



**COMODO**  
Creating Trust Online®

**COMODO ONE**  
MSP

# Comodo Dome Shield

Software Version 2.4

---

## Quick Start Guide

Guide Version 2.4.032019

---

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Comodo Dome Shield - Quick Start Guide

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 policies.

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

- **Step 1 - Purchase a license and login to Dome Shield**
- **Step 2 - Add your network**
- **Step 3 - Enroll networks and devices for protection**
  - **Enroll additional networks to be protected**
  - **Enroll roaming Windows devices**
  - **Enroll mobile devices**
  - **Setup local resolver virtual machines and import networks and sites**
- **Step 4 - Create policy rules**
- **Step 5 - Create and apply security policies**
- **Step 6 - Generate reports**
- **Step 7 - View account details**

### Step 1 - Purchase a License and Login to Dome Shield

Two types of license are available for Dome Shield:

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

**Click here** to compare packages.

There are two ways to enroll for Dome Shield:

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

#### **Stand-alone Customers:**

Sign up for a Gold license

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

## COMODO Dome Shield

### SIGNUP

1 Select Package      2 Enter Account Information      3 Done!

**Welcome**  
**You're about to start securing your network with **Dome Shield!****

Dome Shield provides **Web Visibility, Control** and **Protection** at the DNS-layer.

- Block Advanced Threats, Phishing, Malware and C&C Callbacks
- Create Web Filtering rules using 80+ content categories
- Enforce Protection and Web Access Policies, on and off network
- Get Real-Time Visibility for all internet connected devices

This wizard will help you sign up to Dome Shield **under 2 minutes!**

**Enterprise**    MSP

Already have an account?

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

**1**  
Select Package

**2**  
Enter Account Information

**3**  
Done!

### Dome Shield Gold

— Free —

---

Free up to 300,000 DNS Requests per Month

Available for Enterprises & MSPs

Active Directory not supported

Does not include:

- ✗ Internal IP/Subnet/IP Block Based Policies
- ✗ Internal IP Based Visibility & Monitoring
- ✗ Encrypt All DNS Traffic
- ✗ Dome Shield DNS Resolver Virtual Appliances

**GET STARTED FOR FREE**

Free, No Credit Card Required

[Are you a MSP?](#)

### Dome Shield Platinum

— for Enterprises —

---

24 x 7 x 365 Platinum Support

Includes:

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

**BUY NOW**

[1 Month Trial Option](#)

### Dome Shield Platinum

— for MSPs —

---

24 x 7 x 365 Platinum Support

Includes:

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

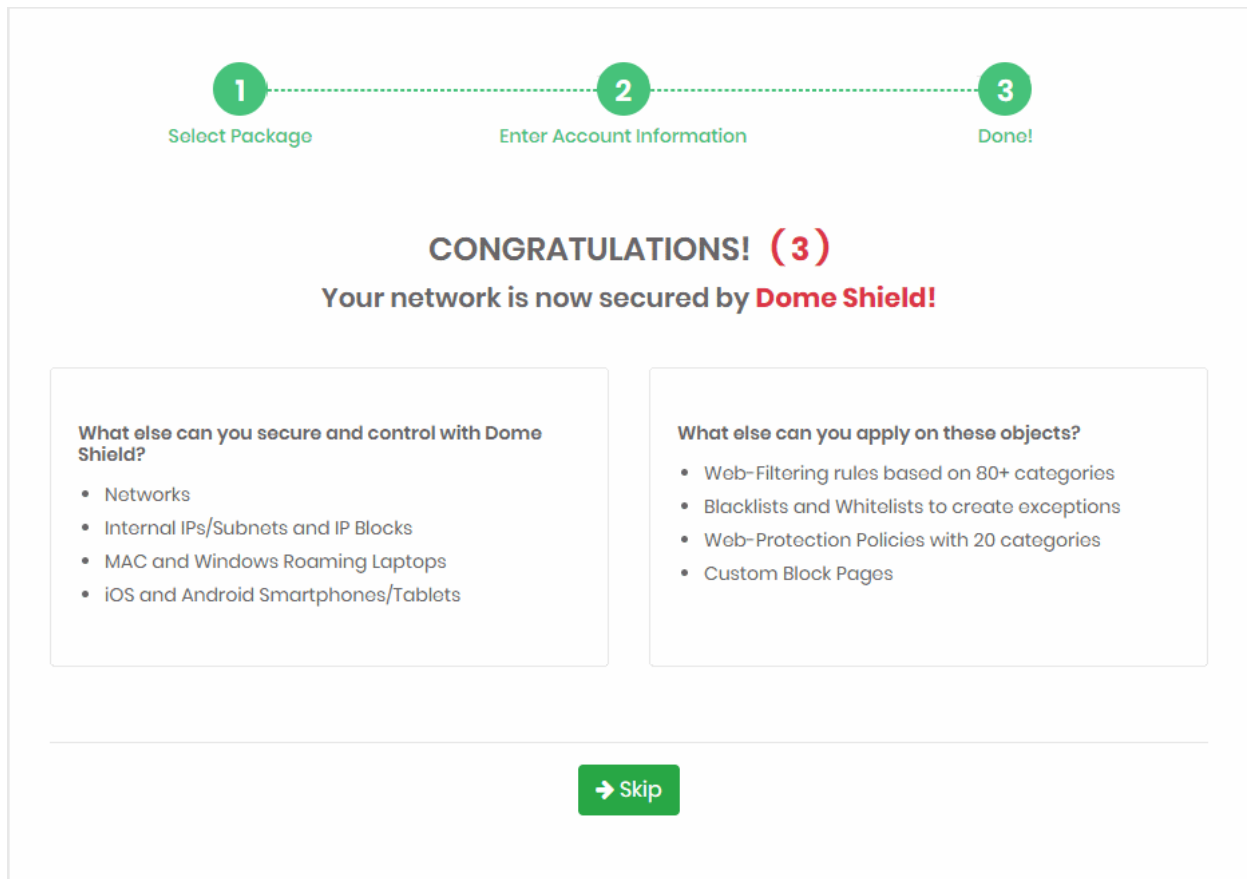
**BUY NOW**

[1 Month Trial Option](#)

- Click 'Get Started for Free' under 'Dome Shield Gold'
- The next step is to provide your account details and accept the end user license agreement.

The screenshot shows a three-step progress bar at the top: 1. Select Package, 2. Enter Account Information (current step), and 3. Done!. Below the progress bar is the heading "Please Enter Customer Details". The form contains three input fields: "Email", "Password", and "Confirm Password". Below the input fields is a checkbox labeled "I have read and agree to the End User license/Service Agreement". At the bottom of the form are two buttons: "Previous" and "Finish".

- **Email** - Enter your contact mail address. The order confirmation email and license keys are sent to this address. Your email address doubles up as your Dome Shield username.
- **Password** and **Confirm Password** - Create a passphrase to login to Dome Shield.
- **End user license agreement** - Read and agree to the terms and conditions.
- Click 'Finish'



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

1

Add Your Network

2

Confirm Rules for your Policy

3


Change your DNS

**Welcome admin@company.com**  
**You're about to start securing your network with **Dome Shield!****

Dome Shield provides **Web Visibility, Control** and **Protection** at the DNS-layer.

- Block Advanced Threats, Phishing, Malware and C&C Callbacks
- Create Web Filtering rules using 80+ content categories
- Enforce Protection and Web Access Policies, on and off network
- Get Real-Time Visibility for all internet connected devices

This wizard will help you setup Dome Shield **under 2 minutes!**

 **Secure my network now!**

Skip Wizard

- Click 'Secure my network now!' to start the wizard. See **Step 2 - Add your network** for help with this.
- Click 'Skip Wizard' if you plan to enroll your network at a later time.

### **Purchase a Platinum package**

There are two ways to get a platinum license:

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

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

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

## COMODO Dome Shield

### SIGNUP

1 Select Package      2 Enter Account Information      3 Done!

**Welcome**  
**You're about to start securing your network with **Dome Shield!****

Dome Shield provides **Web Visibility, Control** and **Protection** at the DNS-layer.

- Block Advanced Threats, Phishing, Malware and C&C Callbacks
- Create Web Filtering rules using 80+ content categories
- Enforce Protection and Web Access Policies, on and off network
- Get Real-Time Visibility for all internet connected devices

This wizard will help you sign up to Dome Shield **under 2 minutes!**

**Enterprise**    **MSP**

[Already have an account?](#)

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



**1**  
Select Package

**2**  
Enter Account Information

**3**  
Done!

### Dome Shield Gold

— Free —

---

Free up to 300,000 DNS Requests per Month

---

Available for Enterprises & MSPs

Active Directory not supported

---

Does not include:

- ✗ Internal IP/Subnet/IP Block Based Polices
- ✗ Internal IP Based Visibility & Monitoring
- ✗ Encrypt All DNS Traffic
- ✗ Dome Shield DNS Resolver Virtual Appliances

**GET STARTED FOR FREE**

Free, No Credit Card Required

[Are you a MSP?](#)

### Dome Shield Platinum

— for Enterprises —

---

24 x 7 x 365 Platinum Support

Includes:

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

**BUY NOW**

[1 Month Trial Option](#)

### Dome Shield Platinum

— for MSPs —

---

24 x 7 x 365 Platinum Support

Includes:

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

**BUY NOW**

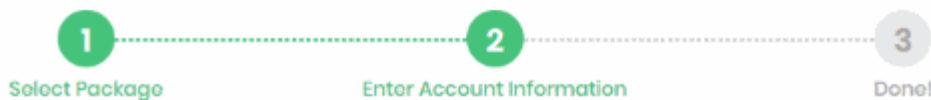
[1 Month Trial Option](#)

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

The screenshot shows a registration interface with a progress bar at the top. Step 1 is 'Select Package', Step 2 is 'Enter Account Information' (highlighted), and Step 3 is 'Done!'. Below the progress bar, the text 'Please Enter Customer Details' is centered. There are three input fields: 'Email', 'Password', and 'Confirm Password'. Below the fields is a checkbox labeled 'I have read and agree to the End User license/Service Agreement'. At the bottom, there are two buttons: 'Previous' and 'Choose License'.

- **Email** - Enter your contact mail address. You will receive the order confirmation email and license keys on this email address. Your email address doubles up as your Dome Shield username.
- **Password** and **Confirm Password** - Enter a passphrase for logging-in to your Dome Shield account. This also serves as password for your Comodo account
- **End user license agreement** - Read and agree to the terms and conditions.
- Click 'Choose License'

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



### Dome Shield Platinum

**Select License Period**

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

**License Type**      **# of Users**

Dome Shield Platinum(1-99 Users)      1

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

**Total Price (\$ 2.45 per User)**  
**\$ 2.45**

### Credit Card Details

**Credit Card No.**

**Cardholder Name**

**CVV**      **Expiration Date**

**Finish** ✓

- **Select License Period** - Pick a license term.
- **License Type:**
  - Pick a license with a range that covers the number of users you want to protect
  - The range determines your price-per-user
- **Number of users** - Specify exactly how many users you want to protect.
- Enter your payment card information and click 'Finish'.

## SIGNUP

1 Select Package      2 Enter Account Information      3 Done!

**CONGRATULATIONS! (0)**  
Your network is now secured by **Dome Shield!**

**What else can you secure and control with Dome Shield?**

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

**What else can you apply on these objects?**

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

- You will receive order confirmation and license emails.

You can now login to Dome Shield at <https://shield.dome.comodo.com/login>.

### Comodo One and ITarian Customers

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

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

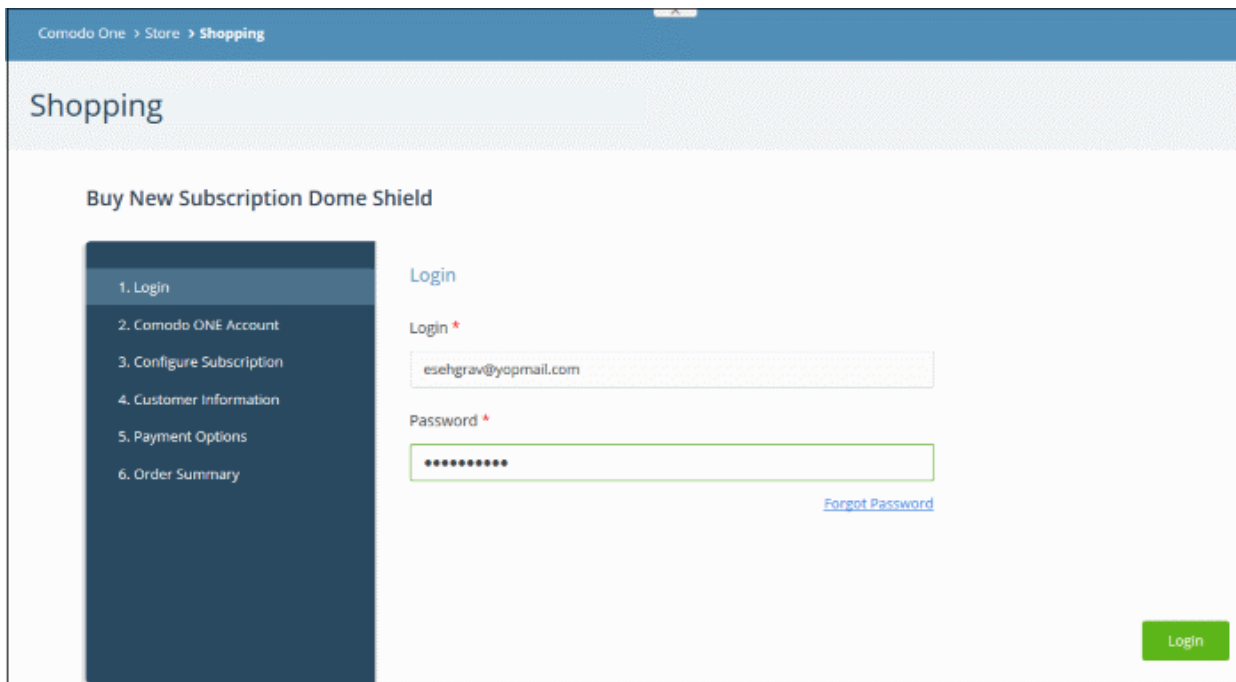
### Upgrade to a Platinum license

- Login to your C1 or ITarian account
- Click 'Management' > 'Applications'
- Select 'Dome Shield' then click the 'Subscriptions' tab

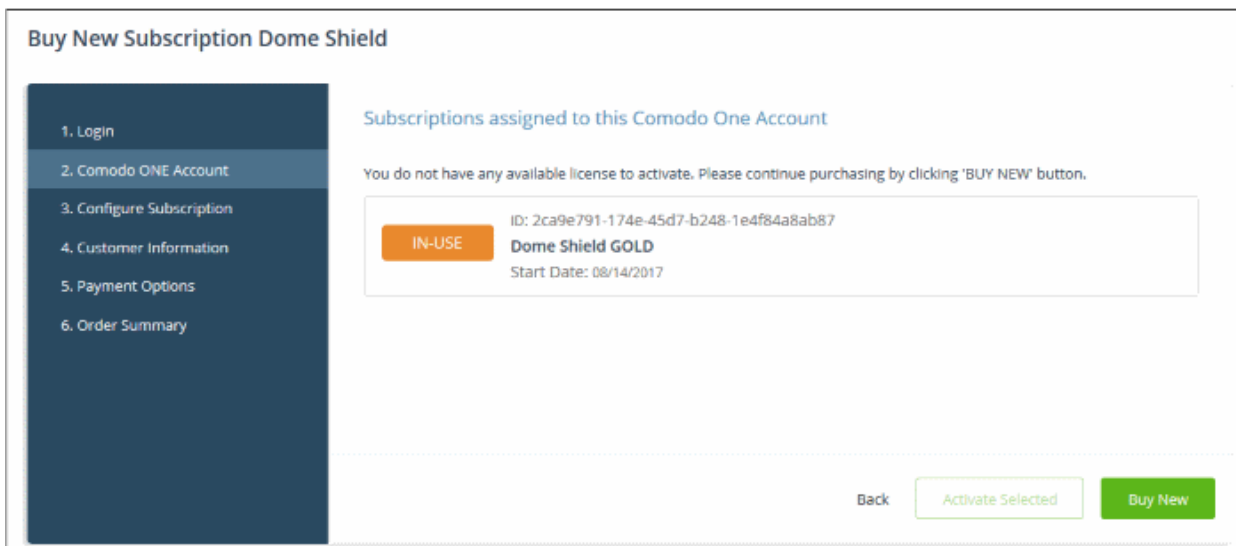
The screenshot displays the 'Applications' section of the Comodo Dome Shield dashboard. It features two main application tiles: 'Endpoint Manager' and 'Dome Shield'. The 'Dome Shield' tile is circled in red. Below the applications, there are four tabs: 'Subscriptions', 'Usage', 'Billing', and 'Settings'. The 'Subscriptions' tab is selected and also circled in red. Under the 'Subscriptions' tab, there is a 'Subscription List' section with a '+ Add New Subscription' button circled in red. The list contains two subscription entries. The first entry is 'Dome Shield GOLD MSP' with ID 'f4c8de8dc1', a quantity of 5, a start date of 07/30/2018, and a status of 'ACTIVE'. The second entry is 'Dome Shield Platinum for MSP(25000-' with ID '...', a quantity of 1, and a status of 'Credit Card'. A 'Details' sidebar is visible on the right side of the subscription list.

ID	Name	Quantity	Start Date	Price	Status
f4c8de8dc1	Dome Shield GOLD MSP	5	07/30/2018	FREE TRIAL Unlimited	ACTIVE
...	Dome Shield Platinum for MSP(25000-	1		Credit Card	

- Click 'Add New Subscription'



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



- **Activate Selected** - Platinum licenses bought via your Comodo Accounts Manager (CAM) account can be activated for use in Comodo One / ITarian.
- **Buy New** - Purchase a new Platinum license.
- Select the number of users you require and the term of the license:

### Buy New Subscription Dome Shield

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

#### Configure Subscription

Amount of Users  Users

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

#### Select Period

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

## \$14,980.00

[Back](#)

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

### Buy New Subscription Dome Shield

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

#### Customer Information

Company Name

Company Website

Phone Number \*

Street Address \*  
Street 1

Street Address 2

City \*

Country \*

State or Province

Postal Code \*

#### Billing Information

The same as Contact Information

#### Terms and Conditions

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

[Back](#)

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

- Complete your payment details


### Buy New Subscription Dome Shield

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

#### Order Confirmation

PRODUCT	LICENSE PERIOD	FULL PRICE
Dome Shield Platinum(1000-2499 Users)	1 Year	\$14,980.00
	<b>TOTAL</b>	<b>\$14,980.00</b>


#### Payment Options

Credit Card Number 

Enter Card Number

Card Holder Name  Expiration Date

[What is it?](#)

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

[Back](#) [Next](#)

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

## Login to Dome Shield

### Stand-alone Dome Shield portal



- This applies to enterprise customers who bought a license from the Dome website at <https://cdome.comodo.com/dns-internet-security.php>.
- Login at <https://shield.dome.comodo.com/login> and select 'Dome Shield'



## Sign in to Dome Shield.

Please fill in the credentials to sign in.

