COMODO
Creating Trust Online®

COMODO ONE
MSP

Comodo Secure Web Gateway

Software Version 2.22

Administrator Guide

Guide Version 2.22.032020

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

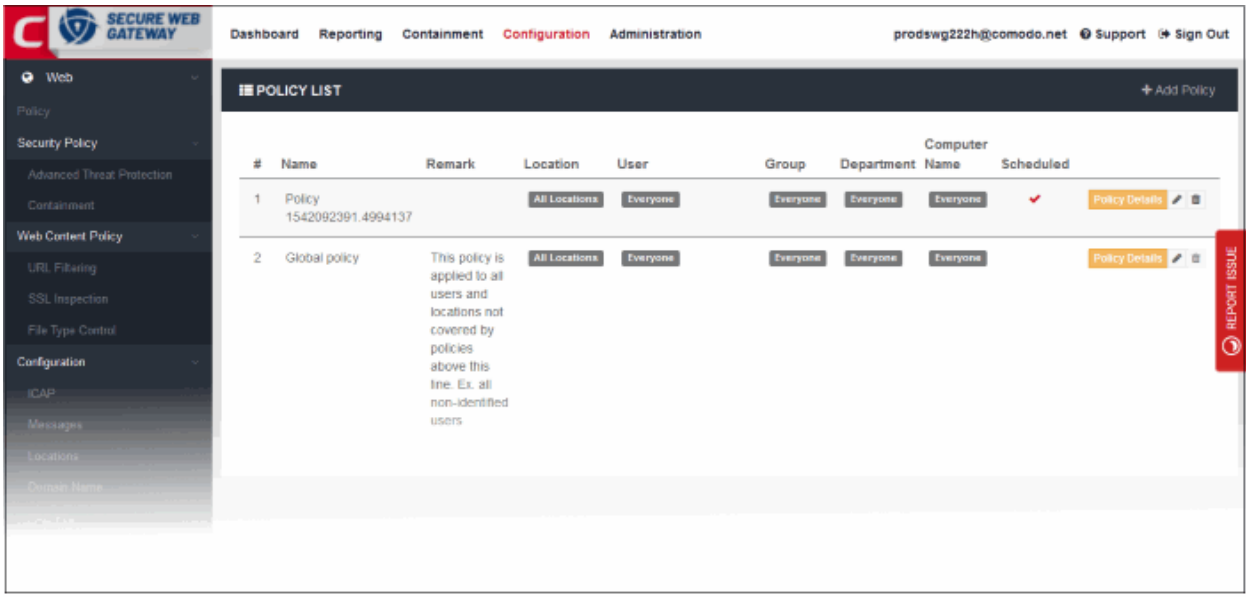
Table of Contents

1 Introduction to Comodo Secure Web Gateway....4
1.1 Purchase Licenses....5
1.2 Login to the Admin Console....6
2 The Admin Console....10
3 The Dashboard....13
3.1 Customize the Dashboard....43
4 Configure Comodo Secure Web Gateway....49
4.1 Connect your Network / Devices to Comodo Secure Web Gateway....50
4.1.1 Traffic Forwarding via Direct Proxy or PAC....50
4.1.2 Traffic Forwarding via Proxy Chaining....53
4.1.3 Traffic Forwarding via Internet Content Adaptation Protocol (ICAP)....55
4.1.4 Traffic Forwarding via SWG Agent....56
4.2 Connect your Roaming Devices to Comodo Secure Web Gateway....56
4.2.1 View Enrolled Roaming Devices....60
4.3 Configure Comodo Secure Web Gateway Messages....60
4.4 Configure Domain Name....62
4.5 Configure PAC File for Exclusions....62
4.6 Configure Data Loss Prevention and View ICAP Service Information....64
4.7 Configure Policy Time-Schedules....66
5 Manage Trusted Networks....70
6 Manage Policies....73
6.1 Security Policy....74
6.1.1 Configure Advanced Threat Protection Settings....75
6.1.2 Configure Containerization Settings....80
6.2 Web Content Policy....81
6.2.1 Manage URL Filtering Policies....82
6.2.2 Configure SSL Inspection Settings....87
6.2.3 Manage File Type Control Rules....90
7 Apply Policies to Networks....94
8 Administration....104
8.1 Configure User Authentication Settings....104
8.2 User Management....111
8.2.1 Manage Users....112
8.2.2 Manage User Groups....116
8.2.3 Manage Departments....118
8.2.4 Manage Computers....121
8.3 My Profile....123
9 Reports....124
9.1 Custom Reports....126
9.2 Scheduled Reports....128
10 Unknown Threat Statistics....131

About Comodo Security Solutions.....134

1 Introduction to Comodo Secure Web Gateway

- Comodo Secure Web Gateway (SWG) is a real-time web traffic scanner which provides comprehensive security for customer websites.
- SWG includes URL filtering, advanced threat protection, Valkyrie file verdict service and automatic containment of unknown files. SWG is hosted on your Amazon Web Services (AWS) platform.



Features

- Default rules which provide blanket protection from malware, botnet, browser exploits, high risk sites and more
- Isolates unknown files in a virtual operating environment, preventing infection from zero-day threats
- Website categories which make it easy to create a specific policy for your organization
- Create your own domain blacklists and whitelists
- Multiple node hosting for load balancing
- Prevents access to sites with untrusted or revoked server certificates
- Advanced reporting grants full visibility of events. Configure and schedule your own custom reports.
- Add multiple networks and configure location-specific policies
- Schedule policies which will take effect for selected time intervals
- Add users, user groups and departments per your requirements
- Seamless integration with Comodo Data Loss Prevention (DLP)

Guide Structure

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

- **Introduction to Comodo Secure Web Gateway**
  - **Purchase Licenses**
  - **Login to the Admin Console**

- The Administrative Console
- The Dashboard
  - Customize the Dashboard
- Configure Comodo Secure Web Gateway
  - Connect your Network / Devices to Comodo Secure Web Gateway
  - Connect your Roaming Devices to Comodo Secure Web Gateway
  - Configure SWG Messages
  - Configure Domain Name
  - Configure PAC File for Exclusions
  - Configure Data Loss Prevention and View ICAP Service Information
  - Configure Policy Time-Schedules
- Manage Trusted Networks
- Manage Policies
  - Security Policy
  - Web Content Policy
- Apply Policies to Networks
- Administration
  - Configure User Authentication Settings
  - User Management
  - My Profile
- Reports
  - Custom Reports
  - Schedule Report Generation
- Unknown Threat Statistics

1.1 Purchase Licenses

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

- **Stand-alone 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 SWG plan best suited to your requirements.
  - 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.

