COMODO
Creating Trust Online®

COMODO ONE
MSP

Comodo Secure Web Gateway

Software Version 2.22

Quick Start Guide

Guide Version 2.22.032020

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo Secure Web Gateway - Quick Start Guide

Comodo Secure Web Gateway (SWG) is a real time web traffic scanning solution capable of providing 100% protection against zero-day malware and advanced threats. You can deploy strong web access policies for endpoints inside the network as well as for roaming devices. SWG can be hosted on your Amazon Web Services (AWS) platform or we can host it for you.

This document explains how you can purchase licenses, connect your networks and devices to SWG, apply policies and generate reports.

Purchase a License

There are two ways to sign-up to Comodo Secure Web Gateway (SWG):

- **Standalone customers** - Purchase a standalone SWG license by logging into your Comodo account at **https://accounts.comodo.com/**

  OR

- **Comodo One / Comodo Dragon / ITarian customers** - Purchase an SWG license from your portal account.

Standalone customers

- Login to your CAM account at **https://accounts.comodo.com/**. Please create an account if you do not have one.
- The 'My Account' tab shows services that are enabled for your account and other products that you can sign up for.
- Click 'Sign Up to Comodo Secure Web Gateway'.
- Select the Comodo SWG plan best suited to your requirements.
  - Comodo SWG is available in two basic versions - Comodo hosted, or hosted on your Amazon Web Services (AWS) account. Each version is available in a variety of plans.
- Complete the payment process.
- A confirmation email will be sent to your registered email address.

Portal Customers

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account

- Click 'Store' on the menu bar
- Locate the 'Comodo Secure Web Gateway' tile.
- Click 'Buy' and complete the purchase process.

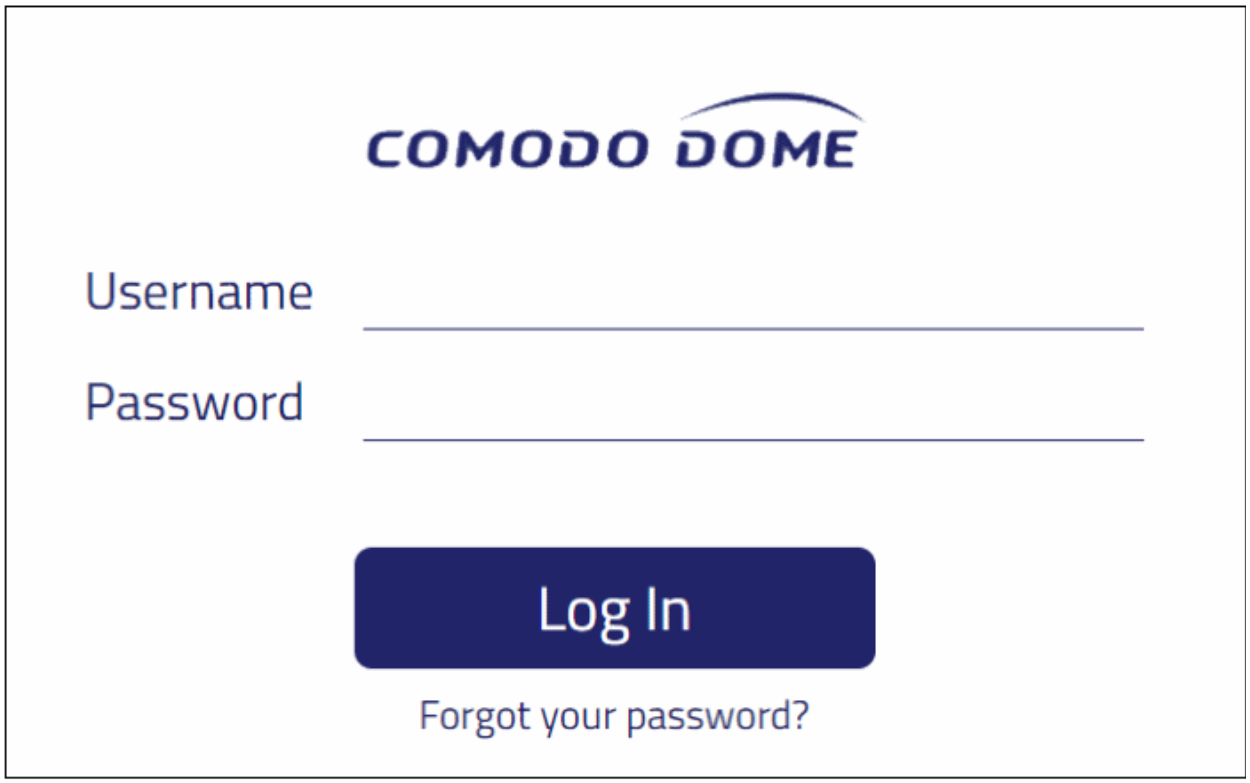
Note: Comodo SWG is hosted on Amazon Web Services (AWS) cloud platform. If you do not have an AWS account, Comodo will host it for you.

Login to your Comodo SWG account

Stand-alone Customers

- After signup, Comodo will provide you with the URL of your Comodo SWG instance.
- Visit the URL using any internet browser to access your login page.

Note: Comodo SWG is hosted on Amazon Web Services (AWS) cloud computing platform. If you do not have an AWS account, Comodo will host it for you.



- Enter your username and password in the respective fields and click 'Sign In'

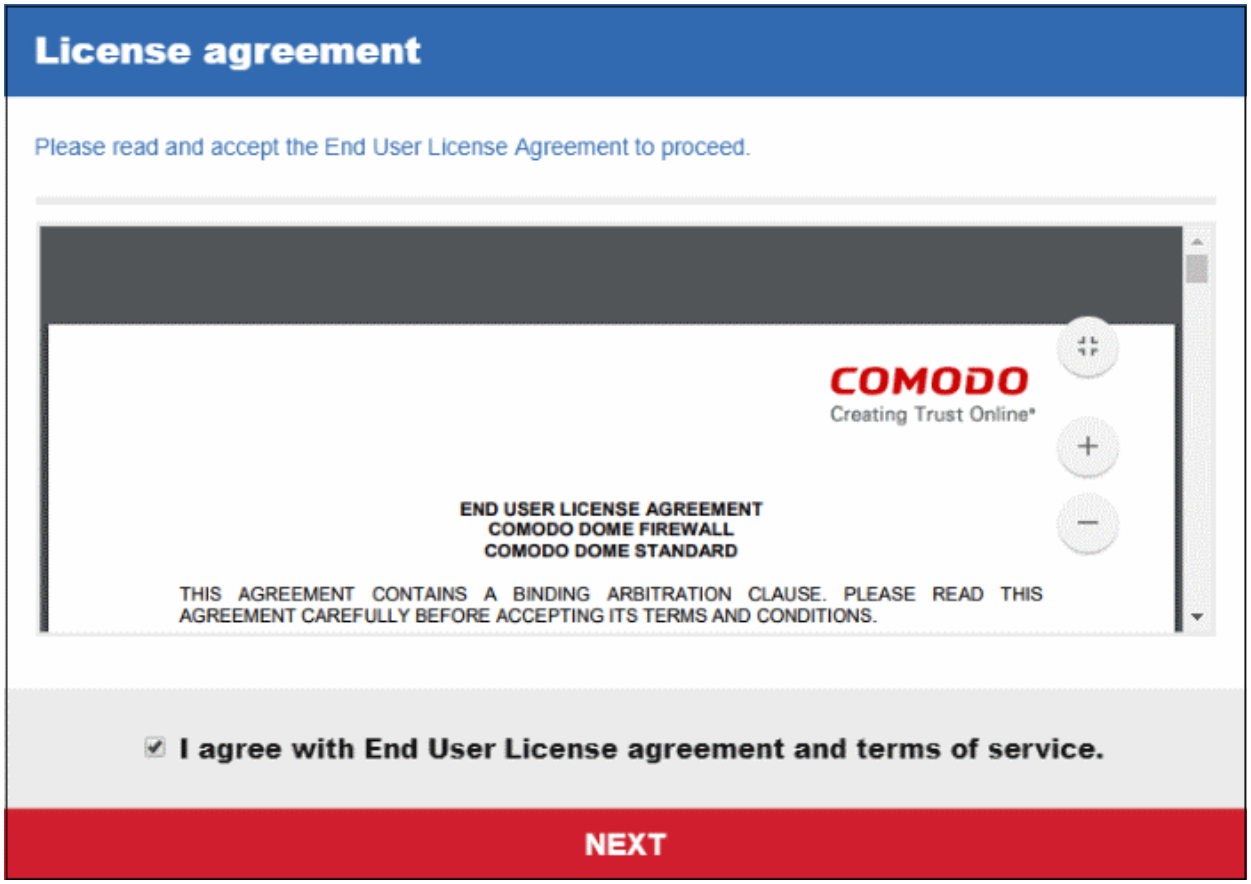
Portal Customers

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Applications' > 'Comodo Secure Web Gateway'

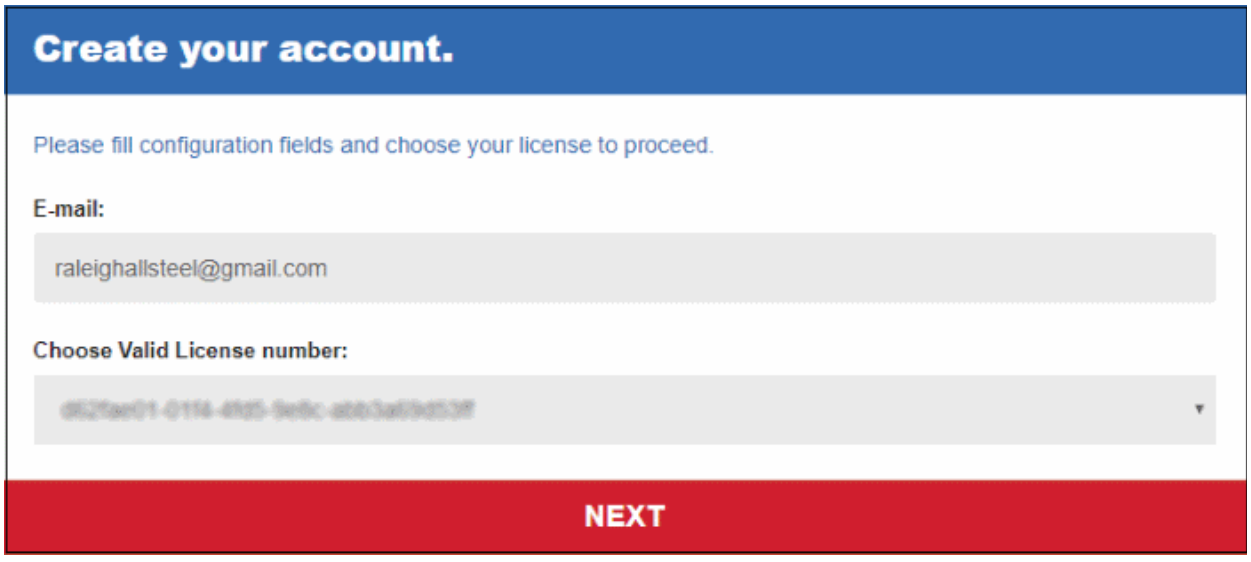
Configure Comodo SWG Nodes

You can host multiple nodes in different locations for traffic load balancing purposes. You can configure the additional

nodes at first login after subscribing.



- Read the EULA fully, select the 'I agree' checkbox and click 'Next'

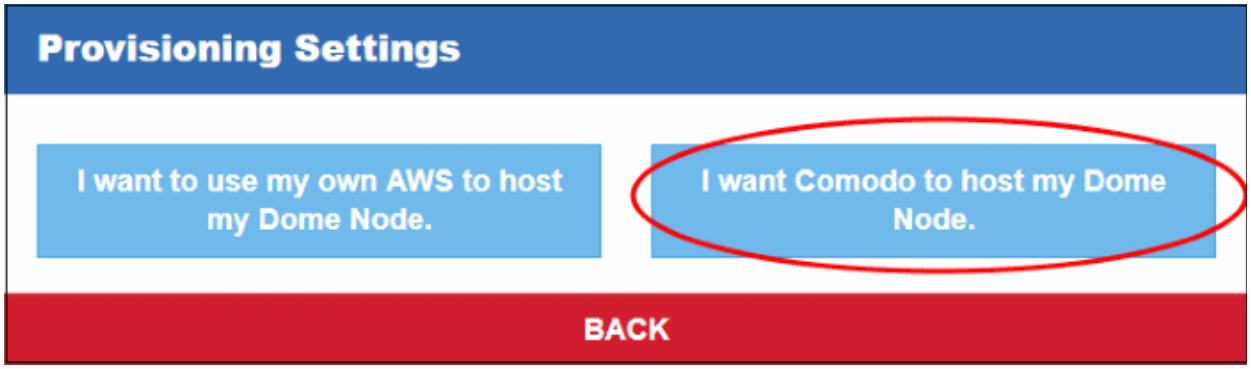


- Select the license you wish to use and click 'Next'

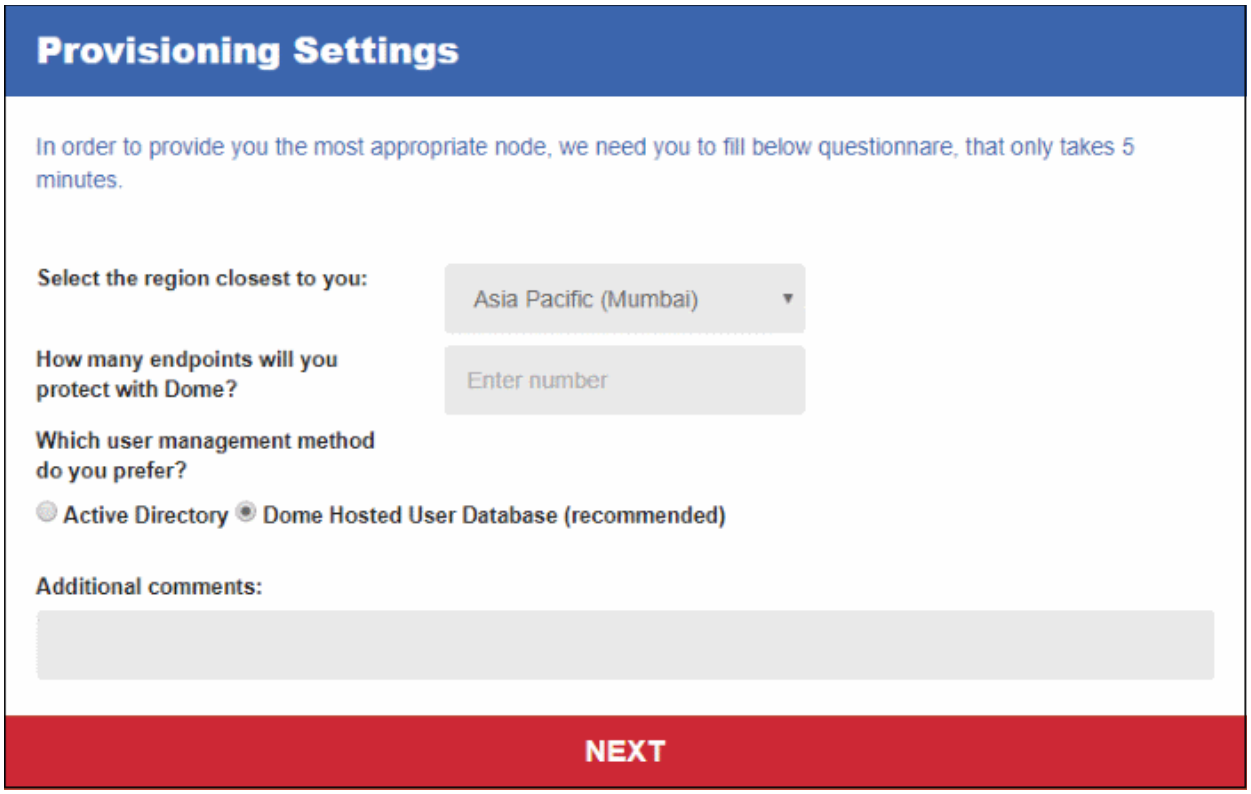
Next, select the hosting type:

- **Comodo hosted account**
- **Customer AWS account**

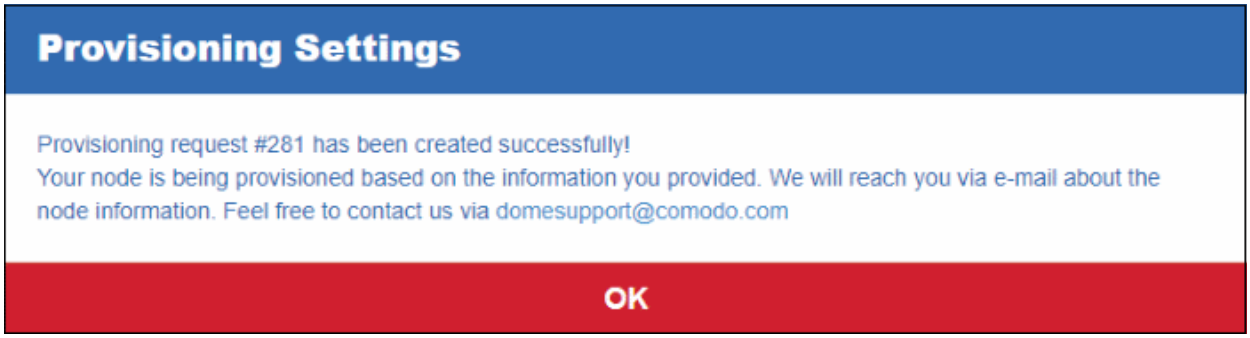
Comodo Hosted Account



- Click 'I want Comodo to host my SWG Node'

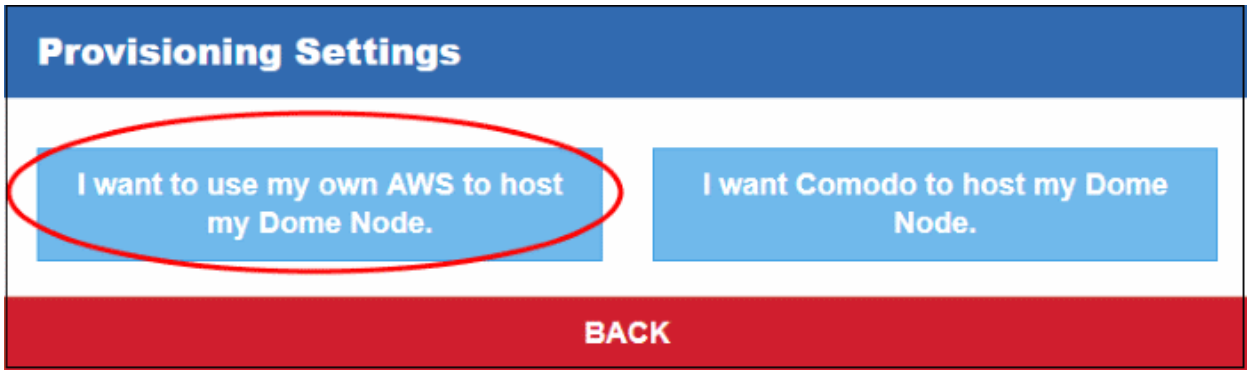


- Select the region closet to you - Choose the region closest to your location. This will improve the performance of the service.
- How many endpoints will you protect with Comodo SWG - Enter the number of endpoints you wish to cover with SWG protection.
- Which user management method do you prefer - Select the method you want to use to authenticate users. Please note the user authentication method can be changed later on from the '**Authentication Settings**' screen.
- Enter brief description in the 'Additional comments' field and click 'Next'

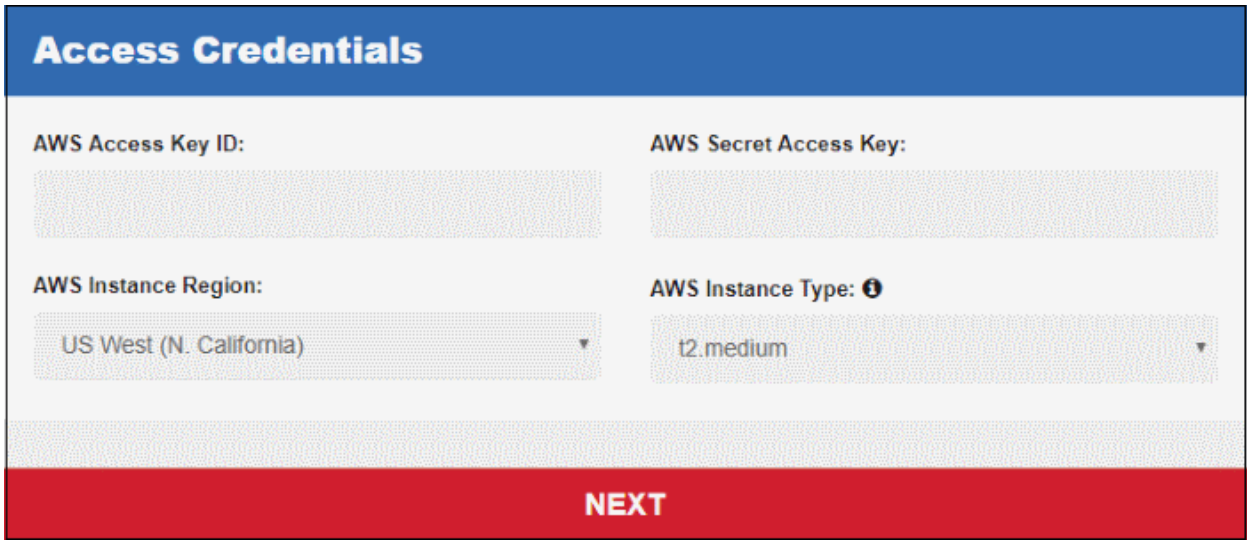


That's it. The Comodo hosted node will be prepared and a confirmation mail sent to your registered address. Contact support at **domesupport@comodo.com** if you have any questions.

Customer AWS Account



- Click 'I want to use my own AWS to host my Comodo SWG Node'



- Enter your AWS account credentials and click 'Next'.
- After your credentials have been authenticated, next complete the 'Provisioning Settings' wizard.

After completing the application, Comodo will provision Comodo SWG on your AWS account. The node(s) will be prepared and a confirmation mail sent to your registered address. Contact support at **domesupport@comodo.com** if you have any questions.

Configure Traffic Forwarding to Comodo SWG

- You need to route your endpoint and network traffic through Comodo SWG in order to deploy web protection policies.
- This traffic forwarding can be done in multiple ways, the most common of which are explained in the sections below.
- The direct proxy method is more suited to smaller organizations with fewer endpoints. Proxy chaining and ICAP methods are better suited to larger organizations with multiple networks in different locations.
- If you don't want to use any of the methods above you can just install the SWG agent on devices and deploy user/endpoint based rules.

Click the following links for more information on each method:

- **Traffic Forwarding via Direct Proxy or PAC**
- **Traffic Forwarding via Proxy Chaining**
- **Traffic Forwarding via Internet Content Adaptation Protocol (ICAP)**
- **Traffic Forwarding via SWG Agent**

After connecting your network(s), make sure to add them as a 'Trusted Network' in the 'Locations' interface. If you do not then Comodo SWG will not function correctly and your network will not be able to connect to the internet. See next step **Connect your network(s) to Comodo SWG**.

- Note – Comodo SWG uses ports 17443, 19443 and 19080 to connect to your networks. Please configure your firewall to allow SWG traffic over these ports.