Login with:

Username

Password

[Forgot password?](#) ▼

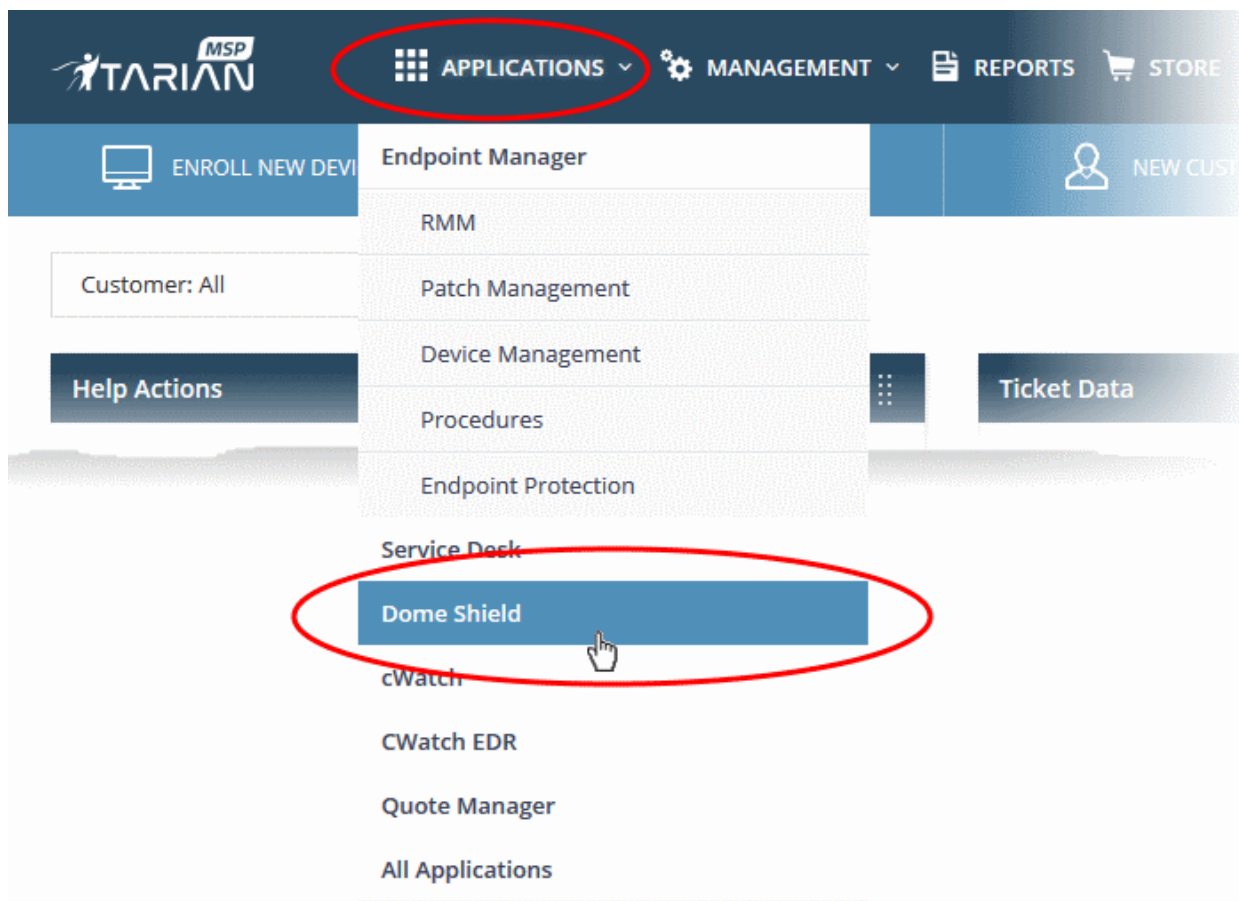
**SIGN IN**

[Create Account](#)

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

### Comodo One / ITarian Portal

- Login to your C1 or ITarian account:
  - Comodo One customers - <https://one.comodo.com/app/login>
  - ITarian customers - <https://www.itarian.com/app/msp/login>
- Username and password are case sensitive. Please make sure that you use the correct case.
- Click 'Forgot password?' if you can't remember your password.
- Click 'Applications' > 'Dome Shield' to open the Shield interface.



## Step 2 - Add Your Network

- You must first add the network from which you are connecting to Dome Shield. You can add additional networks, roaming devices and mobile devices at anytime later.
- The setup wizard lets you quickly enroll networks and roaming devices for 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 the top-right of the interface:

- Click 'Secure my network now!'

## **Step 1 - Add your IP Address**

SETUP WIZARD

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

Please enter IP Address of your Network

IPv4 Address / FQDN: 192.12.3/24      Select Company: vtiger

You can continue with your Public IP or add another IP if you prefer so.

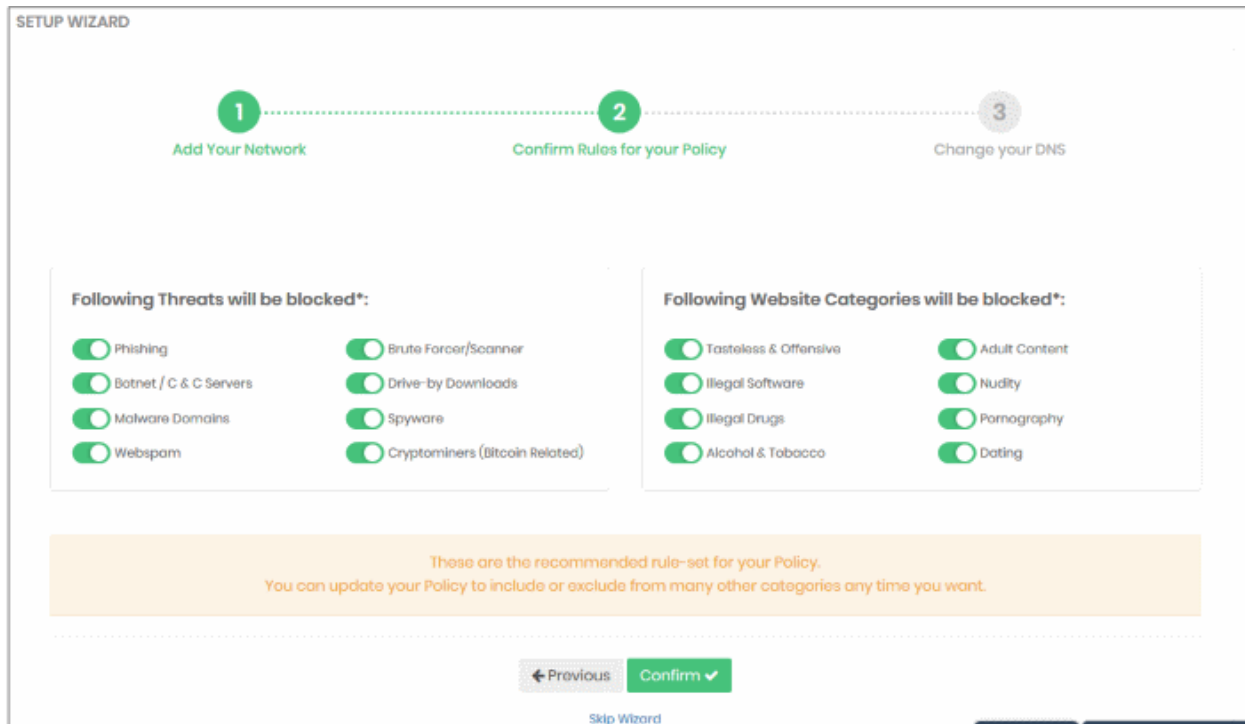
← Previous      Next →

Skip Wizard

- **IP Address / FQDN**
  - By default, this field shows the public IP of the network from which you are connecting to Dome Shield. This network is automatically activated after initial enrollment.
  - You can also add the IP address of a different network that you want to protect.. Enter the network IP address or fully qualified domain name (FQDN) in CIDR (Classless Inter-Domain Routing) notation.
  - Dome Shield can accept network prefixes from /24 to /32.
  - Note 1 - Any IP address you add here will be automatically activated for protection. Make sure you have access to change the network's DNS settings to Dome Shield, as explained in step '**Change your DNS Settings**'
  - Note 2 - Shield also supports dynamic IP addresses. You need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint. See '**Manually Add Networks to Dome Shield**' for more information.
- **Select Company** - MSPs only. Select the customer organization for which you want to enroll the network.
- Click 'Next' to configure rules for the default policy.

## Step 2 - Configure Rules for your Policy

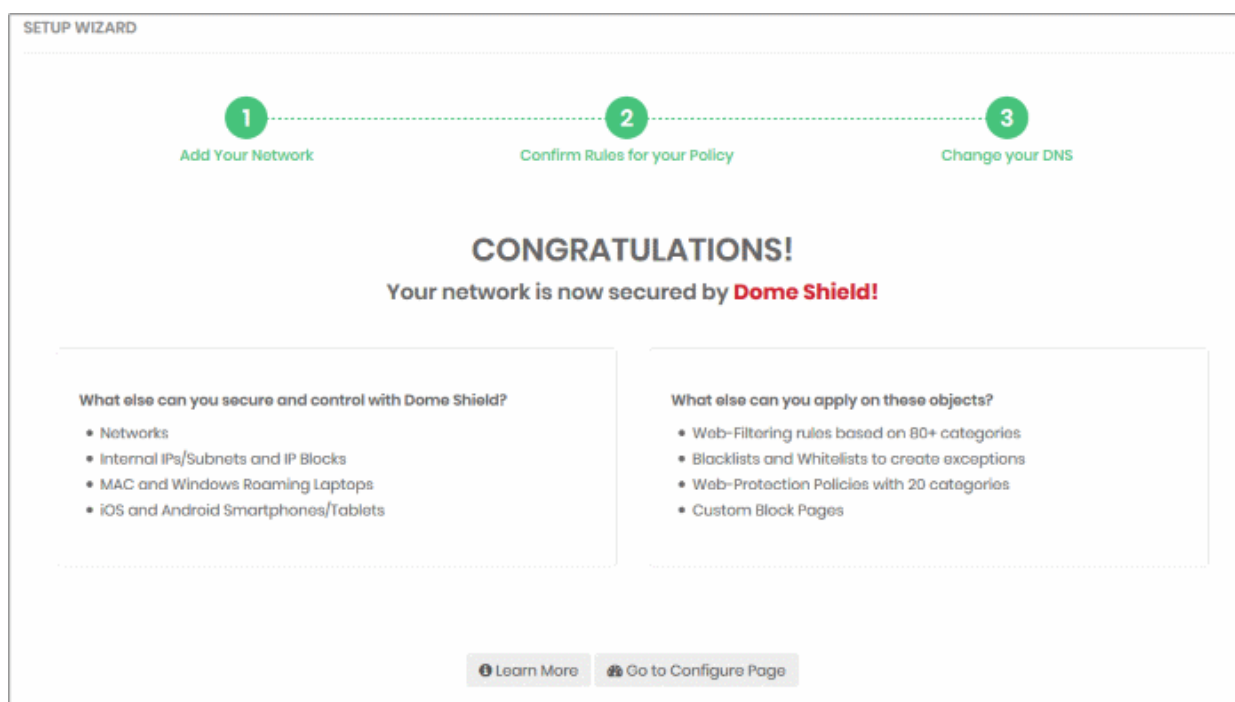
- Configure security and website category rules for the default policy. These will be immediately applied to the network on enrollment.



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

### Step 3 - Change your DNS Settings

- Change your DNS addresses to following Dome Shield addresses:
  - Preferred DNS server - 8.26.56.10
  - Alternate DNS server - 8.20.247.10
- Click 'Yes, My DNS is set to Shield' after configuring the DNS settings.



That's it. You have now added a network to Dome Shield. Note - Networks that are added via the setup wizard will be automatically labeled as 'MyNewtork' with date appended to the label.

- Click 'Configure' > 'Objects' > 'Networks' in the Dome interface to see all networks that you have added.
- The specified static IP address for your network will automatically become active.
- Note:
  - You can also skip the setup wizard and add networks, roaming and mobile devices manually later on. See **Step 3**.
  - To support dynamic IP addresses, you need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint.
  - See '**Manually Add Networks to Dome Shield**' for more information.

## Step 3 - Enroll Networks and Devices For Protection

You can enroll multiple fixed networks and/or mobile/roaming devices to Dome Shield.

The following sections explain how to:

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

### Enroll Networks

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

There are three ways you can enroll additional networks:

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

2. Add networks manually:
  - Networks with static IP addresses can be enrolled by specifying their IP addresses in CIDR notation
  - Networks with dynamic IP addresses can be enrolled by installing an IP updater agent on the network
  - See **Add Networks Manually** for detailed help with this
3. Import networks by deploying local resolvers:
  - Install a local resolver (LR) as a virtual appliance on the network
  - Once deployed, the network will be automatically imported to Dome Shield
  - See **Import networks by deploying local resolvers** for help to setup the local resolvers

## Add Networks Manually

- You can enroll multiple networks for Dome Shield protection. Networks will remain in 'pending' status until the IP/FQDN has been approved by Comodo. Please contact your Comodo account manager or [domesupport@comodo.com](mailto:domesupport@comodo.com) if you have questions on pending networks.
  - **Static IP addresses.** 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.** Install the Comodo IP updater agent to keep Dome 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.
- After enrolling a network, please also make sure all endpoints are configured to use Shield DNS:
  - Preferred DNS server - 8.26.56.10
  - Alternate DNS server - 8.20.247.10
- See the following sections for help to enroll networks with static and dynamic IP addresses:
  - **Add Networks with Static IP Address(es)**
  - **Add Networks with Dynamic IP Address(es)**

## Add Networks with Static IP Address(es)

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

**Add Network**
✕

**Name**

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

**IPv4 Address / FQDN**

**is Dynamic ?**

**Trusted Network Behaviour**

**Disable Roaming Agent when on this network**

**Please select company**

**Remark**

**Additional Settings** +
Add

Add Network - Form Parameters	
Field	Description
Name	Enter an appropriate label for the network
IP Address / FQDN	<p>The IP address or Fully qualified domain name of the network.</p> <ul style="list-style-type: none"> <li>Enter the IP address of the network in CIDR (Classless Inter-Domain Routing) notation.</li> <li>Dome Shield can accept network prefixes from /24 to /32.</li> </ul> <p><b>Note:</b> By default, this field will show the public IP address of the network from which you are connecting to Dome Shield. Any additional IPs you add which are different to the one detected will need to be approved by Comodo. To activate these networks, please contact our support at <a href="mailto:domesupport@comodo.com" style="color: #c00000;">domesupport@comodo.com</a></p> <p>Is Dynamic? - Only select if you want to enroll a network with a dynamic IP address. See <a href="#" style="color: #c00000;">Add Networks with Dynamic IP addresses</a> for more details.</p>
Trusted Network Behavior	<p><b>Disable Roaming Agent when on this network</b> - Select whether policies applied to roaming agents should be active when they connect to this network.</p> <ul style="list-style-type: none"> <li>Enabled = The Shield agent on roaming devices are disabled when they are inside the network. The network policy will apply to the roaming device.</li> </ul>



	<ul style="list-style-type: none"> <li>Disabled - The roaming device's policy will remain active.</li> </ul>
Please select company	<p>MSPs only</p> <ul style="list-style-type: none"> <li>Select the customer organization for which you want to enroll the network.</li> </ul>
Remark	Enter any notes about the network being added.
<p><b>Additional Settings</b> - These settings apply only to roaming devices which have the Dome agent installed.</p> <ul style="list-style-type: none"> <li>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.</li> <li>See '<b>Enroll Roaming Devices</b>' for more details on Shield agents.</li> </ul>	
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. Next.

### Configure your network's DNS to forward queries to Shield DNS

This will ensure all endpoints receive cWatch protection. 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, see <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

#### Important Notes:

- You 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
- By default, no rules are applied to new networks. You need to create and apply a policy to activate rules. See '**Step 5 - Create and Apply Security Policies**' for advice on how to deploy web protection rules to networks.
- Please contact our support at [domesupport@comodo.com](mailto:domesupport@comodo.com) if you face any problems regarding this.

### Add Networks with Dynamic IP Address(es)

- 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 update agent on an endpoint in the network

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

### Add Network ✕

**Name**

If you create a Location with an IP address different than the one that you're currently connecting to 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](mailto:domesupport@comodo.com)

**IPv4 Address / FQDN**

  **is Dynamic ?**

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

**Guidelines:**

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

Add Networks - Form Parameters	
Field	Description
Name	Enter an appropriate label for the network
IP Address / FQDN / Dynamic	<p>'Is Dynamic?' - select enroll a network with dynamic IP addresses. A message box will appear with guidance on enrolling networks with dynamic IP addresses..</p> <ul style="list-style-type: none"> <li>Click the 'Windows Dynamic IP Updater' link under 'Download' in the message box and save the agent setup file.</li> </ul>
Trusted Network Behavior	<p><b>Disable Roaming Agent when on this network</b> - Select whether policies applied to roaming agents should be active when they connect to this network.</p> <ul style="list-style-type: none"> <li>Enabled = The Shield agent on roaming devices are disabled when they are inside the network. The network policy will apply to the roaming device.</li> <li>Disabled - The roaming device's policy will remain active.</li> </ul>
Please select company	<p>MSPs only</p> <ul style="list-style-type: none"> <li>Select the customer organization for which you want to enroll the network.</li> </ul>
Remark	Enter a description for the network being added.
<p><b>Additional Settings</b> - These settings apply only to roaming devices which have the Dome agent installed.</p> <ul style="list-style-type: none"> <li>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.</li> <li>See '<b>Enroll Roaming Devices</b>' for more details on Shield agents.</li> </ul>	
Host File Configuration	Enter the name and IP address of your host in the respective fields. Click the '+' button to add more host entries. To remove an entry, click the corresponding trash can icon.

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

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



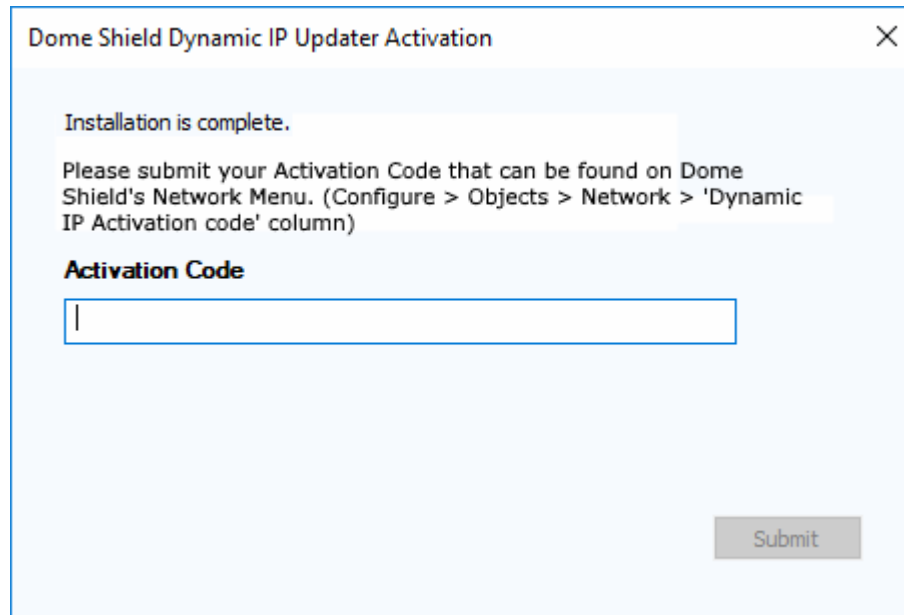
- Transfer the agent setup files to an endpoint in the target network

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

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

## Step 2 - Activate the agent

The activation dialog will appear after installing the agent:



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

#	Company	Name	Type	IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions
1	name	MyNetwork_2018-11-08	Static	172.12.3/32	N/A	Disable	Active		✎ ✖
2	name	MyNetwork_2018-11-07	Static	198.200.12/32	N/A	Disable	Active		✎ ✖
3	vtiger	gozdo	Static	10.100.196.208/32	N/A	Disable	Active		✎ ✖
4	vtiger	demo_ip	Dynamic	95.176.0.26/32	5c753ed0-8229-4add-b848-fa5c0bc433e7	Enable	Active		✎ ✖
5	vtiger	MyNetwork_2018-11-02	Static	10.95.47.85/32	N/A	Disable	Active		✎ ✖
6	vtiger	London -> Manchester2	Static	172.31.21.214/32	N/A	Enable	Active		✎ ✖

- Paste the code and click submit

After successful activation, the network will be added and displayed in the list.

Note - no rules are applied to the new networks by default. You can apply a security policies according to your requirements. See **Step 5 - Create and Apply Security Policies** for help with this.

## Import networks by deploying local resolvers

- The local resolver VM is an alternative method of importing networks to Dome Shield. The feature is available only with Platinum licenses.
- Download the local resolver setup package and deploy it as a virtual machine on the network.
- Once deployed, the network will be automatically imported to Dome Shield.
- The resolver will forward public DNS queries to Dome Shield global DNS servers.
- The resolver method offers some key advantages over 'direct' enrollment:
  - 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.