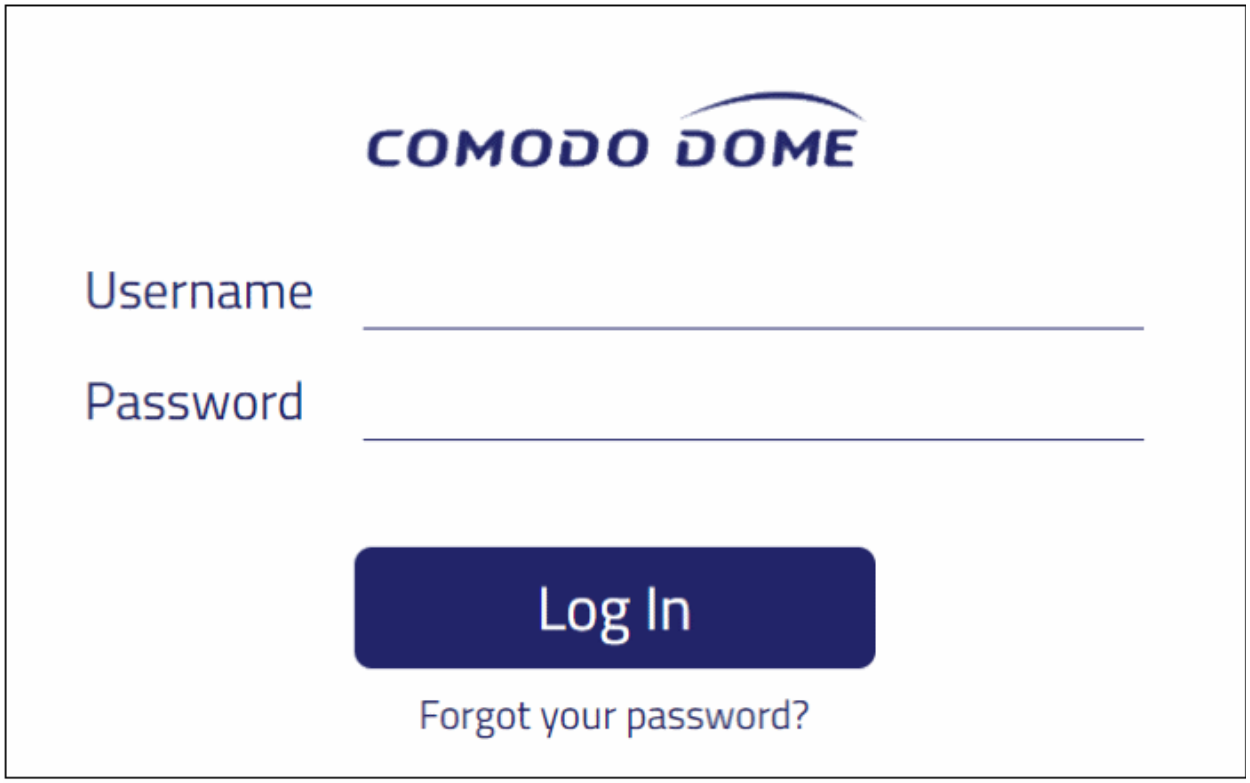
Note: Comodo SWG can be hosted on your Amazon Web Services (AWS) cloud platform. If you do not have an AWS account, Comodo will host it for you.

1.2 Login to the Admin Console

Stand-alone Customers

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

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



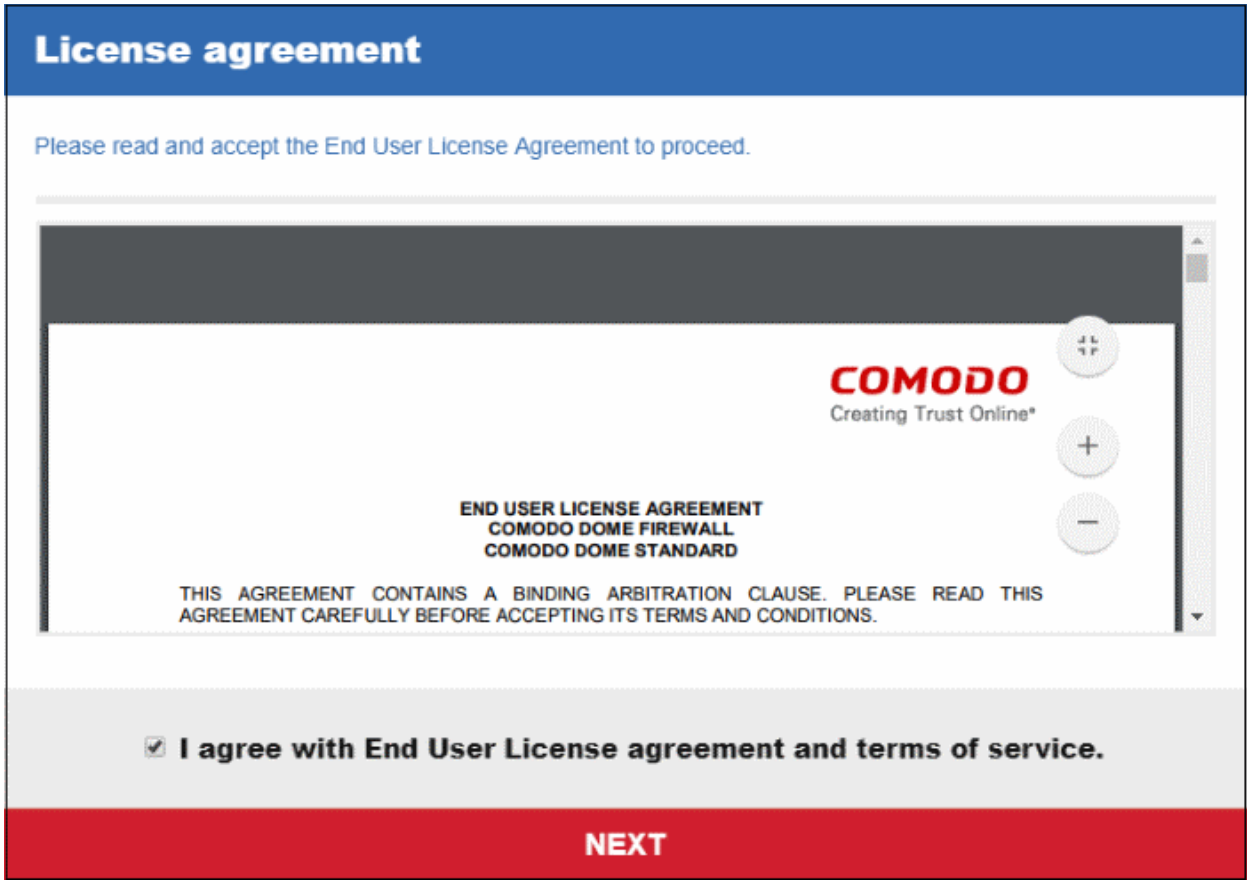
- Enter your username and password in the respective fields and click 'Sign In'

Portal Customers

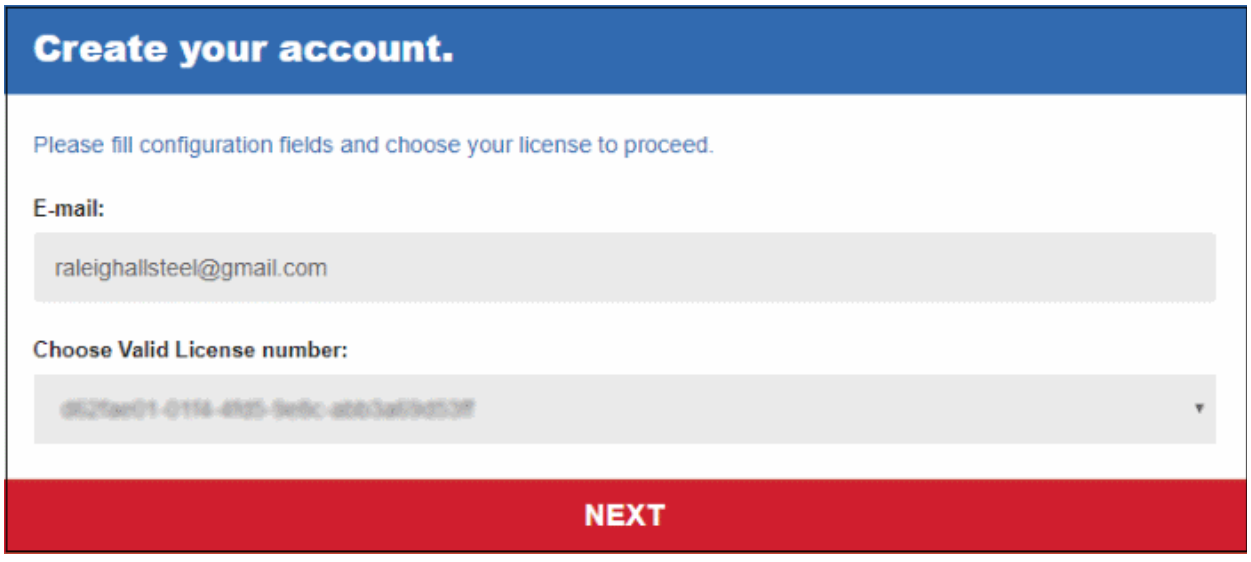
- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Applications' > 'Comodo Secure Web Gateway'