Traffic Forwarding via Direct Proxy or PAC

Direct proxy traffic forwarding is suitable for smaller organizations with fewer endpoints and no other proxy configured on the network. Here are some common methods of configuring a direct proxy:

- **Set SWG Proxy IP in Browsers**
- **Set SWG Proxy via PAC (Proxy Auto-Configuration)**
- **Set SWG Proxy via Windows Group Policy**

Set SWG Proxy IP in Browsers

Note:

- The proxy address details vary for each account. The addresses for your account can be found in the Comodo SWG console.
- Click 'Administration' > 'How to Configure' > 'Set as Proxy' > 'Direct Proxy'
- Choose your preferred browser (Chrome, Firefox, Internet Explorer)
- Your SWG proxy address is shown in a string similar to the following:

  ec2-35-182-130-219.ca-central-1.compute.amazonaws.com:19080

  In the example above,

  - SWG IP address = 35.182.130.219
  - SWG domain name = ec2-35-182-130-219.ca-central-1.compute.amazonaws.com

Chrome

- Open Chrome
- Open 'Settings', type 'Proxy Settings' in the search bar, then click 'Change Proxy Settings'
- Click the 'Connections' tab then click 'LAN settings'

- Select 'Use a proxy server for your LAN' check box and click 'Advanced'
- In the 'HTTP field', enter SWG IP <X.X.X.X> or Domain name and port number as 19080
- In the 'Secure field', enter SWG IP <X.X.X.X> or Domain name and port number as 19443
- In the 'Exceptions' field enter enter SWG IP <X.X.X.X> or Domain name
- Click 'OK'

Internet Explorer

- Open Internet Explorer
- Open 'Tools' > 'Internet Options', open the 'Connections' tab and click 'LAN settings'
- Select 'Use a proxy server for your LAN' check box and click 'Advanced'
- In the 'HTTP field', enter SWG IP <X.X.X.X> or Domain name and port number as 19080
- In the 'Secure field', enter SWG IP <X.X.X.X> or Domain name and port number as 19443
- In the 'Exceptions' field enter enter SWG IP <X.X.X.X> or Domain name
- Click 'OK'

Firefox

- Open Firefox
- Click 'Options' from the 'Tools' menu
- Click 'Advanced' on the left
- Click 'Network', then 'Settings' (under 'Connection')
- Select 'Manual Proxy Configuration'
- In the 'HTTP field', enter SWG IP <X.X.X.X> or Domain name and port number as 19080
- In the 'Secure field', enter SWG IP <X.X.X.X> or Domain name and port number as 19443
- In the 'Exceptions' field enter enter SWG IP <X.X.X.X> or Domain name
- Click 'OK'

Set SWG Proxy via PAC (Proxy Auto-Configuration)

Note:

- The PAC URL for your account can be found in the Comodo SWG console at 'Configuration' > 'Configuration' > 'PAC'.
- You can customize the PAC file to grant direct access to domains and bypass Comodo SWG.
- See '**Configure PAC File**' for more details.

Chrome

- Open Chrome
- Open 'Settings', type 'Proxy Settings' in the search bar, then click 'Change Proxy Settings'
- Click the 'Connections' tab, and then click 'LAN settings'
- Select the 'Use automatic configuration script' check box
- Address box – type the SWG PAC URL, for example, https://dome.comodo.com/pac_file/f09ed11bfe157ae025e33d84012af39c.pac
- Click 'OK'

Internet Explorer

- Open Internet Explorer

- Open 'Tools' > 'Internet Options', open the 'Connections' tab and click 'LAN settings'
- Select the 'Use automatic configuration script' check box
- Address box – type SWG PAC URL, for example, https://dome.comodo.com/pac_file/f09ed11bfe157ae025e33d84012af39c.pac
- Click 'OK'

Firefox

- Click 'Options' from the 'Tools' menu
- Click 'Advanced' on the left
- Click 'Network', then 'Settings' (under 'Connection')
- Select the 'Automatic proxy configuration URL' radio button
- In the 'Automatic proxy configuration URL' field, type SWG PAC URL, for example, https://dome.comodo.com/pac_file/f09ed11bfe157ae025e33d84012af39c.pac
- Click 'OK'

Set SWG Proxy via Windows Group Policy

- Group Policy Objects (GPOs) are used to publish settings to multiple endpoints based on Active Directory group, domain or organization.
- This helps networks with Active Directory to set proxies faster and easier over a Windows Server.

Note: It may take a while for all computers to receive the rule and may require a restart.

Step 1 - Create a New Group Policy Object

1. Log on to your Windows Server in the domain then click Start > Programs > Administrative Tools > Active Directory Users & Computers
2. Right click on the domain or Organizational Unit where the Group Policy should be applied
3. Select "Create a GPO in this domain, and Link it here..."
4. Create a new GPO (e.g. Comodo Web Security)
5. Click 'OK'

Step 2 - Set proxies in endpoint browsers using the created GPO:

Internet Explorer:

Edit the GPO for SWG PAC File

1. Right click on the new GPO and Select 'Edit'.
2. In the Group Policy window, click User Configuration > Windows Settings > Internet Explorer Maintenance > Connection > Click on Automatic Browser Configuration
3. On the Automatic Configuration tab, select 'Automatically detect configuration settings and Enable Automatic Configuration'
4. Enter a time interval in the 'Automatically configure every' check box.
5. Enter the following Comodo SWG PAC URL, for example, https://dome.comodo.com/pac_file/f09ed11bfe157ae025e33d84012af39c.pac
6. Click 'OK'

Firefox and Chrome:

Edit the GPO for SWG PAC File

1. Right-click on the new GPO and Select 'Edit'.

2. Select Computer Configuration > Administrative Templates
3. Choose 'Add Template', click 'Add' and open firefoxlock.adm for Firefox or chrome.adml for Chrome.
4. Refresh the window and go to Computer Configuration > Administrative Templates and double-click the browser related selection for editing.
5. Open 'Proxy Settings'.
6. Select 'Automatic Proxy Configuration option' and paste SWG PAC URL, for example https://dome.comodo.com/pac_file/f09ed11bfe157ae025e33d84012af39c.pac
7. Click 'OK'.

Note:

- The PAC URL for your account can be found in the Comodo SWG console at 'Configuration' > 'Configuration' > 'PAC'.
- You can customize the PAC file to grant direct access to domains and bypass Comodo SWG.
- See '**Configure PAC File**' for more details.
- User-based rules are not supported for traffic forwarded via Direct Proxy or PAC methods.
- Comodo SWG uses ports 17443, 19443 and 19080 to connect to your networks. Please configure your firewall to allow SWG traffic over these ports.

- After connecting your network(s), make sure to add them as a 'Trusted Network' in the 'Locations' interface.
  - If you do not then Comodo SWG will not function correctly and your network will not be able to connect to the internet. See next step **Connect your network(s) to Comodo SWG**
  - No need to select any authentication and traffic forwarding option on the Locations interface.

Please contact us at **domesupport@comodo.com** if you have any issues connecting endpoints / networks to Comodo SWG.

Traffic Forwarding via Proxy Chaining

- As the name implies, proxy chaining is used to link multiple forward proxies to obtain the benefits of each.
- This method is suitable for larger organizations with multiple networks that want to direct web traffic through Comodo SWG.
- Comodo SWG is designed to be placed as the "Upstream Proxy" to other web gateways such as Websense, Bluecoat, iboss and so on.

The following examples use a Bluecoat Proxy SG and Comodo SWG integration scenario, where Bluecoat is downstream and Comodo SWG is the upstream proxy.

1. Basic Chaining

Bluecoat > Comodo SWG

In this scenario, Bluecoat Proxy SG is forwarding requests to Comodo SWG but performing no authentication. SWG can be set to do Active Directory authentication.

Use the Blue Coat Management console to forward requests to the SWG as following:

1. In the Blue Coat Management Interface, under the 'Configuration tab', go to Forwading > Forwarding Hosts.
2. Select 'Install from Text Editor' from the drop-down then click 'Install'.
3. Edit the 'Forwarding Hosts' configuration file to point to SWG. e.g:
   - Add "fwd_host Dome_Proxy X.X.X.X http=19080" at the end of "Forwarding host configuration" section.
   - Add "sequence Dome_Proxy" to the end of "Default fail-over sequence" section.

4. Once editing is complete, click 'Install'.
5. In the 'Configuration' tab, go to 'Policy' and select 'Visual Policy Manager'.
6. Click 'Launch'.
7. In the 'Policy Menu', add a new Forwarding Layer with a chosen policy name.
8. Select the Forwarding Layer tab that is created. Edit source, destination and service columns with necessary information. You can also leave as 'Any' by default.
9. Select the alias name you created in steps 2-5 (e.g: Dome_Proxy) from the list.
10. Click OK.
11. Click Install Policy.

2. X-Authenticated-For Chaining

In this scenario, Bluecoat will be configured to pass X-Authenticated-User headers to SWG Proxy and Bluecoat will be doing user authentication as the downstream proxy.

> **Note 1**: Comodo SWG supports passing X-Forwarded-For headers but can not use them with granular policies. They can, however, be used in reporting. Global Policy will be applied to such traffic.
>
> **Note 2**: Comodo SWG honors X-Authenticated-User headers first and X-Forwarded-For headers next. If you want to set granular policies, use X-Authenticated-User headers.

Edit Bluecoat local policy file:

1. Go to the 'Configuration' tab.
2. Click 'Policy' in the left column and select 'Policy Files'.
3. Edit the text file as following:

   <Proxy>

   action.Add[header name for authenticated user](yes)

   define action dd[header name for authenticated user]

   set(request.x_header.X-Authenticated-User, "WinNT://$(user.domain)/$(user.name)")

   end action Add[header name for authenticated user]

Or use the Visual Policy Manager

1. Go to the 'Policy Menu' and select 'Add Web Access Layer' and give the policy a name
2. Set Source, Destination, Service and Time column as 'ANY'
3. Right click on 'Set' and click 'New' then 'Control Request Header'
4. Enter X-Authenticated-User in the 'Header Name' field.
5. Select 'Set Value' radio button and enter: WinNT://$(user.domain)/$(user.name)
6. Click 'OK'.
7. Click 'New' and select 'Combined Action Object', enter a name, select the previously created headers and Click 'Add'.
8. Click 'OK'.
9. Click 'Install Policy'.

Note:

- After connecting your network(s), make sure to add them as a 'Trusted Network' in the 'Locations' interface.
  - If you don't add the network(s) as 'Trusted Network' then Comodo SWG will not function correctly. Your network will also not be able to connect to the internet.
- See next step **Connect your network(s) to Comodo SWG**
- Select 'Proxy Chain' as authentication and traffic forwarding option in the 'Locations' interface.
- User-based rules are supported for Proxy Chaining traffic forwarding method.
- Comodo SWG uses ports 17443, 19443 and 19080 to connect to your networks. Please configure your firewall to allow SWG traffic over these ports.

Please contact us at **domesupport@comodo.com** if you have any issues connecting endpoints / networks to Comodo SWG.

Traffic Forwarding via Internet Content Adaptation Protocol (ICAP)

- Similar to the proxy chain scenario as explained in the previous step, ICAP integration is required when there is another ICAP client in your network.
- Like the chain scenario, traffic first comes to the network device and communicates with Comodo SWG using the ICAP protocol. Packets go from the endpoint to the ICAP client first, then to Comodo SWG, pass back to the ICAP client and then to the internet.

The following example explains the ICAP method using a Bluecoat Proxy SG and Comodo SWG integration scenario, where Bluecoat is the ICAP Client and Comodo SWG is ICAP Server.

ICAP Integration

In this scenario, the Bluecoat Proxy will be acting as the ICAP client where Comodo SWG is the ICAP server. It's recommended to send both responses and requests to Comodo SWG's ICAP Service.

- Comodo SWG Response Mode URI: icap://ipofdome:1344/response
- Comodo SWG Request Mode URI: icap://ipofdome:1344/request

Click 'Configuration' > 'Configuration' on the left then 'ICAP' to view the Comodo SWG IP for your account.

Note 1: For Comodo SWG to deliver web access controls and URL blocking, responses must be sent to Comodo SWG's Response Service.

Note 2: For Comodo SWG to deliver containerization and Valkyrie services, requests must be sent to Comodo SWG's Request Service.

On Bluecoat Visual Manager

1. Go to 'Configuration, External Services and ICAP'.
2. Click 'New'
3. Give the ICAP Service a name (e.g. ' Comodo SWG Request')
4. In the service list, select the new service you just created and click 'Edit'.
5. Add the SWG Request URL to Service URL (Comodo SWG Service URL is icap://ipofdome:1344/request) and select 'Method Supported' as 'Request Modification'.
6. Click 'OK'.
7. Click 'Apply'.

Repeat the process above for Response modification.

Note: The IP varies for different accounts and the Comodo SWG IP for your account can be found in the section, Configuration > ICAP

- After connecting your network(s), make sure to add them as a 'Trusted Network' in the 'Locations' interface..
  - If you don't add the network(s) as a 'Trusted Network' then Comodo SWG will not function correctly. Your network will also not be able to connect to the internet.
- See next step **Connect your network(s) to Comodo SWG**.
- Select 'ICAP' for user authentication and traffic forwarding option on the Locations interface.
- User-based rules are supported for ICAP traffic forwarding method.
- Comodo SWG uses ports 17443, 19443 and 19080 to connect to your networks. Please configure your firewall to allow SWG traffic over these ports.

Please contact us at **domesupport@comodo.com** if you have any issues connecting endpoints / networks to Comodo SWG.

Traffic Forwarding via SWG Agent

Another method of forwarding traffic from endpoints to Comodo SWG is to install SWG agents on them. This is useful if you:

- Don't want to use any of the first three methods (direct proxy/PAC, proxy chaining or ICAP)
- Have a limited number of endpoints to protect
- Want to protect endpoints outside of your network

The main purpose of installing the SWG agent is to protect roaming devices and deploy user-specific rules. However, these devices can also be used in a protected network. Network location based policies will be applied to such devices.

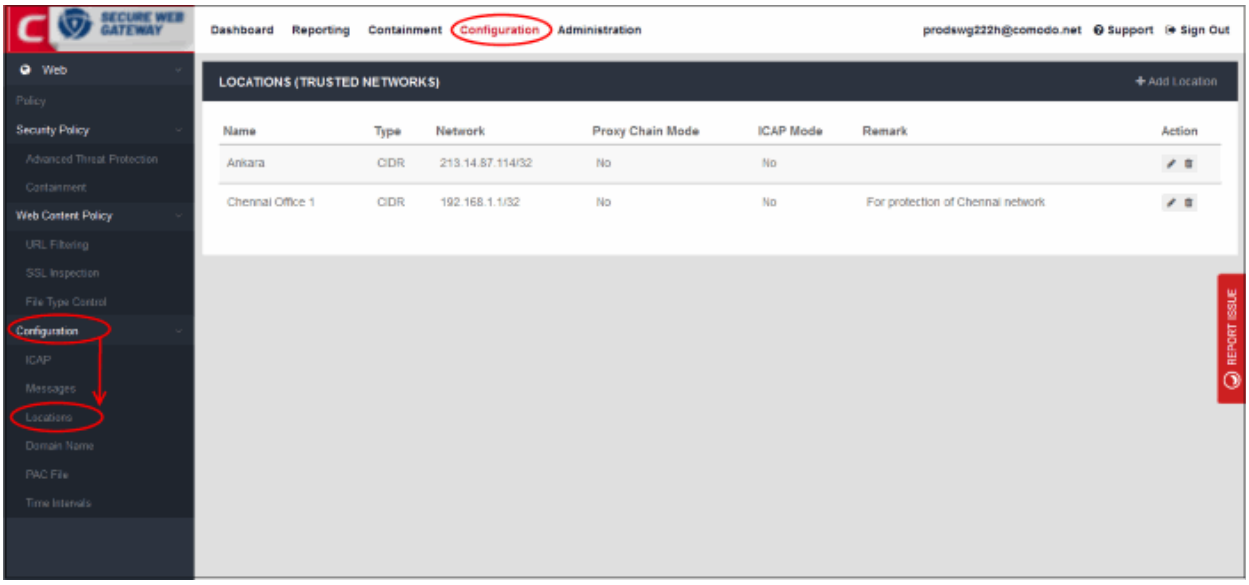
- Supports user specific policies deployment.
- Supports computer specific policies deployment.
- There is no need to select any authentication and traffic forwarding option on the Locations interface.
- See the step '**Connect your roaming device(s) to Comodo SWG**' for information about how to install SWG agents on devices.
- Comodo SWG uses ports 17443, 19443 and 19080 to connect to your networks. Please configure your firewall to allow SWG traffic over these ports.

Connect your Network(s) to Comodo SWG

- After **setting up traffic forwarding**, the next step is to add a 'Trusted Network'. Comodo SWG will not function correctly until you have done so.
- The default security and URL filtering policies are applied to all endpoints in trusted networks.
- You can also create network-specific policies.
  - Policies are prioritized top-to-bottom according to the list in 'Configuration' > 'Policy'.
  - In the event of a conflict between policies over a security setting, the setting in the policy nearer the top of the list will prevail.
  - You can change the priority of a policy by clicking 'Edit' > 'Policy Order' in the 'Configuration' > 'Policy' interface.

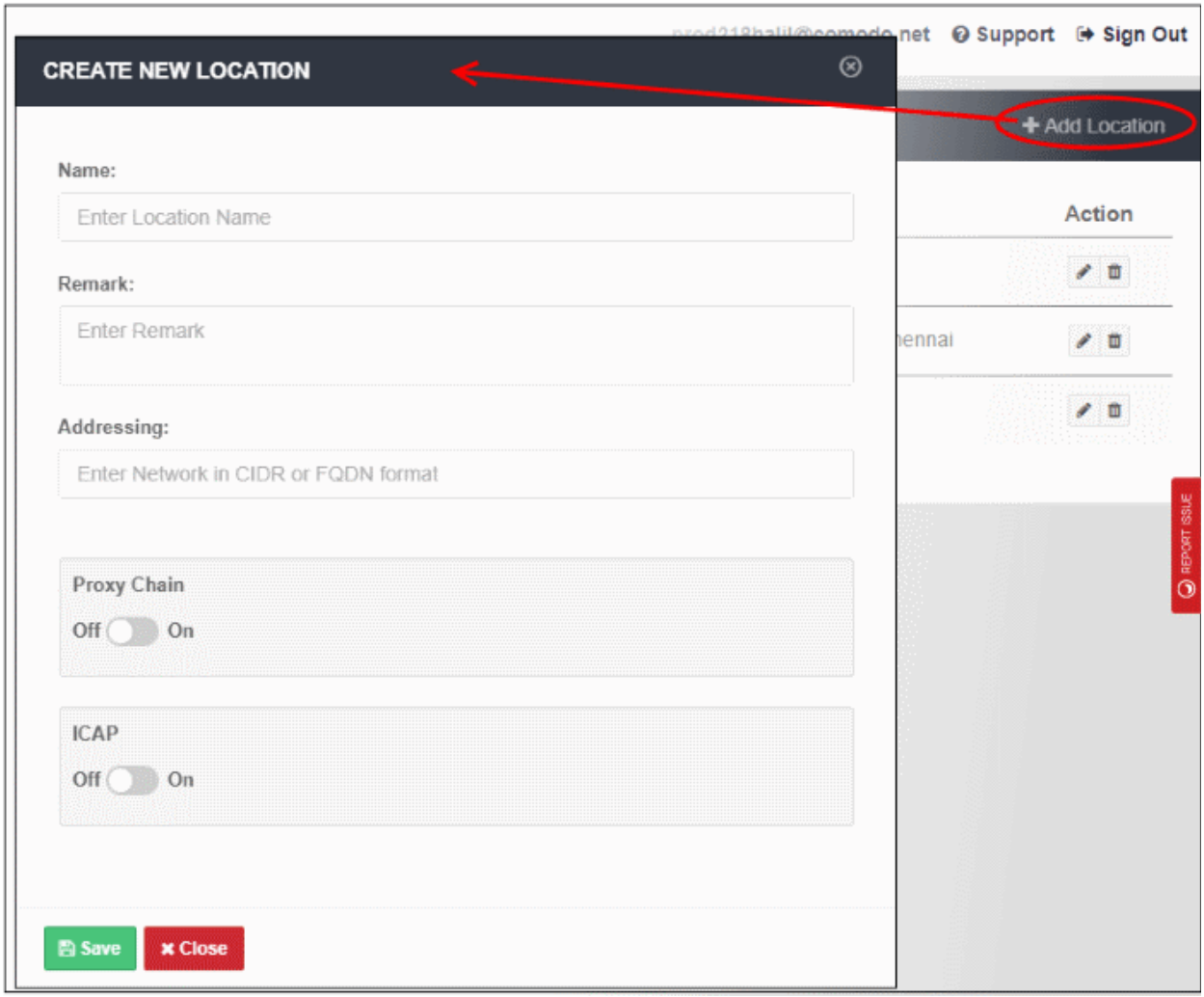
This step explains how to add and manage networks in the 'Locations (Trusted Networks)' interface.

- Click 'Configuration' > 'Configuration' > 'Locations' to open the trusted networks interface:



Add your location

- Click 'Add Location' at the top right of the interface



- **Name** - Enter an appropriate label for the location.

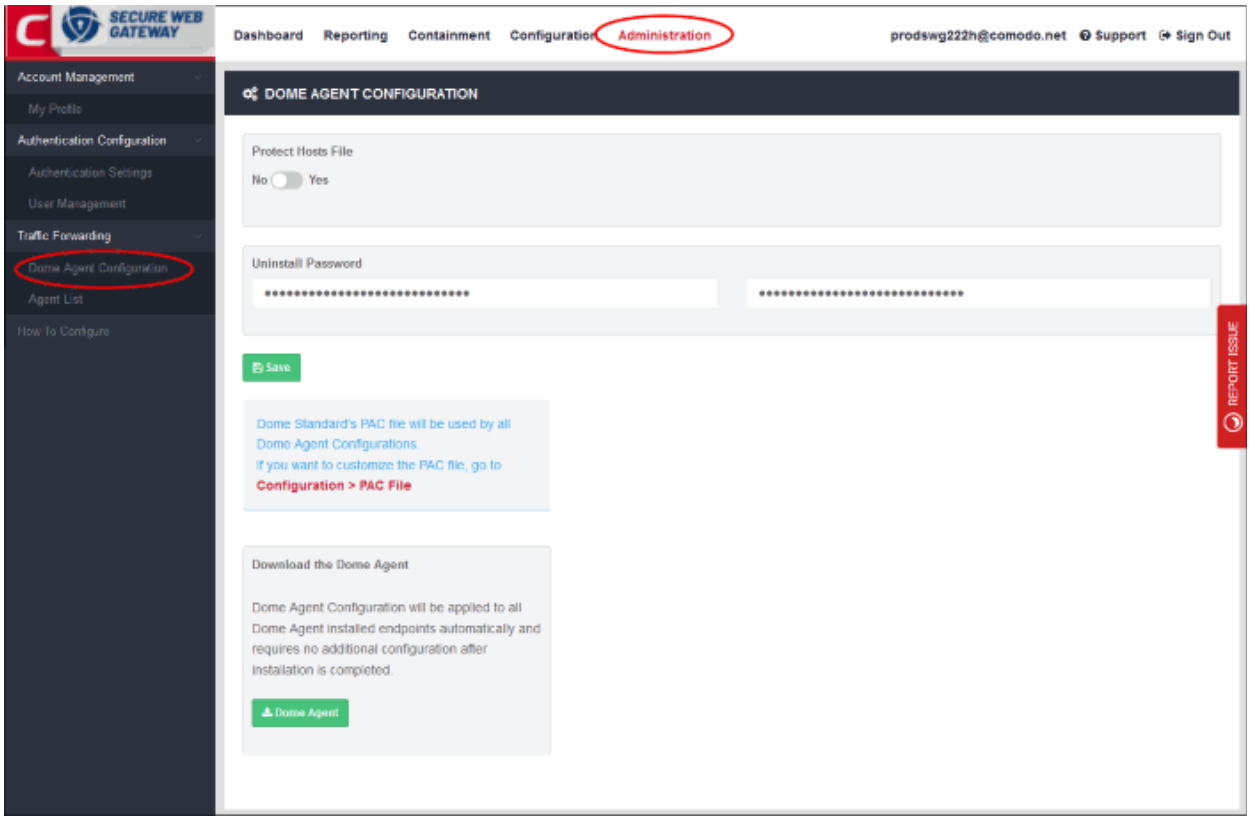
- **Remark** - Enter comments, if any, about the location.
- **Addressing** – The public IP or fully qualified domain name (FQDN) of the network that you have added. See **Connect your Network to Comodo Secure Web Gateway** if you need help with this.
- **End user authentication and traffic forwarding** - The method used for traffic forwarding and user authentication.
  - Available options are 'Proxy Chain' and 'ICAP'. Select the appropriate method for your network.
    - If you don't enable either then SWG agent authentication and traffic forwarding will be used.
  - Note - If you enable user authentication then you must add and configure users in the 'User Management' interface.
    - If you don't enable user authentication, then you cannot deploy user-based policies. Instead, network based rules or default rules will be applied to all users in the network.
    - See steps '**Add Users**' and '**Configure User Authentication Settings**'.
- Click 'Save' to apply your changes

The location will be added and shown in the list. The default policy will be automatically applied to newly added network.

Connect your Roaming Device(s) to Comodo SWG

Comodo SWG can protect roaming users who are outside a fixed network. This is especially useful for users on the move like field sales teams. It is also useful for remote workers who access the internet from outside your network.