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

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

## Step 1 - Download the Setup File

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

The screenshot shows the Comodo Dome Shield Platinum web interface. The 'Configure' tab is selected, and the 'Sites & Virtual Appliances' section is active. The 'Download Component' button is circled in red. A red arrow points from this button to a modal window titled 'DOWNLOAD COMPONENTS'. The modal window contains the following text:

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 LR's.  
Check [How To Deploy](#) to start!

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

- Click the 'Download' button beside the VM application you want to use
- The setup package will be downloaded in .zip format
- The package contains an OVA or HYPER-V file depending on the VM application you chose. The package

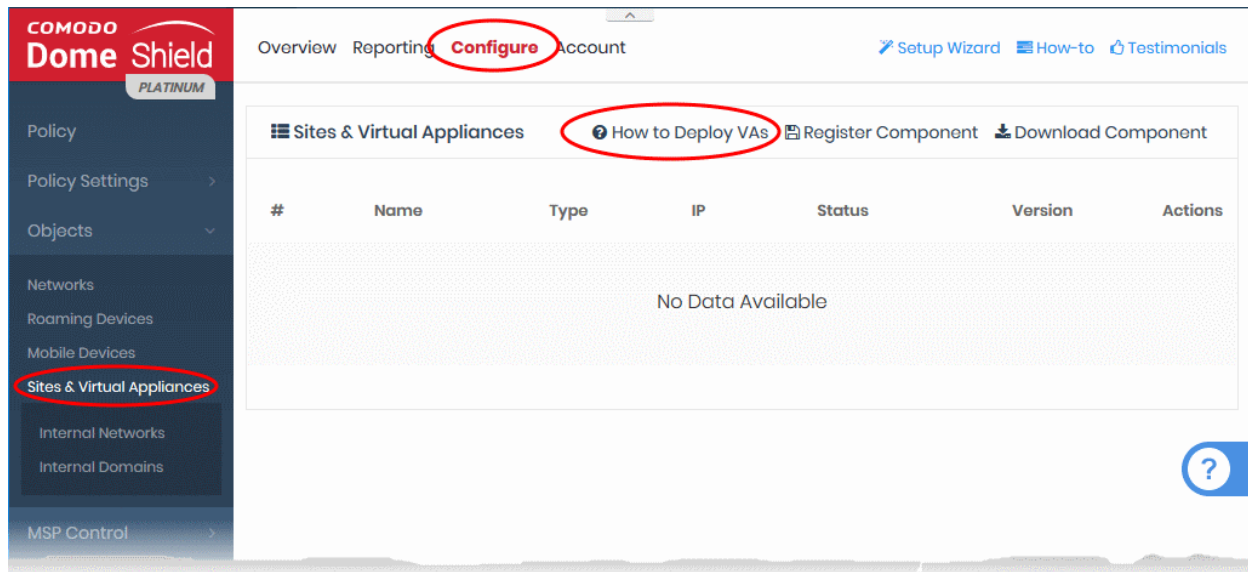
also contains a text file with login credentials to access the appliance.

## Step 2 - Setup the Master Virtual appliance

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

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

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



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

### HOW TO DEPLOY SHIELD VIRTUAL APPLIANCES

#### A. Introduction

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

#### B. Prerequisites

- Prerequisites

#### C. Deployment Guidelines

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

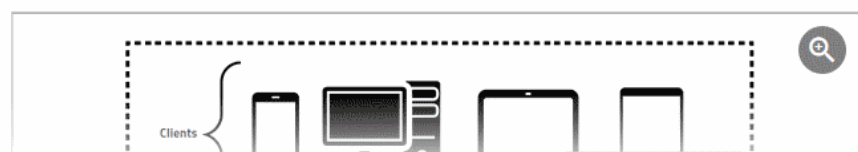
#### D. Deploy Shield Local Resolvers

- Before Deployment

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

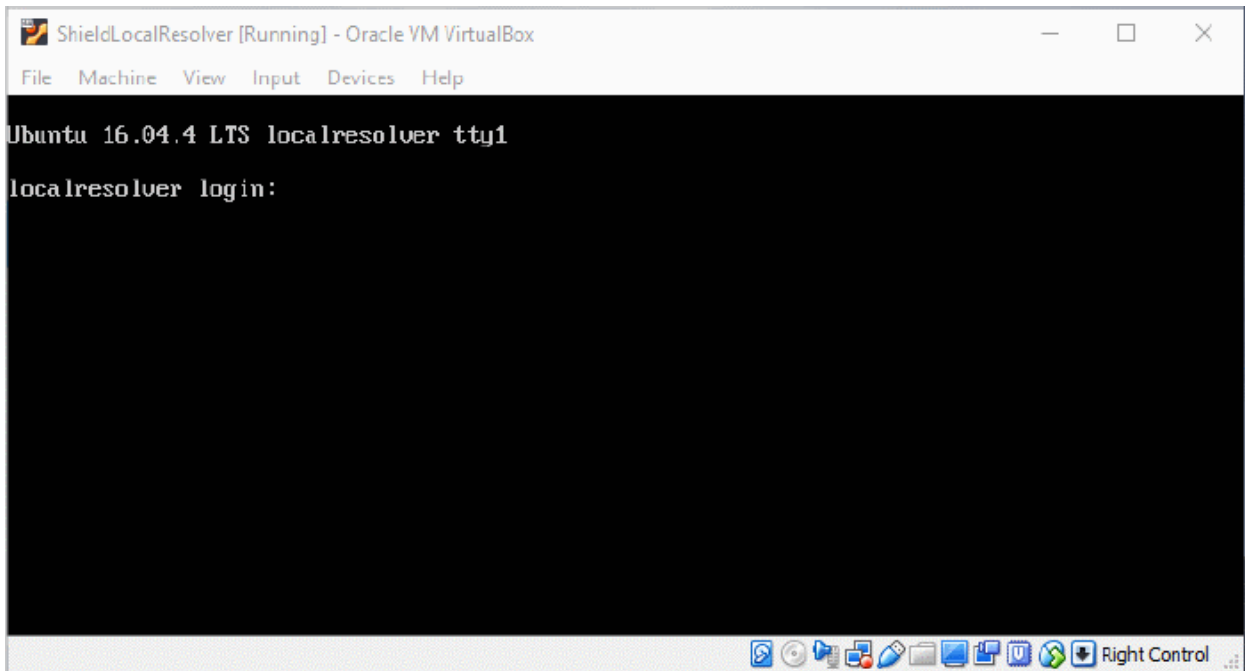
Comodo Dome Shield Local Resolver Virtual Appliances (Shield LR) are virtual machines that are compatible with VirtualBox, VMware ESXi and Windows Hyper-V hypervisors. Acting as conditional DNS forwarders, Comodo Dome Shield Local Resolver Virtual Appliances forward public DNS queries to Dome Shield's global DNS servers, while encrypting and authenticating 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.

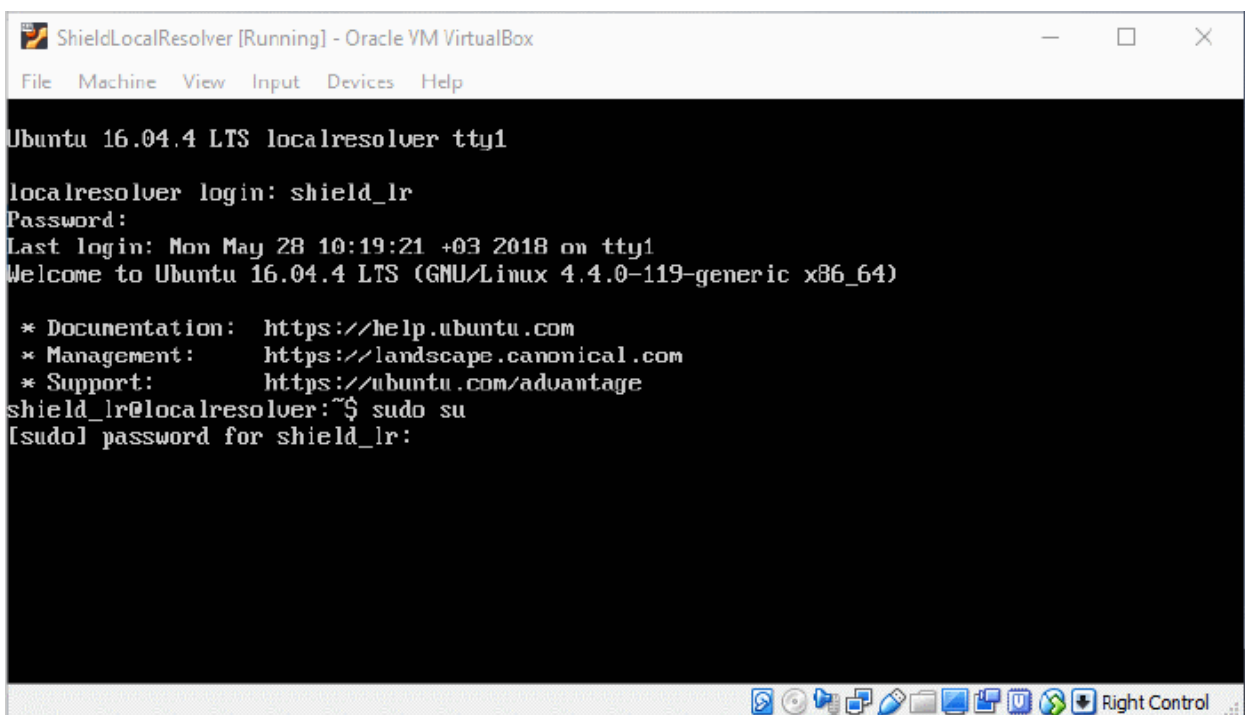


## Configure the Local Resolver

- Start up the VA once installation is complete.



