints to Dome Shield and apply security policies to them.

- **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.



SETUP GUIDE

Set up your network to Dome Shield

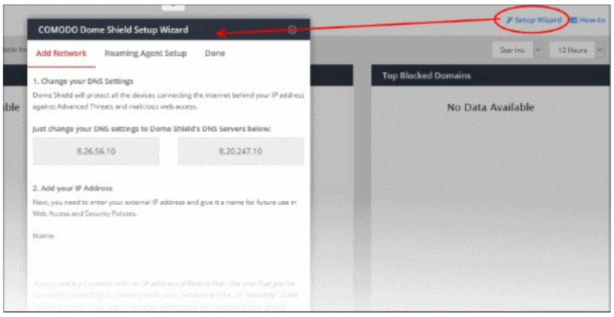
Tip: Suggested for routers/networks with static IP addresses

Set up your roaming endpoints to Dome Shield

Tip: Suggested for covering endpoints behind routers with dynamic IP addresses or roaming corporate laptops.

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

Setup Wizard - Add network quickly and download the agent for roaming devices.



COMODO Dome Shield Setup Wizard

Add Network | Roaming Agent Setup | Done

1. Change your DNS Settings

Dome Shield will protect all the devices connecting the internet behind your IP address against Advanced Threats and malicious web access.

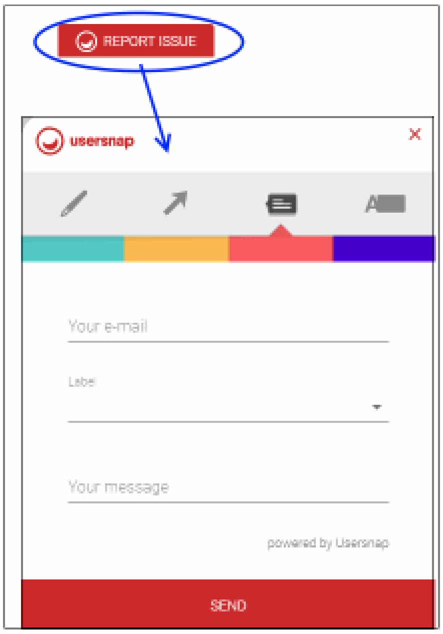
Just change your DNS settings to Dome Shield's DNS Servers below:

8.26.56.10 | 8.20.247.10

2. Add your IP Address

Next, you need to enter your external IP address and give it a name for future use in Web Access and Security Policies.

Name



Your e-mail

Label

Your message

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.

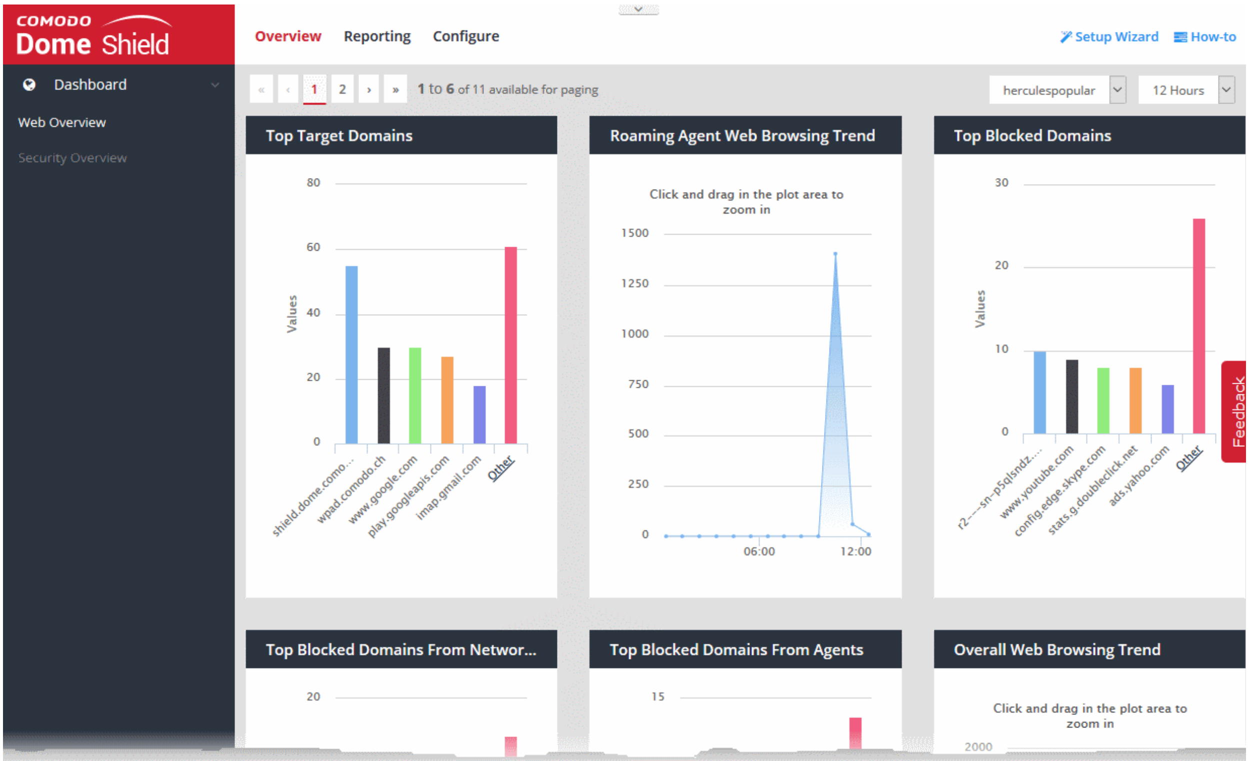
3 The Dashboard

- Click 'Overview' to open the Dome Shield 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 or concern. 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 - Contains statistics about top websites by category, general browsing trends, top targets and blocked domains.
- Security Overview - Contains statistics about security trends and top malicious sites that were blocked.



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

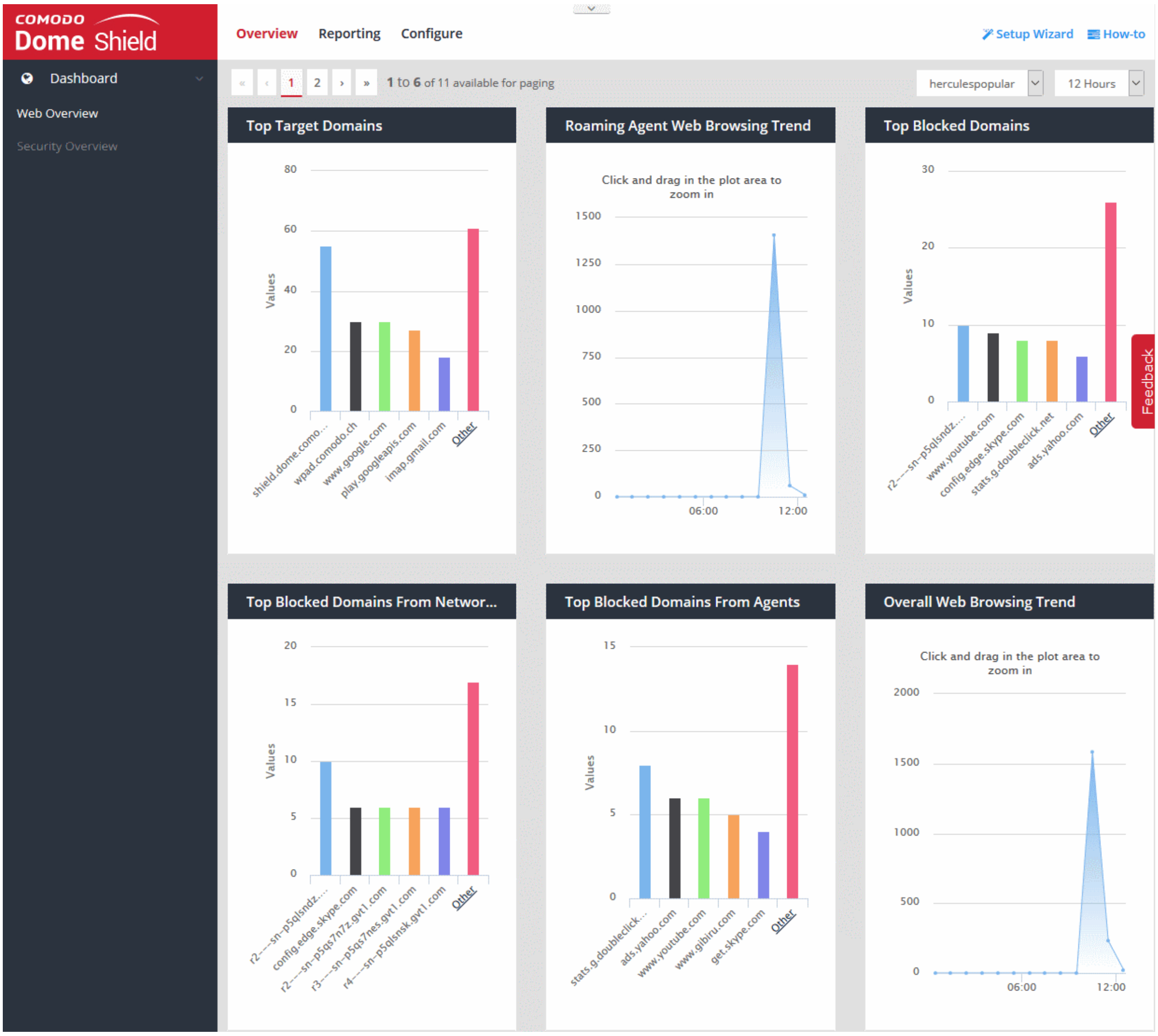
The following sections explain more about:

- 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



1 to 6 of 11 available for paging

herculespopular

12 Hours

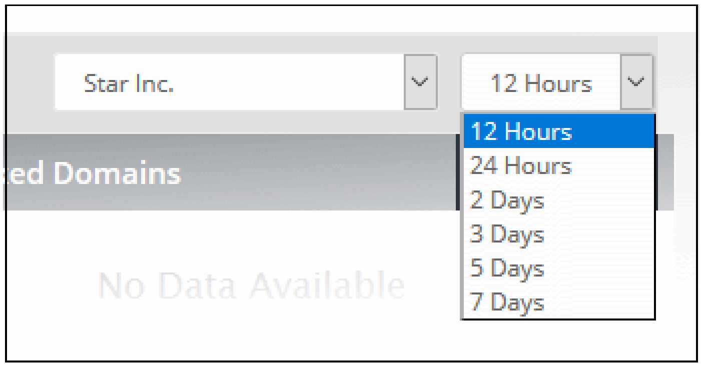
Click and drag in the plot area to zoom in

'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

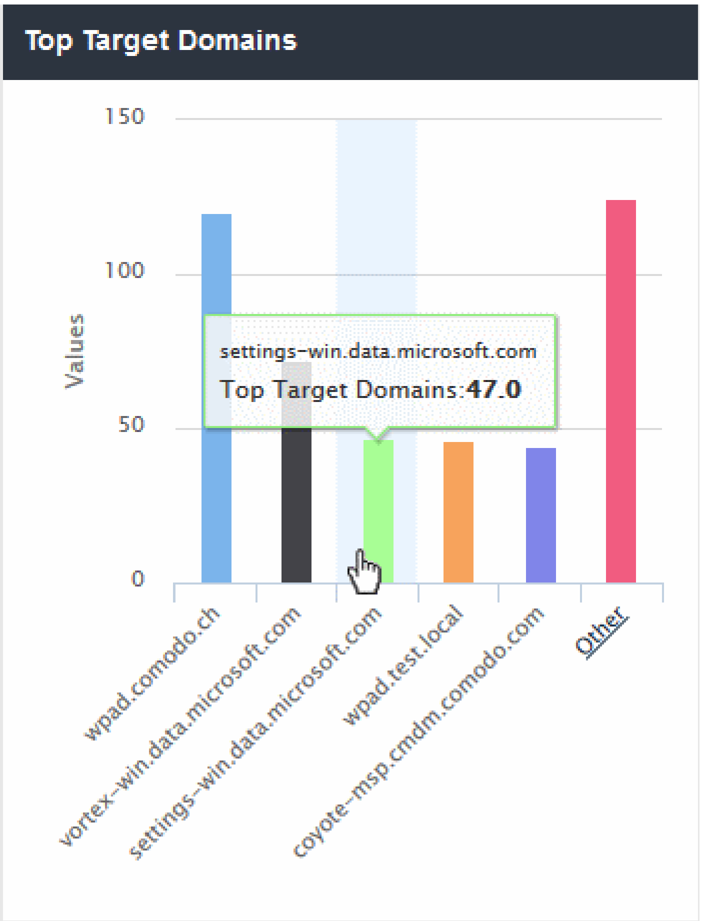
MSP customers can view statistics for particular customers. Possible data ranges are from the last 12 hours to the previous 7 days.



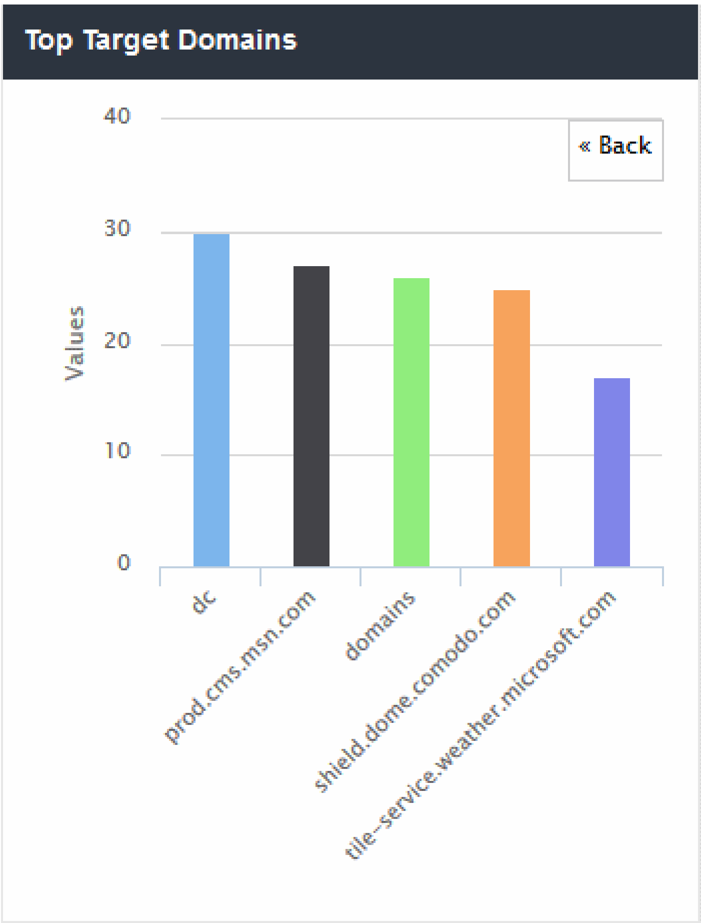
Top Target Domains

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.


Top Target Domains
150
100
50
0
Values
settings-win.data.microsoft.com
Top Target Domains:47.0
wpad.comodo.ch
vortex-win.data.microsoft.com
settings-win.data.microsoft.com
wpad.test.local
coyote-msp.cmdm.comodo.com
Other

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

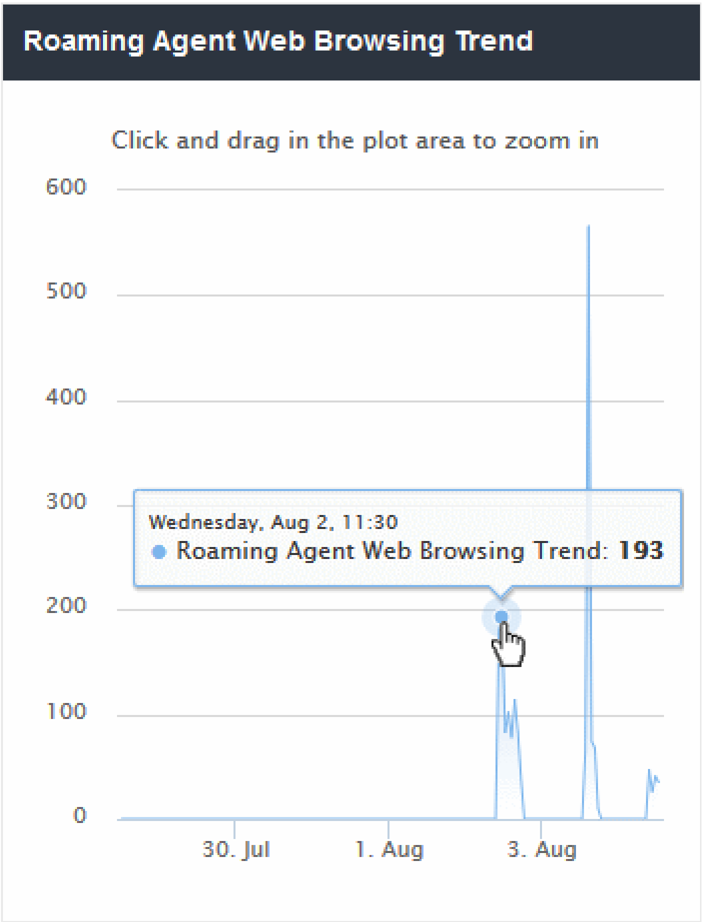


  - Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See 'View Logs' for more details.

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.

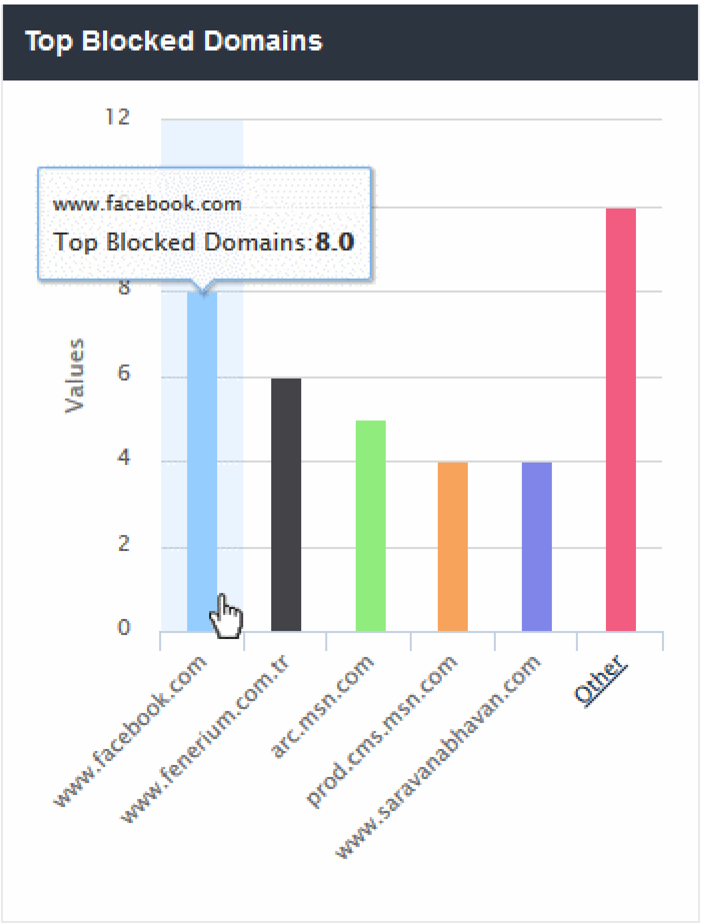

Roaming Agent Web Browsing Trend
Click and drag in the plot area to zoom in
600
500
400
300
200
100
0
30. Jul
1. Aug
3. Aug
Wednesday, Aug 2, 11:30
Roaming Agent Web Browsing Trend: 193

- 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.

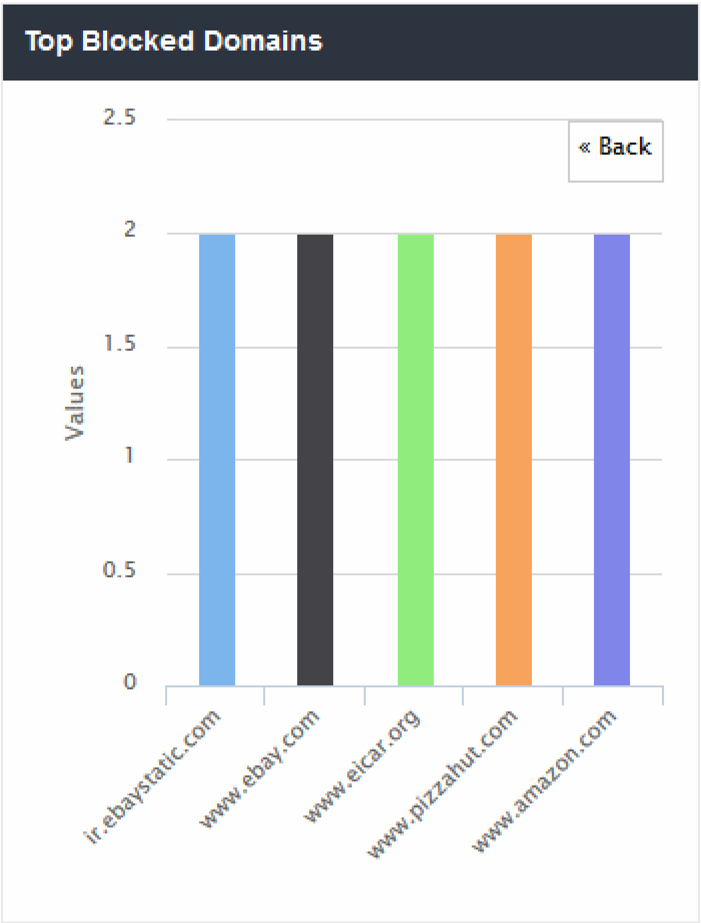
Top Blocked Domains

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.

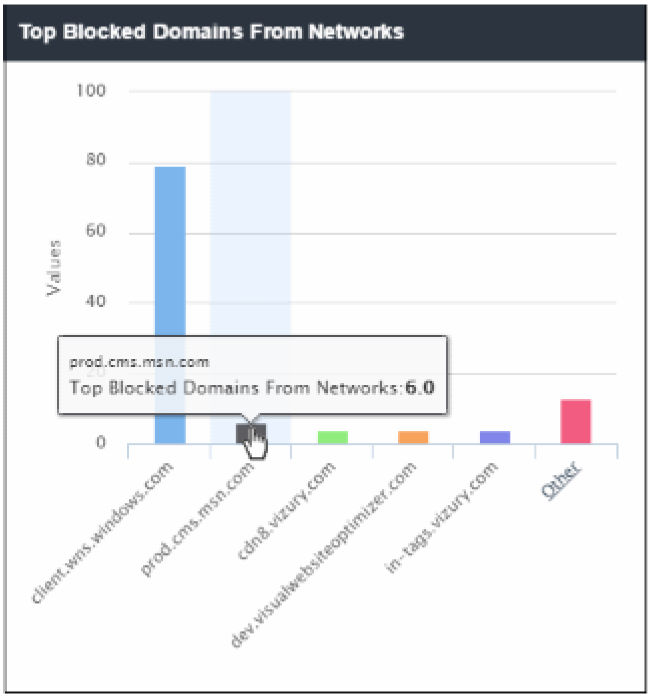


  - Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See 'View Logs' for more details.

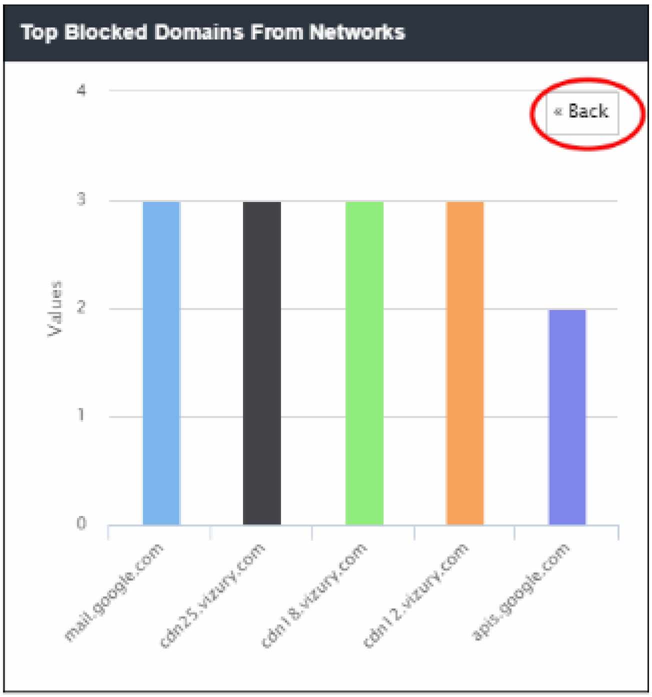
Top Blocked Domains from Networks

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.



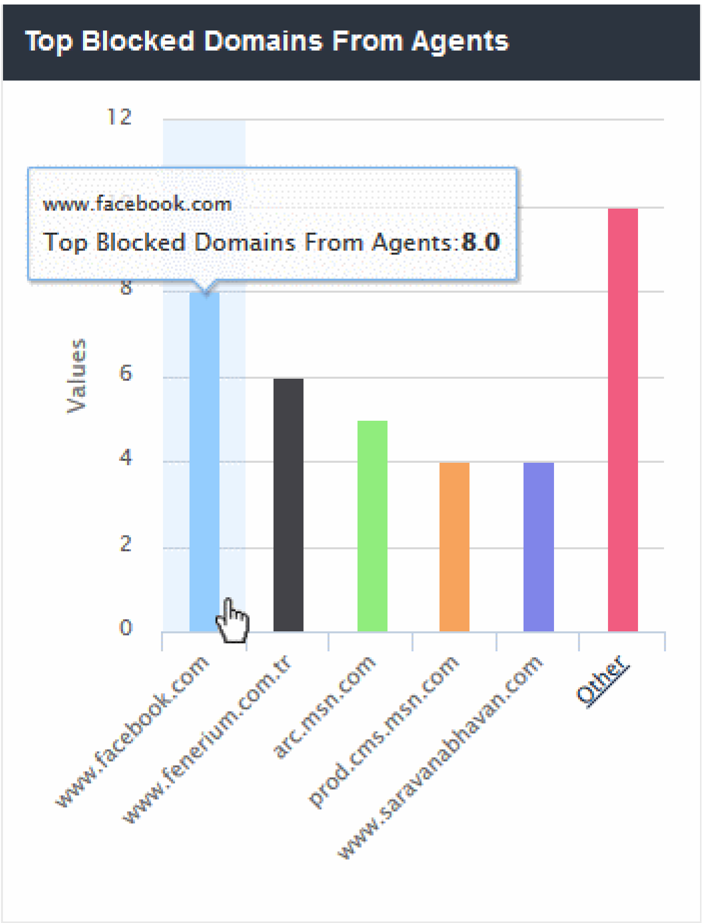
  - Click 'Back' to return to the original view.

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

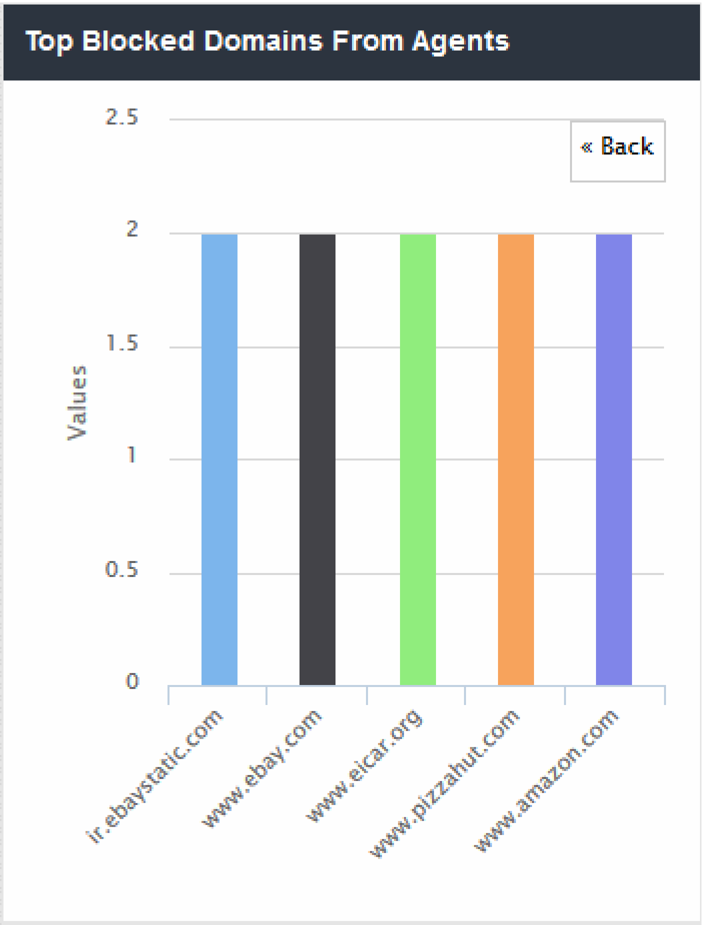
Top Blocked Domains from Agents

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.



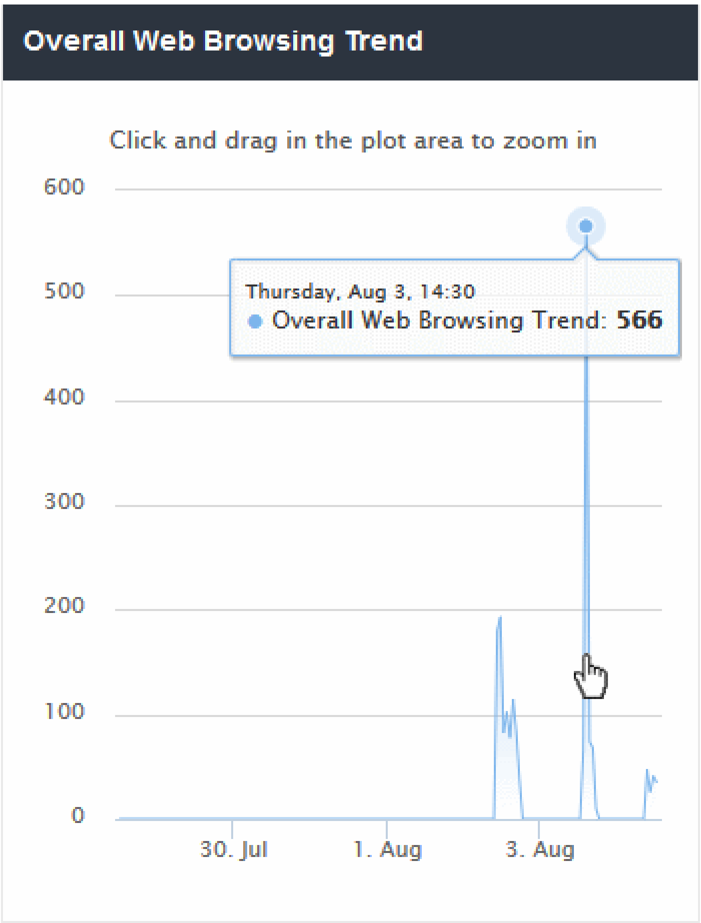
- Click 'Back' to return to the original view.

- 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.

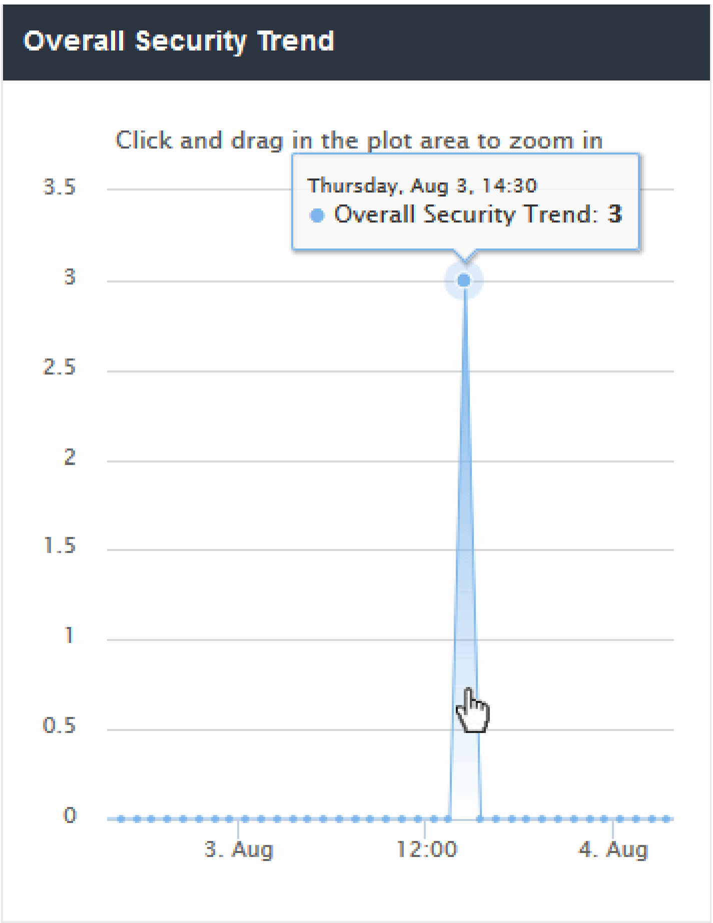


- Click and drag on the chart to zoom into a particular time period.
    - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See 'View Logs' for more details.

Overall Security Trend

Shows the number of harmful sites blocked on your network(s) and endpoints based on security rules over time.

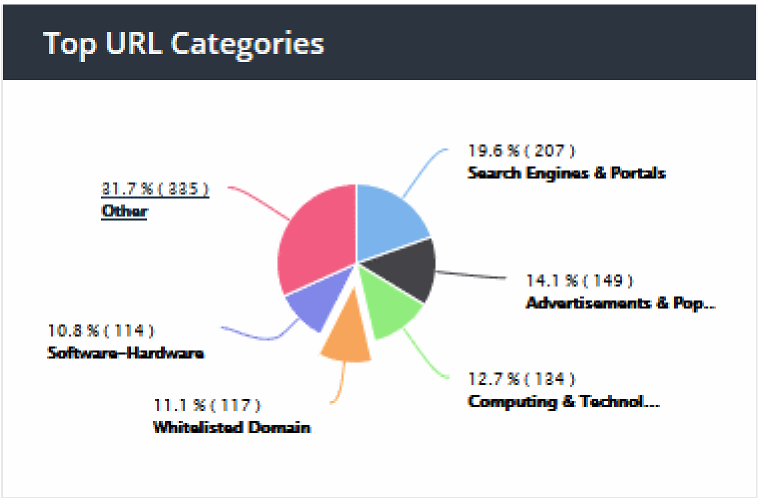
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.



- 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

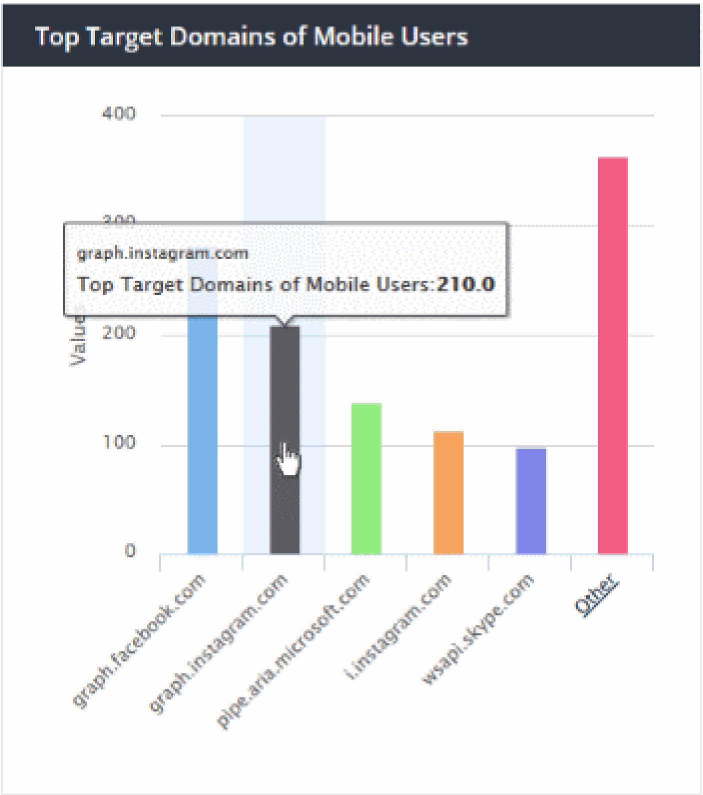
- The website categories and whitelisted domains most often visited by your users.
- Place your mouse cursor over a sector to view further details.
- Click on a sector to see a log of requested domains in that category. See 'View Logs' for more details..



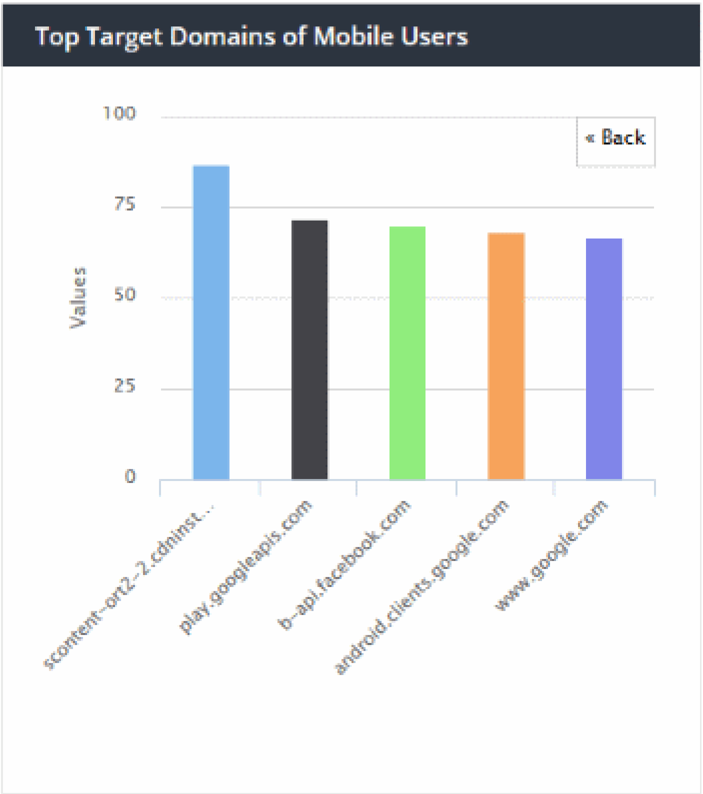
Top Target Domains of Mobile Users

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.



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

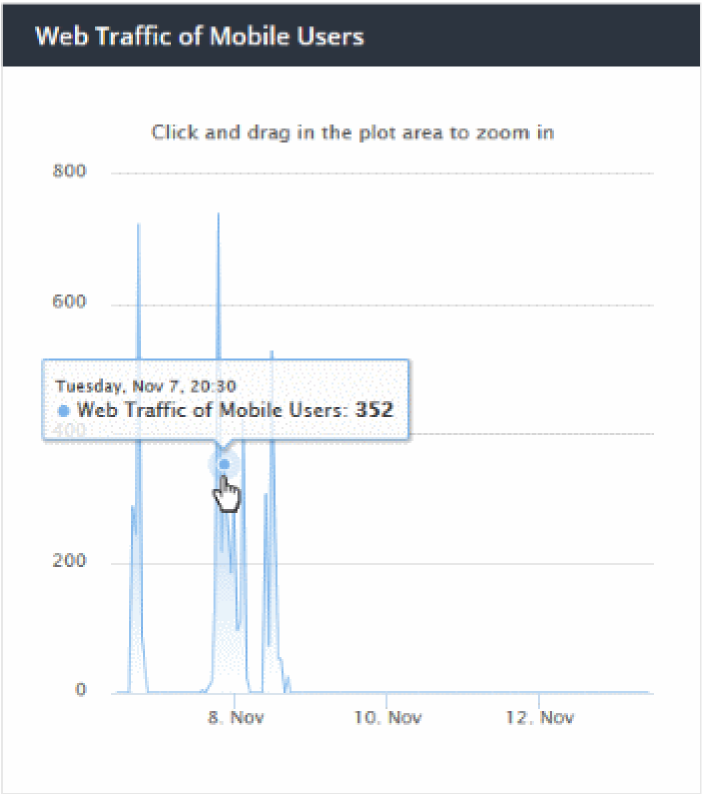


  - Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See 'View Logs' for more details.

Web Traffic of Mobile Users

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

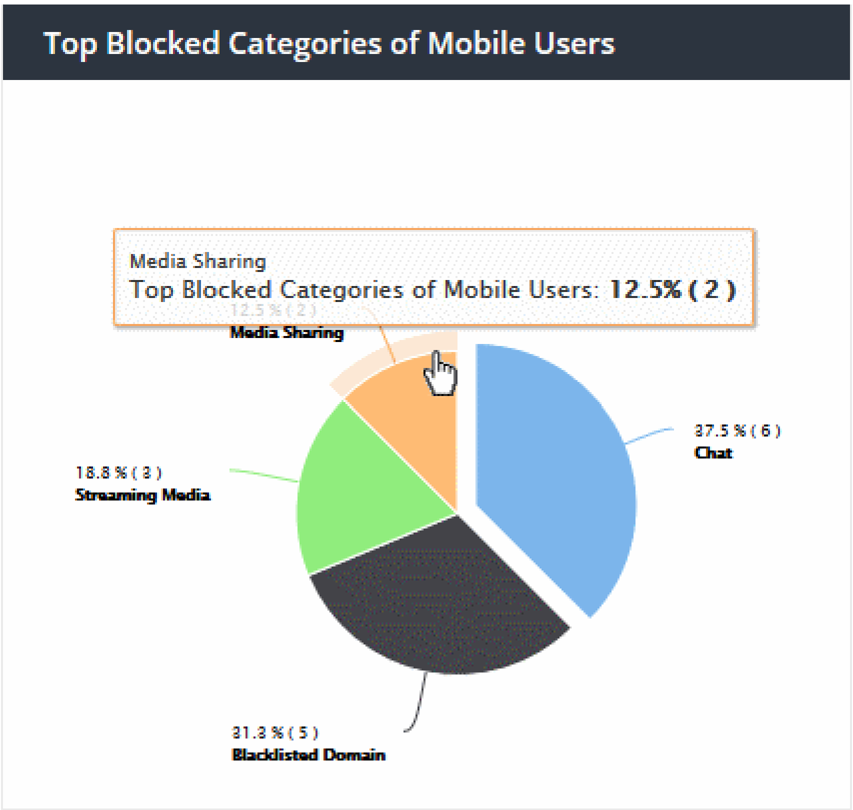
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.


Web Traffic of Mobile Users
Click and drag in the plot area to zoom in
800
600
400
200
0
8. Nov
10. Nov
12. Nov
Tuesday, Nov 7, 20:30
● Web Traffic of Mobile Users: 352

- 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.

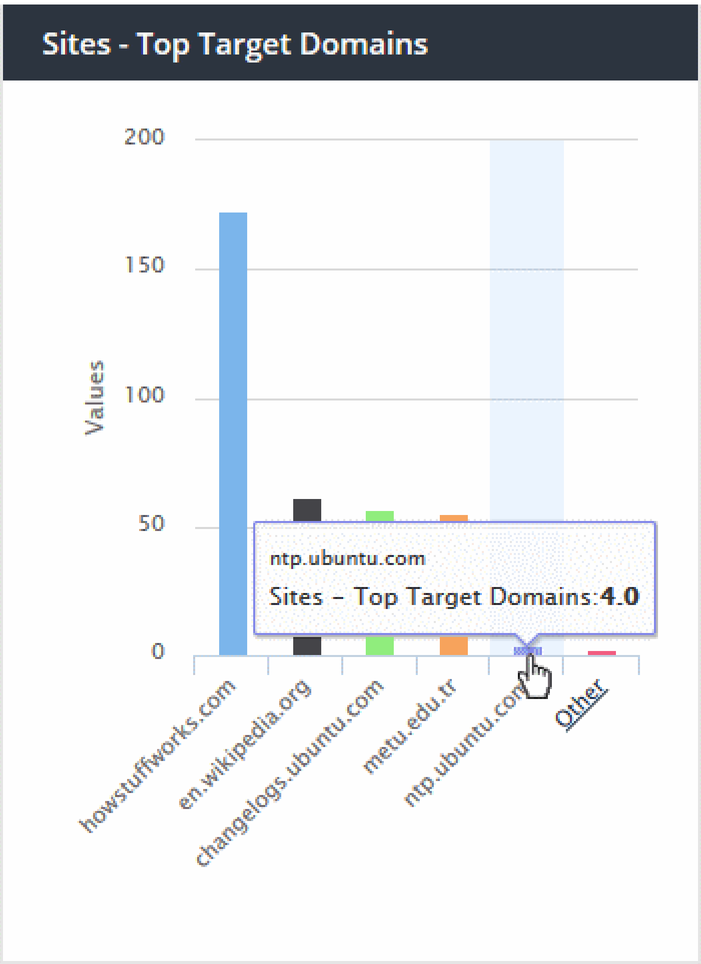


- Click on a sector to see a log of blocked categories for mobile users. See 'View Logs' for more on this.

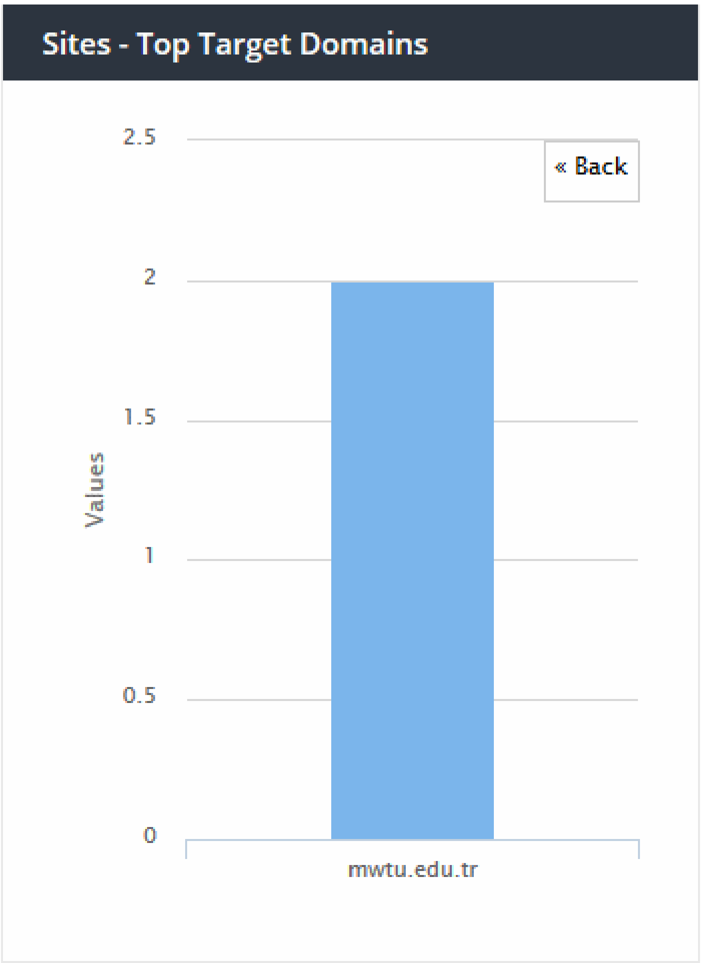
Sites - Top Target Domains

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.

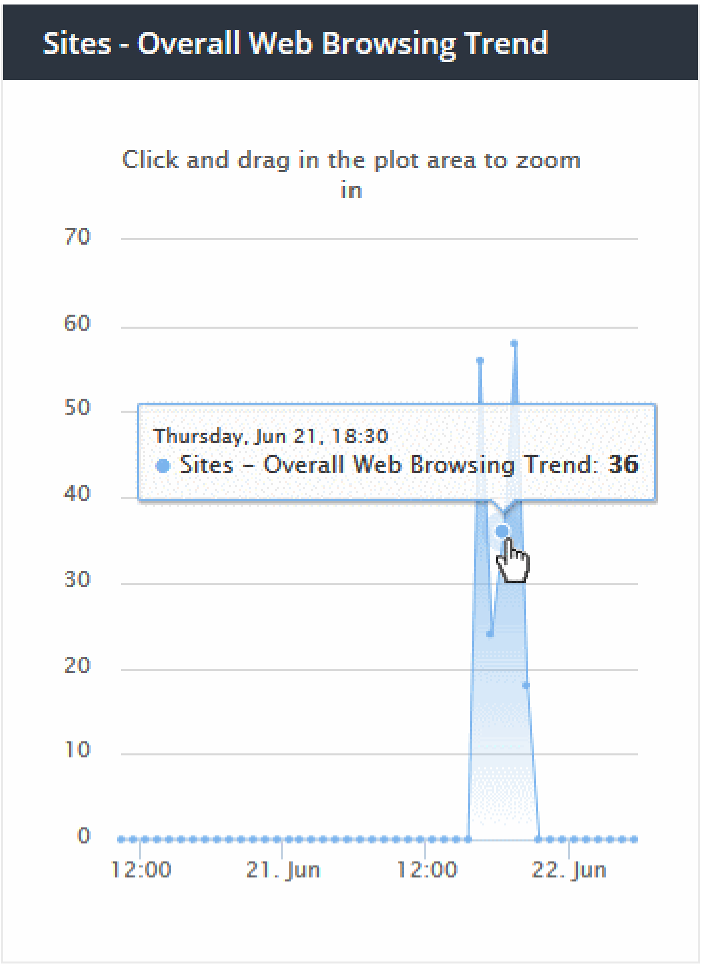


- Click 'Back' to return to the original view.
- Click on a chart bar to view domain request logs. See '**View Logs**' for more details.

Sites - Overall Web Browsing Trend

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

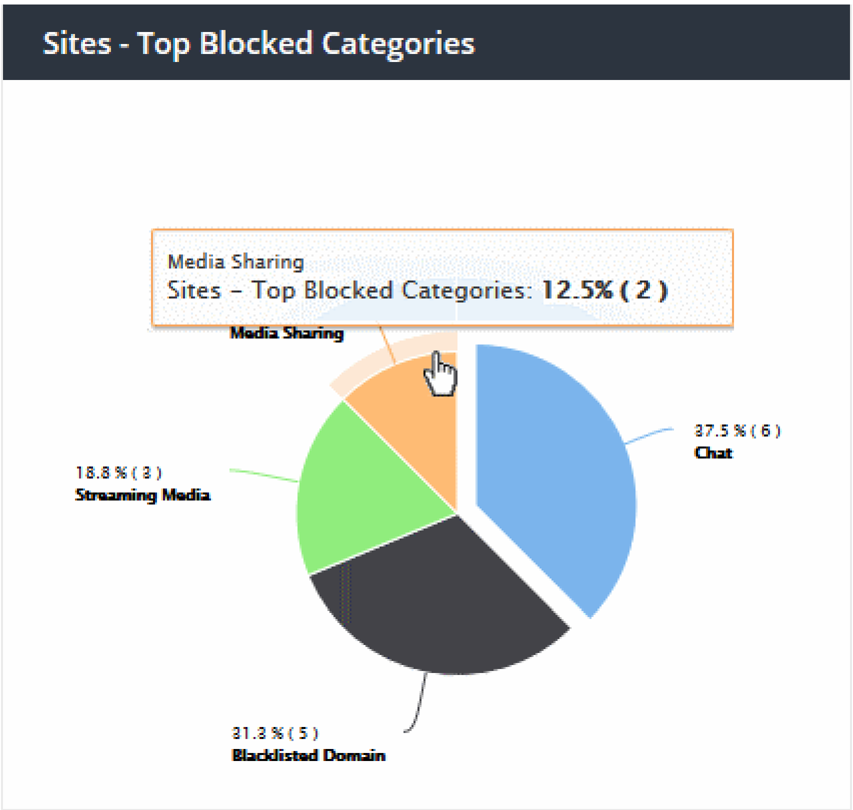
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.


Sites - Overall Web Browsing Trend
Click and drag in the plot area to zoom in
70
60
50
40
30
20
10
0
12:00
21. Jun
12:00
22. Jun
Thursday, Jun 21, 18:30
● Sites – Overall Web Browsing Trend: 36

- 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.

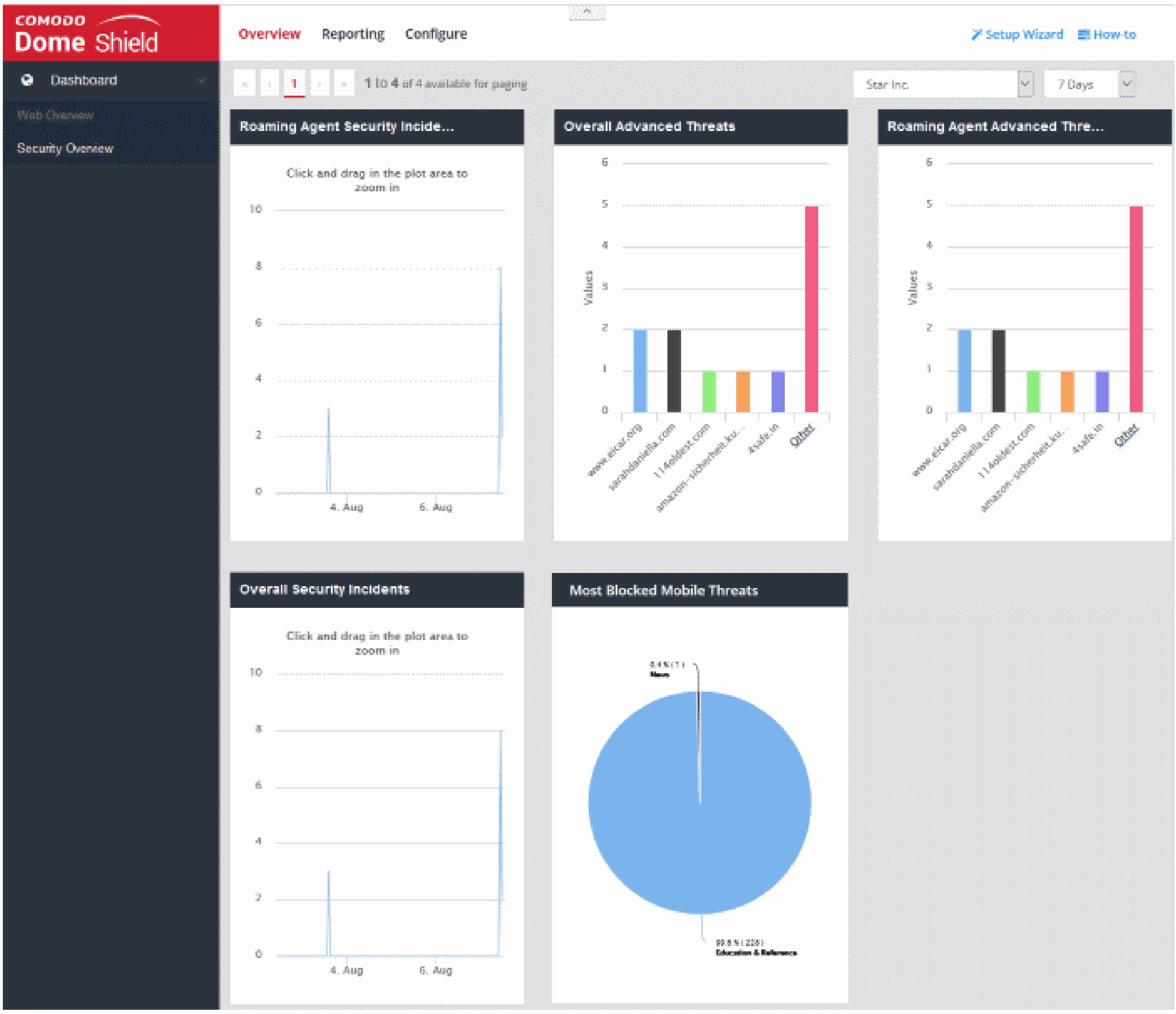


- Click on a sector to see a log of blocked categories. See 'View Logs' for more on this.