- You must install the roaming agent on a device to connect it to SWG protection. This is because the device will use dynamic IP addresses.
- Once installed, any policies defined for 'Roaming users' will be applied to the device. If none are defined then the default 'Global Policy' is applied.
- Click 'Administration' > 'Traffic Forwarding' > 'SWG Agent Configuration' to download and configure the agent:

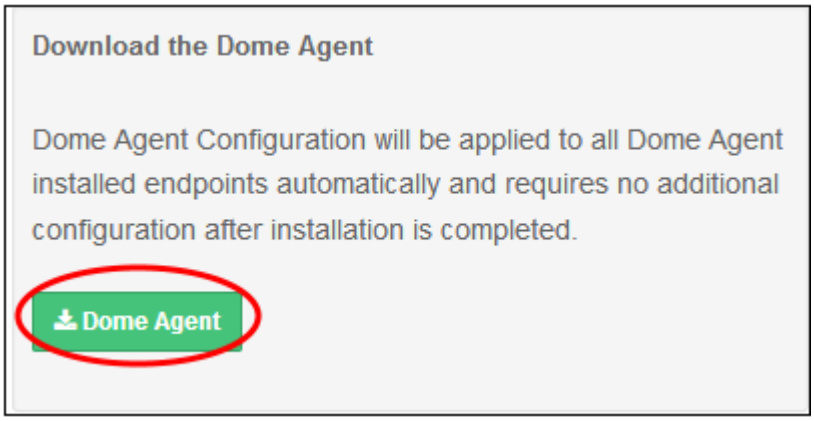


- **Protect Hosts File** - Determines whether a user can access non-public, internal domains.
  - For example, if you have added an internal domain to the 'Hosts' file, then 'Comodo SWG' proxy cannot resolve it since it is not available publicly.
  - The default setting is 'No'. If you select 'Yes', the internal domain will be accessible to the user. A direct connection is established between the internal domain and the remote device.
  - Note – you can achieve the same result by configuring the PAC file or the proxy setting on the device's internet browser.
- **Uninstall Password** - The password required to uninstall the SWG agent from the roaming device.
- **Configure PAC file** - A proxy auto-config (PAC) file determines which proxy servers a browser or client should use to access a given URL. You can customize the PAC file according to your requirement. See '**Configure PAC File**' if you want more help with this.

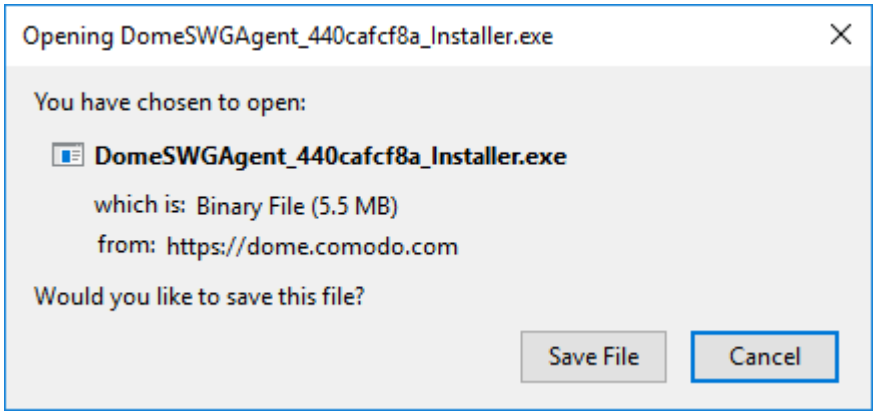
- Click 'Save' to apply the settings to the agent.

Download the 'SWG Agent'

- Click the 'SWG Agent' button:



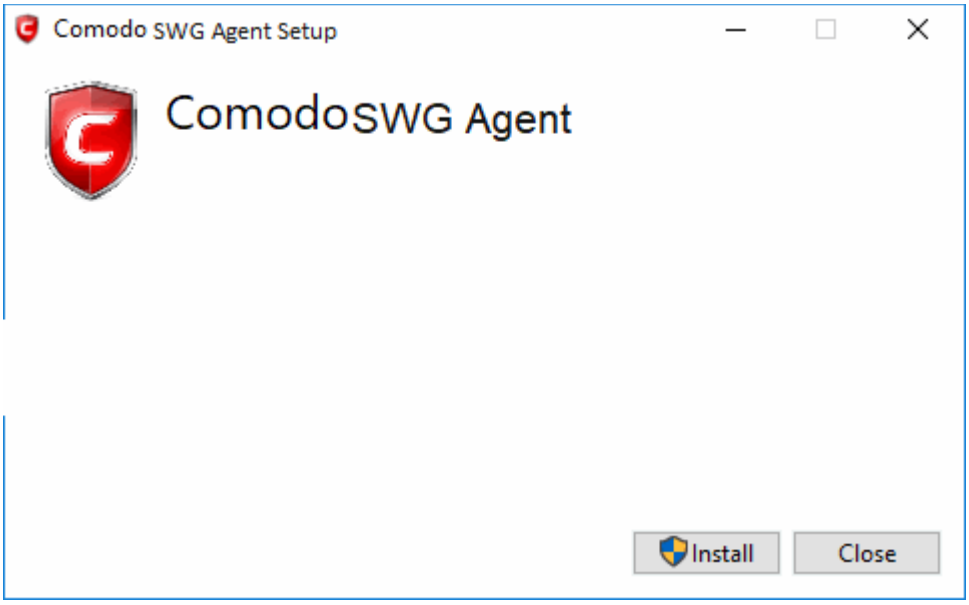
Click 'Save File' in the download dialog:



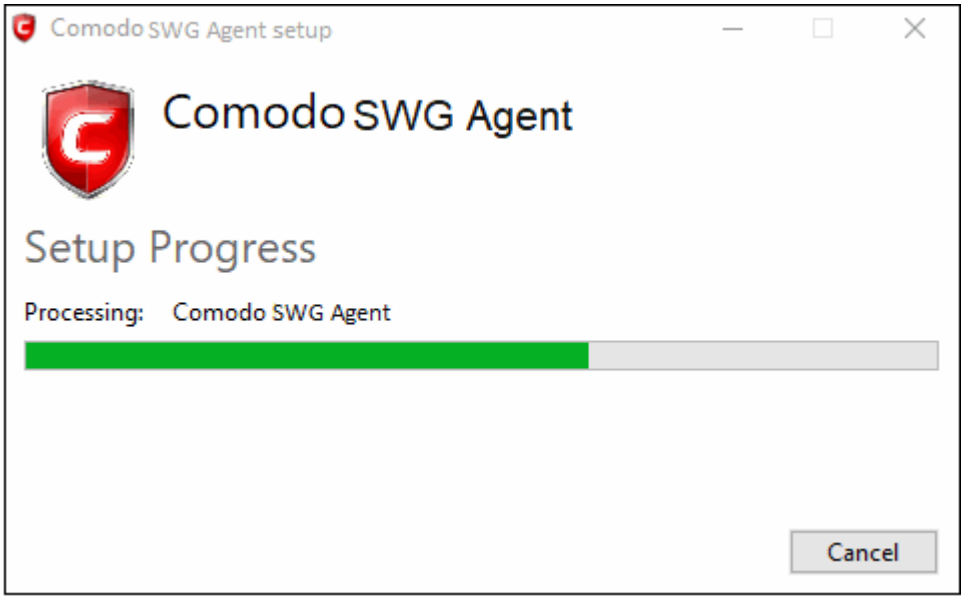
- Copy the agent to all roaming devices you want to protect.

Install the agent

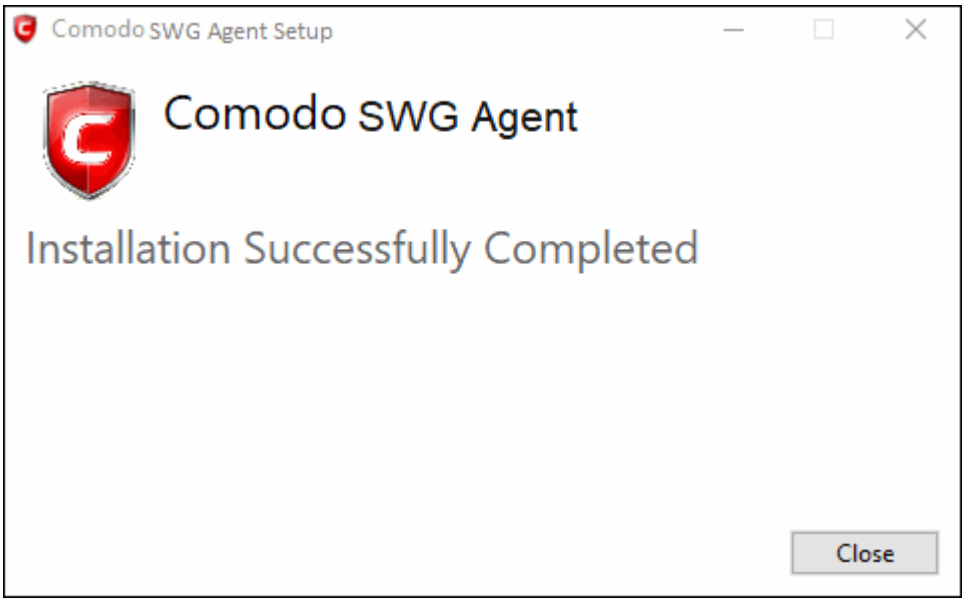
- Run the agent setup file



- Click 'Install'



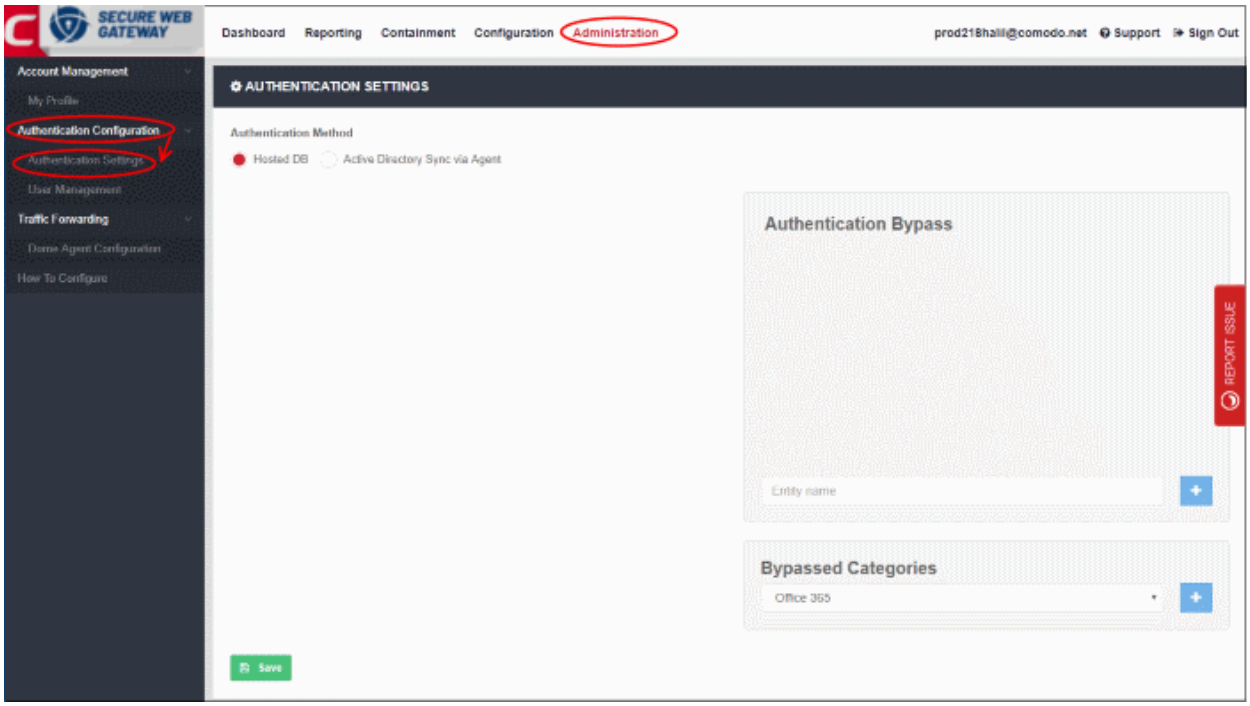
- Click 'Close' after the agent installation is complete.



- Click 'Administration' > 'Traffic Forwarding' > 'Agent List' to view computers that have the agent installed. See '**View Enrolled Roaming Devices**' if you need help with this interface.
- Note - If the devices are connected to networks that have been added to **Locations** then the location based rules will apply to them. Rules at the top of the list take precedence.
- You must have added users before you can apply policies to them. See steps '**Add Users**' and '**Apply Policies**'

Configure User Authentication Settings

- Click 'Administration' > 'Authentication Configuration' > 'Authentication Settings' to open this interface.
- You have to choose a user authentication method if you want to apply policies to specific users. You do not need to do this if you only plan to apply policy to networks/devices.
- There are two methods available - 'Hosted DB' and 'Active Directory'. You can select only one authentication method per account.
- After **connecting your networks** and adding them to 'Locations', the default security and URL filtering polices are applied to endpoints (unless custom policies exist).
- You must first have added users before you can apply custom polices to them. You can add users in 'Administration' > 'Authentication Configuration' > 'User Management'. See next step '**Add Users**'.



Authentication Method

- Comodo SWG supports 'Active Directory' and 'Hosted Database' authentication. You can only use one of these types.
- You can combine auth types with **traffic forwarding types**
- Comodo recommends the following types of combinations:

S.No	Auth Type	Traffic Forwarding Types
1	Hosted DB	SWG Agent, ICAP and Proxy Chain
2	Active Directory	SWG Agent
Note: You can only create network location rules for 'Direct Proxy' and 'PAC' traffic forwarding. You cannot create user based rules for these forwarding types.		

Authentication methods for user-based rules explained:

- **Traffic forwarding via SWG Agent** – The SWG agent authenticates users via Windows authentication on the device. There is no need to select any **authentication and traffic forwarding option** on the **Locations** interface. Hosted DB and Active Directory authentication methods are supported.
- **Traffic forwarding via Direct Proxy or PAC** – User-based rules are not supported for these forwarding types, so no authentication is required. No need to select any **authentication and traffic forwarding option** on the **Locations** interface.
- **Traffic forwarding via Proxy Chaining / ICAP methods** – If you plan to use a 3rd party proxy such as Websense or Bluecoat, then you can integrate with SWG and use **Proxy Chaining** / **ICAP** to forward traffic. Once done, you can create user-based rules if the 3rd party product authenticates and sends user names to SWG. You have to select the appropriate **authentication and traffic forwarding option** on the **Locations** interface. Only Hosted DB authentication is supported.

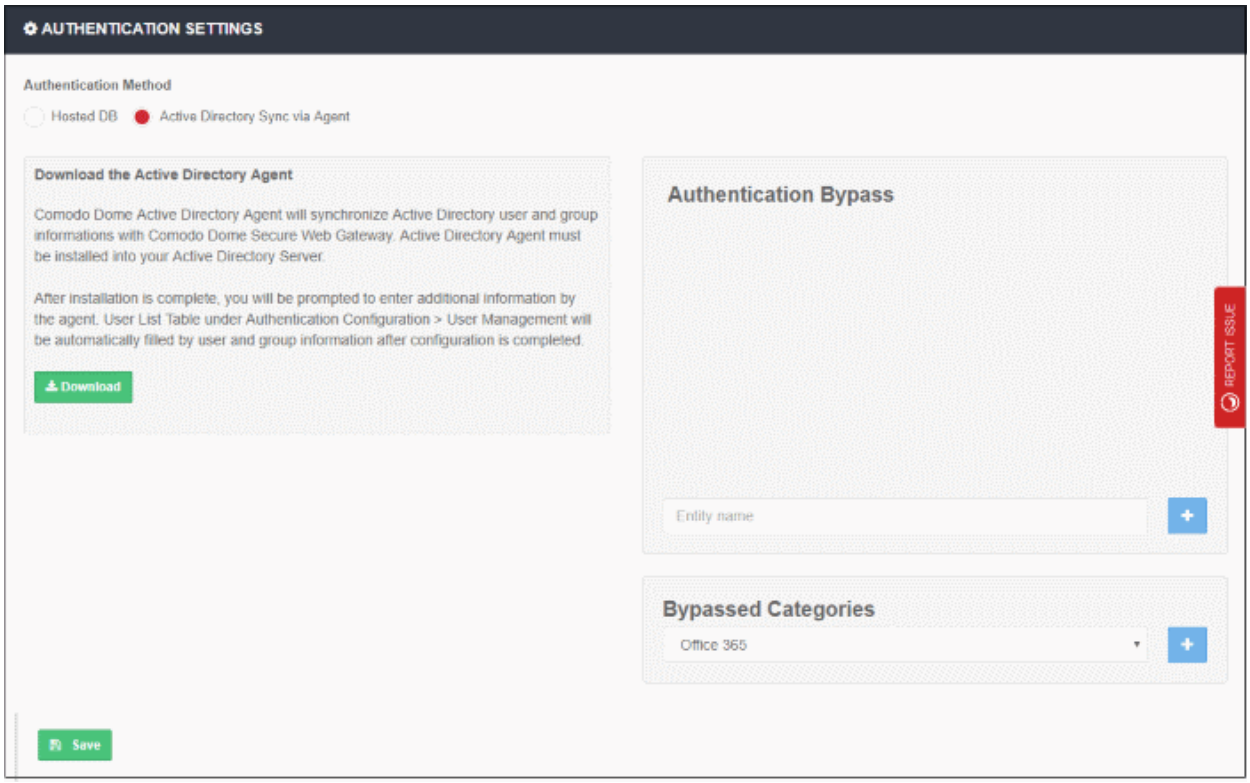
Hosted DB

A user database hosted on Comodo SWG is used for authentication and identification. You will need to provide additional details including group and department in the 'Add User' dialog. See step '**Add Users**'.

Active Directory

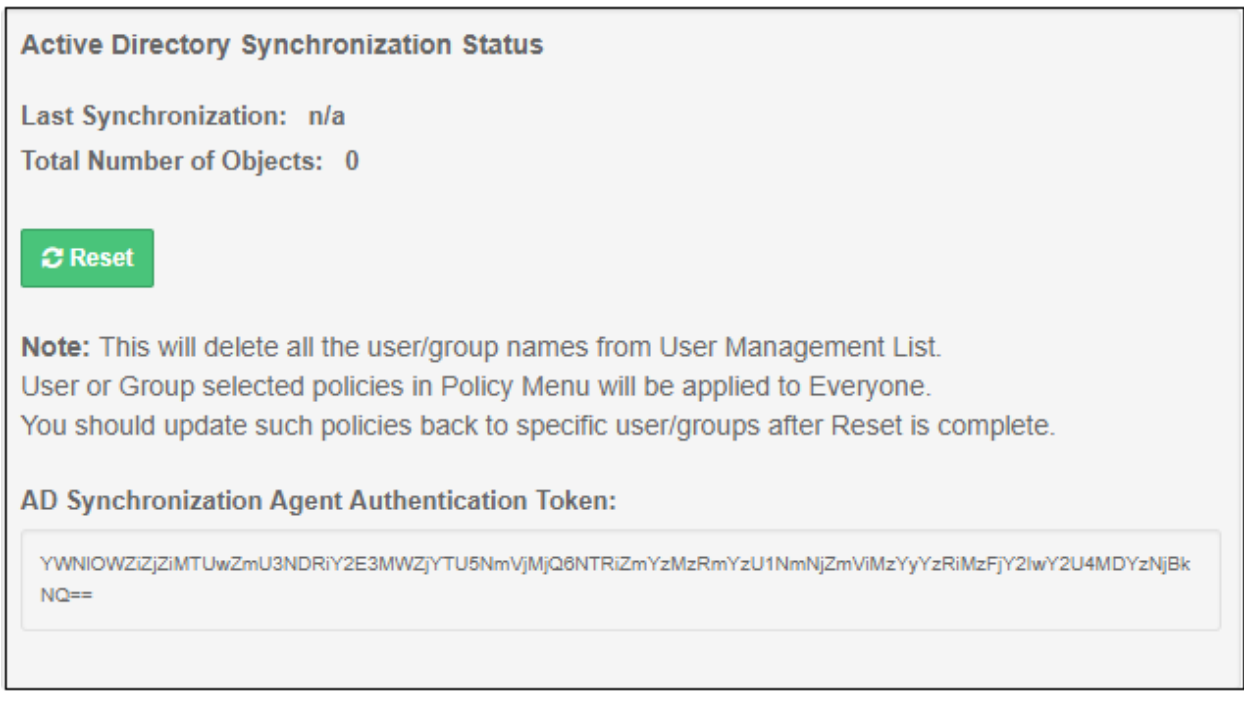
Users are authenticated using Active Directory. To use this method, you need to download the SWG AD agent and install it in your AD server. After installation and configuration, AD users and groups will be automatically enrolled to Comodo SWG and be visible under 'User Management'.

- Select 'Active Directory Sync via Agent' under 'Authentication Method'



- Click 'Download'
- The agent setup file will be downloaded to your default location
- Click 'Save' in the 'Authentication Settings' screen

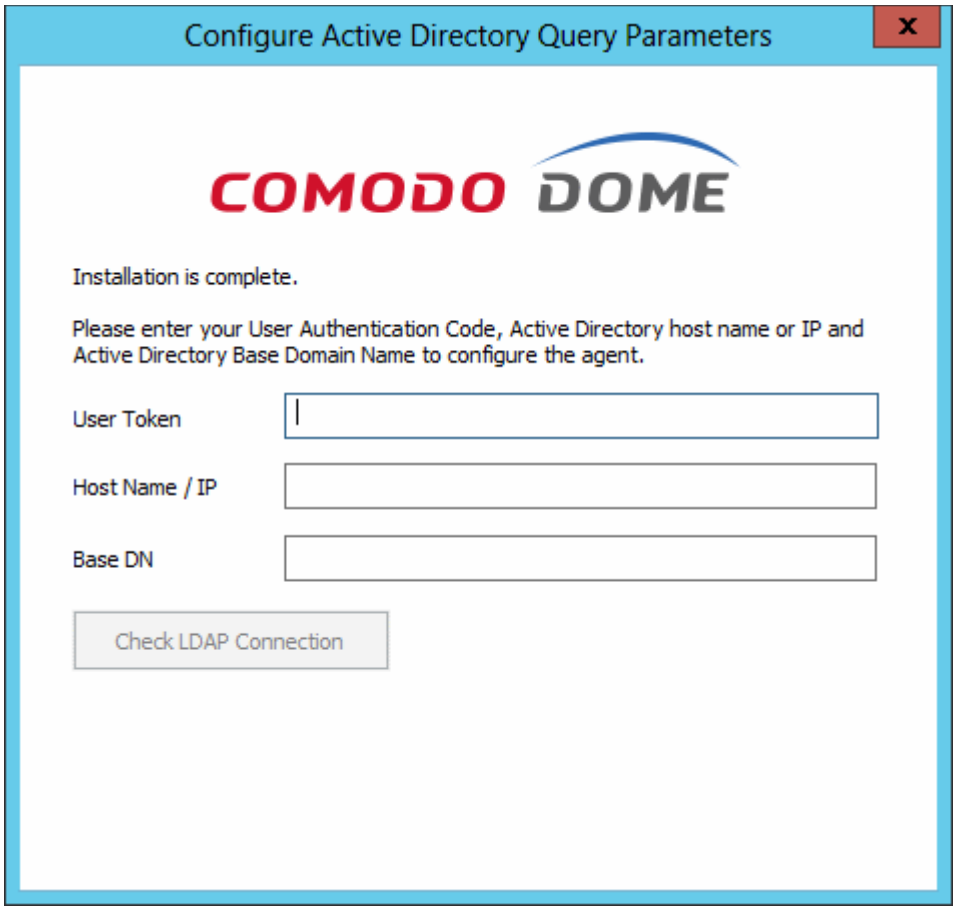
A unique AD sync agent authentication token will be generated.



- Copy this token and save it
- Next, transfer the setup file to any client machine which is included in the AD server, or to the AD server itself.