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



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

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

```

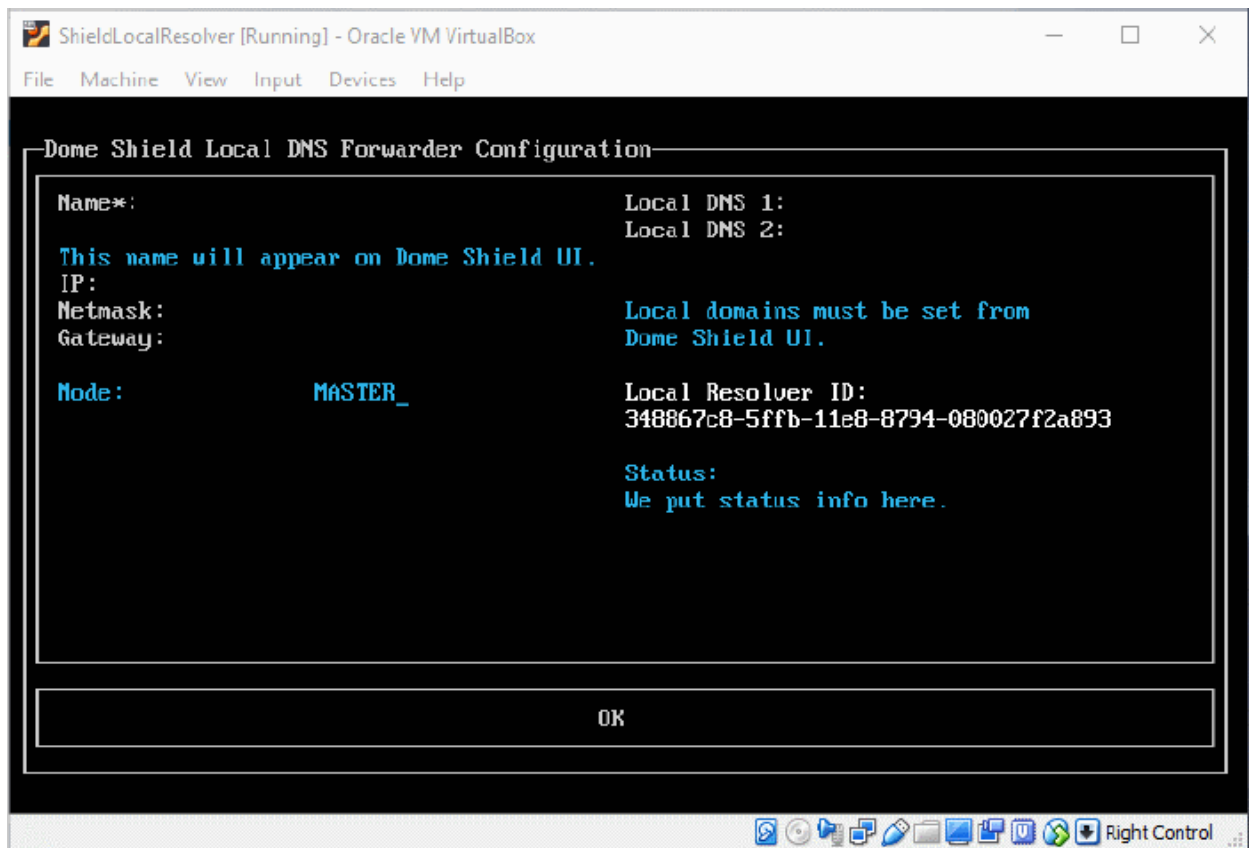
ShieldLocalResolver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

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.



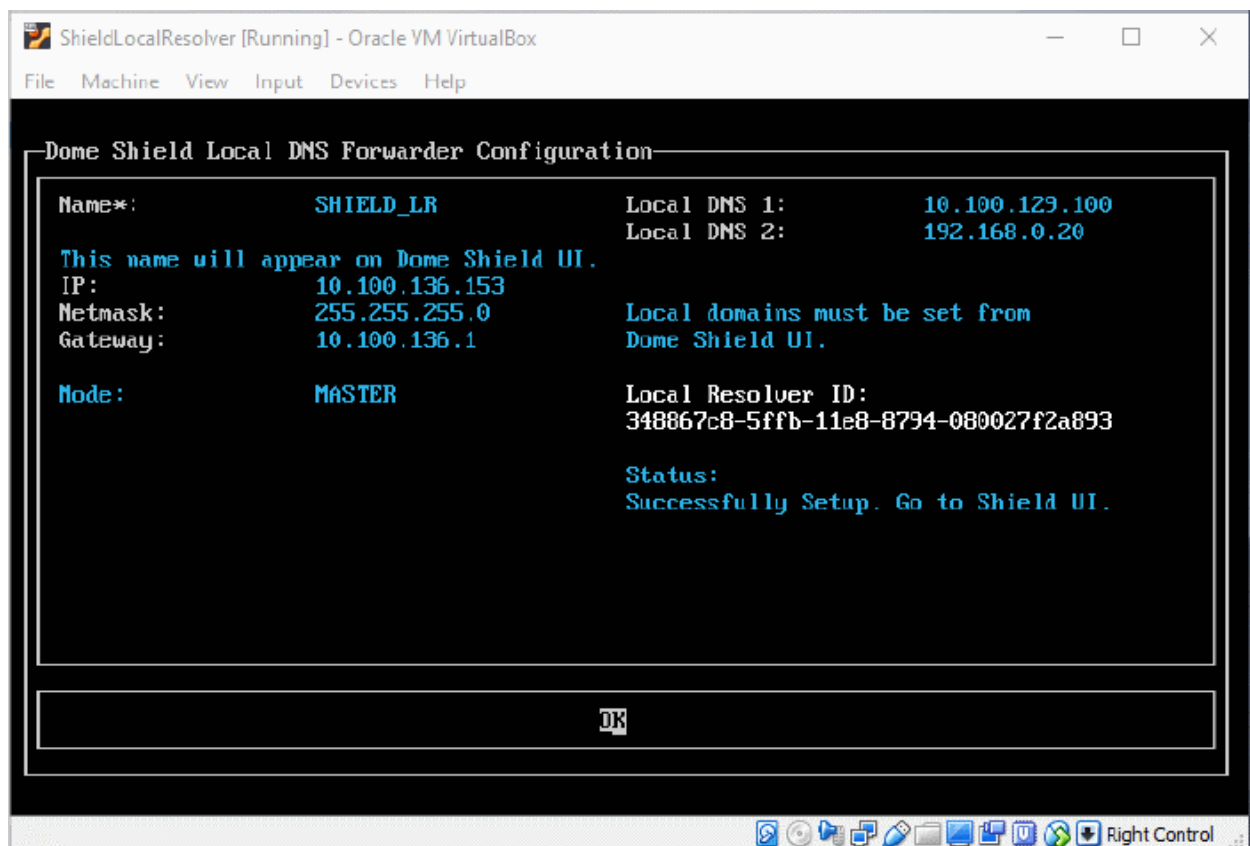
LR Configuration Screen - Table of Parameters	
Form Element	Description
Name	Type a label to identify the master VA. This name will appear in the Dome Shield interface after registration.
IP	Assign an IP address to the local resolver.
Netmask	Enter the LR netmask
Gateway	Enter the IP address of the network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



LR Configuration Screen - Table of Parameters	
Form Element	Description
Local DNS 1 and Local DNS 2	Enter the IP addresses of the primary and secondary DNS servers in the network.
Local Resolver ID	Make a note of this ID string. You need this to register the resolver and import the network into Dome Shield. See Step 3 - Register the Master VA for more help.
Status	Progress of the VA setup process.

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

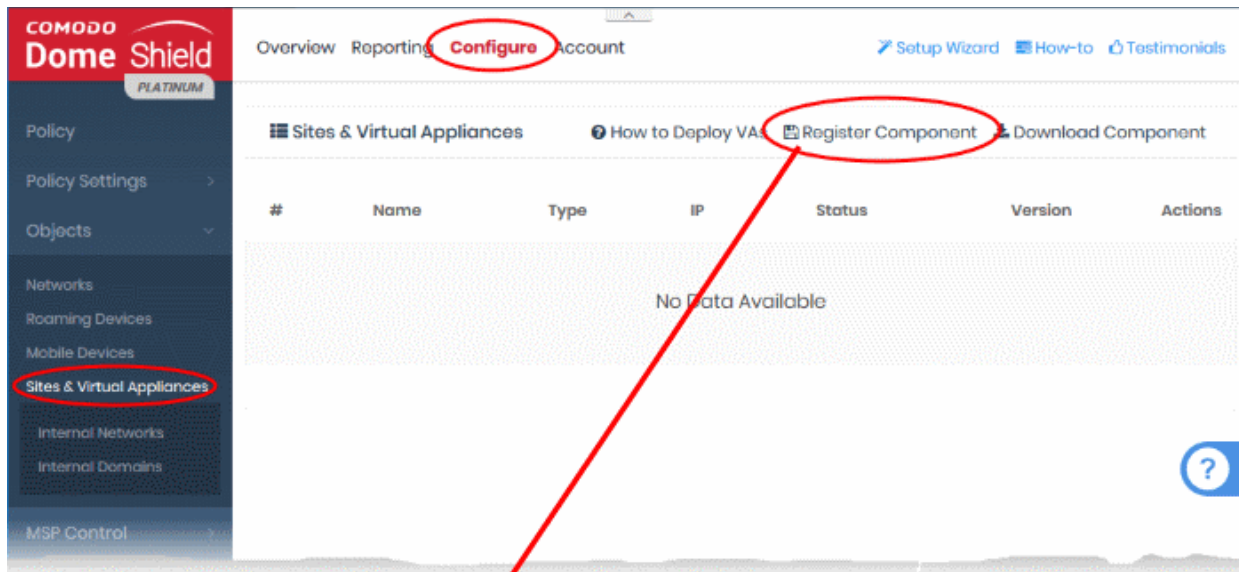
Your configuration will be saved.



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

### Step 3 - Register the Master VA

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



### ADD LOCAL RESOLVER ✕

**Enter Registration ID of the Component**

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

**Enter Site Name**

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

**Select Company**

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

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

'Add Local Resolver' dialog - Table of Parameters	
Form Element	Description
Enter Registration ID of the	The local resolver identity string generated for the resolver during setup. See

'Add Local Resolver' dialog - Table of Parameters	
Form Element	Description
Component	the last screen in <b>Step 2 - Setup the Master Virtual appliance</b> if you need help.
Enter Site Name	Type a label for the network you are about to import. The name is used to identify the network in the Dome Shield interface.
Select Company	MSPs' only. <ul style="list-style-type: none"> <li>Choose the customer organization whose network you want to import</li> </ul>

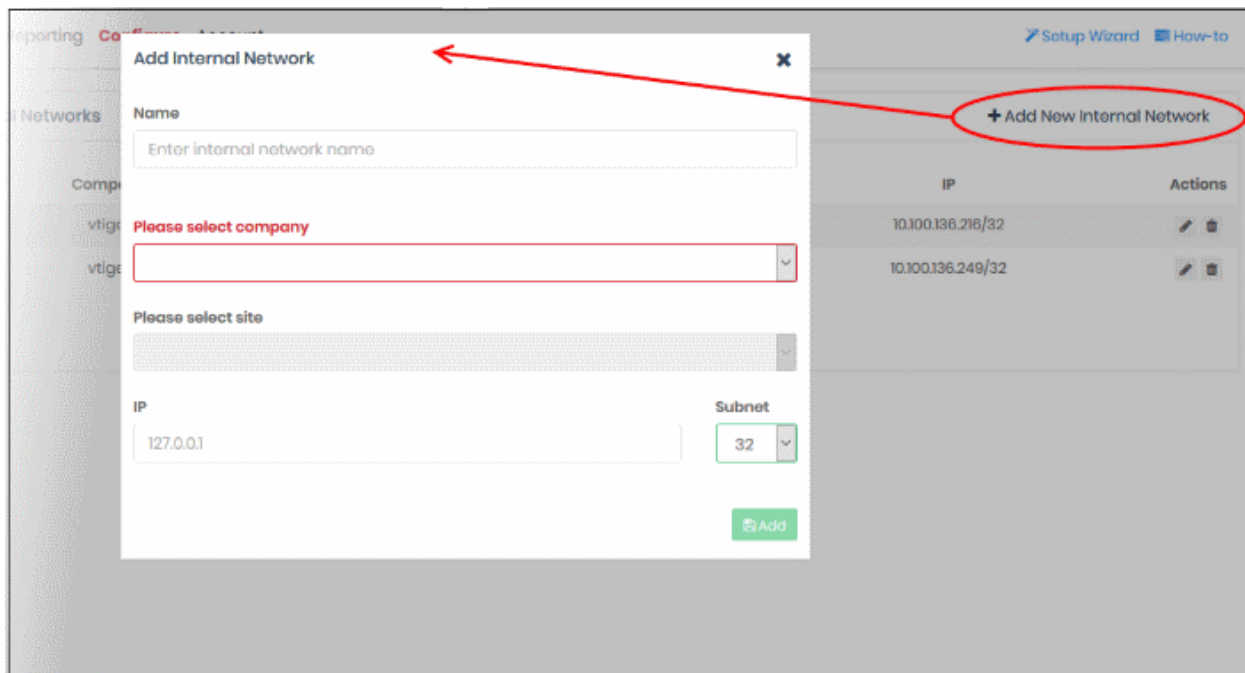
- Click 'Save' to register the local resolver and import the network

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

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

### Add Internal Network Objects (optional)

- Login to Dome Shield
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances' > 'Internal Networks'
- Click 'Add New Internal Network'



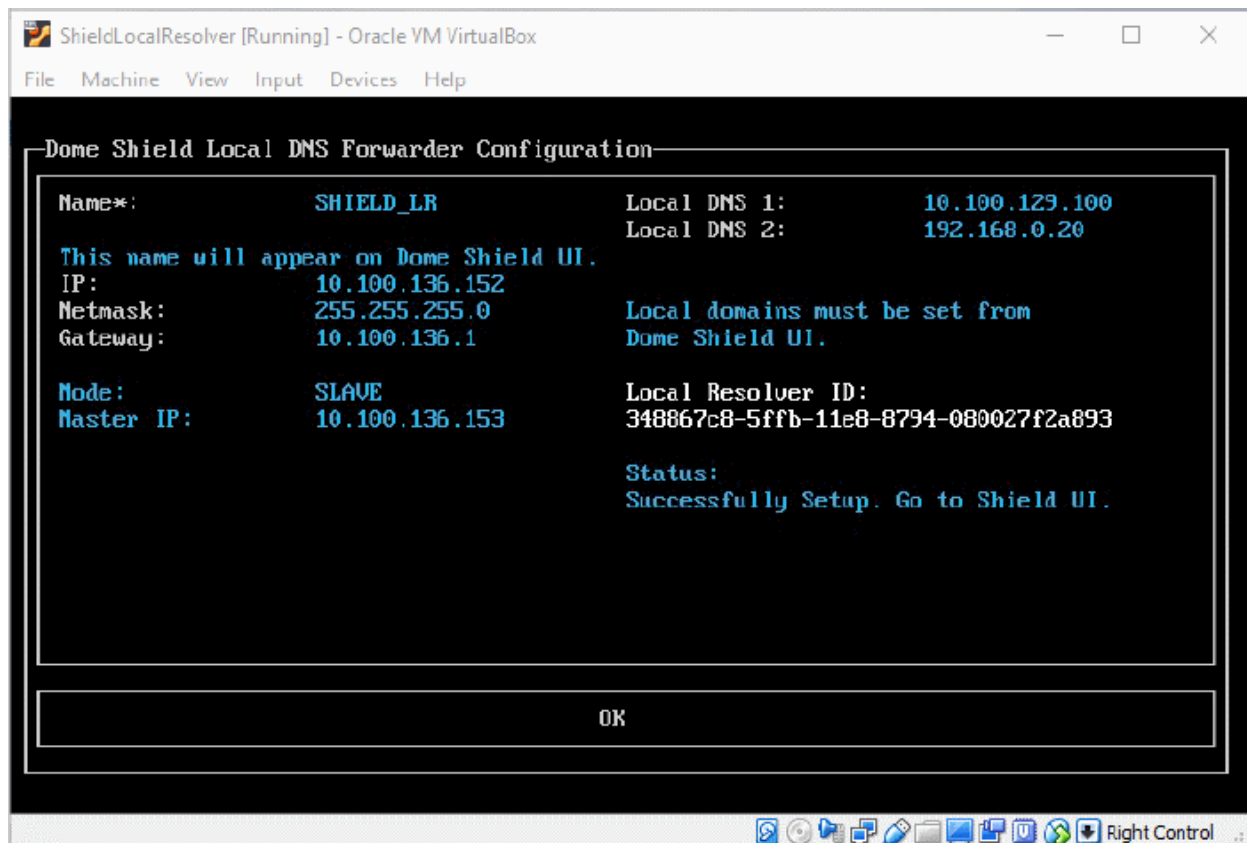
'Add Internal Network' dialog - Table of Parameters	
Form Element	Description
Name	Label of the internal network object. This name appears in the object drop-down under the network site when you create a policy.
Please select company	MSP customers only. <ul style="list-style-type: none"> <li>Choose the company for whom you want to add the network</li> </ul>

'Add Internal Network' dialog - Table of Parameters	
Form Element	Description
Please select site	Choose the site to which the internal network belongs
IP	<p>IP address of the internal network in CIDR notation.</p> <ul style="list-style-type: none"> <li>• Enter the start IP address of the internal network block.</li> <li>• Select the network prefix from the 'Subnet' drop-down.</li> <li>• Dome Shield can accept network prefixes from /24 to /32.</li> <li>• To add a single endpoint, enter the IP address of the endpoint and choose 32 as network prefix</li> </ul>

- 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.
- Repeat the process to define more internal network objects

#### Step 4 - Setup the Slave VA (Optional)

- For high-availability, we recommend you deploy two local resolvers (LR's) for each network you import. The resolvers can be configured in a master-slave relationship. If the master fails, the slave will continue to forward queries to Dome Shield DNS.
- Install another local resolver virtual appliance on a different server/host on the network. The process is similar to setting up the master LR.
- Start the VA and open the configuration screen as explained **above**. Setup the VA as a slave resolver:



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

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

Your configuration will be saved. The Local Resolver will be automatically registered as 'Slave' to the pre-registered 'Master' LR.

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

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

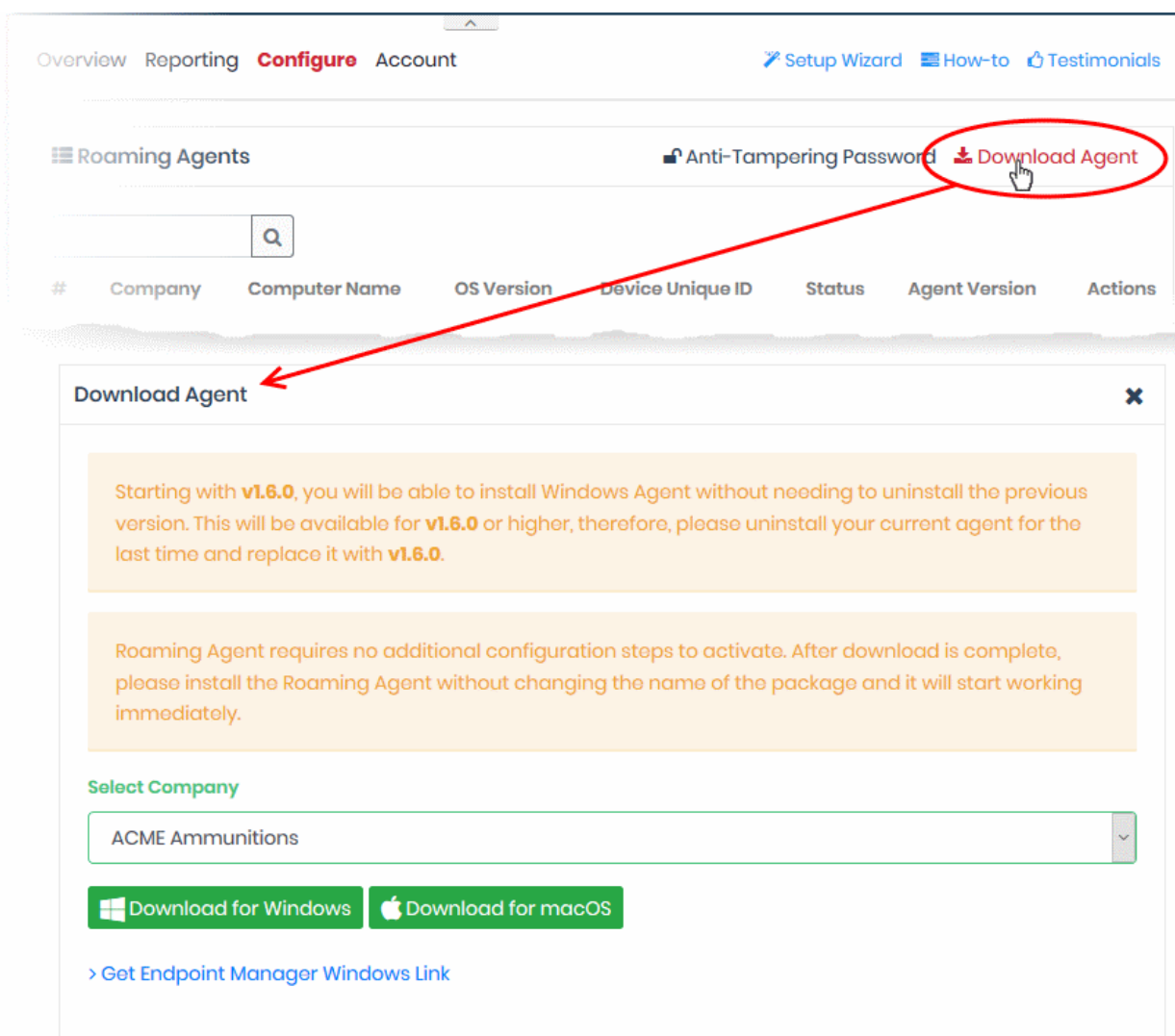
- Preferred DNS server - IP address assigned to the Master LR VA
- Alternate DNS server - IP address assigned to the Slave LR VA

## Enroll Roaming Devices

- Install the Shield agent on Windows and Mac devices to protect them when they are outside your network.
  - Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'
  - You can manually install the agent on devices, or install it remotely through Endpoint Manager (formerly ITSM).
- Once the agent is installed, the devices will be automatically added to Dome Shield. You can deploy policies to the devices as required.
- Set an anti-tampering password to prevent users uninstalling the agent from the device. Windows devices only.

To add new devices

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




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

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

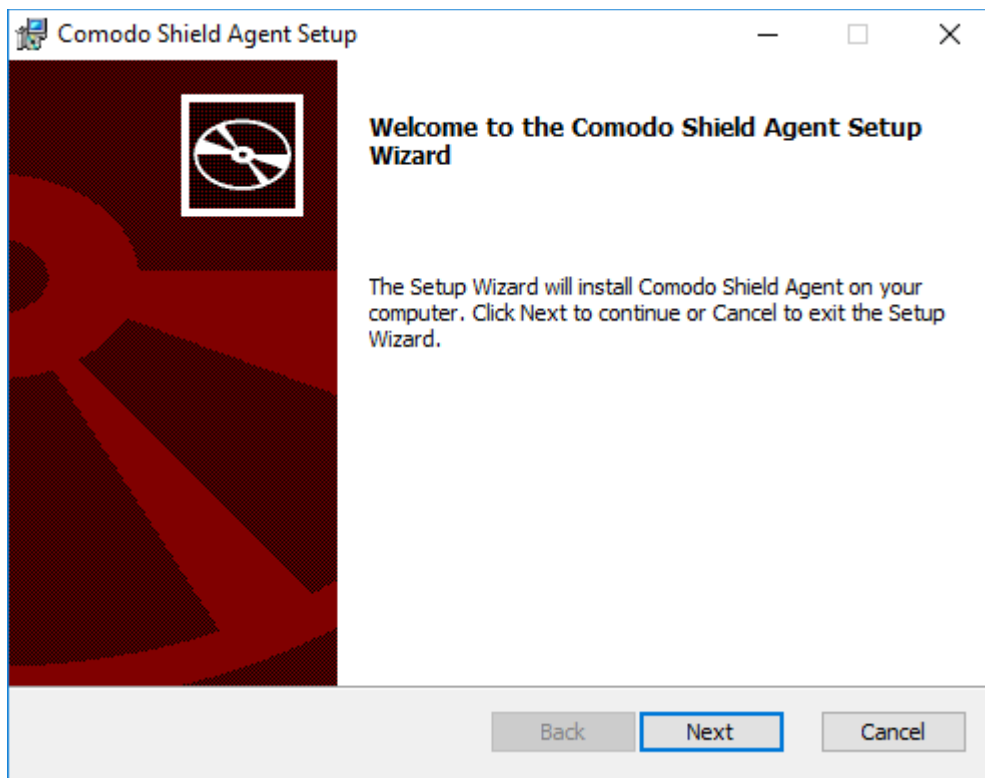