Configure 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'

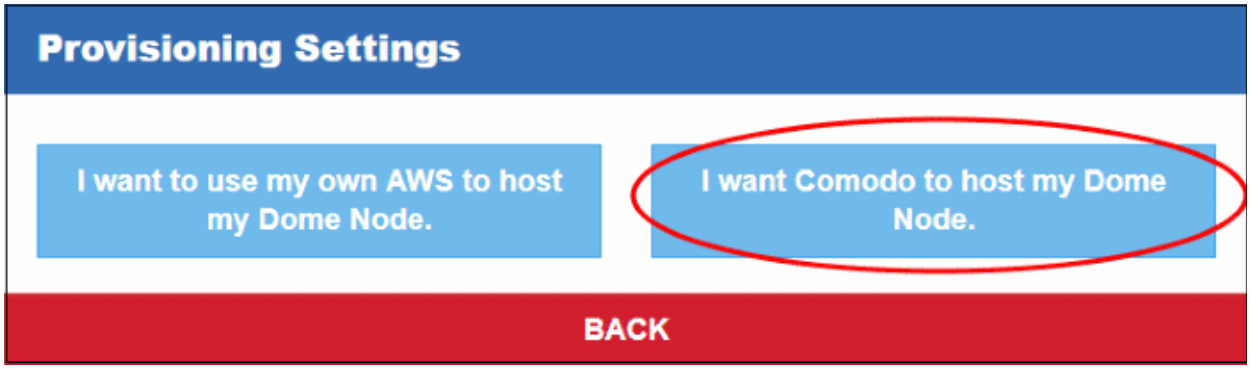


- Select the license you wish to use and click 'Next'

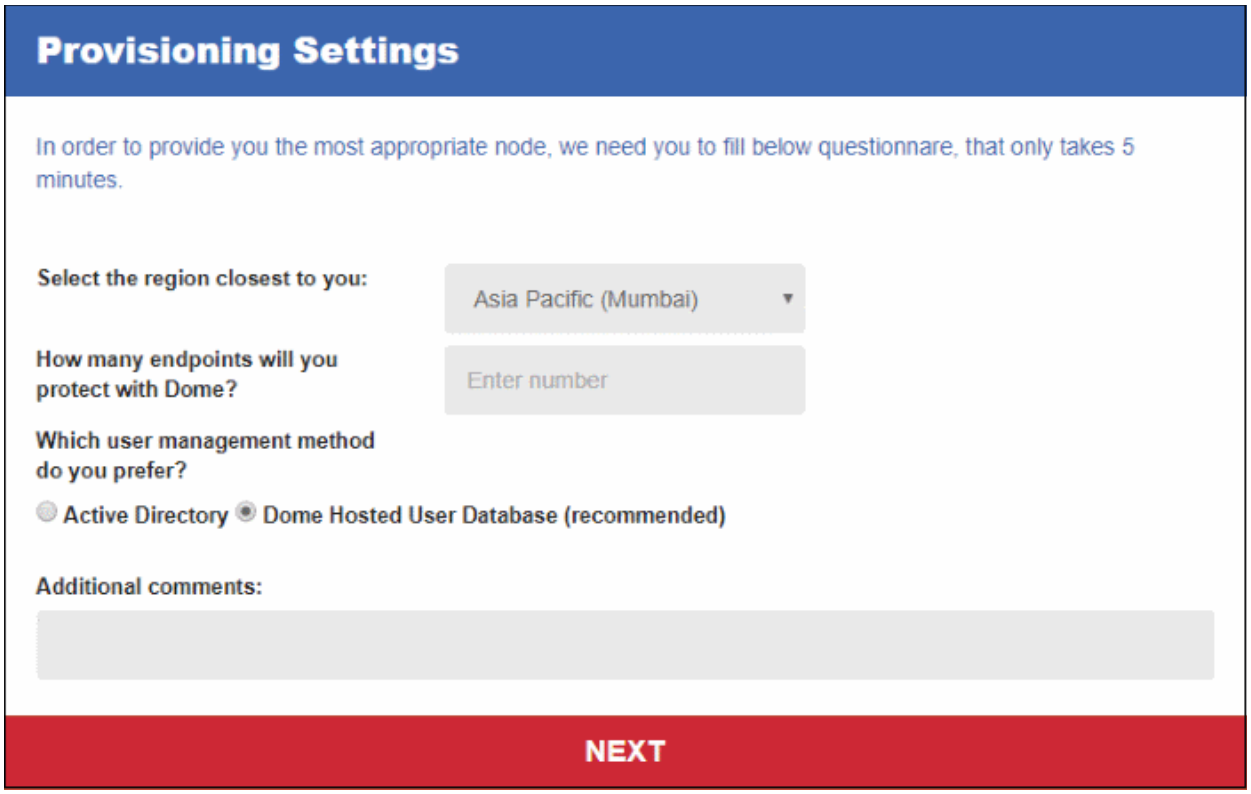
Next, select the hosting type:

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

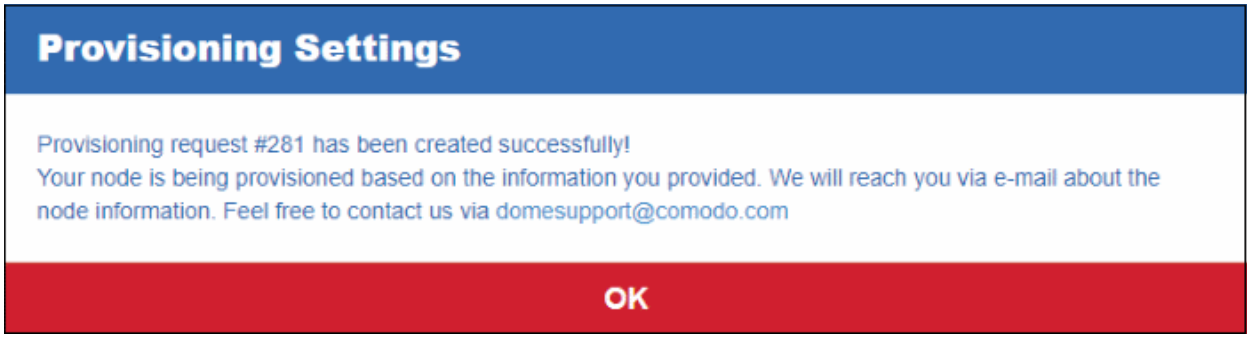
Comodo Hosted Account



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

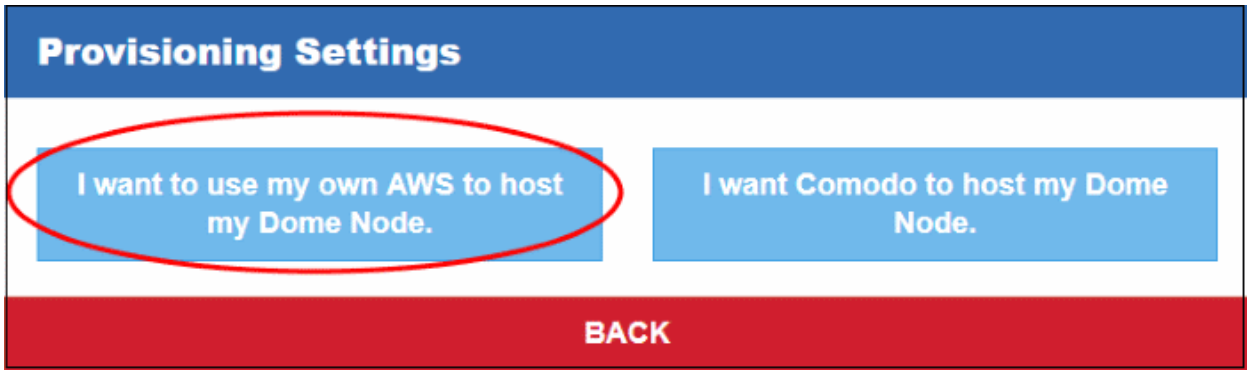


- Select the region closet to you - Choose the region closest to your location. This will improve the performance of the service.
- How many endpoints will you protect with SWG - Enter the number of endpoints you wish to cover with SWG protection.
- Which user management method do you prefer - Select 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'