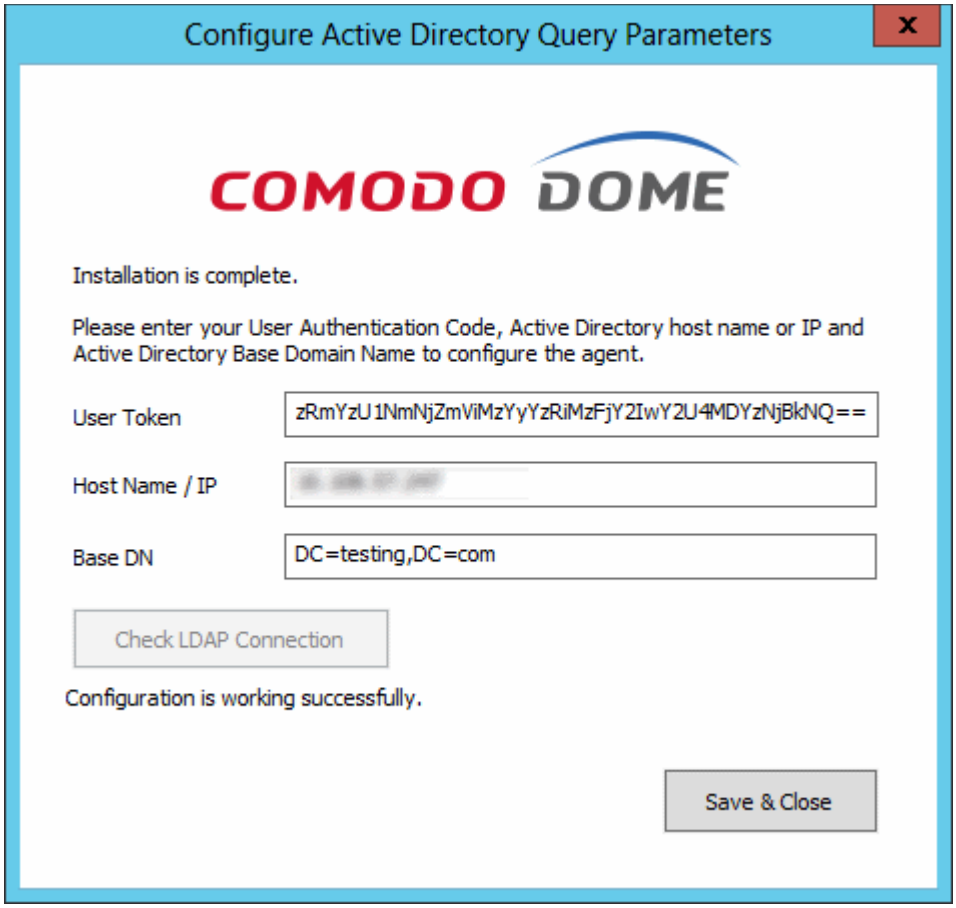
Install SWG AD agent

- Run the setup file and complete the AD connection details form:



- User Token – Copy and paste the AD sync authentication token that you saved earlier
- Host Name / IP – Enter the host name or IP of the AD server
- Base DN – Enter the user base DN details, for example, DC=testing,DC=net
- Click 'Check LDAP Connection

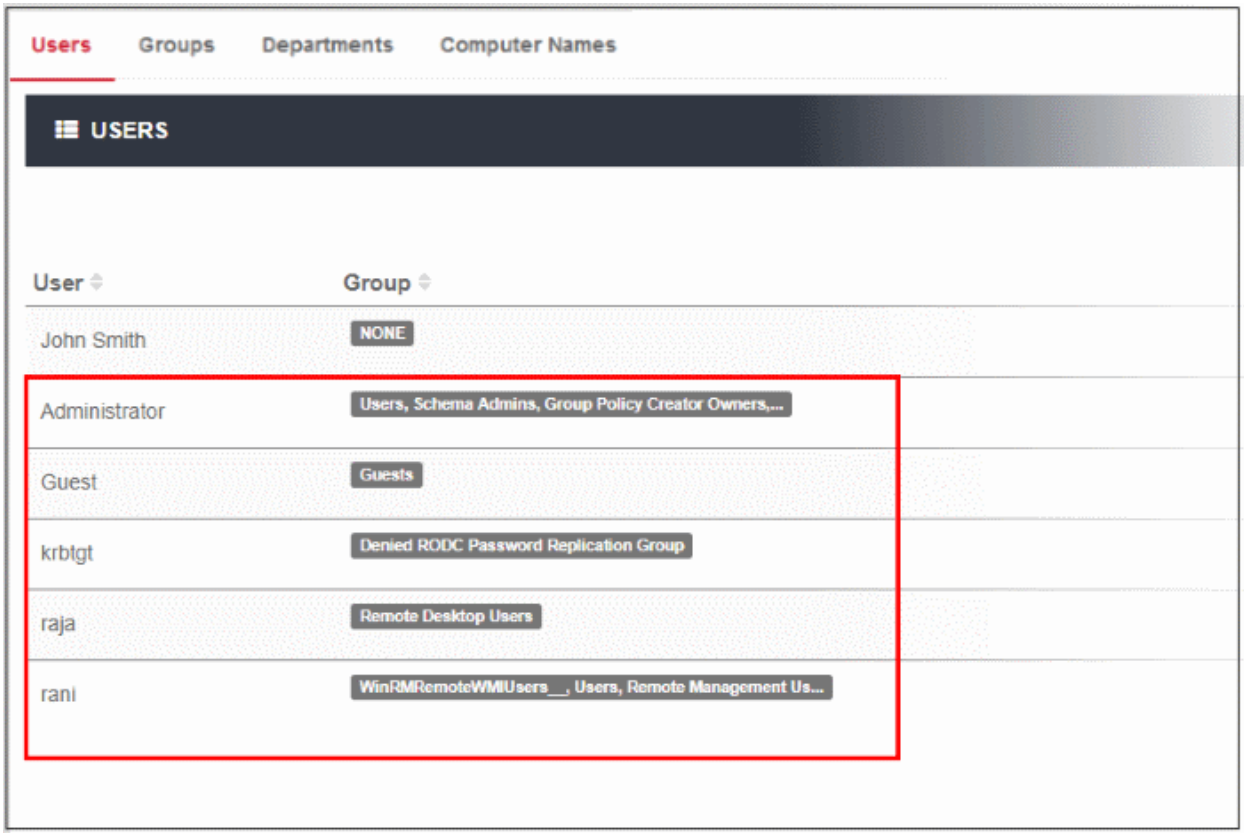
You will see the following dialog after a successful connection:



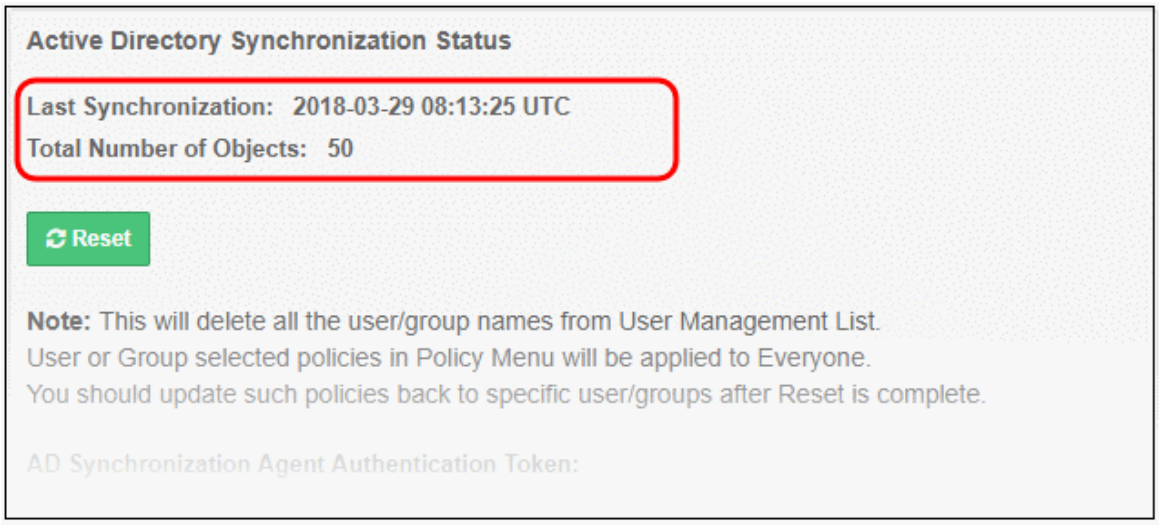
- Click 'Save & Close'

AD users and groups will be automatically added to Comodo SWG after the first synchronization.

- Click 'User Management' and 'Users' / 'Groups' to view the enrolled users and group via AD.



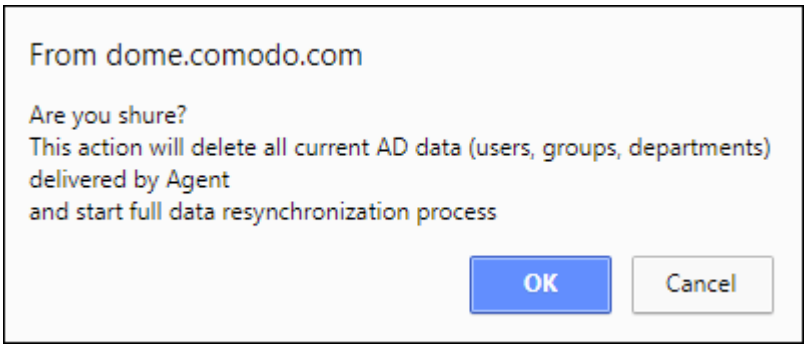
The AD agent will initiate subsequent synchronizations every 3 hours automatically.



- Last Synchronization – Date and time that Comodo SWG most recently synchronized with the LDAP server
- Total Number of Objects – The number of users and groups enrolled to Comodo SWG via AD

Reset Synchronization

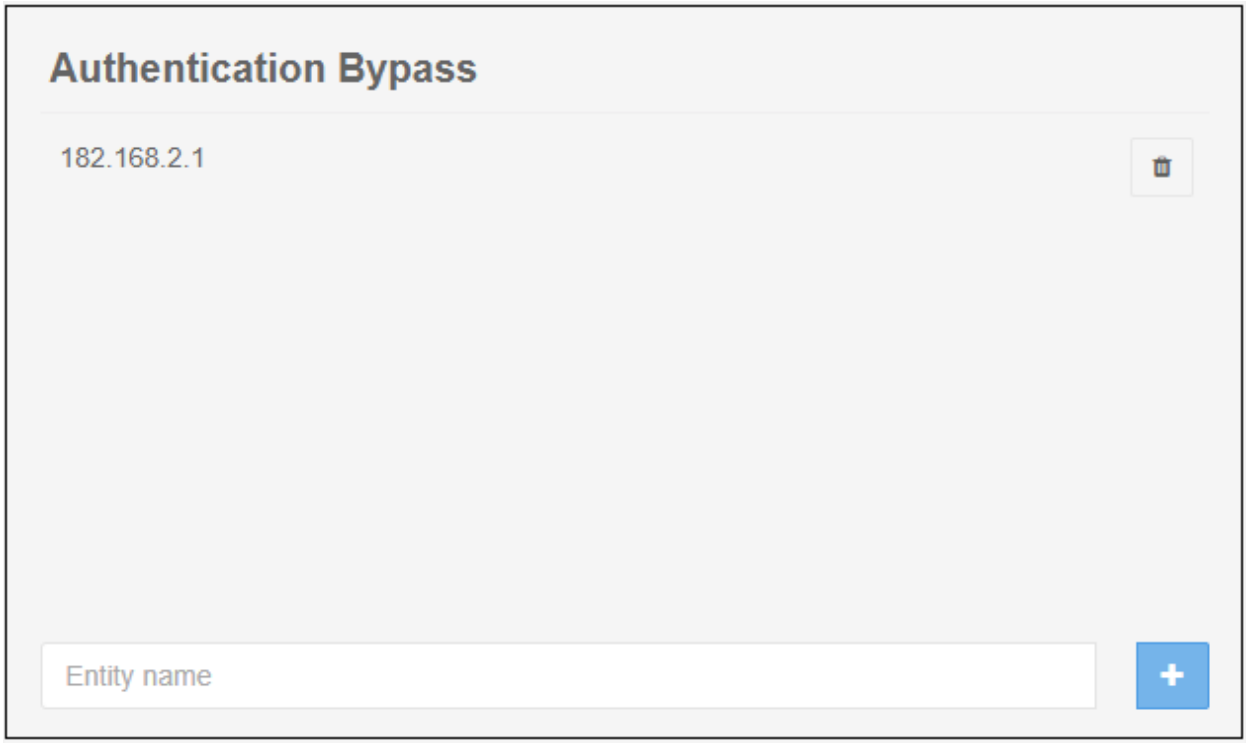
- Click 'Reset'



- Click 'OK'
- All the users / groups enrolled via AD will be removed from the 'User Management' list.
- SWG agent will initiate re-synchronization process and will complete in few minutes.
- Specific users / groups policies should be reapplied.

Authentication Bypass

- Specify the domain, wildcard domain, IP address or network for which you want to skip authentication



- Enter the details and click the '+' button on the right to add the exception
- Click the trash can icon beside an entry to remove it
- Click 'Save' for your changes to take effect

Bypassed Categories

- Specify the category of applications that you want to exempt from authentication.

- Choose the application from the list and click the '+' button on the right to exempt a category.
  - If the user is within the network then they will be automatically authenticated by the domain controller.
  - If the user is outside the network then the browser will ask the user to authenticate themselves with their AD credentials. Comodo SWG will direct the credentials to the domain controller for authentication.
- Click the trash can icon beside an entry to remove it
- Click 'Save' for your changes to take effect

Add Users

In order to apply specific policies for users, you have to:

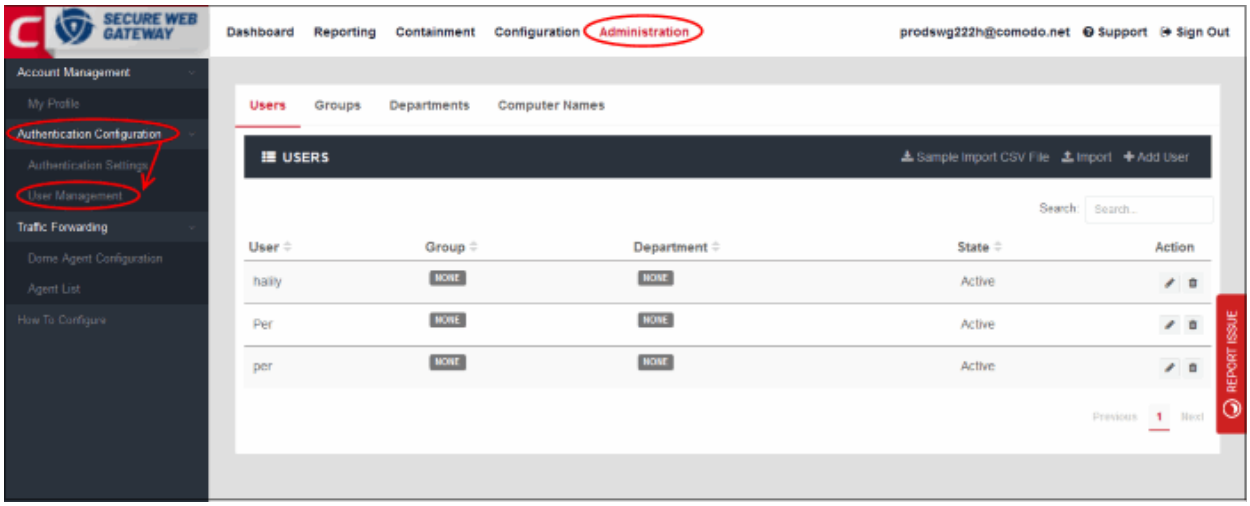
- **Install SWG agent on the devices** (recommended), or use traffic forwarding via the **proxy chaining** / **ICAP** methods.
- Configure **user authentication settings**
  - Traffic forwarding via SWG agent - No need to select an **authentication and traffic forwarding option** on the **Locations** interface.
  - Traffic forwarding via **proxy chaining** / **ICAP** - Select the appropriate **authentication and traffic forwarding option** in the **Locations** interface.
  - Select a user authentication method – Hosted DB auth method supports traffic forwarding via all three methods – SWG agent, proxy chaining and ICAP. Active Directory supports only SWG Agent.
- Create user-specific policies and apply them. See **Create Policies** and **Apply Policies**.
- Add users to Comodo SWG. This section explains how to add users.

There are three ways to add users:

- **Add users manually**
- **Import via a CSV file**
- **Sync via Active Directory**

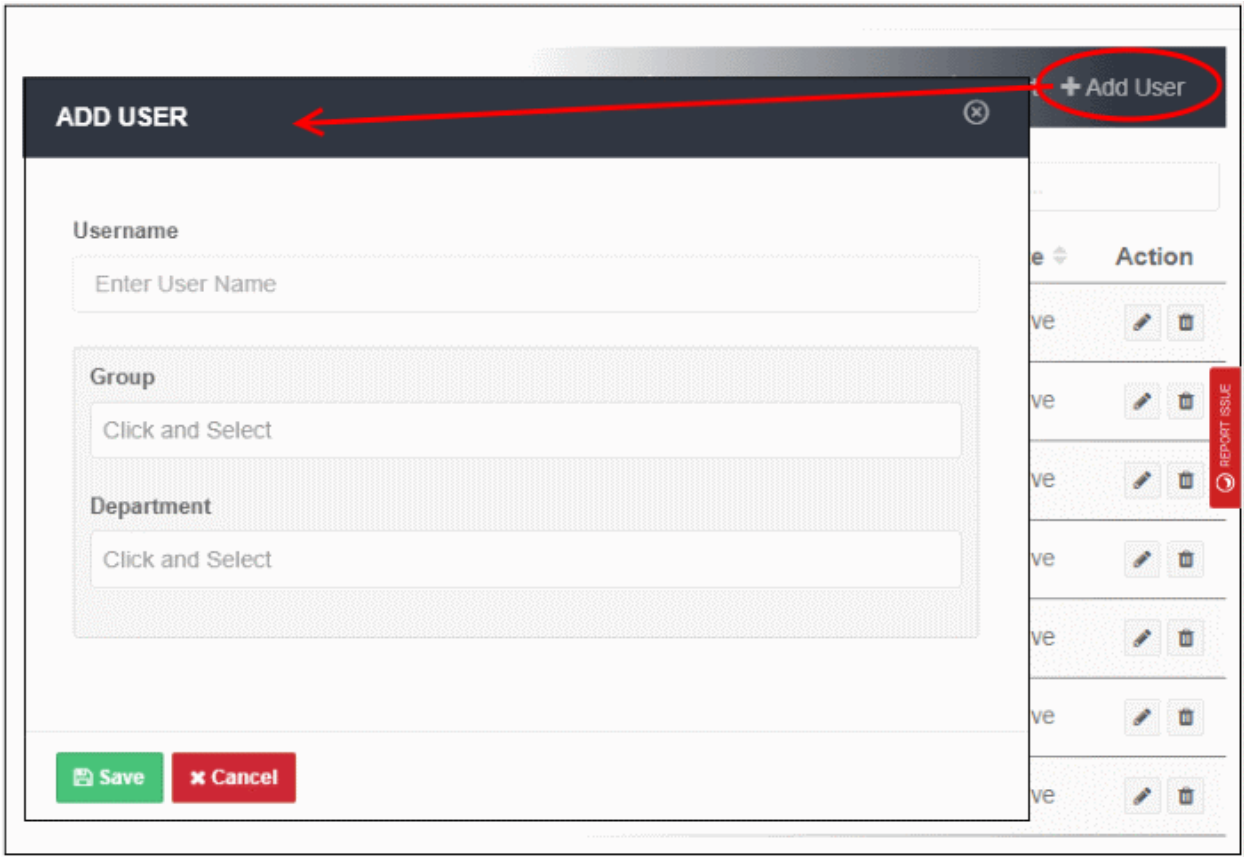
Add Users Manually

- Click 'Administration' > 'Authentication Configuration' > 'User Management'



- Click 'Users' and then 'Add User' at top-right

The 'Add User' dialog will open:



- **Username** - Enter the username of the user. Please make sure this is same as in 'Users' in Windows.
- **Group** - Relevant only if 'Hosted DB' is selected in the '**Authentication Settings**' interface. Click in the field and select the appropriate group for the user. Groups added to the 'Groups' interface will be listed here.
  - To add a group, click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Groups' tab > 'Add Group'
  - Enter a name for the group and add any comments in the 'Remarks' field.
  - Click 'Save'

- **Department** - Relevant only if 'Hosted DB' is selected in '**Authentication Settings**'. Click on the field and select the appropriate department for the user. Departments added to the 'Departments' interface will be listed here.
  - To add a department, click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Departments' tab > 'Add Department'
  - Enter a name for the dept. and add any comments in the 'Remarks' field.
  - Click 'Save'
- Click 'Save' in the 'Add User' dialog when done

The 'User' will be added and displayed in the list.

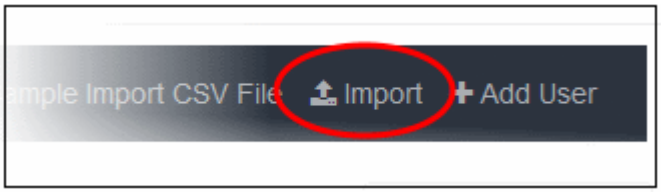
Import users from a CSV file

You can bulk import users from a CSV file.

- There is a sample .csv file in 'Administration' > 'Authentication Configuration' > 'User Management' > 'Users' > 'Sample Import CSV File'.
- Enter user data separated by commas, as follows:
  - username,group,department
- Username is mandatory. Other fields are optional.
- Each user should be on a separate line
- Each user can be member of one, several or no groups. They may also be a member of one or no departments.
- If a user is a member of more than one group, the groups should be listed as a comma-separated string and enclosed in double quotes. An example is given below:
  - user1,"group1,group2,group3",dept1
- If you want add only the username, then add two commas after the username. See example below:
  - user2,,
- If you add a non-existent group or department to the .csv, then the group/department will be auto-created in the interface. Click 'Administration' then 'Groups' or 'Departments' to view these items.

Import users from a CSV file

- Click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Users' tab
- Click 'Import' on the right



- Locate your .csv file and click 'Open'

All 'Users' will be imported and displayed in the list.

Sync via Active Directory

- Relevant if you chose 'Active Directory' as the method of user authentication.
- After installation and configuration, AD users and groups will be automatically added to Comodo SWG and will be visible under 'User Management'.

- The agent will automatically synchronize with AD every 3 hours.
- This method is explained in '**Active Directory**'

Create Policies

- Click 'Configuration' in the top-menu to open the policy configuration interface.
- Comodo SWG ships with default profiles for 'Security Policy', 'Web Content Policy' and 'Policy Time-Schedule'
- Default 'Global Policy' is applied to users / devices under trusted networks and roaming users / devices with SWG agent.
- You can create user-specific, endpoint-specific and network-specific policies.

Create a new policy

To create a policy, you first need to configure and save three components:

- **Security Policy**
- **Web Content Policy**
- **Policy Time-Schedule**

Once you have saved them:

- Click 'Policy' at the top of the left-hand menu.
- Click 'New Policy' on the right to start the policy creation wizard.

Before that, though, let's configure the security, web content policies and time-schedules.

Create a Security Policy

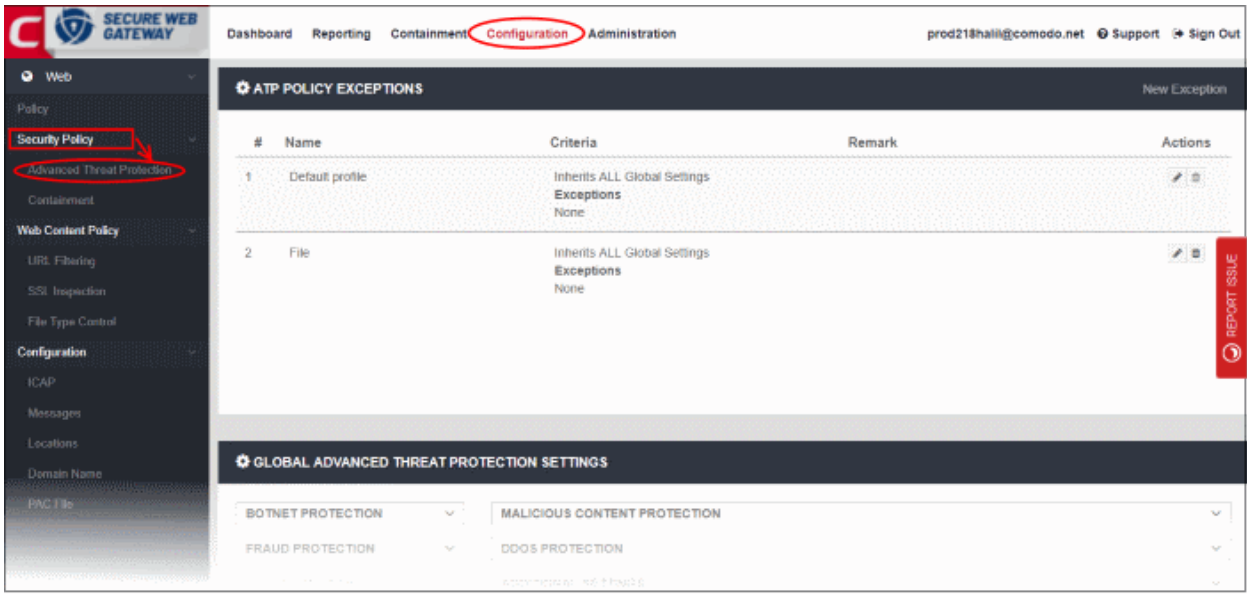
A security policy contains two elements:

- **Advanced Threat Protection**
- **Containment**

Advanced Threat Protection Settings

Click 'Configuration' > 'Security Policy' > 'Advanced Threat Protection' to open this interface.