## Enroll Windows devices

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

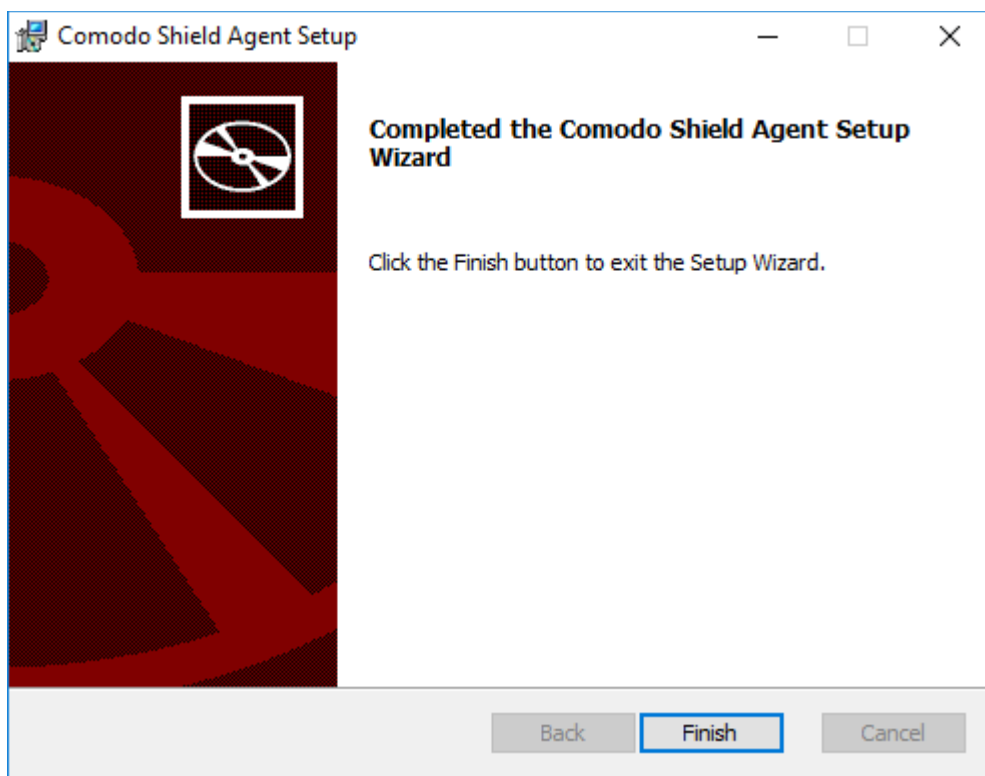
Next, install the agent on the device(s).

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

The installation wizard will start.



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



- Click 'Finish'

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

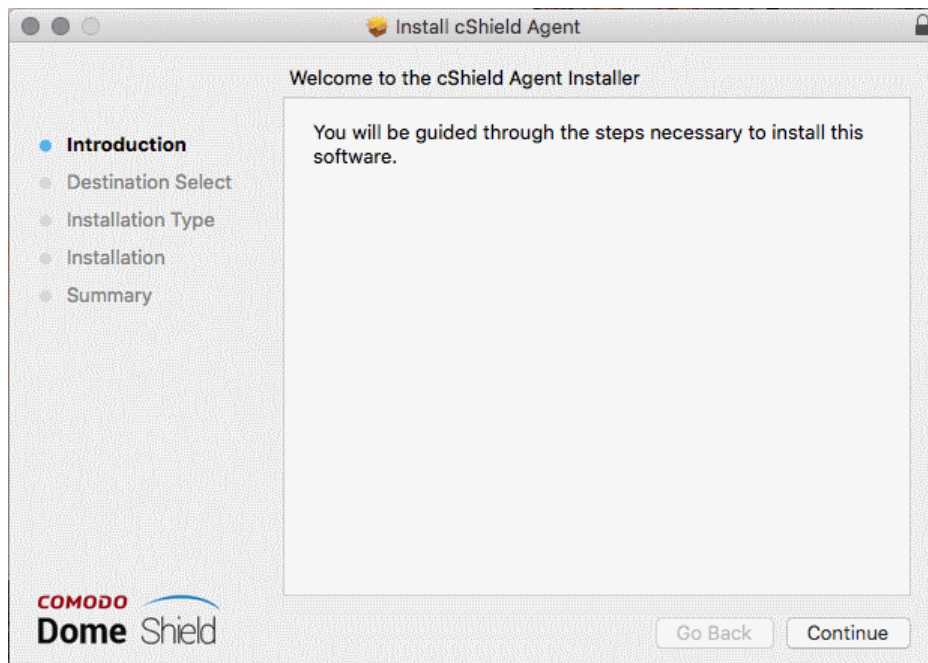
- Note - no security rules are applied to roaming device by default. You can create and apply device specific policies according to your requirements.
- See '**Step 4**' and '**Step 5**' for advice on how to configure and deploy security policies to roaming devices.

## Enroll Mac OS devices

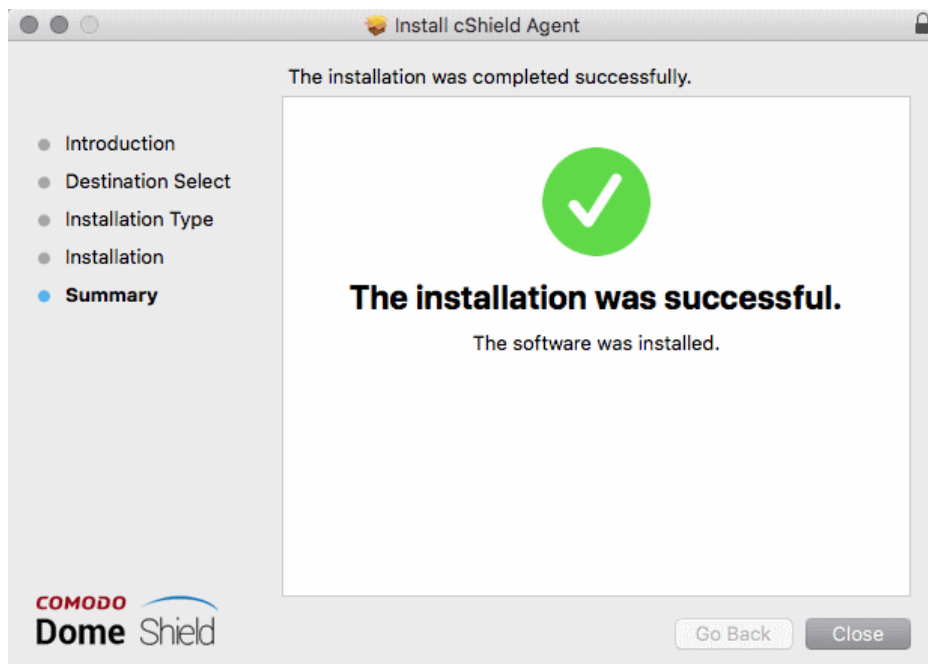
- Click the 'Download for Mac OS' button in the 'Download Agent' dialog. The installation file is in .pkg format.
- Transfer the agent to the Mac OS devices that you want to enroll.

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

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



- Click 'Continue' and follow the wizard.
- 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. You can create and apply device specific policies according to your requirements.



- See '**Step 4**' and '**Step 5**' for advice on how to configure and deploy security policies to roaming devices.

## Import Windows Devices from Endpoint Manager

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

**Download Agent** [X]

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

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

Select Company

ACME Ammunitions

Download for Windows Download for macOS

> Get Endpoint Manager Windows Link

Download for Windows Download for macOS

Get Endpoint Manager Windows Link

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

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

Process in brief:

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

## Configure Anti-Tampering Password

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

## Set an uninstallation password

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Anti-Tampering Password' on the top right

The screenshot shows the 'Roaming Agents' configuration page. A red circle highlights the 'Anti-Tampering Password' link in the top right corner. A red arrow points from this link to a modal window titled 'Anti-Tampering Password'. The modal contains the following text:

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

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

**Select Company**

postprodtest

**Password**

password

Save

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

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

## Enroll Mobile Devices

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

- **Dome Shield App** - Includes a VPN client and a VPN profile.

- **VPN Profile** - Contains only the profile. Android users need to install the StrongSwan VPN client.

## To enroll mobile devices

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

The screenshot shows the 'Mobile Devices' management page. At the top right, there are links for 'Setup Wizard', 'How-to', and 'Testimonials'. Below these is a table with columns: 'Remark', 'Mode', 'Status', 'Last Login/Logout Activity', and 'Actions'. One row is visible with 'VPN + Mobile Agent' in Mode and 'Installed, Not Active' in Status. A red circle highlights the '+ Add New Mobile Device' button in the top right corner of the table. A red arrow points from this button to the 'ADD MOBILE DEVICE' modal window shown below.

**ADD MOBILE DEVICE** [X]

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**

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

Please select company

[Dropdown menu]

[Add]

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

mobile devices

- Click 'Add'

## VPN

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

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

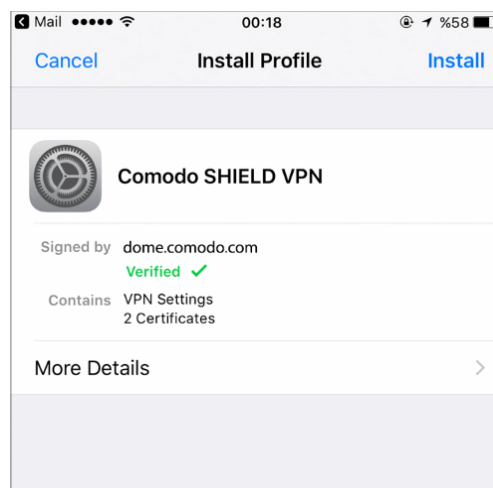
The user is initially added to the list with a device status of 'Not installed':

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

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

## Instructions for iOS

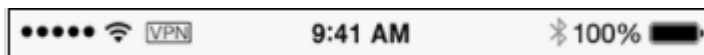
- Tap the attachment 'iOS\_VPN\_Profile' in the mail
- Install the profile as shown below:



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

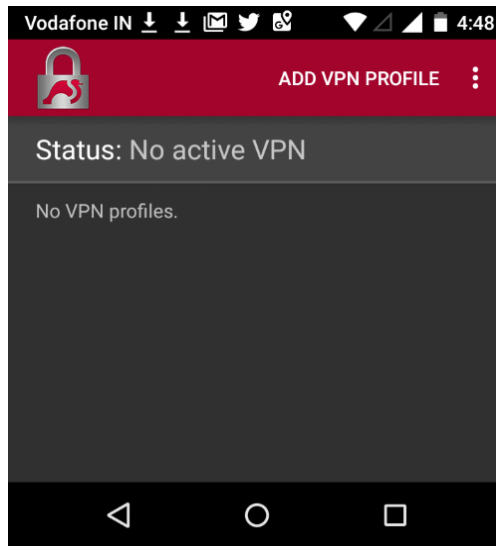
- You also need to trust the SSL certificates in iOS in order to view HTTPS pages over the VPN.
- Go to 'Settings' > 'General' > 'About' > 'Certificate Trust Settings' and enable full trust for root certificates.

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

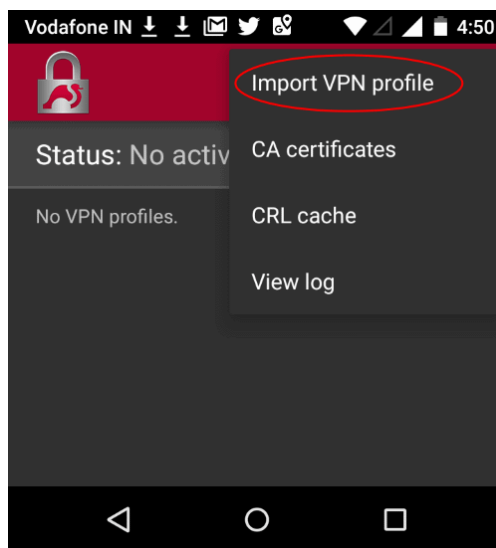


## Instructions for Android

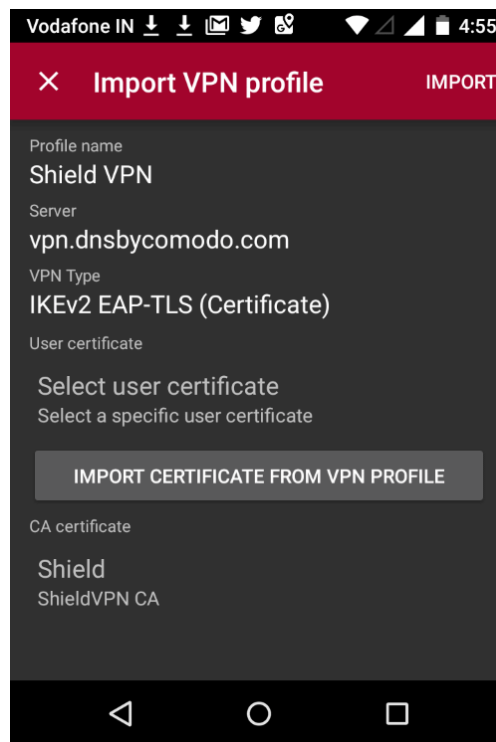
- Open the enrollment mail and select 'Android\_VPN\_Profile'
- Open StrongSwan VPN app:



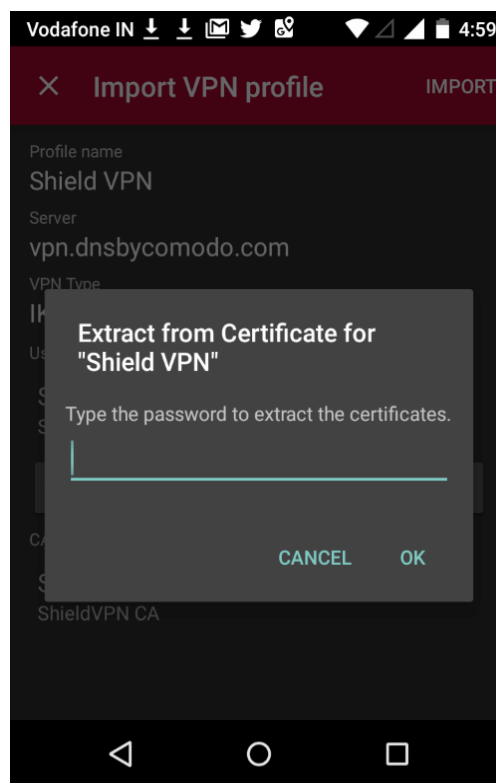
- Select 'Add VPN Profile' > 'Import VPN profile':



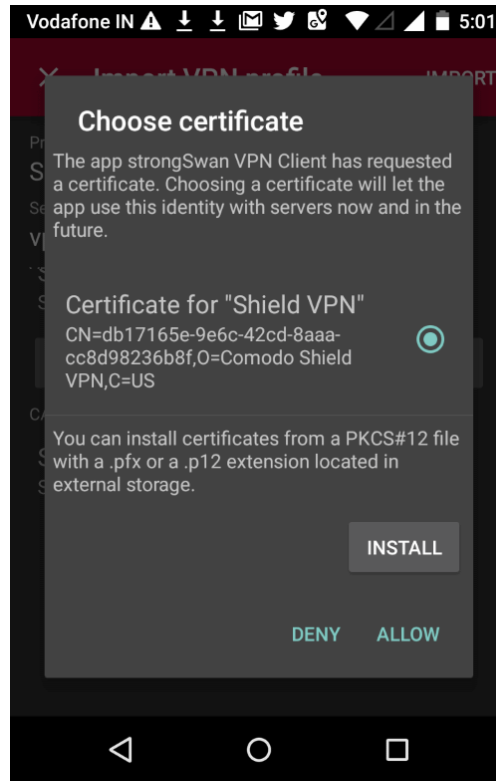
- Open the 'Android\_VPN\_Profile' that you saved earlier



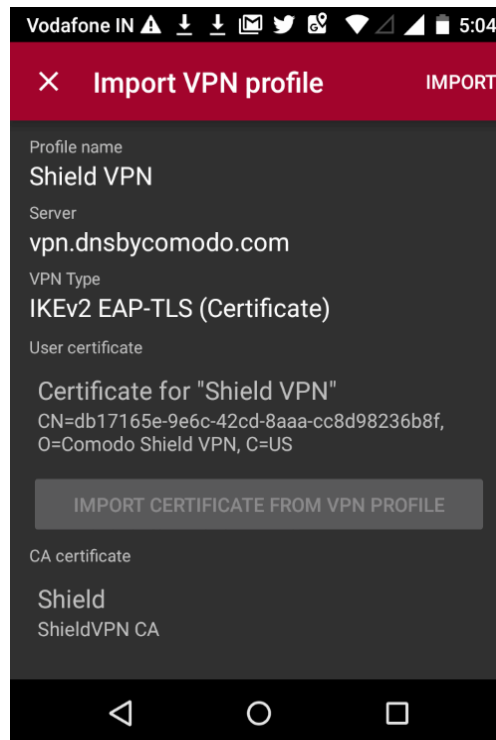
- Select 'Import Certificate from VPN Profile'



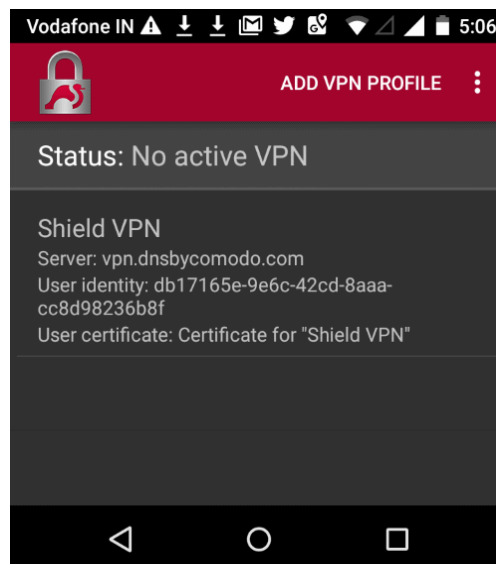
- Enter the password in the email and select 'OK'



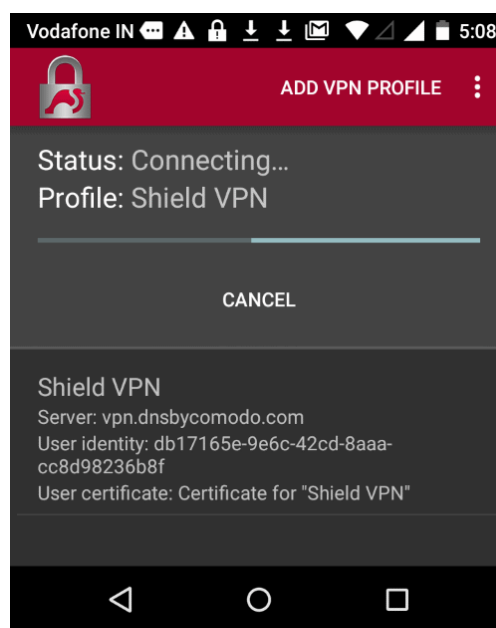
- Tap 'Allow' instead of 'Install'



- Select 'Import' at the top-right

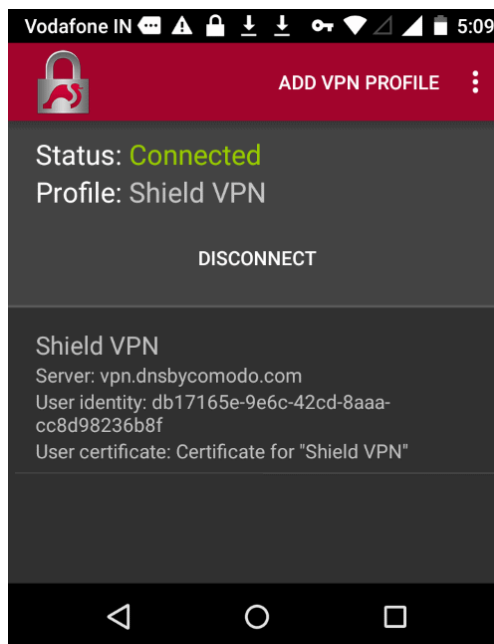


- Open the profile you just imported to start the connection to Dome Shield:



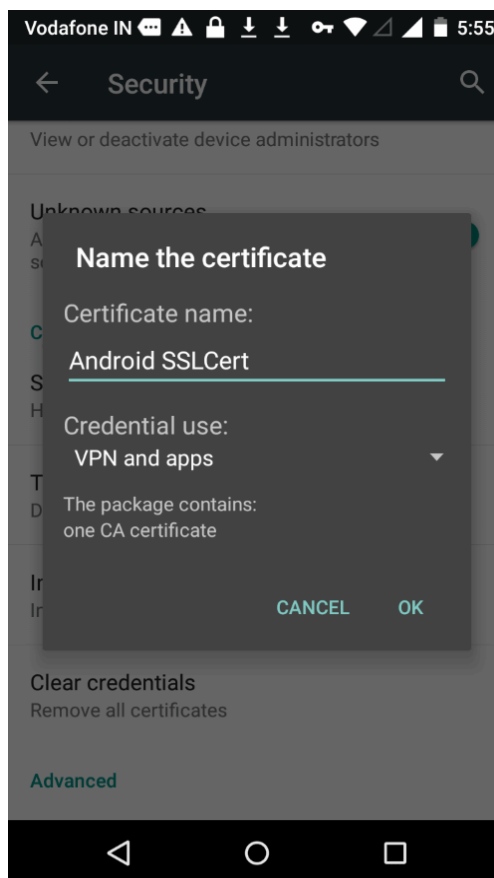
You will see the following screen when connected:





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

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