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:

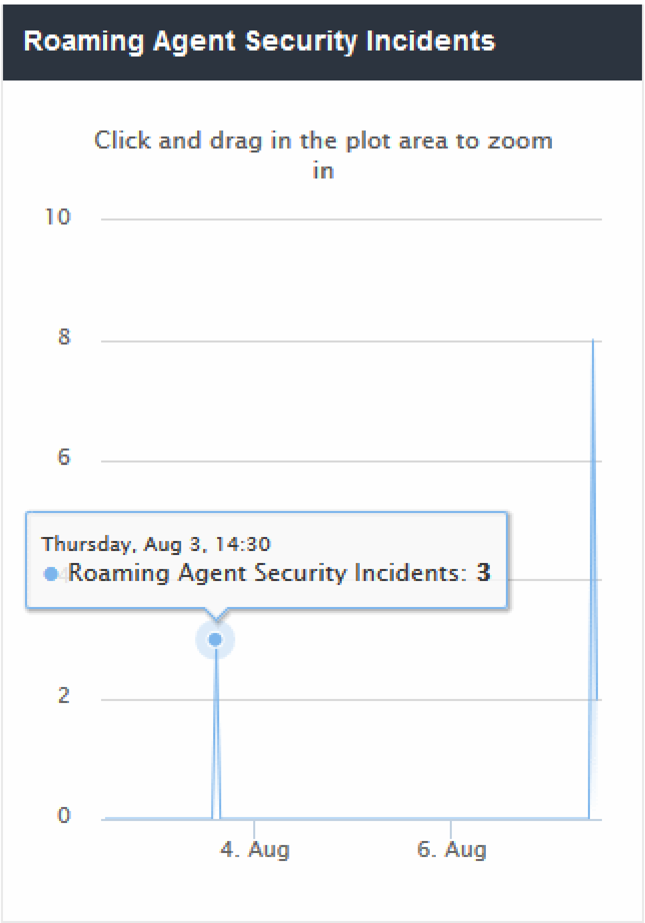
- Roaming Agent Security Incidents
- Overall Advanced Threats
- Roaming Agent Advanced Threats
- Overall Security Incidents
- Most Blocked Mobile Threats
- Sites - Most Blocked Threats

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.

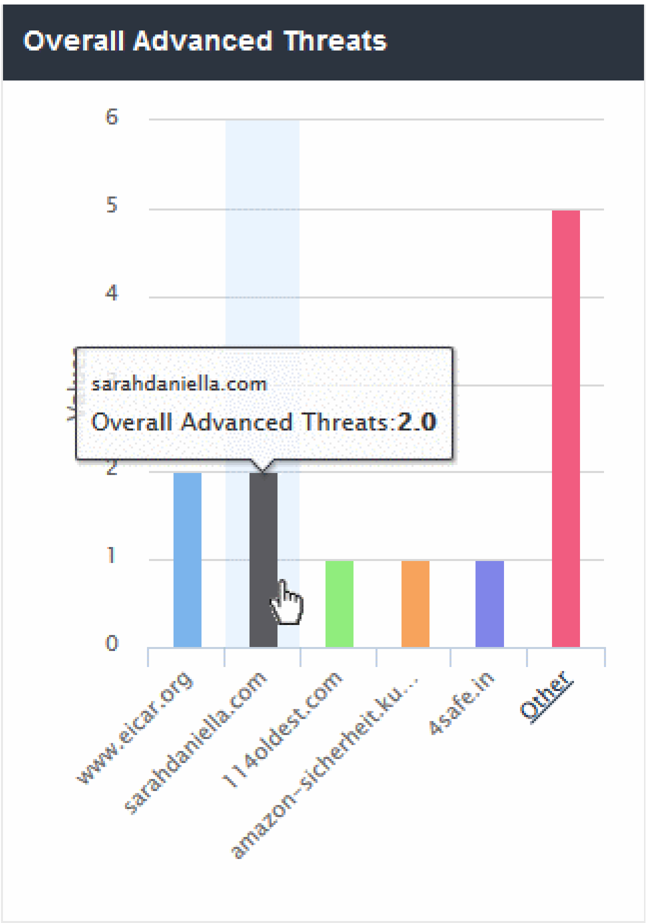


- Click and drag on the chart to zoom into a particular time period.
    - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See 'View Logs' for more details.

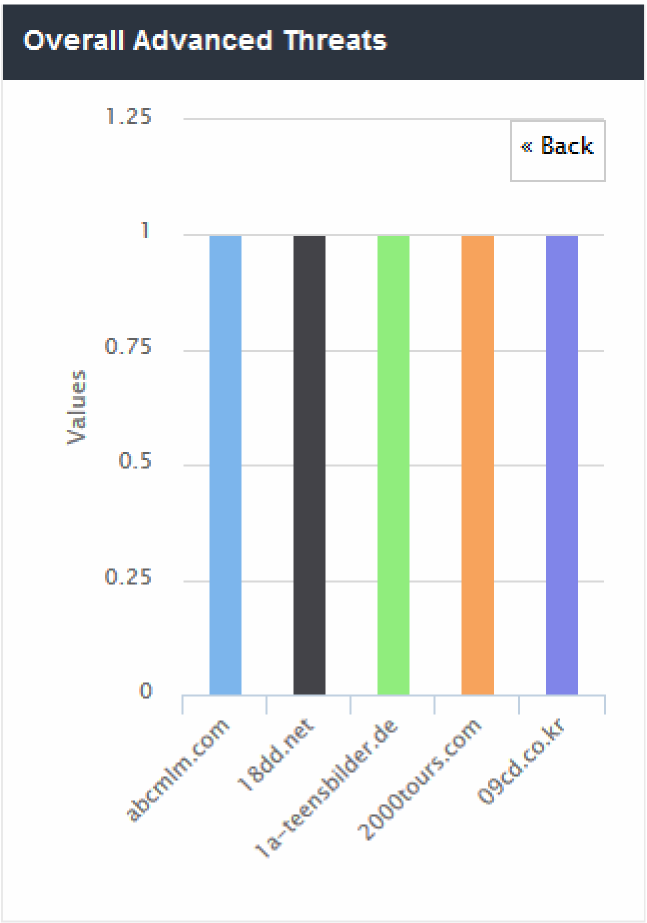
Overall Advanced Threats

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.

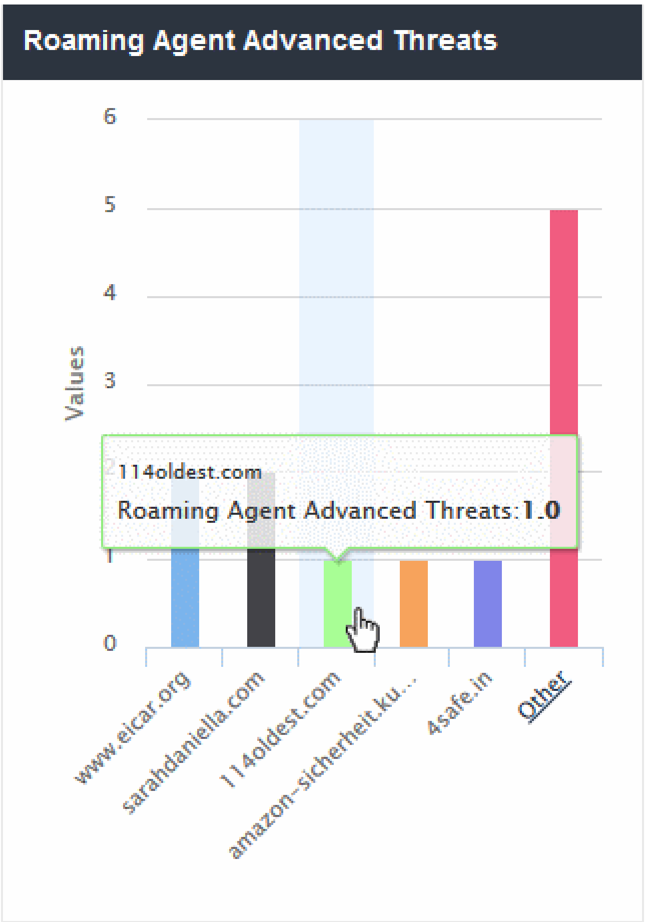


  - Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See 'View Logs' for more details.

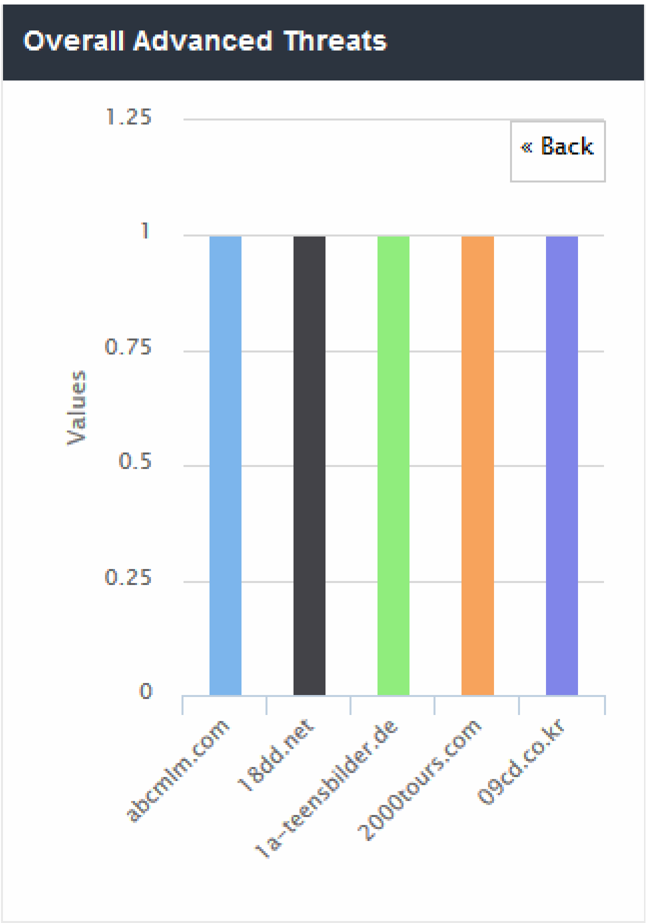
Roaming Agent Advanced Threats

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.



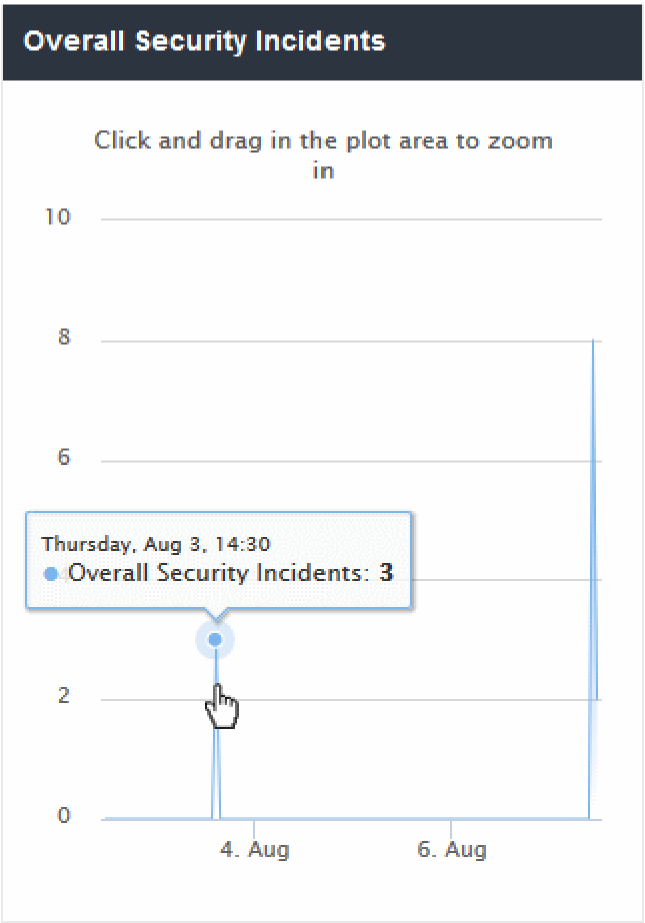
- Click 'Back' to return to the original view.

- 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.



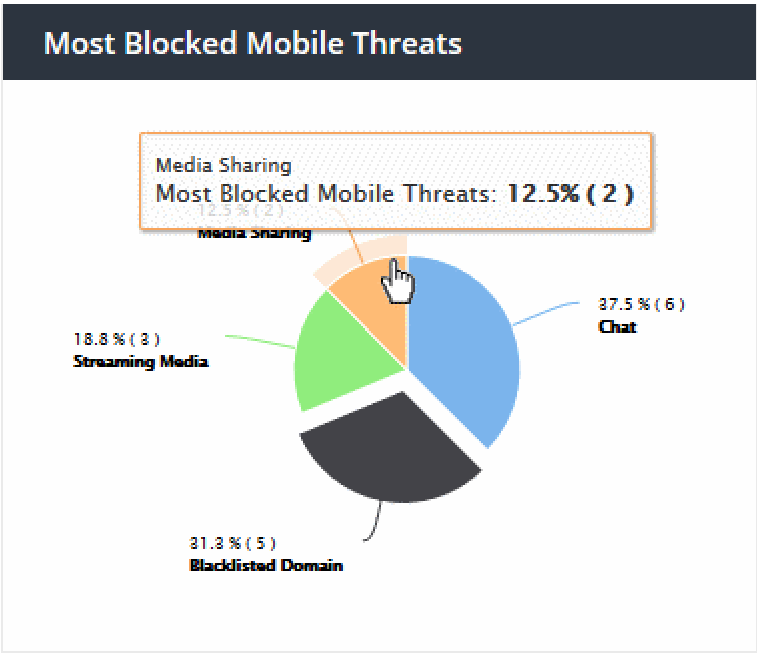
Overall Security Incidents
Click and drag in the plot area to zoom in
10
8
6
2
0
Thursday, Aug 3, 14:30
● Overall Security Incidents: 3
4. Aug
6. Aug

- 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.

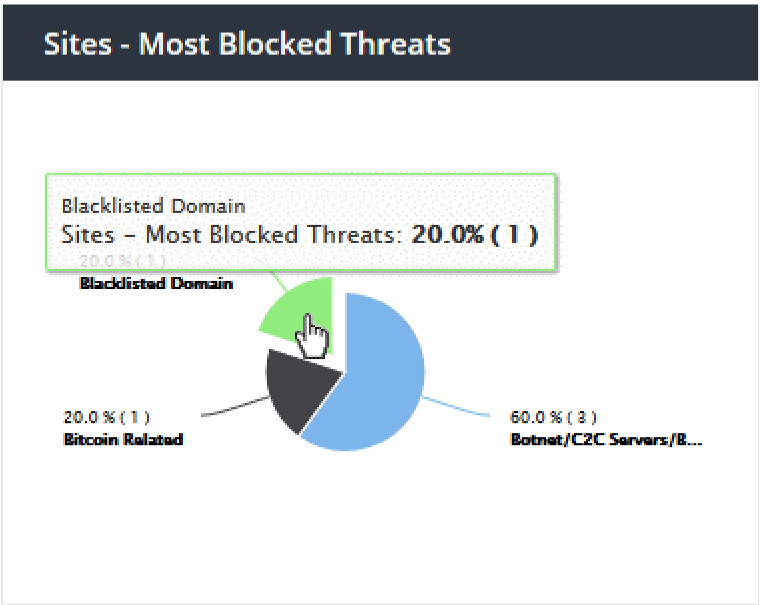


- Click on a sector to see a log of most blocked categories for mobile users. See 'View Logs' for more on this.

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.



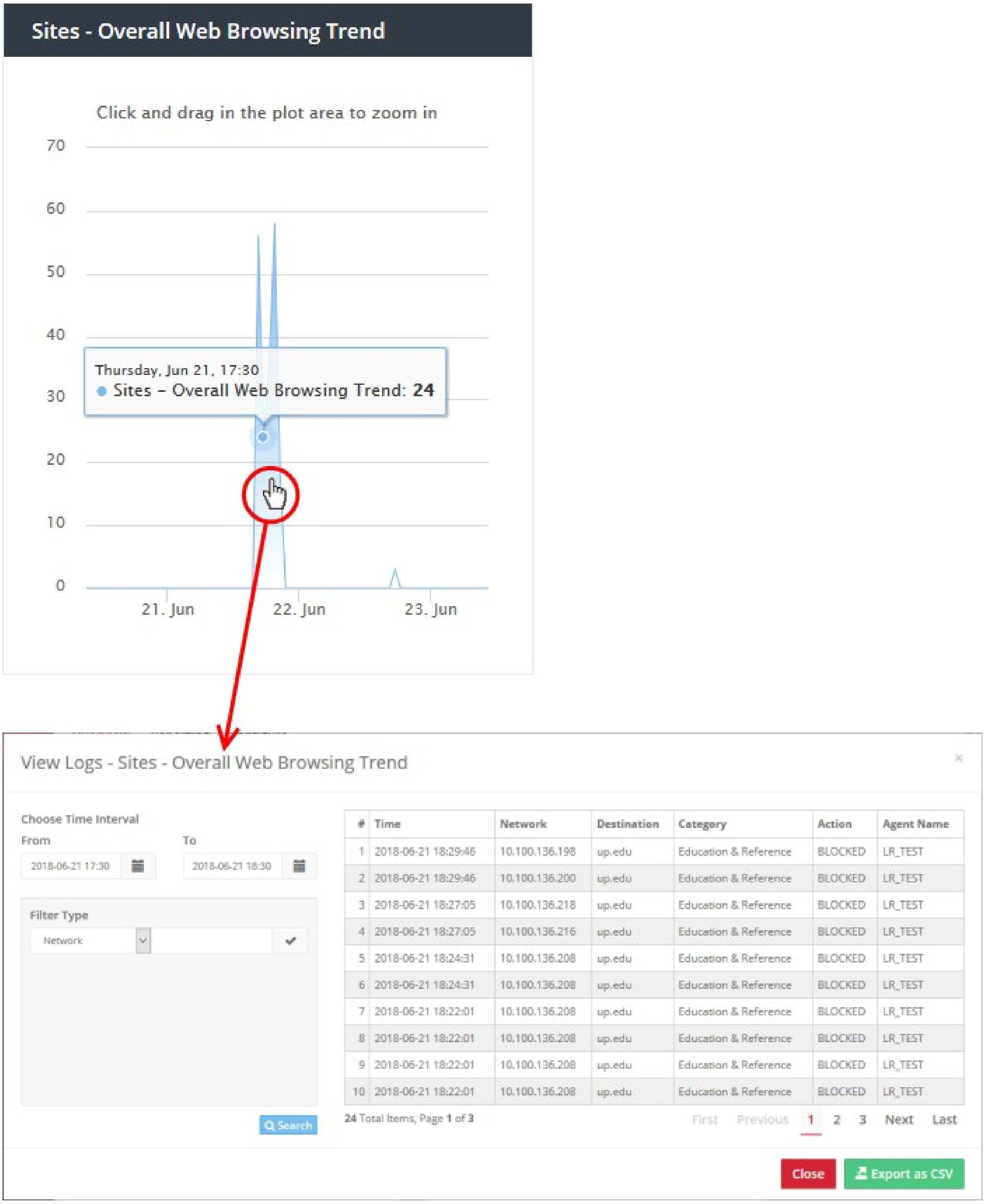
- Click on a sector to see a log of most blocked categories for mobile users. See 'View Logs' for more on this.

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:


Sites - Overall Web Browsing Trend
Click and drag in the plot area to zoom in
70
60
50
40
30
20
10
0
21. Jun
22. Jun
23. Jun
Thursday, Jun 21, 17:30
Sites – Overall Web Browsing Trend: 24

View Logs - Sites - Overall Web Browsing Trend

Choose Time Interval

From: 2018-06-21 17:30

To: 2018-06-21 18:30

Filter Type: Network

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

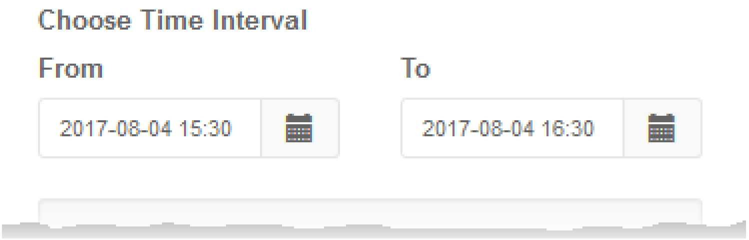
24 Total Items, Page 1 of 3

- 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

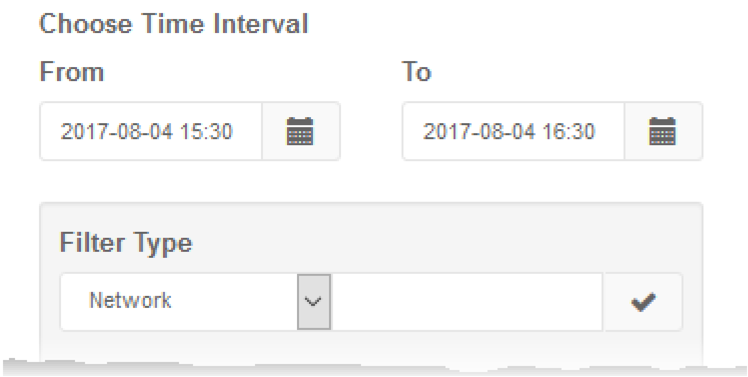
From: 2017-08-04 15:30

To: 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.

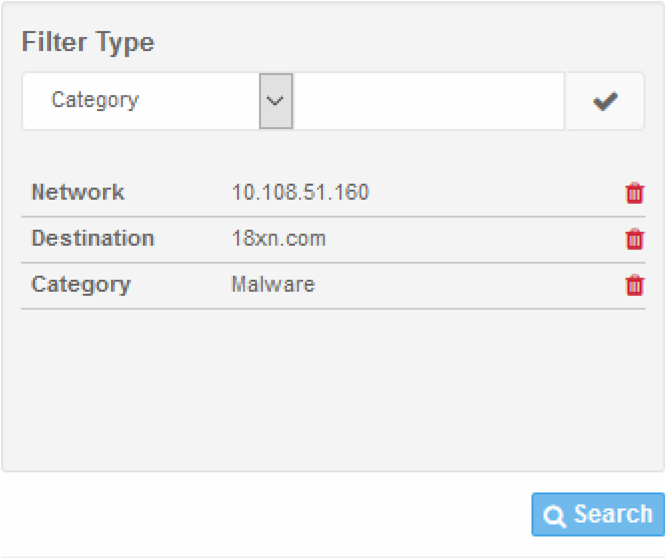

Choose Time Interval

From: 2017-08-04 15:30

To: 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

  - 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.

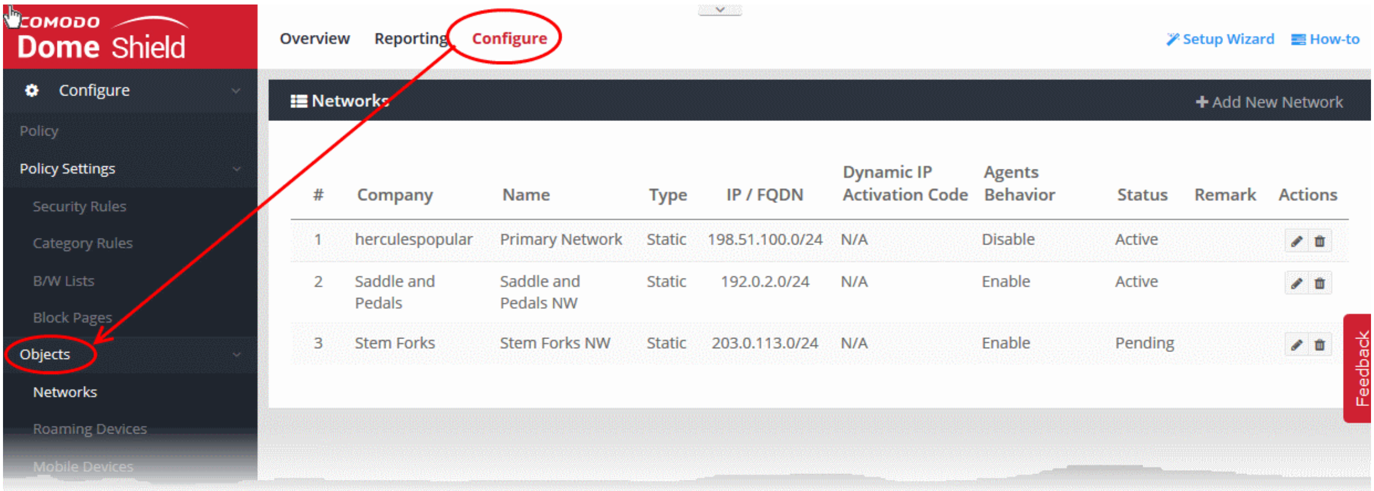
The following types of logs are available:

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** Roaming Agent Security Incidents	• 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.

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:



#	Company	Name	Type	IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
1	herculespopular	Primary Network	Static	198.51.100.0/24	N/A	Disable	Active		
2	Saddle and Pedals	Saddle and Pedals NW	Static	192.0.2.0/24	N/A	Enable	Active		
3	Stem Forks	Stem Forks NW	Static	203.0.113.0/24	N/A	Enable	Pending		

- **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.

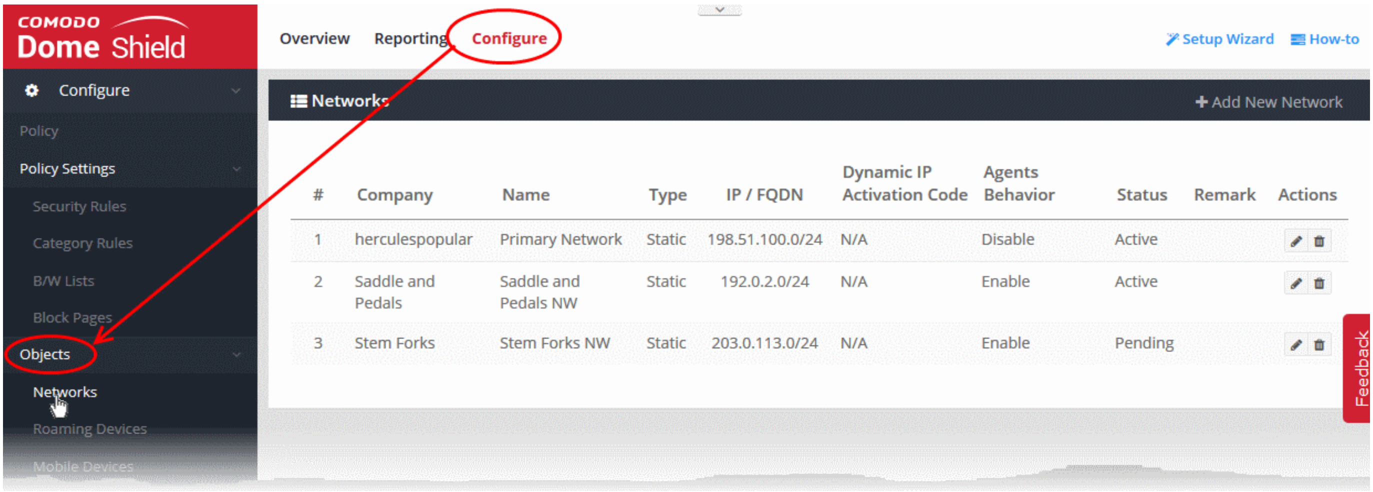
See **Setup Options Explained** for an overview of choices to add networks.

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 will have been automatically added during enrollment. The network will be active immediately.
- 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. Comodo provides an IP updater agent which will keep Dome Shield and your policies updated with the address of dynamic networks. 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)



#	Company	Name	Type	IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
1	herculespopular	Primary Network	Static	198.51.100.0/24	N/A	Disable	Active		
2	Saddle and Pedals	Saddle and Pedals NW	Static	192.0.2.0/24	N/A	Enable	Active		
3	Stem Forks	Stem Forks NW	Static	203.0.113.0/24	N/A	Enable	Pending		

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	Allows to update or delete a network.

The interface allows you to:

- Add new networks
- Edit the details of a network
- Delete a network

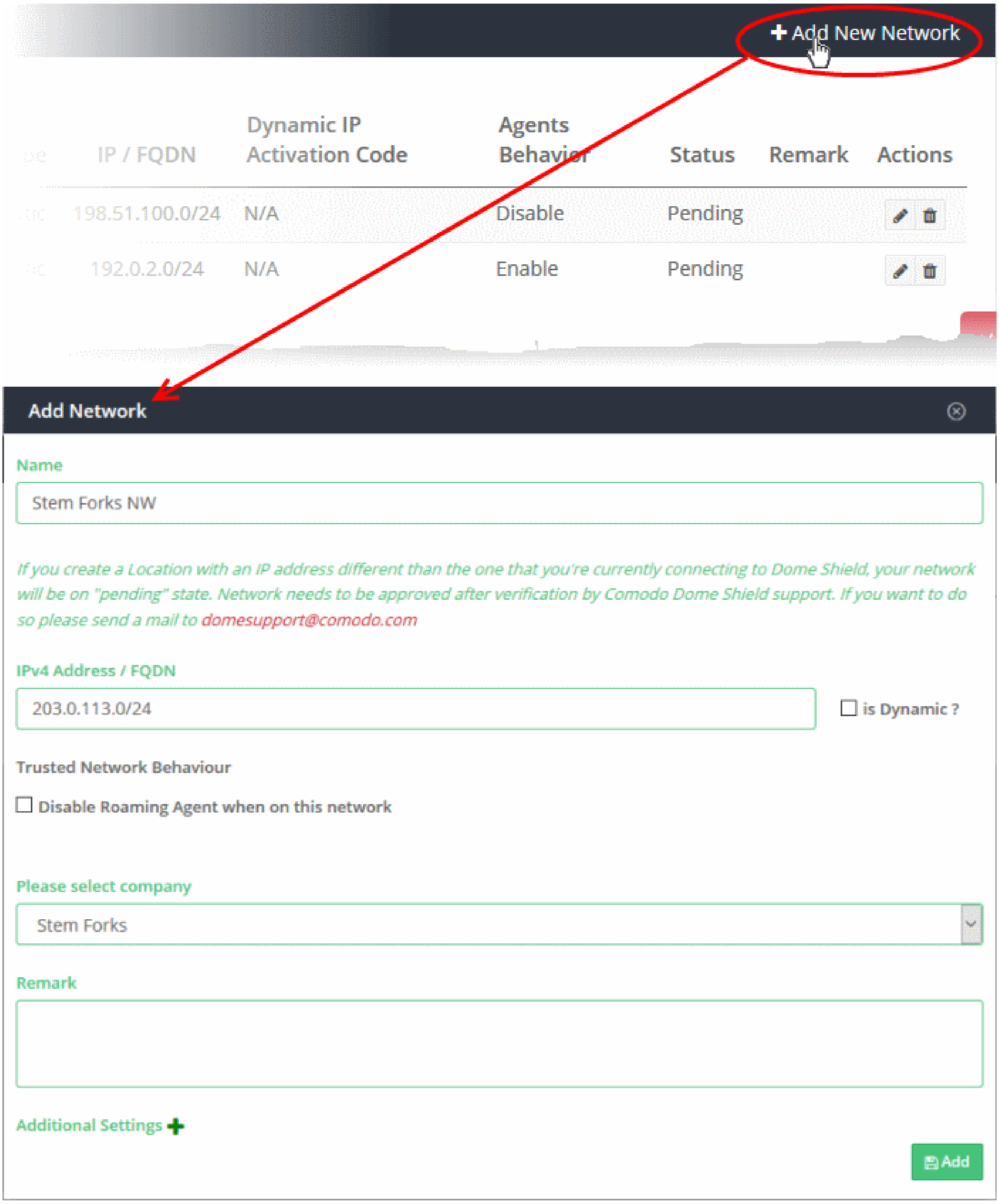
Add New Networks

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':



IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
198.51.100.0/24	N/A	Disable	Pending		
192.0.2.0/24	N/A	Enable	Pending		

Add Network

Name

Stem Forks NW

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

IPv4 Address / FQDN

203.0.113.0/24

□ is Dynamic ?

Trusted Network Behaviour

□ Disable Roaming Agent when on this network

Please select company

Stem Forks

Remark

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.

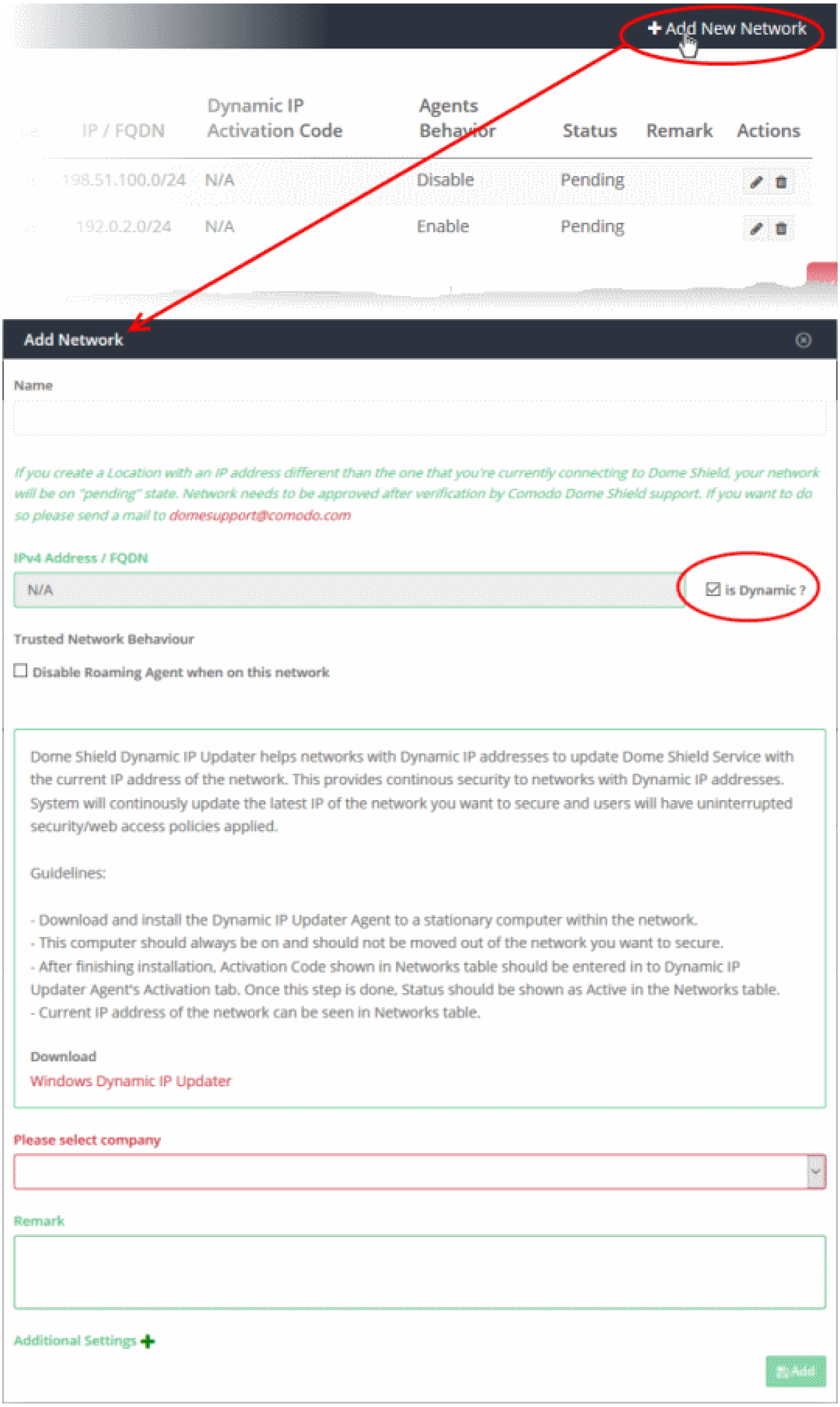
Add Networks with Dynamic IP Address(es)

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':



IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
198.51.100.0/24	N/A	Disable	Pending		
192.0.2.0/24	N/A	Enable	Pending		

Add Network

Name

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

IPv4 Address / FQDN

N/A

☑ is Dynamic ?

Trusted Network Behaviour

□ Disable Roaming Agent when on this network

Dome Shield Dynamic IP Updater helps networks with Dynamic IP addresses to update Dome Shield Service with the current IP address of the network. This provides continous security to networks with Dynamic IP addresses. System will continously update the latest IP of the network you want to secure and users will have uninterrupted security/web access policies applied.

Guidelines:

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

Download

Windows Dynamic IP Updater

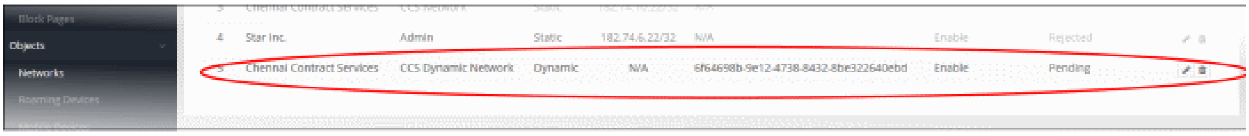
Please select company

Remark

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.



4	Star Inc.	Admin	Static	182.74.6.22/32	N/A	Enable	Rejected
5	Chennai Contract Services	CCS Dynamic Network	Dynamic	N/A	6f64698b-9e12-4738-8432-8be322640ebd	Enable	Pending

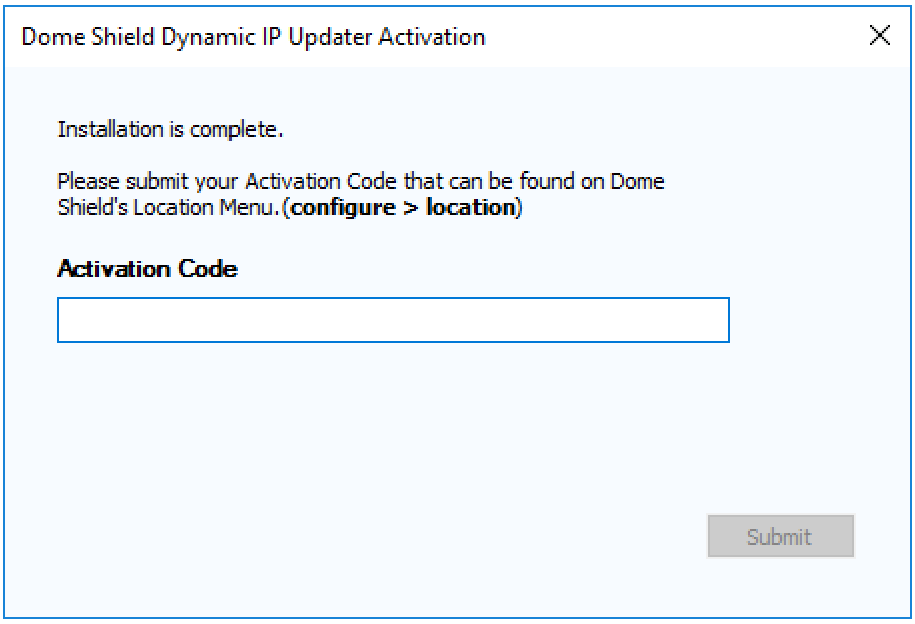
- Transfer the agent setup files to an endpoint in the target network

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:



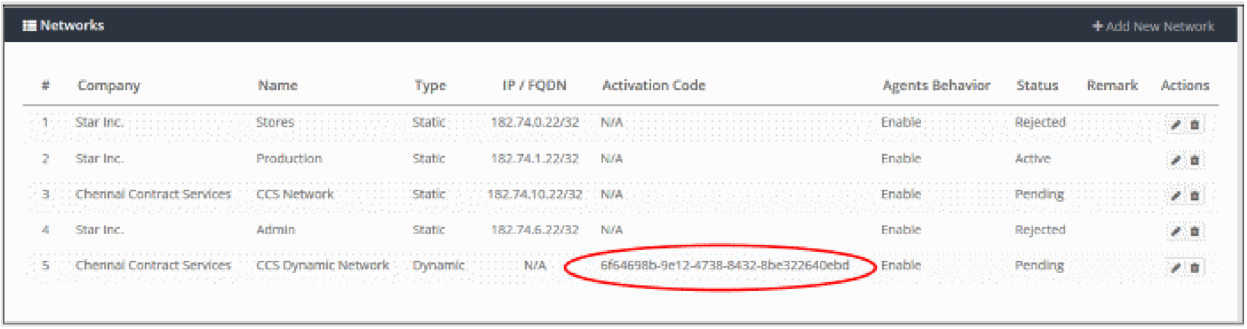
Dome Shield Dynamic IP Updater Activation

Installation is complete.

Please submit your Activation Code that can be found on Dome Shield's Location Menu.(**configure > location**)

Activation Code

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



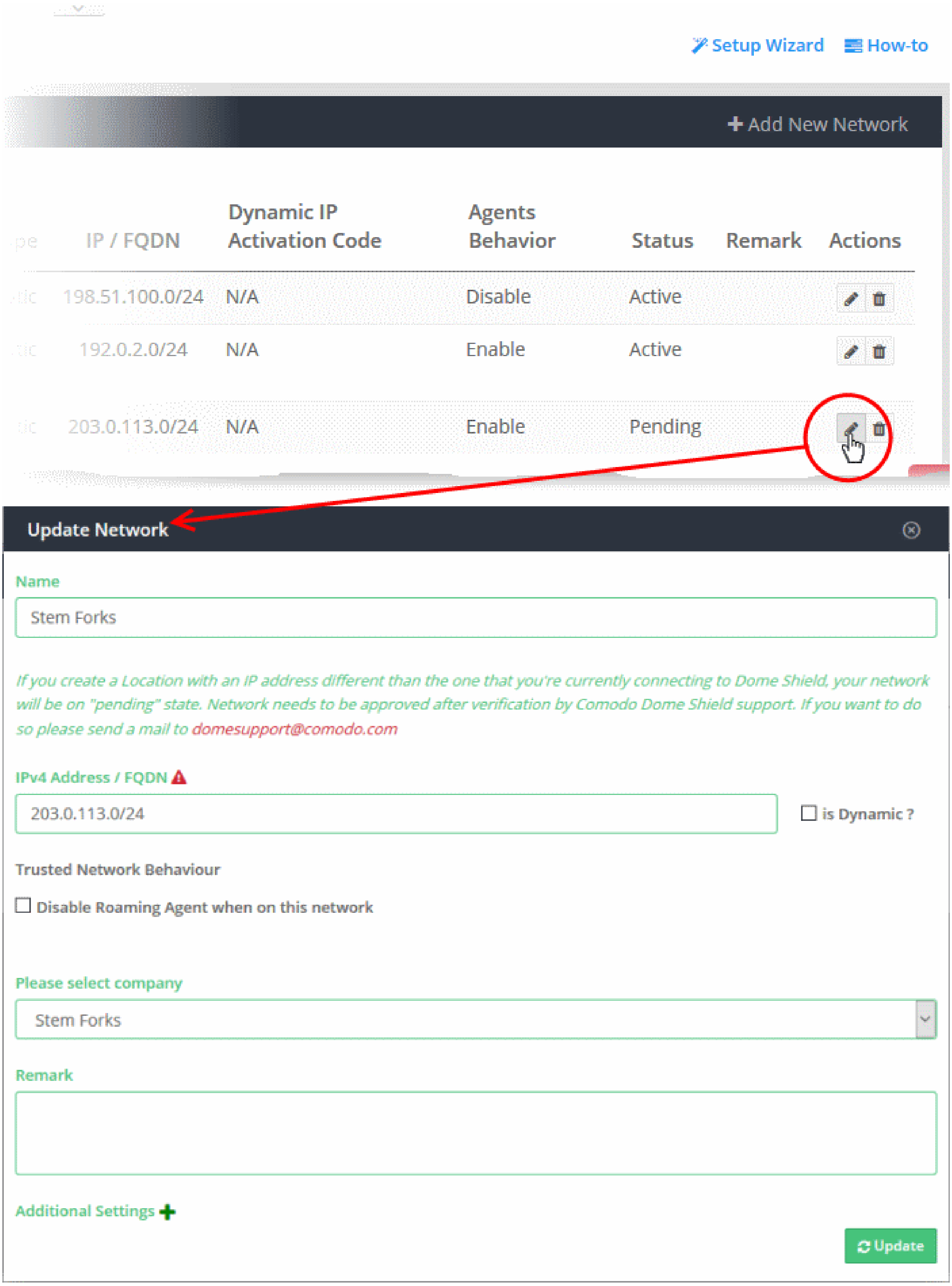
#	Company	Name	Type	IP / FQDN	Activation Code	Agents Behavior	Status	Remark	Actions
1	Star Inc.	Stores	Static	182.74.0.22/32	N/A	Enable	Rejected		
2	Star Inc.	Production	Static	182.74.1.22/32	N/A	Enable	Active		
3	Chennai Contract Services	CCS Network	Static	182.74.10.22/32	N/A	Enable	Pending		
4	Star Inc.	Admin	Static	182.74.6.22/32	N/A	Enable	Rejected		
5	Chennai Contract Services	CCS Dynamic Network	Dynamic	N/A	6f64698b-9e12-4738-8432-8be322640ebd	Enable	Pending		

- 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.



pe	IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
tic	198.51.100.0/24	N/A	Disable	Active		
tic	192.0.2.0/24	N/A	Enable	Active		
tic	203.0.113.0/24	N/A	Enable	Pending		

Update Network

Name

Stem Forks

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

IPv4 Address / FQDN

203.0.113.0/24

□ is Dynamic ?

Trusted Network Behaviour

□ Disable Roaming Agent when on this network

Please select company

Stem Forks

Remark

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

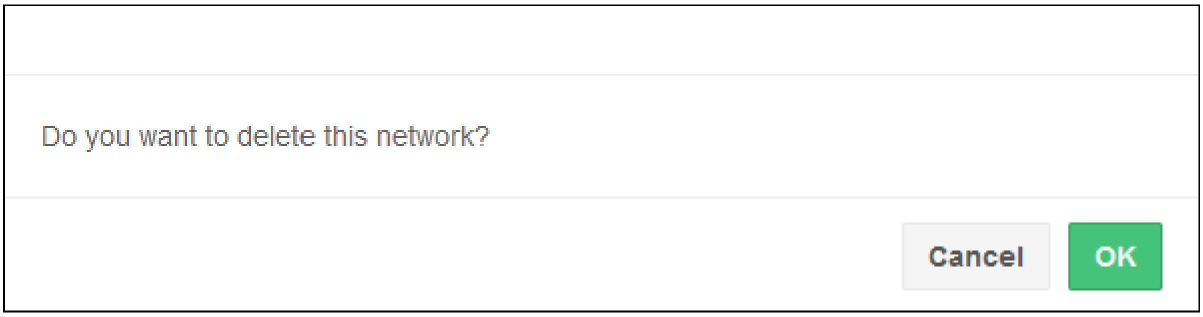
- Click the 'Update' button

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.



Do you want to delete this network?

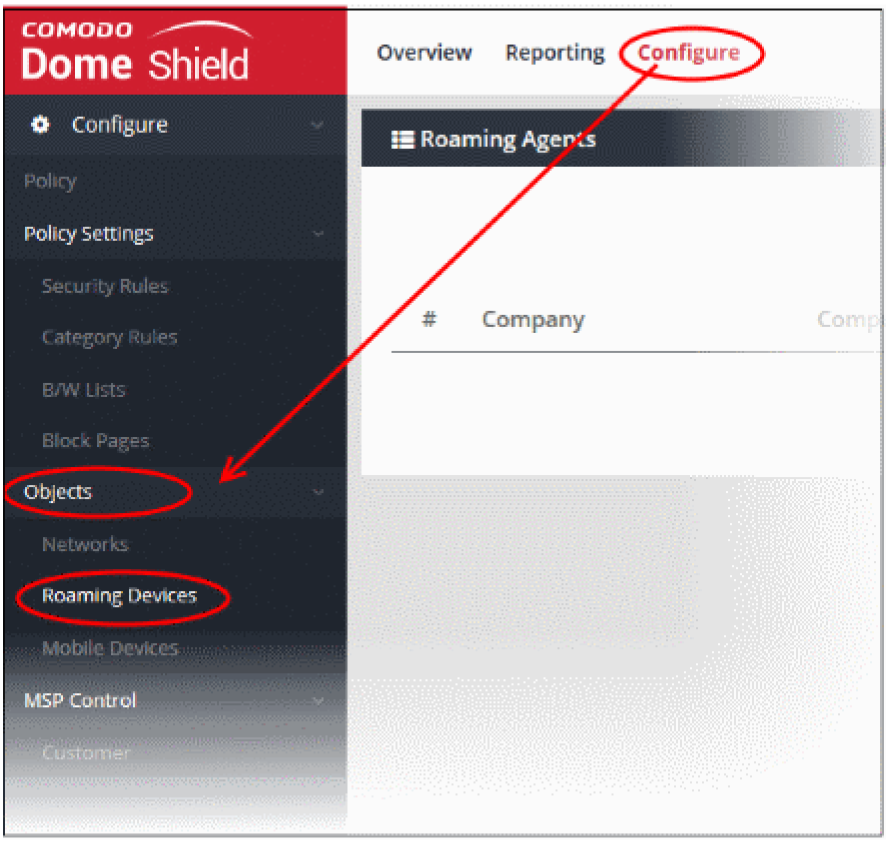
- Click 'OK' to confirm removal of the network from the list.

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 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.
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)

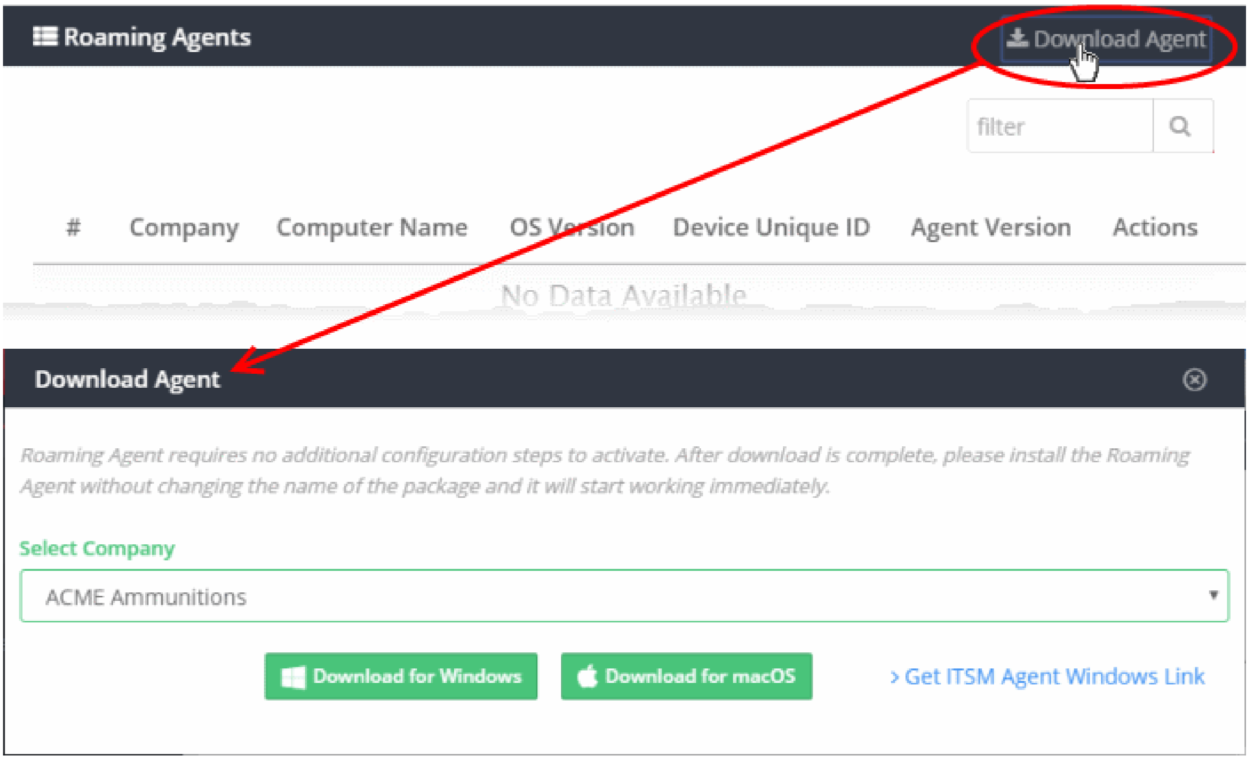
- Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'

You can enroll roaming devices in two ways:

- Import Windows devices from ITSM - If you use ITSM , you can remotely install the Dome Shield agent on managed Windows endpoints from the ITSM console. The agent installation package is available in the 'Download Agent' interface.
- 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.

To add new devices

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' on the top right.


Roaming Agents
Download Agent
filter
# Company Computer Name OS Version Device Unique ID Agent Version Actions
No Data Available

Download Agent

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

Select Company

ACME Ammunitions

Download for Windows
Download for macOS
> Get ITSM Agent Windows Link

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 ITSM Agent Windows Link** - Displays the agent download link for remotely installing the agent on Windows endpoints through ITSM. See Import Windows Devices from ITSM for more details.