- Global Advanced Threat Protection Settings (lower panel) - Configure overall protection settings, blocked files and blocked countries. These settings are automatically applied to ALL policies. If you make changes here they will be automatically implemented in all policies.
- APT Policy Exceptions (upper panel) - Lets you create a profile with blacklisted and whitelisted items. These will form exceptions to the settings in the 'Global Advanced...' section.
  - You can then add the exceptions profile to a policy. The final policy will implement the 'Global Advanced Threat...' settings minus the items in the exception profile.
  - If you do not want to specify any exceptions then simply use the 'Default Profile' in your policy.



The interface is divided into four sections:

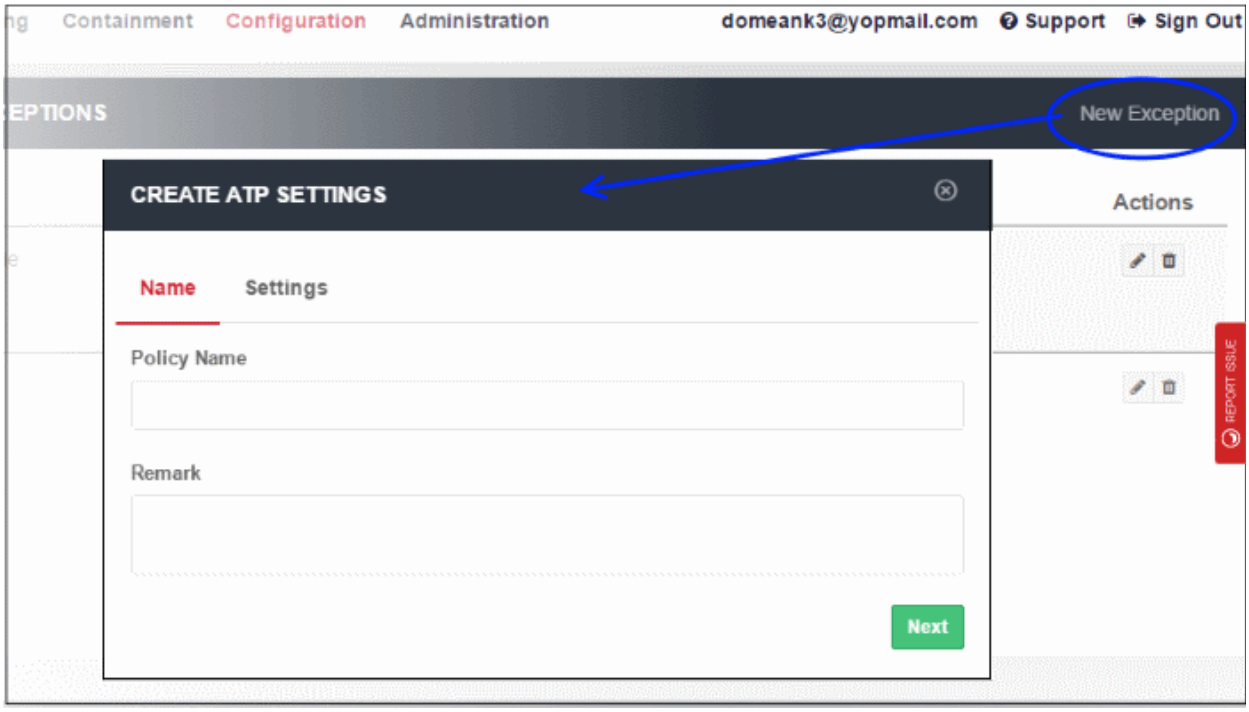
- **ATP Policy Exceptions**
- **Global Advanced Threat Protection Settings**
- **Global Blocked Files List**
- **Blocked Country List**

ATP Policy Exceptions

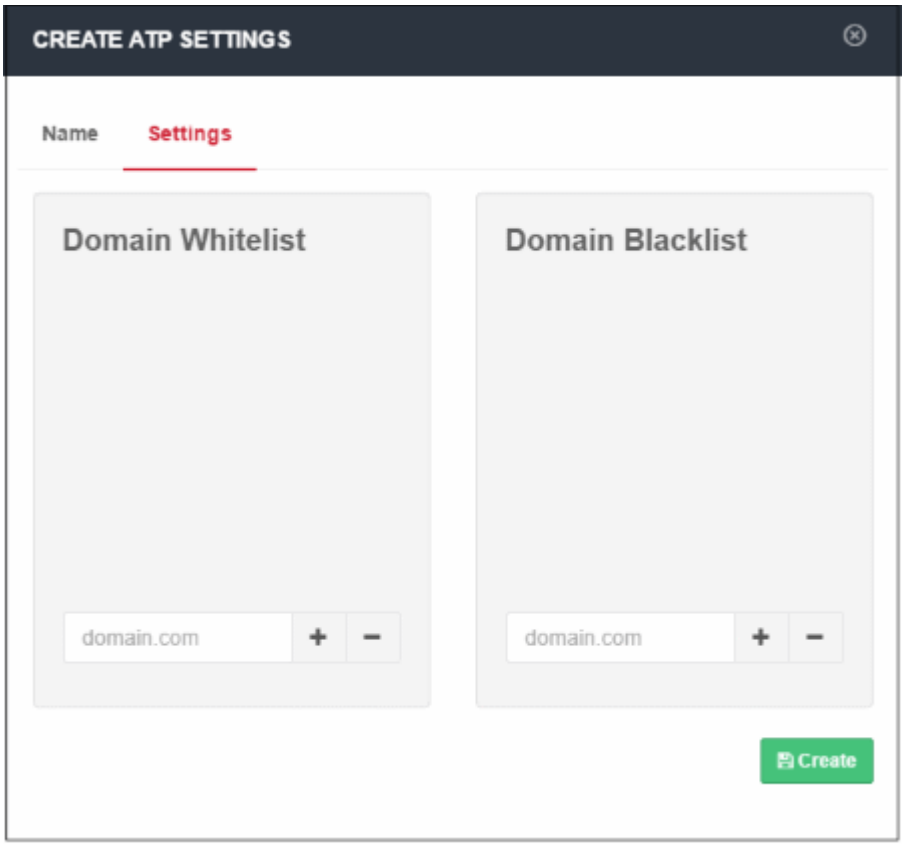
Allows you to specify domains will should ignored by the Advanced Threat Prevention system.

Add Policy Exceptions - Table of Column Descriptions	
Column Header	**Description**
Name	The label of the policy containing the exceptions.
Criteria	Specifics of the exception • 'Inherits All Global Settings' - The policy will enforce all settings configured in the 'Global Advanced Threat Protection Settings' in the lower-half of the interface, except... • Exceptions - Blacklisted items will always be blocked. Whitelisted items will always be allowed. These are regardless of settings in the lower pane.
Remark	Comments provided for the policy exception
Actions	You can edit and / or delete an exception. Please note that the default profile cannot be deleted but exceptions can be added.

To add a new ATP policy exception, click 'New Exception' at the top right.



- Policy Name - Enter a descriptive label for the ATP exception.
- Remark - Enter any comments you wish to add about the exception.
- Click 'Next' to proceed or 'Settings' if you wish to specify domain whitelist and blacklist.



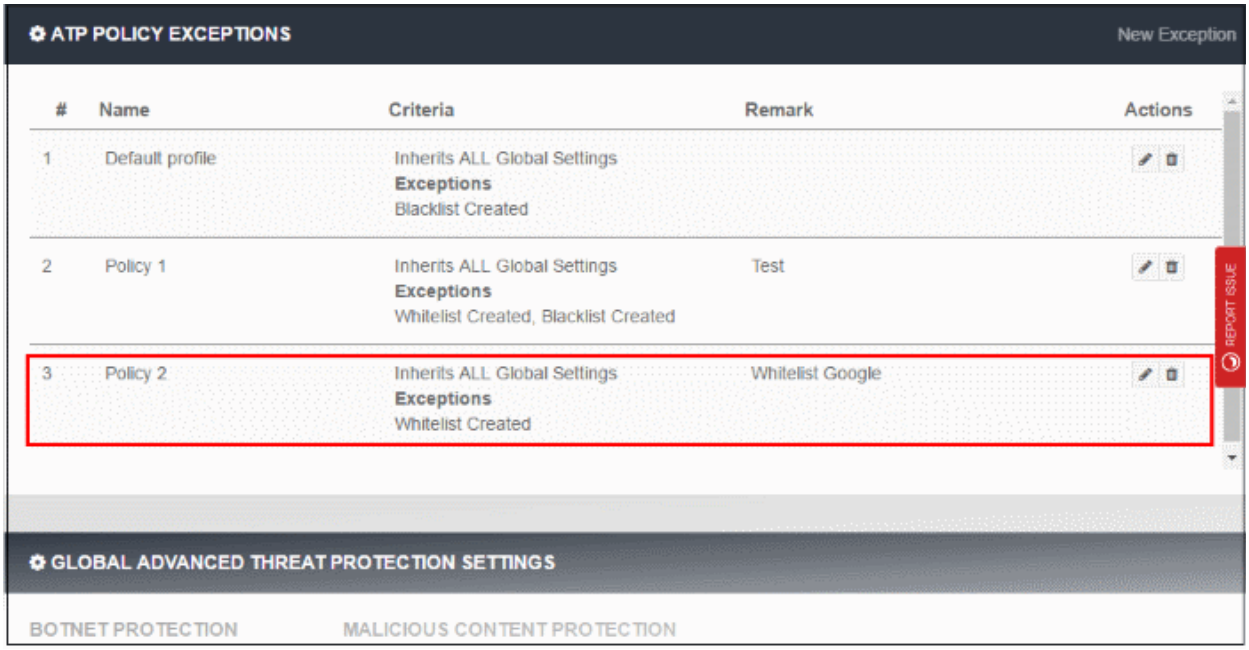
- Domain Whitelist - Domains that you want to exempt from SWG filtering rules. Please note this list takes priority over all other settings. All files downloaded from white-listed websites will be allowed, even those that are potentially malicious. Make sure the sites that are white-listed are safe. Click the '+' button after entering the domain name in the field. To remove a domain name, select it and click the '-'

button.

- Domain Blacklist - Domains from which users are banned from downloading files. Users are still allowed to visit blacklisted sites, but are not able to download files from them. The 'Blacklisted Domains' tile on the dashboard shows attempts to download files from blacklisted sites. Click the '+' button after entering the domain name in the field. To remove a domain name, select it and click the '-' button.

- Click 'Create'

The new ATP policy exception will be created and displayed on the list.

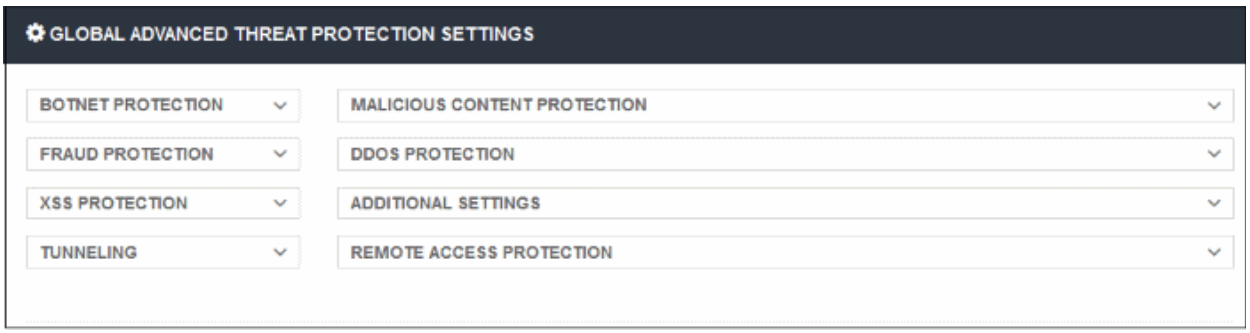


This new ATP policy will be available for selection when creating / editing a SWG policy. See **Apply Policies.**

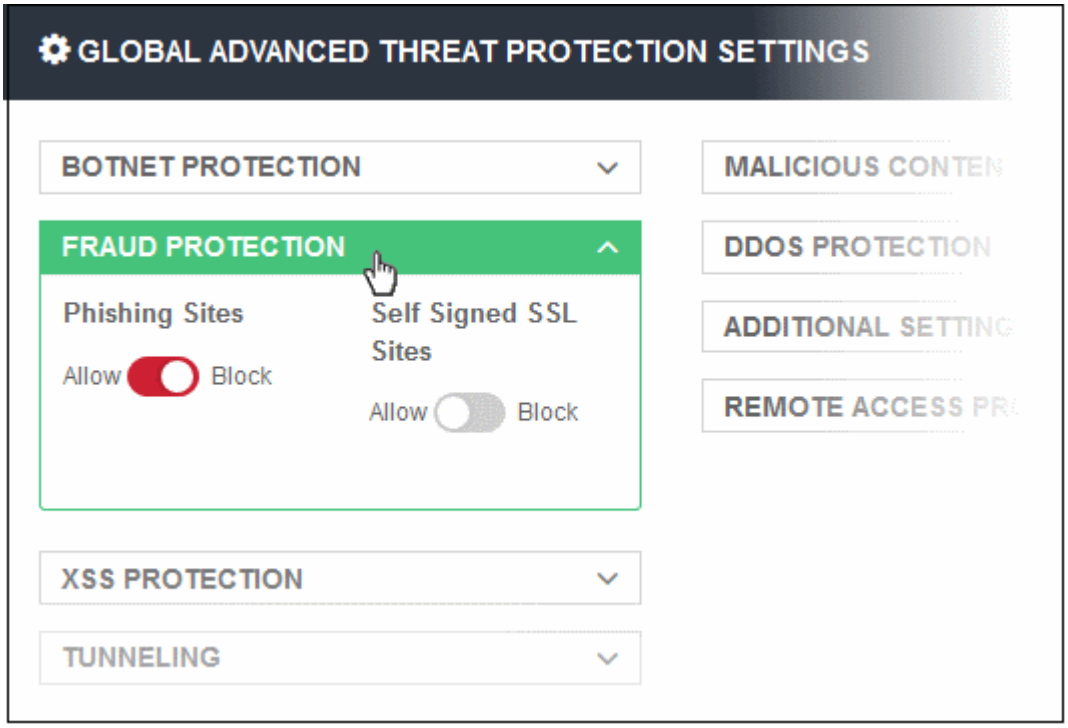
Global Advanced Threat Protection Settings

Displays the built-in protection settings. The available settings are:

- Botnet Protection - Command and Control Servers (C & C Servers)
- Malicious Content Protection - Malicious content sites, Malicious URLs, Browser exploits
- Fraud Protection - Phishing sites
- DDOS Protection - Distributed Denial of Service attacks
- XSS Protection - Cookie stealing
- Additional Settings - Password-protected archive files, Unscannable file types
- Tunneling - TOR nodes, P2P nodes and VPN servers
- Remote Access Protection - Remote access services and brute force / scanner



- Click on a protection type to expand the box and view all settings.
- Use the switches to enable or disable specific settings.

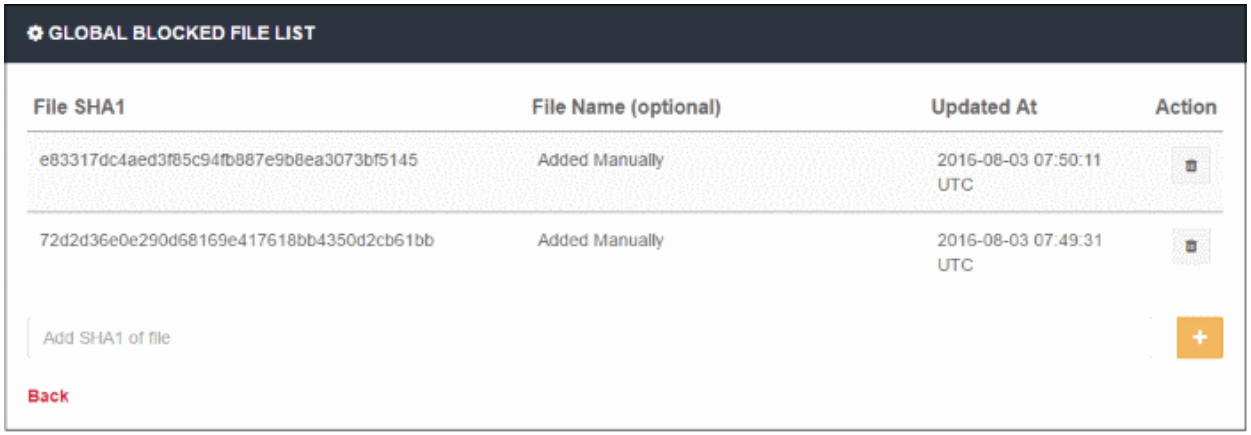


- The setting will be applied globally, to all protected domains and endpoints.
- You can create a policy with exceptions which you can to deploy to a particular network or endpoint. See '**ATP Policy Exceptions**' to find out how to add exceptions to the global settings.

Global Blocked Files List

Allows to upload SHA1 hash values of files that should be blocked globally on the enrolled networks while trying to download.

- Clicking on the link will open the 'Global Blocked File List' page from where you can upload the SHA1 hash values of the files that you want to be blocked from downloading.



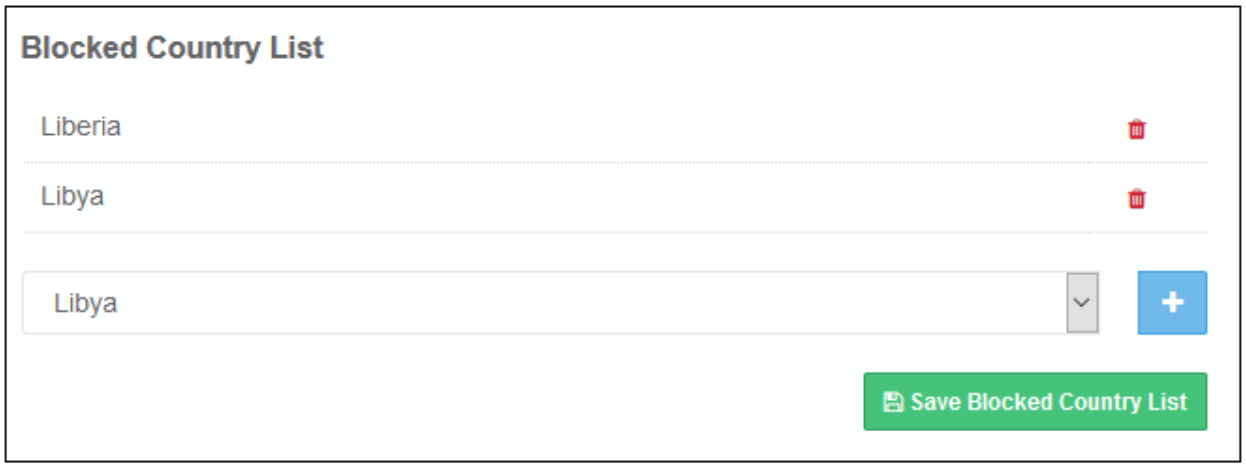
The list of SHA1 hash values already uploaded will be displayed.

- To upload hash value of a file, enter the value in the field and click the '+' button. The value will be added and displayed.
- To remove a hash value from the list, click the trash can icon beside it. Click' OK' in the confirmation screen to remove the SHA1 value.

- Click 'Back' to return to ATP settings interface.

Blocked Country List

Allows you to block websites that are hosted in specific countries. You can add multiples countries.



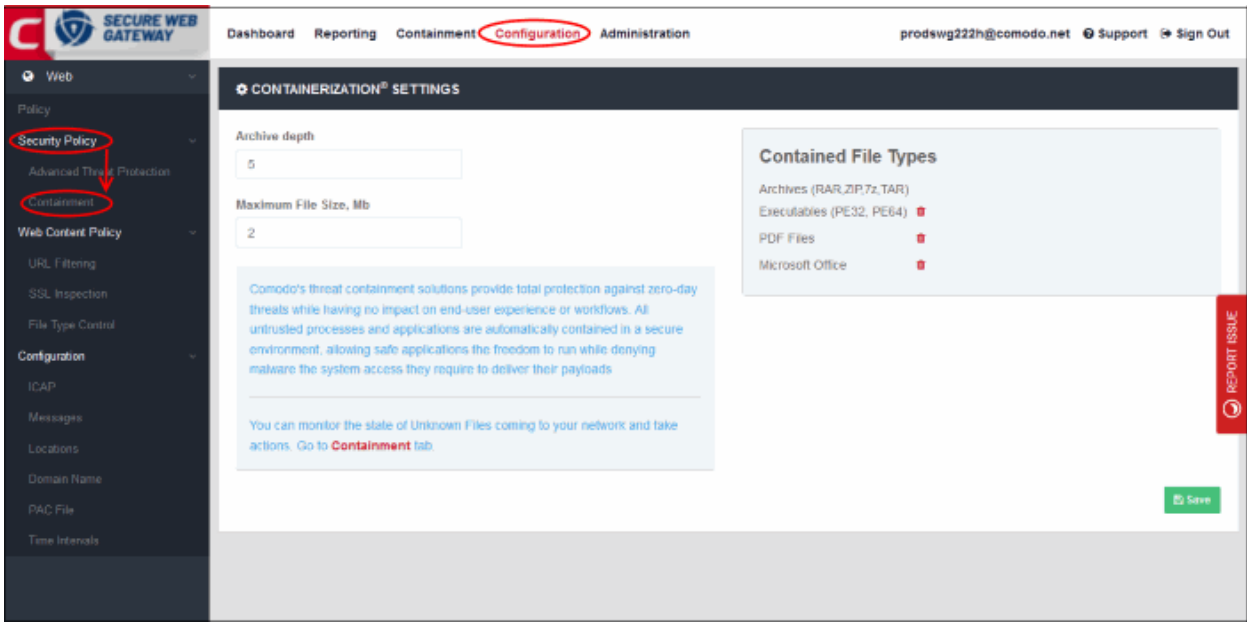
- Select the country from the drop-down and click the '+' button
- Click 'Save Blocked Country List' to save your changes

To remove a country from the list, click the trash can icon beside it.

Configure Containerization Settings

- Click 'Configuration' > 'Security Policy' > 'Containment', to open this interface.
- Containerization is a security technology whereby 'unknown' files are run inside a secure, virtual environment. This isolation prevents them from potentially attacking the endpoint or stealing data.
  - A file can have one of three trust ratings – 'safe', 'malicious' or 'unknown'. Safe files are allowed to run on the host, while malicious files are deleted or quarantined.
  - 'Unknown' files are those for which no trust rating exists in our database. They could not be classified as definitely safe, nor definitely malicious.
  - Unknown files are delivered to the endpoint wrapped in Comodo's containment technology. Contained files write to a virtual file-system, cannot modify other processes, and are denied access to the registry and user data.
- The 'Containerization Settings' interface lets you configure which file-extensions are run in the container. You can also specify the maximum number of nested archives that should be unpacked and checked.

Click 'Configuration > 'Security Policy' > 'Containment'



- Archive Depth - Maximum level the archive files will be unpacked to check for file within archive files. Enter the value till which the zip files will be checked. If the archive depth is more than the provided value, the files inside the exceeded layer will not be checked. For example, if the value is provided as 5, then files will be checked up to 5 layers only and others will be allowed to pass.
- Maximum File Size, MB - Enter the maximum file size that SWG should scan the archive files.
- Contained File Types - Displays the types of files that are scanned and sandboxed if required.
  - Archives - File types with extensions RAR, ZIP, 7z and TAR. This type cannot be deleted from the list.
  - Executables - Executable files of both 32 and 64 bit types inside the archive. You can remove this type by clicking the trash can icon beside it. If required, it can be added again by clicking the '+' button.
  - PDF Files - Files with PDF extension inside the archive will be scanned. You can remove this type by clicking the trash can icon beside it. If required, it can be added again by clicking the '+' button.
  - Microsoft Office - Files inside the archive with extensions of MS Office such as .doc, .xls and so on. You can remove this type by clicking the trash can icon beside it. If required, it can be added again by clicking the '+' button.
- Click the 'Save' button at the bottom.