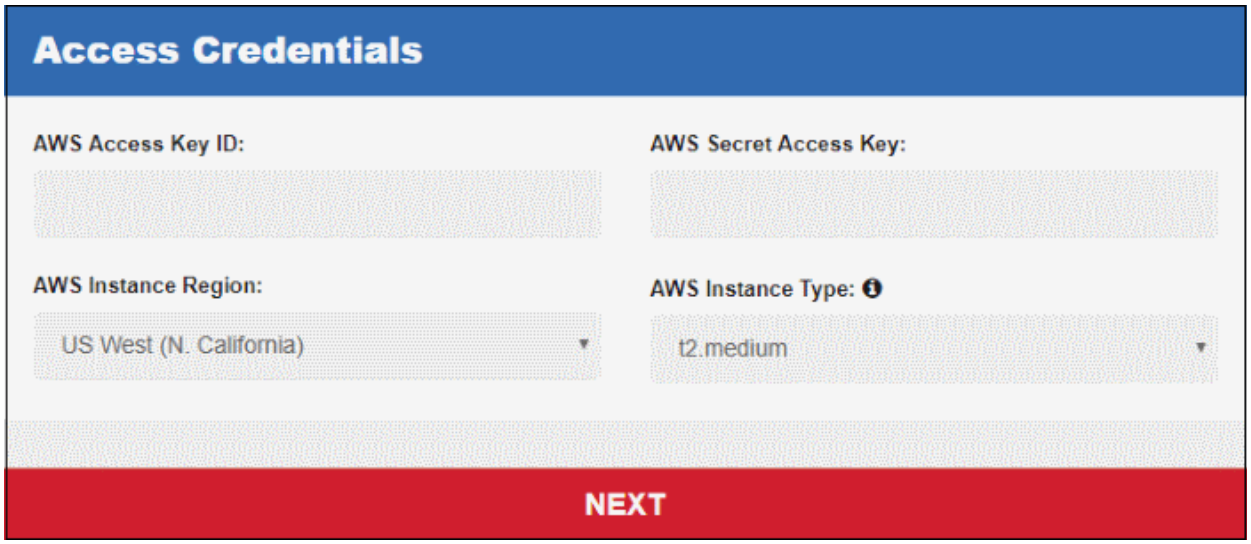


That's it. The Comodo hosted node will be prepared and a confirmation mail sent to your registered address. Contact support at **domesupport@comodo.com** if you have any questions.

Customer AWS Account



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

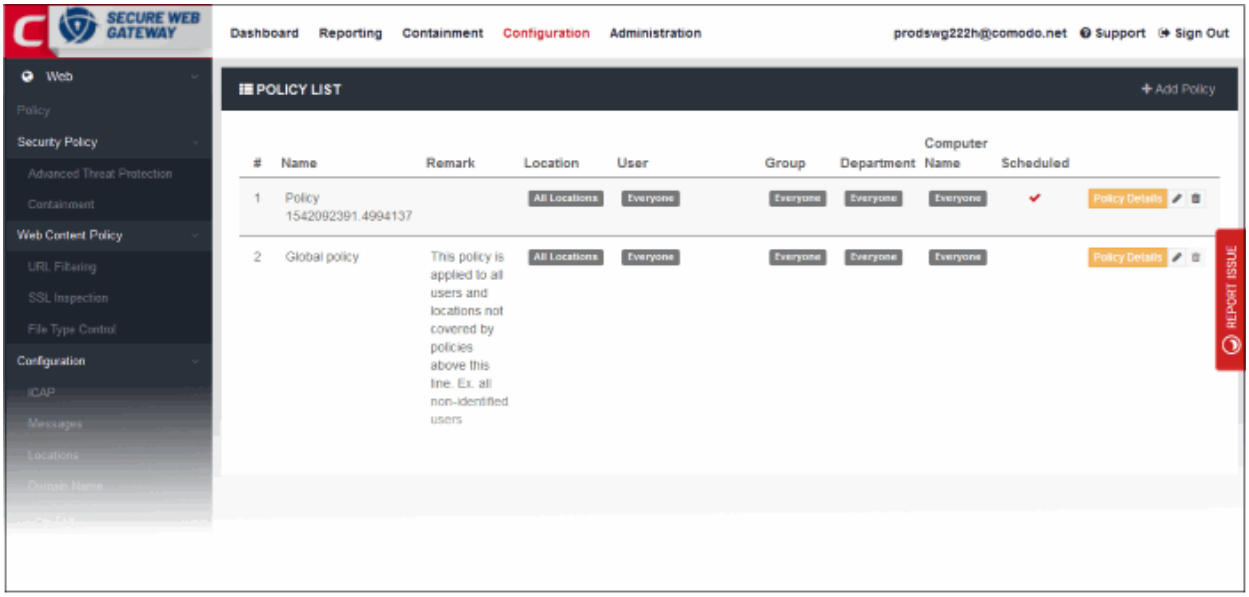


- Enter your AWS account credentials and click 'Next'.
- After your credentials have been authenticated, next complete the 'Provisioning Settings' wizard.

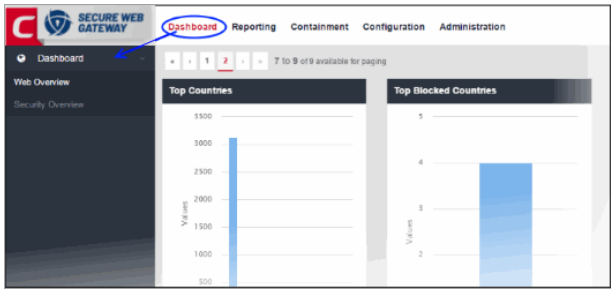
After completing the application, Comodo will provision SWG on your AWS account. The node(s) will be prepared and a confirmation mail sent to your registered address. Contact support at **domesupport@comodo.com** if you have any questions.

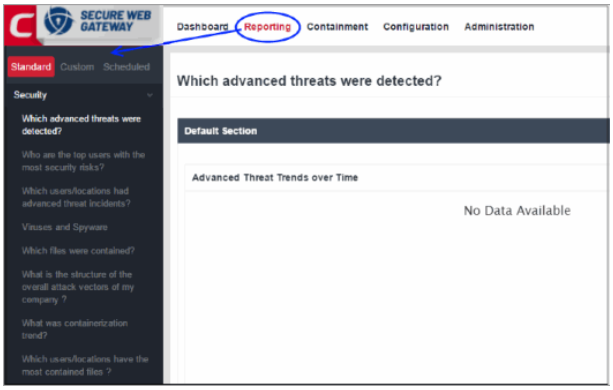
2 The Admin Console

The admin console lets you add networks you want to protect, create security policies, add users, create domain blacklist/whitelists, view dashboard stats and more.



The items in the left-hand menu vary according to the tab selected at the top:

Dashboard - Shows statistics on browsing trends, security trends, top URL categories and more. You can also customize the dashboard according to your requirements. See '**The Dashboard**' for more details.	