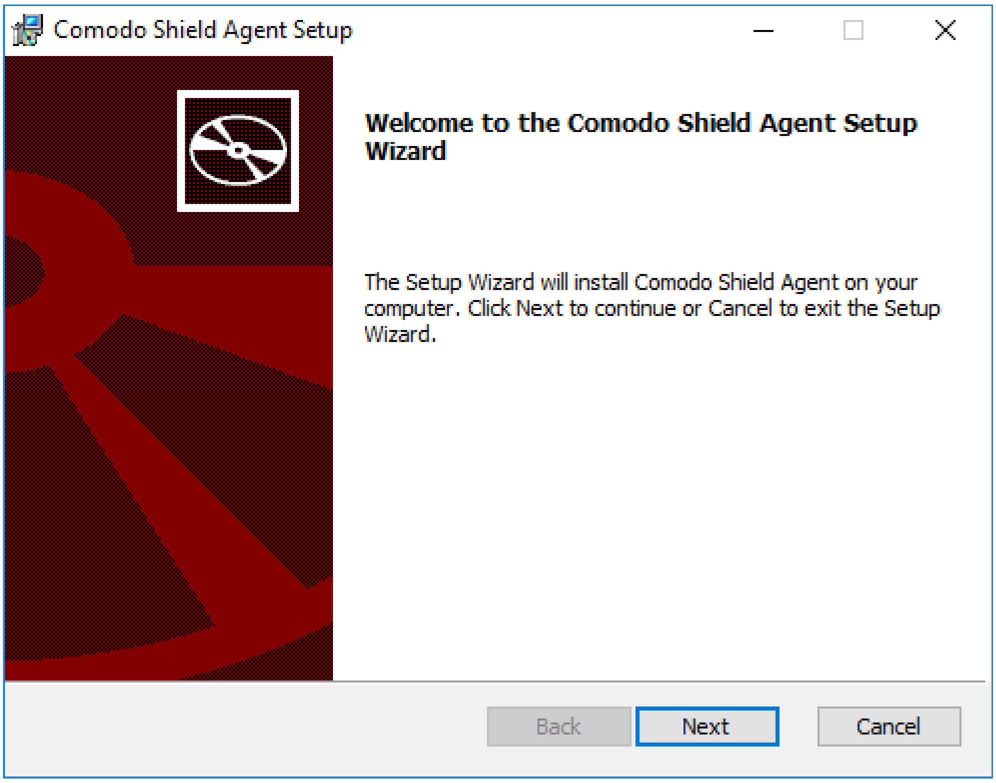
Enroll Windows devices

- 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.

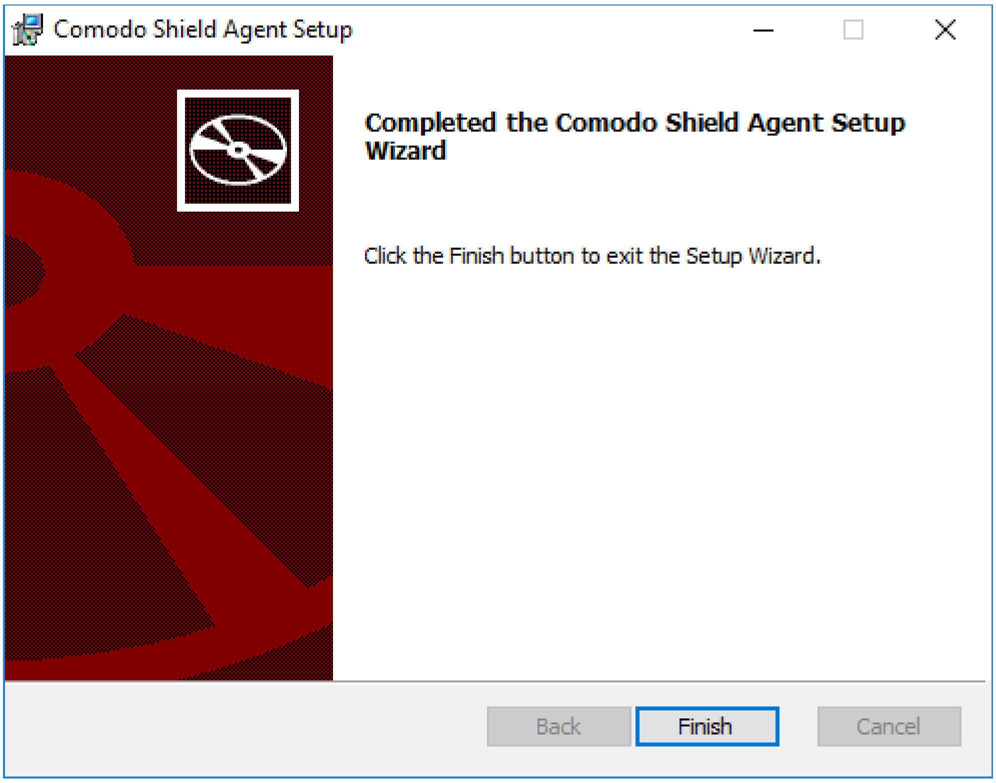
The installation wizard will start.


Comodo Shield Agent Setup

Welcome to the Comodo Shield Agent Setup Wizard

The Setup Wizard will install Comodo Shield Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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


Comodo Shield Agent Setup

Completed the Comodo Shield Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

- Click 'Finish'

That's it. The device will be added and will be displayed in the 'Configure' > 'Objects' > 'Roaming Devices' interface.

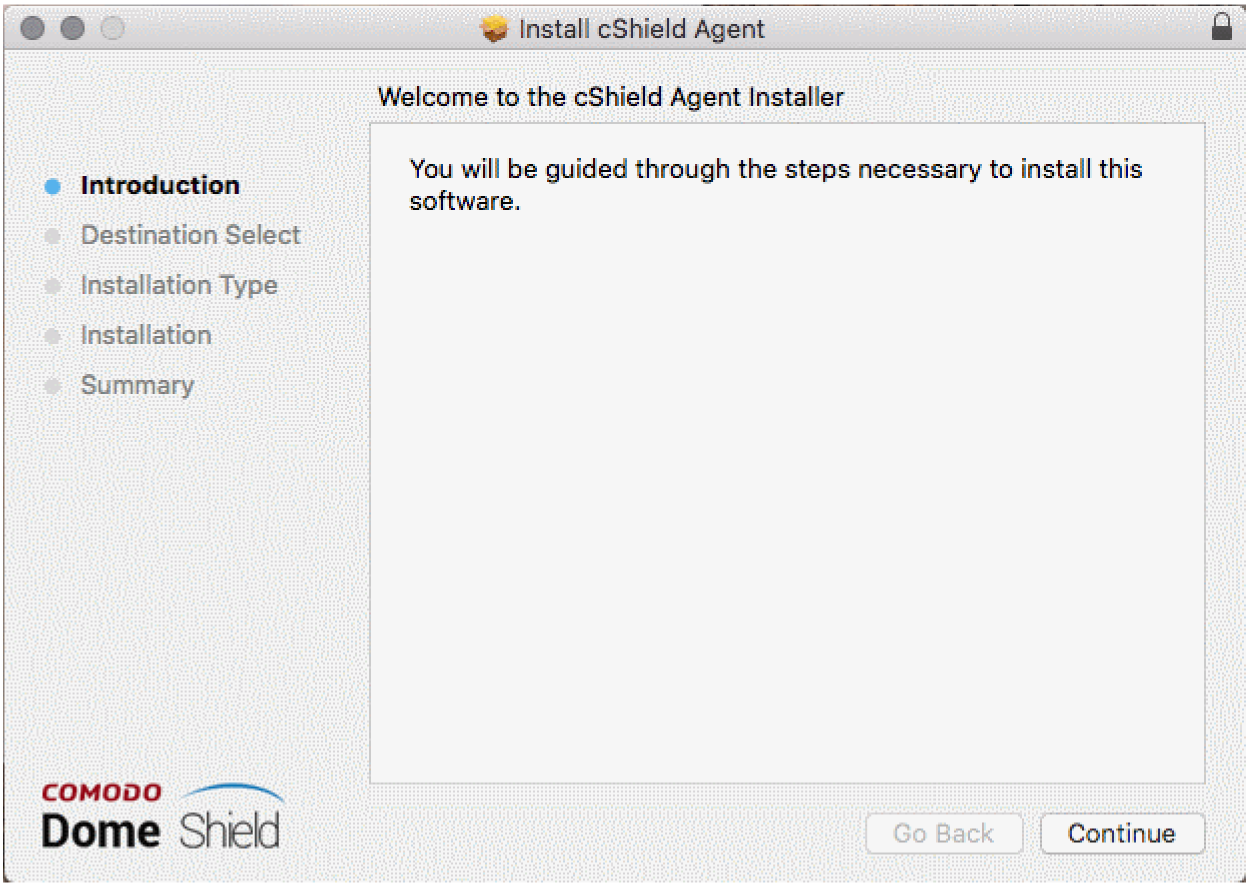
- Note - no security rules are applied to roaming device by default. You can create and apply device specific policies according to your requirements.
- See 'Apply Policies to Networks, Roaming and Mobile Devices' for advice on how to configure and deploy security policies to roaming devices.

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.



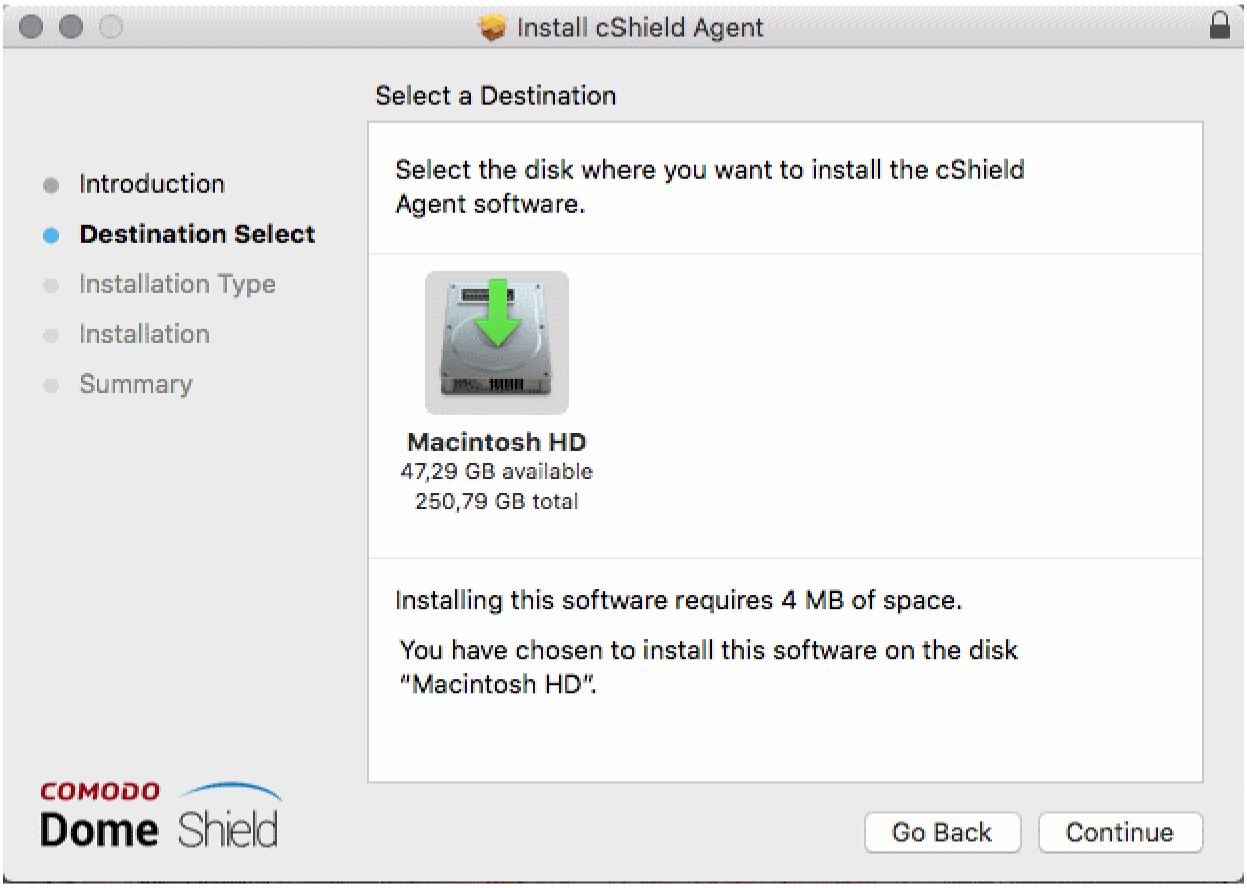
Install cShield Agent

Welcome to the cShield Agent Installer

You will be guided through the steps necessary to install this software.

- Click 'Continue'

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



Select a Destination

Select the disk where you want to install the cShield Agent software.

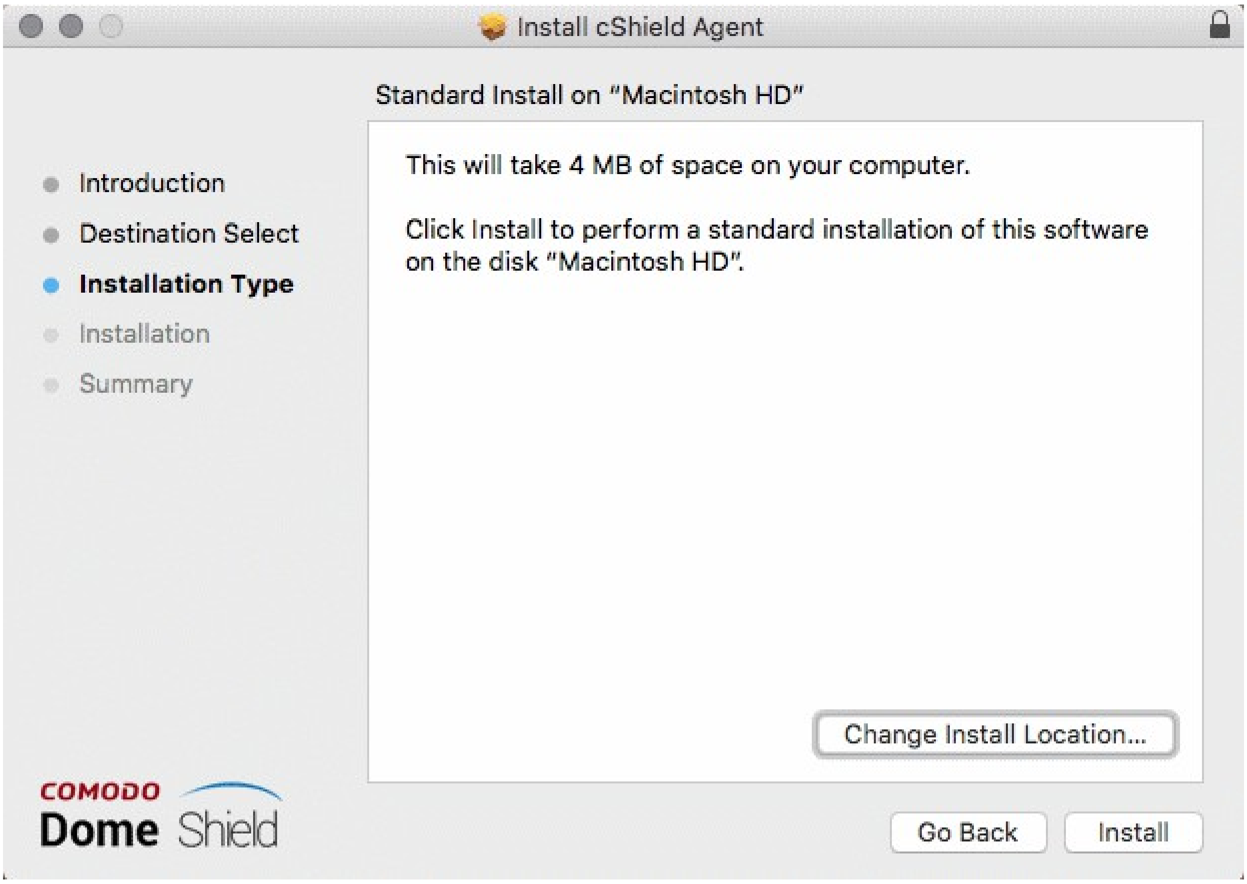
Macintosh HD
47,29 GB available
250,79 GB total

Installing this software requires 4 MB of space.

You have chosen to install this software on the disk "Macintosh HD".

- 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.



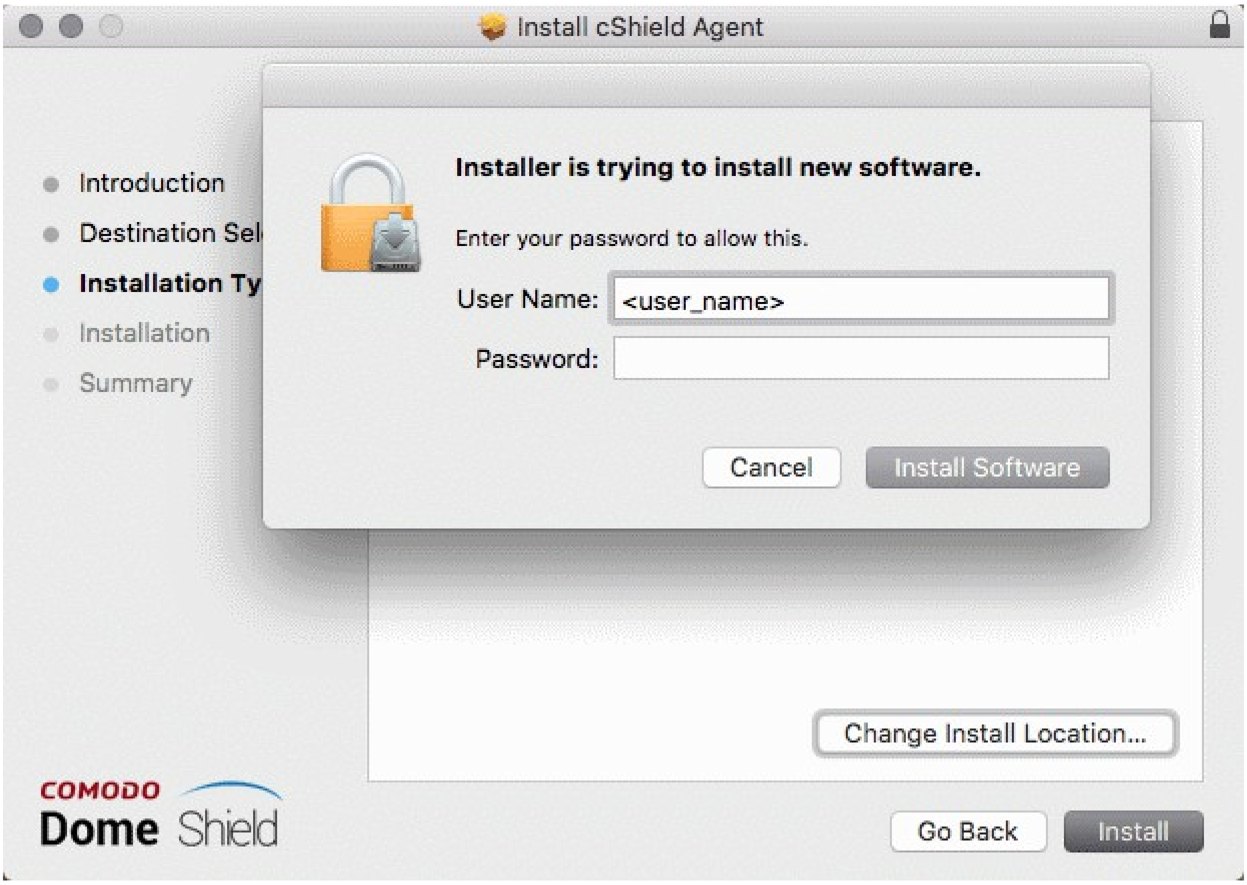
Standard Install on "Macintosh HD"

This will take 4 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

- Click 'Install'

The installation requires your user account to continue.



Install cShield Agent

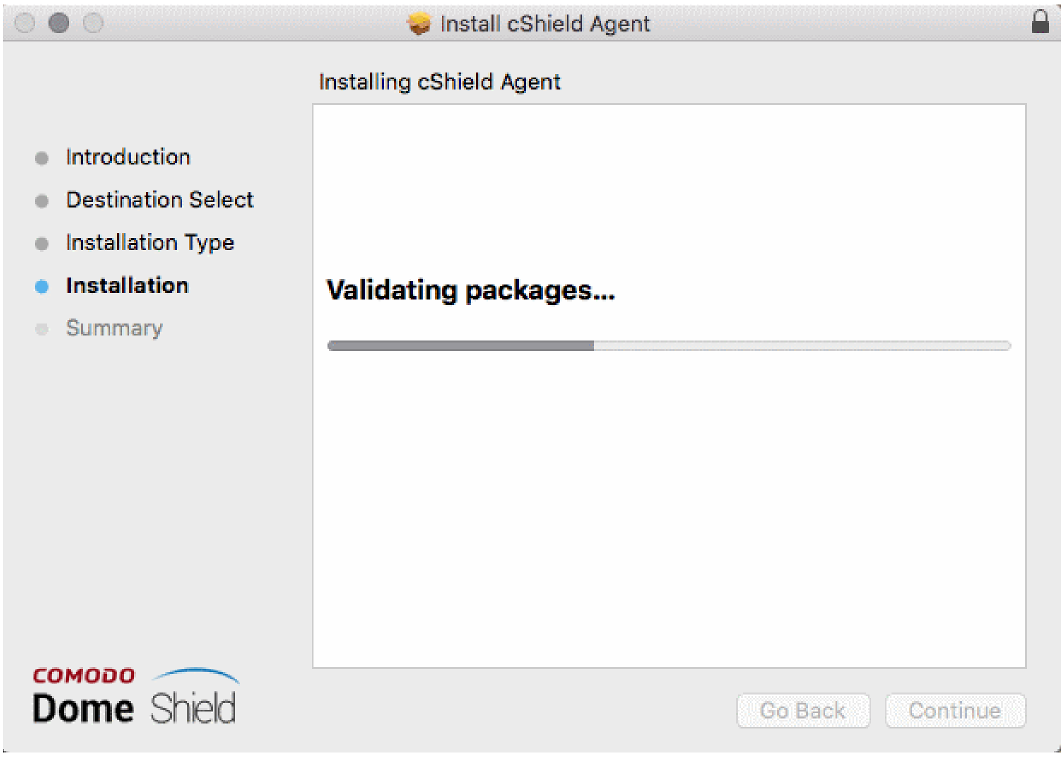
Installer is trying to install new software.

Enter your password to allow this.

User Name: <user_name>

Password:

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

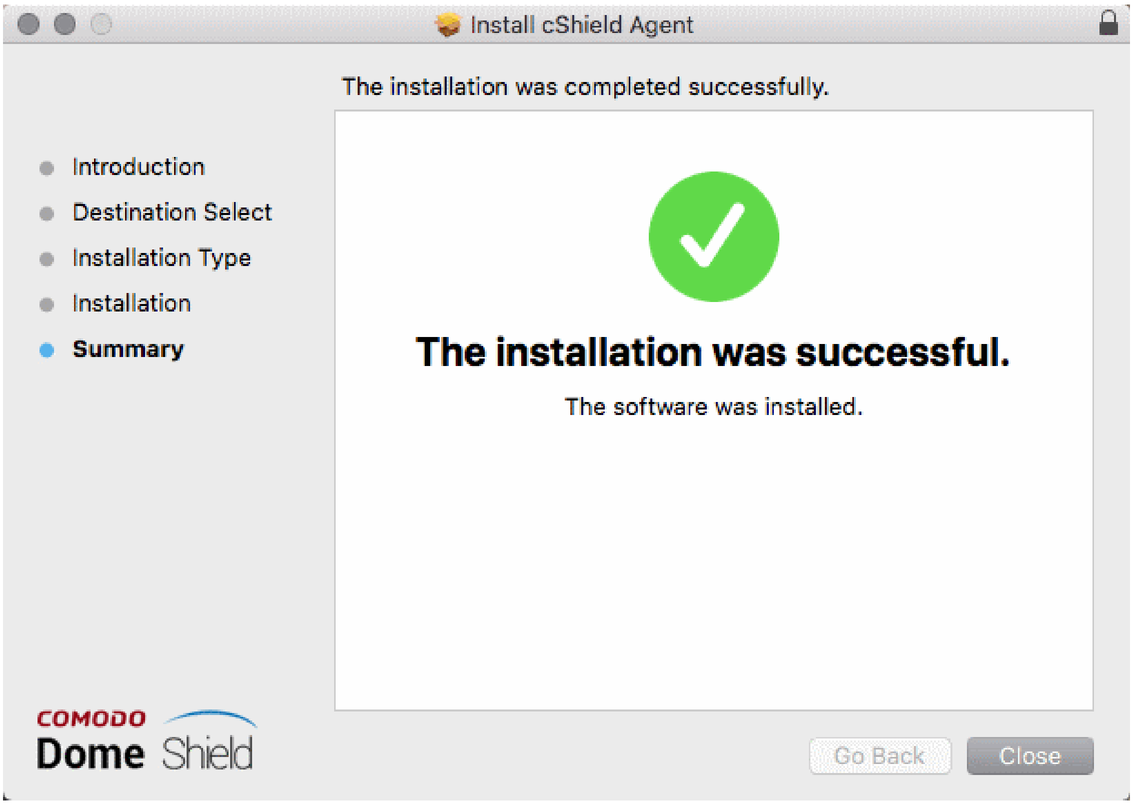


Install cShield Agent

Installing cShield Agent

Validating packages...

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

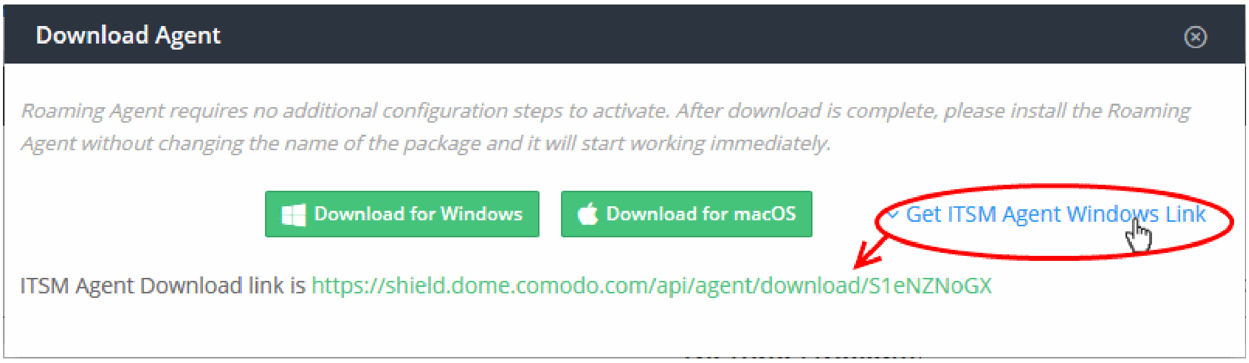


Once installed, the agent will start communicating with the Dome Shield server. The device will be visible in 'Configure' > 'Objects' > 'Roaming Devices'.

- 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 ITSM

- Click 'Get ITSM Agent Windows Link':



Download Agent

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

ITSM Agent Download link is https://shield.dome.comodo.com/api/agent/download/S1eNZNoGX

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

Process in brief:

- Login to ITSM
- Click 'Devices' > 'Device List' > 'Device Management' tab
- Select the Windows device(s) on which you want install the packages

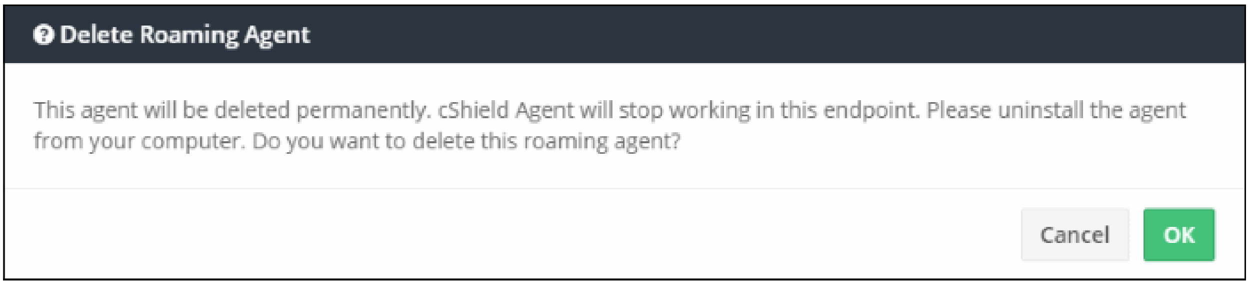
  - Click 'Install or Update Packages' and select 'Install Custom MSI/Packages'
  - Paste the agent download link into the 'MSI/Package URL' field
  - Configure the other remote installation options as required
  - Click 'Install'
- See https://help.comodo.com/topic-399-1-786-10139-Remotely-Install-and-Update-Packages-on-Windows-Devices.html if you need additional help to install packages via ITSM.

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.



Delete Roaming Agent

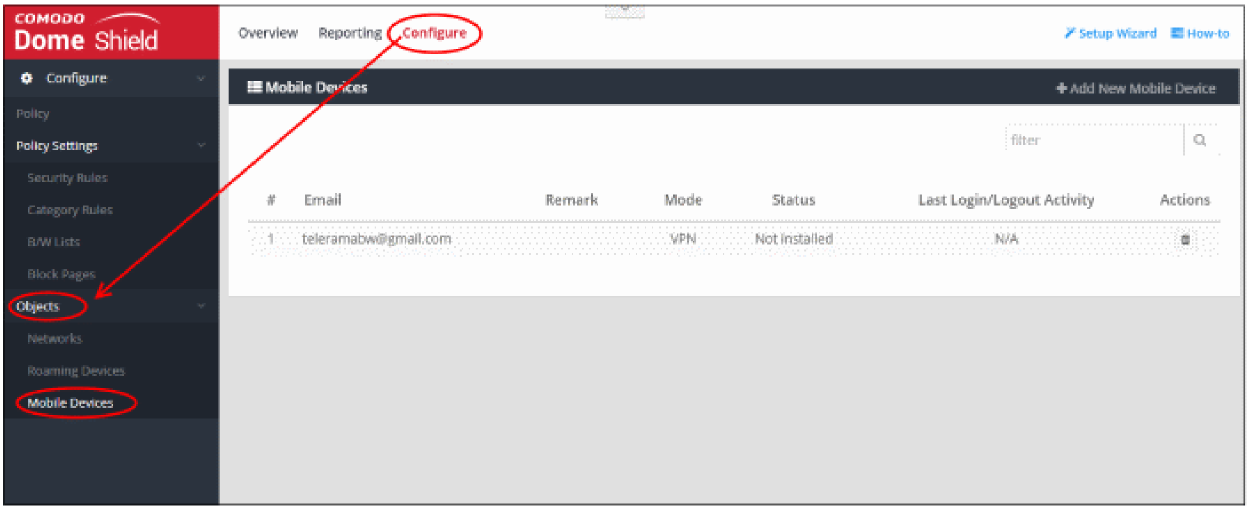
This agent will be deleted permanently. cShield Agent will stop working in this endpoint. Please uninstall the agent from your computer. Do you want to delete this roaming agent?

- Click 'OK' to confirm device removal

4.3 Add Mobile Devices to Dome Shield

Dome Shield provides web protection to mobile devices in addition to network endpoints and roaming devices.

- Dome Shield can protect all iOS and Android based devices using its VPN service.
- You need to install the VPN profile or the Dome mobile app on each mobile device to enable protection.
  - VPN Profile - Requires a third-party VPN client to be installed on the device. Currently Dome Shield supports only StrongSwan VPN tool.
  - Dome Shield App - This comes bundled with VPN client and profile. No need to install any third-party VPN app. Just download the Shield app and install on devices.
- Please note you should use different email addresses for each device to download the profile / mobile app. The same email should not be used on different devices to download the profile / mobile app.
- Supported versions: Android - 4.4 and above; iOS - 9 and above.
- Once installed, you can deploy polices to mobile devices as required.
- Click 'Configure' > 'Objects' > 'Mobile Devices' to view all enrolled mobile devices:



#	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	teleramabw@gmail.com		VPN	Not Installed	N/A	🗑

Mobile Devices - Table of Column Descriptions	
Column Header	**Description**
Company	Applies to MSPs only. The name of the company to which the mobile device is enrolled.
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	Indicates the status 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	Provides the user login details including date and time. • Login - Indicates the device is connected to Shield • Logout - Indicates the device is disconnected from Shield.
Actions	Controls for removing endpoints

Search and Filtering options:

- Enter the company name, email, status, last login\logout activity in part or full in the search box at top-right. Results matching the entered parameters will be automatically displayed.

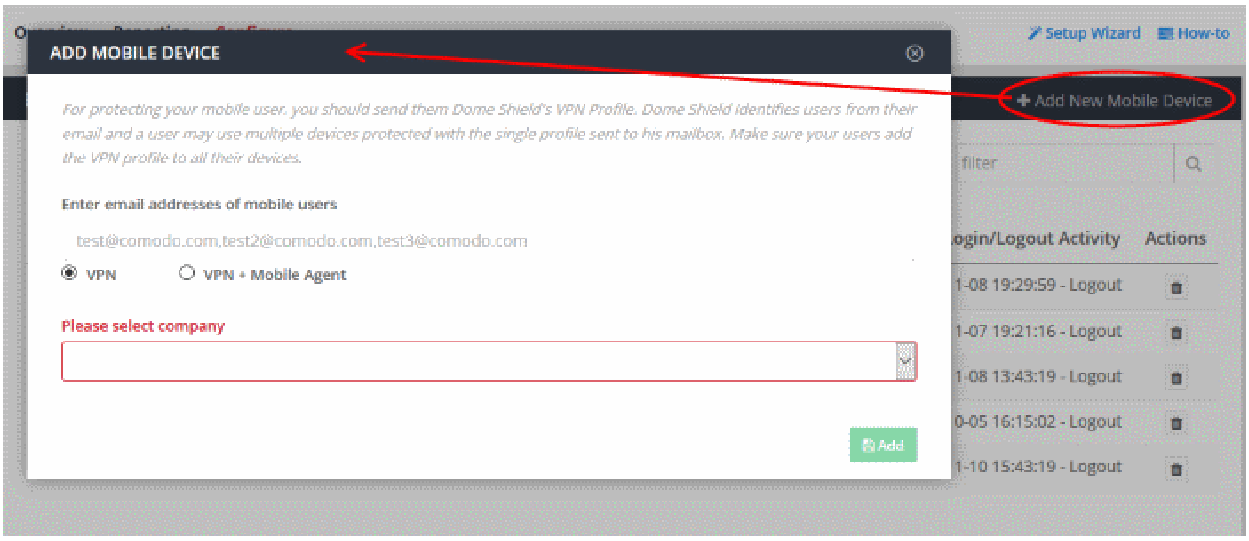
The interface allows you to:

- Add a new mobile device
- Delete a device

Adding a mobile device

- Click 'Configure' > 'Objects' > 'Mobile Devices'
- Click 'Add New Mobile Device' at top-right

The 'Add Mobile Device' form will be displayed.



ADD MOBILE DEVICE

For protecting your mobile user, you should send them Dome Shield's VPN Profile. Dome Shield identifies users from their email and a user may use multiple devices protected with the single profile sent to his mailbox. Make sure your users add the VPN profile to all their devices.

Enter email addresses of mobile users

test@comodo.com,test2@comodo.com,test3@comodo.com

● VPN ○ VPN + Mobile Agent

Please select company

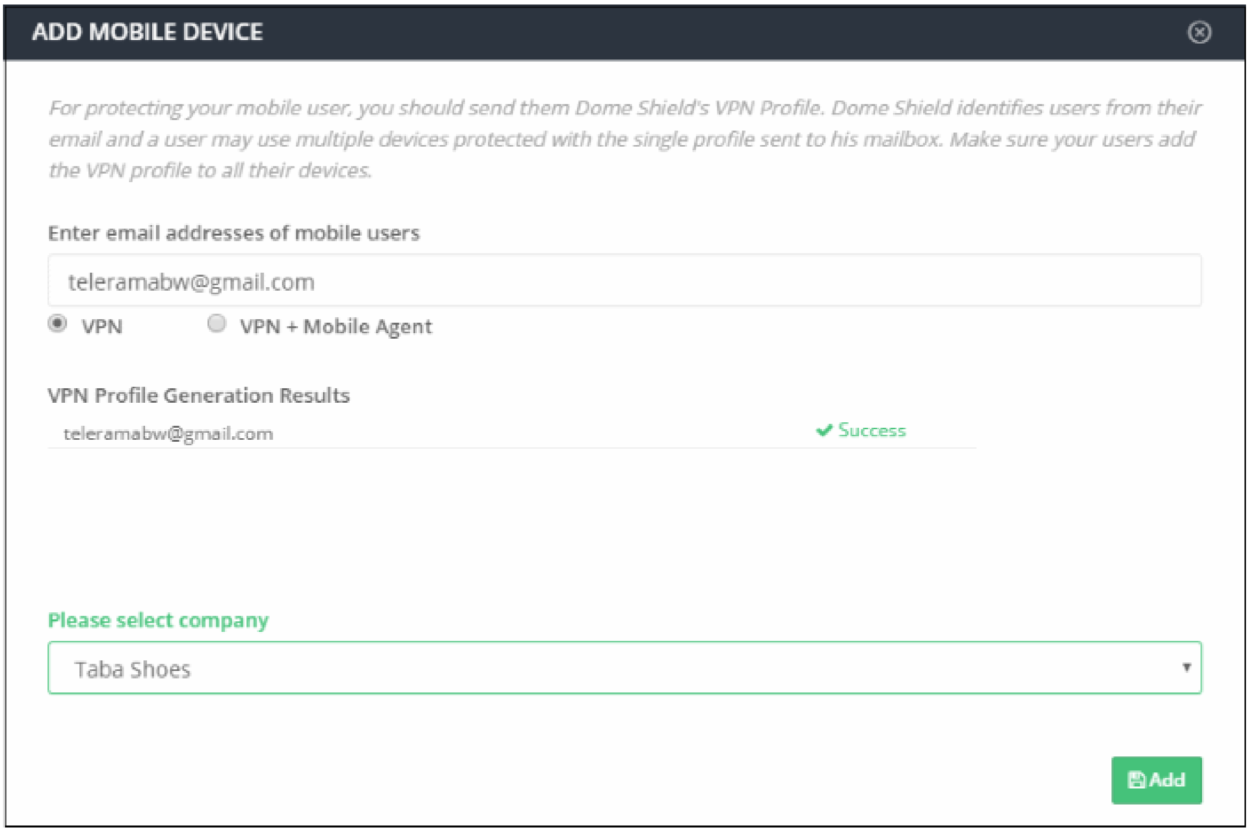
Add

- Enter email addresses of mobile users - Provide the email address of the mobile users. You can enter multiple addresses. Please note that each device requires a unique email address. The same email address cannot used on different devices to download the profile / mobile app.
- VPN and VPN + Mobile Agent (aka Shield mobile app) option:
  - VPN - If you select this, the user has to install a third party VPN client on the device (currently Shield supports only StrongSwan app). Installation of the third party VPN applies to Android devices and is not required for iOS devices. Click here to see instructions for this option.
  - VPN + Mobile Agent - If you select this, the user need not install any third party VPN client. 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'

The enrollment instructions email will be sent to the users and a confirmation message will be displayed:



ADD MOBILE DEVICE

For protecting your mobile user, you should send them Dome Shield's VPN Profile. Dome Shield identifies users from their email and a user may use multiple devices protected with the single profile sent to his mailbox. Make sure your users add the VPN profile to all their devices.

Enter email addresses of mobile users: teleramabw@gmail.com

● VPN ○ VPN + Mobile Agent

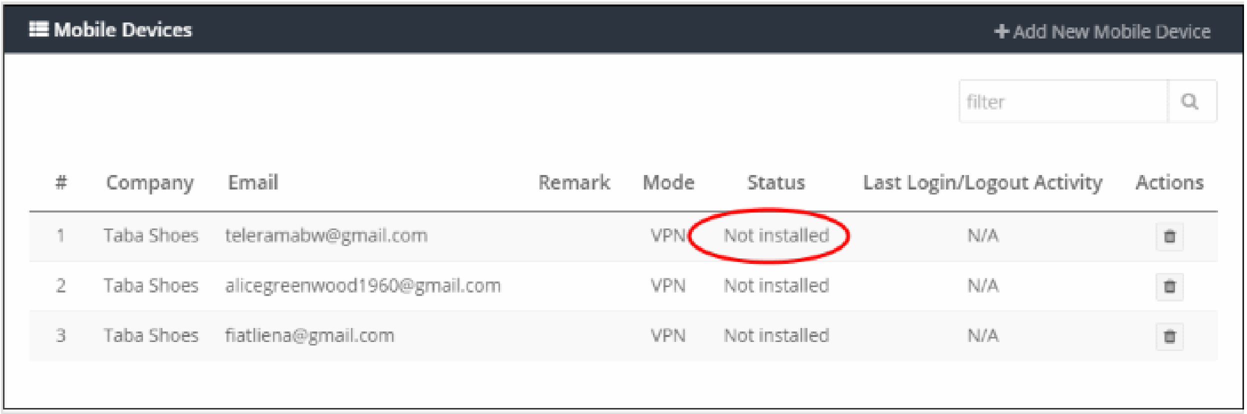
VPN Profile Generation Results

teleramabw@gmail.com	✓ Success

Please select company: Taba Shoes

- Click to close the dialog.

The user will be added to the list but the status will show as 'Not installed'



Mobile Devices

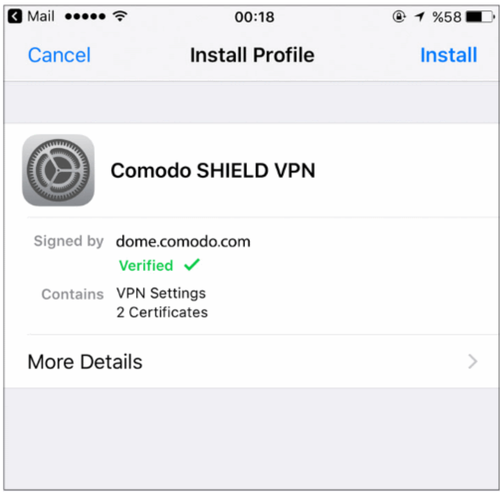
#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	Taba Shoes	teleramabw@gmail.com		VPN	Not installed	N/A	🗑
2	Taba Shoes	alicegreenwood1960@gmail.com		VPN	Not installed	N/A	🗑
3	Taba Shoes	fiatliena@gmail.com		VPN	Not installed	N/A	🗑

The user should open the email on the device. In addition to enrollment advice, the email will also include three attachments:

- iOS_VPN_Profile.mobileconfig
- Android_VPN_Profile.sswan
- Android SSLCert.pem

Instructions for iOS

- Tap the attachment 'iOS_VPN_Profile' in the mail
- Install the profile as shown below:



Mail ●●●●● 00:18 %58

Cancel Install Profile Install

Comodo SHIELD VPN

Signed by dome.comodo.com

Verified ✓

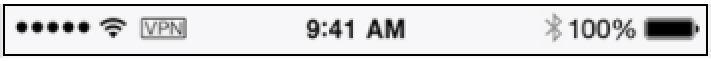
Contains VPN Settings
2 Certificates

More Details

That's it. The VPN profile is installed on the iOS device.

- Note: In order to view HTTPS website, go to Settings > General > About > Certificate Trust Settings and Enable Full Trust for Root Certificates.

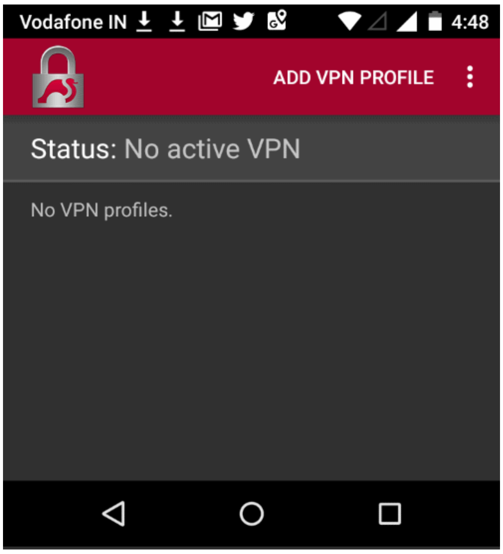
Once connected, the VPN icon will be available on the navigation bar.



If you need to turn off the VPN temporarily, for example authenticating with Wi-Fi hotspots, go to VPN Settings on the device and disable the connection.

Instructions for Android

- Open the enrollment mail and tap the attachment 'Android_VPN_Profile' and download
- Open your VPN App (currently Shield supports only StrongSwan app)



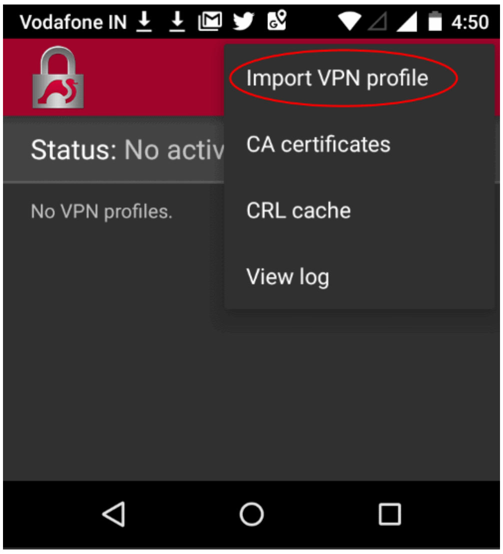
Vodafone IN 4:48

ADD VPN PROFILE

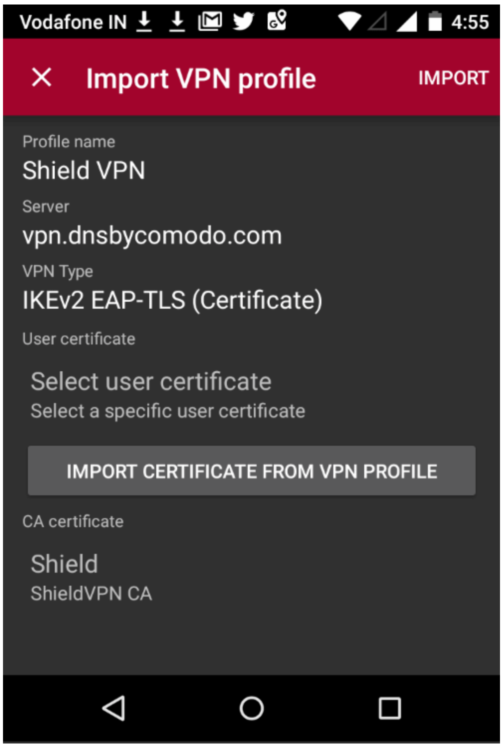
Status: No active VPN

No VPN profiles.

- Tap the menu icon beside 'Add VPN Profile' and tap 'Import VPN profile'



- Choose 'Android_VPN_Profile' from the downloaded location



Profile name
Shield VPN

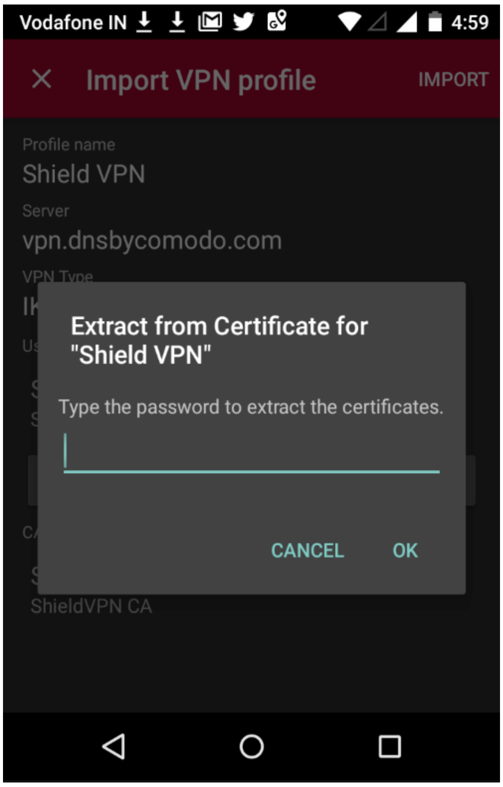
Server
vpn.dnsbycomodo.com

VPN Type
IKEv2 EAP-TLS (Certificate)

User certificate
Select user certificate
Select a specific user certificate

CA certificate
Shield
ShieldVPN CA

- Tap 'Import Certificate from VPN Profile'



Vodafone IN 4:59

Import VPN profile IMPORT

Profile name
Shield VPN

Server
vpn.dnsbycomodo.com

VPN Type

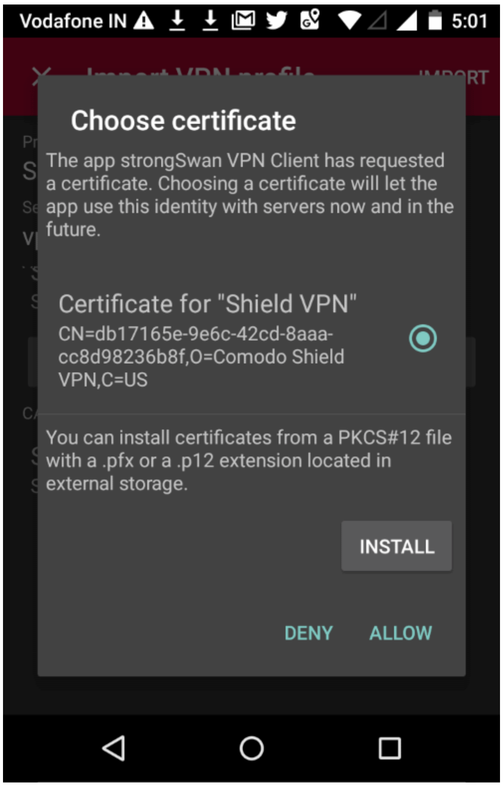
ShieldVPN CA

Extract from Certificate for "Shield VPN"

Type the password to extract the certificates.

CANCEL OK

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



Vodafone IN 5:01

Choose certificate

The app strongSwan VPN Client has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

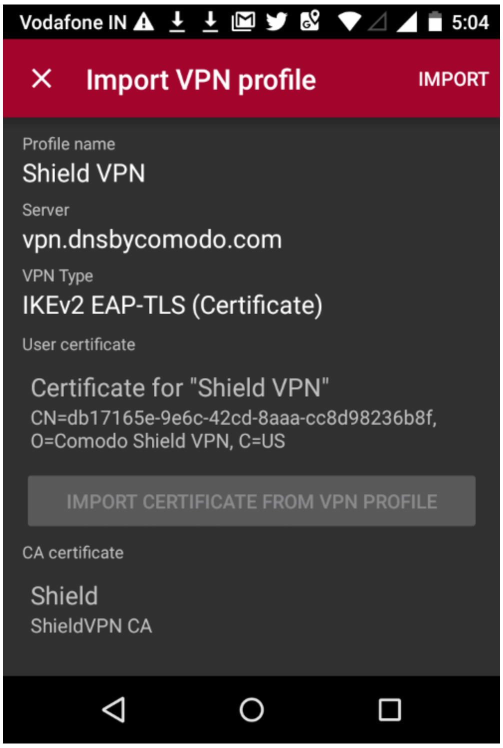
Certificate for "Shield VPN" ●
CN=db17165e-9e6c-42cd-8aaa-cc8d98236b8f,O=Comodo Shield VPN,C=US

You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.

INSTALL

DENY ALLOW

- Tap 'Allow' instead of 'Install'



Import VPN profile

Profile name
Shield VPN

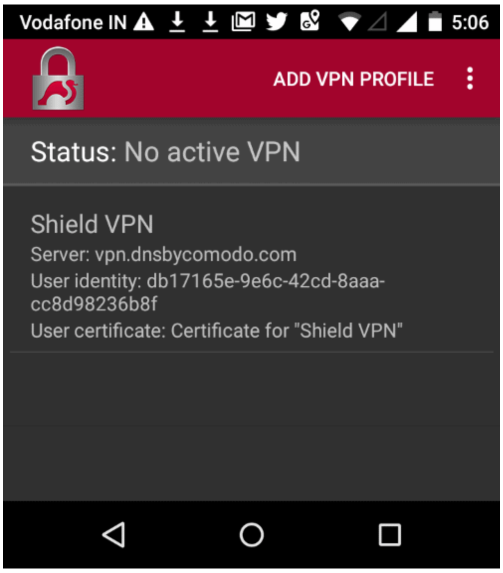
Server
vpn.dnsbycomodo.com

VPN Type
IKEv2 EAP-TLS (Certificate)

User certificate
Certificate for "Shield VPN"
CN=db17165e-9e6c-42cd-8aaa-cc8d98236b8f, O=Comodo Shield VPN, C=US

CA certificate
Shield
ShieldVPN CA

- Tap 'Import' at the top-right

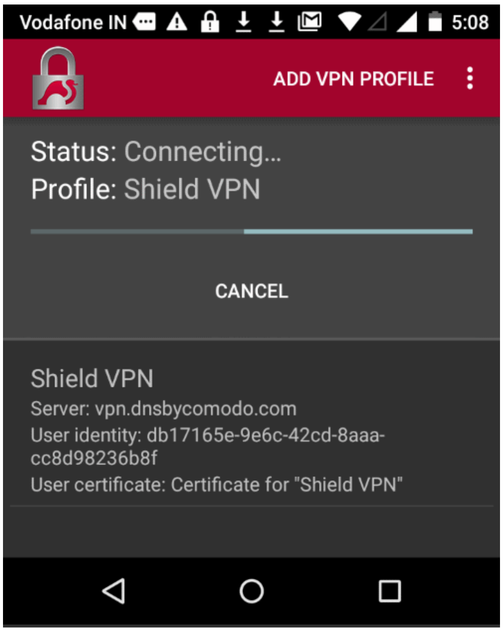


Status: No active VPN

Shield VPN
Server: vpn.dnsbycomodo.com
User identity: db17165e-9e6c-42cd-8aaa-cc8d98236b8f
User certificate: Certificate for "Shield VPN"

- After importing the profile, tap on it.

Connection to Shield will start...

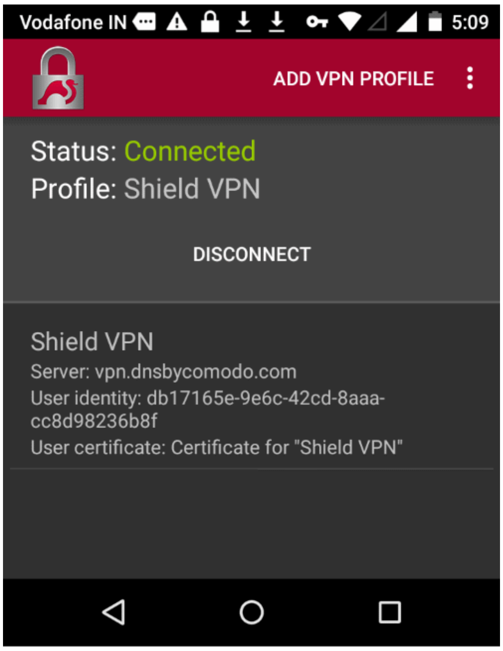


Vodafone IN 5:08

Status: Connecting...
Profile: Shield VPN

Shield VPN
Server: vpn.dnsbycomodo.com
User identity: db17165e-9e6c-42cd-8aaa-cc8d98236b8f
User certificate: Certificate for "Shield VPN"

...and on success, the 'Connected' status will be displayed.