The statuses of unknown files that are downloaded can be viewed in the 'Containment' interface. You can navigate to the page by clicking the 'Containment' tab at the top of the interface. See '**Unknown Threat Statistics**' for more details.

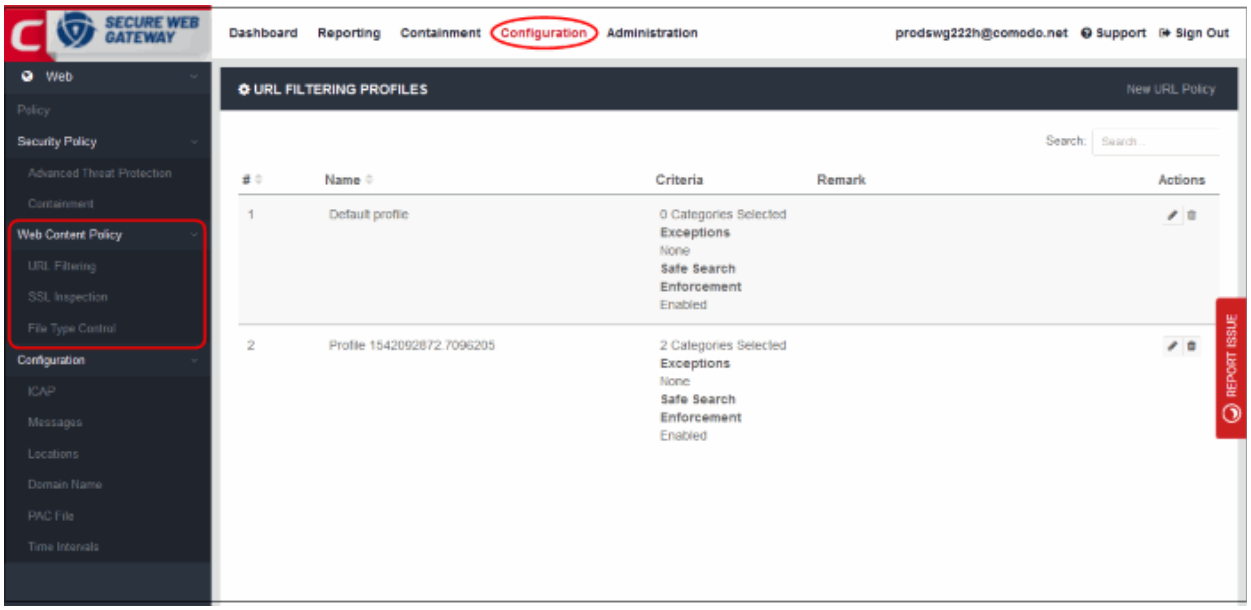
Create a Web Content Policy

There are three elements in a web content policy:

- **URL Filtering**
- **SSL Inspection**
- **File Type Control**

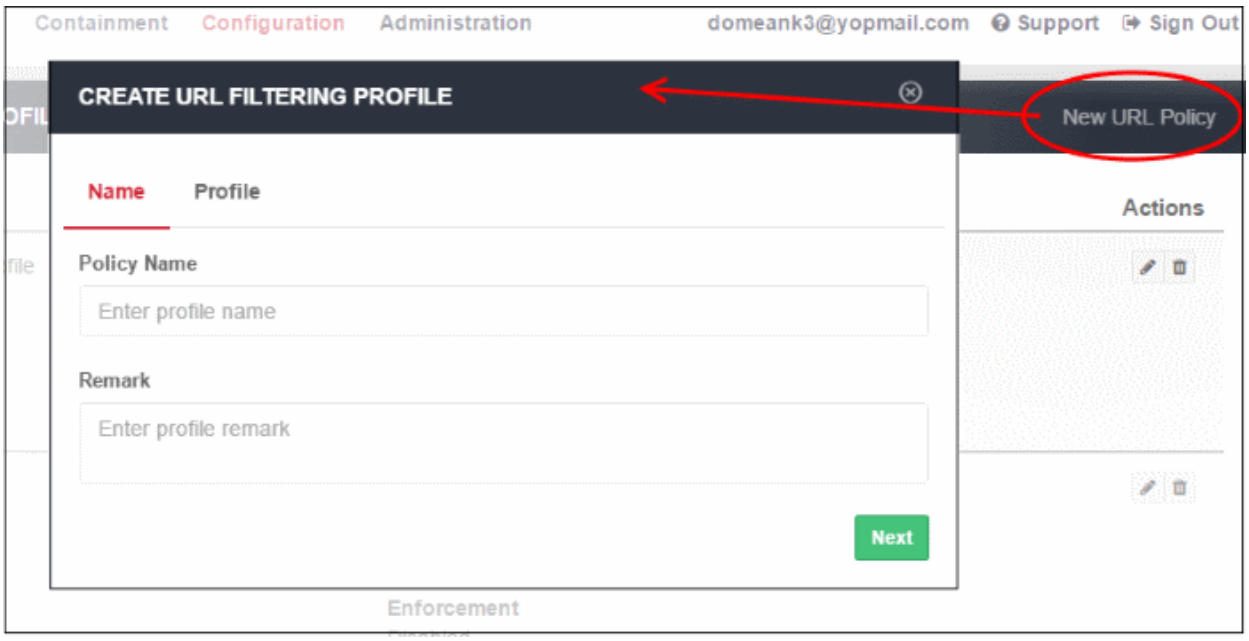
Create URL Filtering Policy

- Configure which categories of website should be allowed or blocked. You can also create your own domain whitelist or blacklist.
- Click 'Configuration' > 'Web Content Policy' > 'URL Filtering', to open this interface.

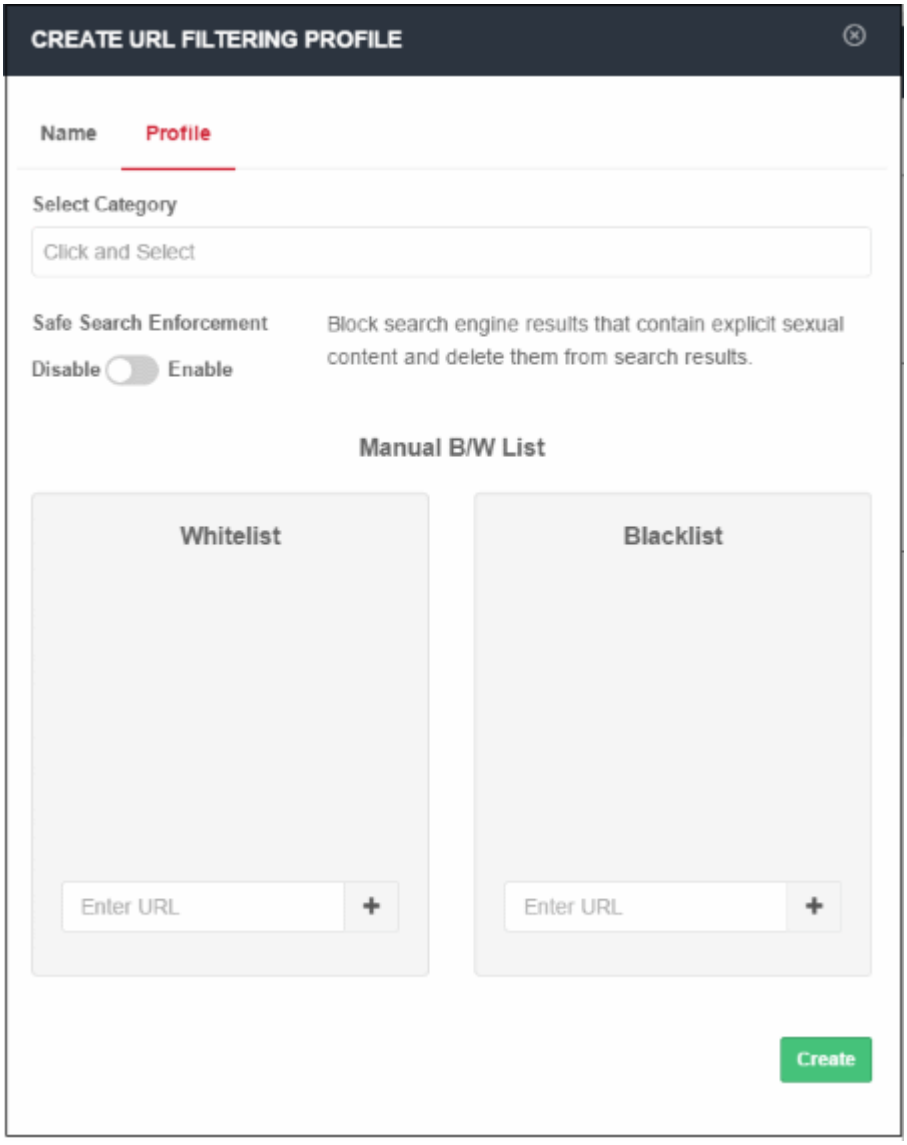


URL Filtering Profiles - Table of Column Descriptions	
Column Header	**Description**
Name	Label of the URL filtering profile. You can sort the profiles in alphabetical order by clicking on the column header.
Criteria	The number of categories included in the profile. Place your mouse anywhere in the criteria area to view the categories.
Remark	Comments for the profile
Actions	Edit or delete a profile

- Click 'New URL Policy' at the top right

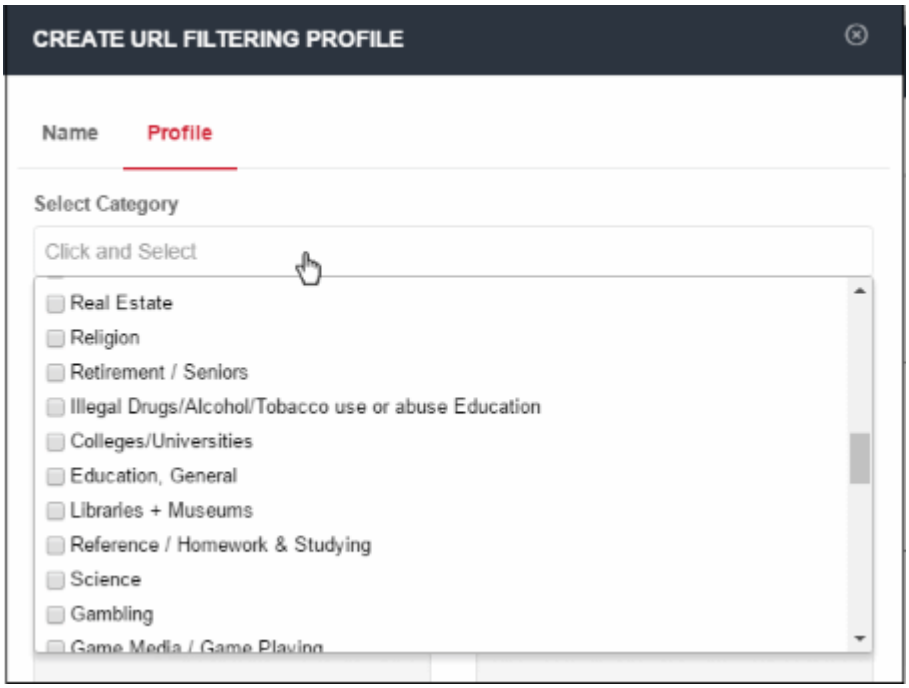


- Name:
  - Policy Name – Create a label for the URL filtering profile.
  - Remark – Add helpful comments about the profile.
- Click 'Next' or 'Profile' to specify categories:

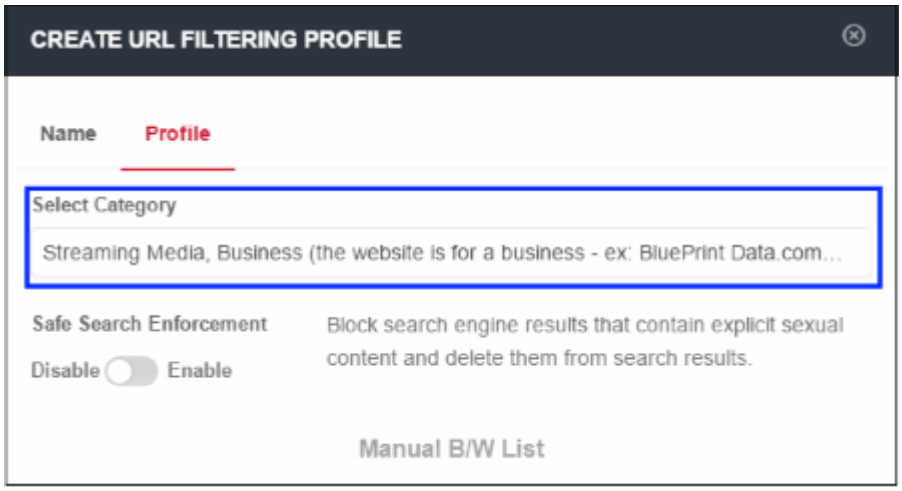


Category

- Website categories that can be allowed or blocked will be displayed in the 'Select Category' drop-down.



- You can select multiple categories at the same time. 'Select all' allows you to include all available categories. Please review and deselect any categories you wish to allow.
- All selected categories will be blocked. Website categories that are not selected will be allowed.
- Click anywhere outside the drop-down to add your selected categories.



- You can choose to add exclusions to a category. See **Manual B / W List** for more details.

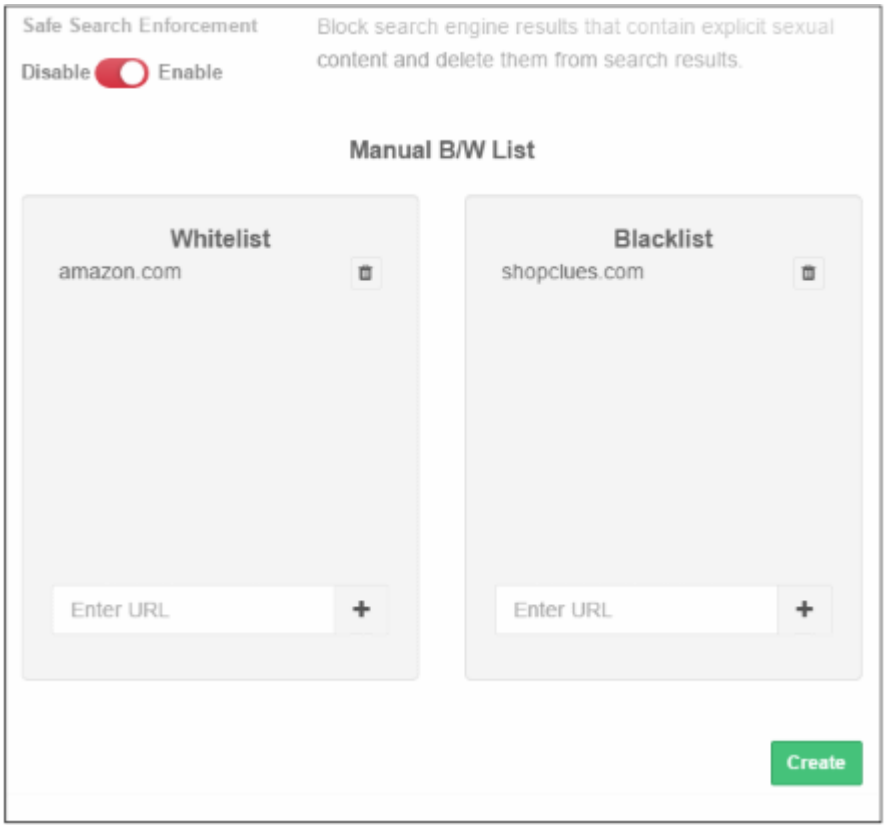
Safe Search Enforcement

Allows you to configure so as to block and delete inappropriate search engine results such as results that contain explicit sexual content.

- Click on the toggle button to enable or disable safe search enforcement feature.

Manual B / W List

- This section lets you add exceptions to the URL filtering categories that were defined above.
- For example, if you block 'Shopping websites' but add amazon.com to the whitelist, then amazon.com is allowed but all other shopping sites are blocked.
- Similarly, any website you add to the blacklist will be blocked even if it belongs to an allowed category.
- The B /W list defined here is different from the one done in ATP under security policy. The Security Policy B/W list allows the user to visit the blacklisted websites but prevents them from downloading any files. See '**ATP Policy Exceptions**'.



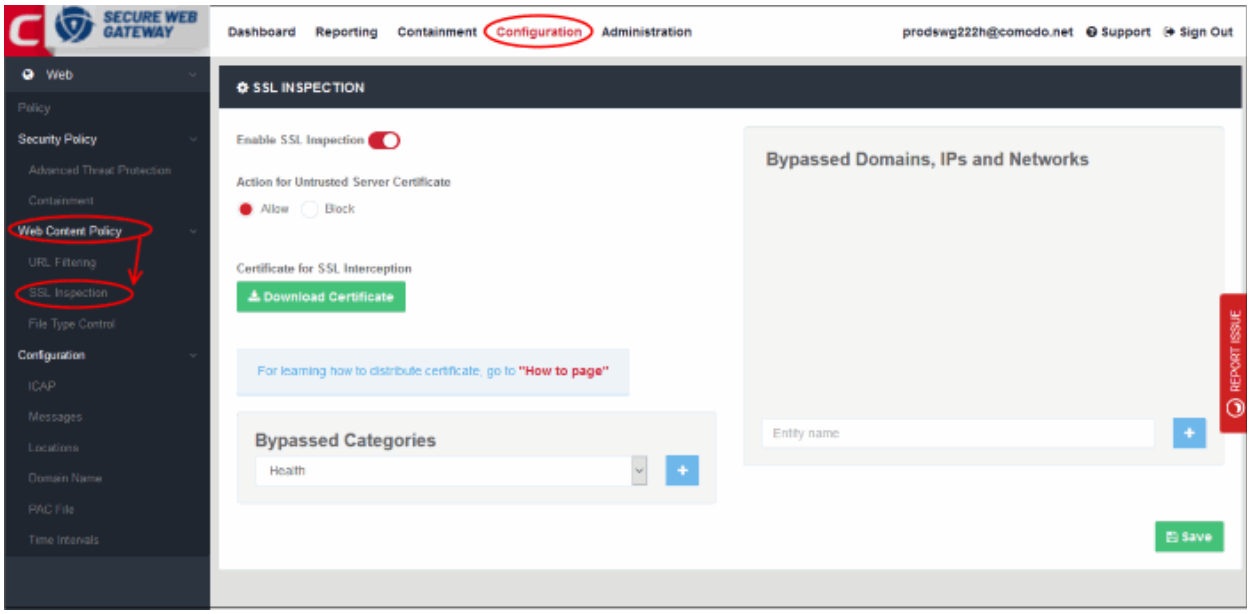
  - Whitelist - Add domains that you want to exempt from Comodo SWG URL filtering rules. Please note the list here takes priority over the category setting. Make sure the sites that are whitelisted are safe. Click the '+' button after entering the domain name in the field. To remove a domain name, click the trash can icon beside it.
  - Blacklist - Specify domains that should be blocked even if it belongs to an allowed category. Click the '+' button after entering the domain name in the field. To remove a domain name, click the trash can icon beside it.
- Click 'Create'

The URL filtering policy will be added and will be available for selection while creating / editing a policy. See '**Apply Policies**'.

Configure SSL Inspection Settings

- Specify whether Comodo SWG should check if websites use an SSL certificate from a trusted CA. You can then choose whether to allow or block sites that use an untrusted certificate.
- Download and install the Comodo SWG certificate. This is required if you want SWG to decrypt, analyze and apply policies to content served by https websites. The certificate should be installed on users' browsers or deployed to networks via Group Policy Object (GPO).

- Create exceptions to allow trusted domains, IPs and networks
- Click 'Configuration' > 'Web Content Policy' > 'SSL Inspection', to open this interface.



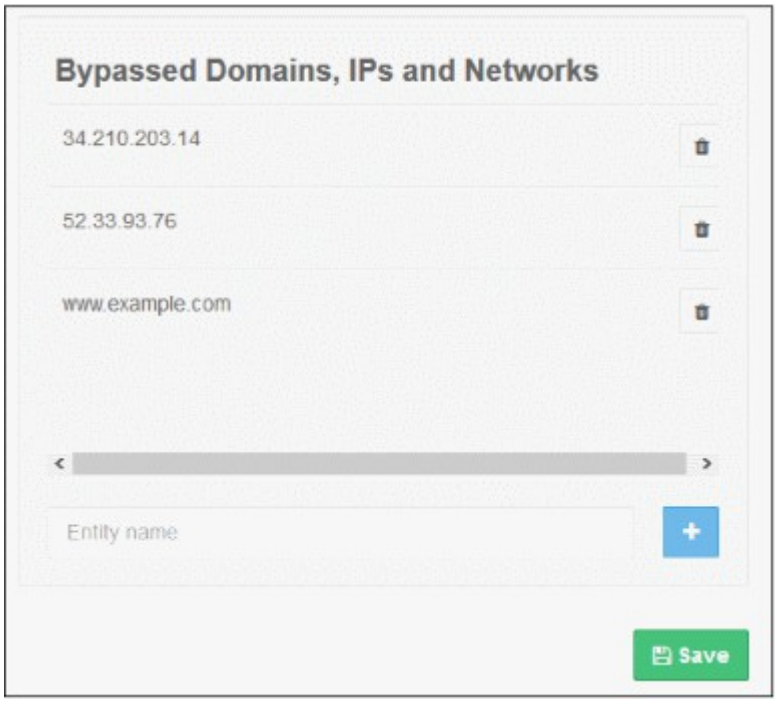
Enable SSL Inspection

- SSL inspection checks whether a website uses a certificate from a trusted certificate authority (CA).
- Choose whether you want to allow or block sites which use an untrusted certificate - one that is not from a trusted CA.
- You must enable this for SWG to monitor HTTPS traffic and apply relevant policies. See '**Certificate for SSL Interception**' for help to install the SWG SSL certificate.
- Click 'Save' for your changes to the page to take effect.

Bypassed Domains

Add domains, IPs and networks whose certificates will be not checked by Comodo SWG.

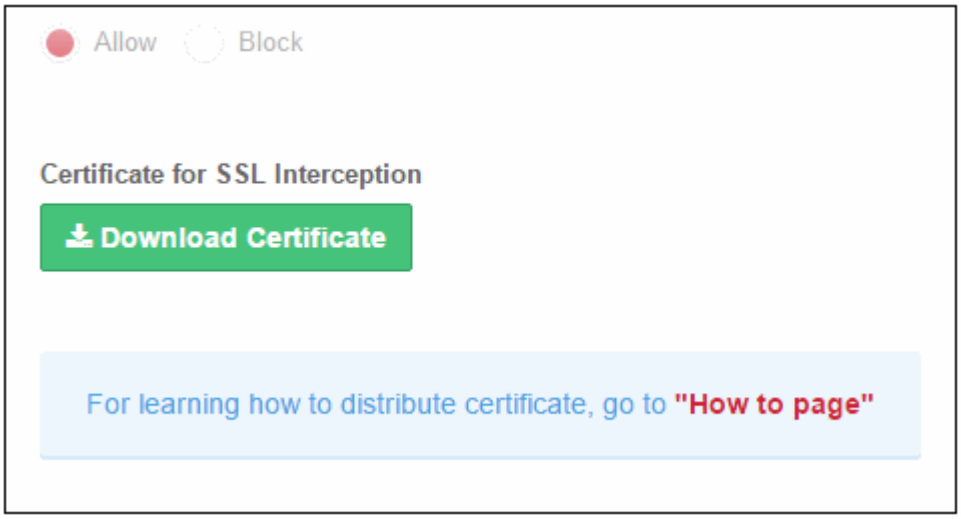
- Enter the URL of a website, domain, domain name with wildcard, IP or network in CIDR format in the field and click the '+' button. Repeat the process to add more exceptions.



- To remove a website from the list, click the trash can icon beside it.
- Click 'Save' for your changes to the page to take effect.