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

The mobile device will be enrolled and shown as follows:

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

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

### Shield Mobile Device App

- Enter device owner email addresses in the 'Add Mobile Device' as before
- Select 'VPN + Mobile Agent'

#### 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

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

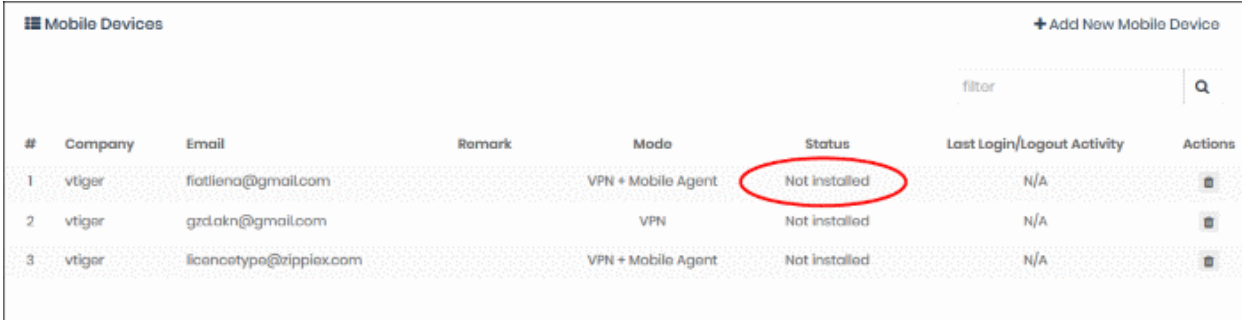
Please select company

vtiger ▼

Add

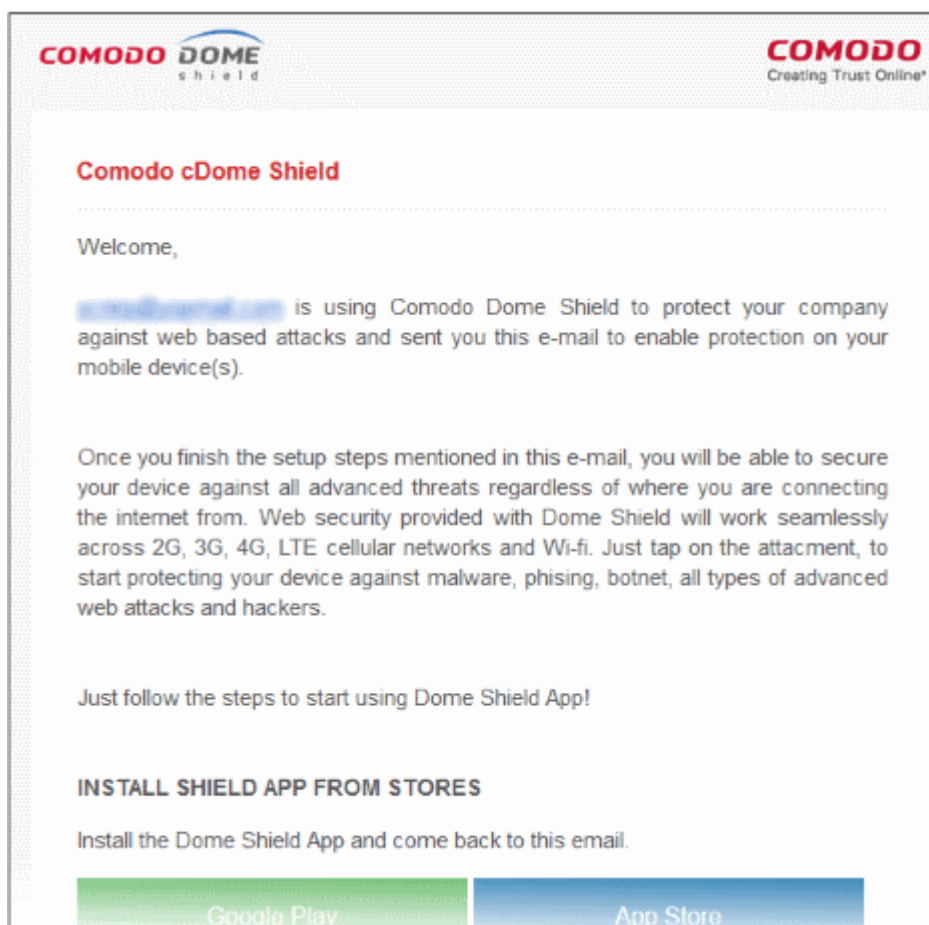
- Select Company - Applies to MSPs only. Select the company to whom the devices belong.
- Click 'Add'
- Shield will send device enrollment emails to all users that you added.

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



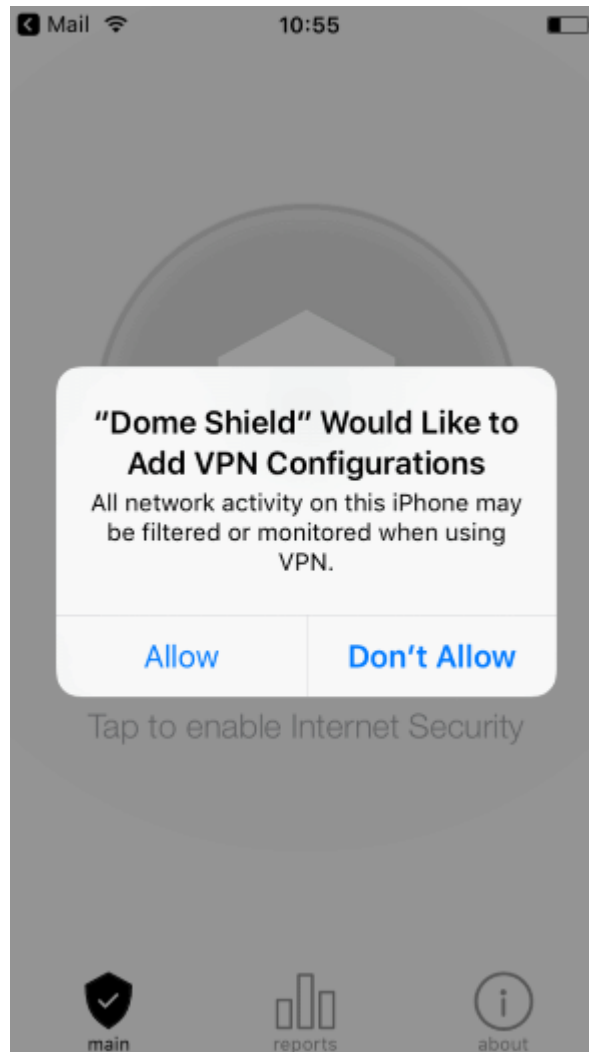
#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	vtiger	fiatlina@gmail.com		VPN + Mobile Agent	Not installed	N/A	
2	vtiger	gzd.ahn@gmail.com		VPN	Not installed	N/A	
3	vtiger	licencetype@zipplix.com		VPN + Mobile Agent	Not installed	N/A	

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

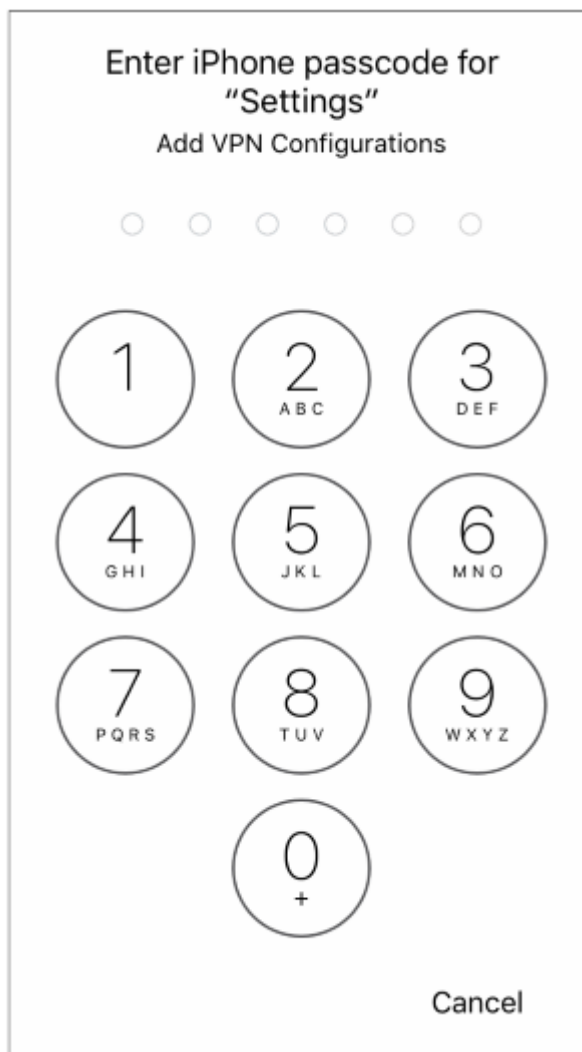


## Instructions for iOS

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



- Select 'Allow'
- Provide the device password if requested:

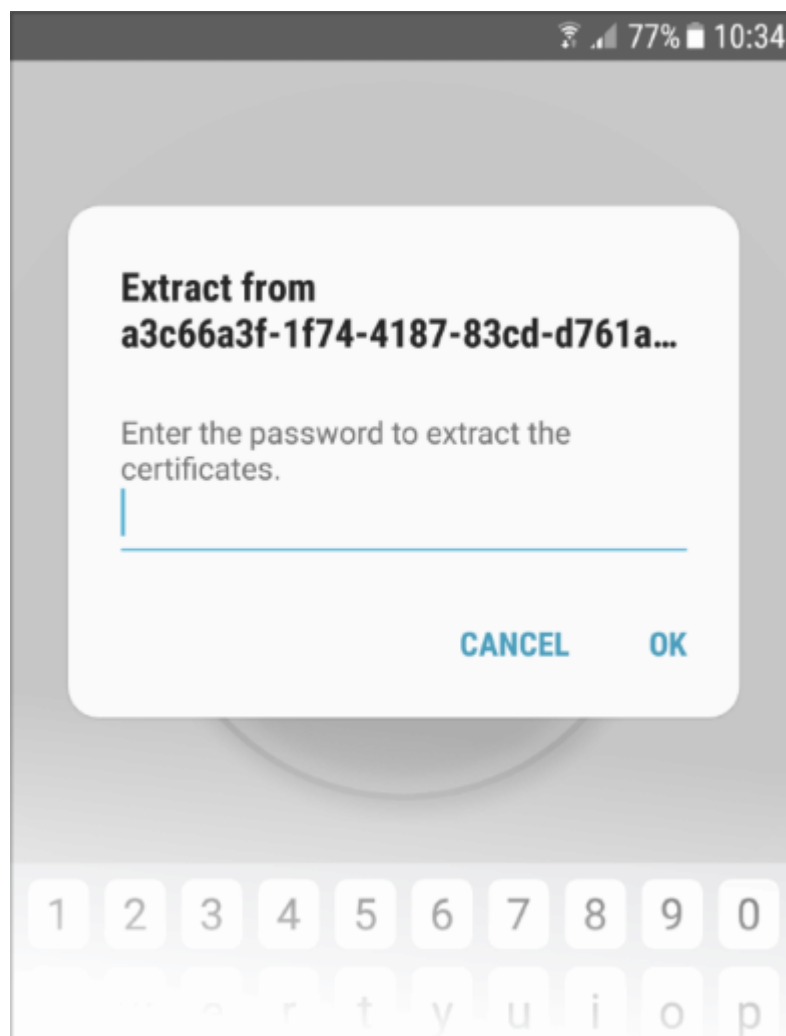


That's it. The iOS device is successfully enrolled to Dome Shield.

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

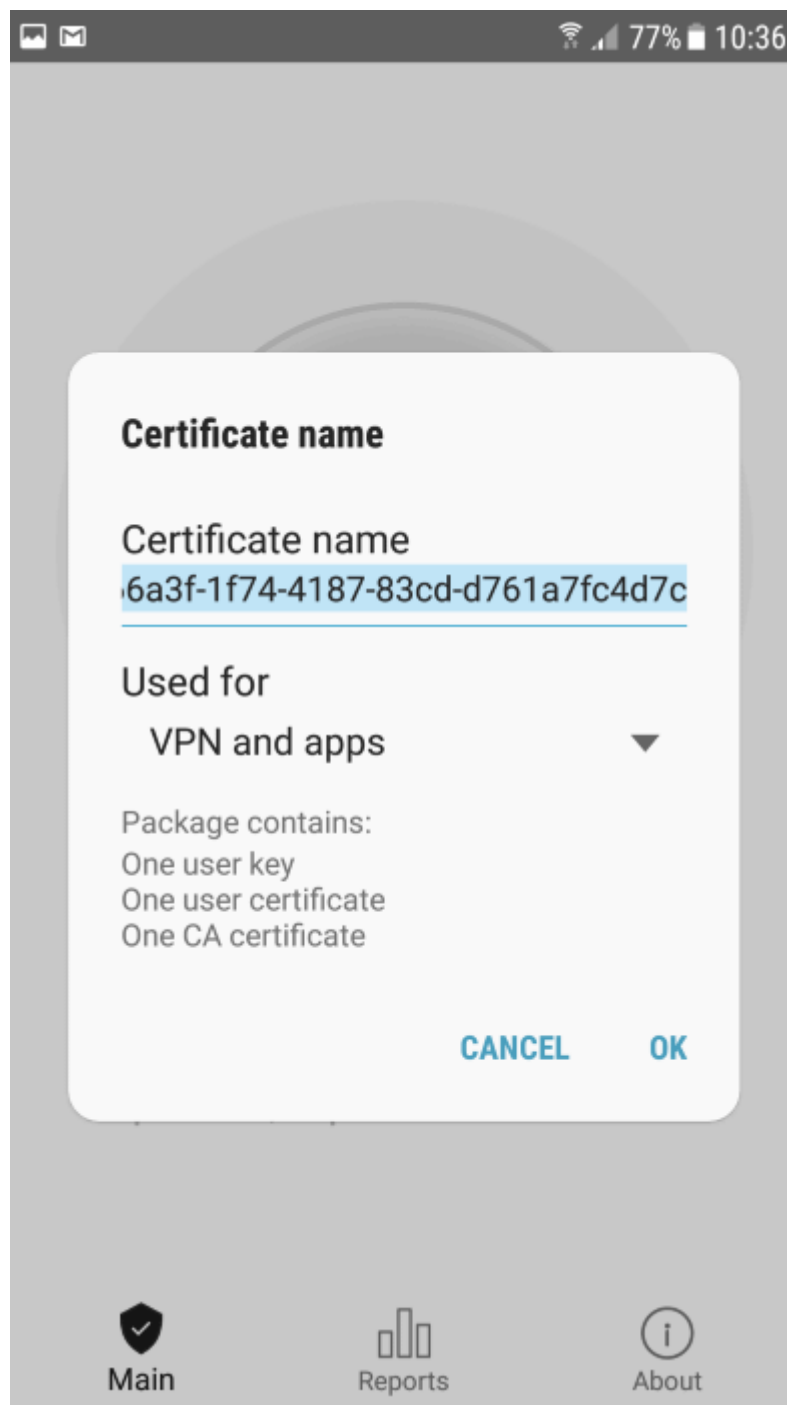
## Instructions for Android

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



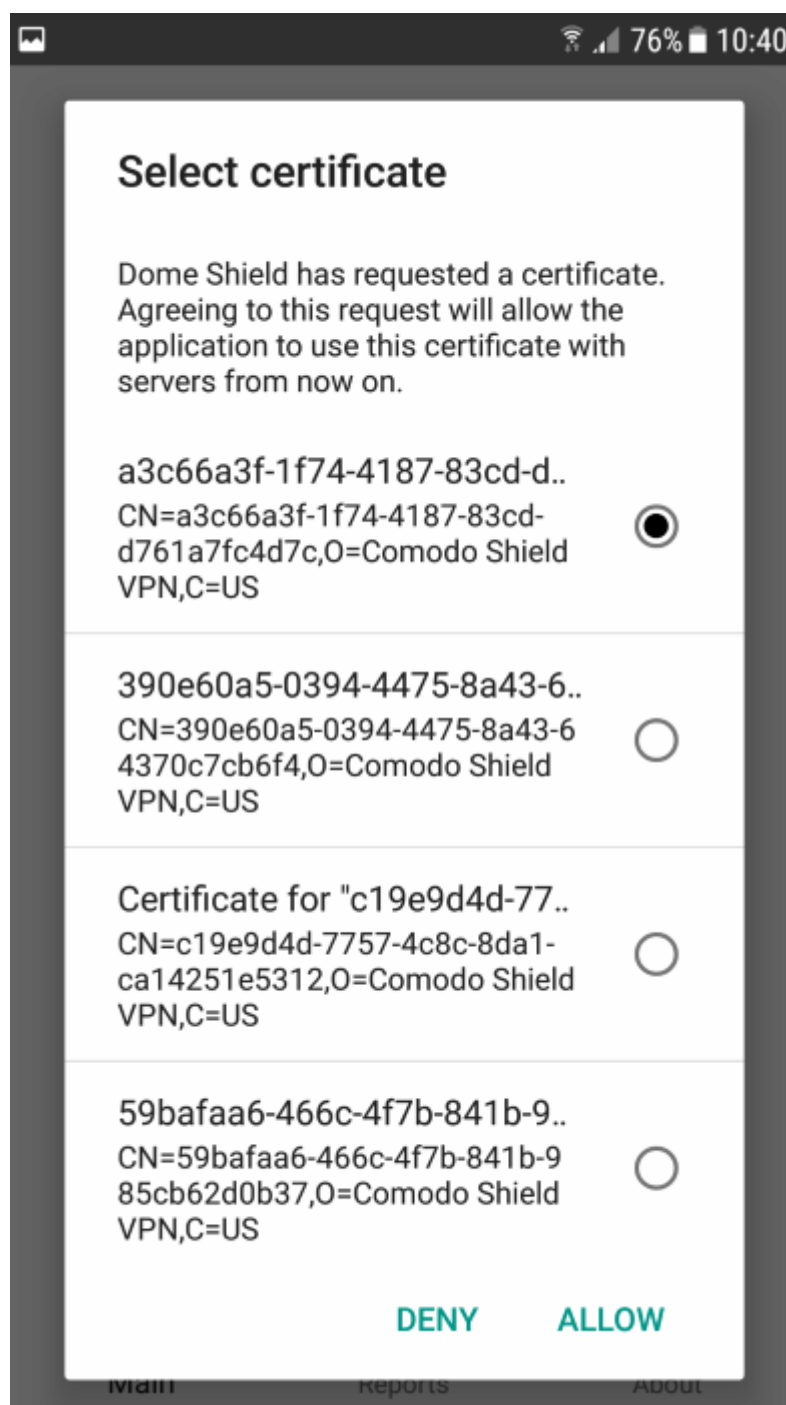
- Long press in the password field and select 'Paste'
- Select 'OK'

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



- Touch 'OK'

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



- Select 'Allow'

That's it. The app is activated and the device enrolled. Device details are shown in the 'Mobile Devices' screen in Dome Shield.

## Step 4 - Create Policy Rules

Dome policies are constructed from security rules. It is a good idea to familiarize yourself with rules before implementing a policy. There are three types of rules:

- Security Rules - Allow you to block access to sites known to host specific types of threat. Example threat types include malware, phishing, spyware etc.
- Category Rules - Allow you to control access to websites by content type. Example categories include social media, gambling, sports etc



- Domain Blacklist and Whitelist - Create custom whitelists and blacklists of specific websites.

You can also create block pages which are shown when a site is blocked by Dome Shield.

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

The following sections explain how to create each type of rule:

- **Add Security Rules**
- **Add Category Rules**
- **Add Domain Blacklist and Whitelist**
- **Add Block Pages**

## Add Security Rules

- Comodo operates a huge database of harmful websites categorized by threat type. Dome Shield uses this database to power its security rules.
- Security rules let you block access to sites known to host specific types of threat. Security rule categories include:
  - Malware
  - 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.

### To create a security rule

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

The screenshot shows a web interface for creating a security rule. At the top right, there is a button labeled "+ Create Security Rule" which is circled in red. Below this, a modal dialog box titled "Create Security Rule" is open. The dialog has a close button (X) in the top right corner. It contains two tabs: "Name" (which is selected and underlined in red) and "Settings". Under the "Name" tab, there is a text input field for "Name" and a larger text area for "Remark". A green "Next" button is located at the bottom right of the dialog. A red arrow points from the circled button to the dialog title.

- Name and remarks - Create a label for the rule and add any comments. These should help you, or another admin, identify the purpose of the rule.
- Click 'Next' or 'Settings' to specify the security categories that you want to allow or block:

**Create Security Rule** [X]

**Name**      **Settings**

---

Malware Domains	Allowed <input type="checkbox"/>
Botnet/C2C Servers/Bot Infected Sources	Allowed <input type="checkbox"/>
Phishing	Allowed <input type="checkbox"/>
Spyware	Allowed <input type="checkbox"/>

[Create]

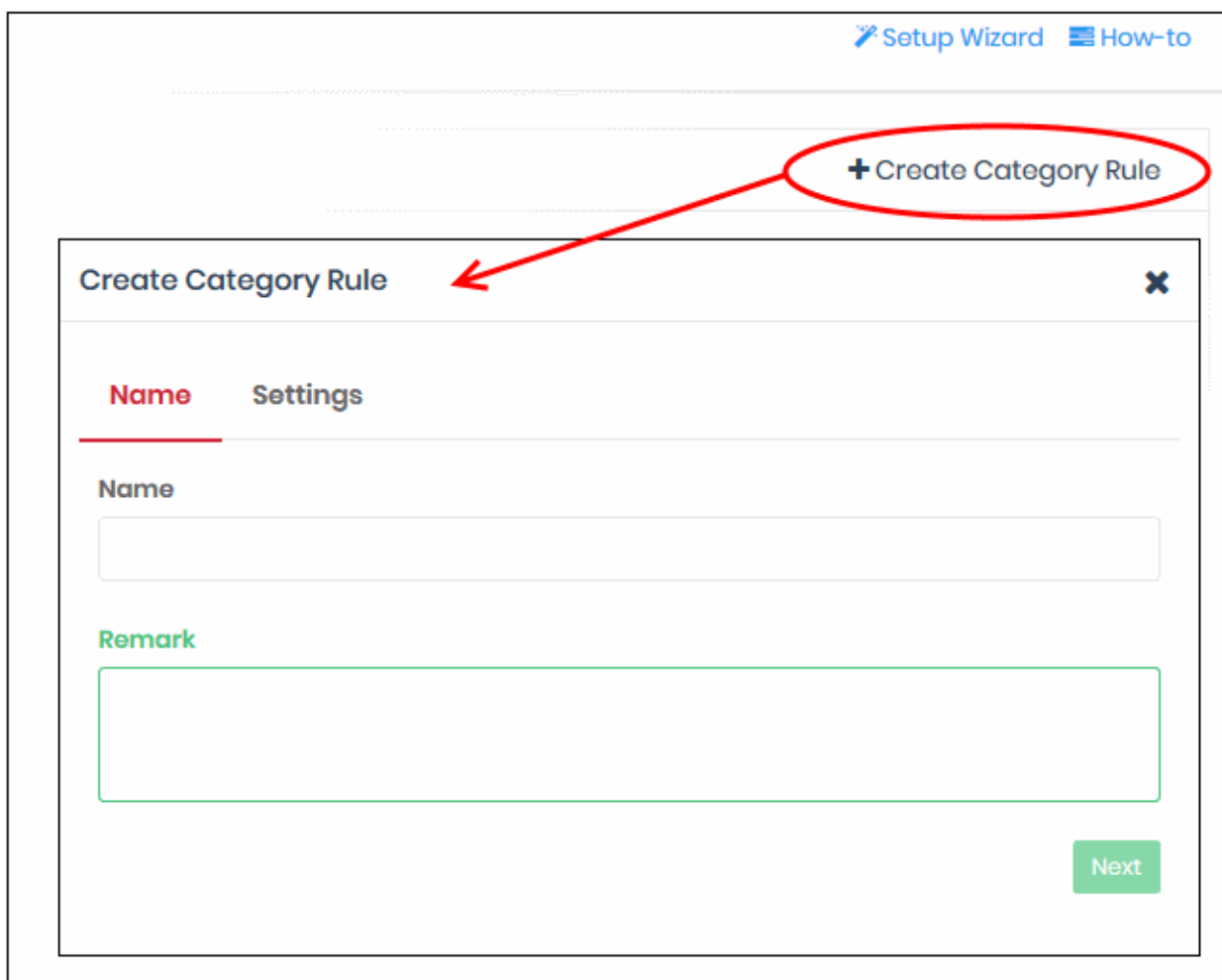
- Use the switches on the right to allow or block sites in a specific category
- Click the 'Create' button to save your rule
- Your new security rule will now be available for selection when **creating a policy**.
- Repeat the process to add more security rules

## Add Category Rules

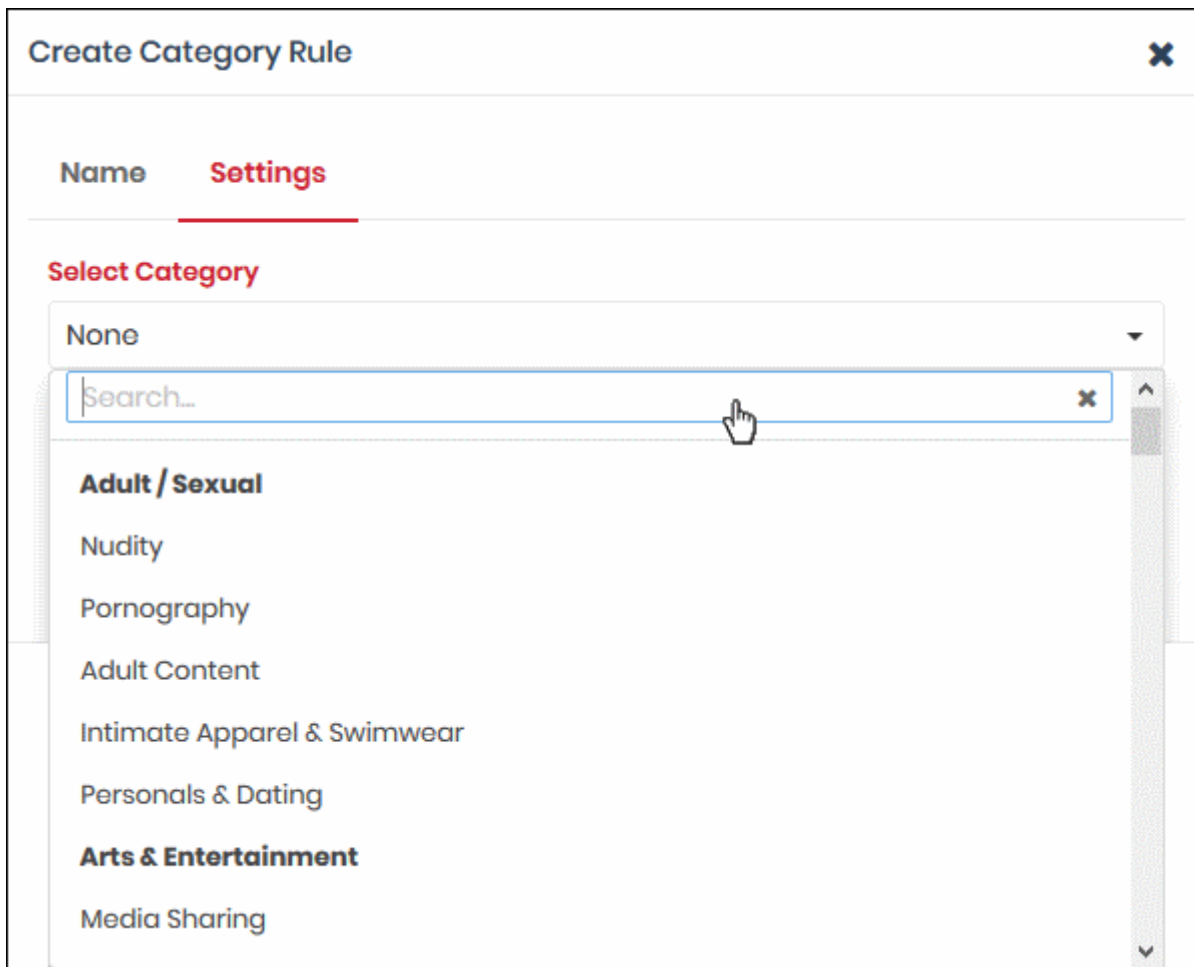
- Category rules let you control access to websites based on their content type. For example, you may wish to block access to adult websites, comedy sites, social media sites or sports websites.
  - Security rules focus on harmful categories like phishing and malware. Category rules let you apply policy to sites falling under a broader range of topics.
- You can add multiple website categories to a single category rule.

### To create a category rule

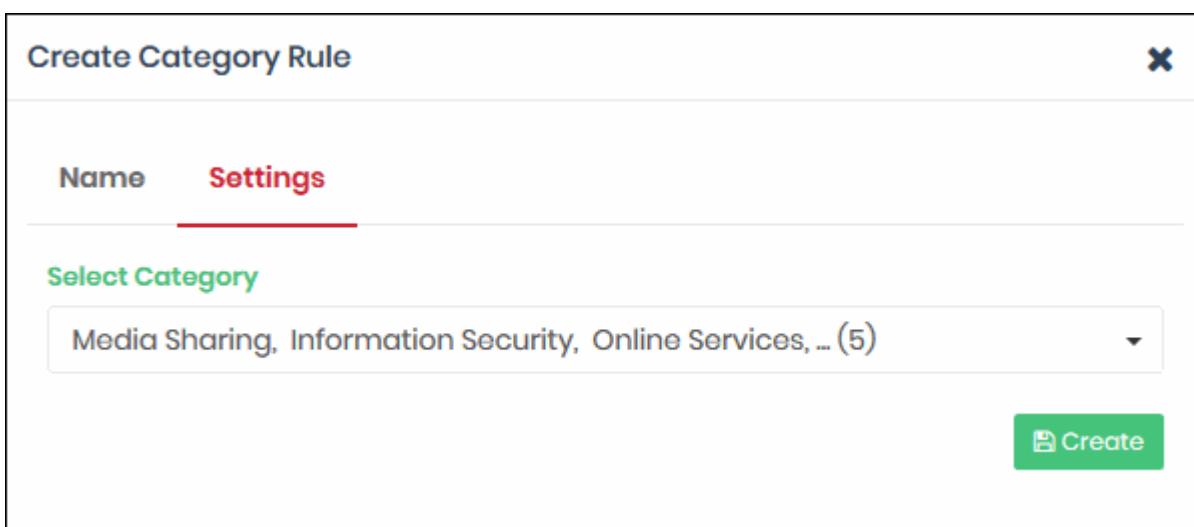
- Click 'Configure' > 'Policy Settings' > 'Category Rules'
- Click 'Create Category Rule' at top-right



- Name and remarks - Create a label for the rule and add any comments. These should help you, or another admin, identify the purpose of the rule.
- Click 'Settings' or 'Next' to choose which categories you want to block/allow:



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



- Click the 'Create' button at the bottom of the dialog when done.
- The website category will be created and available for selection when **creating a policy**.

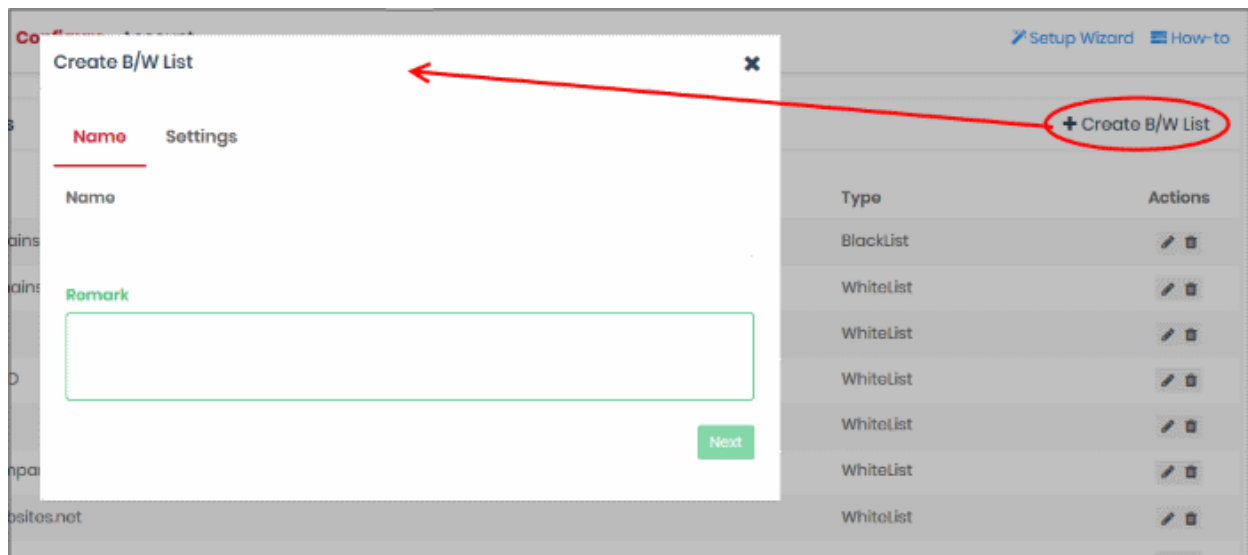
- Repeat the process to add more category rules

## Add Domain Blacklists and Whitelists

- You can add specific websites to a blacklist or whitelist according to your organization's web security policies.
- Black and whitelists over-rule category and security rules. E.g. - If you block shopping sites in a category rule, but add 'shop.com' to the whitelist, then 'shop.com' is allowed.
- If you enable 'Only B/W Mode' when configuring a policy, then only the black and white lists are consulted. All security and category rules are ignored.
- You can select any number of blacklists and white lists to be included in a policy

### To create a blacklist or whitelist

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



- Name and remarks - Create a label for the rule and add any comments. These should help you, or another admin, identify the purpose of the rule.
- Click 'Next' or 'Settings' to 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.* Create

- 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 list. 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  +



- 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**.

- Repeat the process to add more blacklists and whitelists.

### Add Block Pages

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

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

### To create a block page

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



- Click 'Add a New Block Page' at top-right

Setup Wizard How-to

Download Certificate + Add a New Block Page

Create Block Page

Name Settings

Name

Remark

Next

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

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

Upload image

Your image goes here

Block page preview

Domain Blocked Your message goes here

Create

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

## 1 - Configure Block Page Content

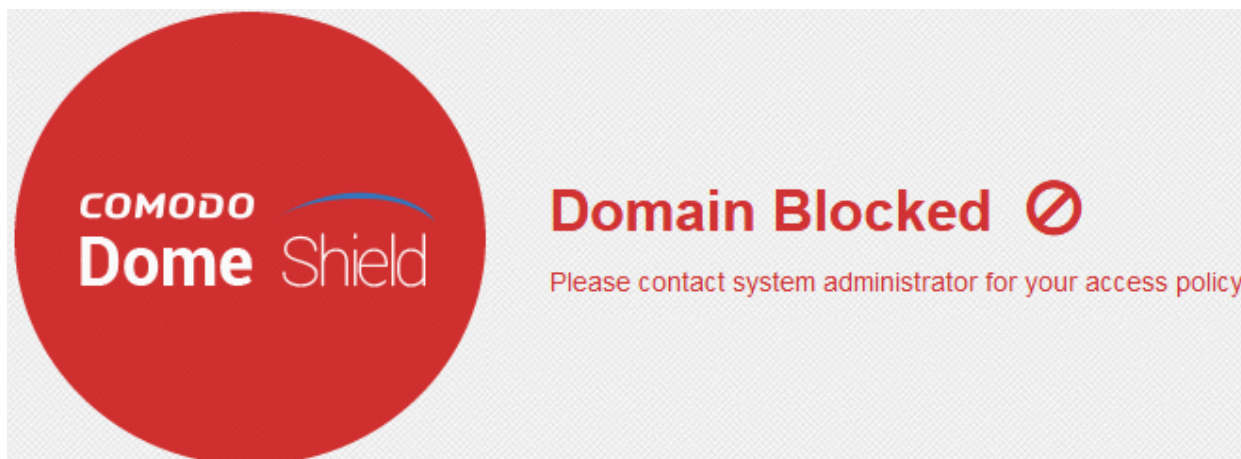
First, choose whether to show a single block page or different block pages:

- **Show a single page for all blocked domains** - A single block page or redirect page is shown regardless of which type of rule is violated.
- **Show different pages for blocked domains** - Show specific block pages if a certain type of rule is violated. You can show different pages for category rule breaches, security rule breaches and blacklist rule breaches:

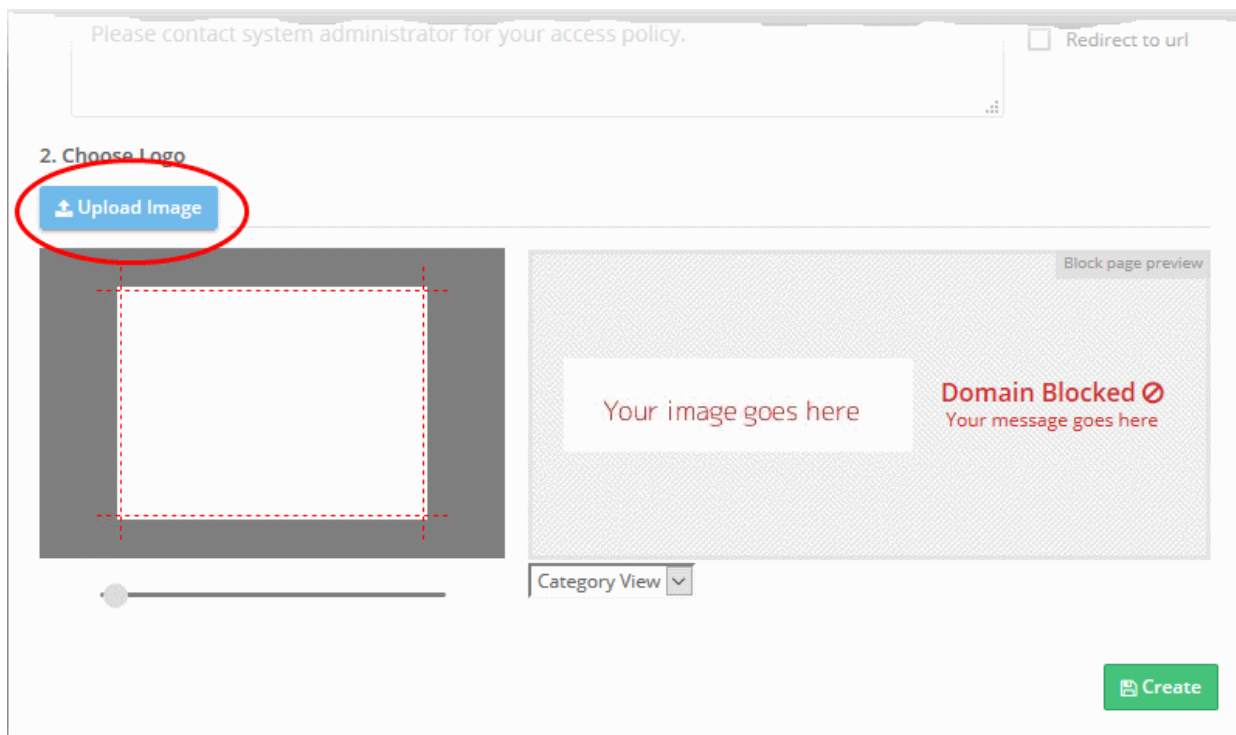
- You can type a custom message for each page if required.
- Alternatively, you can use the default message of 'Please contact your system administrator for your access policy'
- You also have the option to redirect to a specific URL instead. Please specify the full URL if you use this option. For example,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

## 2 - Upload Your Logo

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

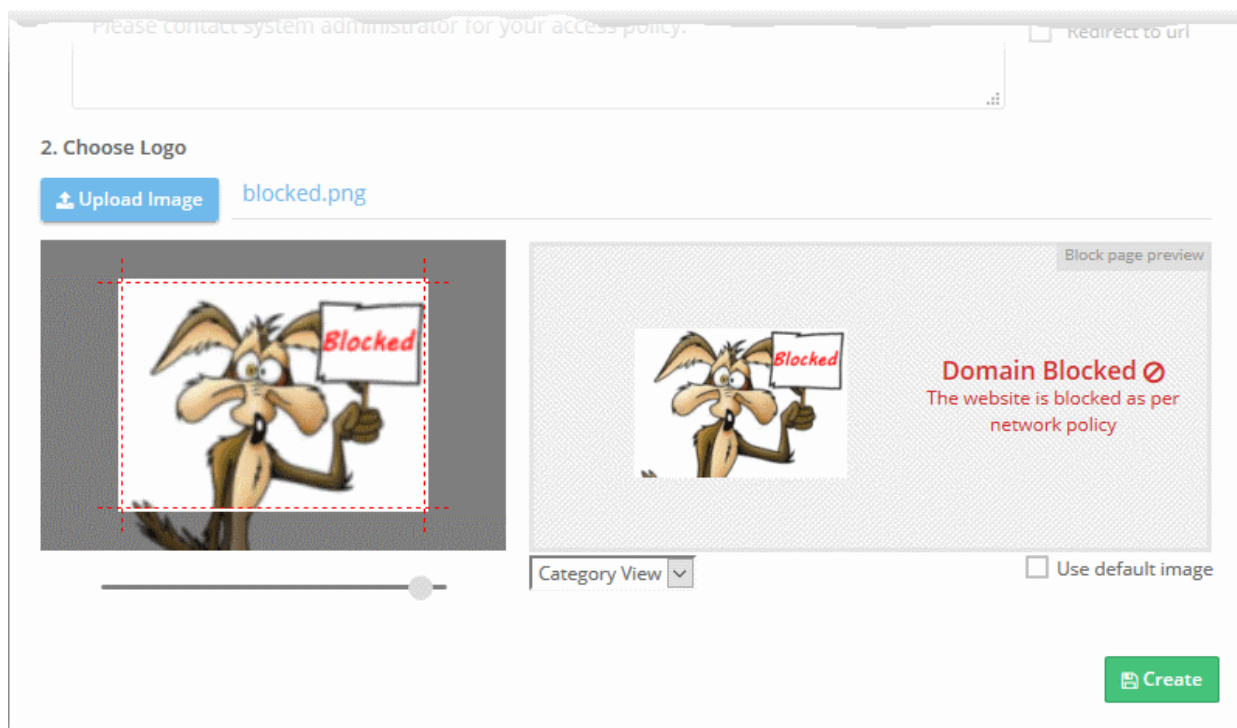


- Click 'Upload Image' under 'Choose Logo'. Browse to the location of your image and click 'Open'



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

Your image will appear on the left:



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

A preview of your block page will appear on the right.

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

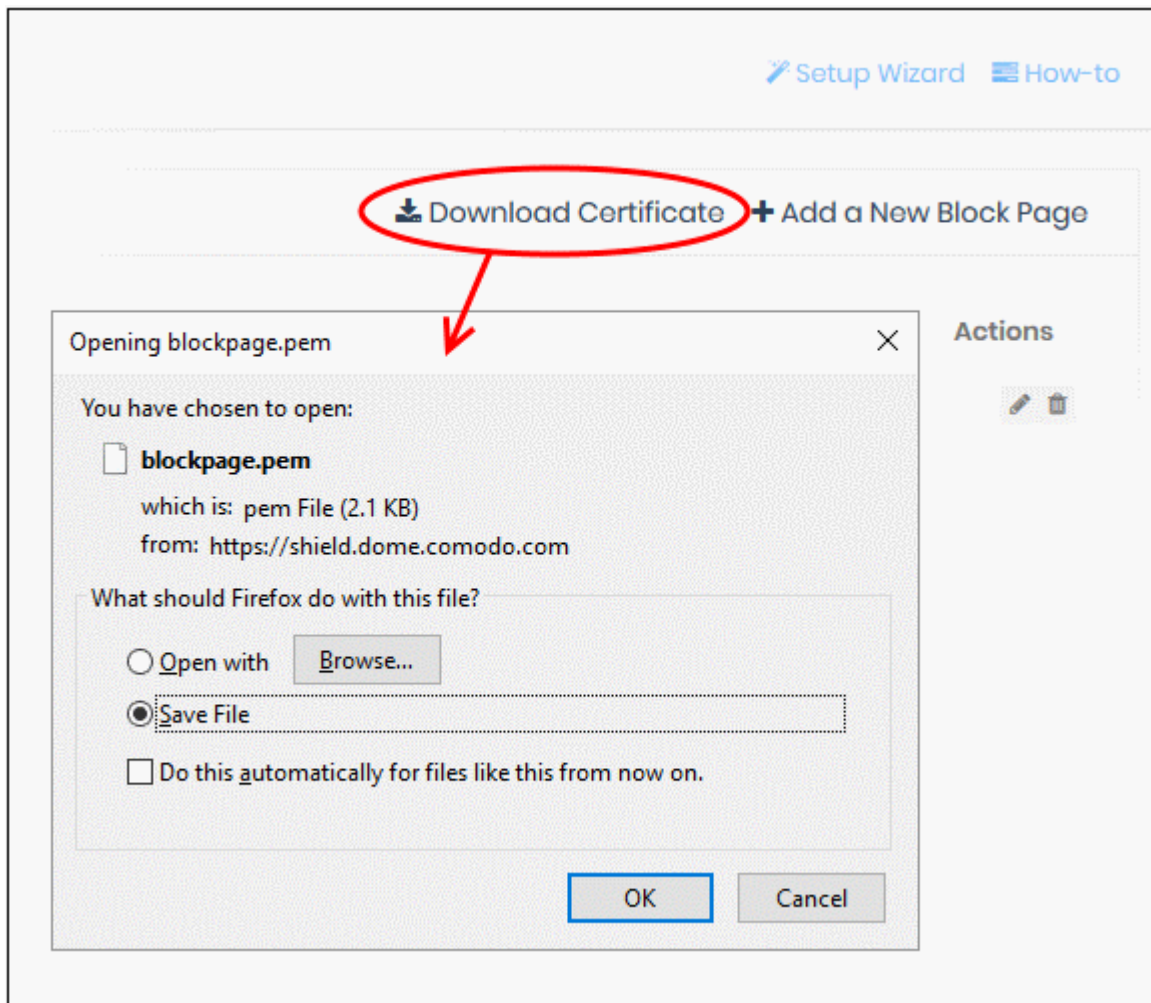
The new block page will be available for selection when **creating a policy**.

## Install the SSL certificate for block pages

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

### To download the certificate

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



The certificate will be downloaded in .pem format.

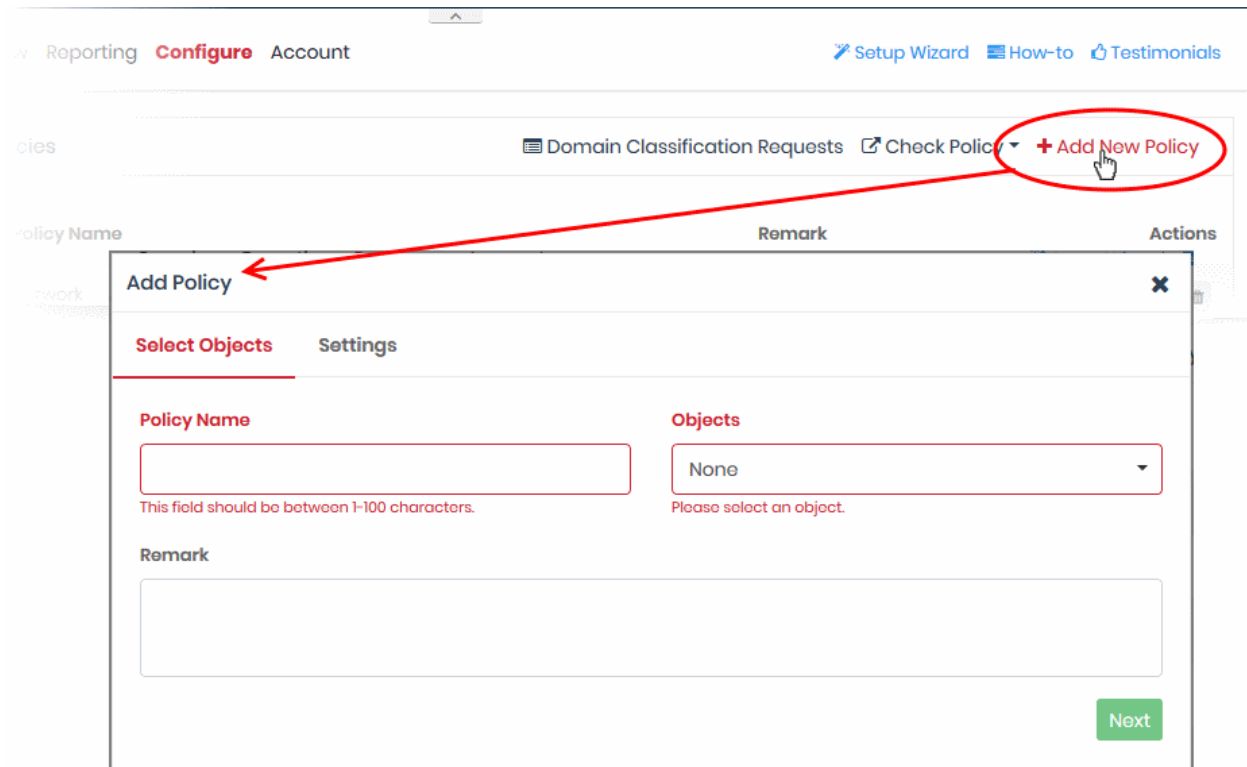
- See <https://help.comodo.com/topic-434-1-840-11971-Manage-Block-Pages.html> if you need additional help to install the certificate.

## Step 5 - Create and Apply Security Policies

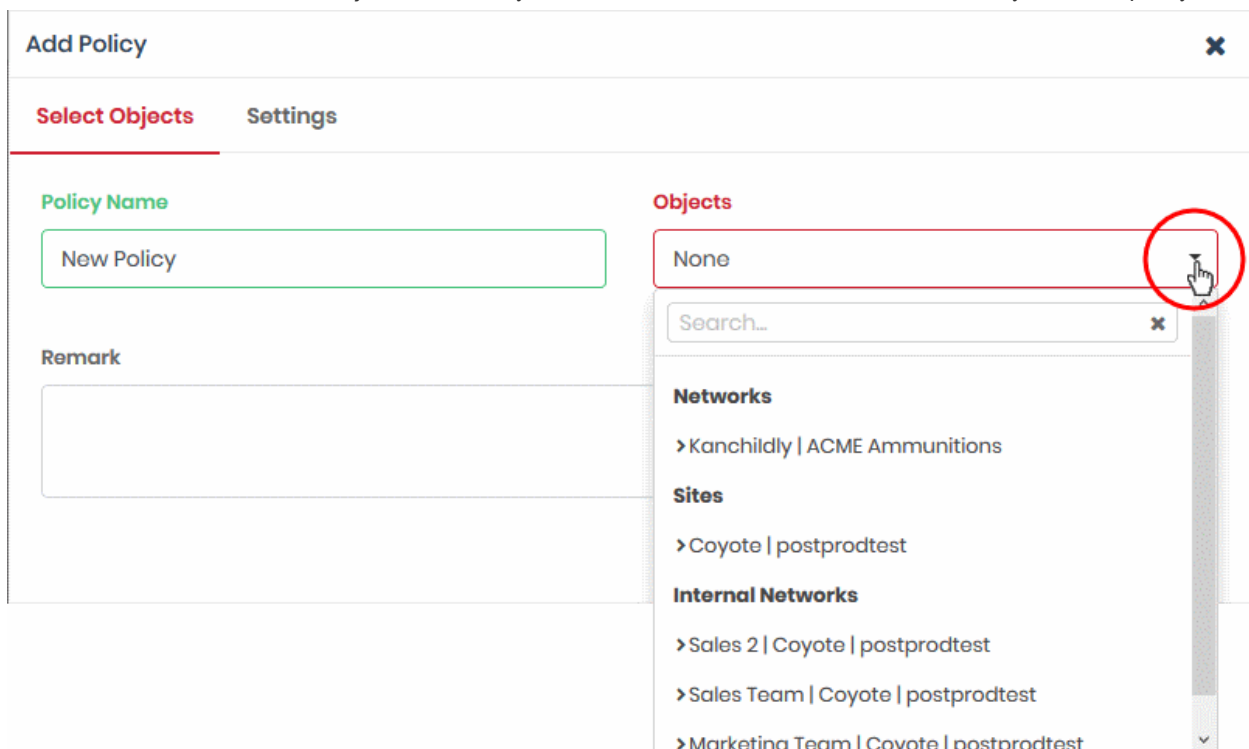
- A policy is a security profile which contains at least one 'Security Rule', 'Category Rule' or 'Black/White list'.
- You add the rules to a policy then apply the policy to a device or network. You can also add block pages which are shown when users visit a banned website.
- You must have already created at least one rule before you can create a policy
- You must also have added at least one device or network, or have imported a site using the local resolver .
  - See [Step 3 - Enroll Networks and Devices for Protection](#) for help with enrolling
  - See [Step 4 - Create Policy Rules](#) for help with adding rules

### To create a policy

- Click 'Configure' > 'Policy' to open the 'Policies' screen
- Click 'Add New Policy' at top-right



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



- **Networks** - List of manually added networks
- **Agents** - List of roaming Windows and Mac OS devices enrolled by installing the 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.
- **Remark** - Enter a description for the policy (optional)
- Click 'Next' or 'Settings' to configure the policy:

**Add Policy**
✕

Select Objects
Settings

Only B/W Mode Disabled

Block All Mode Disabled

Safe Search Disabled

**Security Rule**

None

**Category Rule**

None

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

**Domain B/W List**

Name	Type	Action
1000bl	BlackList	<input type="checkbox"/>
whitelist	WhiteList	<input type="checkbox"/>

**Block Page Appearance** ⚠

None

Add

- **Only B/W Mode** - If enabled, 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'