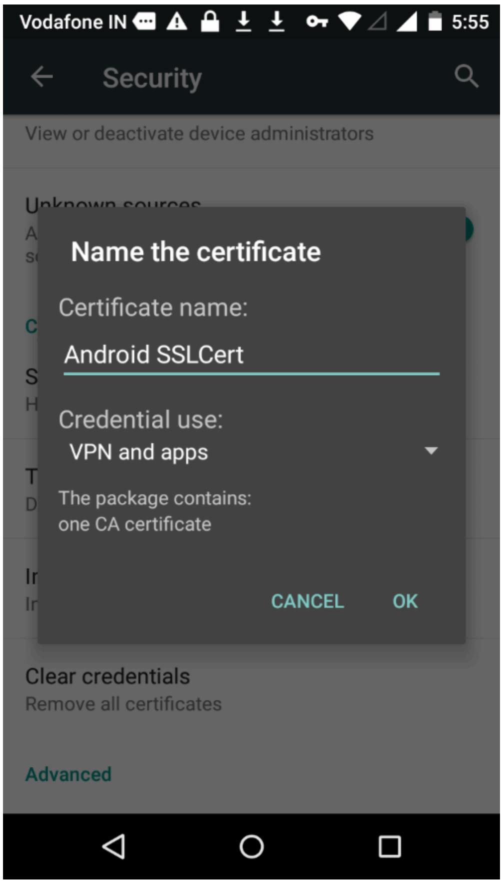
Vodafone IN 5:09

Status: Connected
Profile: Shield VPN

Shield VPN
Server: vpn.dnsbycomodo.com
User identity: db17165e-9e6c-42cd-8aaa-cc8d98236b8f
User certificate: Certificate for "Shield VPN"

Note: In order to view HTTPS websites, tap on the attachment 'AndroidSSLCert.pem and download.

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



Name the certificate

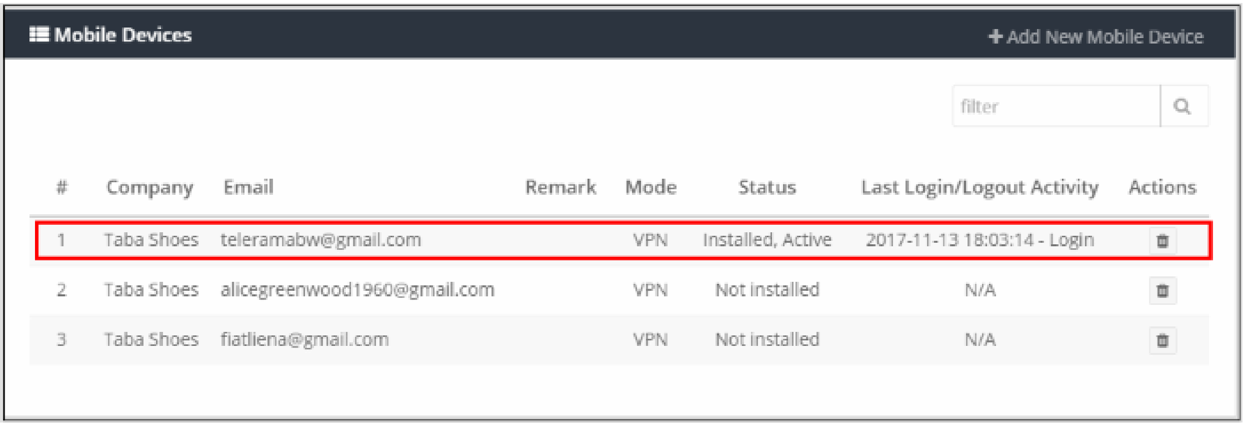
Certificate name: Android SSLCert

Credential use: VPN and apps

The package contains:
one CA certificate

You can view the certificate under Settings > Security > Trusted Credential > User.

The mobile device will be enrolled and displayed in the screen.

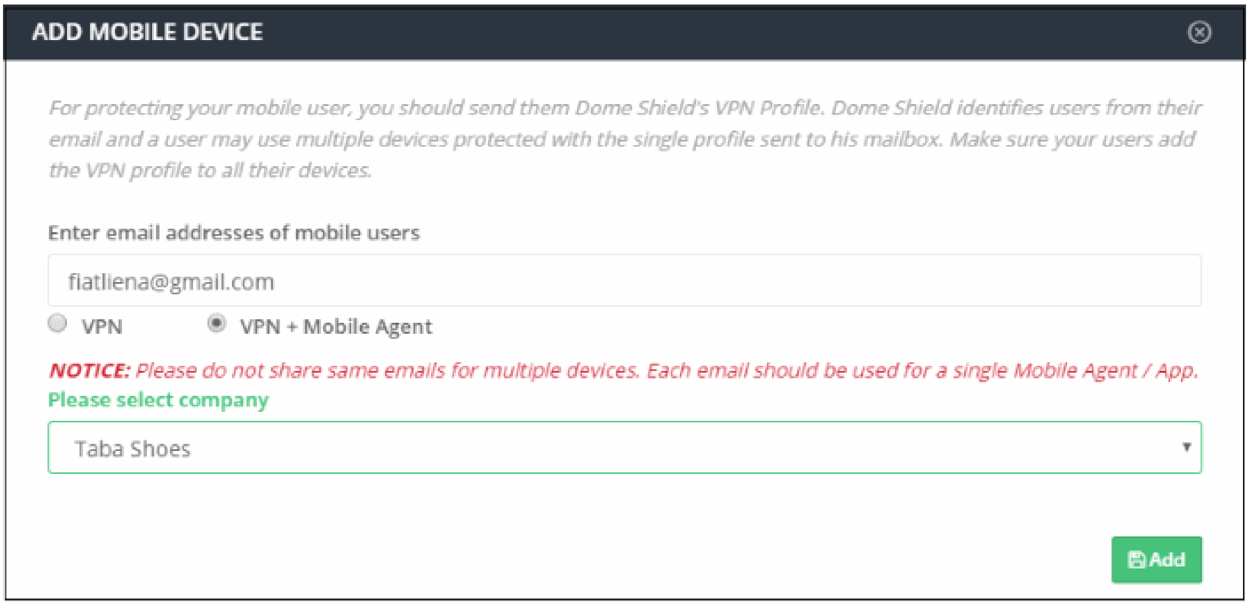


#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	Taba Shoes	teleramabw@gmail.com		VPN	Installed, Active	2017-11-13 18:03:14 - Login	🗑
2	Taba Shoes	alicegreenwood1960@gmail.com		VPN	Not installed	N/A	🗑
3	Taba Shoes	fiatliena@gmail.com		VPN	Not installed	N/A	🗑

Please note no rules will be applied to the mobile device(s) 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 advice on how to configure and deploy security policies to mobile devices.

Shield Mobile Device App

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



ADD MOBILE DEVICE

For protecting your mobile user, you should send them Dome Shield's VPN Profile. Dome Shield identifies users from their email and a user may use multiple devices protected with the single profile sent to his mailbox. Make sure your users add the VPN profile to all their devices.

Enter email addresses of mobile users

fiatliena@gmail.com

○ VPN ● VPN + Mobile Agent

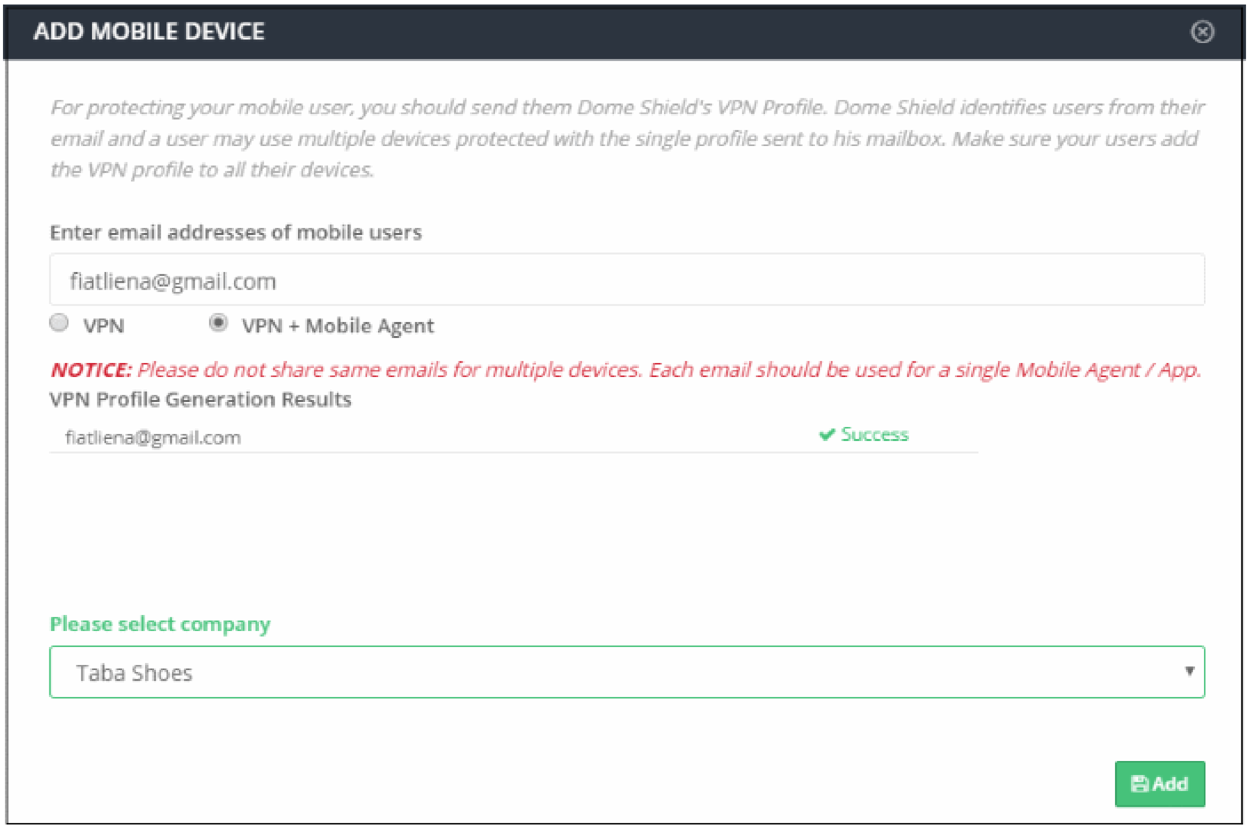
NOTICE: *Please do not share same emails for multiple devices. Each email should be used for a single Mobile Agent / App.*

Please select company

Taba Shoes

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

The enrollment instructions email will be sent to the users and a confirmation message will be displayed:



ADD MOBILE DEVICE

For protecting your mobile user, you should send them Dome Shield's VPN Profile. Dome Shield identifies users from their email and a user may use multiple devices protected with the single profile sent to his mailbox. Make sure your users add the VPN profile to all their devices.

Enter email addresses of mobile users

fiatliena@gmail.com

○ VPN ● VPN + Mobile Agent

NOTICE: *Please do not share same emails for multiple devices. Each email should be used for a single Mobile Agent / App.*

VPN Profile Generation Results

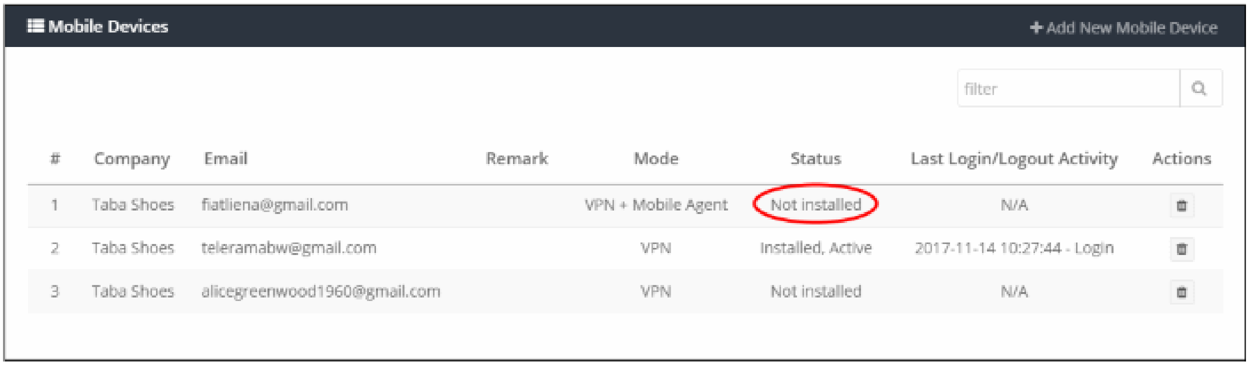
fiatliena@gmail.com ✓ Success

Please select company

Taba Shoes

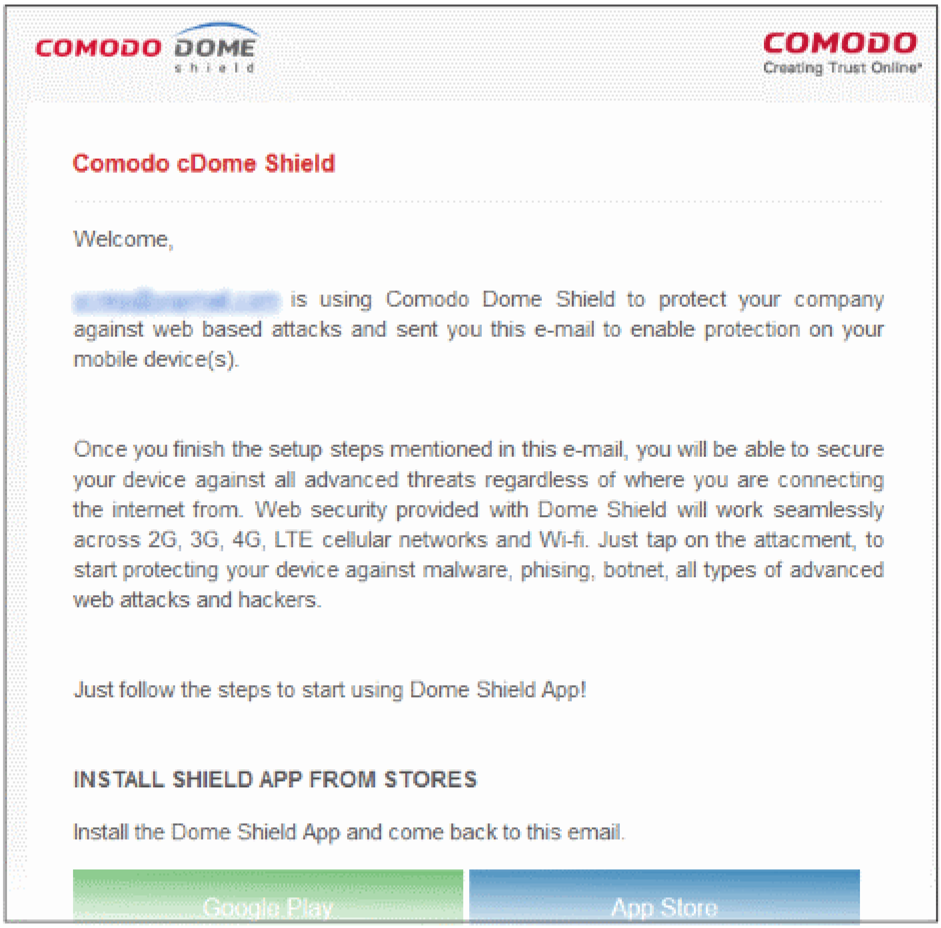
- Click ⊗ to close the dialog.

The user will be added to the list but the status will show as 'Not installed'.



#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	Taba Shoes	fiatliena@gmail.com		VPN + Mobile Agent	Not installed	N/A	🗑
2	Taba Shoes	teleramabw@gmail.com		VPN	Installed, Active	2017-11-14 10:27:44 - Login	🗑
3	Taba Shoes	alicegreenwood1960@gmail.com		VPN	Not installed	N/A	🗑

The user should open the email on the device. The email will contain clear instructions how to install the Shield app on Android and iOS devices.



Comodo cDome Shield

Welcome,

[redacted] is using Comodo Dome Shield to protect your company against web based attacks and sent you this e-mail to enable protection on your mobile device(s).

Once you finish the setup steps mentioned in this e-mail, you will be able to secure your device against all advanced threats regardless of where you are connecting the internet from. Web security provided with Dome Shield will work seamlessly across 2G, 3G, 4G, LTE cellular networks and Wi-fi. Just tap on the attacment, to start protecting your device against malware, phising, botnet, all types of advanced web attacks and hackers.

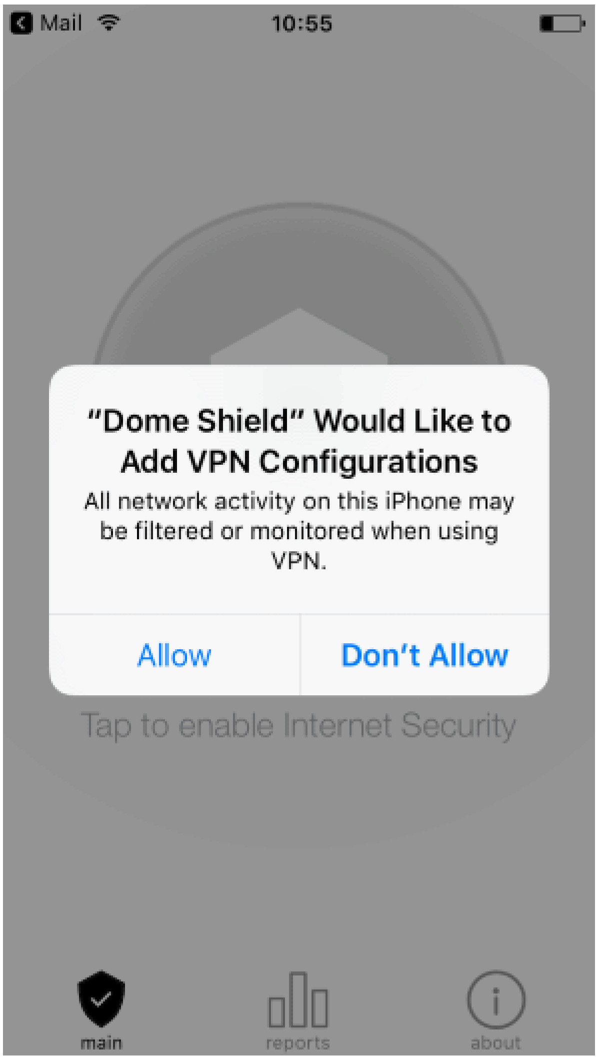
Just follow the steps to start using Dome Shield App!

INSTALL SHIELD APP FROM STORES

Install the Dome Shield App and come back to this email.

Instructions for iOS

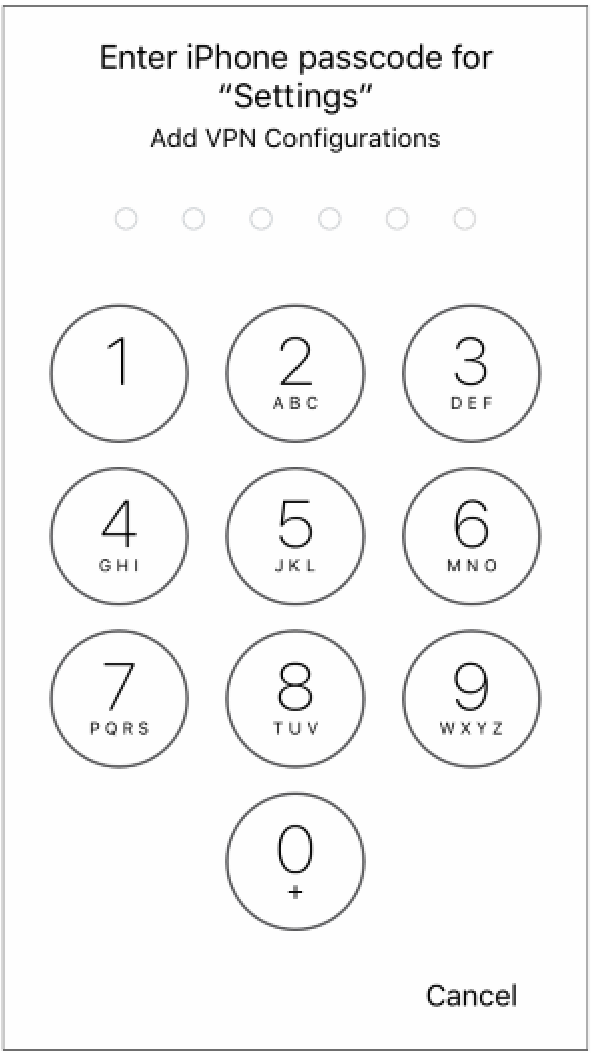
- Open the enrollment mail on the iOS device
- Tap 'App Store' and download the Dome Shield app from the Apple store
- After installing the app, tap 'Activate iOS App' in the mail.
- Next, open the app and tap the 'Shield' button



"Dome Shield" Would Like to Add VPN Configurations

All network activity on this iPhone may be filtered or monitored when using VPN.

- Tap 'Allow'
- Provide password if applicable



Enter iPhone passcode for "Settings"

Add VPN Configurations

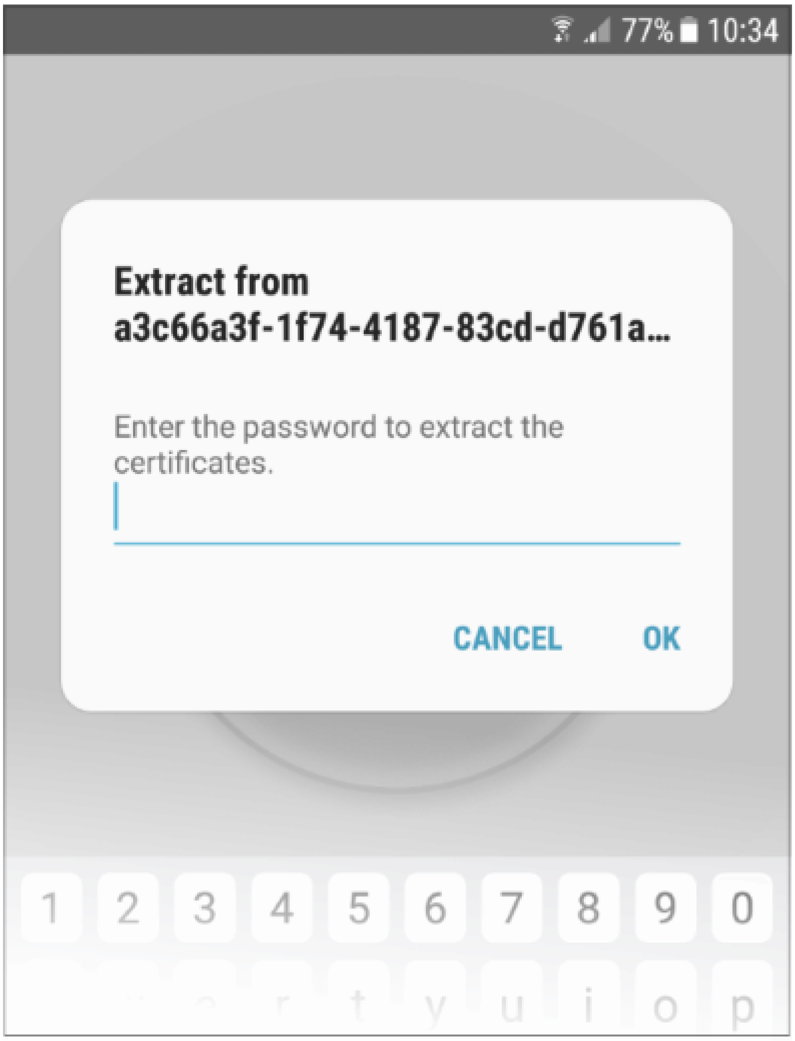
That's it. The iOS device will be successfully enrolled to Dome Shield.

Important Note: In order to be able to view HTTPS websites, the user should trust the root certificate.

- Go to 'Settings' > 'Security' > 'About' > 'Certificate Trust Settings' and tap 'Enable Full Trust for Root Certificates'

Instructions for Android

- Open the enrollment mail.
- Tap 'Google Play' and install the Dome Shield app from Play Store.
- Please note the screens may vary depending on the Android version.
- After installing the app, tap 'Activate Android App' in the mail.
- The activation password will be copied to the clipboard automatically after tapping 'Activate Android App'.
- Next, tap the 'Shield' icon.

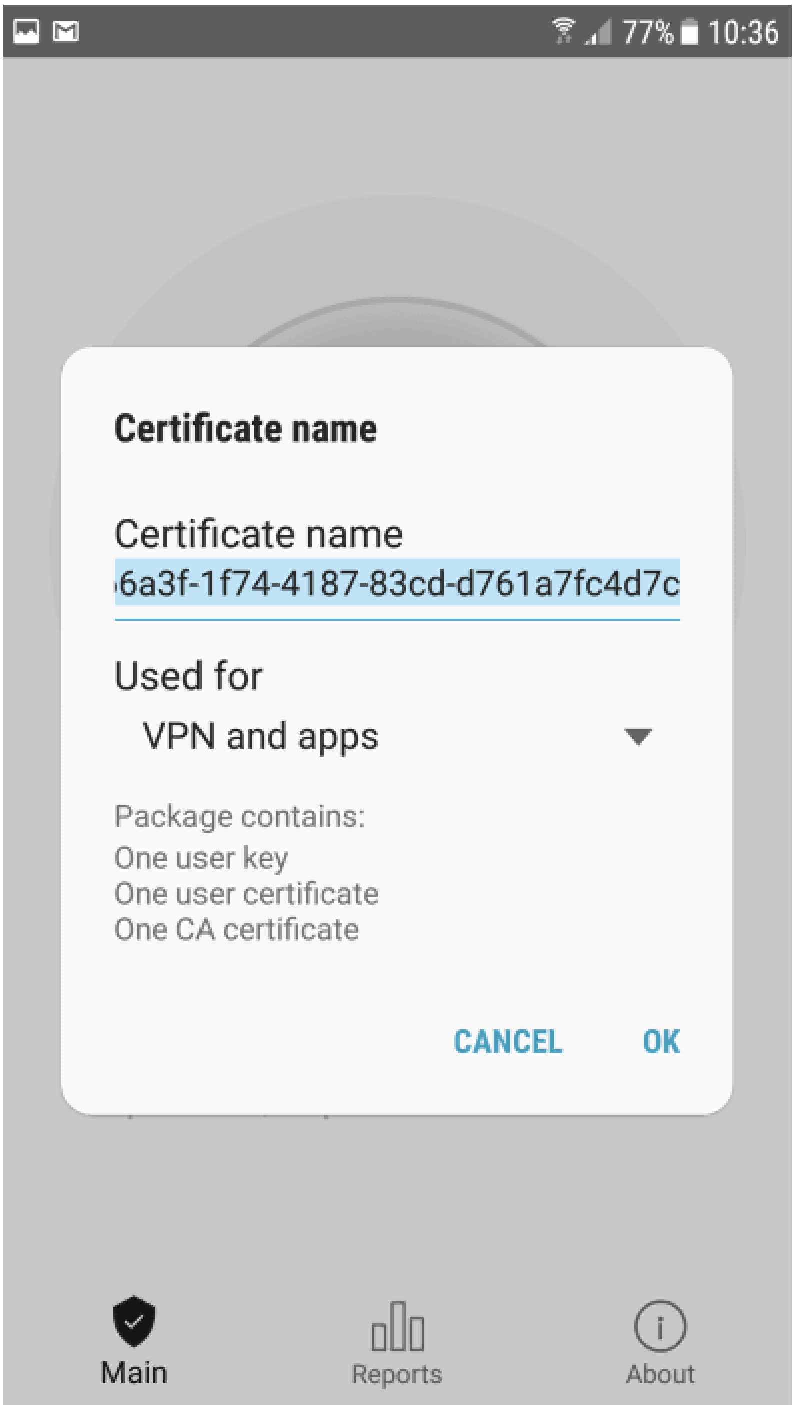


Extract from a3c66a3f-1f74-4187-83cd-d761a...

Enter the password to extract the certificates.

- Long press in the password field and tap 'Paste'
- Tap 'OK'

The unique identifier of the user VPN certificate will be auto-filled.



Certificate name

Certificate name

6a3f-1f74-4187-83cd-d761a7fc4d7c

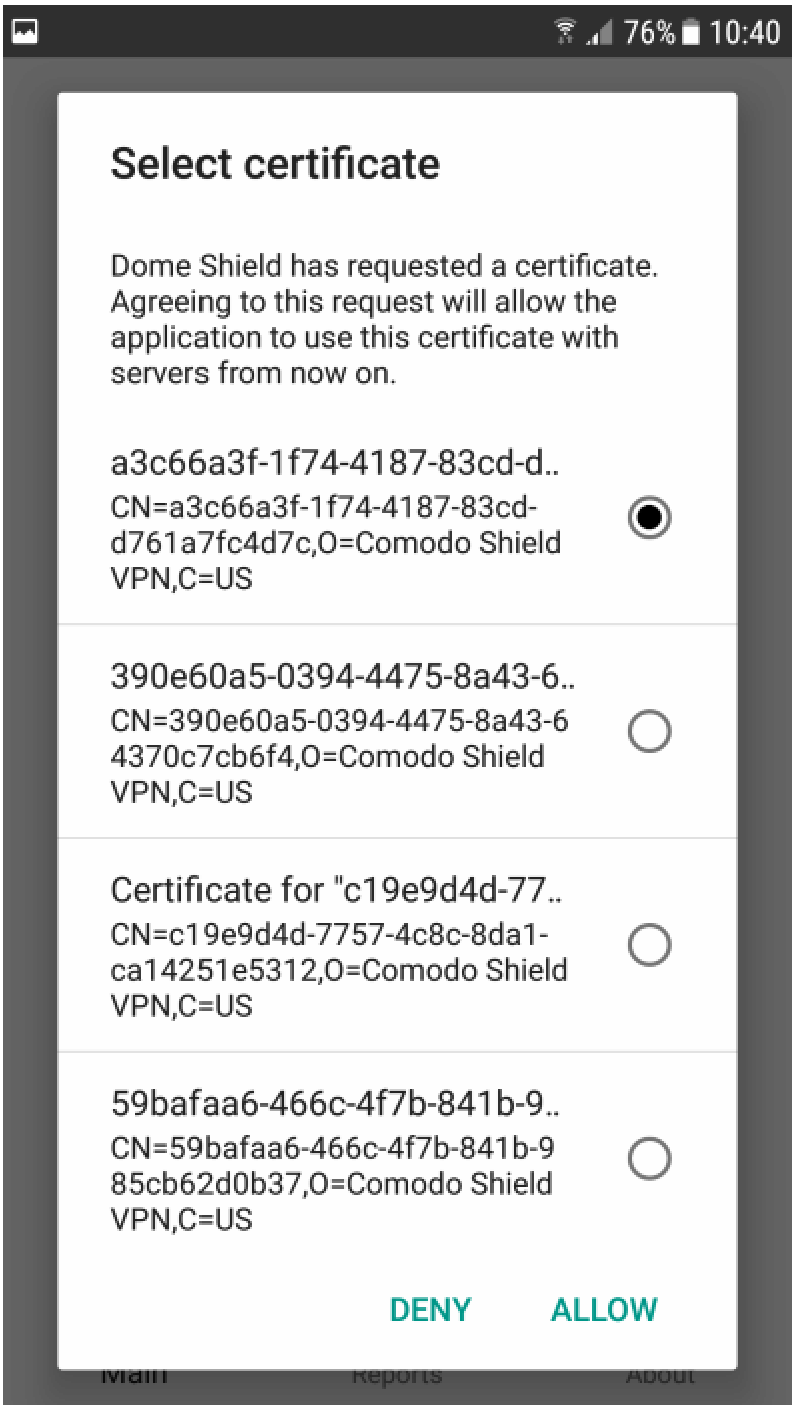
Used for

VPN and apps

Package contains:
One user key
One user certificate
One CA certificate

- Tap 'OK'

The user VPN certificate will be pre-selected in the 'Select certificate' screen:



Select certificate

Dome Shield has requested a certificate. Agreeing to this request will allow the application to use this certificate with servers from now on.

● a3c66a3f-1f74-4187-83cd-d..
CN=a3c66a3f-1f74-4187-83cd-d761a7fc4d7c,O=Comodo Shield VPN,C=US

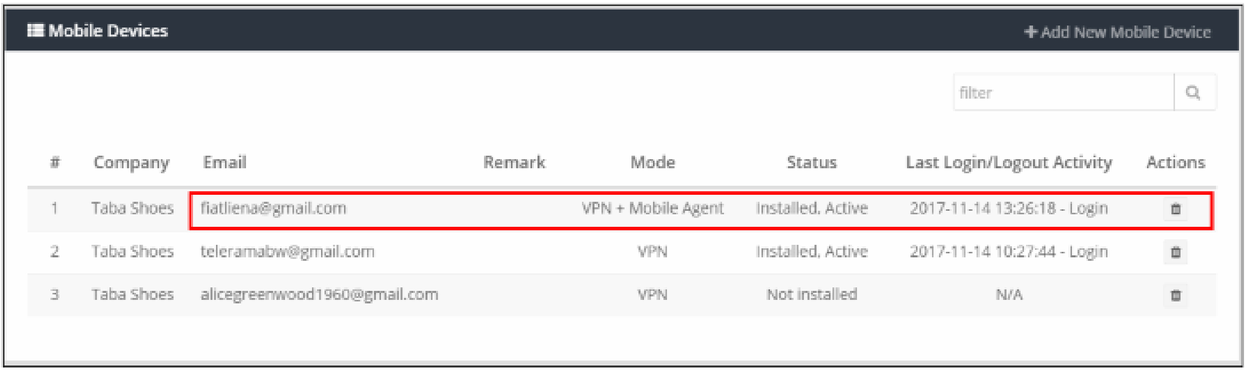
○ 390e60a5-0394-4475-8a43-6..
CN=390e60a5-0394-4475-8a43-64370c7cb6f4,O=Comodo Shield VPN,C=US

○ Certificate for "c19e9d4d-77..
CN=c19e9d4d-7757-4c8c-8da1-ca14251e5312,O=Comodo Shield VPN,C=US

○ 59bafaa6-466c-4f7b-841b-9..
CN=59bafaa6-466c-4f7b-841b-985cb62d0b37,O=Comodo Shield VPN,C=US

- Tap 'Allow'

That's it. The Dome Shield app will be activated and the device enrolled. The device details will also be displayed in the 'Mobile Devices' screen.



Mobile Devices

#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	Taba Shoes	fiatliena@gmail.com		VPN + Mobile Agent	Installed, Active	2017-11-14 13:26:18 - Login	🗑
2	Taba Shoes	teleramabw@gmail.com		VPN	Installed, Active	2017-11-14 10:27:44 - Login	🗑
3	Taba Shoes	alicegreenwood1960@gmail.com		VPN	Not installed	N/A	🗑

Important Note: In order to be able to view HTTPS websites, the user should download and install the 'AndroidSSLCert.pem' file in the enrollment mail.

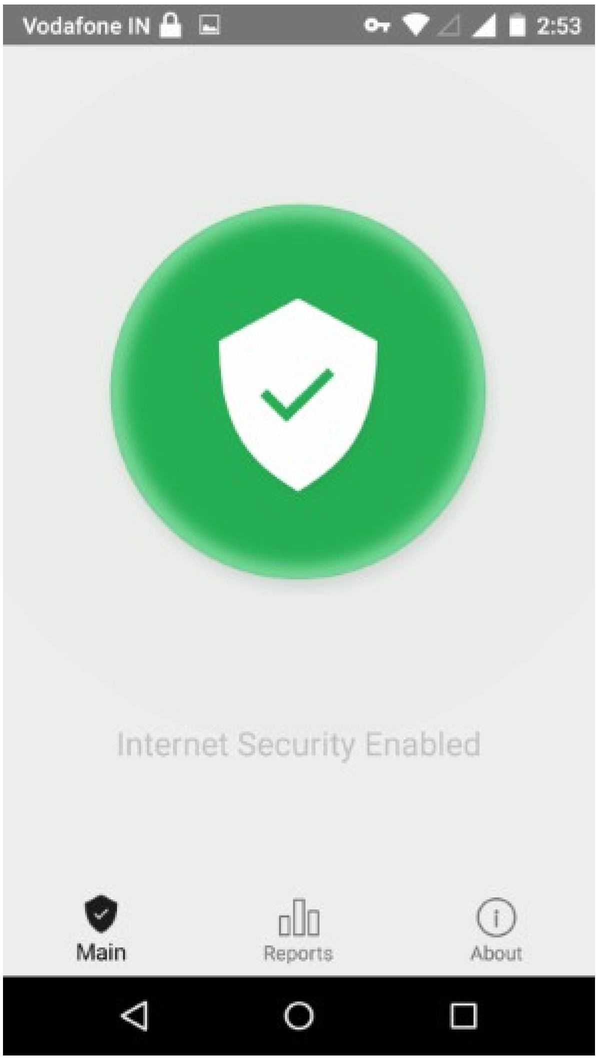
- Go to 'Settings' > 'Security'
- Tap 'Install from SD card'
- Select the downloaded certificate 'AndroidSSLCert.pem'
- Enter 'AndroidSSLCert' in the 'Name the certificate' screen.
- Tap 'OK'

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

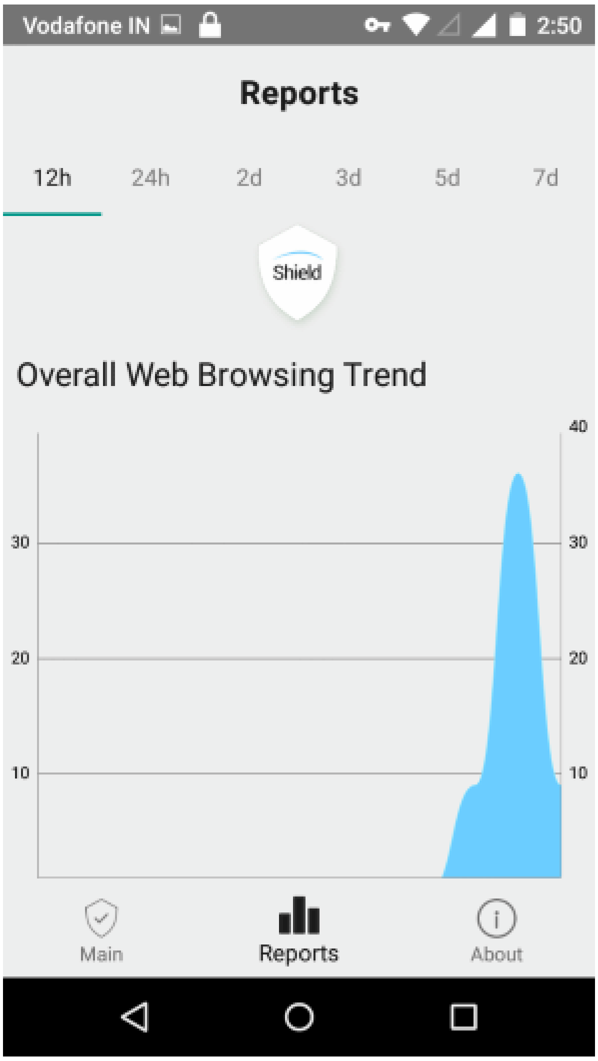
- Tap the Shield icon

The Shield app will open:

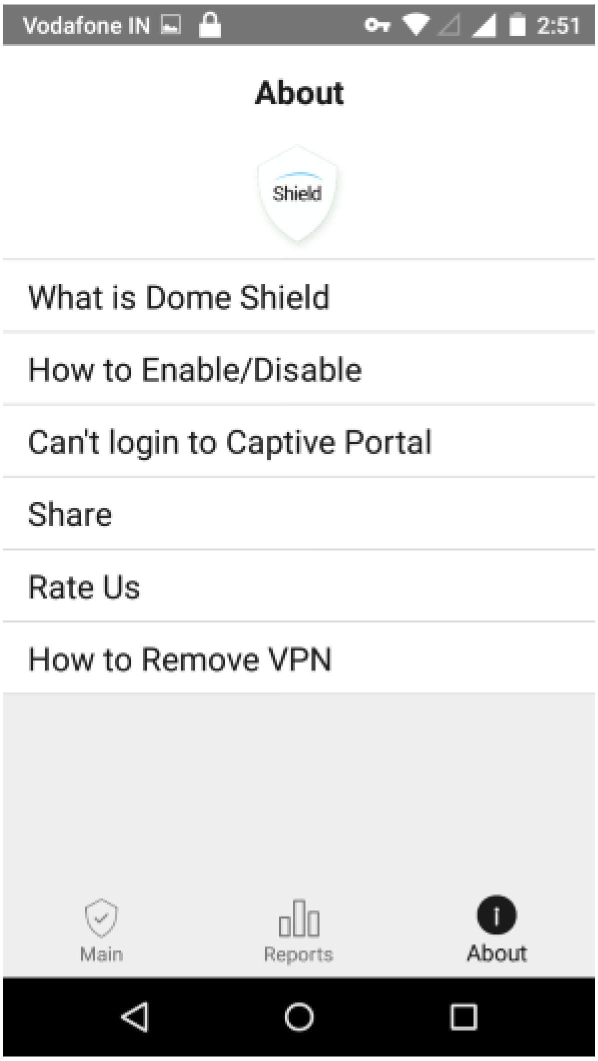
- Main - Tapping the icon will connect / disconnect to Shield.



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



- About - Detailed information about Dome Shield

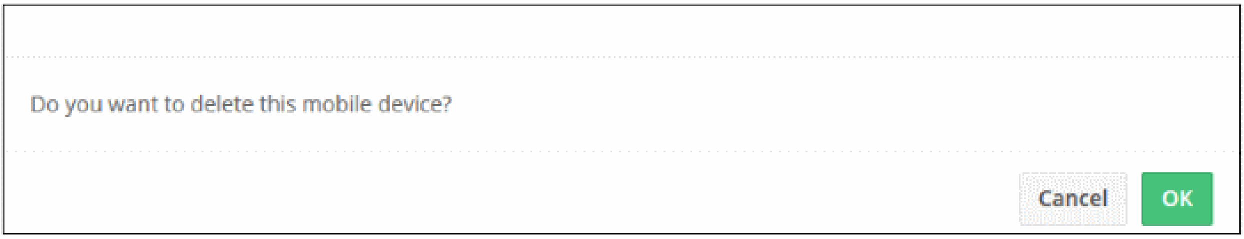


- **What is Dome Shield** - Brief description about the product
- **How to Enable / Disable** - Instructions how to connect / disconnect to Shield
- **Can't login to Captive Portal** - Troubleshooting instructions
- **Share** - Send the app location details to your friends
- **Rate Us** - Rate the Shield 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.


Do you want to delete this mobile device?

- 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'

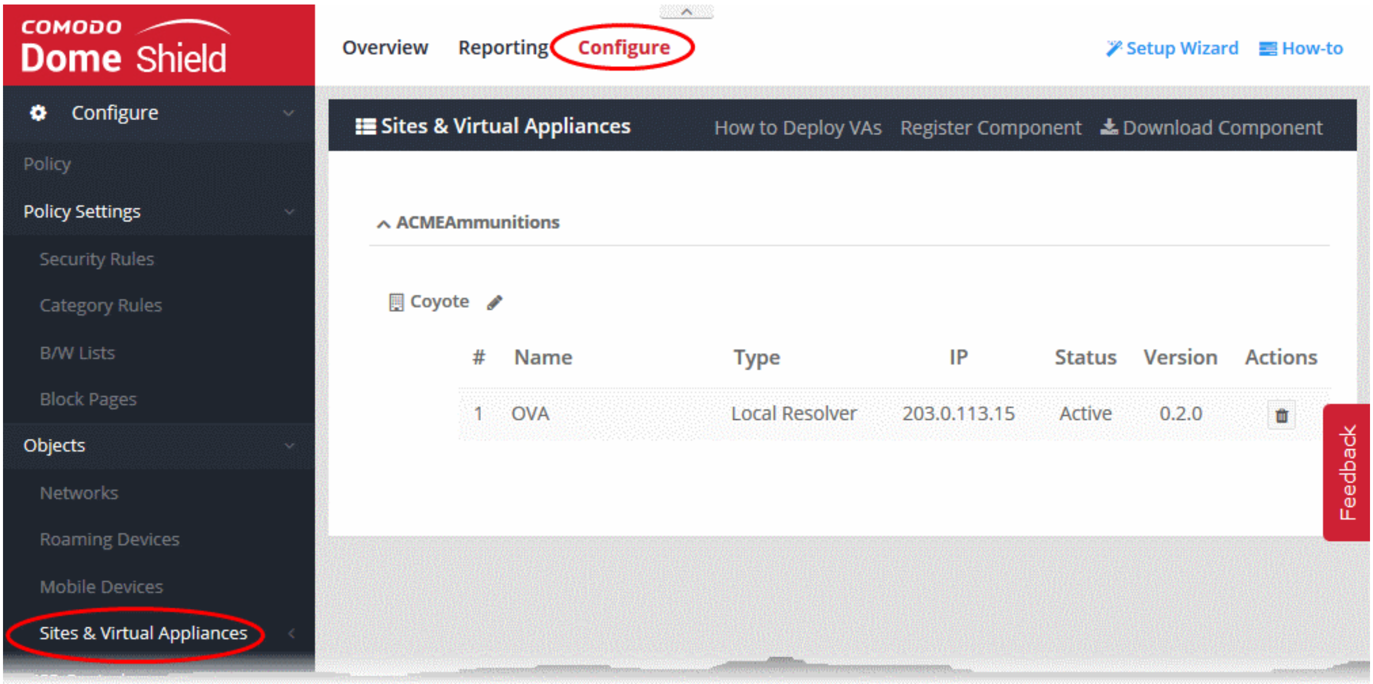
The 'Sites & Virtual Appliances' area lets you:

- 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'



#	Name	Type	IP	Status	Version	Actions
1	OVA	Local Resolver	203.0.113.15	Active	0.2.0	🗑

- The links on the title bar help you to download and register the VA's:
  - **How to Deploy VAs** - Opens the built-in guide for deploying the Local Resolver VA's. The guide contains detailed tutorials on setting up the LR virtual appliance, registering it to Dome Shield and importing the network, defining internal networks as objects and applying policies to them.
  - **Register Component** - Allows you register a deployed virtual appliance and import the network site 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** - Allows you to download the setup package for deploying 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.
- For MSP customers the list is sorted by the companies.
- The site name is displayed at the top left of set of virtual appliances registered for that site.

Sites & Virtual Appliances - Column Descriptions	
Column Header	Description

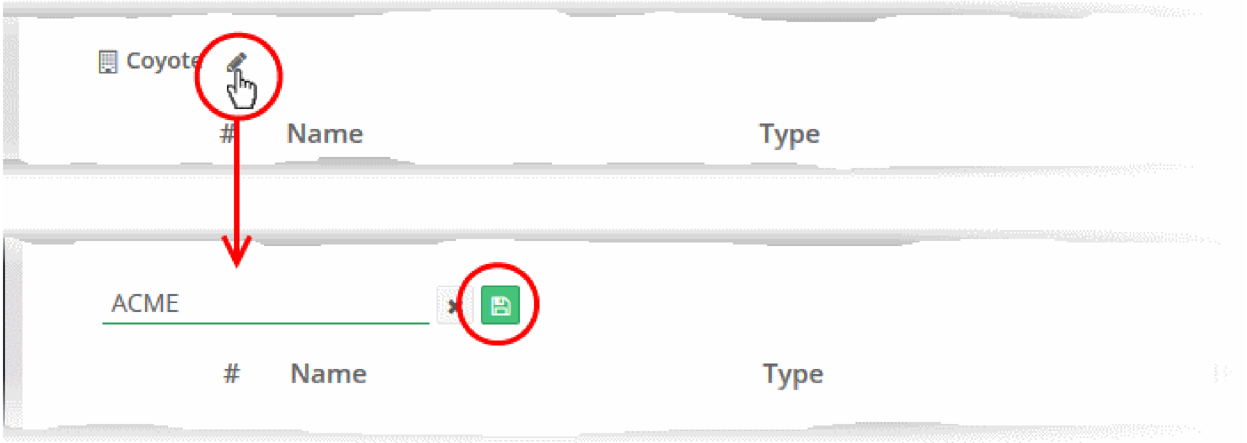
Name	The label assigned to the VA during its initial configuration.
Type	Indicates kind of the virtual appliance.
IP	The IP address assigned to the virtual appliance.
Status	Whether the virtual appliance is connected to Dome Shield to apply the policies to the network endpoints or not.
Version	The software version number of the virtual appliance
Actions	Allows to remove a virtual appliance.

The interface allows you to:

- 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

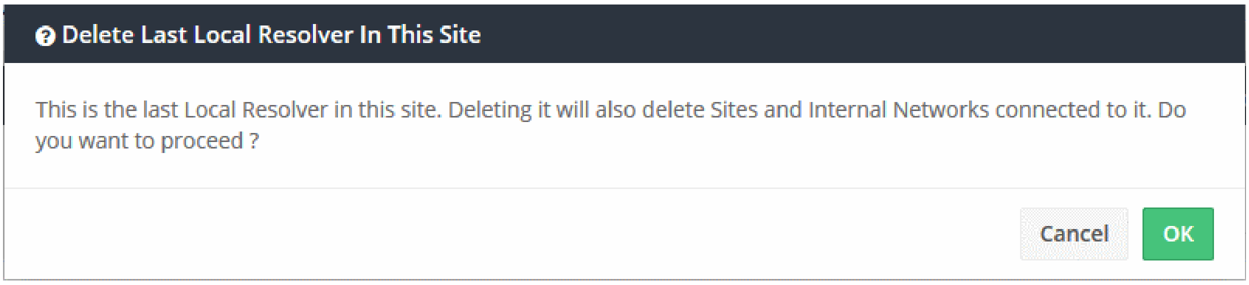


- Click the 'Save' icon

To remove a virtual appliance

- Click the trashcan icon in the row of the appliance

A confirmation dialog will be displayed.



Delete Last Local Resolver In This Site

This is the last Local Resolver in this site. Deleting it will also delete Sites and Internal Networks connected to it. Do you want to proceed ?

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

The appliance will be deleted from Dome Shield.

- If no other appliance is registered for the same network site, the site will also be removed and the web protection policies will no longer be applied to the endpoints.

Define Internal Networks and Internal Domains

- You can define single internal IP address or IP address ranges within the site as network objects. This enables you to apply different web protection policies to them as required. See Add Internal Networks for more details
- You can specify the internal domains within the imported sites. The local resolvers will then use the local DNS servers in the networks for resolving the DNS requests from the clients for these domains, and do not forward the requests to the global DNS servers, this reducing your bandwidth usage. See Add Internal Domains for more details.

4.4.1 Add Internal Networks

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

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

- The 'Internal Networks' interface lets you define and manage individual IP address or ranges as objects. You can then apply security policies to these objects.

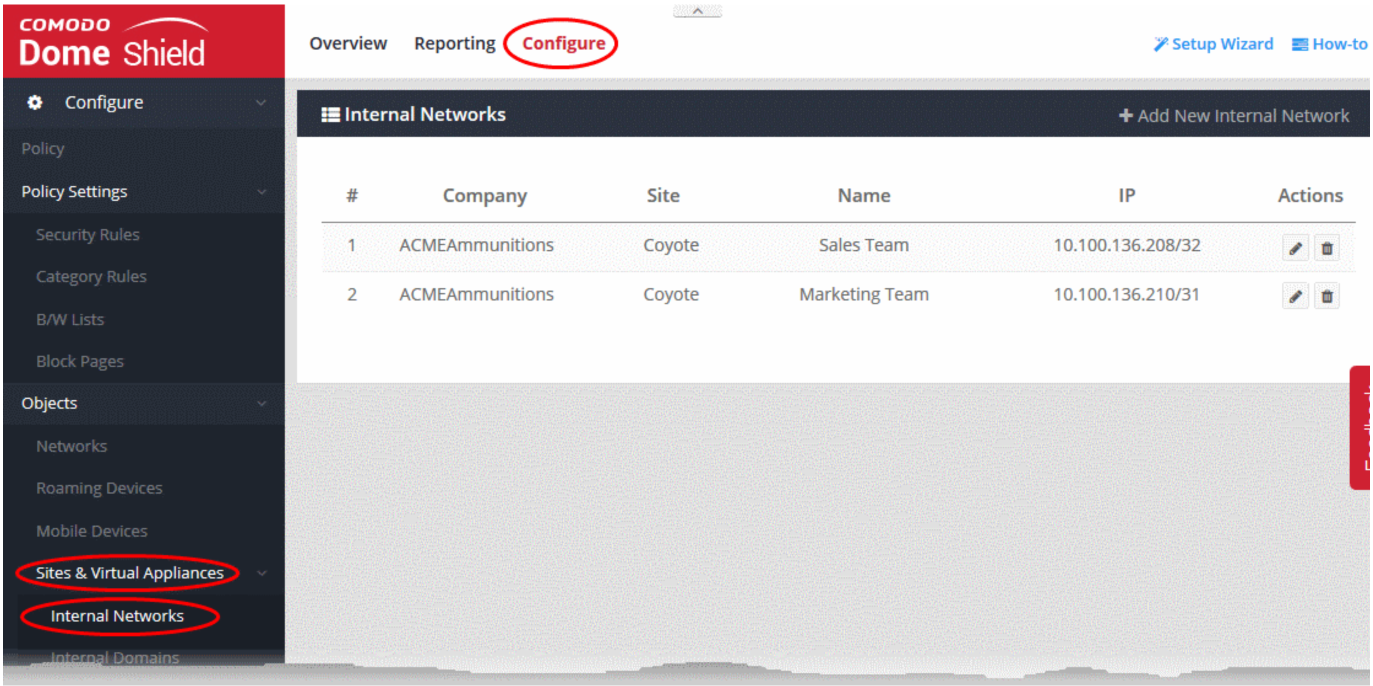
Process in brief:

- Add the IP address of the endpoint and/or the internal IP address 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' > 'Sites & Virtual Appliances' > 'Internal Networks'



#	Company	Site	Name	IP	Actions
1	ACMEAmmunitions	Coyote	Sales Team	10.100.136.208/32	
2	ACMEAmmunitions	Coyote	Marketing Team	10.100.136.210/31	

Internal Networks - Column Descriptions	
Column Header	Description

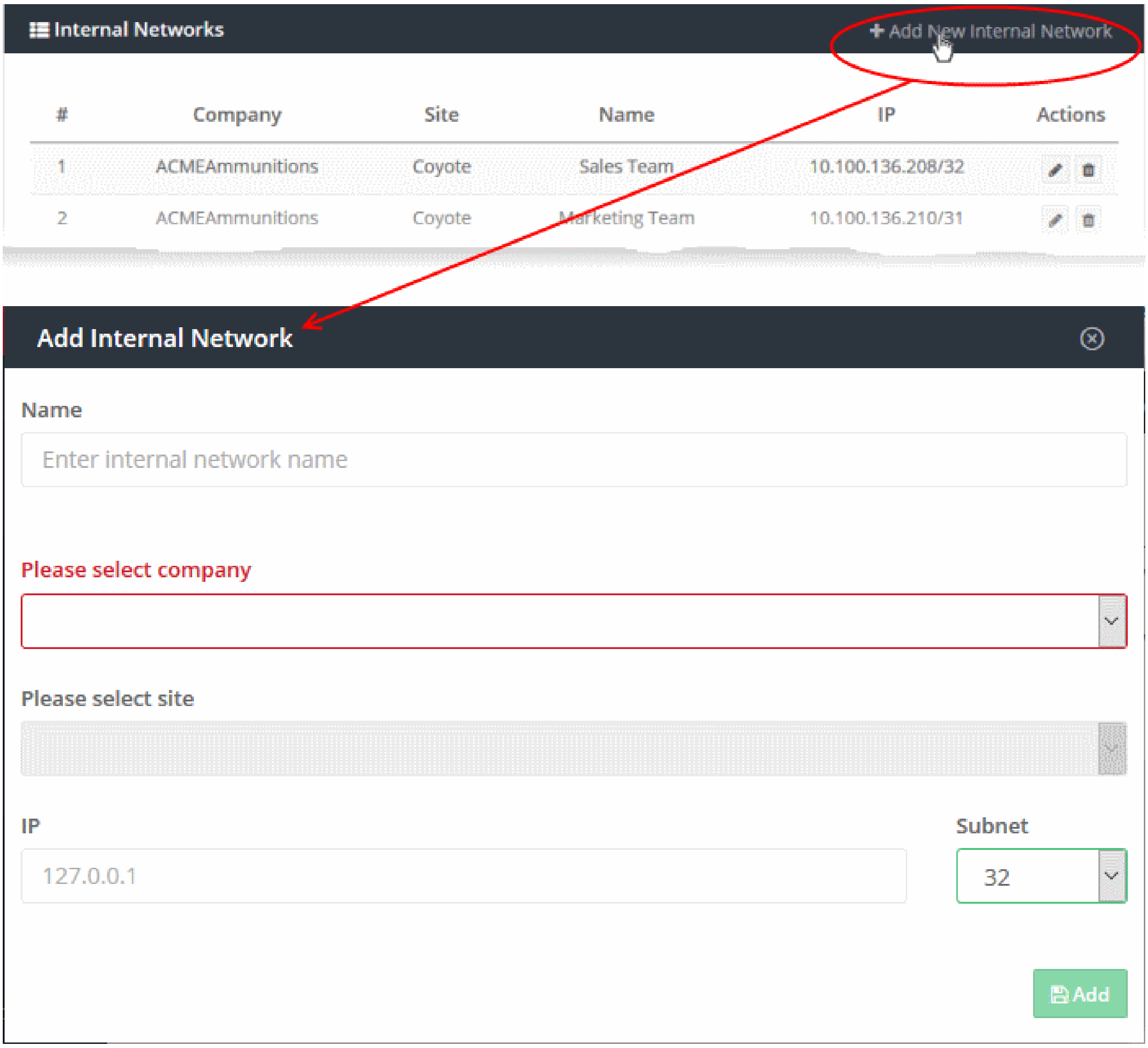
Company	Applies to MSPs only. Name of the organization to which the network site belongs.
Site	The network site to which the individual endpoint or the sub network belongs.
Name	The label assigned to the individual endpoint or the sub network.
IP	The IP address of the individual endpoint or the sub network
Actions	Allows to edit or remove the endpoint/internal network from the list.