Certificate for SSL Interception

- You have to download and install the Comodo SWG certificate in order to decrypt and apply policy to HTTPS websites.
- Once the certificate is installed, Comodo SWG can apply all rules to HTTPS sites as it does for non-secure sites.
- Make sure 'Enable SSL Inspection' is on.
- Click the 'Download Certificate' button. You can also download the certificate from 'Administration' > 'How to Configure' > 'SSL Interceptions' > 'Download Node Certificate'.



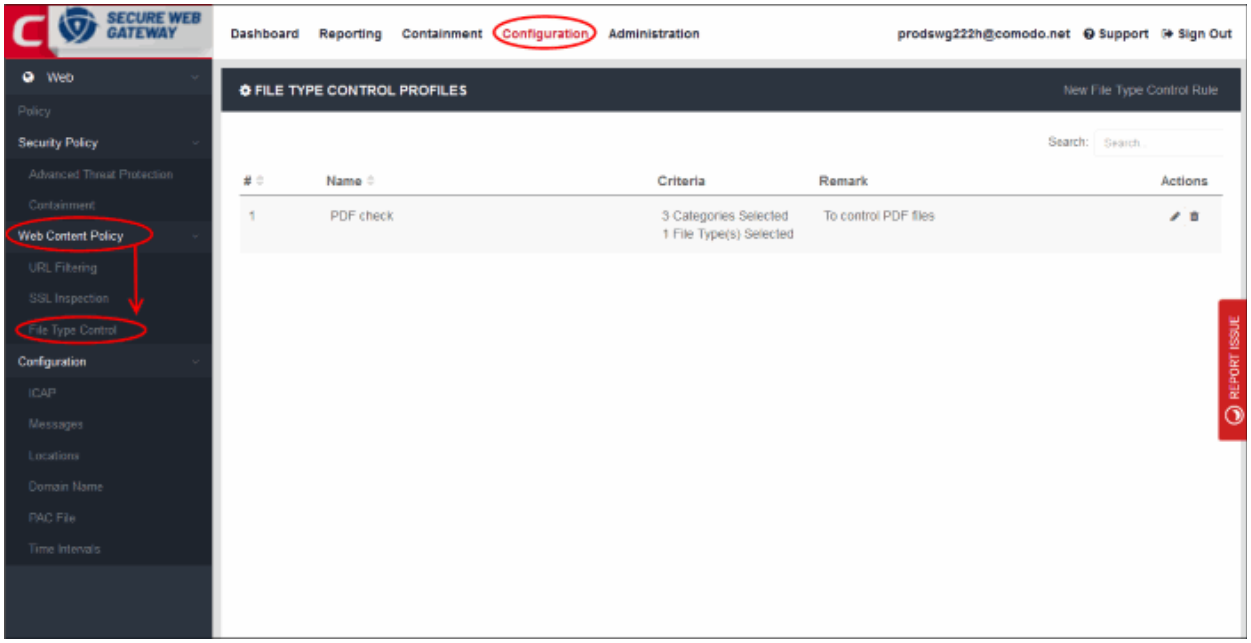
- Installation - click the 'How to page' link and follow the instructions in the 'SSL Interception' tab.
- Note – You can generate a new Comodo SWG certificate or upload your own certificate for HTTPS traffic monitoring.
  - Go to 'Administration' > 'How to Configure' > 'SSL Interceptions' tab
    - Click 'Generate Certificate' under 'Generate Node Certificate' – This will replace the current SSL certificate in the node.
    - Upload Combined PEM File – To use your own SSL certificate, click 'Browse...' , select the certificate then click 'Upload'.
    - Click 'Download Certificate' and to install the certificate follow the instructions under 'Browsers' / 'Windows Group Policy'

Bypassed Categories

The list of bypassed categories is provided by Comodo. Sites in bypassed categories are not subject to Comodo SWG filters and can be freely accessed by end-users. Please contact us at **domesupport@comodo.com** if you want to add or remove categories from the list.

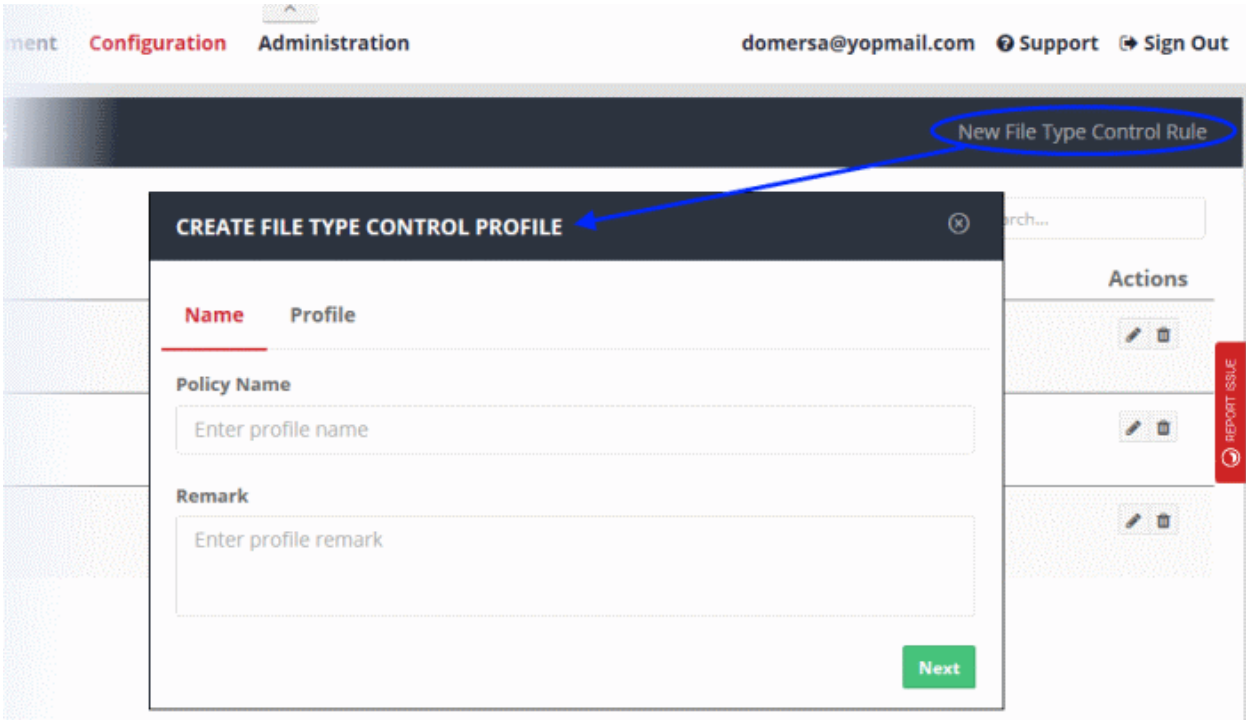
Create File Type Control Rule

- Click 'Configuration' > 'Web Content Policy' > 'File Type Control' to open this interface.
- File type control lets you block the download of certain file types from specific website categories.
- Example. If you select 'ZIP' as the file type and 'Gambling' as the category, then .zip files cannot be downloaded from any site in the gambling category.

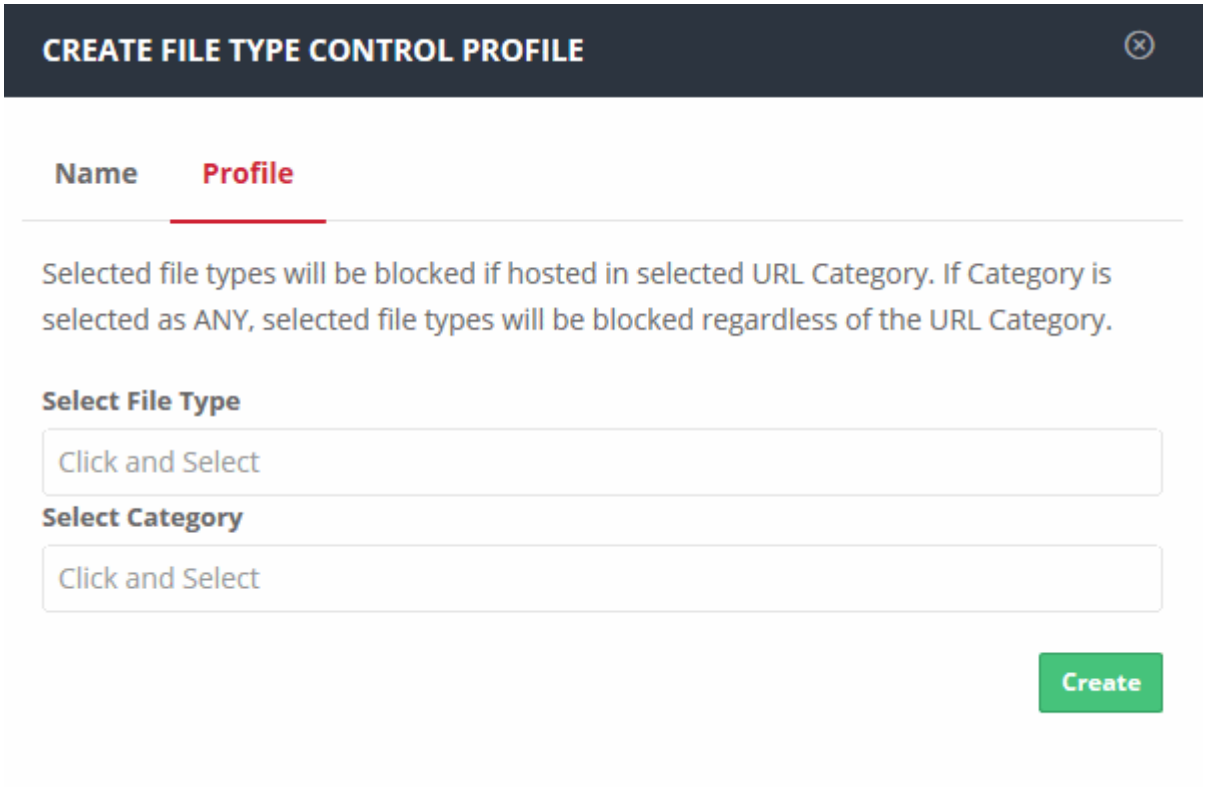


File Type Control Profiles - Table of Column Descriptions	
Column Header	**Description**
#	Rule number.
Name	Label of the file control profile. You can sort the profiles in alphabetical order by clicking on the column header.
Criteria	Displays the number of file types selected for the profile and the website categories selected. Place your mouse cursor over 'Categories Selected' to view individual categories and file types.
Remark	Comments for the profile.
Actions	Edit or delete a profile.

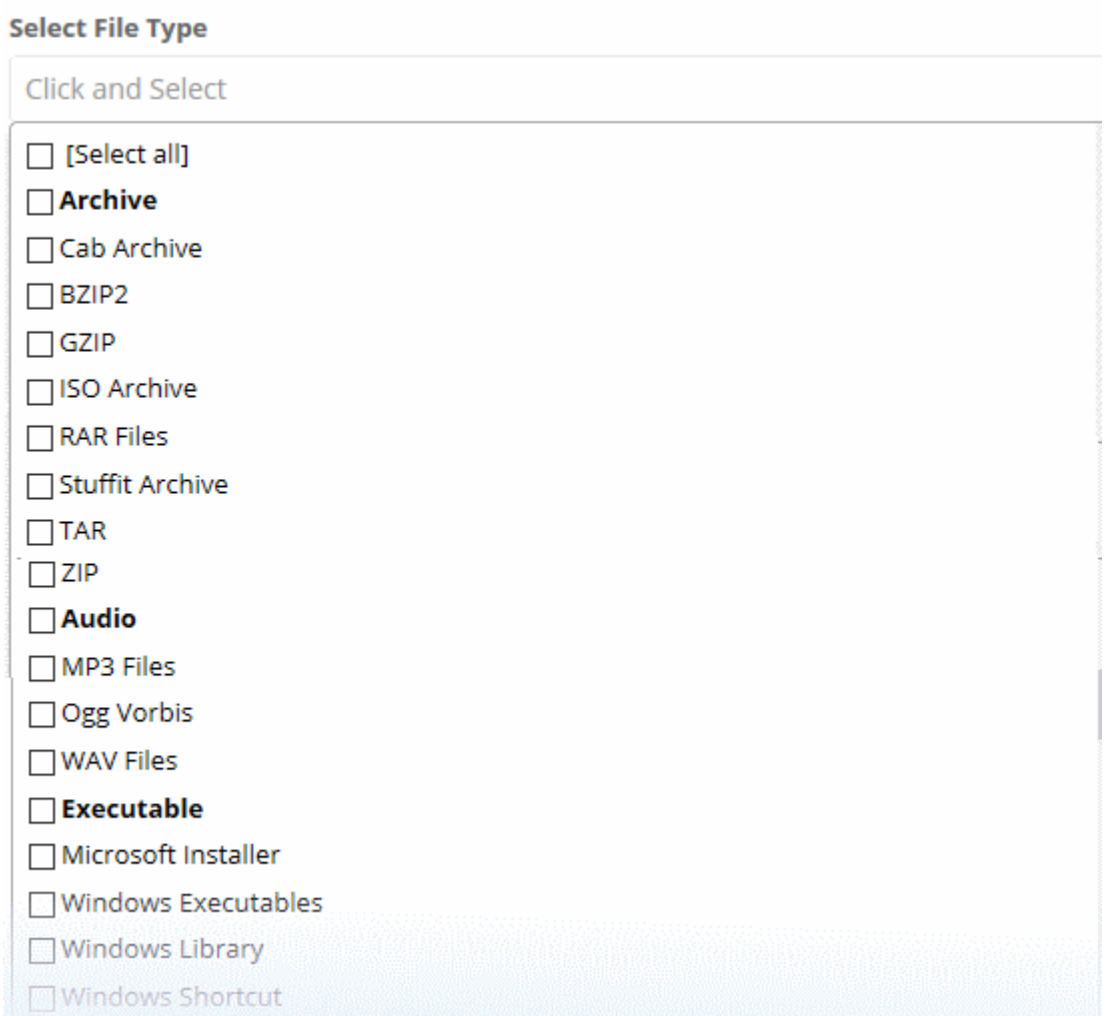
- Click 'New File Type Control Rule' at type right



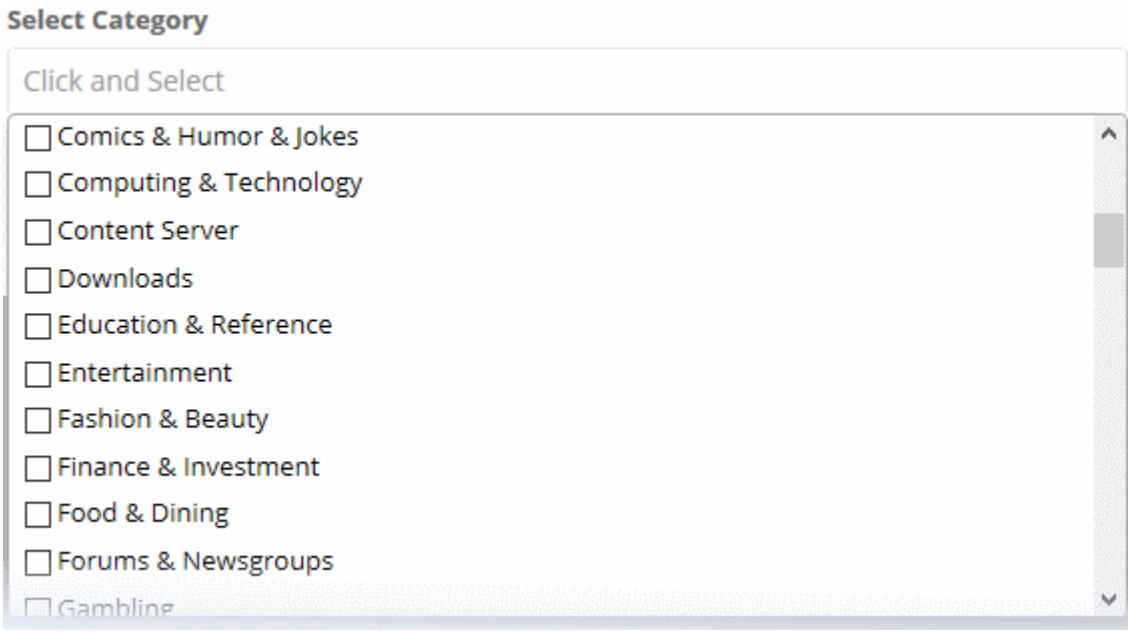
- Name:
  - Policy Name – Create a label to identify the policy.
  - Remark – Add comments to describe the policy.
- Click 'Next' or 'Profile' to specify file types and categories:



- Select the file formats you want to restrict from the available list in the 'Select File Type' field



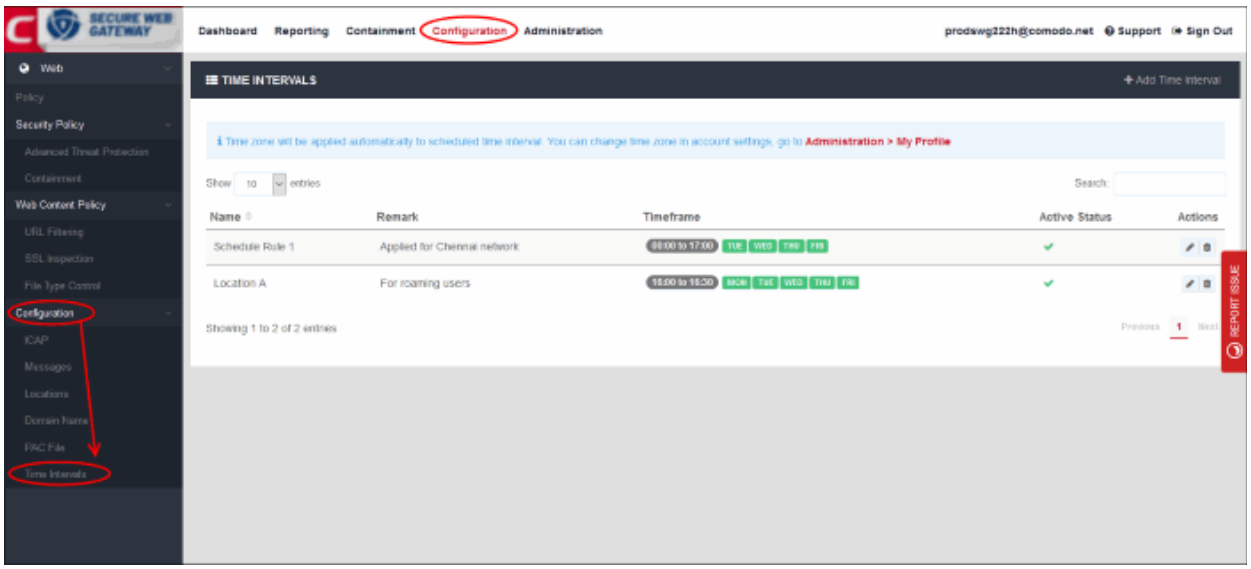
- Select the category of websites from where you want to the selected file types to be blocked.



- Click 'Create'

Create a Policy Time-Schedule

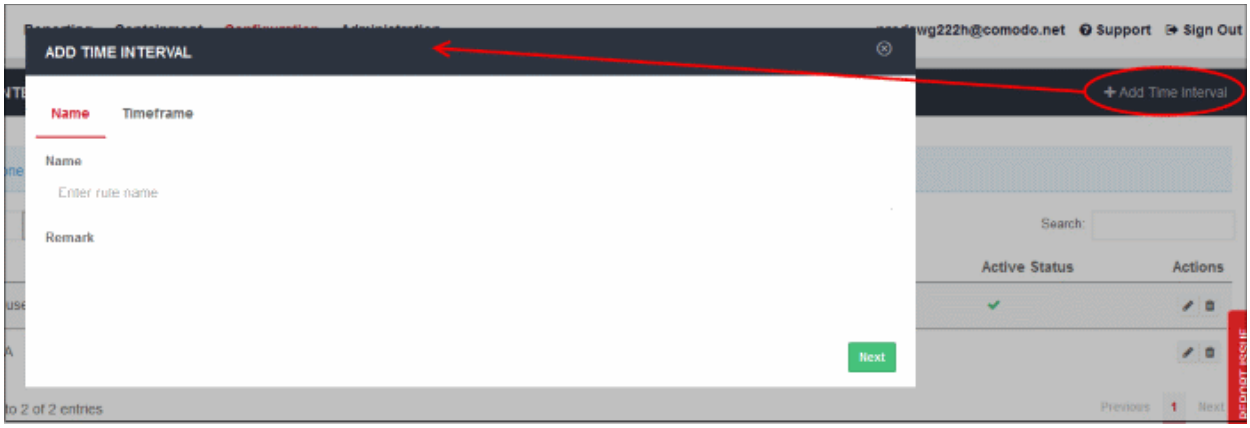
- Click 'Configuration' > 'Configuration' > 'Time Intervals'
- You can configure Comodo SWG to activate a policy only at specific times. This interface lets you create the schedules which you then add to a policy.
- The time zone used is as set in '**Administration**' > '**My Profile**'



Time Intervals - Table of Column Descriptions	
Column Header	**Description**
Name	Schedule label.
Remark	Short description of the schedule.
Timeframe	Shows the times when a policy is active under this schedule.

Active Status	Shows whether or not the schedule is currently active. This status also applies to any policies which use the schedule. For example, a schedule of 16:00 to 16:30 will show inactive if you view the screen outside this time-frame.
Actions	Edit or delete a schedule.

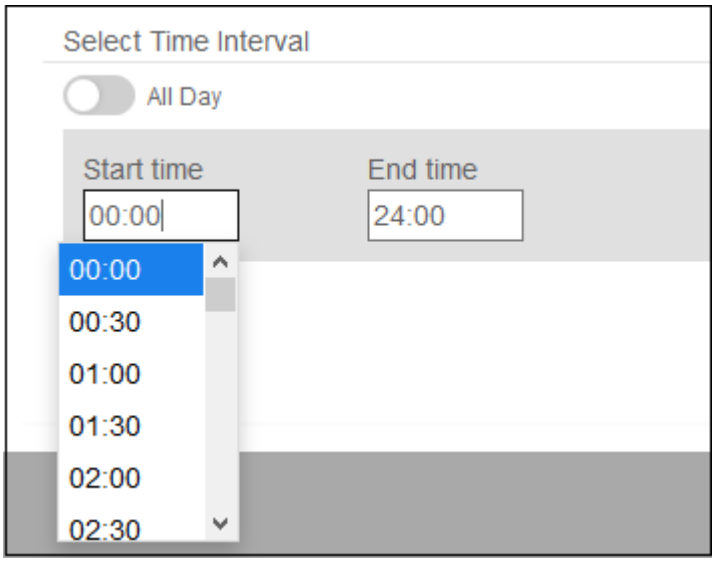
Create a new time schedule



- Name – Enter an appropriate label for the schedule
- Remark – Enter a short description for the schedule
- Click 'Next' or 'Timeframe' to pick the times that the schedule should apply

'Saturday' and 'Sunday' are disabled by default. The default interval is 'All Day'.

- Select Days – Click the days that you want the schedule to be active
- Select Time Interval:
  - All Day – The schedule will be active 24 hrs for the scheduled days
  - To configure a particular time period, switch 'All Day' to disable it and select the period



- Select the time period from the 'Start time' and 'End time' drop-downs. The schedule will be active for the configured period for the scheduled days.