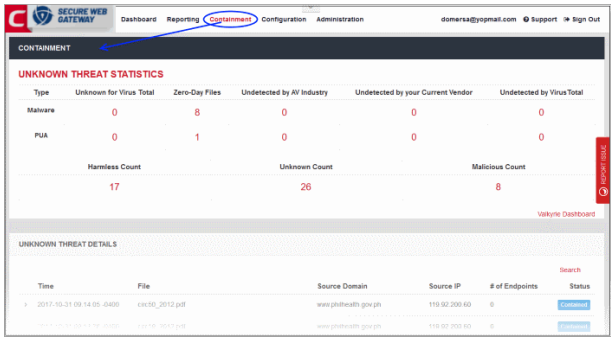


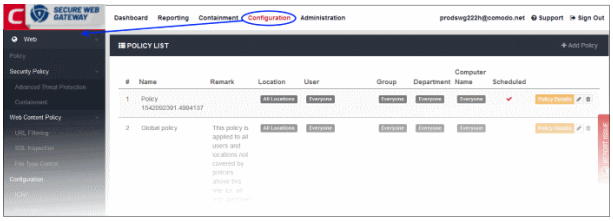
Reporting - Comprehensive reports on:

- Threats detected on your networks
- Which users have encountered the most security risks
- Domains which were blocked most often
- Activity from mobile devices
- Much, much more.

You can also configure custom reports and schedule report generation. See '**Reports**' for more details.

Containment - Shows the status of downloaded unknown files. Full details of the analysis is also available in Comodo Valkyrie. See '**Unknown Threat Statistics**' for more details.

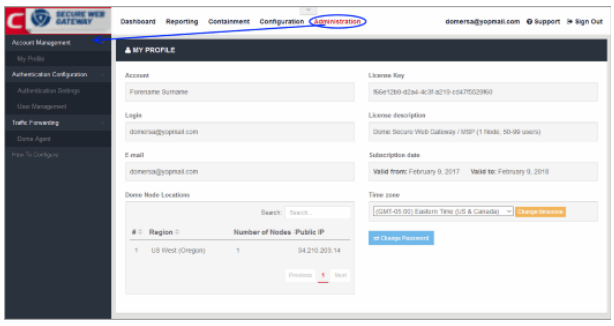


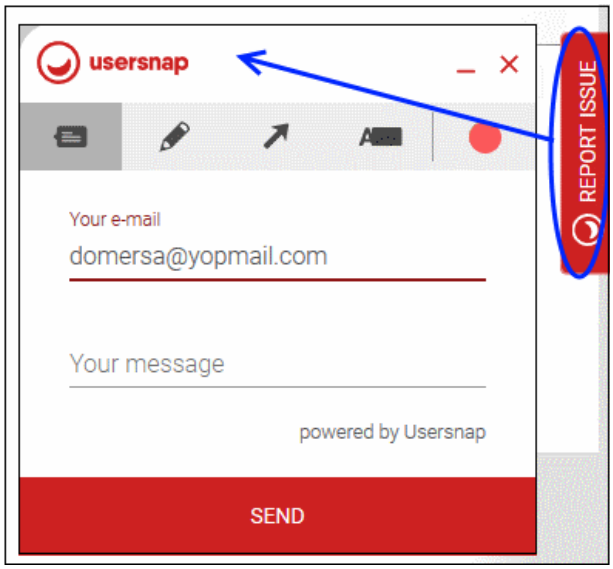


Configuration - Add networks you want to protect and create security and web content rules. The security and web content rules can then be added as a policy to a selected network from the 'Policy' interface.

- **Policy** - Deploy comprehensive security schemes to protected networks. Each policy is made up of security rules and web content rules. See '**Apply Policies to Networks**' for more details.
- **Security Policy** - Create and manage security rules and containerization settings. See '**Security Policies**' for more details.
- **Web Content Policy** - Create and manage rules which control internet access permissions. See '**Web Content Policy**' for more details.
- **Configuration** - Add networks you wish to protect. See '**Connect your Network Comodo Secure Web Gateway**' for more details.

Administration - Configure user authentication settings, add and manage users and download SWG agent and configuration files. See '**Administration**' for more details.





Feedback – Send your comments, questions or report a bug.

- Click 'Report Issue' on the right-side of the interface
- Use the tools at the top of the feedback form to mark, point, highlight or comment on the SWG interface.
- Complete the feedback form and click 'Send'
- This will create a support ticket which our support team will respond to as soon as possible.

Menus on the top right:

- Logged in user name - Click the user name to open the '**My Profile**' page. You can change your password, change timezone and view account details.
- Support - Submit support tickets to Comodo.
- Sign Out - Log out of the admin console.

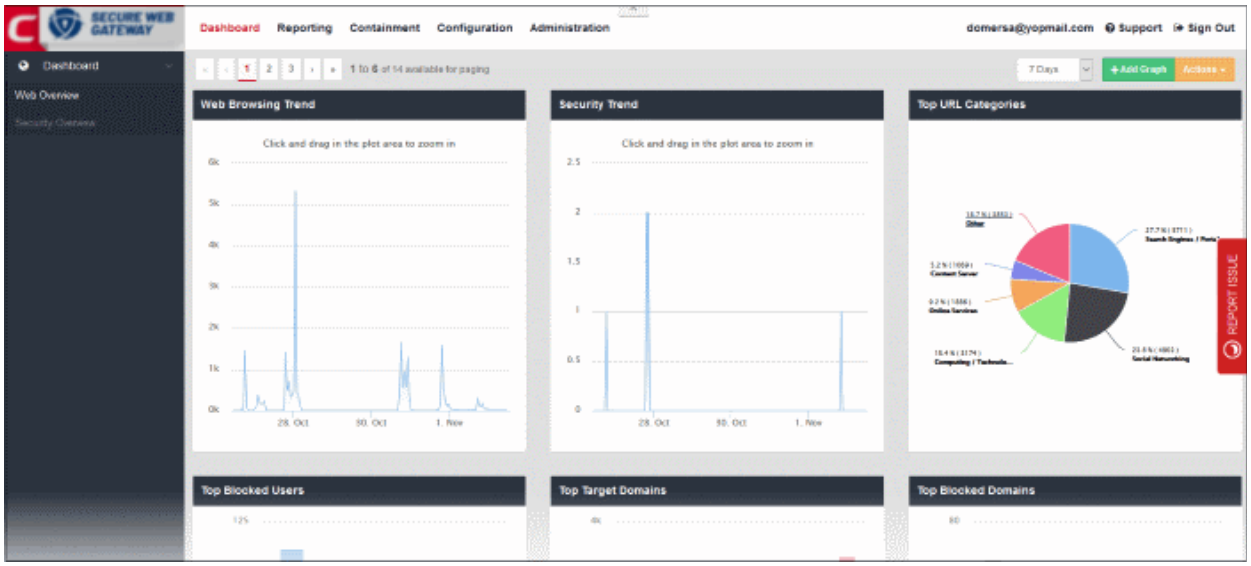
3 The Dashboard

The dashboard provides an 'at-a-glance' summary of the protection status of your networks.

- Using a range of statistics and charts, the dashboard clearly displays vital information about your policy deployment and allows you to drill-down to further areas of interest or concern.
- Charts include general web browsing trends, security trends, top URL categories, top visited domains, top blocked domains, top blocked users and more.
- You can also create your own dashboard tiles tailored to your requirements.