The interface lets you:

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

Add Internal Network Objects

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances' > 'Internal Networks'
- Click 'Add New Internal Network'



Internal Networks

#	Company	Site	Name	IP	Actions
1	ACMEAmmunitions	Coyote	Sales Team	10.100.136.208/32	
2	ACMEAmmunitions	Coyote	Marketing Team	10.100.136.210/31	

Add Internal Network

Name: Enter internal network name

Please select company

Please select site

IP: 127.0.0.1

Subnet: 32

'Add Internal Network' dialog - Table of Parameters	
Form Element	**Description**
Name	The label for the internal network object. This name will appear in the object drop-down under the network site when you create a policy.
Please select company	Available only to MSP customers. • 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'

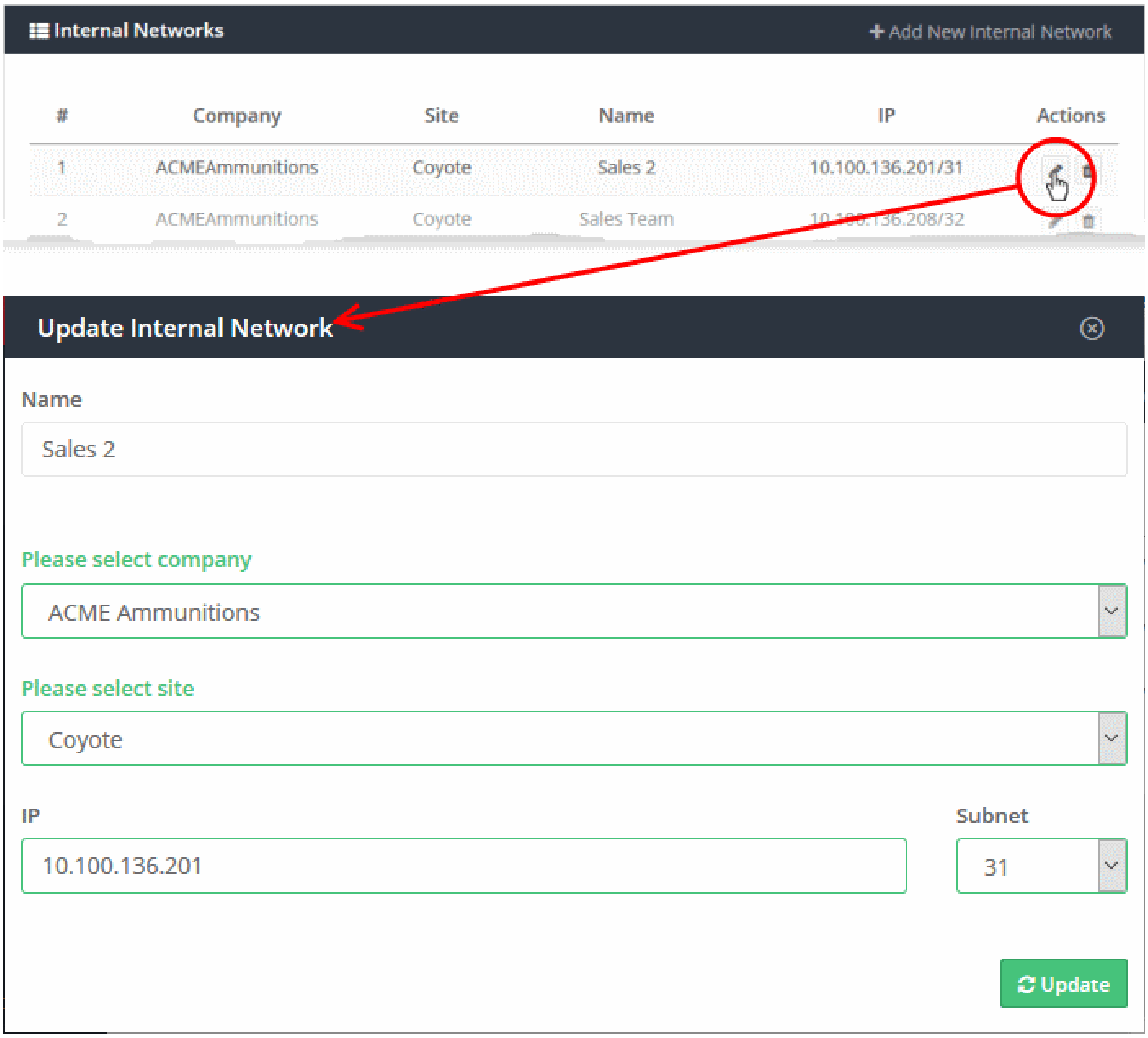
The internal network object will be added to the list. It will be available in the 'Object' drop-down as a target when creating a new policy. See **Apply Policies to Networks, Roaming and Mobile Devices** for more details.

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' > 'Sites & Virtual Appliances' > 'Internal Networks'.
- Click the pencil icon beside the internal network object to be edited.



Internal Networks

#	Company	Site	Name	IP	Actions
1	ACMEAmmunitions	Coyote	Sales 2	10.100.136.201/31	
2	ACMEAmmunitions	Coyote	Sales Team	10.100.136.208/32	

Update Internal Network

Name: Sales 2

Please select company: ACME Ammunitions

Please select site: Coyote

IP: 10.100.136.201

Subnet: 31

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.

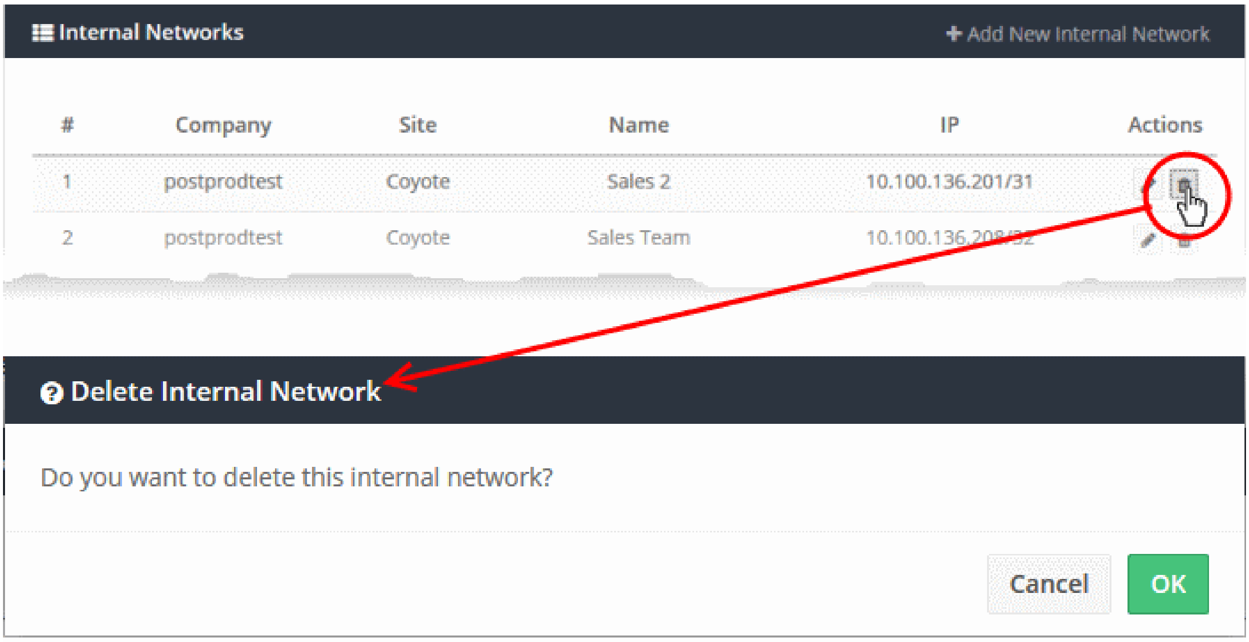
Once removed:

- 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' > 'Sites & Virtual Appliances' > 'Internal Networks'.

- Click the trashcan icon beside the internal network object to be removed.



#	Company	Site	Name	IP	Actions
1	postprodtest	Coyote	Sales 2	10.100.136.201/31	
2	postprodtest	Coyote	Sales Team	10.100.136.208/32	

Delete Internal Network

Do you want to delete this internal network?

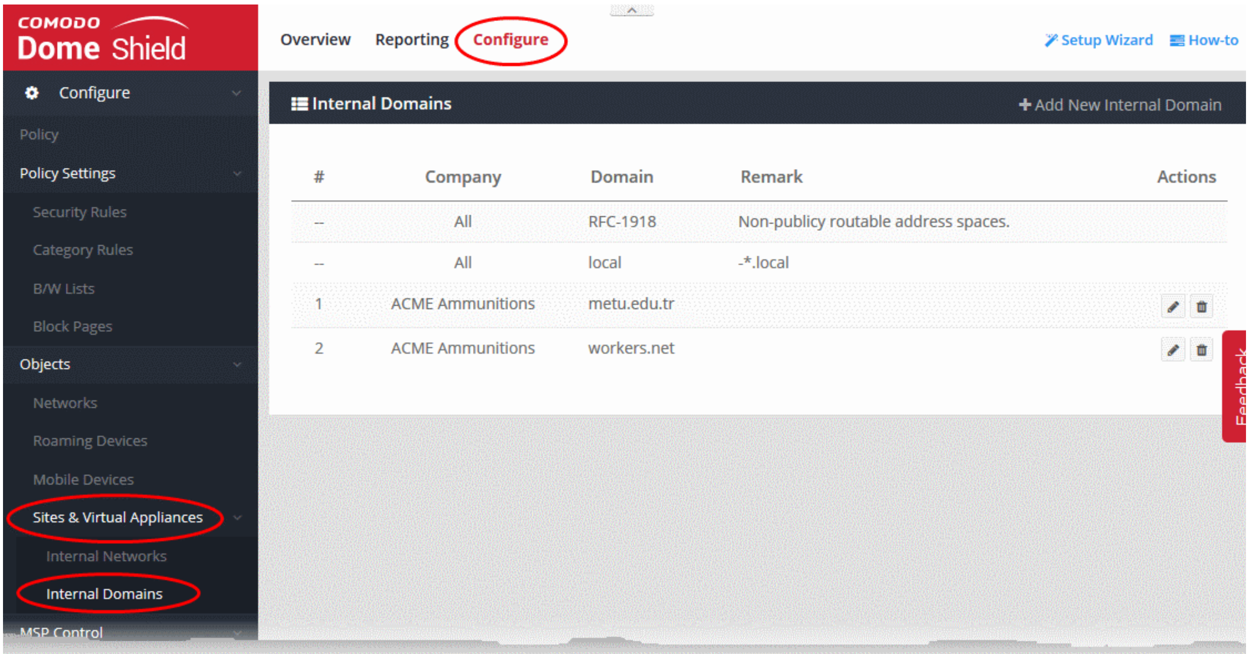
- Click 'OK' in the confirmation dialog to remove the internal network object.

4.4.2 Add Internal Domains

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



#	Company	Domain	Remark	Actions
--	All	RFC-1918	Non-publicy routable address spaces.	
--	All	local	-*.local	
1	ACME Ammunitions	metu.edu.tr		
2	ACME Ammunitions	workers.net		

Internal Domains - Column Descriptions	
Column Header	**Description**
Company	Applies to MSPs only. Name of the organization to which the internal domain belongs.
Domain	The domain name of the internal domain.
Remark	A short description of the internal domain
Actions	Allows to edit or remove the internal domain.

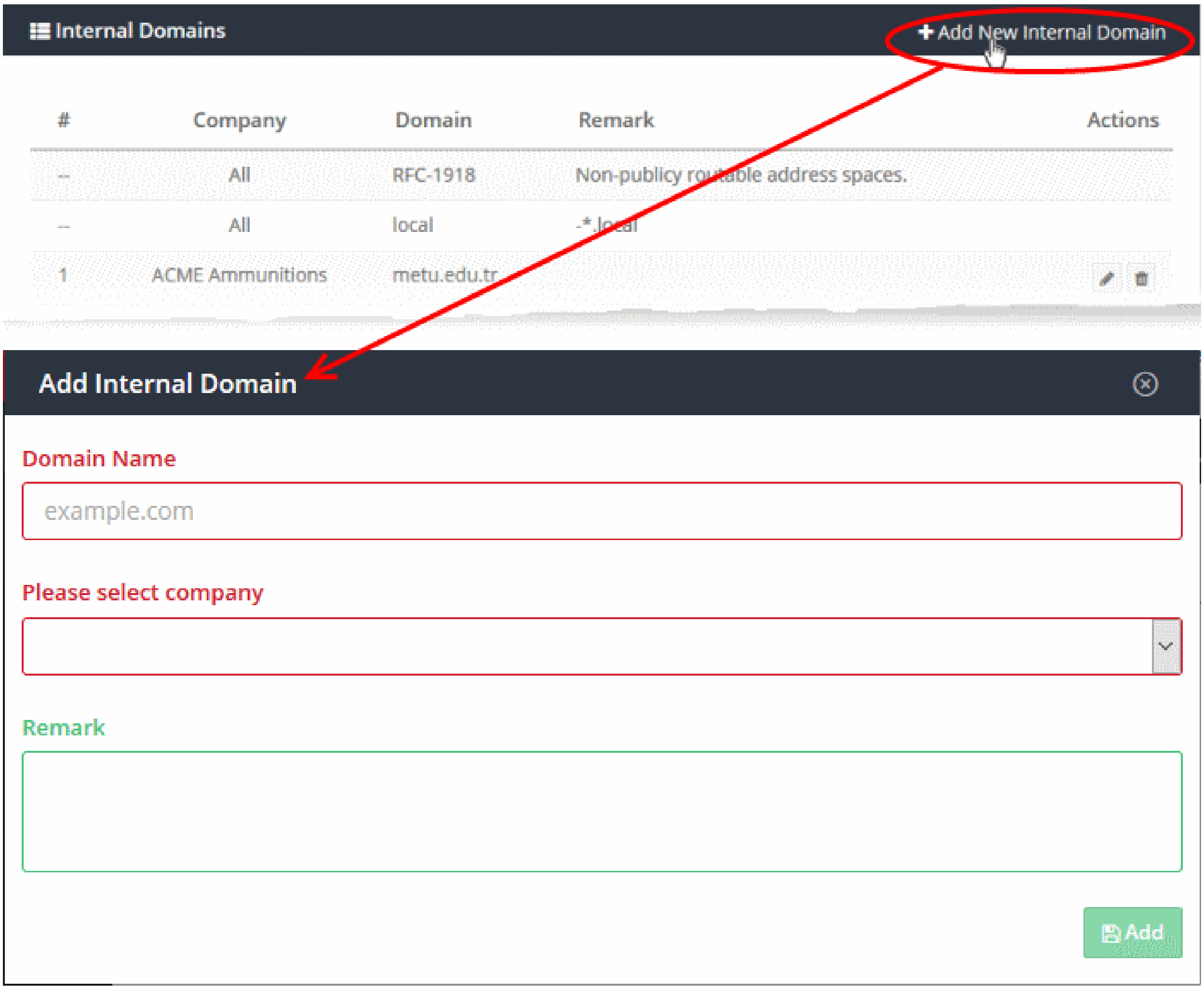
The list contains two default items, including non-publicly routable address spaces and the local domains in the networks.

The interface lets you:

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

Add Internal Domains

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances' > 'Internal Domains'
- Click 'Add New Internal Domain'



#	Company	Domain	Remark	Actions
--	All	RFC-1918	Non-publicly routable address spaces.	
--	All	local	-*.local	
1	ACME Ammunitions	metu.edu.tr		

Domain Name: example.com

Please select company

Remark

'Add Internal Domain' dialog - Table of Parameters	
Form Element	**Description**
Domain Name	The registered domain 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 of an internal domain. Wildcard character = *. For example: *.internaldomain.com
Please select company	Applies to MSP customers only. • Choose the company for whom you want to add the network
Remark	A short description of the internal domain

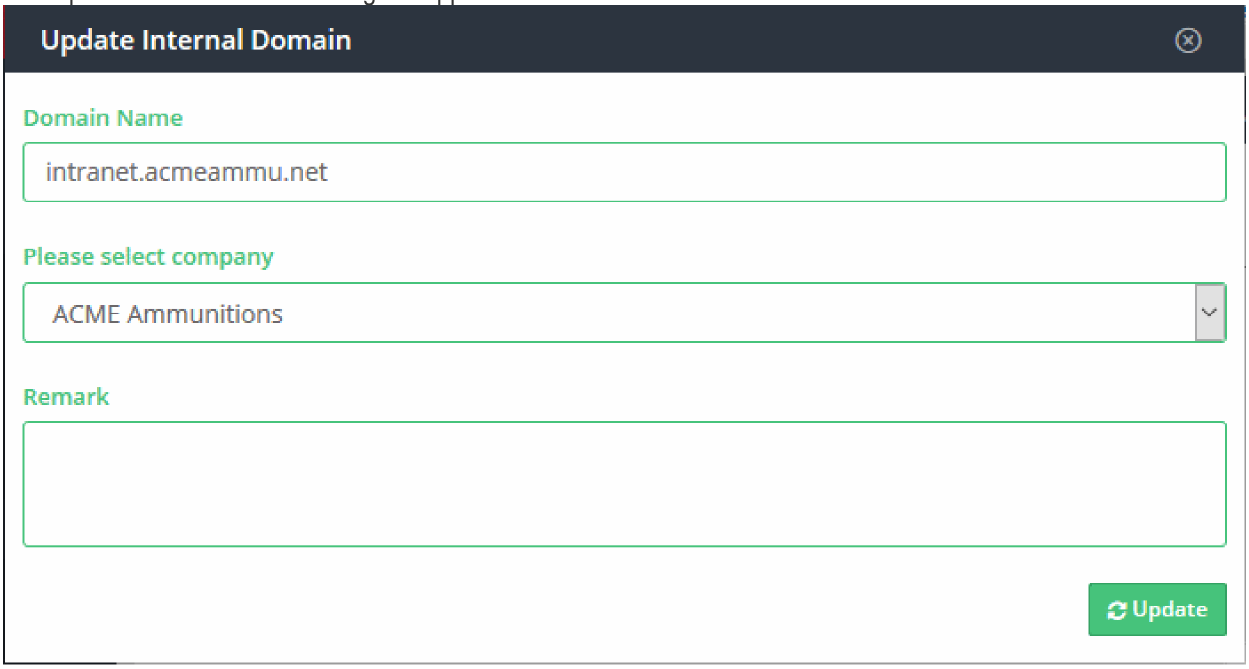
- Enter the parameters and click 'Add'.

The internal domain will be added to the list.

Edit Internal Domains

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances' > 'Internal Domains'
- Click the pencil icon beside the internal domain to be edited.

The Update Internal Domain dialog will appear.



Update Internal Domain

Domain Name: intranet.acmeammu.net

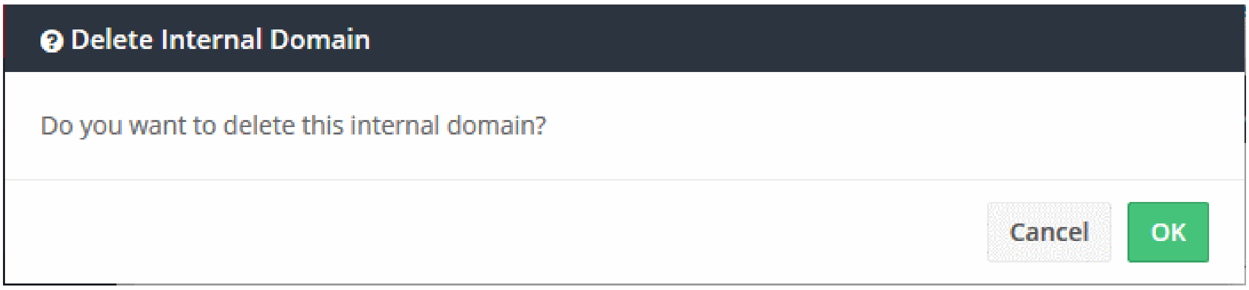
Please select company: ACME Ammunitions

Remark:

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

Remove Internal Domains

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances' > 'Internal Domains'
- Click the trashcan icon beside the internal domain to be removed.



Delete Internal Domain

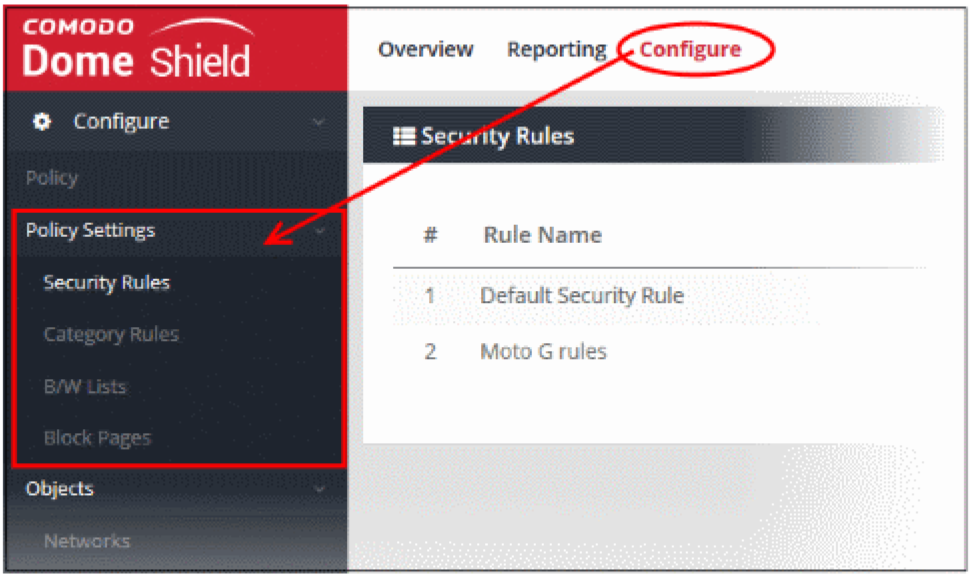
Do you want to delete this internal domain?

- 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:



#	Rule Name
1	Default Security Rule
2	Moto G rules

- Security, category and blacklist/whitelist rules can be added to any policies you create. You can add one rule of each type to a policy.
- You can also create block pages which will be shown to users attempting to access resources that you have blocked in a policy. Policies consist of security rules, category rules, B/W list rules and a block page.
- 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 according to your requirements.
- If you edit a rule, the changes will be automatically reflected in any policies which use the rule
- You can use this interface to create custom security, category and B/W rules. Custom rules can be added to policies as required.
- 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 white lists over-rule any 'Security' or 'Category' rules, allowing you to create exceptions in your policy.
- To view the details of each category, click 'Configure' > 'Policy', then click 'Check Domain Category'

Click the links below for more details:

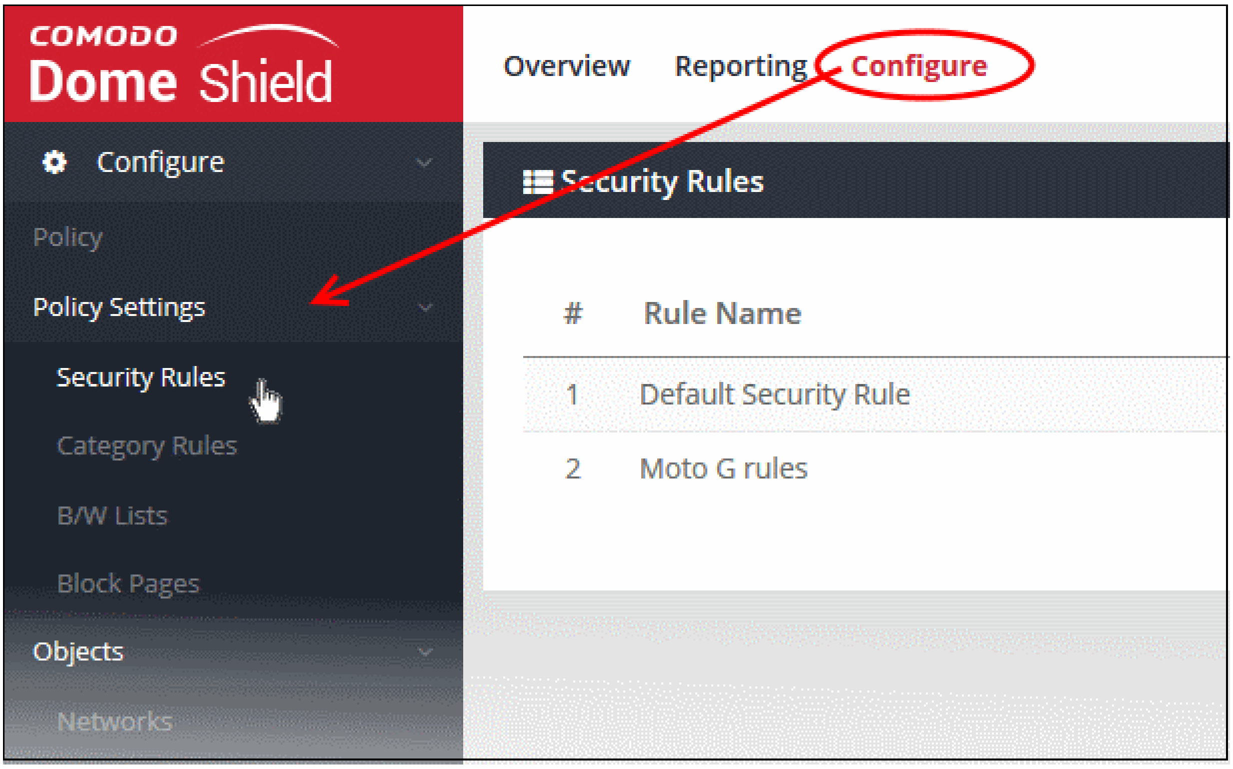
- Manage Security Rules
- Manage Category Rules
- Manage Domain Blacklist and Whitelist
- Manage Block Pages

5.1 Manage Security Rules

Comodo maintains a huge database of harmful websites categorized by threat type. Dome Shield uses this database to power its security rules. To view details about each category, click 'Configure' > 'Policy', then 'Check Domain Category'.

- Security rules let you block access to sites known to host specific types of threat. Security rule categories include:
  - Malware
  - Botnet/c2c Servers/Bot Infected Sources
  - Phishing
  - Spyware
  - Webspam
  - Drive-by Downloads
  - Tor Nodes
  - P2P Nodes
  - Fake AV
  - Blackhole/Sinkhole Systems
  - VPN Servers
  - Mobile Threats
  - Known DDoS Sources
  - Bitcoin Related
  - PUA Domains
  - Remote Access Services
  - Self Signed SSL Sites
  - Domains with no MX records
  - Spam Sources
  - Brute Forcer/Scanner

- 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 new security rules according to your requirements.
- Click 'Configure' > 'Policy Settings' > 'Security Rules' to open the 'Security Rules' area:



#	Rule Name
1	Default Security Rule
2	Moto G rules

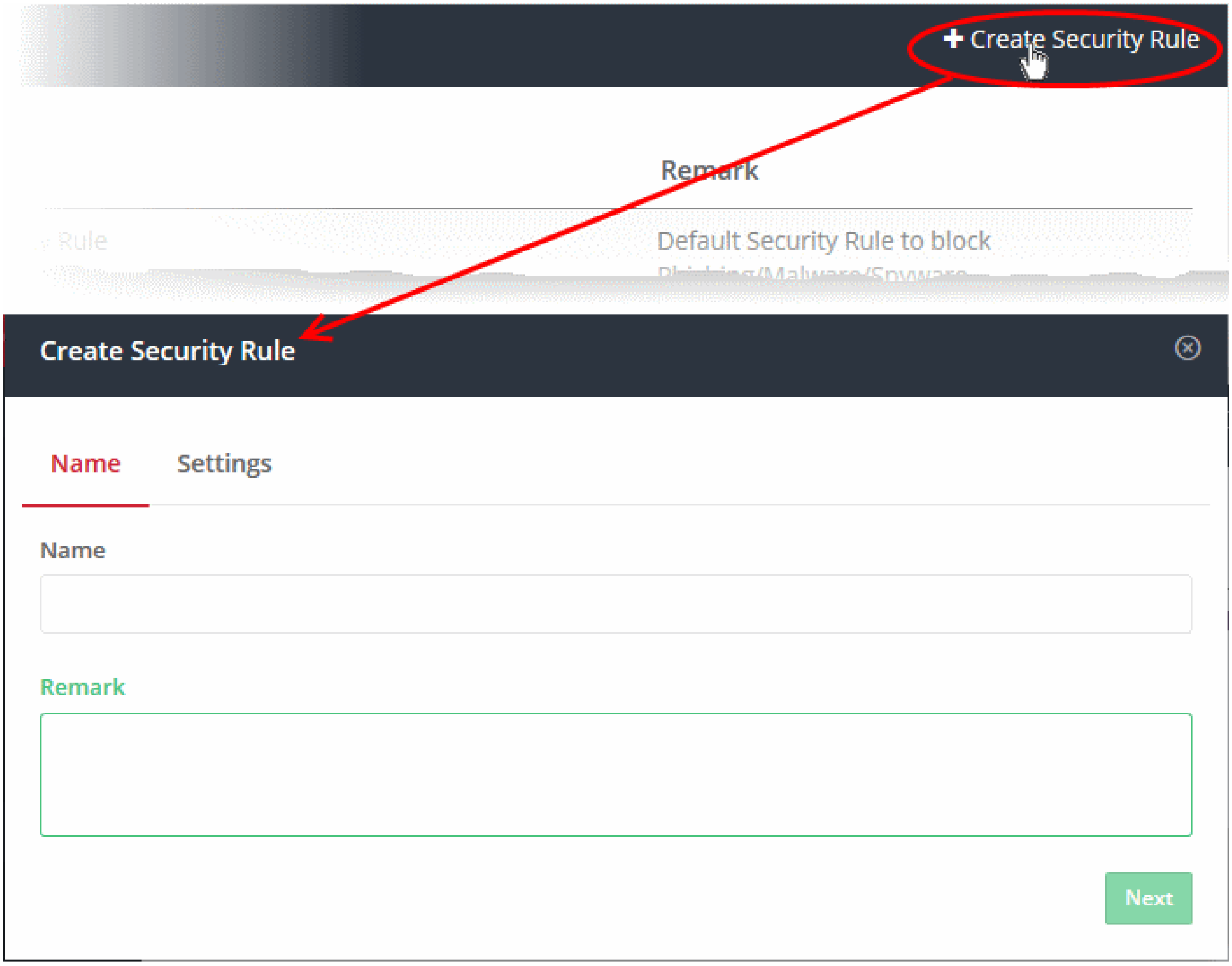
Security Rules - Table of Column Descriptions	
Column Header	**Description**
Rule Name	The name of the rule
Remark	Comments provided for the rule
Actions	Controls to edit / delete the rule

The interface allows you to:

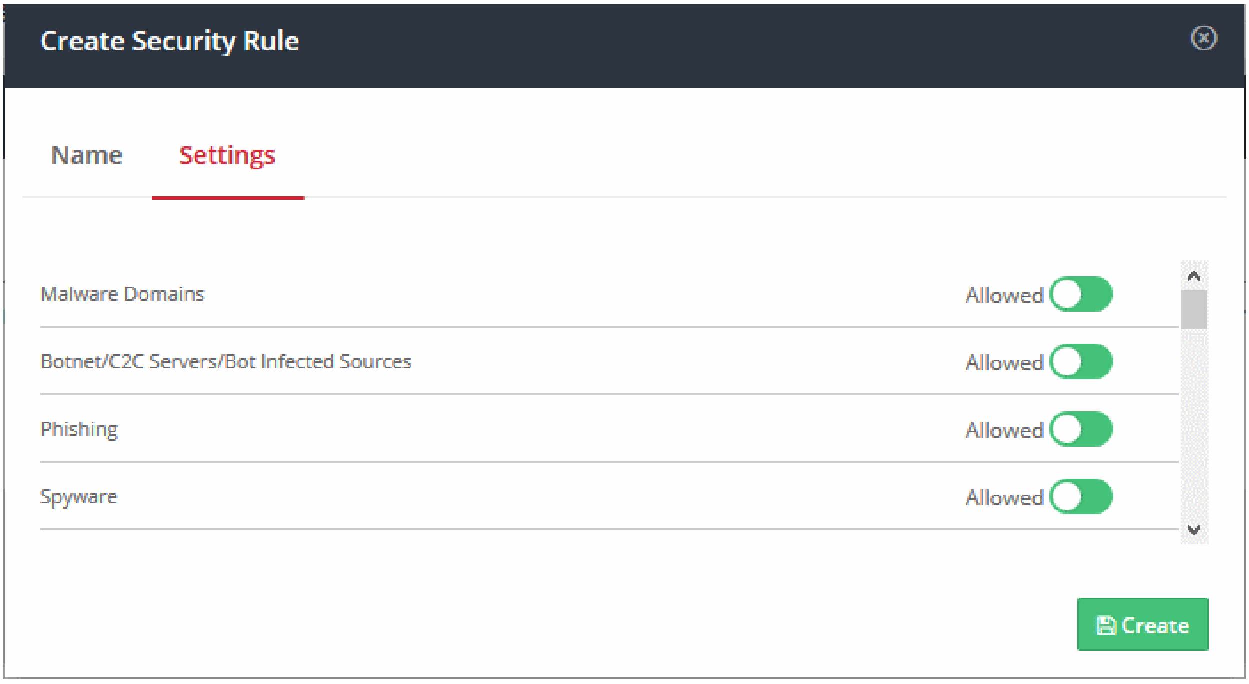
- Create a new security rule
- Edit a security rule
- Delete a security rule

Creating a new security rule

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



- Enter an appropriate name for the rule in the 'Name' field.
- Enter a short description of the rule in the 'Remark' field, if required.
- Click 'Next' or 'Settings' to specify the security categories that you want to allow or block:



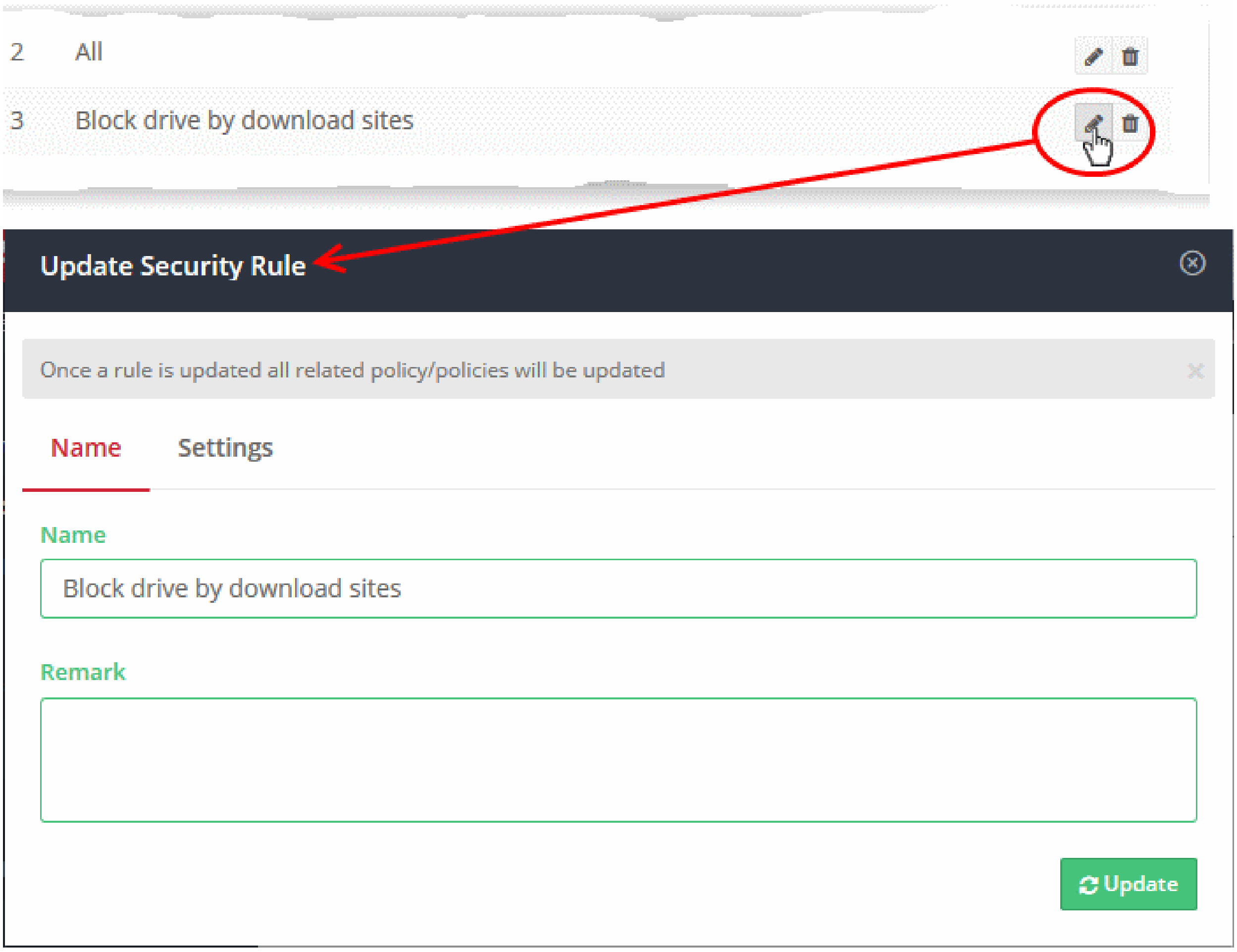
Malware Domains	Allowed
Botnet/C2C Servers/Bot Infected Sources	Allowed
Phishing	Allowed
Spyware	Allowed

- Use the switches on the right to allow or block websites 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.

Editing a security rule

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



2 All

3 Block drive by download sites

Update Security Rule

Once a rule is updated all related policy/policies will be updated

Name: Block drive by download sites

Remark:

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

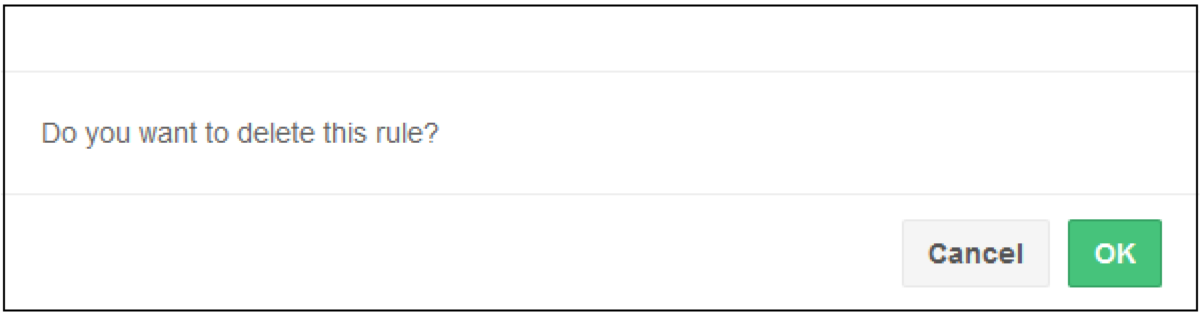
Any policies containing the rule will be updated accordingly.

Deleting a security rule

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

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

A confirmation dialog will be displayed:

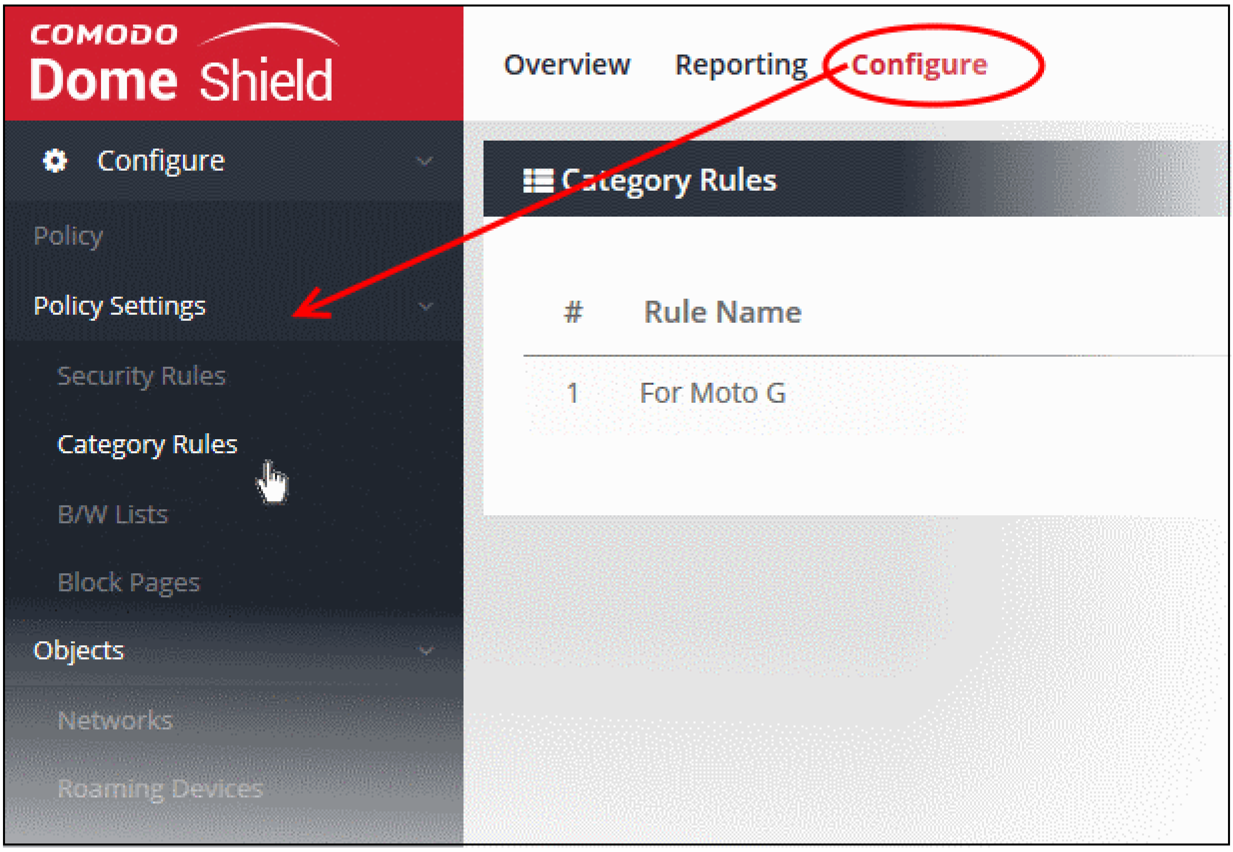


Do you want to delete this rule?

- 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.
- Unlike security rules which focus specifically on harmful websites, '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 name of the rule
Remark	Comments provided for the rule
Actions	Controls to edit / delete the rule

Related information:

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

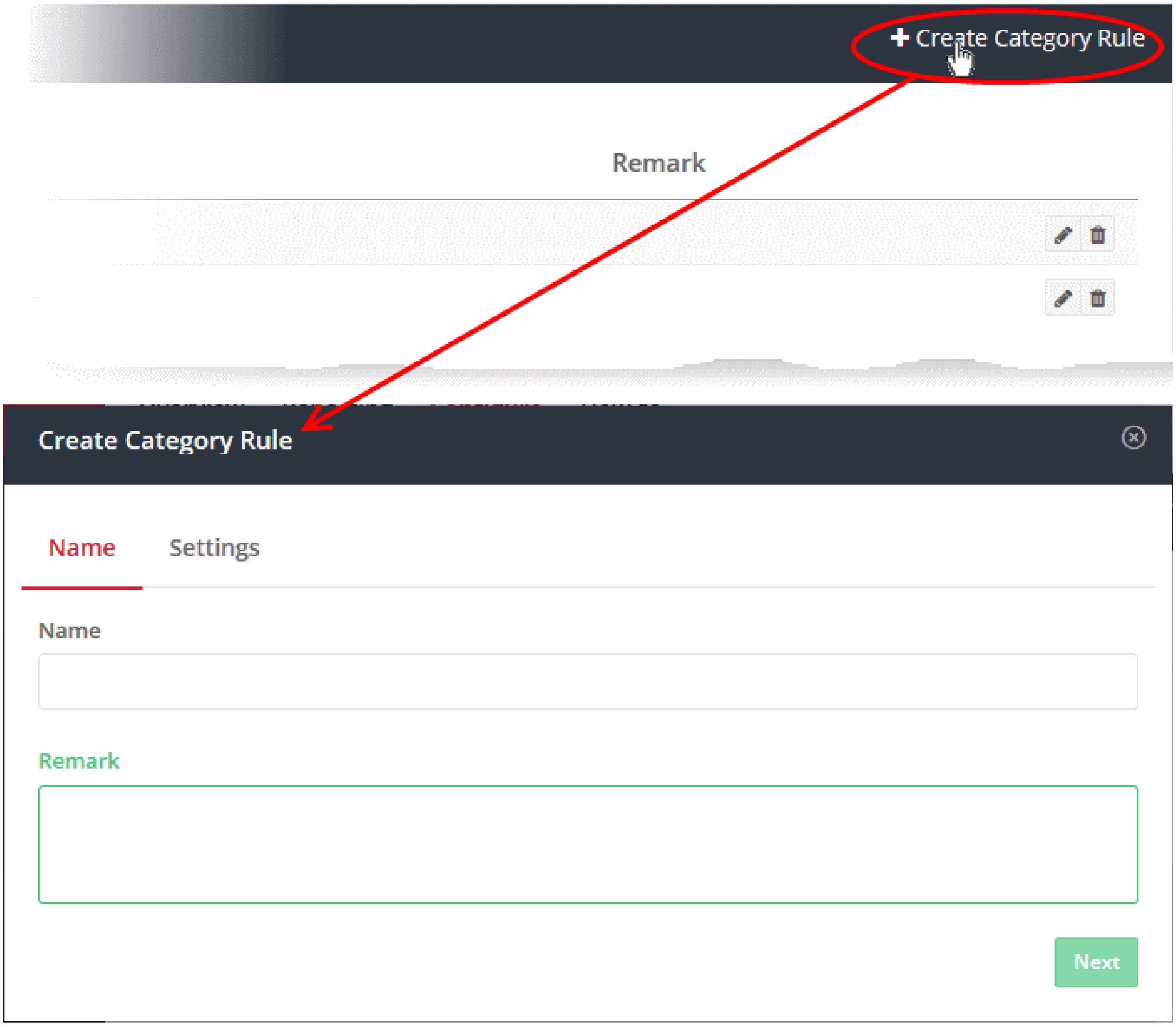
The category rules area lets you:

- Create a new category rule

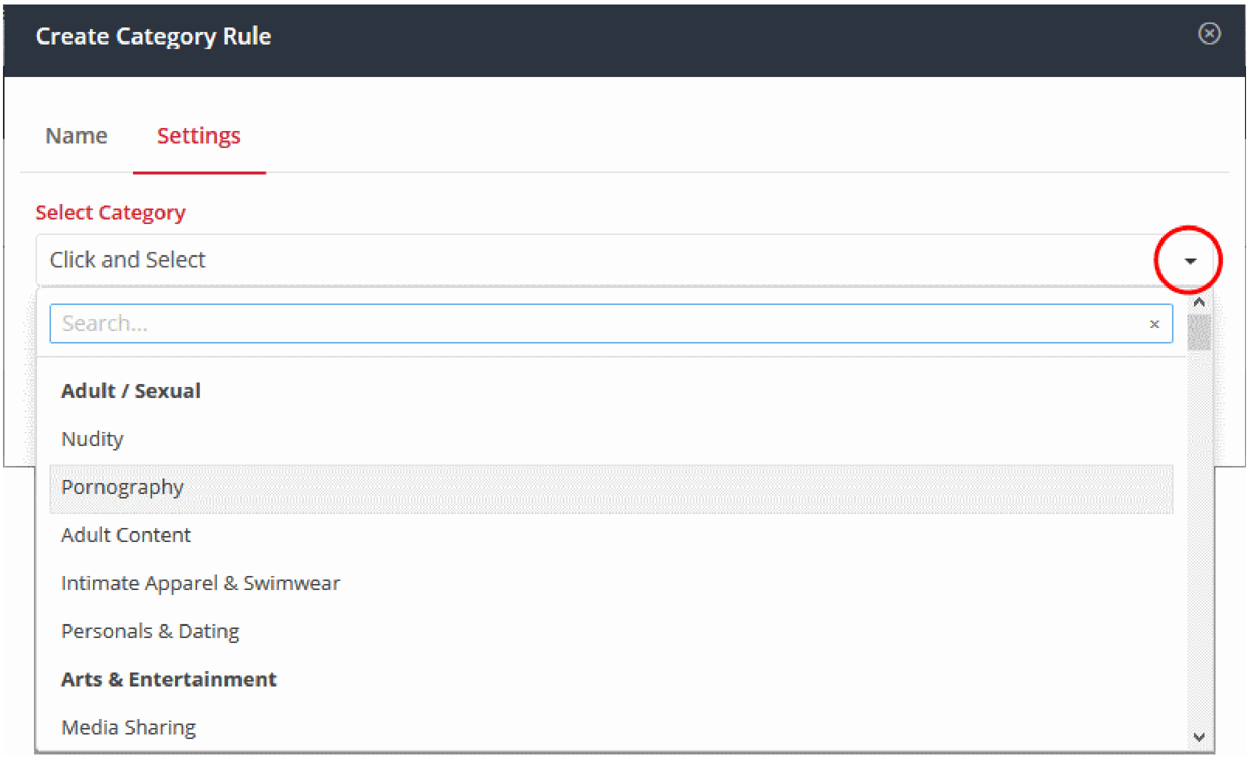
- Edit a category rule
- Delete a category rule

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:



Create Category Rule

Name | Settings

Select Category

Click and Select

Search...