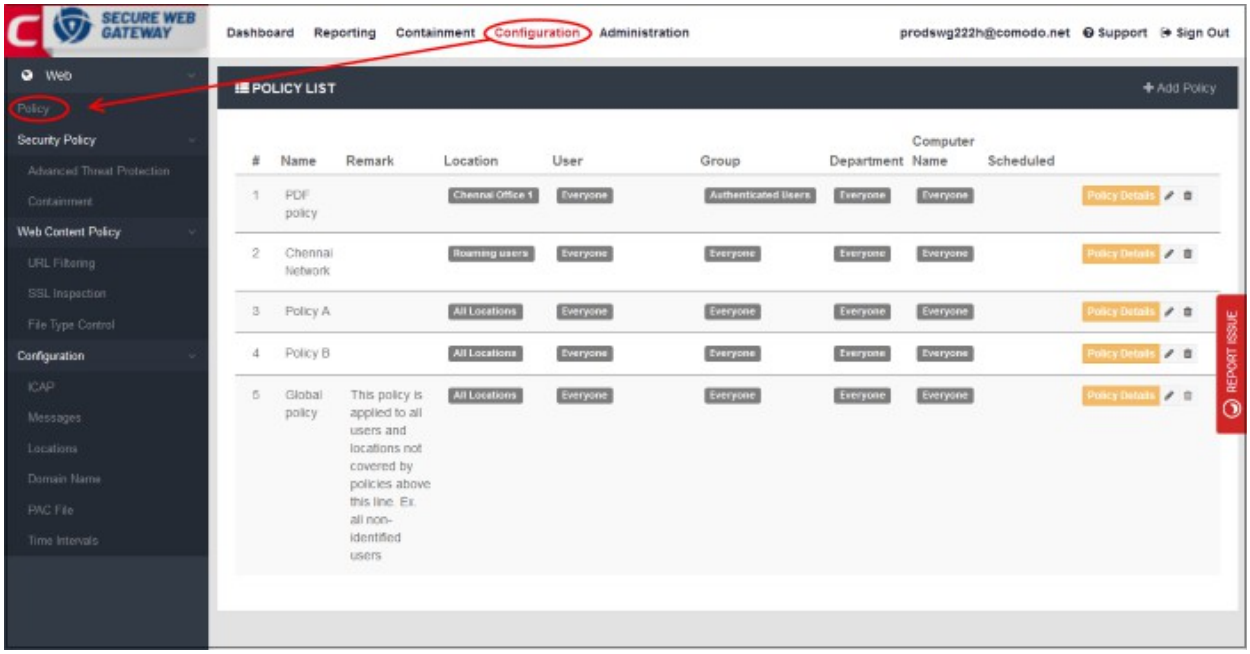
- Click 'Create' when done.

The time-schedules will be added to the list and will be available for selection when creating a policy.

The next step is to apply policies to networks / users. See **Apply Policies**.

Apply Policies

- After enrolling networks, the default global policy will be automatically applied to end users in your networks.
- You can configure new policies and deploy them to your networks as required. You can tailor polices and schedule them to specific users, groups, departments and computers.
- Click 'Configuration' > 'Policy' to open the policy list.
- This screen allows you to create new policies and view/edit existing policies.



Policy List - Table of Column Descriptions	
Column Header	**Description**
#	The priority of the policy. The policy that is nearer the top of the list will be implemented on matching objects. Tip – Put user/location specific policies above 'catch-all' policies like 'All locations', 'Everyone', 'All computers' etc. You want to make sure the targeted policy does not get over-ruled.
Name	Label of the policy. The default 'Global Policy' cannot be deleted. This policy contains the default Security Policy and Web Content Policy.
Remark	Comments provided for the policy.
User	The name of the user that is applied the policy.
Location	The name of the network location to which the policy is applied.
Group	The name of the group to which the policy is applied.
Department	The name of the department to which the policy is applied.
Computer Name	The name of the computer to which the policy is applied. Note – This will be available only if 'Hosted DB' is selected as **user authentication method**.
Scheduled	Check mark - The policy is active only at specific times. Blank - The policy is active at all times.
Policy Details	Click to view policy rule settings. These include security rules, web content control rules and any schedules.
Control buttons 	• Click the pencil icon to update a policy • Click the trash can icon to remove a policy

How policy deployment works

- Comodo SWG applies policy after analyzing the connection used by a device.
- It uses five criteria, or 'Objects', to determine whether it should apply a particular policy to a device. These are 'Location', 'User', 'Group', 'Department' and 'Computer Name'. If a connection matches all five objects then Comodo SWG will apply the policy. SWG also checks if the policy is scheduled for specific days / time-period and applies it appropriately.
- Note – 'Computer Name' object will be available only if 'Hosted DB' is selected as **user authentication method**.
  - Comodo SWG ships with a default 'Global Policy' that is applied to all connections. Its objects are set as 'Location' = 'All', 'Users' = 'Everyone', 'Group' = 'Everyone', 'Department' = 'Everyone' , 'Computer Name' = 'Everyone', 'Scheduled' = "Always'
  - You cannot modify the objects in the global policy as it is intended to be a catch-all if no other policy has been set. However, you can modify the settings that it implements (the 'Security' and 'Web Content' components).
- You can add as many new policies as you want for specific locations, users, groups, departments and computers.
- Policies are prioritized according to their rank the in the policy list ('Configuration' > 'Policy').
  - The first policy from the top that matches all five objects for a connection will be applied. You can change the priority of a policy by clicking 'Edit' > 'Policy Order'.

- Note - The first policy with a schedule that matches all five objects will be applied during the scheduled times. During non-scheduled times, SWG will move down the policy list and apply the next matching policy. Make sure to place a scheduled policy above 'Always on' policies.
- The 'Global Policy' is always last in the list. If a device is not covered by any custom policy then the global policy will be implemented.

- To deploy policies by 'Computer Name', you must install the SWG agent on the endpoints.
- To protect a device that is outside a trusted network, you must install the SWG agent on the device.
  - If you want to create a specific policy for outside devices then you must set the 'Location' object as 'Roaming Users'. You can then set the 'Users', 'Group' , 'Department' and 'Computer Name' objects as required.
  - FYI – 'All Locations' also covers 'Roaming Users' (if you want a policy to apply to both internal and external connection types).

Examples

a) A policy that apples to a single user, regardless of location:
- Location = All locations
- Users = < User Name >
- Group = Everyone
- Department = Everyone
- Computer Name = Everyone
- Scheduled = Always

b) A policy that only applies to members of a group, regardless of location:
- Location = All locations
- Users = Everyone
- Group = < Group Name >
- Department = Everyone
- Computer Name = Everyone
- Scheduled = Always

c) A policy that applies to any user connecting from outside the network:
- Location = Roaming Users
- Users = Everyone
- Group = Everyone
- Department = Everyone
- Computer Name = Everyone
- Scheduled = Always

d) A policy that applies to a specific endpoint, regardless of other objects
- Location = All locations
- Users = Everyone
- Group = Everyone
- Department = Everyone
- Computer Name = < Computer Name > Note: The SWG agent should be installed on endpoints to deploy policies by computer names.
- Scheduled = Always

e) A policy that only applies to members of a group on specific days / time-period regardless of location
- Location = All locations
- Users = Everyone

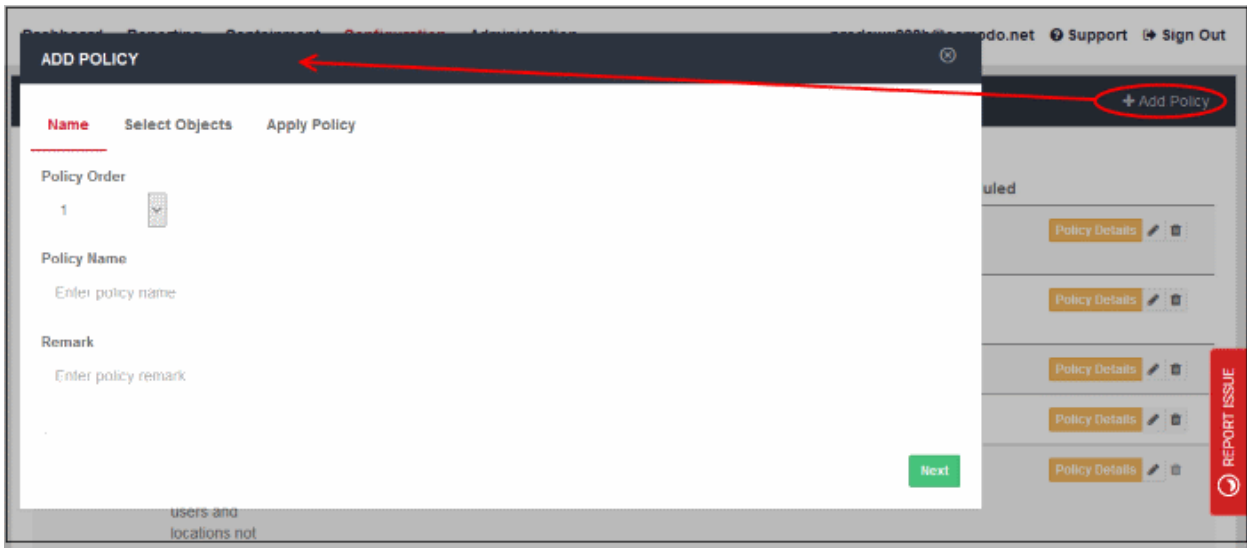
- Group = < Group Name >
- Department = Everyone
- Computer Name = Everyone
- Scheduled = <Time frame>

Tip

- Give policies which target a specific audience a higher rank than policies which cover large user bases. This is to ensure your targeted policies are not over-ruled by the policy above it. The 'All locations' and 'All Users' settings will over-rule every corresponding object below them if the policy has a high rank.

Add a new policy

- Click 'Add Policy' at top-right. The 'Add Policy' dialog will be displayed.



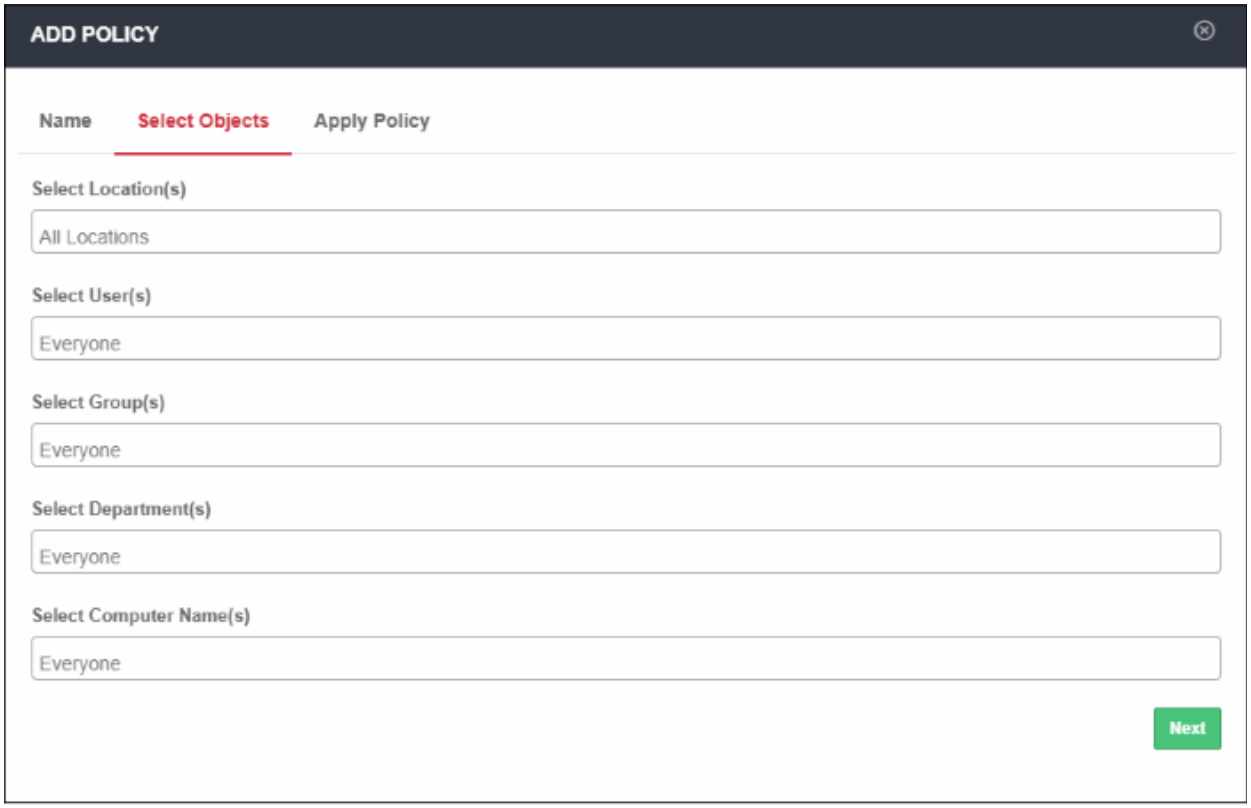
Step 1 - Policy Details

- Policy Order - Select where the rule has to be placed.
  - The drop-down will display the number of rules that are currently available.
  - Policies are prioritized according to their rank in the the policy list.
  - The first policy from the top that matches all the five objects defined in step 2 for a connection will be applied.
  - If you select '1', then the policy will be placed at the top of the list.
- Name - Create a label for the policy.
- Remark - Enter appropriate comments for the policy.

Click 'Next' or 'Select Objects' at the top to process further.

Step 2 - Define Objects

In the 'Select Objects' section, you can specify the object(s) for which you want to apply the policy.

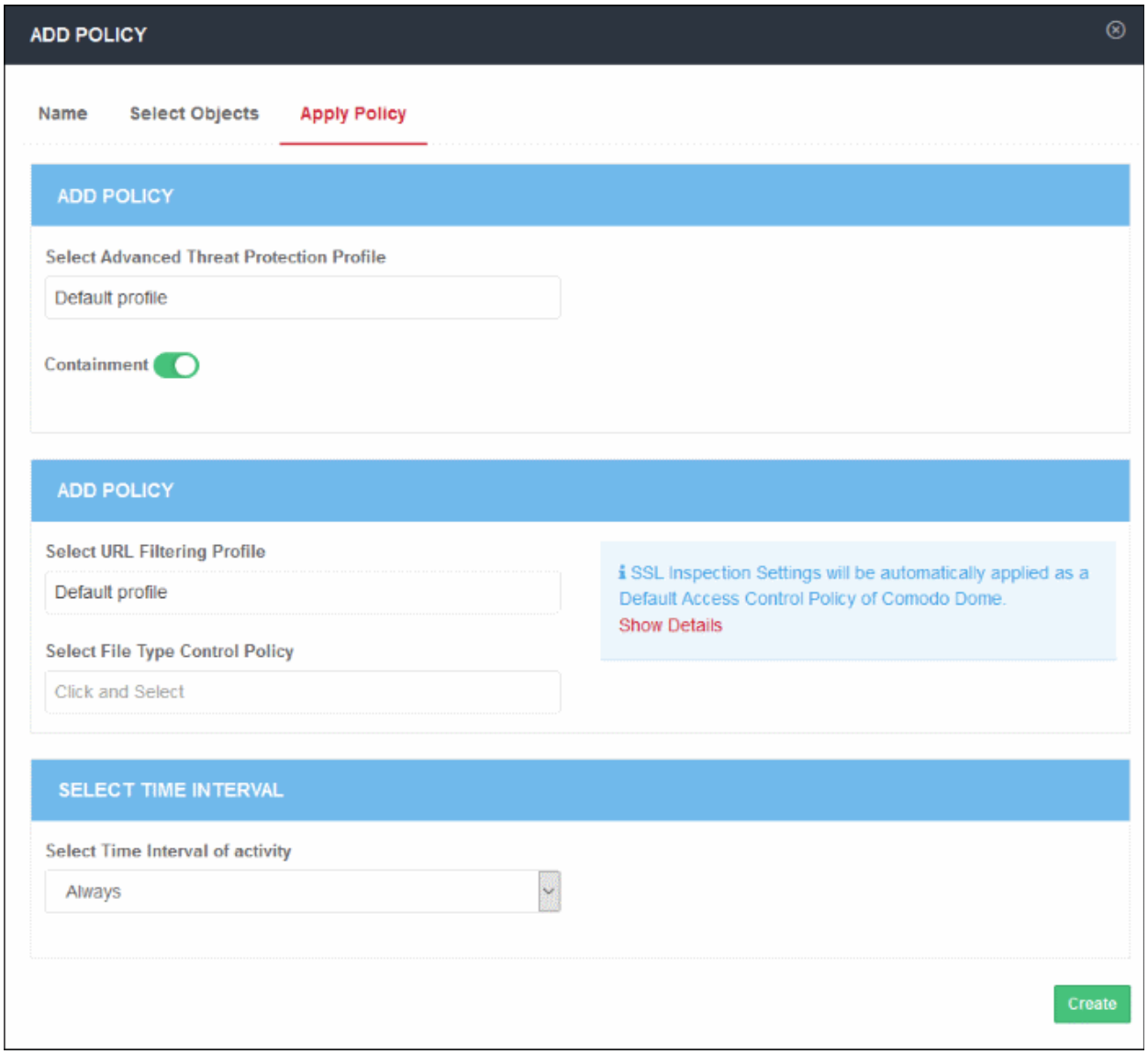


- **Location** - Select the required trusted network from the list. 'All Locations' is selected by default. You can add networks in the Locations area ('Administration' > 'Locations').
- **User** - Select the required users from the list. 'Everyone' is selected by default. You can add users in the User Management area ('Administration' > 'User Management').
- **Group** - Select any required user-groups from the list. 'Everyone' is selected by default. You can create user-groups in the User Management area ('Administration' > 'User Management').
- **Department** - Select any required department from the list. 'Everyone' is selected by default. You can create departments in the User Management area ('Administration' > 'User Management').
- **Computer Name** - Select required endpoints from the list. 'Everyone' is selected by default. You can add endpoints the User Management area ('Administration' > 'User Management').

Click 'Next' or 'Apply Policy' to proceed.

Step 3 - Select Security Policy, Web Content Policy and Schedule it

In the 'Apply Policy' section, specify the security and web content profiles that you want to add to the policy. Select the time interval that the policy should be active.



Add Security Profile

- Select Advanced Threat Protection Profile - Select the appropriate ATP profile from the list. The default profile is selected by default. The drop-down will display the ATP exception profiles that are available in the Security Policy section.
- Containment - Select whether you want to run unknown files in the sandbox. Containment is enabled by default.

Add Access Control Profile

- Select URL Filtering Profile - The default profile will be selected. The drop-down will display the URL filtering profiles that are available in URL Filtering section. Select the appropriate URL filtering profile from the list.
- SSL Inspection Settings - Allows you to configure how Comodo SWG should act if SSL certificates for the visited websites are untrusted or revoked. Please note this is a global setting, meaning any modification done will apply for all the policies. Clicking the 'Show Details' link will open the 'SSL Inspection' page.
- File Type Control Policy - Displays file download restriction rules that were created in 'Configuration' > 'Web Content Policy' > 'File Type Control'. Select the appropriate file control rule you wish to apply.

Define Policy Schedule

- Select Time Interval of Activity – By default it will be 'Always' meaning the policy will be applied at all times. The drop-down lists the schedules that you have configured in Configuration' > 'Configuration' > 'Time

Intervals'. Select the schedule from the drop-down list. Note – Make sure to place a scheduled policy above a non scheduled policy.

Click 'Create' to deploy the policy. The policy will be displayed in the Policy List.

Policy Deployment Examples

Example 1 – Deploy same policy for all users, either roaming or inside the network

Step 1 - Name

- Name – Select policy order as 1
- Policy Name – Enter a name for the policy
- Remark – Comment for the policy

Step 2 – Select Objects

- Select Location(s) – Select 'All Locations'
- Select User(s) – Select 'Everyone'
- Select Groups(s) – Select 'Everyone'
- Select Department(s) – Select 'Everyone'
- Select Computer Name(s) - Select 'Everyone'

Step 3 – Apply Policy

- Select the Security component profile and Web Content component profiles
- Click 'Create'

In this example, all users will be applied the same policy since 'All Locations' include 'Roaming users' and 'Trusted Network'.

Example 2 – User specific and Location specific policy

- Create two trusted networks – Location A and Location B
- Add usernames in User Management
- Create four polices
  - Policy 1 – Location = Location B, User = John Smith, Group = Everyone, Department = Everyone, Computer Name = Everyone
  - Policy 2 – Location = Roaming Users, User = Everyone, Group = Everyone, Department = Everyone, Computer Name = Everyone
  - Policy 3 – Location = All Locations, User = John Smith, Group = Everyone, Department = Everyone, Computer Name = Everyone
  - Policy 4 – Global Policy (default profile), All Locations and Everyone

Scenario 1

- John Smith is out of trusted location – Policy 2 will be applied since it matches the current location (Roaming) and other objects are 'Everyone', which includes John Smith.

Scenario 2

- John Smith connects to Location A – SWG first checks first rule, then second and third. Policy 3 will be applied since 'All Locations' in rule 3 includes Location A and username John Smith is specified in that policy with other objects as 'Everyone'.

Scenario 3

- John Smith connects to Location B – Policy 1 will be applied since it matches location and other objects.

Scenario 4

- Another user Angel is out of trusted location - Policy 2 will be applied since it matches the current location

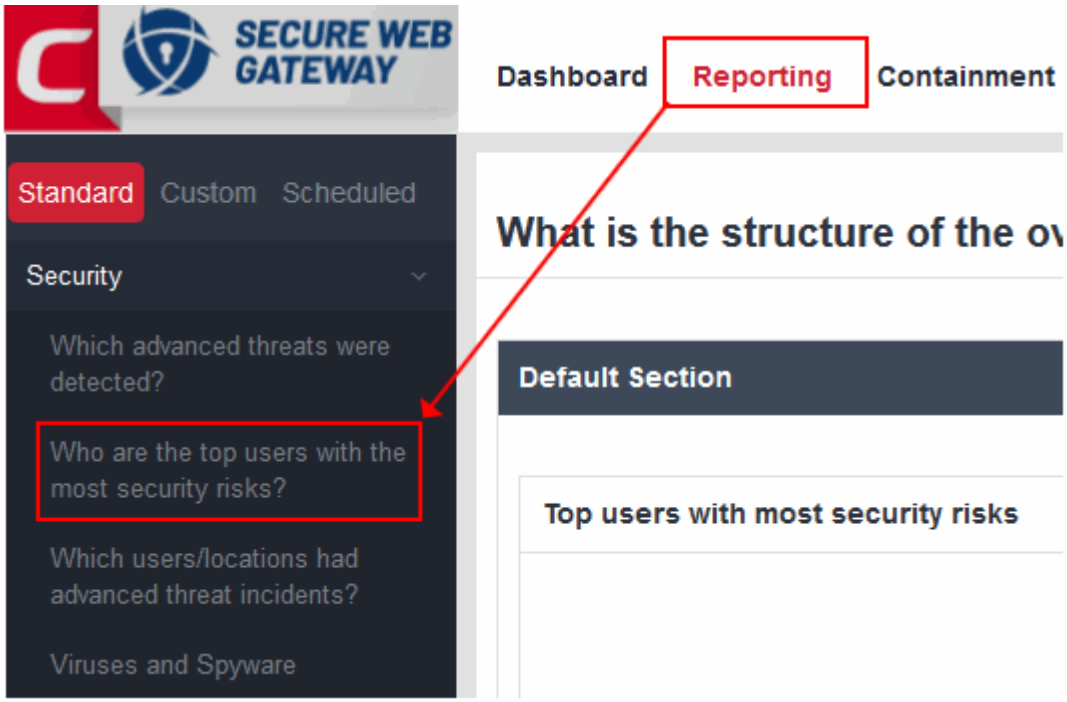
(Roaming) and other objects are 'Everyone', which includes Angel.

Scenario 5

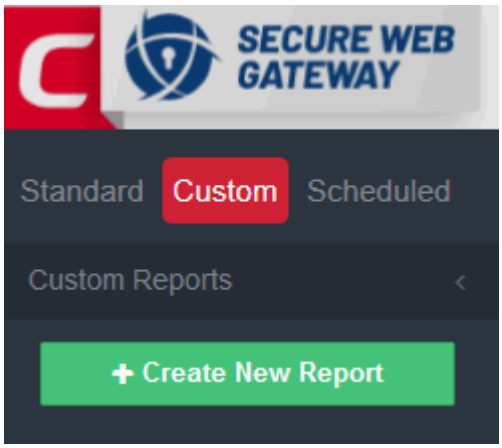
- Angel connects to Location B
  - Policy 1 is matching on locations but not the username.
  - Policy 2 is for roaming users only and Angel is connected to Location B and hence will not be applicable.
  - Policy 3 is also not valid since username is different in that.
  - Policy 4 (Global Policy) will apply since it has 'All Locations' and 'Everyone'.

Generate Reports

Reports provide in-depth insights into security, user activity and web activity on your network.



- Click 'Reporting' in the top-menu to open the reports area.
- 'Standard', canned reports are shown in the left-menu. The content of the report will be shown in the main pane.
  - Comodo SWG ships with various standard reports in three categories - 'Security', 'User/Location Activity' and 'Web Activity'.
  - The default period covered by a standard report is 7 days. This cannot be changed.
- You can create your own custom reports by clicking the 'Custom' button on the left:



- Click 'Scheduled' to generate a report at a specific date/time. Scheduled reports can also be emailed to recipients of your choice.
- See '**Custom Reports**' and '**Schedule Report Generation**' if you need more help with these items.

See the full admin guide at **https://help.comodo.com/topic-436-1-842-10771-Introduction-to-Comodo-Secure-Web-Gateway.html** if you need more help on the topics covered in this guide.

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**