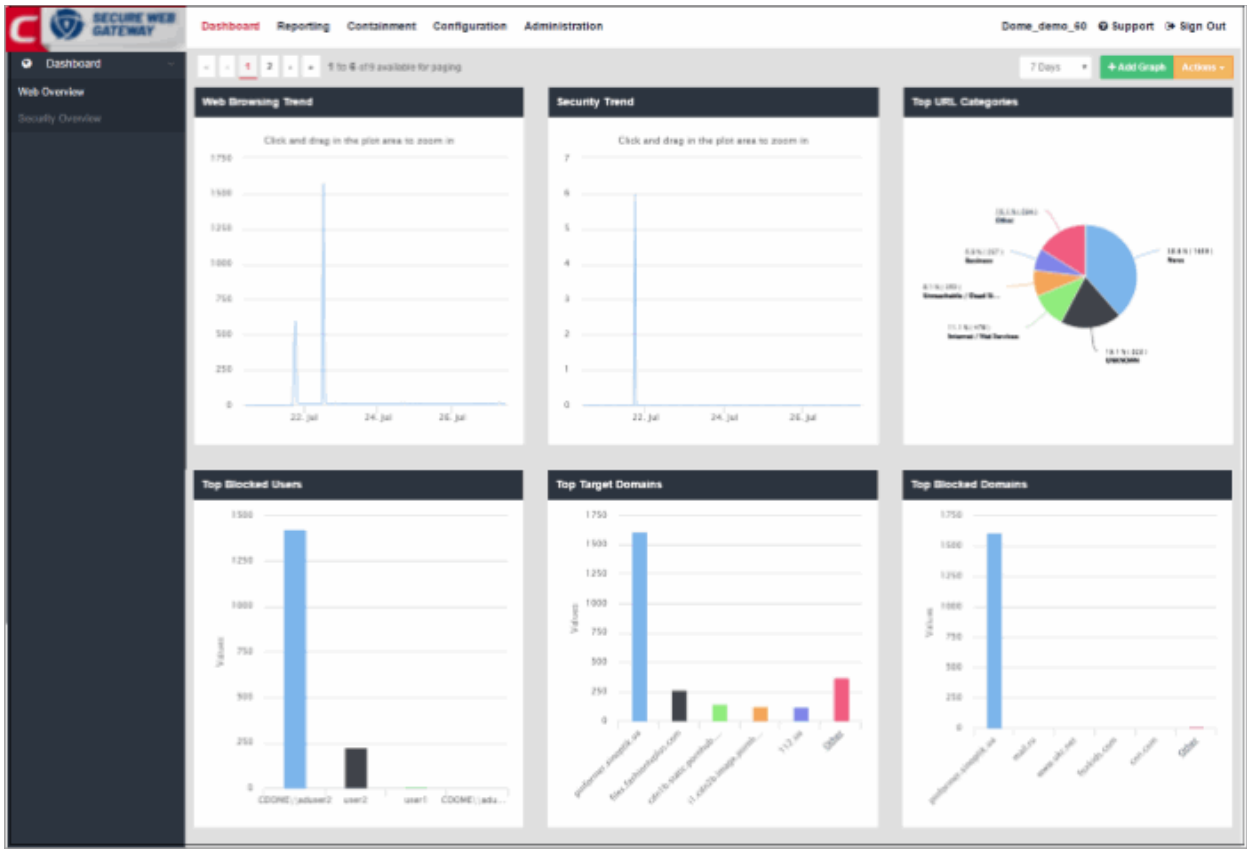
The dashboard contains two sections:

- **Web Overview** - Categorized statistics about activity on your protected domains. Includes top targets/blocked domains, top users/blocked users, top countries/blocked countries and more.
- **Security Overview** - Statistics about security trends, top malicious sites that were blocked and more.



Web Overview

- To open the 'Web Overview' section, click 'Dashboard' at the top, then 'Web Overview' under 'Dashboard' on the left.



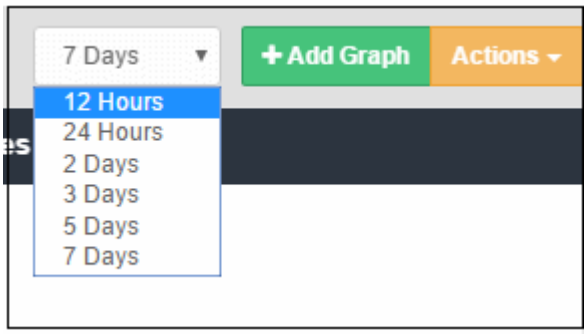
By default, the 'Web Overview' section in the dashboard displays the following tiles:

- **Web Browsing Trend**
- **Security Trend**
- **Top URL Categories**

- **Top Blocked Users**
- **Top Target Domains**
- **Top Blocked Domains**
- **Top Countries**
- **Top Blocked Countries**
- **Top Users**
- **Top Blocked File Types**
- **Most Downloaded File Types**

You can add more tiles to the dashboard as required. See '**Customize the Dashboard**' for more details. A dashboard page will contain a maximum of 6 tiles and you can navigate to other tiles in the section by clicking the page numbers at the top.

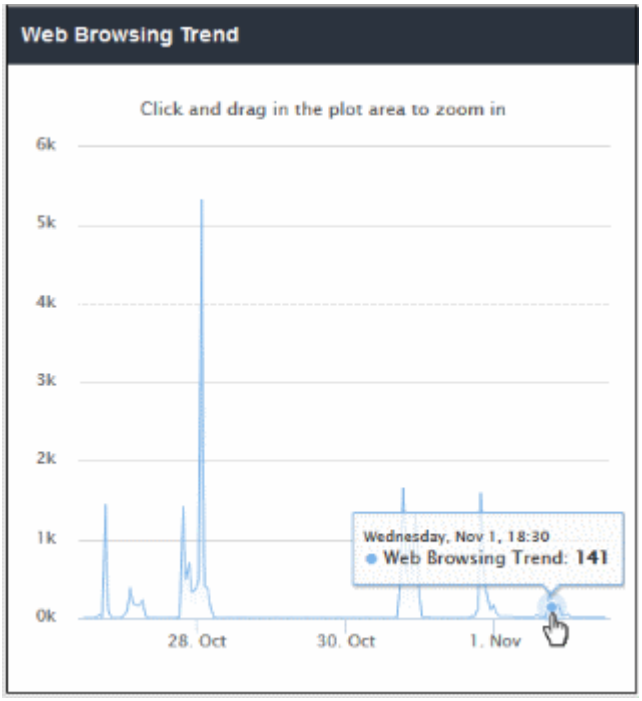
By default, statistics are displayed for the past 12 hours. You can view statistics going back up to 7 days in the drop-down at top-right:



- **Add Graph** - Add more tiles according to your requirements. For example, you may want to add a tile to view only blocked traffic stats and so on. See '**Customize the Dashboard**' for more details.
- **Actions** - Make notes, place tiles in a different order and export the dashboard to pdf. **Click here** for more details.

Web Browsing Trend

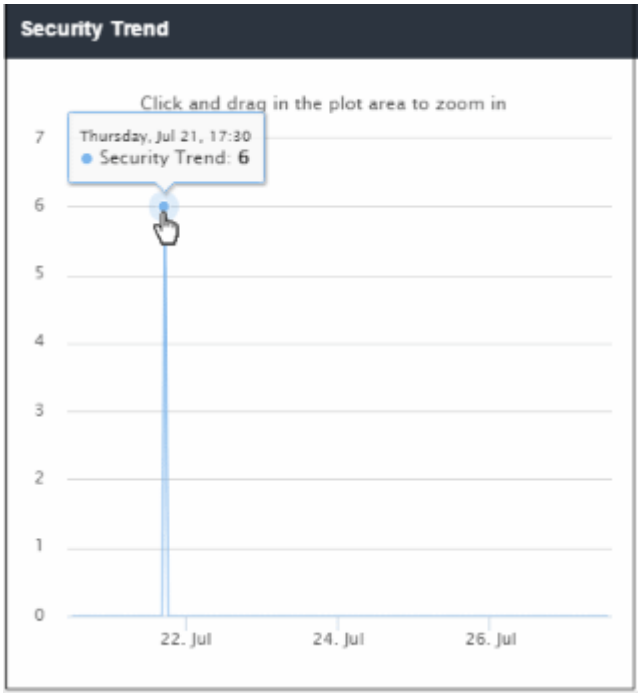
The 'Web Browsing Trend' line chart displays the number of websites visited and their HTTP requests for a particular date and time. The X-axis displays the date/time and the Y-axis displays the number of websites. The results are displayed for the latest 5 events. Placing the mouse cursor over a point will display further details.