Adult / Sexual

Nudity

Pornography

Adult Content

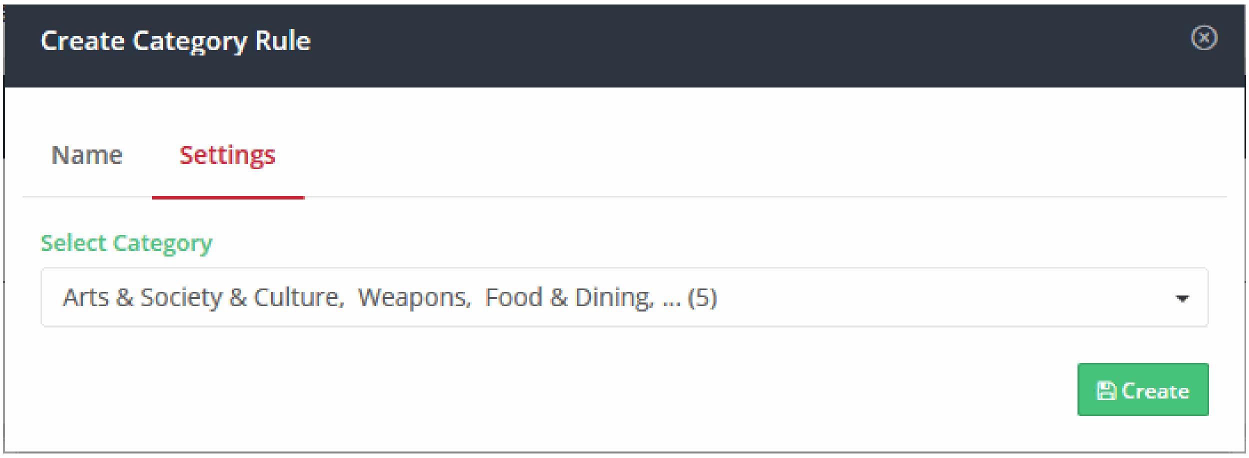
Intimate Apparel & Swimwear

Personals & Dating

Arts & Entertainment

Media Sharing

- 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:



Create Category Rule

Name | Settings

Select Category

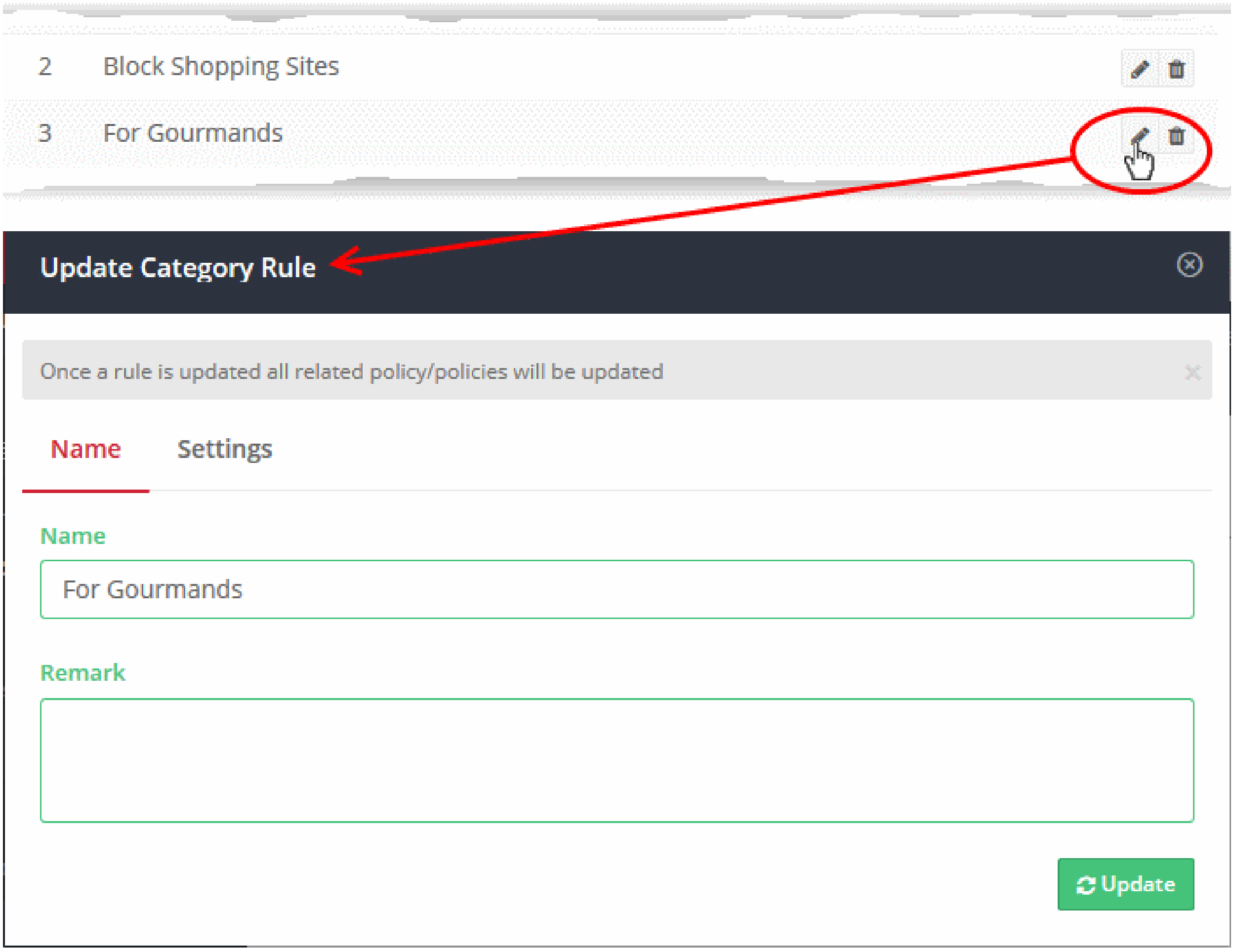
Arts & Society & Culture, Weapons, Food & Dining, ... (5)

- 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:



2 Block Shopping Sites

3 For Gourmands

Update Category Rule

Once a rule is updated all related policy/policies will be updated

Name: For Gourmands

Remark:

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

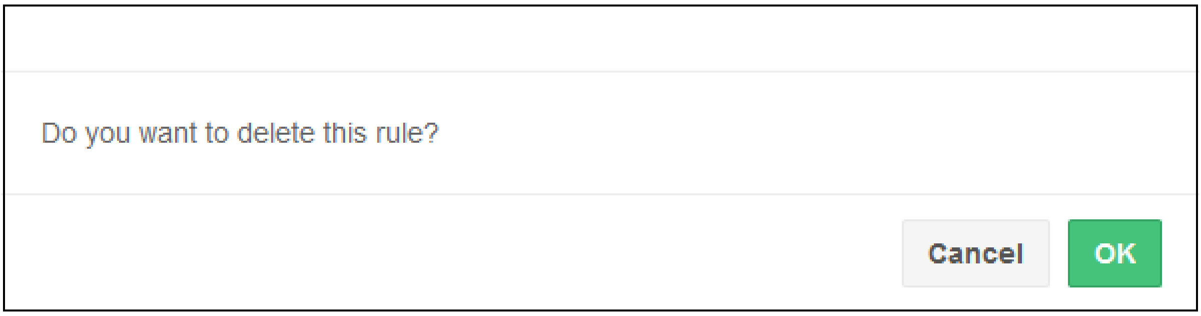
Any policies which use this rule will be updated accordingly.

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.



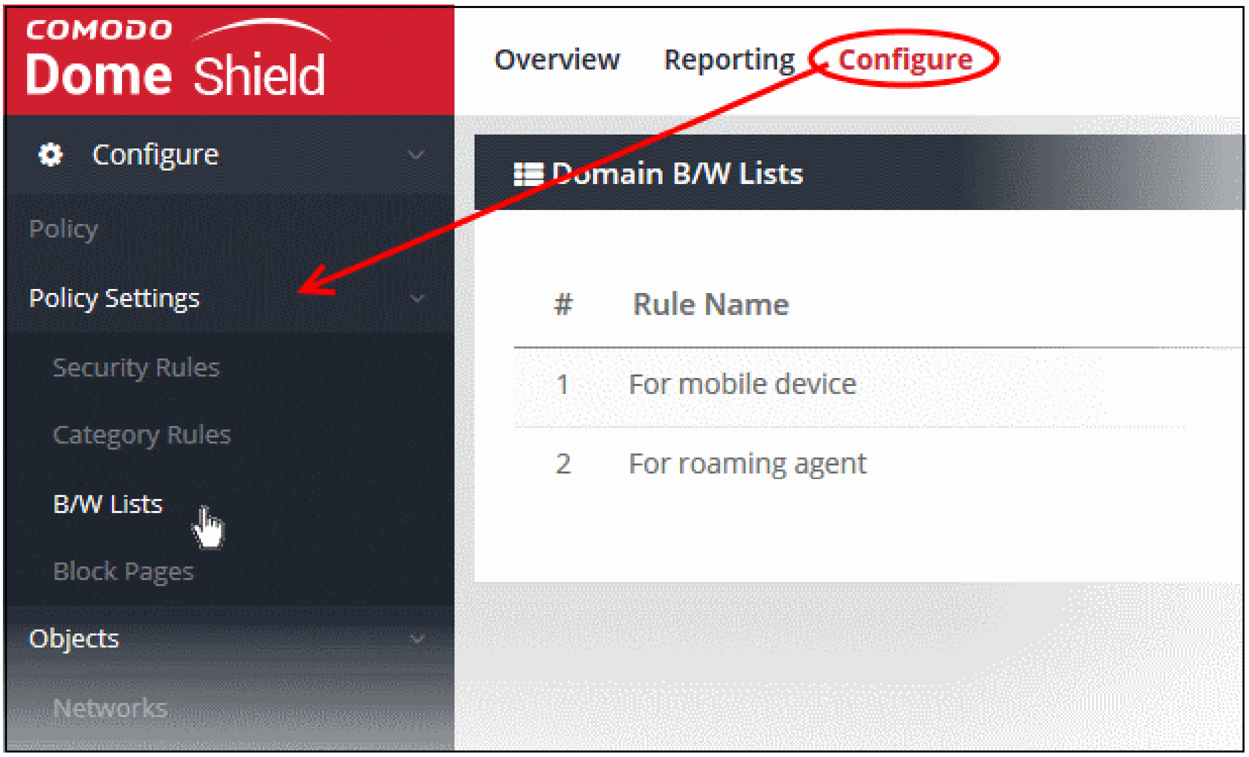
Do you want to delete this rule?

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

5.3 Manage Domain Blacklist and Whitelist

Black and white lists let you specify access privileges to 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. For example, if you block shopping sites in a category rule but decide to white-list 'example-shop.com', then 'example-shop.com' will be allowed.
- If you enable 'Only B/W Mode' when configuring a policy then only the black and white lists in the policy will be consulted. All security and category rules will be ignored.
- Click 'Configure' > 'Policy Settings' > 'B/W Lists' to open the 'B/W Lists' area:



Domain B/W Lists

#	Rule Name
1	For mobile device
2	For roaming agent

The list of B/W list rules will be displayed.

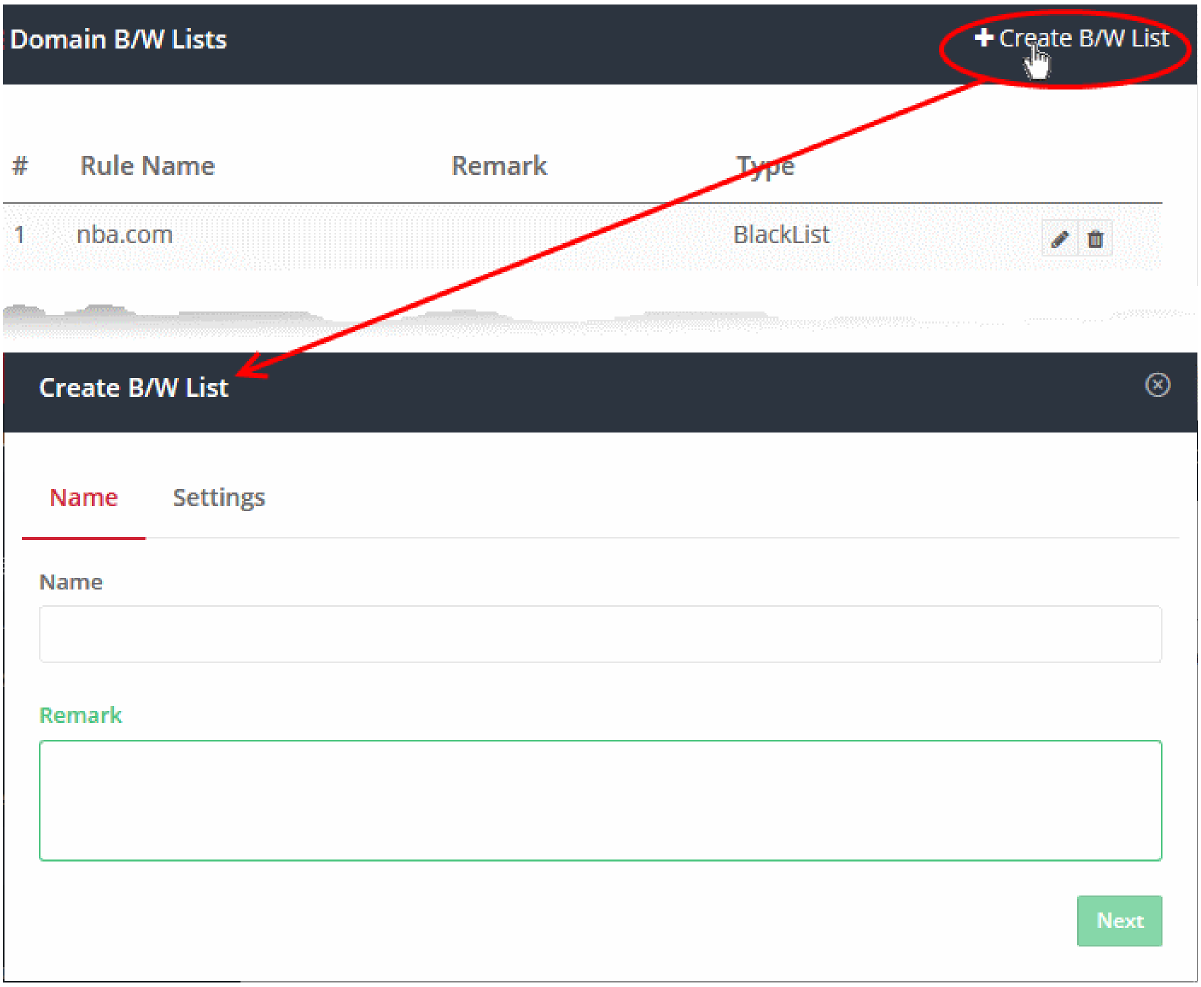
Domain B/W Lists - Table of Column Descriptions	
Column Header	**Description**
Rule Name	The name of the domain B/W list
Remark	Comments provided for the rule
Type	Indicates whether the rule is categorized as Whitelist or Blacklist
Actions	Controls to edit / delete the rule

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



Domain B/W Lists

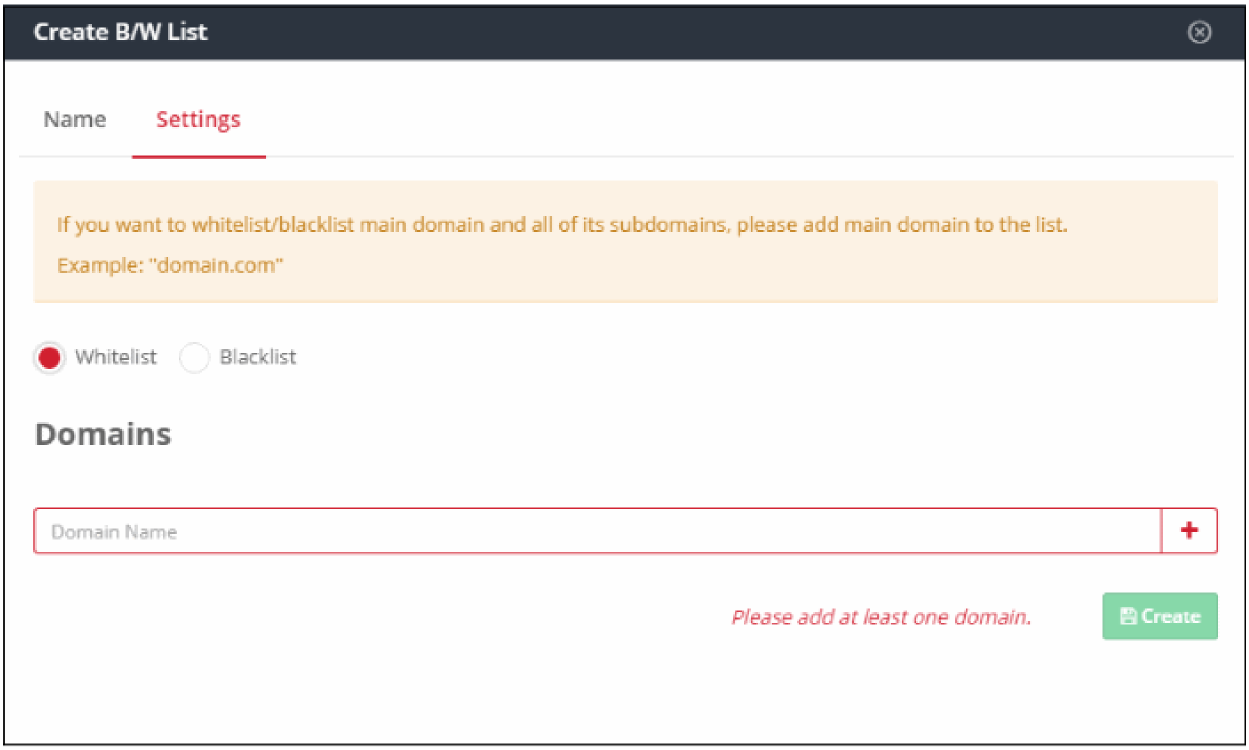
#	Rule Name	Remark	Type
1	nba.com		BlackList

Create B/W List

Name

Remark

- 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.



Create B/W List

Name Settings

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

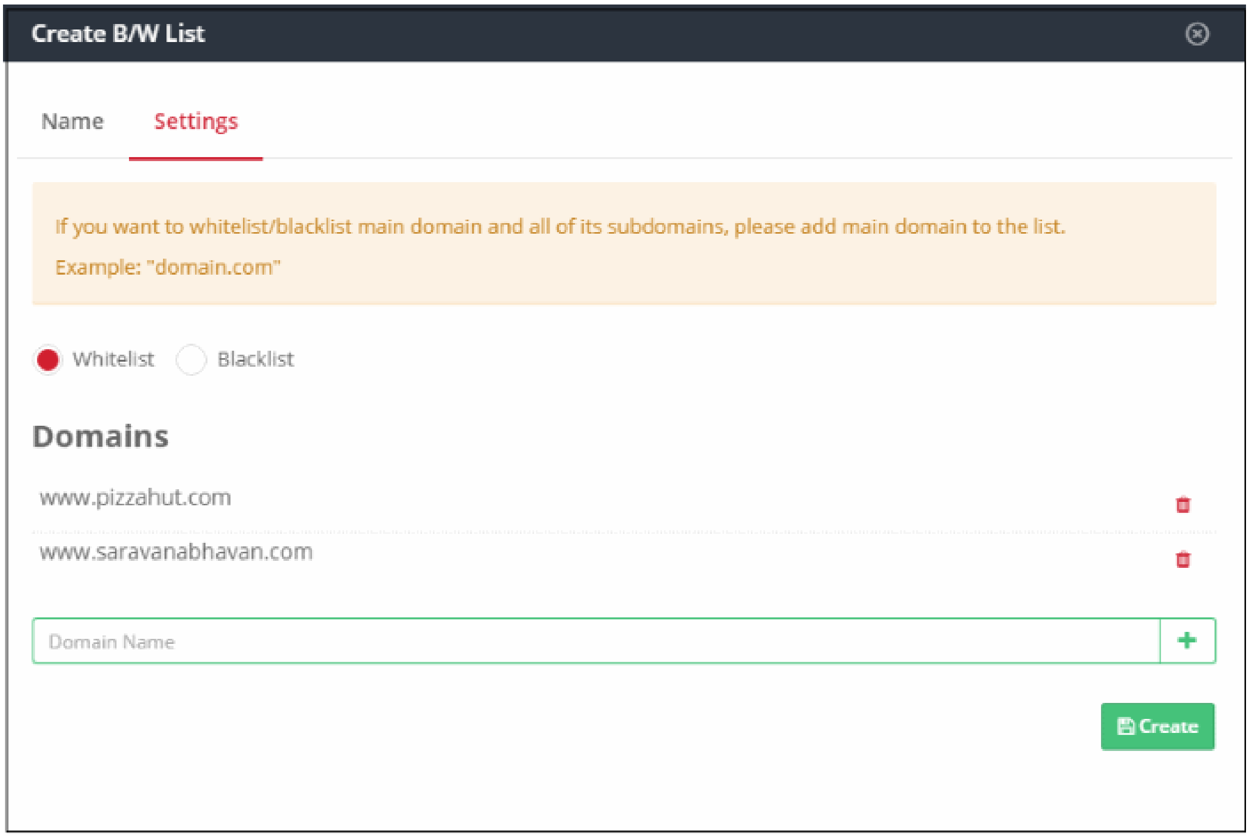
● Whitelist ○ Blacklist

Domains

Domain Name +

Please add at least one domain.

- Select 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.



Create B/W List

Name Settings

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

● Whitelist ○ Blacklist

Domains

www.pizzahut.com

www.saravanabhavan.com

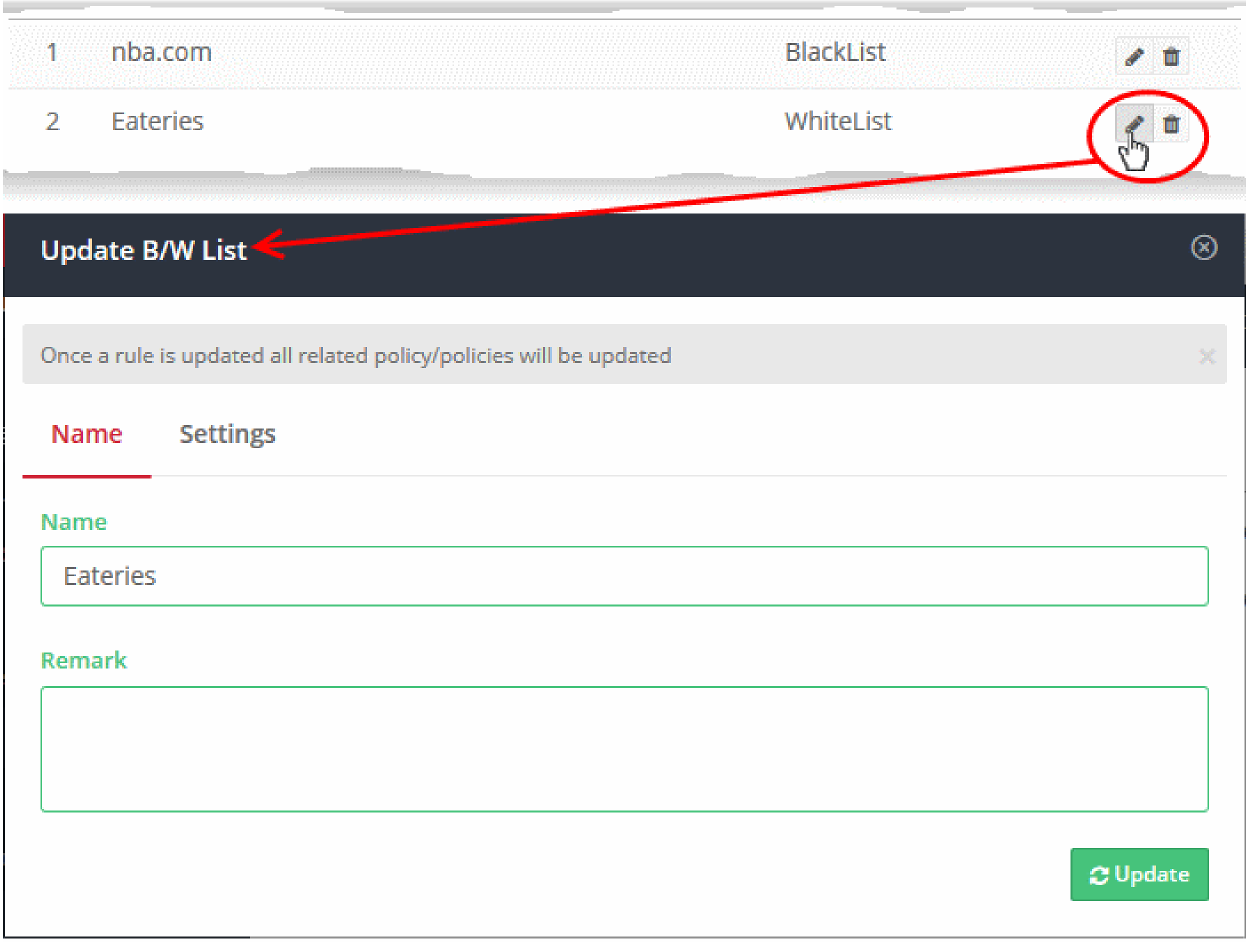
Domain Name +

- 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



1	nba.com	BlackList	✎ 🗑
2	Eateries	WhiteList	✎ 🗑

Update B/W List

Once a rule is updated all related policy/policies will be updated

Name: Eateries

Remark:

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.

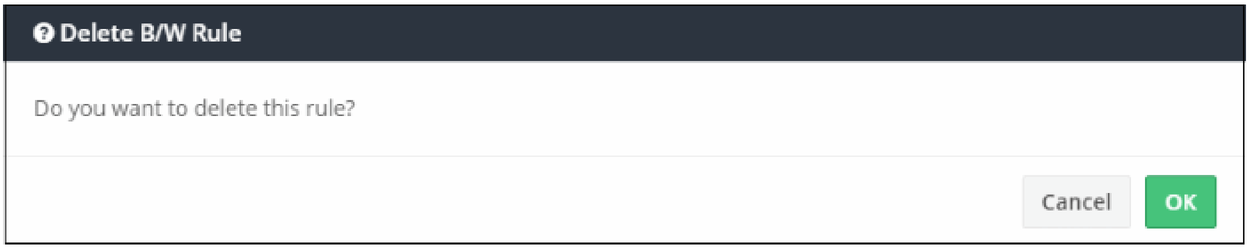
Please note that the policy/policies containing the B/W list will also be updated according to the new settings and name.

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.



Delete B/W Rule

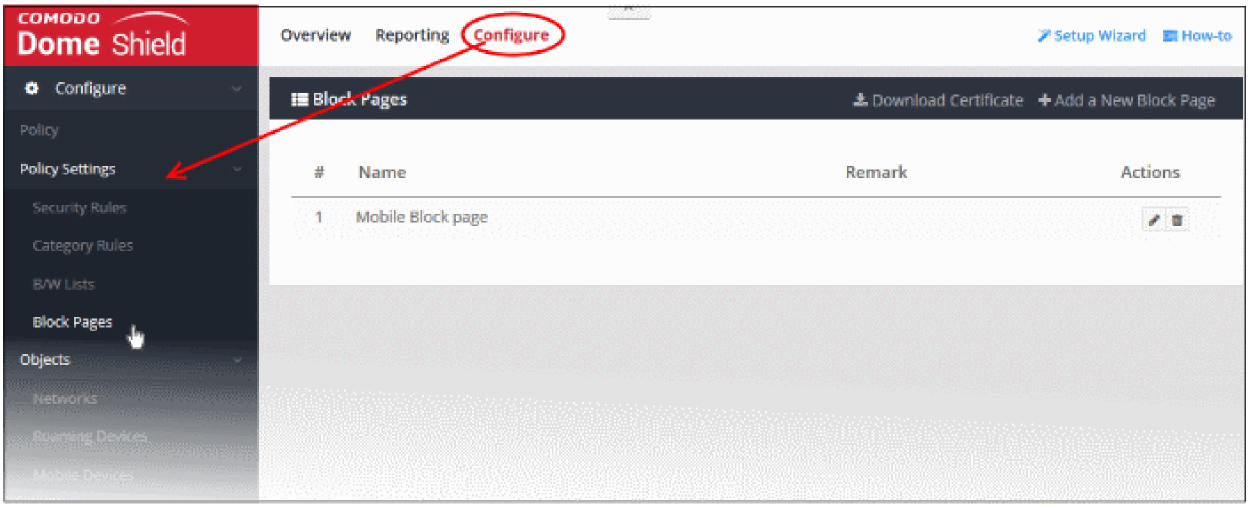
Do you want to delete this rule?

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

5.4 Manage Block Pages

'Block' pages are shown to end-users when they attempt to visit a site that is blocked 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 message(s) with your custom banner(s)
  - Redirect users to a specific web-page
- You can download an SSL/TLS certificate for the block page which should be installed on your protected endpoints. This will avoid errors being shown on endpoint browsers when a HTTPS website is blocked.
- Click 'Configure' > 'Policy Settings' > 'Block Pages' to open the 'Block Pages' area:



#	Name	Remark	Actions
1	Mobile Block page		

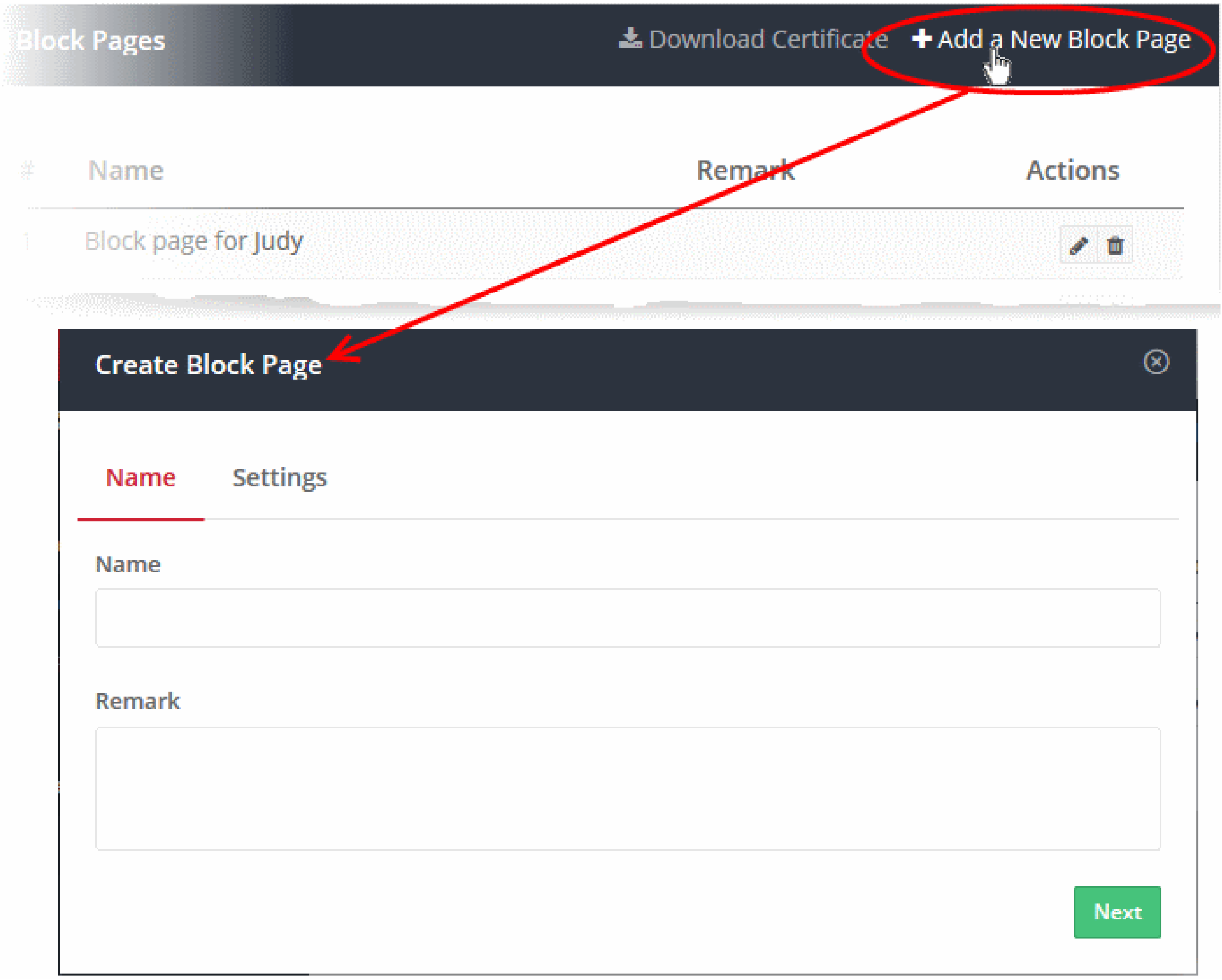
Block Pages - Table of Column Descriptions	
Column Header	**Description**
Name	The name of the block page
Remark	Comments provided for the page
Actions	Controls to edit / delete the block page

The following sections explain how to:

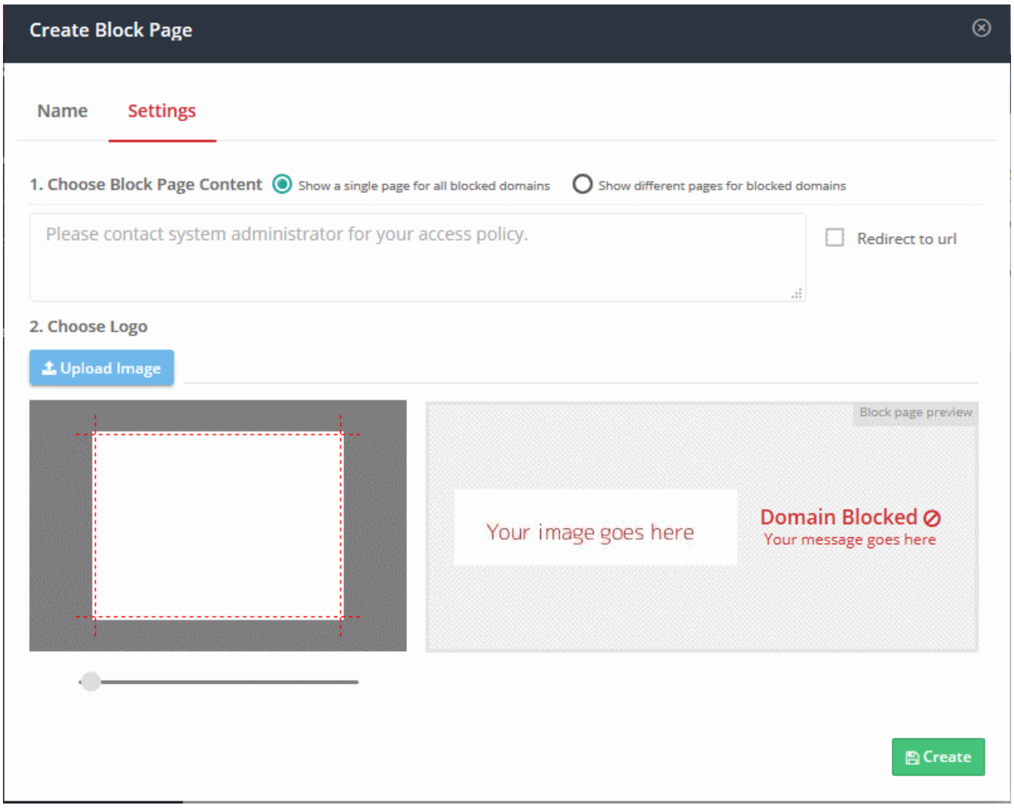
- Create a new block page
- Install an SSL certificate for block pages
- Edit a block page
- Delete a block page

Create a Block Page

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



- Enter a descriptive name for the block page in the 'Name' field.
- Use the 'Remark' field to leave internal notes about the page if required. Text you leave here will not be shown in the block page itself.
- Click 'Next' or 'Settings' to configure the block page



Create Block Page

Name | Settings

1. Choose Block Page Content ● Show a single page for all blocked domains ○ Show different pages for blocked domains

Please contact system administrator for your access policy.

□ Redirect to url

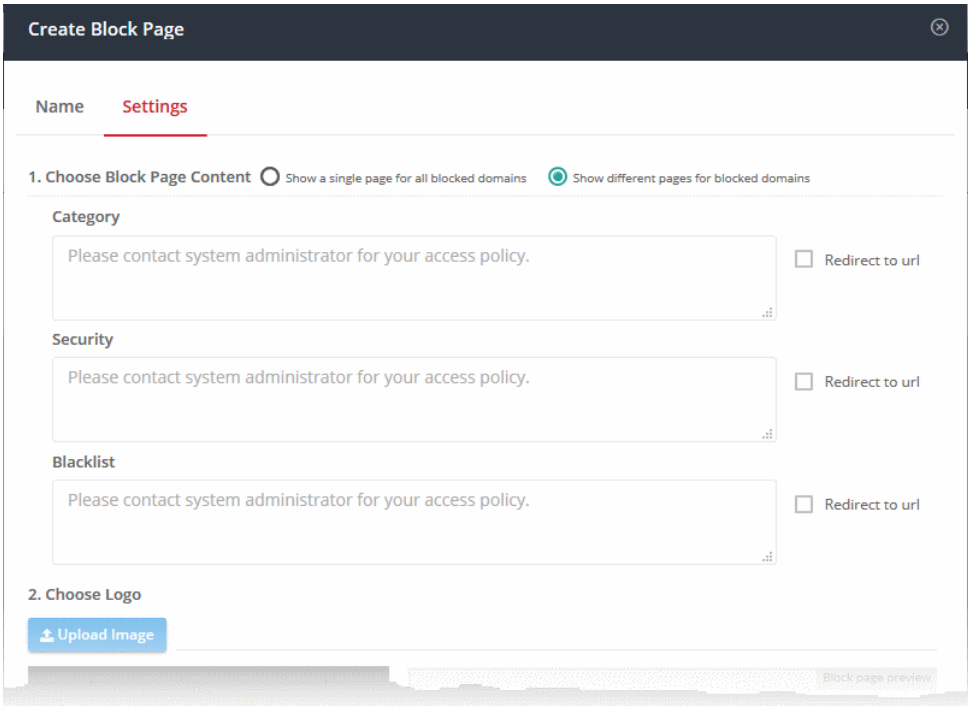
2. Choose Logo

You 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 a specific block page if a certain type of rule is violated. You can show different pages for category rule breaches, security rule breaches and blacklist rule breaches:



Create Block Page

Name | Settings

1. Choose Block Page Content ○ Show a single page for all blocked domains ● Show different pages for blocked domains

Category

Please contact system administrator for your access policy.

□ Redirect to url

Security

Please contact system administrator for your access policy.

□ Redirect to url

Blacklist

Please contact system administrator for your access policy.

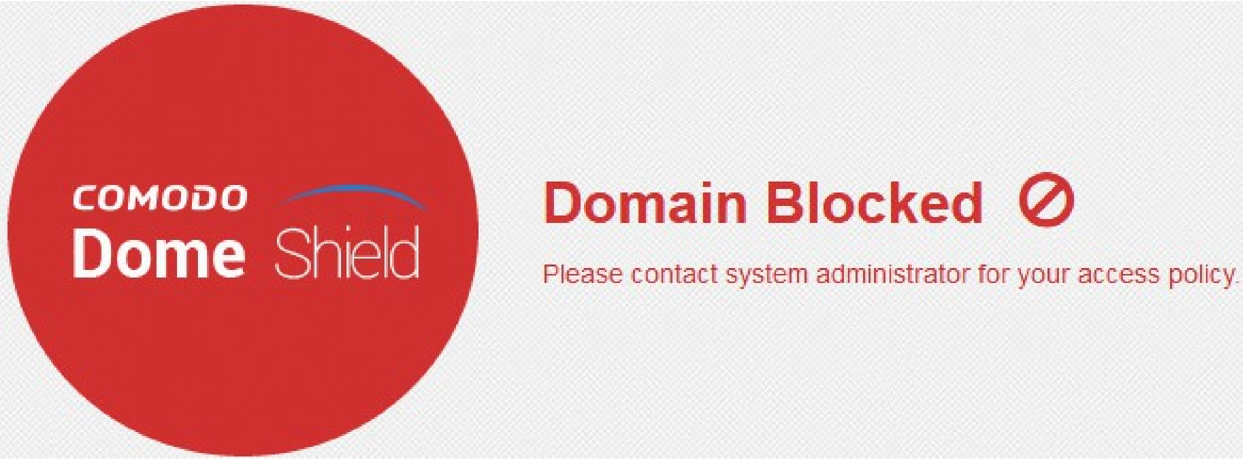
□ Redirect to url

2. Choose Logo

- You can type a custom message in the text box 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

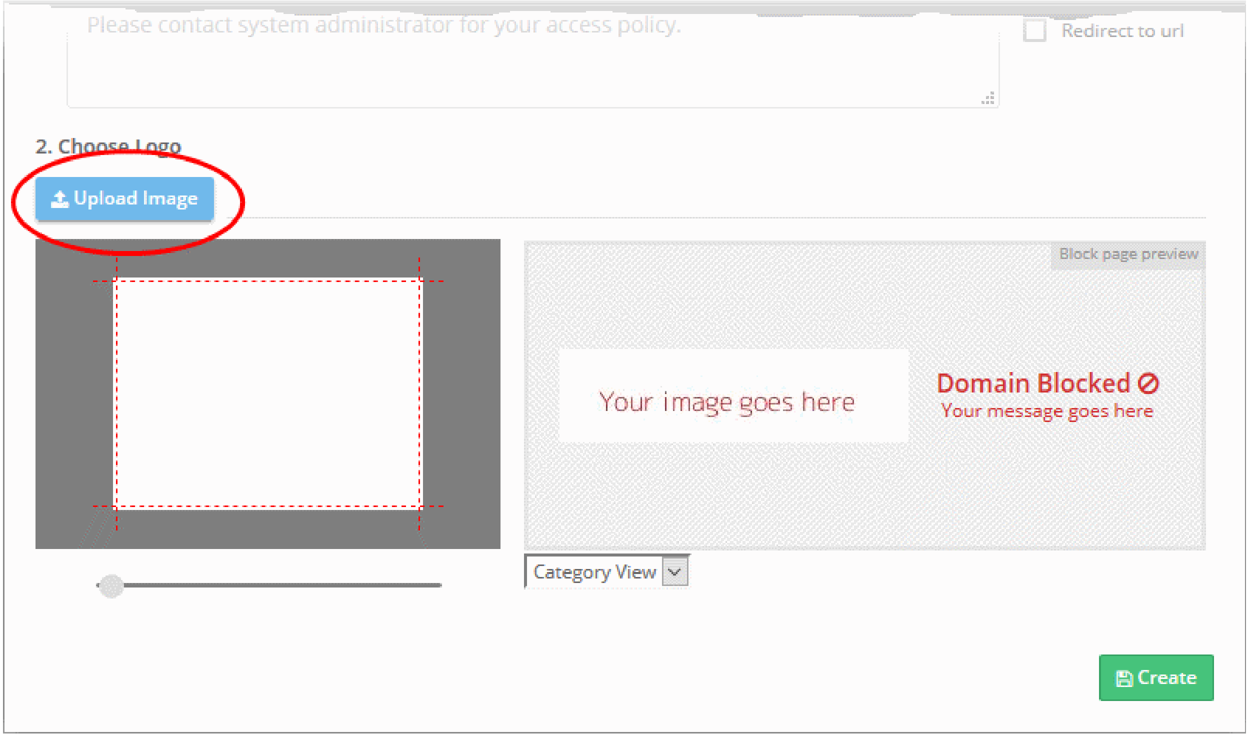
- The interface shows the Dome Shield logo on the block page by default.
- You can change this to your own company logo by uploading a suitable .png or .svg file



Domain Blocked

Please contact system administrator for your access policy.

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



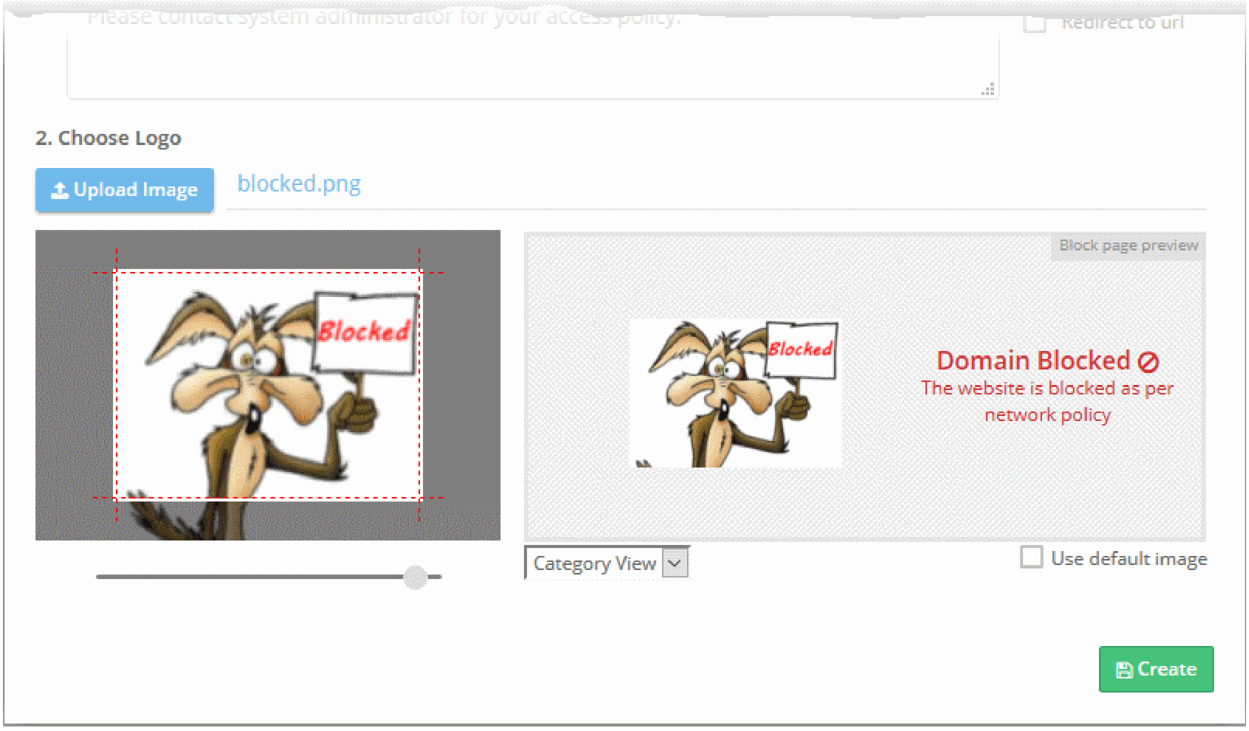
Please contact system administrator for your access policy.

□ Redirect to url

2. Choose Logo

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

Your image will appear on the left:



Please contact system administrator for your access policy.

□ Redirect to url

2. Choose Logo

blocked.png

Domain Blocked ⊘

The website is blocked as per network policy

□ Use default image

- 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 separate block pages for security, category and blacklist rules (if you opted for different pages for each).
- To use the default Dome Shield logo, select 'Use default image'
- Click 'Create'

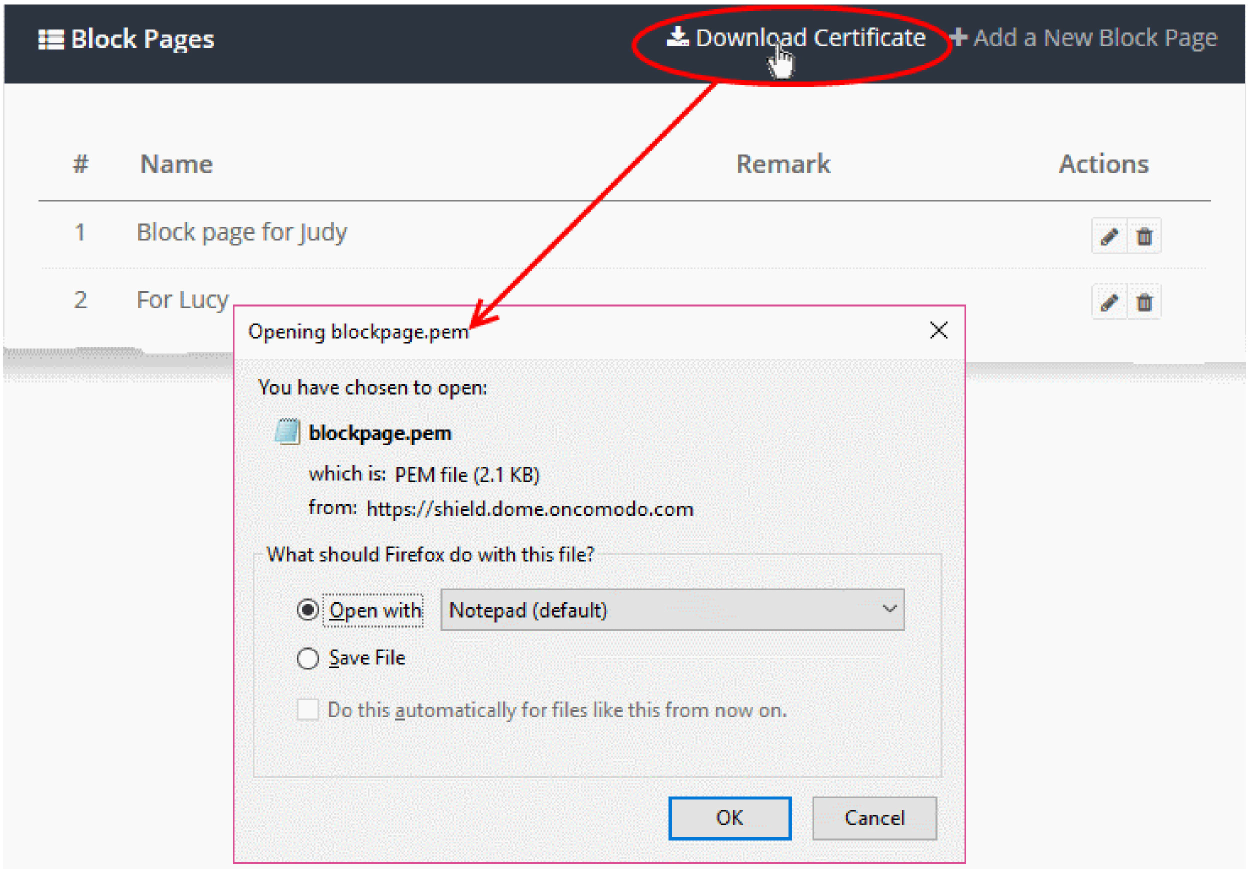
The block page will be added to the list and will be available for selection while creating a policy.

Install SSL certificate for block pages

Browsers on endpoint computers may show errors when some HTTPS enabled webpages are blocked by Dome Shield. You can avoid the error messages by installing the block page certificate on all protected endpoints.

To download the certificate

- Click 'Configure' > 'Policy Settings' > 'Block Pages' on the left:
- Click 'Download Certificate' at the top right



Opening blockpage.pem

You have chosen to open:

blockpage.pem

which is: PEM file (2.1 KB)

from: https://shield.dome.oncomodo.com

What should Firefox do with this file?

● Open with Notepad (default)

○ Save File

□ Do this automatically for files like this from now on.

The certificate will be downloaded in .pem format.

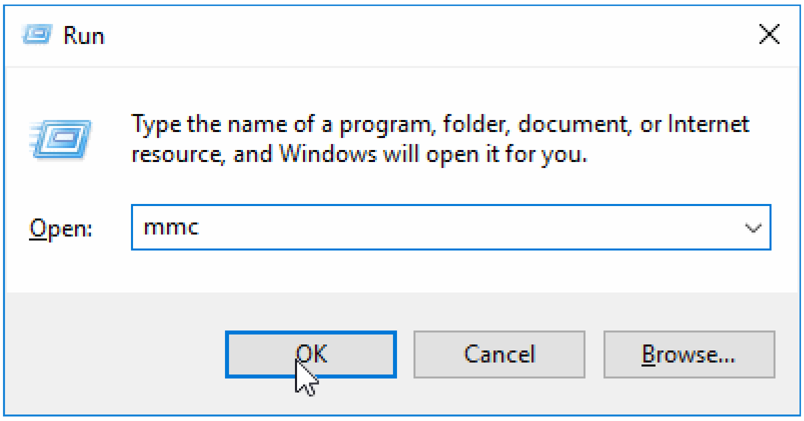
- Distribute the file to the endpoints and install on them.

There are two steps to install the certificate on endpoints:

- Step 1 - Add 'Certificates' snap-in to Microsoft Management Console (MMC) (If you haven't done already)
- Step 2 - Import the block page certificate to 'Trusted Root Certification Authorities' store

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

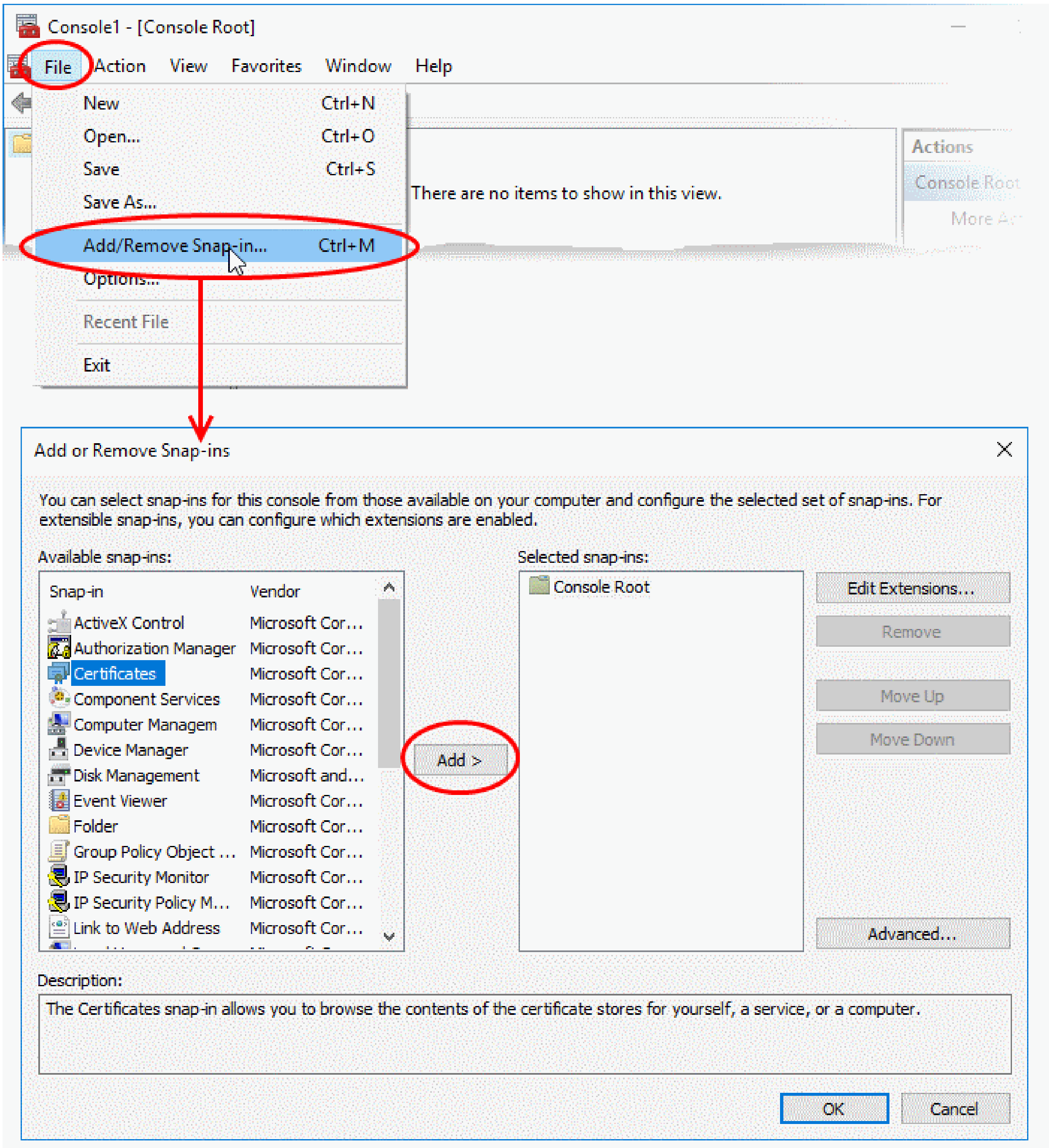
- Open the MMC - Enter 'mmc' in the 'Run' dialog ('Win' key + 'R'):



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

- Click 'File' > 'Add/Remove snap-in' in the console interface



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

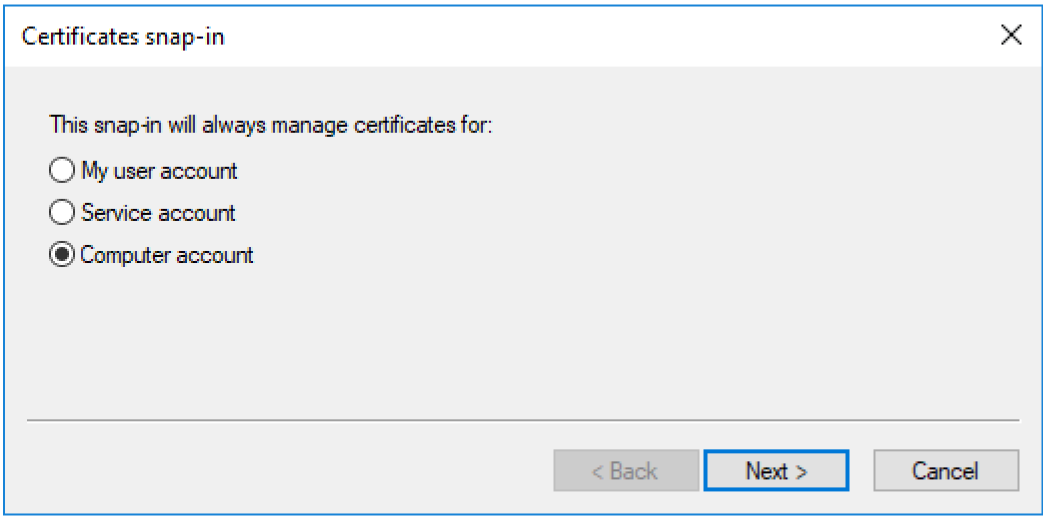
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

The 'Add or Remove Snap-ins' panel will open.