- **Safe Search** - Activates the content filtering feature of search engines like Google, Bing and Yahoo. Safe search eliminates explicit and potentially offensive websites from the results page of a search. This setting is disabled by default.
  - Use the switch to enable or disable safe search.
- **Security Rule** - Rules which block websites that host specific types of threats. The drop-down lists security rules that have been added to the 'Policy Settings' section. See '[Add Security Rules](#)' for more details.
- **Category Rule** - Rules which block websites by their content-type. The drop-down lists category rules that have been added to the 'Policy Settings' section. See '[Add Category Rules](#)' for more details.
- **Domain B/W List** - Select a list to either block or allow specific domains. The dialog shows blacklists and whitelists added to the the 'Policy Settings' section. See '[Add Domain Blacklist and Whitelist](#)' for more details.

**Note** - B/W lists 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 the policy. The drop-down displays block pages added via the 'Policy Settings' area. See **Add Block Pages** for more details.
  - **Note** - The block page is shown on all devices to which the policy is applied, except mobile devices.

Example policy settings are shown in the following screenshot:

Name	Type	
Social Media	BlackList	<input checked="" type="checkbox"/>
Eateries	WhitoList	<input checked="" type="checkbox"/>
For Shopping Addicts	BlackList	<input type="checkbox"/>
Banned Food Delivery	BlackList	<input checked="" type="checkbox"/>

- Click 'Add' to save your policy.

The policy will be applied to the chosen network(s) and/or roaming / mobile device(s).

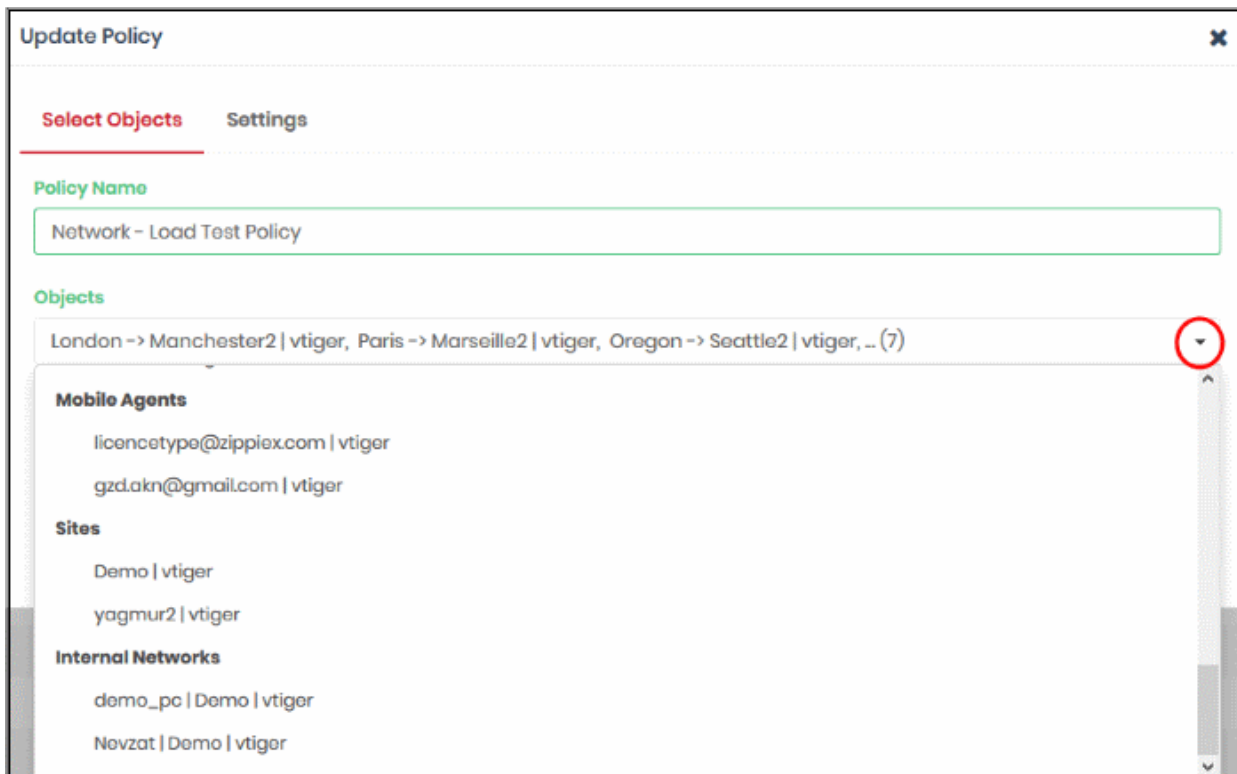
- Repeat the process to add more policies.

**To add an existing policy to newly added networks and roaming/mobile devices**

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

The 'Update Policy' pane will appear.





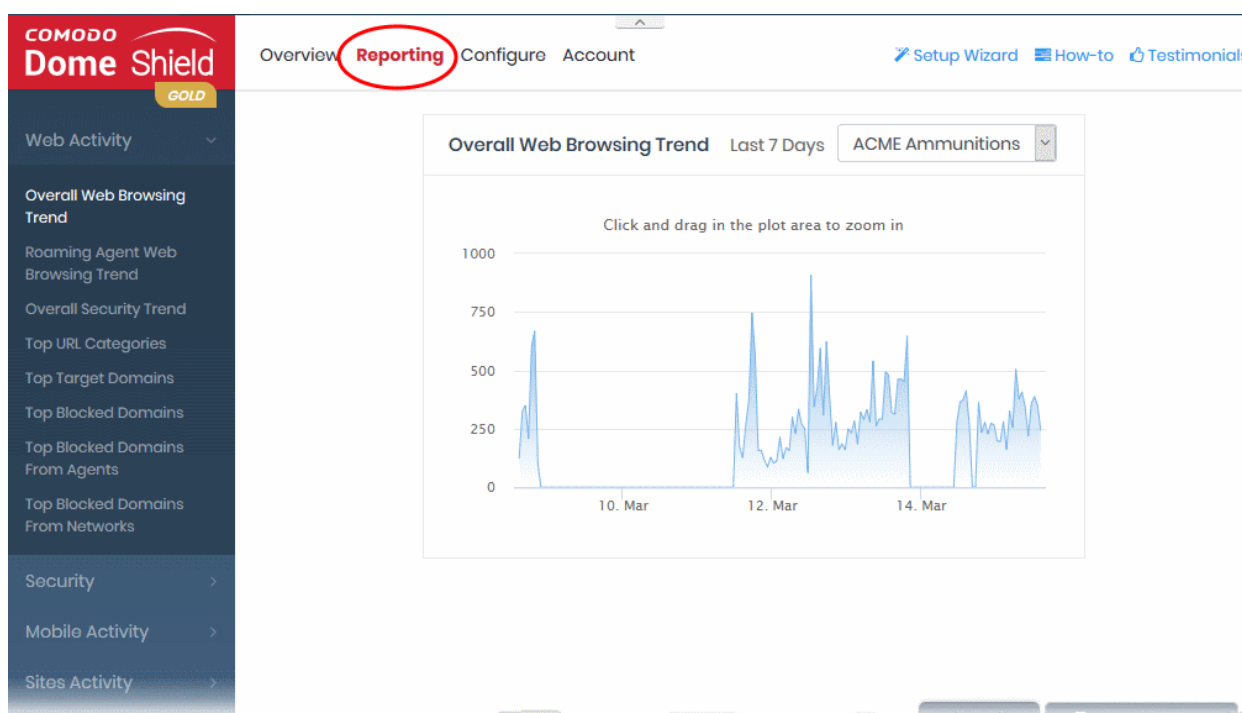
- Select the new network(s)/roaming/mobile device(s) from the 'Objects' drop-down
- Click 'Update'

The policy will be applied to the new network(s)/roaming/mobile device(s).

## Step 6 - Generate 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 categories of reports, 'Web Activity', 'Security', 'Mobile Activity' and 'Site Activity' reports.
- The charts in each report are larger, easier-to-manipulate-versions of those on the dashboard.
- Use the drop-down at top-right to choose the time period covered by the report.

## Web Activity Reports

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

## Security Reports

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

## Mobile Activity Reports

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

## Sites Activity Reports

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

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

## Step 7 - View Account Details

- The 'Account Info' page shows user information, total DNS requests for the month and licenses associated with your account.
- You can also upgrade your free licenses to a Platinum license.
  - [Click here](#) to compare packages.
- Click 'Account' to open the account info page:

The screenshot shows the 'Account Info' page in the Comodo Dome Shield dashboard. The page is divided into several sections:

- Account Info Header:** Includes navigation links (Overview, Reporting, Configure, Account), utility links (Setup Wizard, How-to, Testimonials), and user information (admin@company.com, Sign Out).
- User Info:** Displays the user's email (admin@company.com) with a green checkmark, their user type (Enterprise), and their joining date (2018-05-21).
- Total DNS Requests (March):** Shows a large '22k' value and a progress bar indicating 7.3% usage.
- Licenses Table:**

License Type	Retrieval Date	Expiration Date	Status	# of Endpoints	Quantity
<b>GOLD</b>	2017-02-24	2117-02-24	Active	N/A	5
- Upgrade Prompt:** A message encourages upgrading to 'Dome Shield PLATINUM' for no DNS requests limit and more features, with a 'BUY' button.
- Dome Shield Platinum-only Features:**
  - ✓ Local DNS Resolver Virtual Appliances
  - ✓ Internal IP based Visibility & Control
  - ✓ Bypass Domains to Existing Internal DNS
  - ✓ Encrypt Network-wide DNS Traffic
  - ✓ Manage by Sites and DNS Egress Points

### User Info

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

### Total DNS Requests

- Shows the number of requests received by Dome Shield from the enrolled devices for the current month.
- The number of requests you can make depends on your license type:
  - **Platinum license**

- Unlimited DNS requests
- **Gold license**
  - DNS requests are capped at 300 K per month for the account. Account = requests from all your endpoints/networks.
  - DNS requests are mainly used up by first-time requests to external sites. Subsequent requests for the same site are handled by the local cache until TTL expires.
  - Requests to the Dome Shield Portal are *not* included in the 300 K limit.
  - Once 300 K limit is reached:
    - All existing policies will continue to function as before.
    - You can edit existing rules and policies
    - You cannot add new rules, policies or objects. Objects = networks, roaming agents and mobile agents.
  - The request count is reset to zero at the beginning of each month. At this point you can add new objects, policies and rules.

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

## Licenses

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

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

## About Comodo Security Solutions

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

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

## About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)