- To view full details for a particular period in the chart, click and drag to zoom the plot. Click 'Reset Zoom' to return to full chart. Clicking on a particular point on the chart will open the 'View Logs' screen displaying full details of the visited websites and HTTP requests. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Security Trend

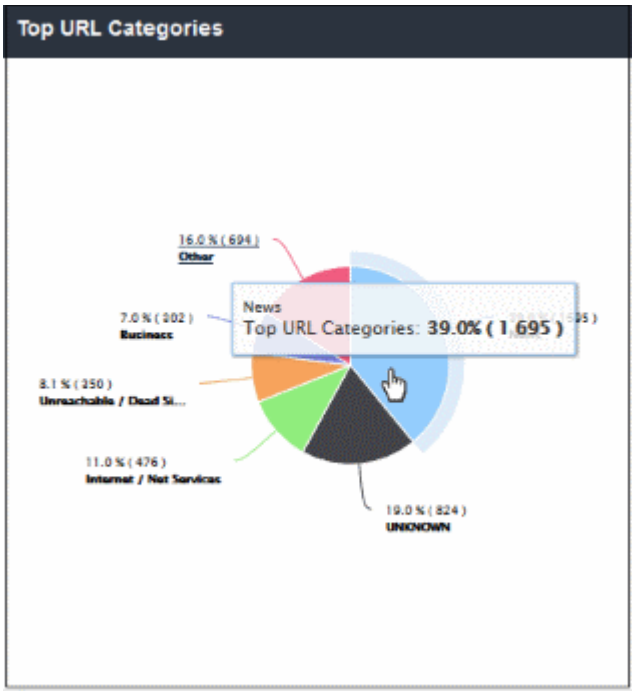
The 'Security Trend' tile shows sites from which malicious files were blocked. The X-axis displays the date/time of the event and the Y-axis displays the number of blocked files. The results are displayed for the latest 5 events. Placing the mouse cursor over a point will display further details.



- To view full details for a particular period in the chart, click and drag to zoom the plot. Click 'Reset Zoom' to return to full chart. Clicking on a particular point on the chart will open the 'View Logs' screen displaying full details of the websites, blocked file names, file hash and signature. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Top URL Categories

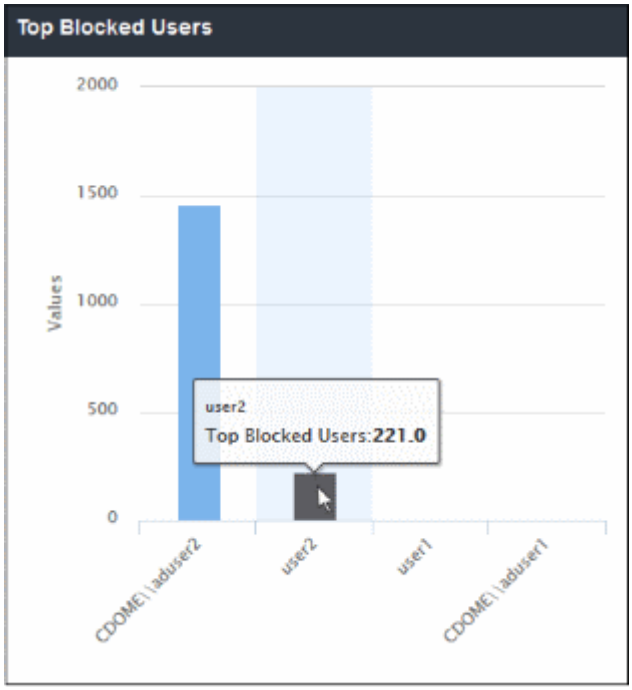
The 'Top URL Categories' chart displays the most visited websites in each category. The results are displayed for the top 10 categories. Placing your mouse cursor over a sector will display further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays full details of visited websites and HTTP requests by category. You can filter details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Top Blocked Users

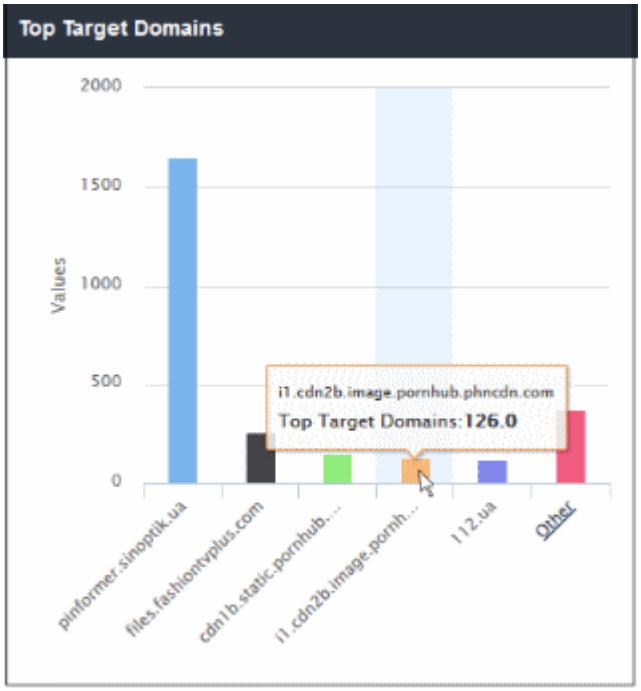
'Top Blocked Users' shows those users in the network that were most often blocked by SWG security policies. The results are displayed for the top 10 users. The X-axis displays the name of the users and the Y-axis displays the number of websites that were blocked including their HTTP requests. Placing the mouse cursor over a bar will display further details.



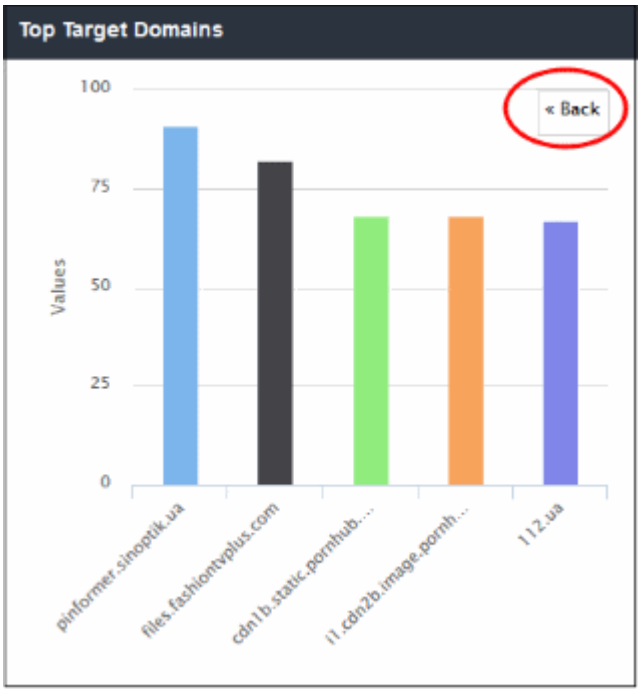
- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the top blocked users and websites including HTTP requests. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Top Target Domains

'Top Target Domains' shows those websites which were most often visited by users in your organization. The results are displayed for the top 10 domains. The X-axis displays the name of the domain and the Y-axis displays the number of times the websites were visited, including their HTTP requests. Placing your mouse cursor over a bar will display further details.



- The number of domains shown is limited to 5 in the chart. Details of the next 5 domains can be viewed by clicking 'Other'. Click 'Back' to return to the original view.