- Select 'Certificates' from the list of available snap-ins on the left pane and click 'Add' to add it to the list of selected snap-ins on the right pane.

The next step allows you to select the account for which the snap-in to be added.



Certificates snap-in

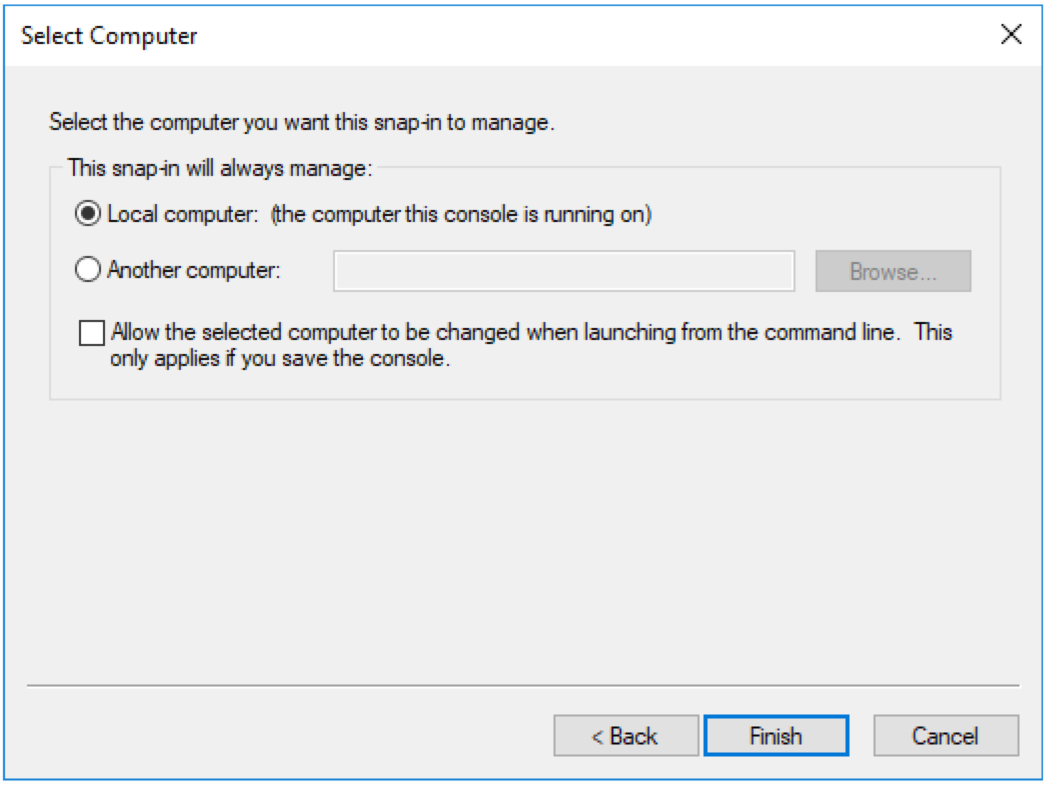
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

- Select 'Computer account' and click 'Next'
- The next step requires you to select the computer in the network in which the snap-in is to be added,



Select Computer

Select the computer you want this snap-in to manage.

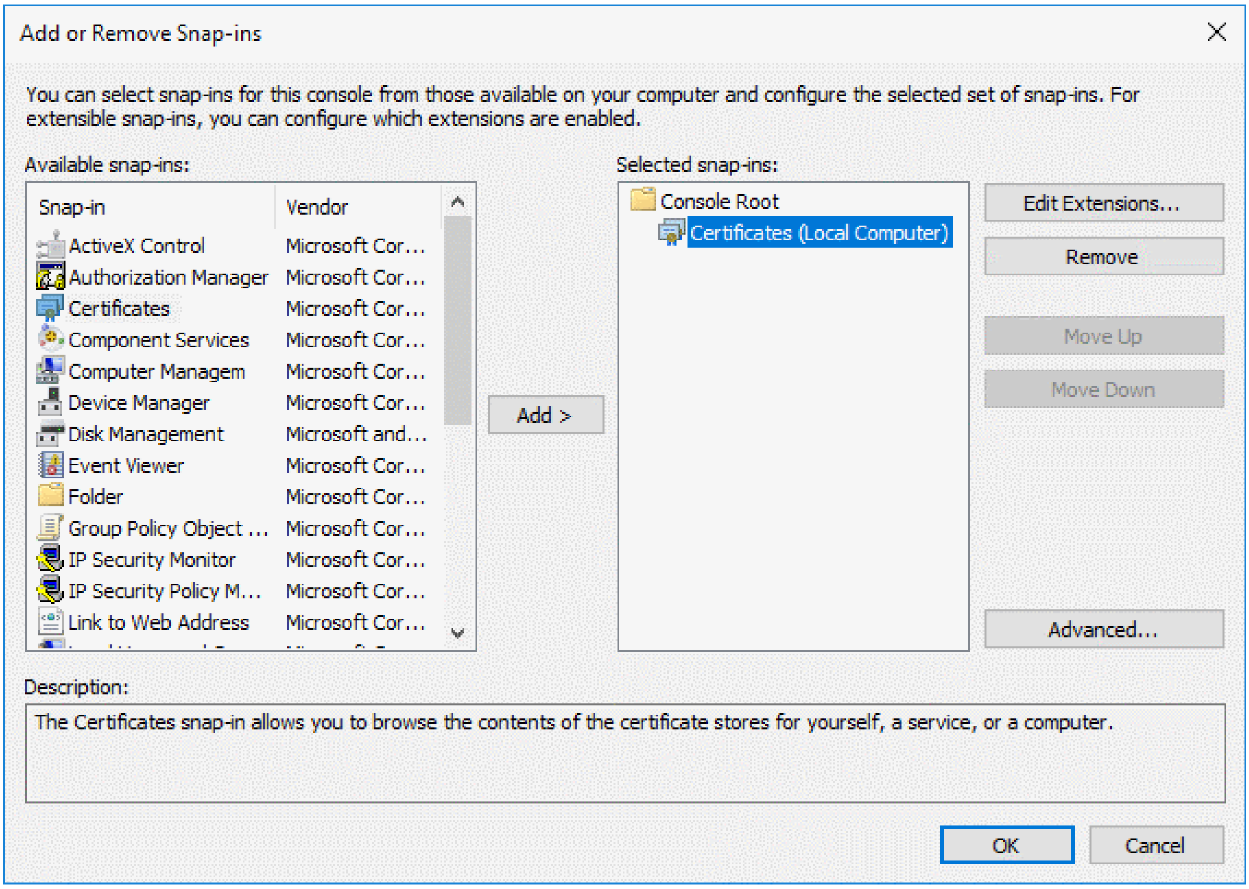
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

- Select 'Local computer' and click 'Finish'
- The snap-in will be added to the list on the right



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root
- Certificates (Local Computer)

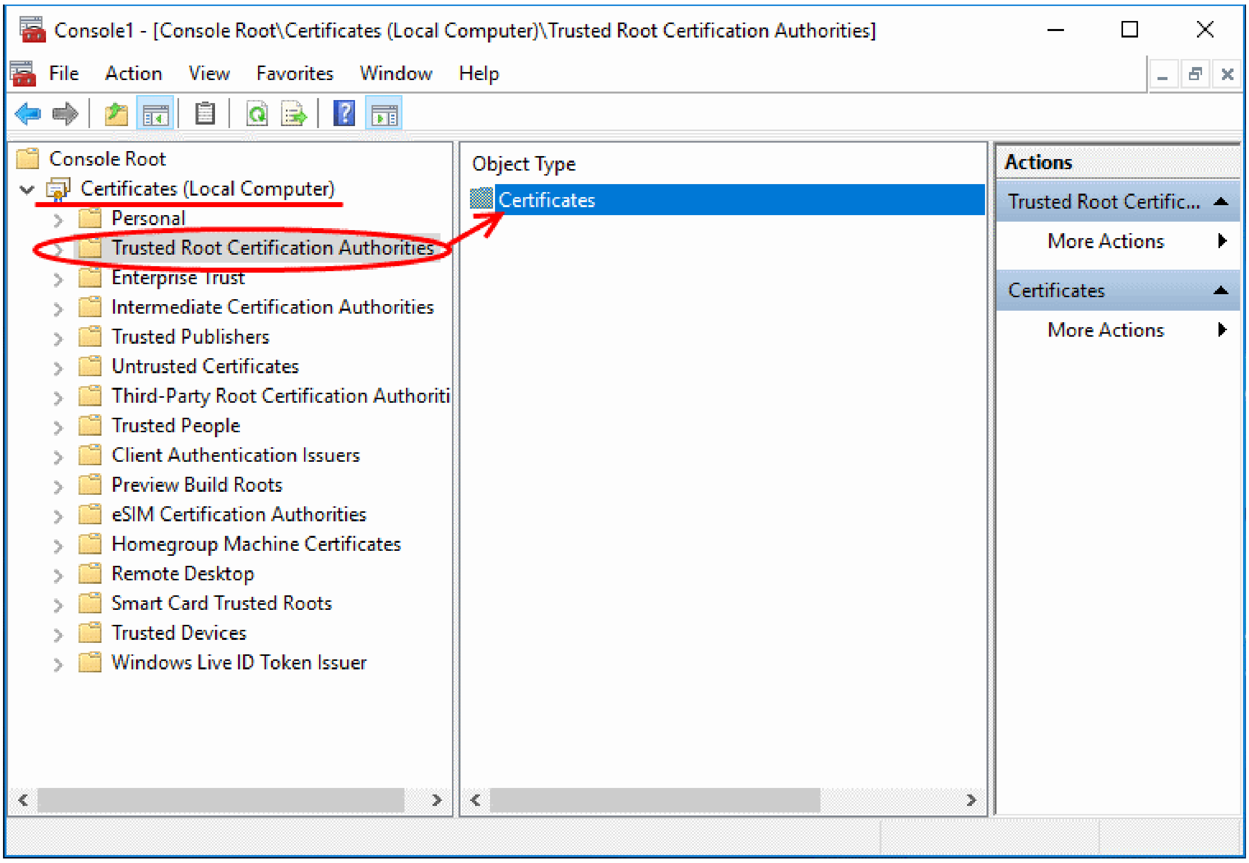
Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

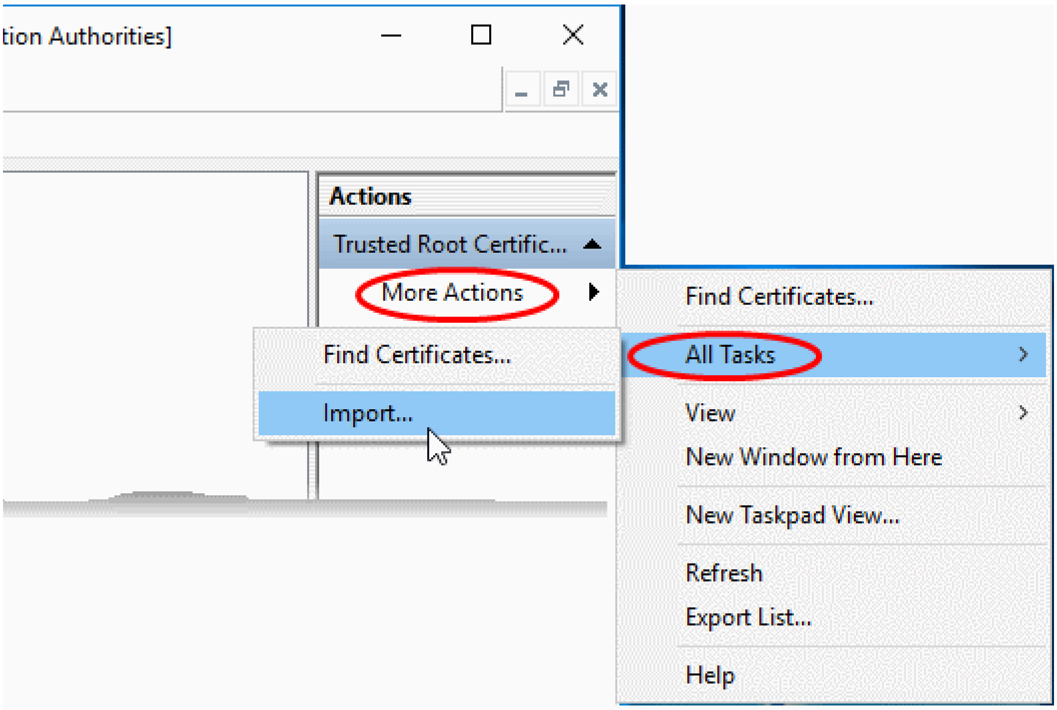
- Click 'OK' to add the snap-in to the console.

Step 2 - Import the block page certificate to 'Trusted Root Certification Authorities' store

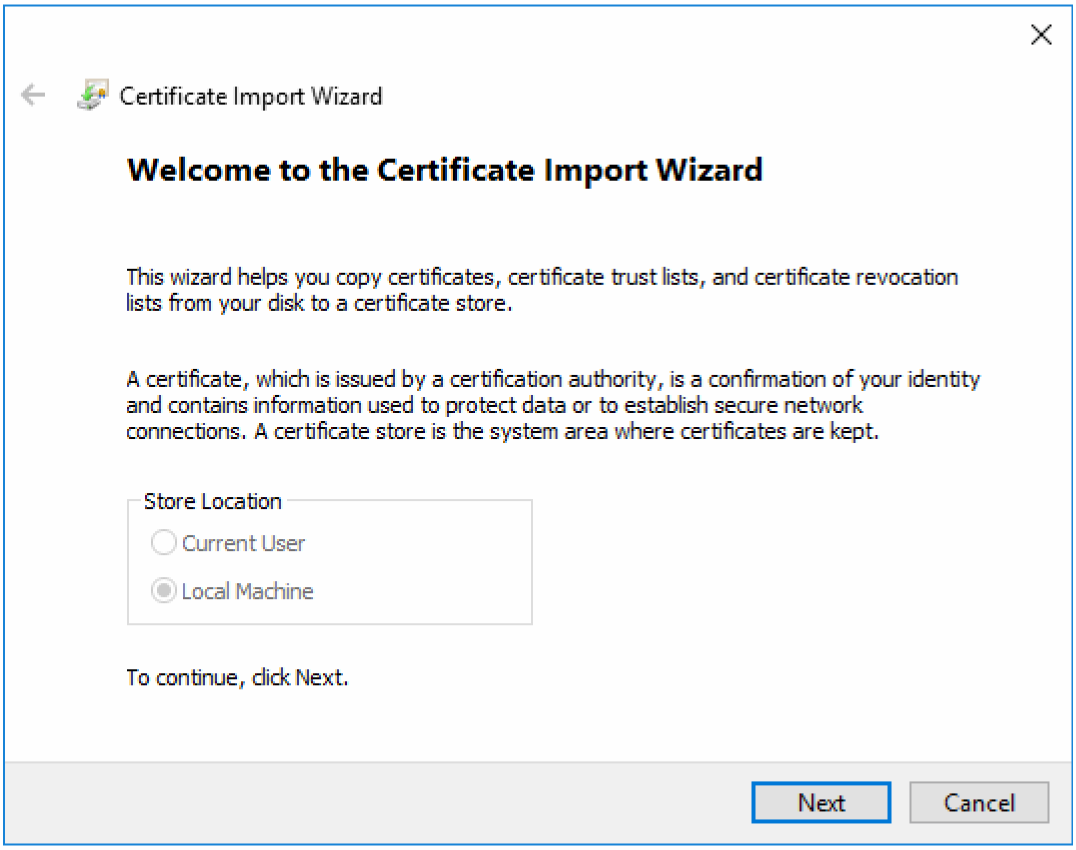
- Expand the 'Certificates' tree on the left in the MMC console
- Select 'Trusted Root Certification Authorities' folder under 'Certificates (Local Computer)'


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Preview Build Roots
eSIM Certification Authorities
Homegroup Machine Certificates
Remote Desktop
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
Object Type
Certificates
Actions
Trusted Root Certific...
More Actions
Certificates
More Actions

- Click 'More Actions' under 'Actions' > 'Trusted Root Certificates' on the right pane then choose 'All Tasks' > 'Import'



The 'Certificate Import wizard' will start



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

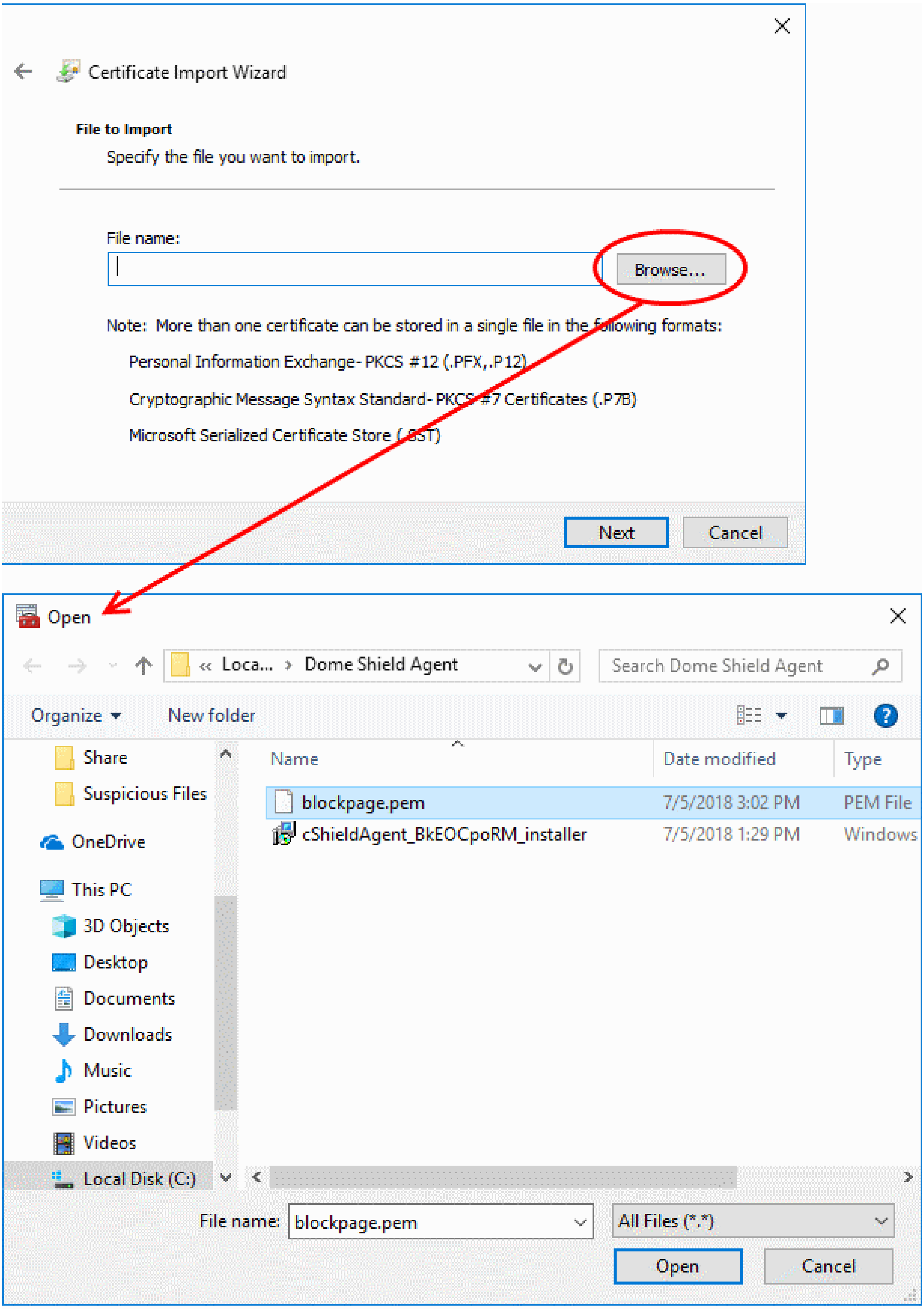
○ Current User

● Local Machine

To continue, click Next.

- Click 'Next' to continue

The next step is to select the certificate to be imported.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Open

Name	Date modified	Type
blockpage.pem	7/5/2018 3:02 PM	PEM File
cShieldAgent_BkEOCpoRM_installer	7/5/2018 1:29 PM	Windows

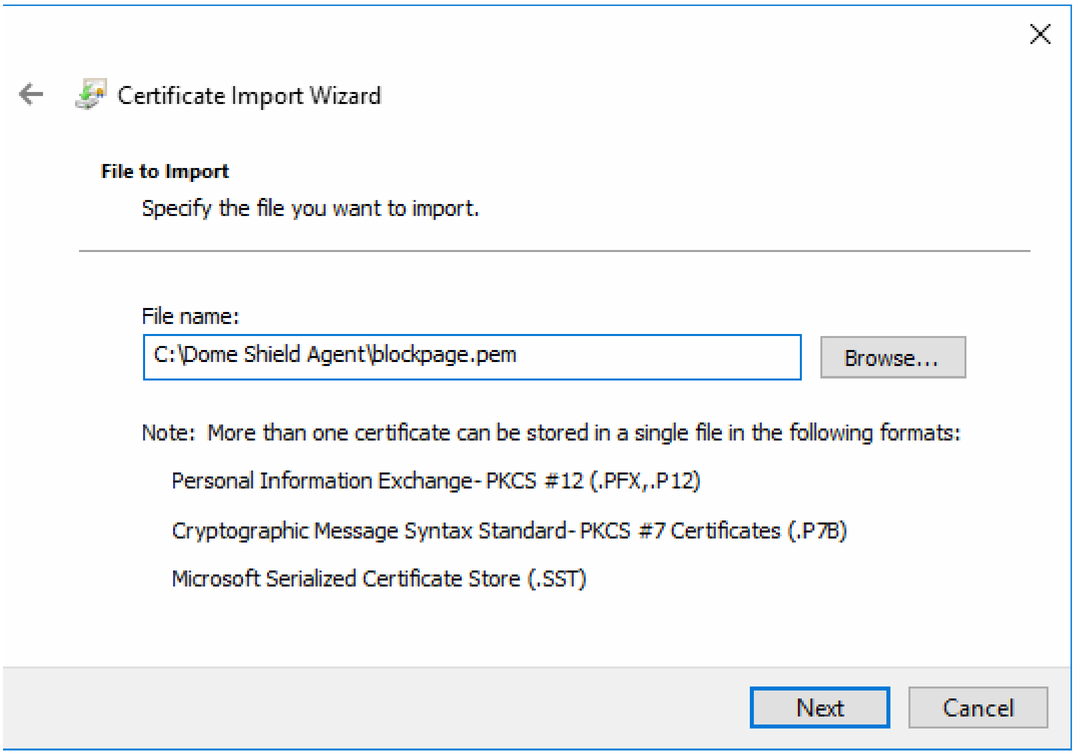
File name: blockpage.pem

All Files (*.*)

Click 'Browse', navigate to the location of the certificate and select the certificate file 'blockpage.pem'

Tip: If the 'blockpage.pem' file is not listed, select 'All Files' as file type in the drop-down beside file name at the bottom.

- Click 'Open'



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Dome Shield Agent\blockpage.pem

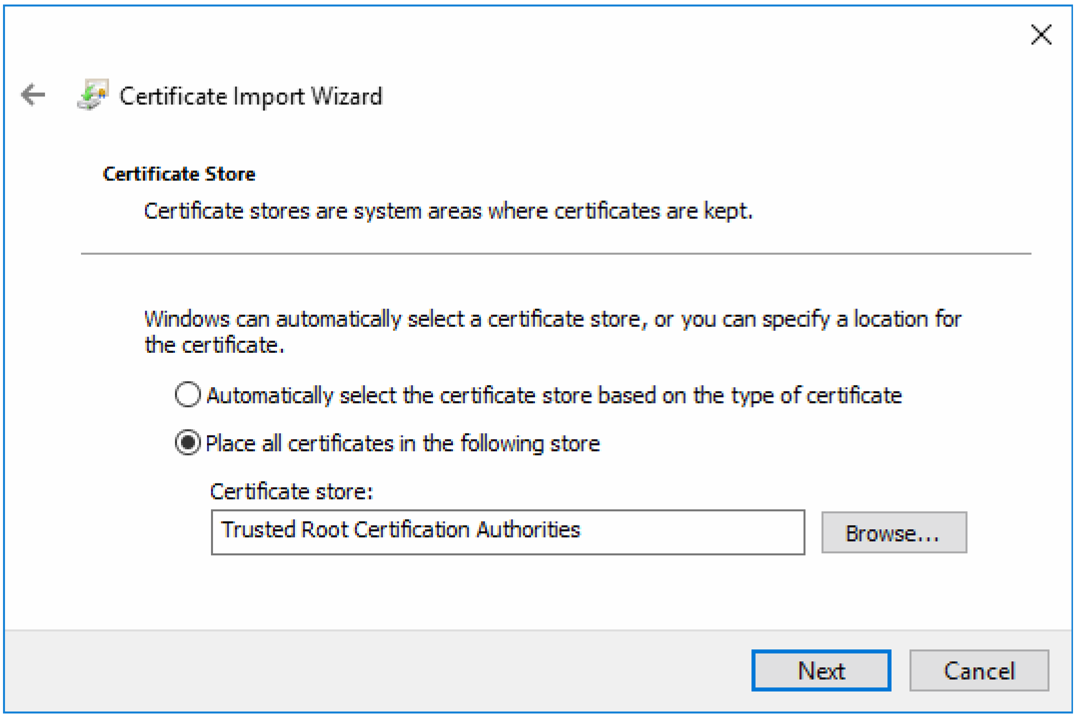
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

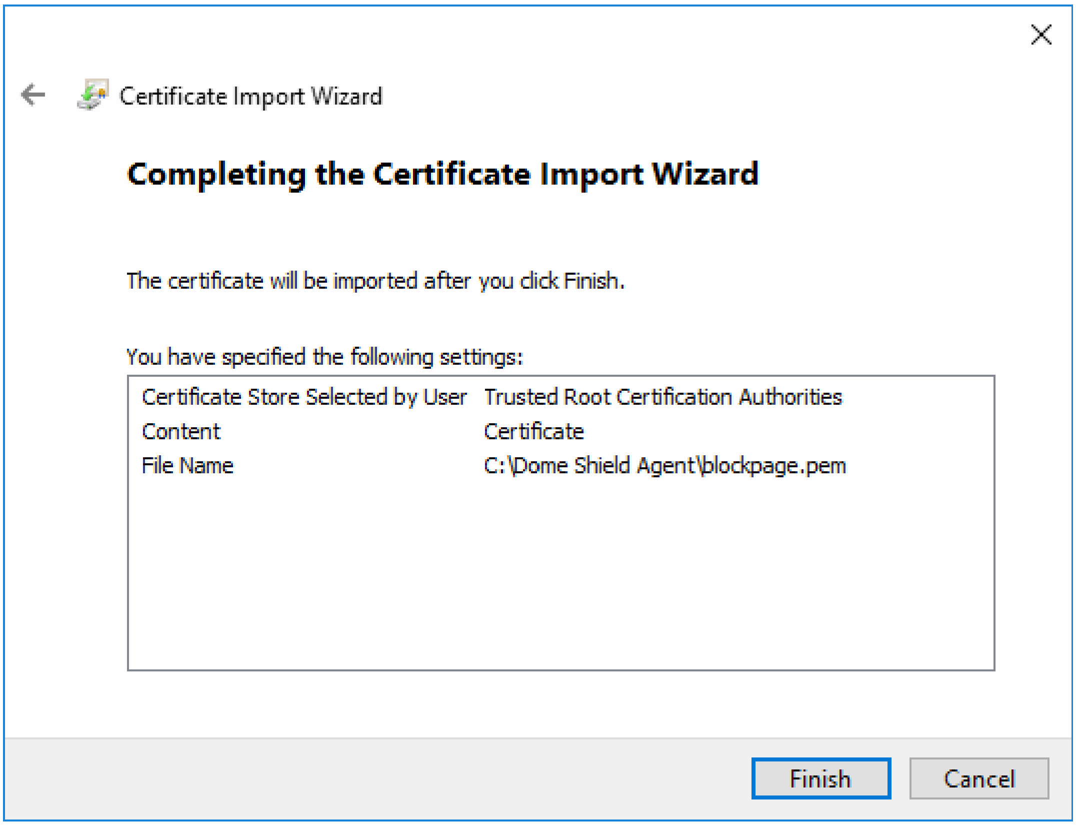
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

- Confirm that the 'Trusted Root Certification Authorities' store is pre-selected and click 'Next'
- A confirmation dialog will be displayed.



Certificate Import Wizard

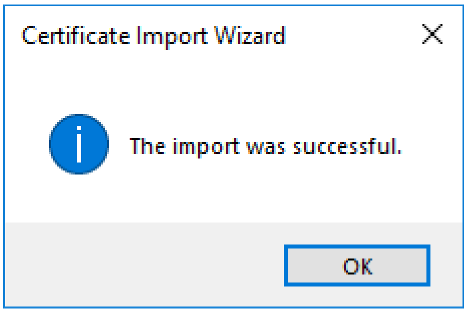
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Dome Shield Agent\blockpage.pem

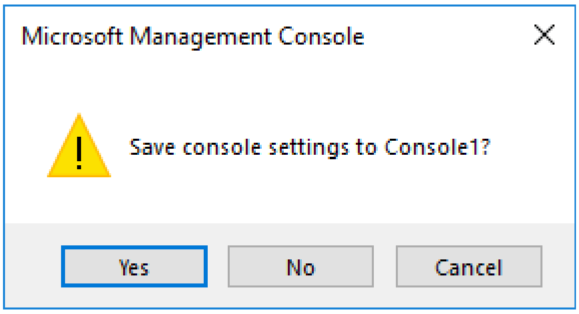
- Click 'Finish' to import the certificate.



Certificate Import Wizard

The import was successful.

- Click 'OK' to exit the wizard.



Microsoft Management Console

Save console settings to Console1?

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

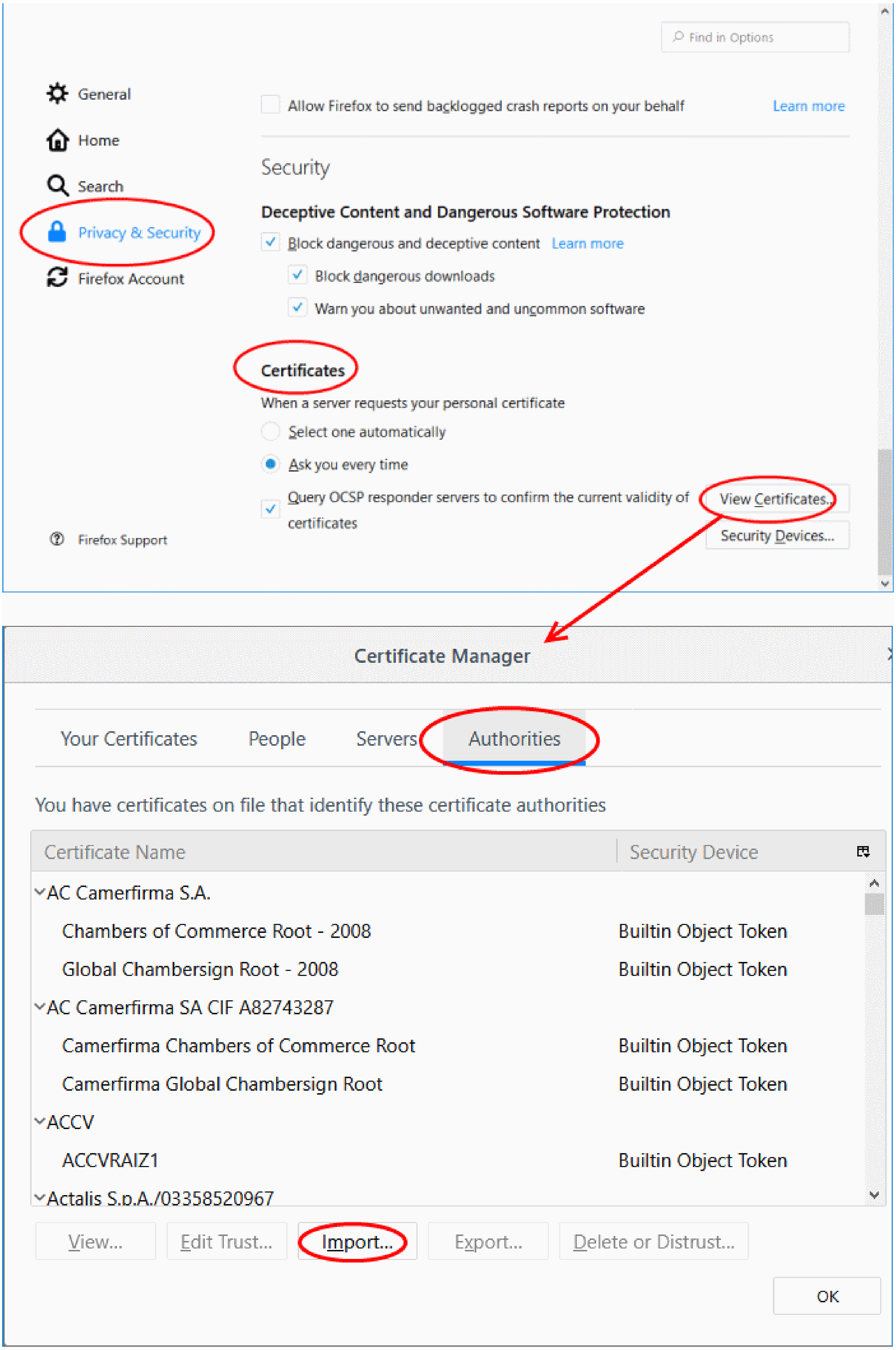
Mozilla Firefox browser users

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

To import the block page certificate to Firefox certificate store

- Open the Firefox browser

- Click the hamburger icon at the top-right and choose 'Options'
- Click 'Privacy & Security' on the left then scroll down to the 'Certificates' area
- Click 'View Certificates'
- The Firefox 'Certificate Manager' will open.



□ Allow Firefox to send backlogged crash reports on your behalf Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

○ Select one automatically

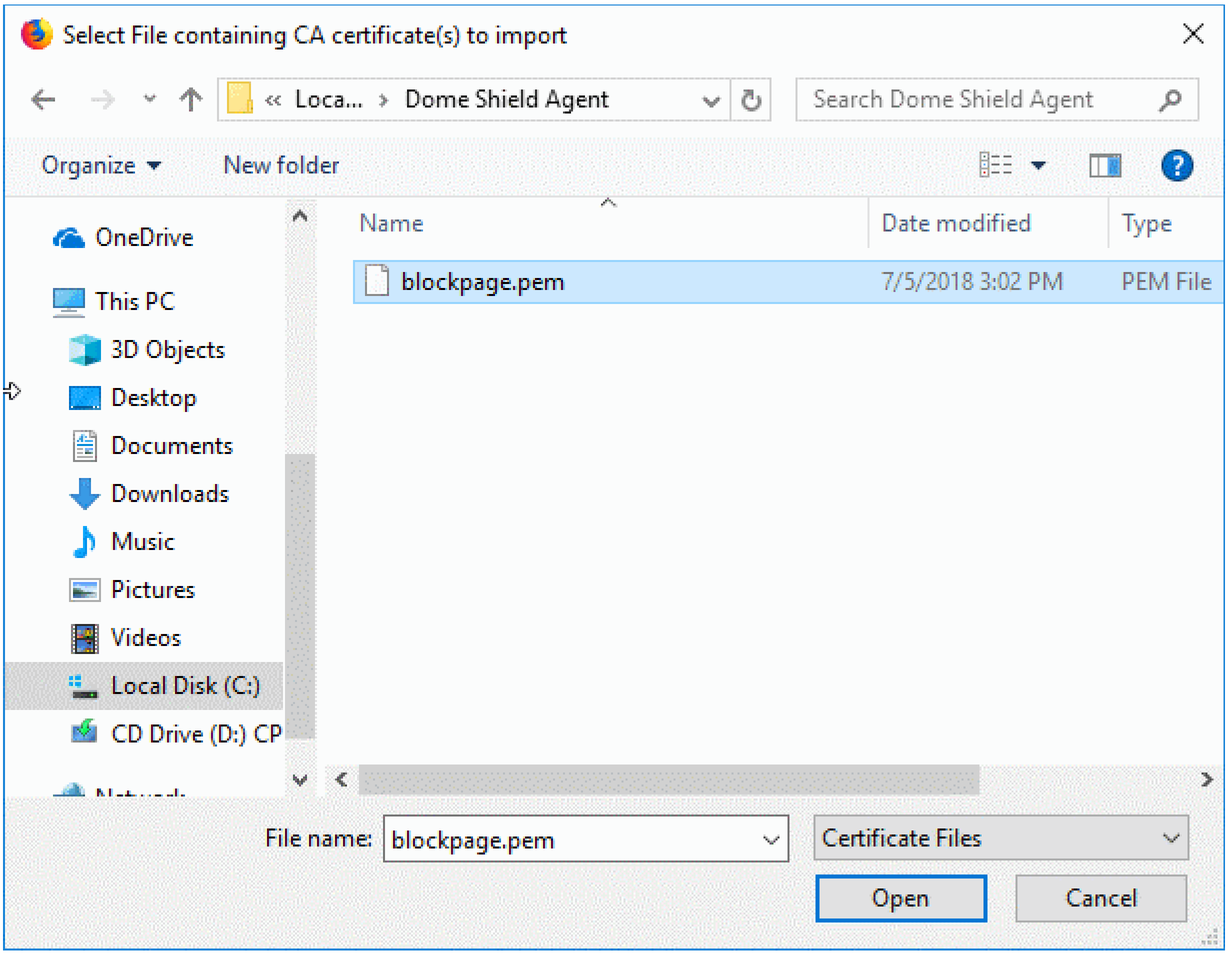
● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

You have certificates on file that identify these certificate authorities

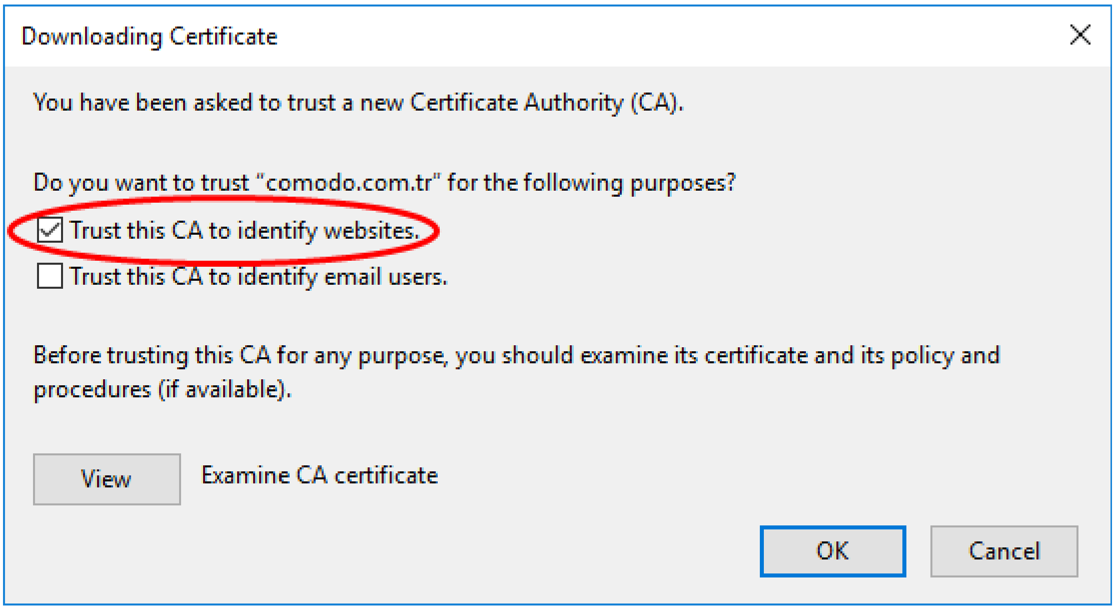
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

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



- Navigate the location of the certificate file, select the 'blockpage.pem' certificate file and click 'Open'.

The certificate download certificate dialog will appear.


Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "comodo.com.tr" for the following purposes?

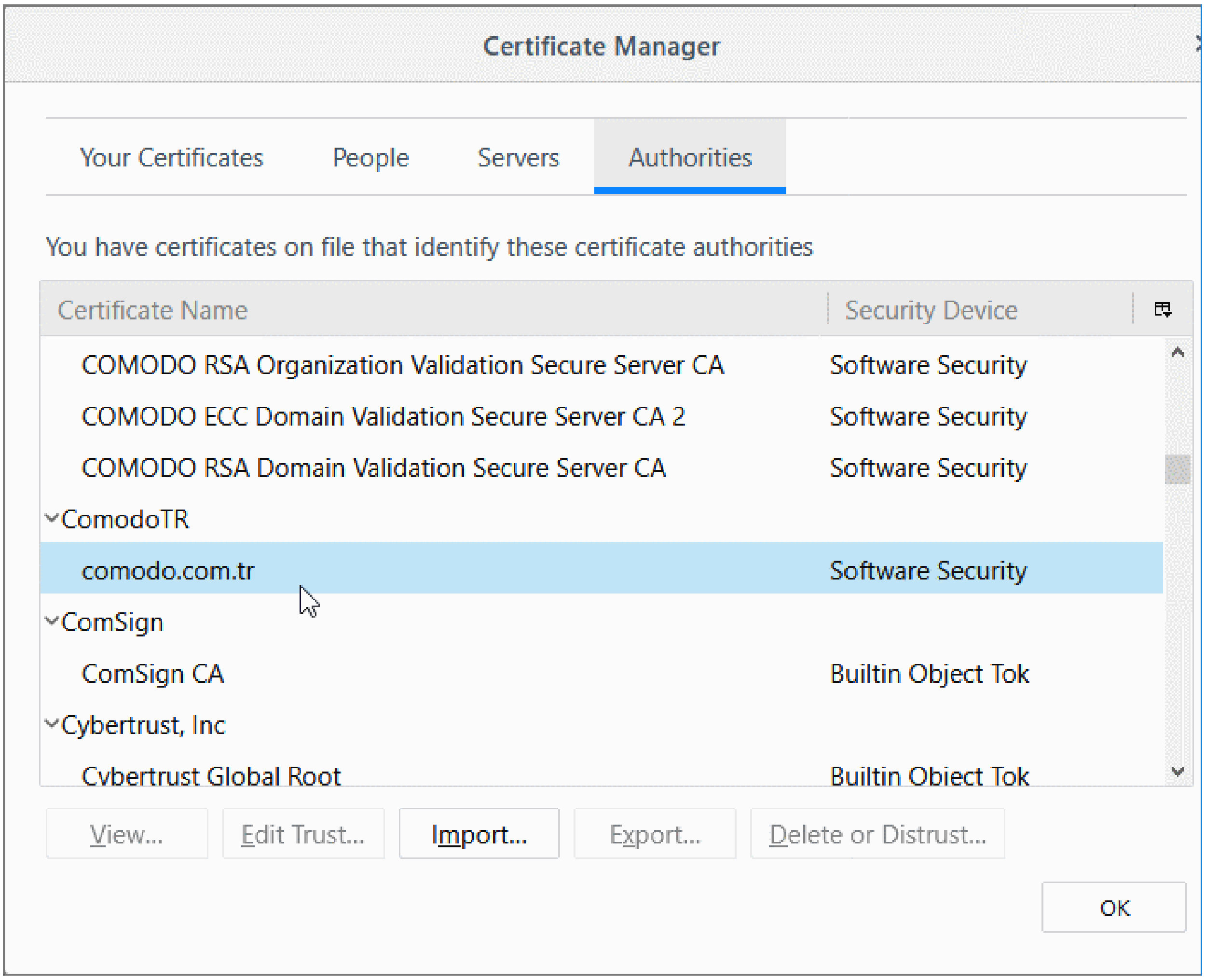
☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

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

The certificate will be imported,



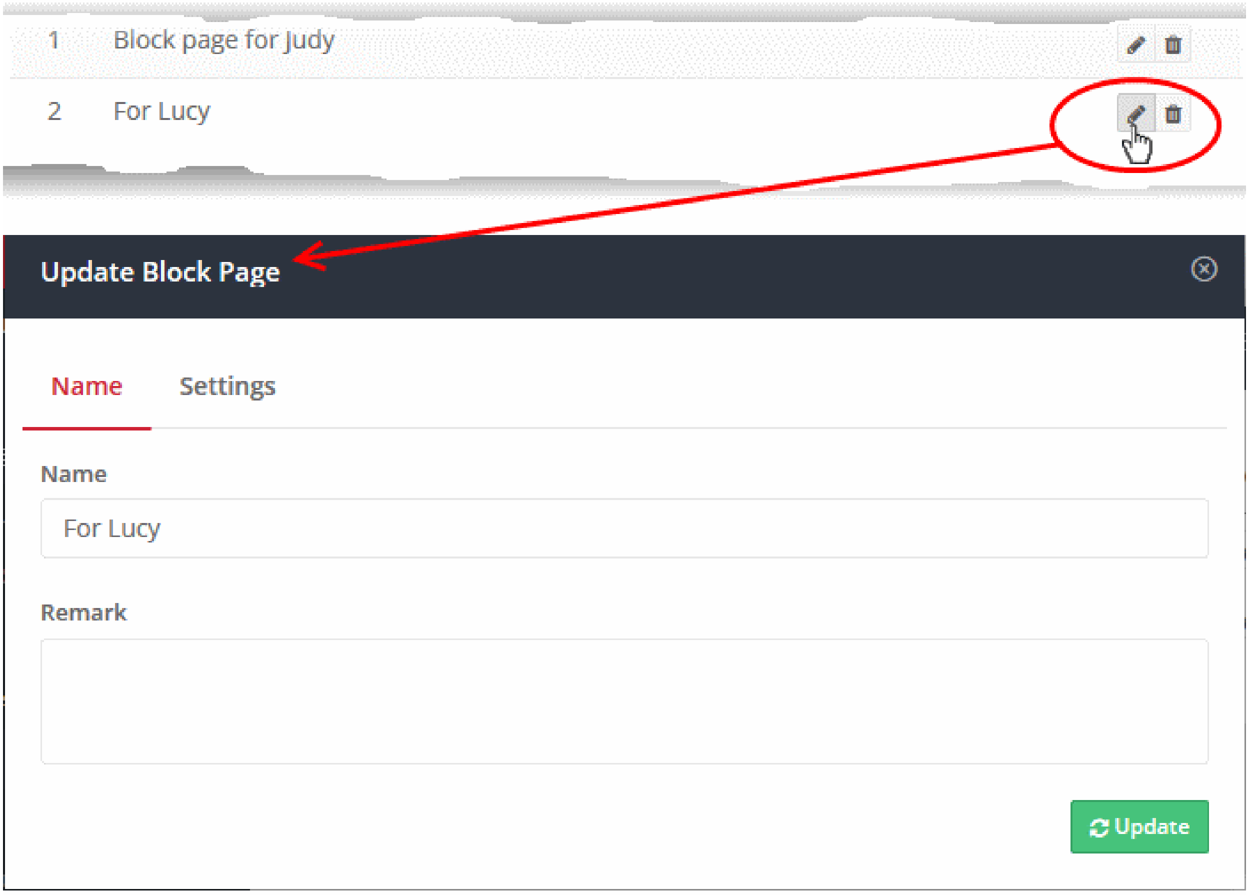
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
COMODO RSA Organization Validation Secure Server CA	Software Security
COMODO ECC Domain Validation Secure Server CA 2	Software Security
COMODO RSA Domain Validation Secure Server CA	Software Security
ComodoTR	
comodo.com.tr	Software Security
ComSign	
ComSign CA	Builtin Object Tok
Cybertrust, Inc	
Cybertrust Global Root	Builtin Object Tok

- Click 'OK' in the 'Certificate Manager' interface to save your changes.

Edit a Block Page

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



1 Block page for Judy

2 For Lucy

Update Block Page

Name: For Lucy

Remark:

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

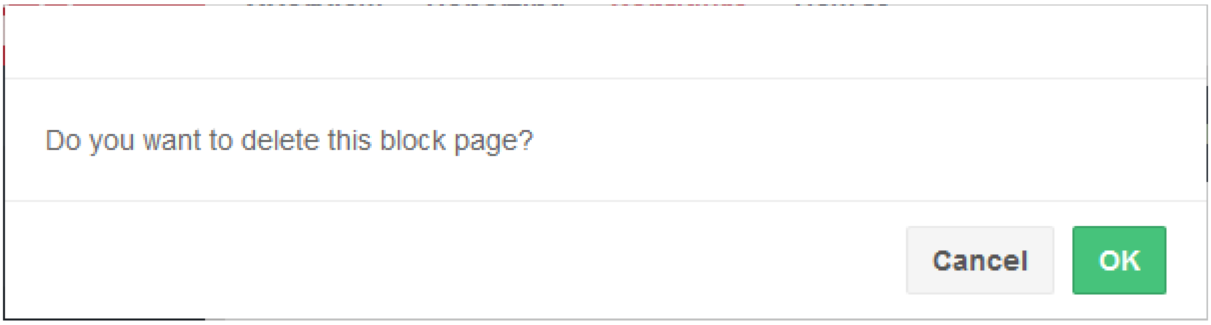
Please note that the policy/policies containing the block page will also be updated according to the new settings and name.

Deleting a category rule

Please note that 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.

A confirmation dialog will be displayed.

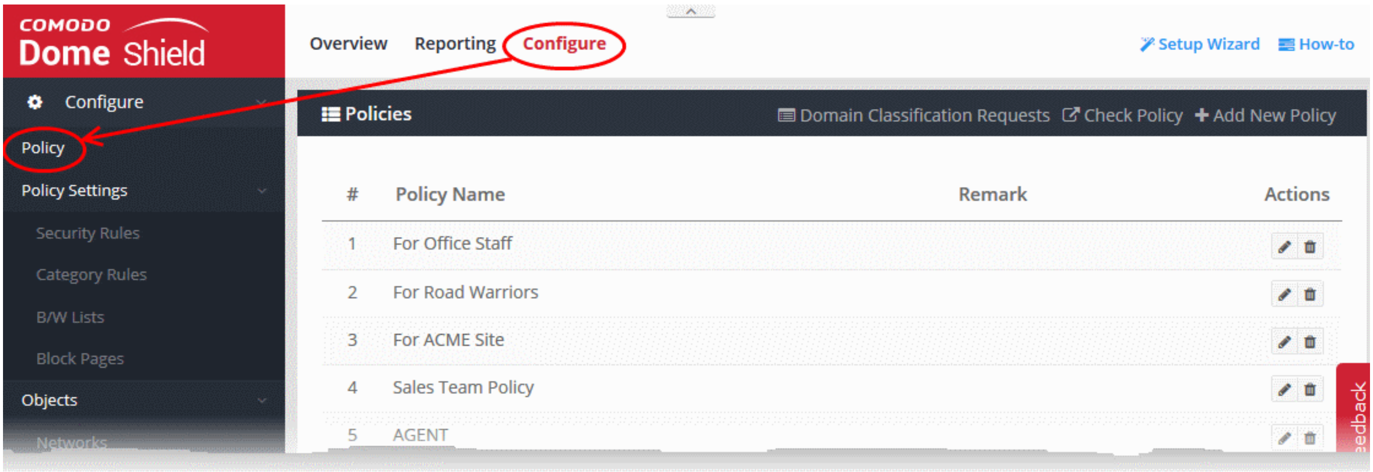


Do you want to delete this block page?

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

6 Apply Policies to Networks, Roaming and 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 'B/W 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 blocked 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 network 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 and 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



#	Policy Name	Remark	Actions
1	For Office Staff		
2	For Road Warriors		
3	For ACME Site		
4	Sales Team Policy		
5	AGENT		

- The links on the title bar let you do the following:
    - **Add New Policy** - Create a new policy and apply it to network(s), devices and imported network sites. See **Create a new policy** for assistance 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 work** for more help.

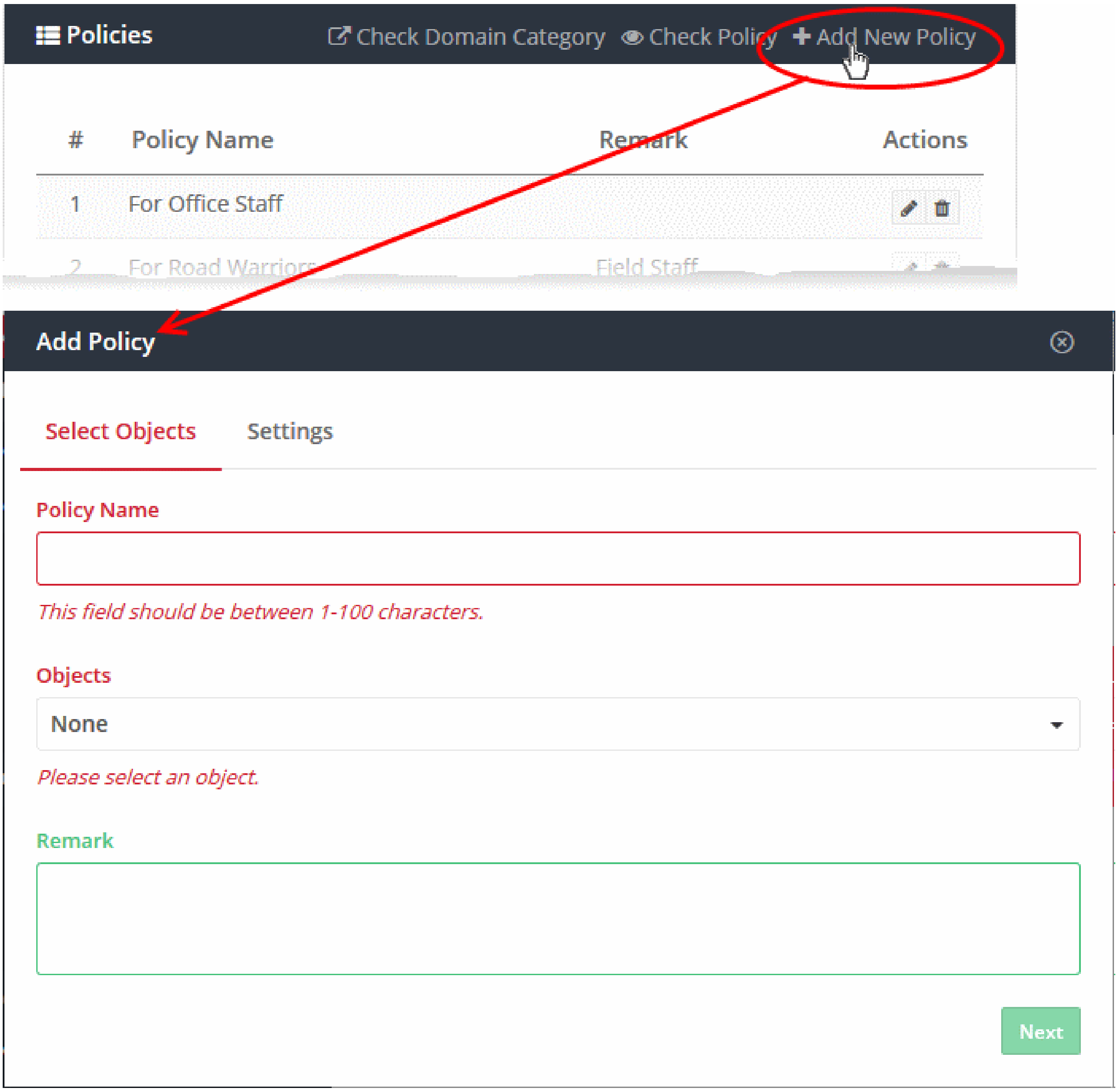
The following links contain help on this interface:

- **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' at the top right



Policies · Check Domain Category · Check Policy · + Add New Policy

#	Policy Name	Remark	Actions
1	For Office Staff		
2	For Road Warriors	Field Staff	

Add Policy

Select Objects · Settings

Policy Name

This field should be between 1-100 characters.

Objects

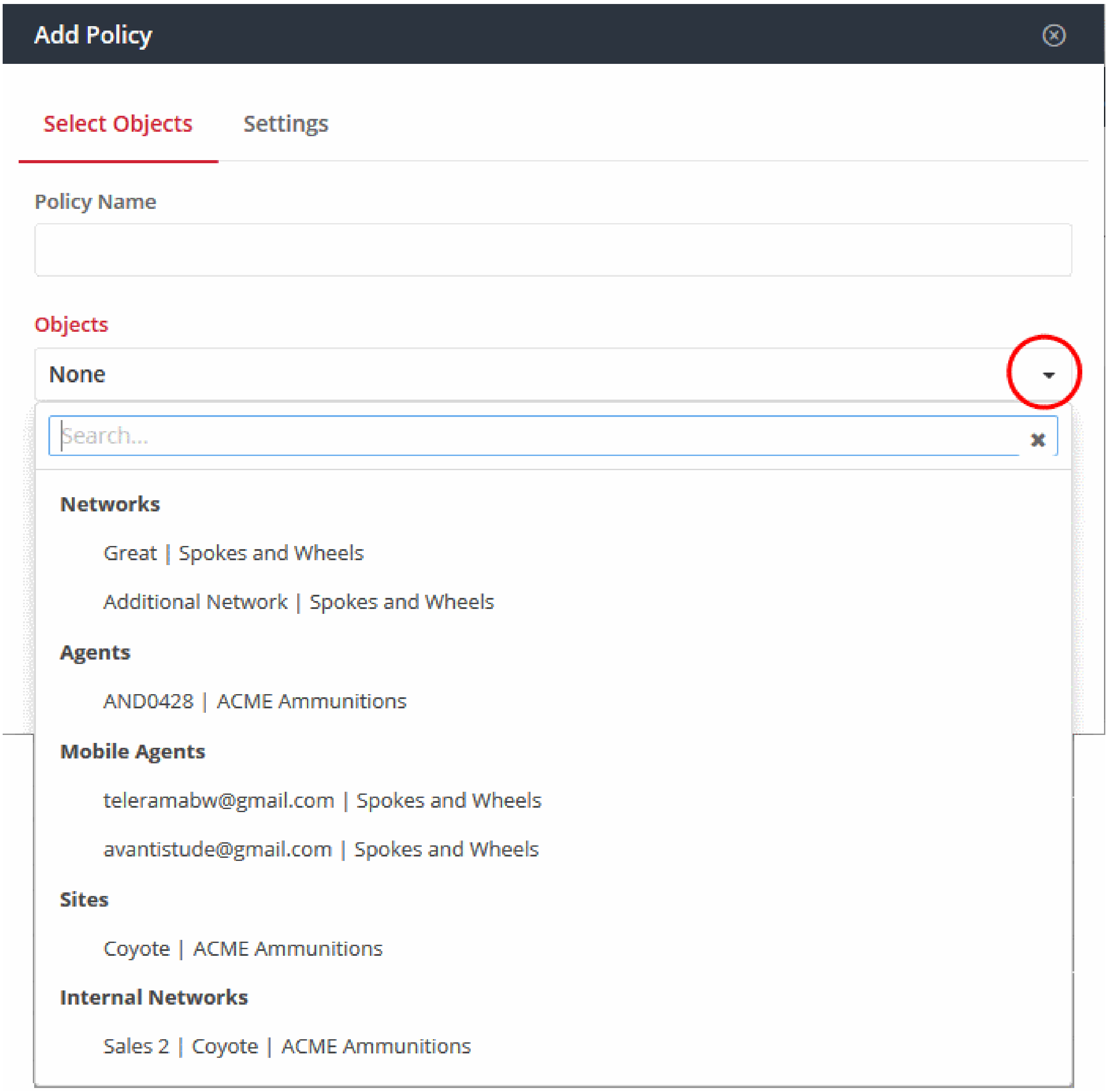
None

Please select an object.

Remark

Next

- Create a label for the policy in the 'Policy Name' field.
- 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.



Add Policy

Select Objects Settings

Policy Name

Objects

None

Search...

Networks

Great | Spokes and Wheels

Additional Network | Spokes and Wheels

Agents

AND0428 | ACME Ammunitions

Mobile Agents

teleramabw@gmail.com | Spokes and Wheels

avantistude@gmail.com | Spokes and Wheels

Sites

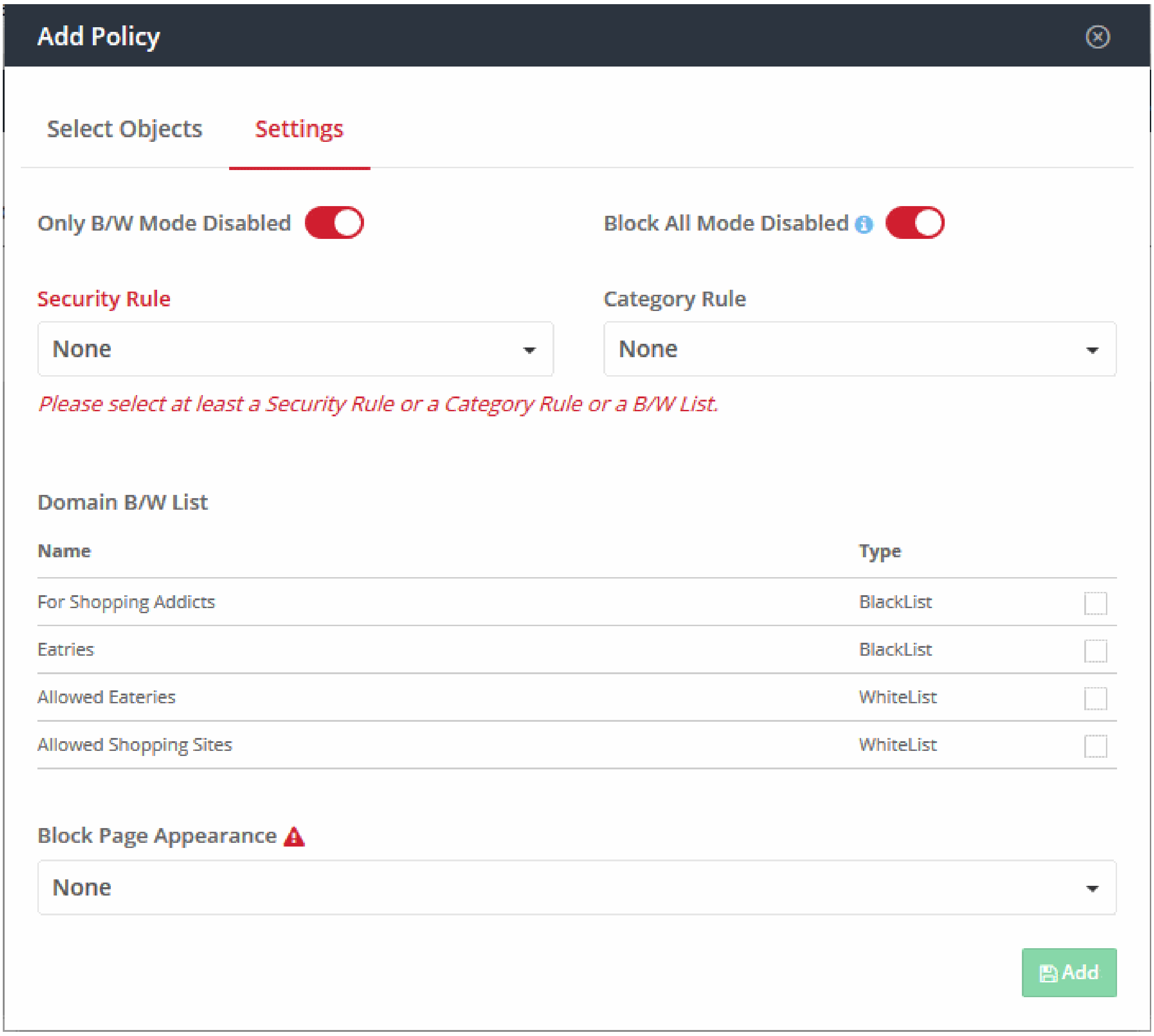
Coyote | ACME Ammunitions

Internal Networks

Sales 2 | Coyote | ACME Ammunitions

- **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:



Add Policy

Only B/W Mode Disabled

Block All Mode Disabled

Security Rule: None

Category Rule: None

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

Domain B/W List

Name	Type	
For Shopping Addicts	BlackList	□
Eatries	BlackList	□
Allowed Eateries	WhiteList	□
Allowed Shopping Sites	WhiteList	□

Block Page Appearance ⚠

None

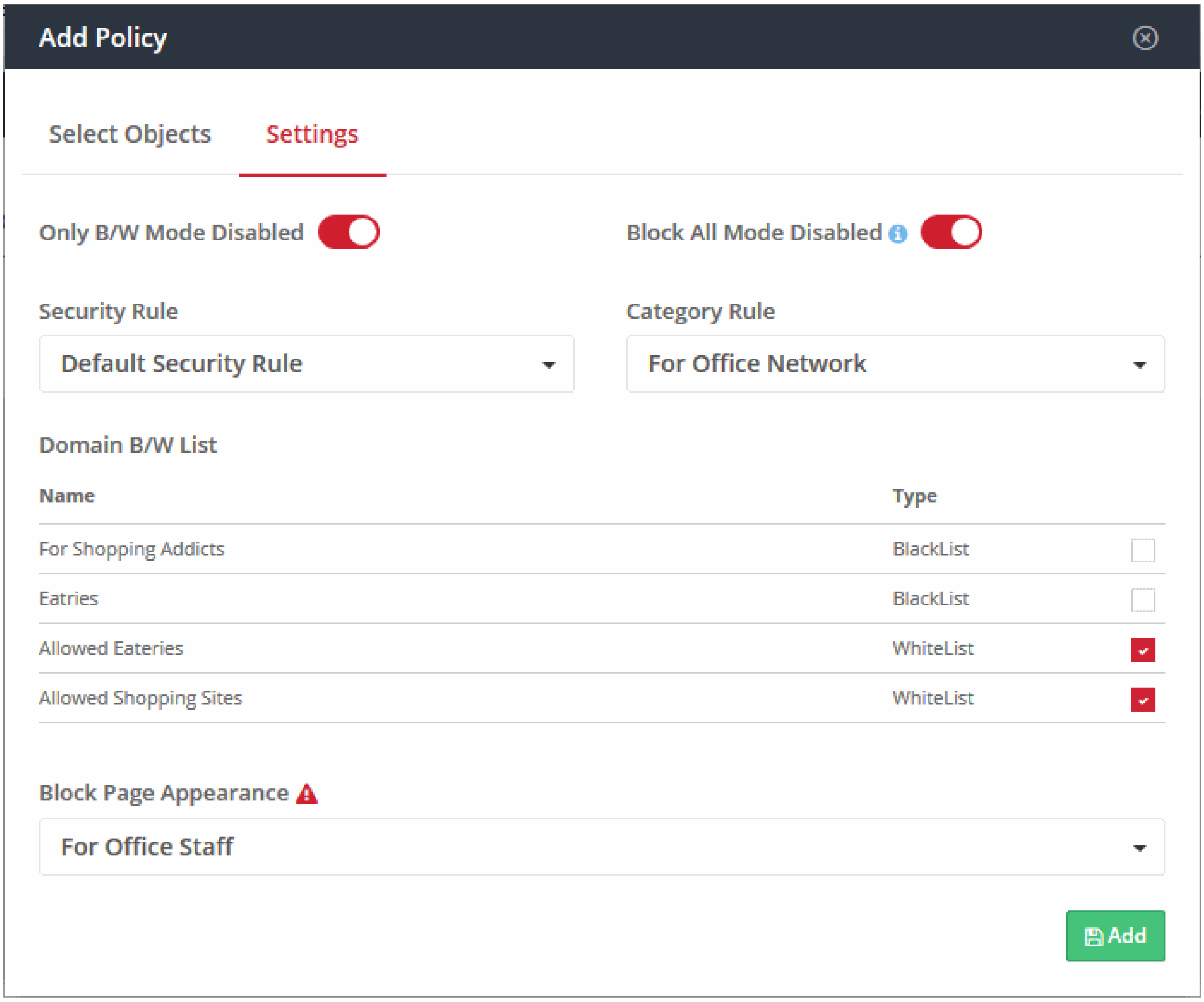
- **Only B/W Mode** - If enabled, only you will only be able to add blacklist or white-list rules to this policy. You will not be able to add security or category rules to the policy. By default, this setting is disabled.
  - Use the switch to enable or disable 'Only B/W Mode'
- **Block All Mode** -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



Add Policy

Select Objects | Settings

Only B/W Mode Disabled

Block All Mode Disabled

Security Rule: Default Security Rule

Category Rule: For Office Network

Domain B/W List

Name	Type	
For Shopping Addicts	BlackList	□
Eatries	BlackList	□
Allowed Eateries	WhiteList	☑
Allowed Shopping Sites	WhiteList	☑

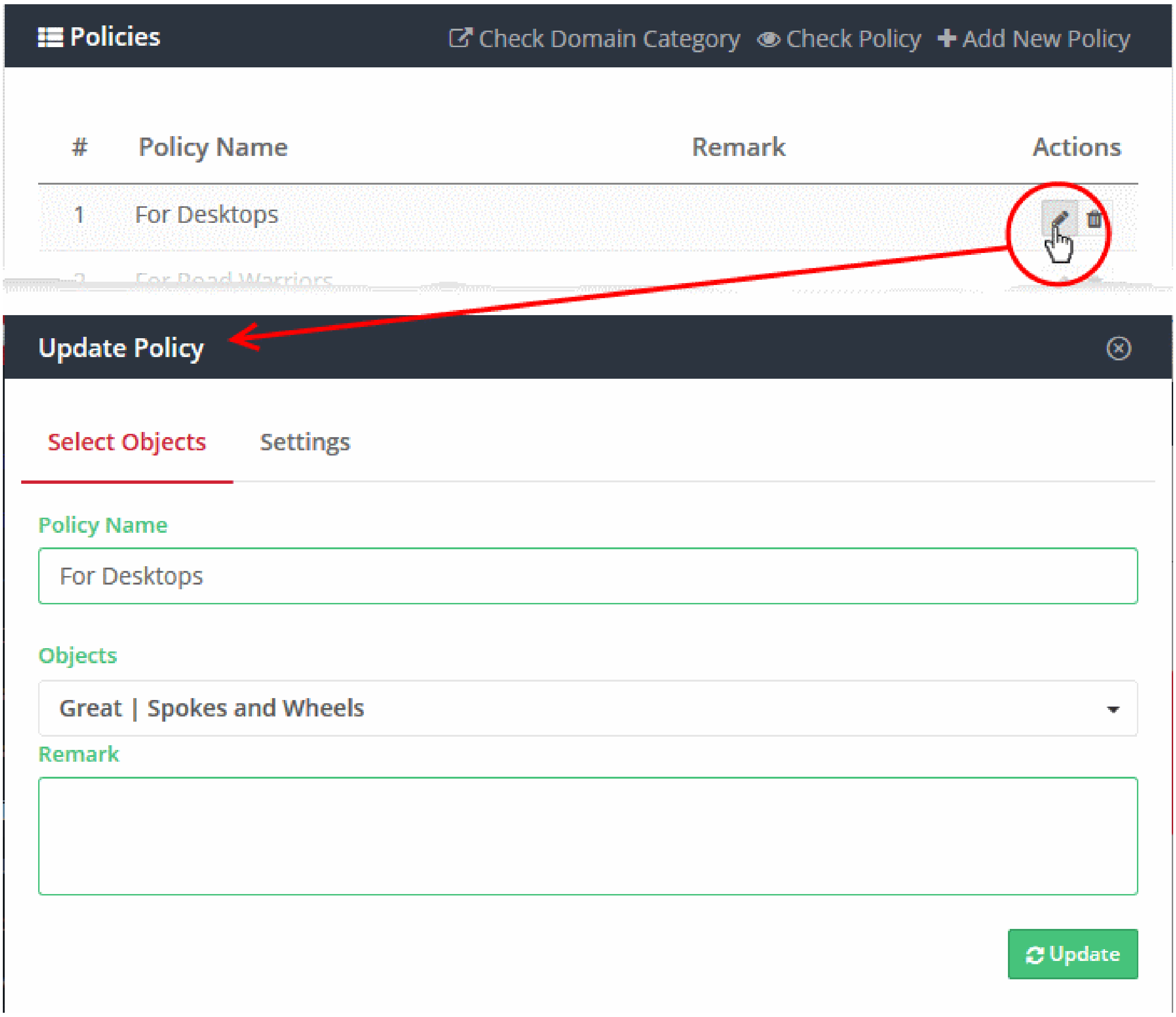
Block Page Appearance: For Office Staff

- 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:



Policy Name: For Desktops

Objects: Great | Spokes and Wheels

Remark:

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

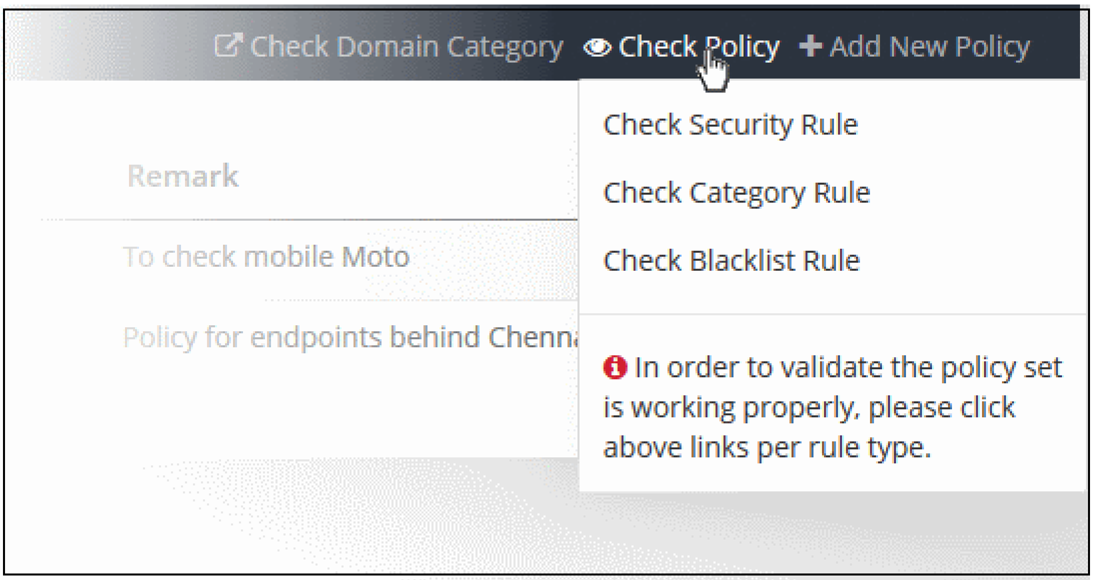
The updated policy will be applied to the network/roaming device/mobile device.

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:

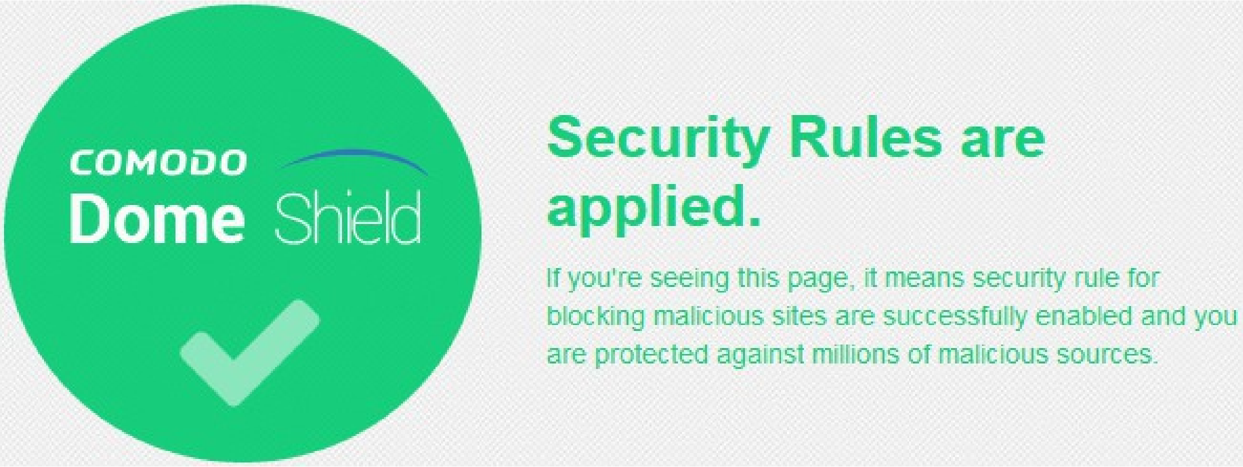
- Login to Dome Shield from any endpoint in an enrolled network, or from an enrolled roaming/mobile device.
- See **Logging-in to the Administrative Console** if you need help with this.
- Click 'Configure' > 'Policy'
- Click 'Check Policy' at the top-right



In order to validate the policy set is working properly, please click above links per rule type.

- 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'

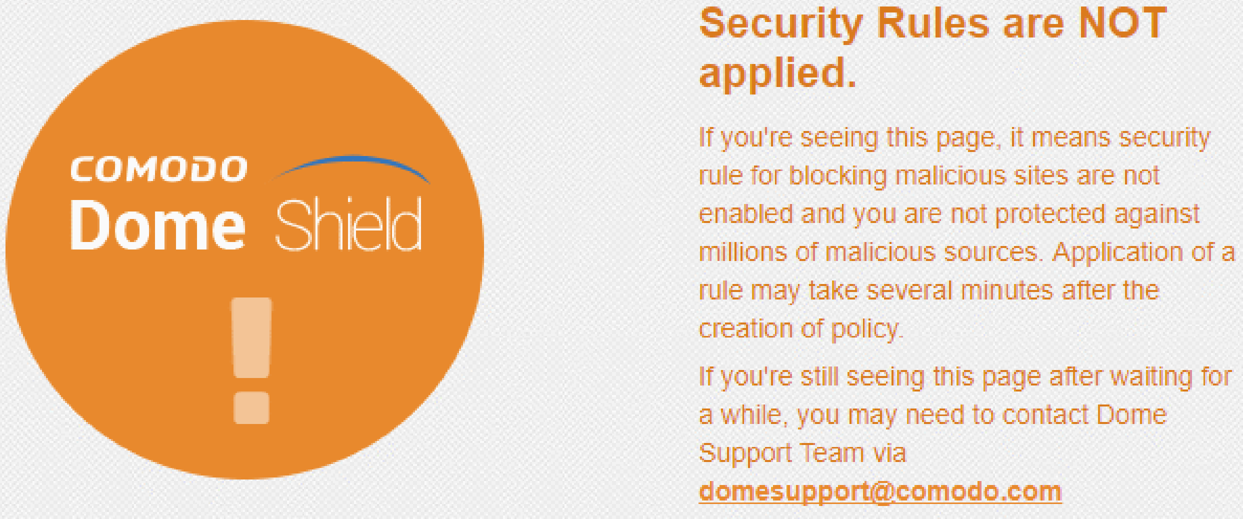
You will see the following message if the selected type of rule is active:



Security Rules are applied.

If you're seeing this page, it means security rule for blocking malicious sites are successfully enabled and you are protected against millions of malicious sources.

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



Security Rules are NOT applied.

If you're seeing this page, it means security rule for blocking malicious sites are not enabled and you are not protected against millions of malicious sources. Application of a rule may take several minutes after the creation of policy.

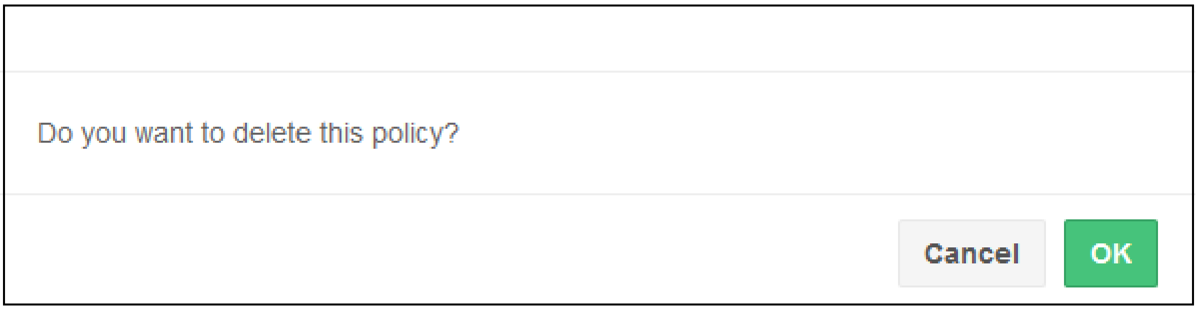
If you're still seeing this page after waiting for a while, you may need to contact Dome Support Team via domesupport@comodo.com

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.



Do you want to delete this policy?

- 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'.
- These rules can be added to a policy to stop devices/networks accessing sites in those categories.

Domain classification tools:

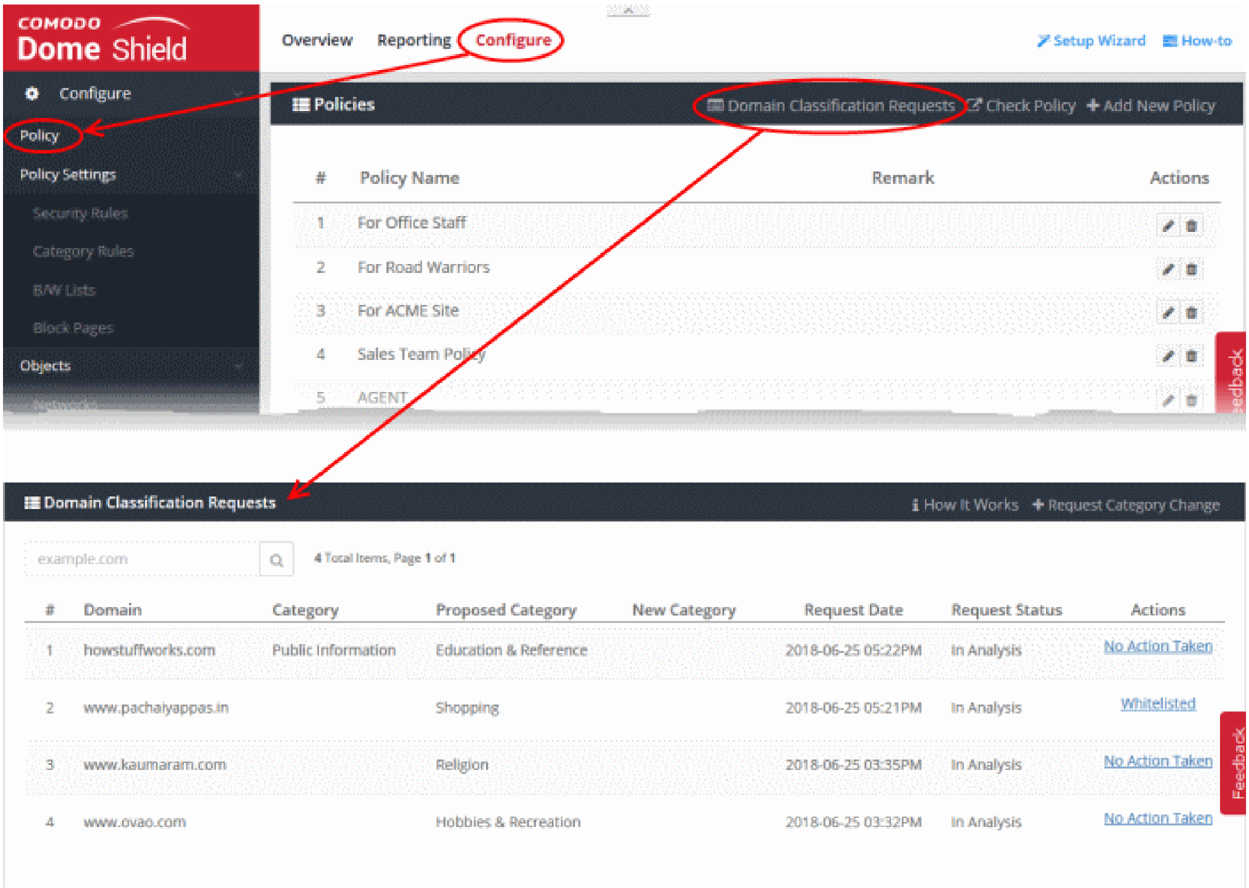
- You can suggest a category for a domain which is not in the database. For example, you may chance upon a gambling site which is not yet recognized by the filter.
- You can also suggest a different category for a domain if you feel it has been categorized inaccurately.

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 will be automatically applied to all your policies.

To view the 'Domain Classification Requests' interface

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



#	Policy Name	Remark	Actions
1	For Office Staff		
2	For Road Warriors		
3	For ACME Site		
4	Sales Team Policy		
5	AGENT		

#	Domain	Category	Proposed Category	New Category	Request Date	Request Status	Actions
1	howstuffworks.com	Public Information	Education & Reference		2018-06-25 05:22PM	In Analysis	No Action Taken
2	www.pachaiyappas.in		Shopping		2018-06-25 05:21PM	In Analysis	Whitelisted
3	www.kaumaram.com		Religion		2018-06-25 03:35PM	In Analysis	No Action Taken
4	www.ovao.com		Hobbies & Recreation		2018-06-25 03:32PM	In Analysis	No Action Taken

The list of your requests will be displayed.

Customer - Table of Column Descriptions	
Column Header	**Description**
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

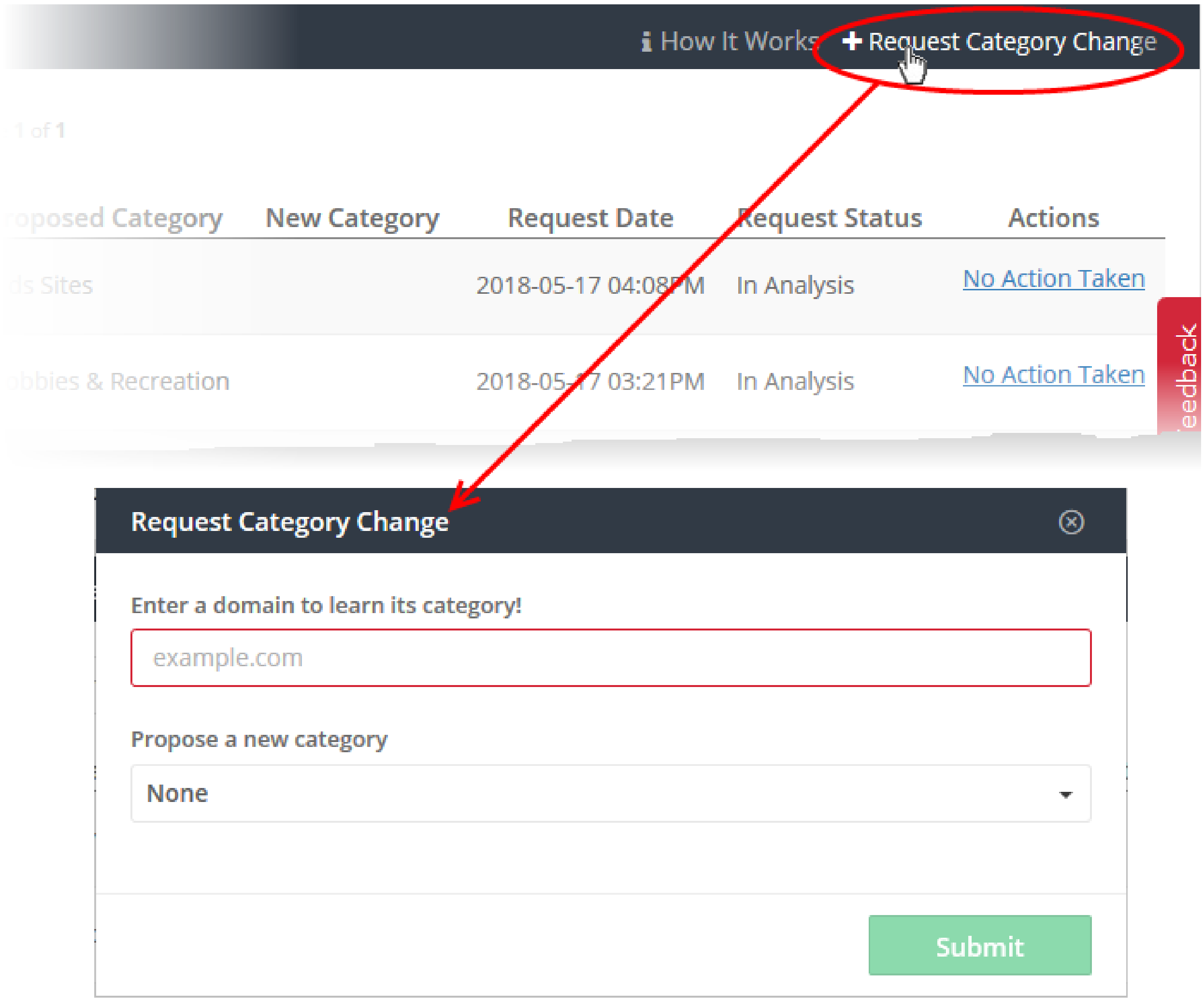
Submit a Domain Classification Request

- 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'



oposed Category	New Category	Request Date	Request Status	Actions
ds Sites		2018-05-17 04:08PM	In Analysis	No Action Taken
bbies & Recreation		2018-05-17 03:21PM	In Analysis	No Action Taken

Request Category Change

Enter a domain to learn its category!

example.com

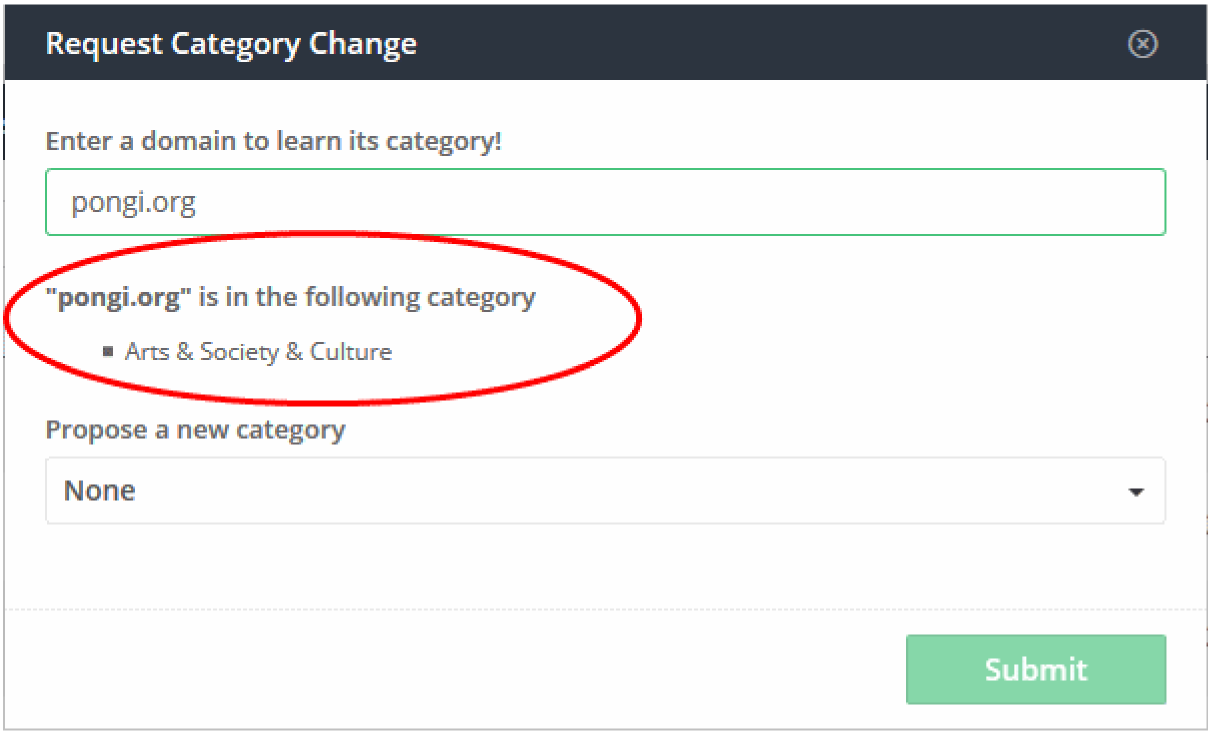
Propose a new category

None

- 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:



Request Category Change

Enter a domain to learn its category!

pongi.org

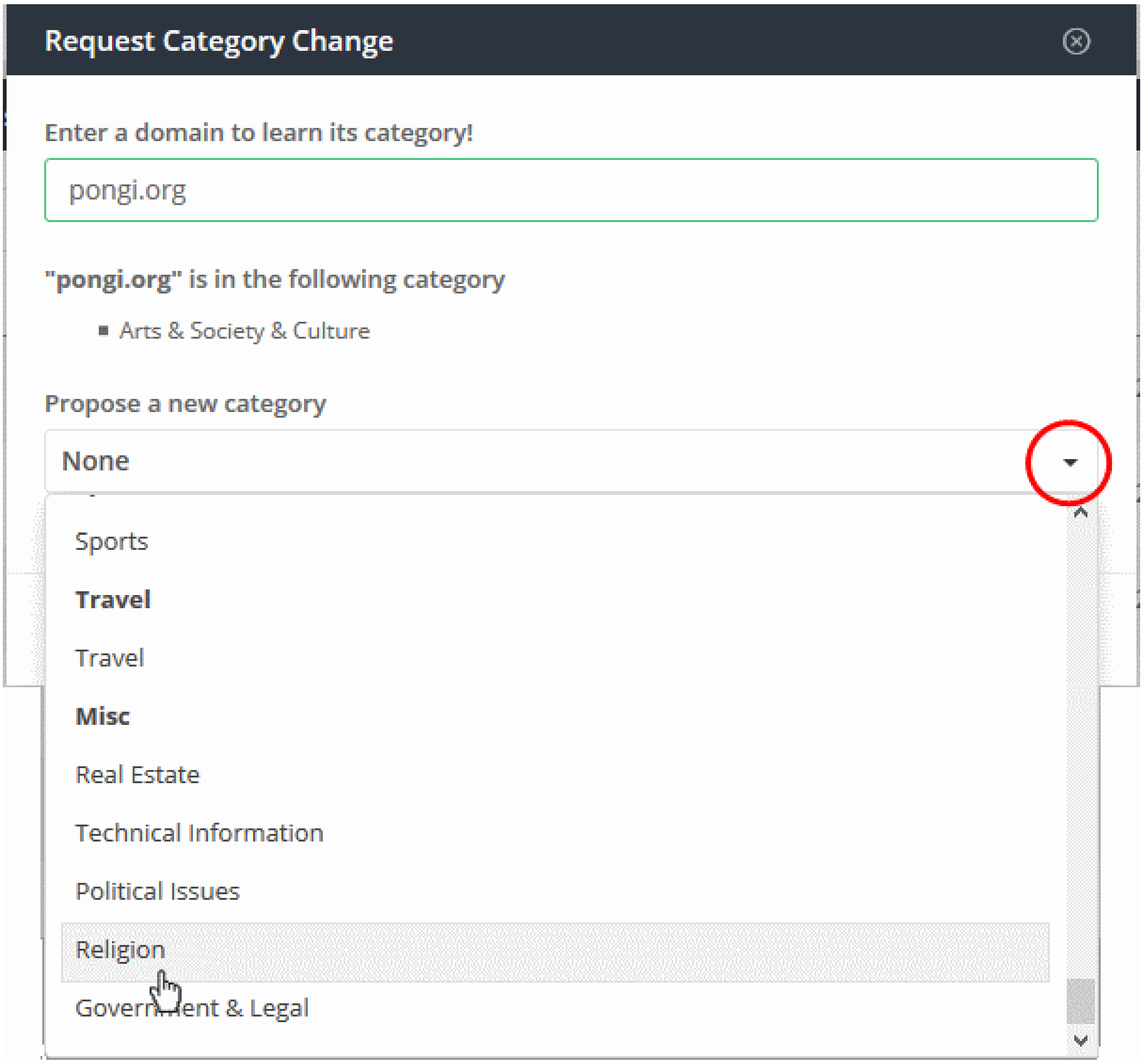
"pongi.org" is in the following category

- Arts & Society & Culture

Propose a new category

None

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



Request Category Change

Enter a domain to learn its category!

pongi.org

"pongi.org" is in the following category

- Arts & Society & Culture

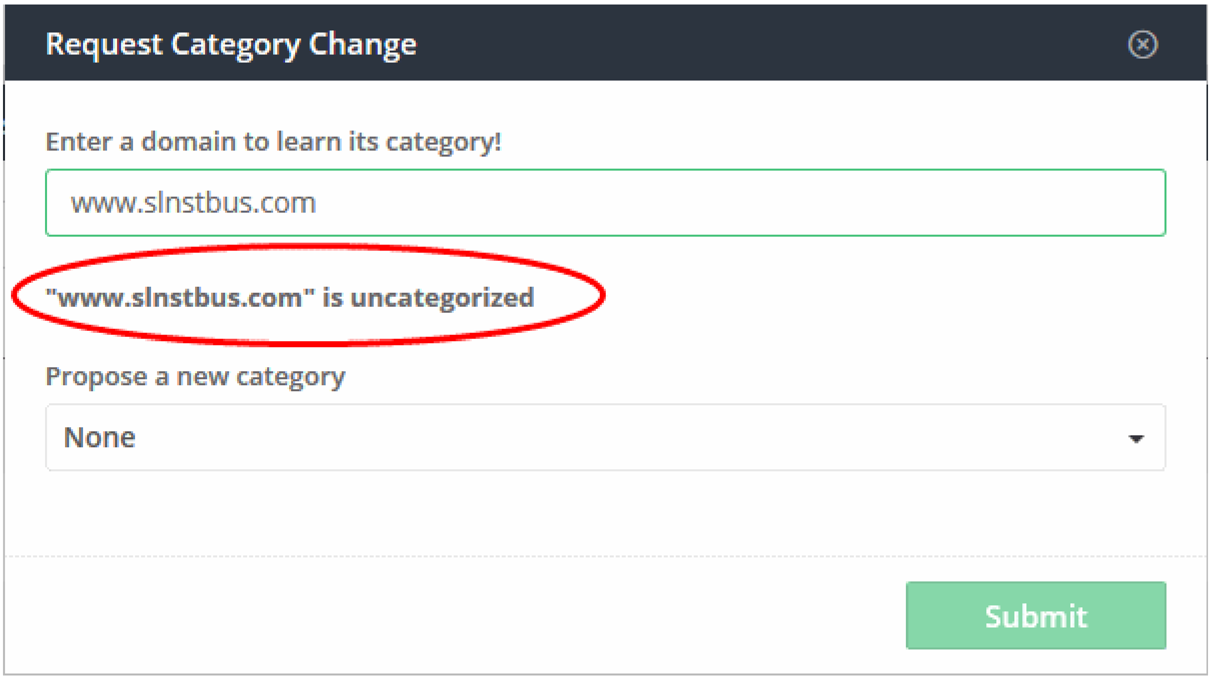
Propose a new category

None

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'.



Request Category Change

Enter a domain to learn its category!

www.slnstbus.com

"www.slnstbus.com" is uncategorized

Propose a new category

None

- 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..

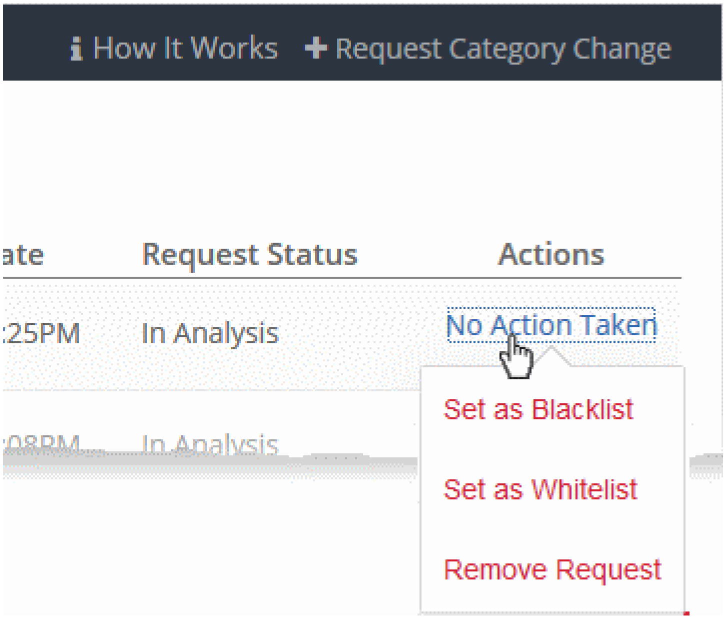
- If your request is accepted, the domain will be blocked or allowed depending on whether the new category is allowed or blocked in the 'Category Rules' included in the respective policies.
- If your request is rejected, the domain will be allowed or blocked depending on whether it is included in any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



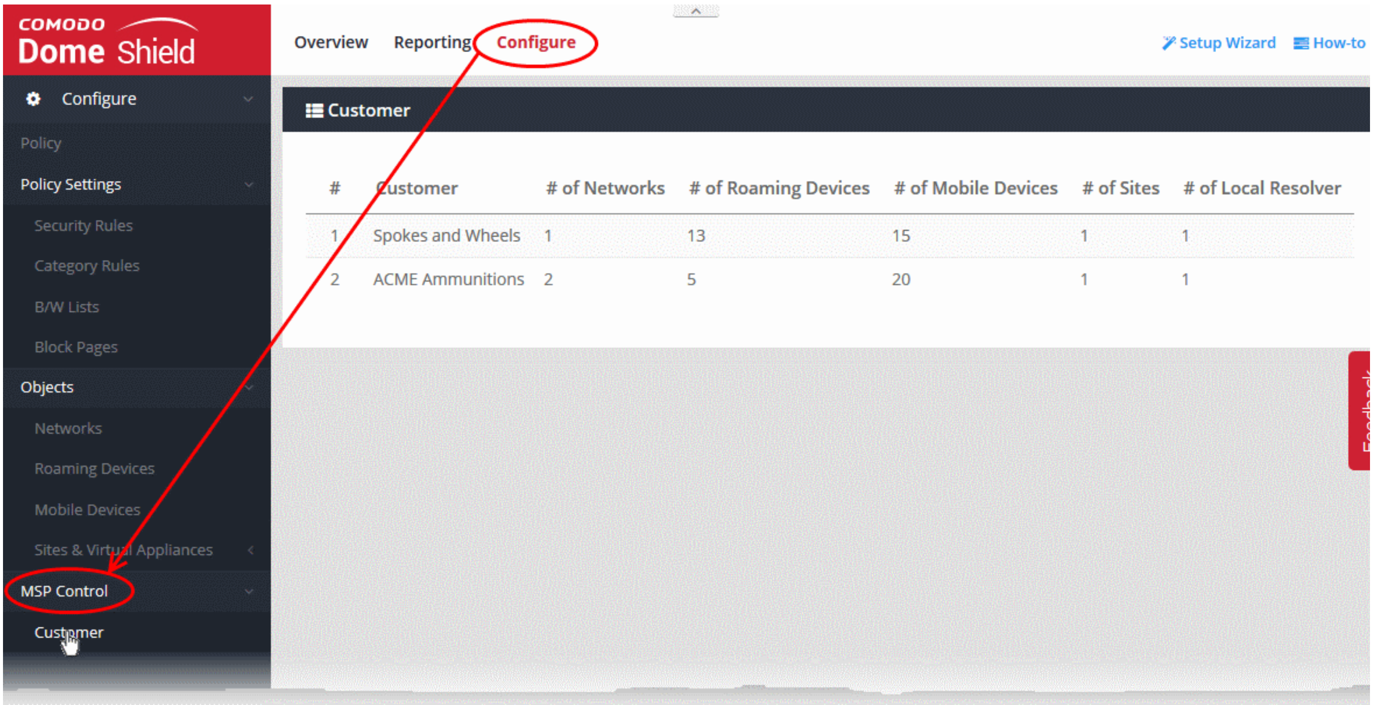
- Select the option from the drop-down
  - Set as Blacklist - The domain will be added to the global blacklist and applied to all your policies. It will be blocked on all protected networks, roaming and mobile devices.
  - Set as Whitelist - The domain will be added to the global whitelist and applied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

Provides 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

#	Customer	# of Networks	# of Roaming Devices	# of Mobile Devices	# of Sites	# of Local Resolver
1	Spokes and Wheels	1	13	15	1	1
2	ACME Ammunitions	2	5	20	1	1

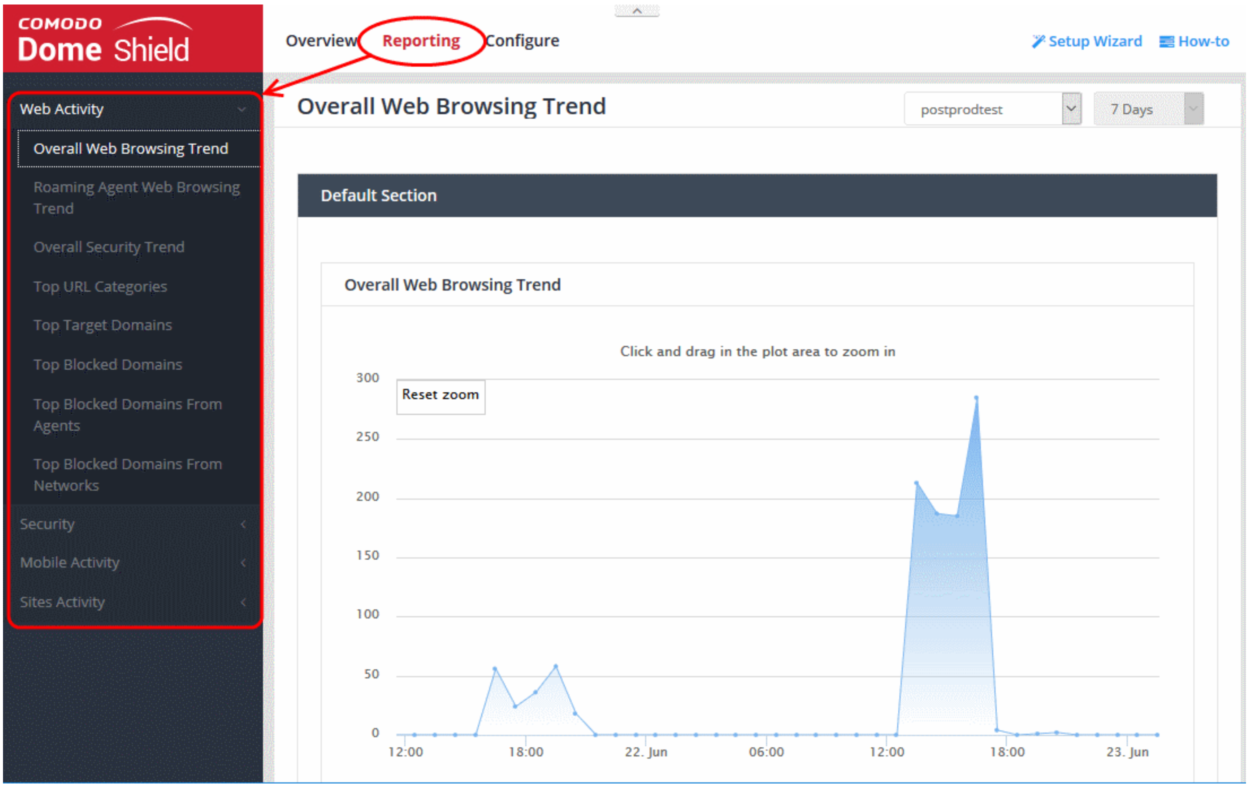
Customer - Table of Column Descriptions	
Column Header	**Description**
Customer	The name of the MSP's customer
# of Networks	Number of networks enrolled for the customer
# of Roaming Devices	Number of out-of-network Windows devices enrolled for the customer. Install the Dome Shield roaming agent to enroll 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.

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 'Sites 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.

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 : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email: EnterpriseSolutions@Comodo.com