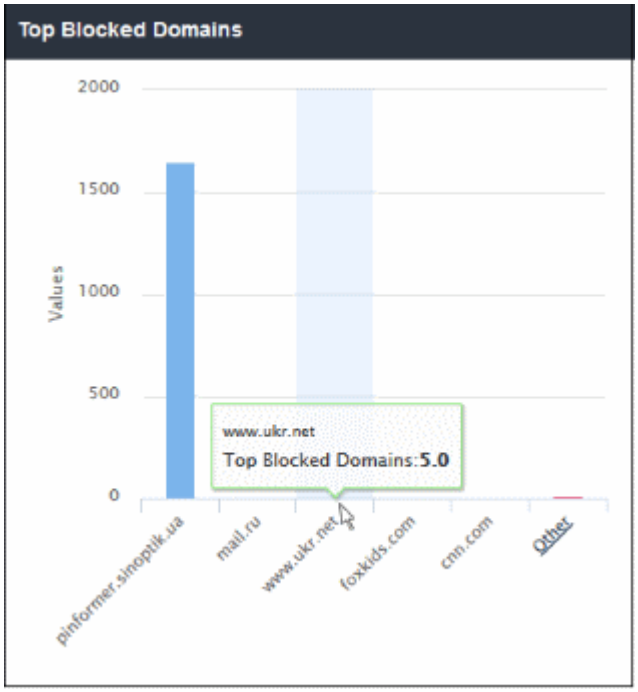


- Clicking on a particular bar on the chart will open the 'View Logs' screen displaying full details of the top visited domains and HTTP requests. You can filter the details according to your needs. See '**View Web**

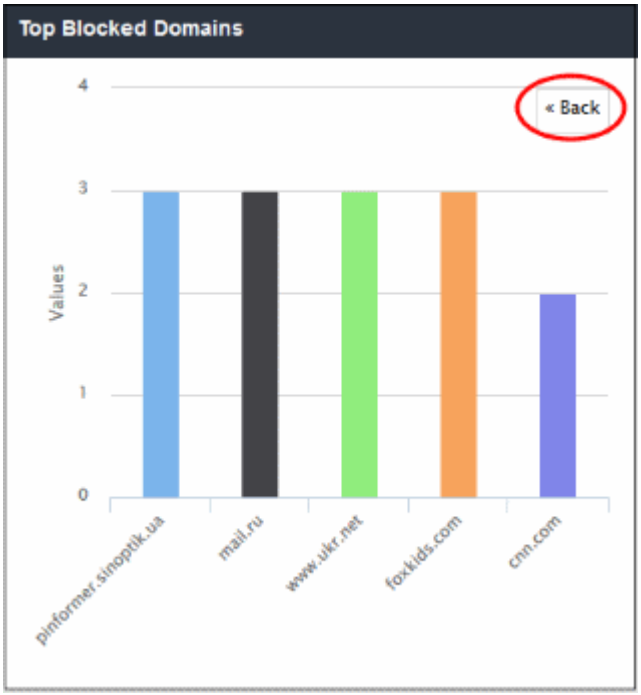
Overview Dashboard Logs' for more details.

Top Blocked Domains

'Top Blocked Domains' shows those websites that were most often blocked by SWG security policies. The results are displayed for the top 10 blocked domains. The X-axis displays the name of the domain and the Y-axis displays the number of times the websites were blocked including their HTTP requests. Placing the mouse cursor over a bar will display further details.



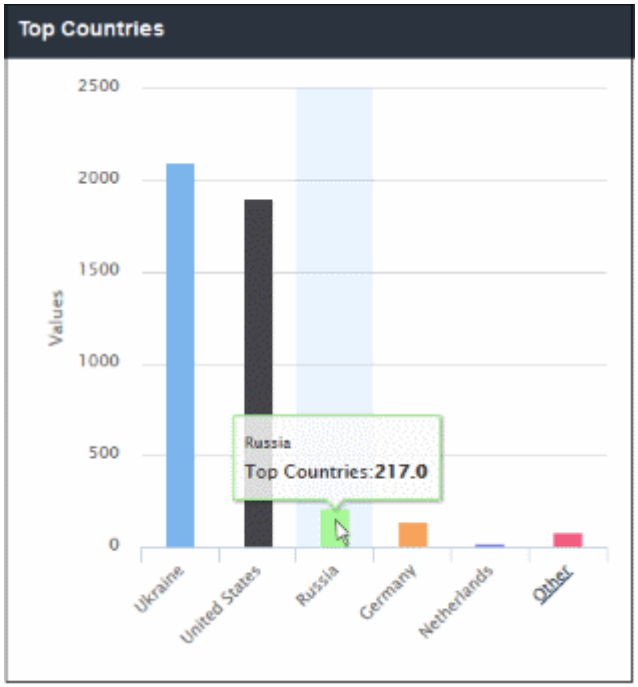
- The number of domains shown is limited to 5 in the chart. Details of the next 5 domains can be viewed by clicking the 'Other' link. Click 'Back' to return to the original view.



- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the top blocked domains and HTTP requests. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Top Countries

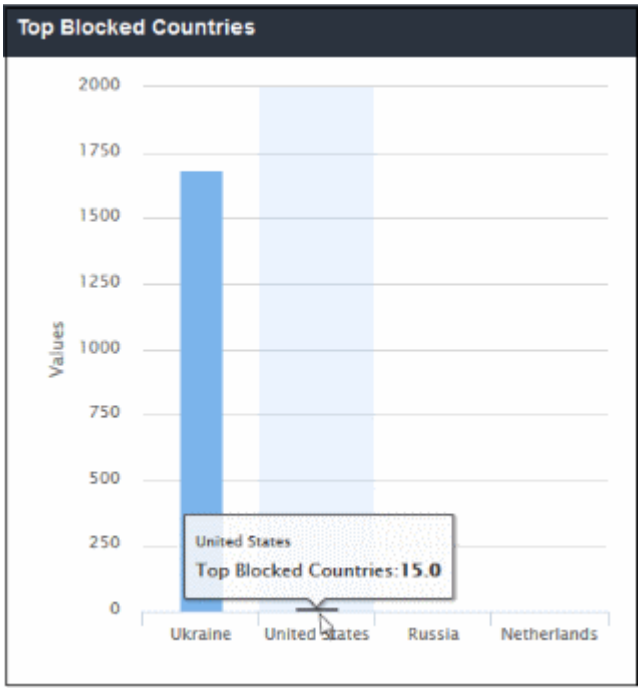
'Top Countries' shows the details of countries from where the most websites are hosted. The results are displayed for the top 10 countries. The X-axis displays the name of the country and the Y-axis displays the number of websites, including their HTTP requests. Placing the mouse cursor over a bar will display further details.



- The number of countries shown is limited to 5 in the chart. Details of the next 5 countries can be viewed by clicking the 'Other' link. Click 'Back' to return to the original view.
- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the top countries. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Top Blocked Countries

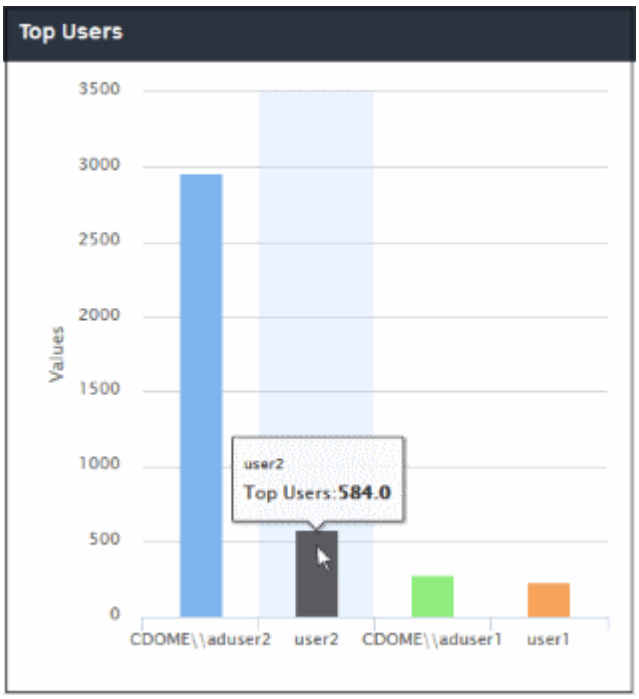
'Top Blocked Countries' shows the details of countries from where the most websites that were blocked by SWG security polices, are hosted. The results are displayed for the top 10 countries. The X-axis displays the name of the blocked country and the Y-axis displays the number of websites, including their HTTP requests. Placing the mouse cursor over a bar will display further details.



- The number of blocked countries shown is limited to 5 in the chart. Details on the next 5 countries can be viewed by clicking the 'Other' link. Click 'Back' to return to the original view.
- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the top blocked countries. You can filter the details according to your needs. See '**Viewing Web Overview Dashboard Logs**' for more details.

Top Users

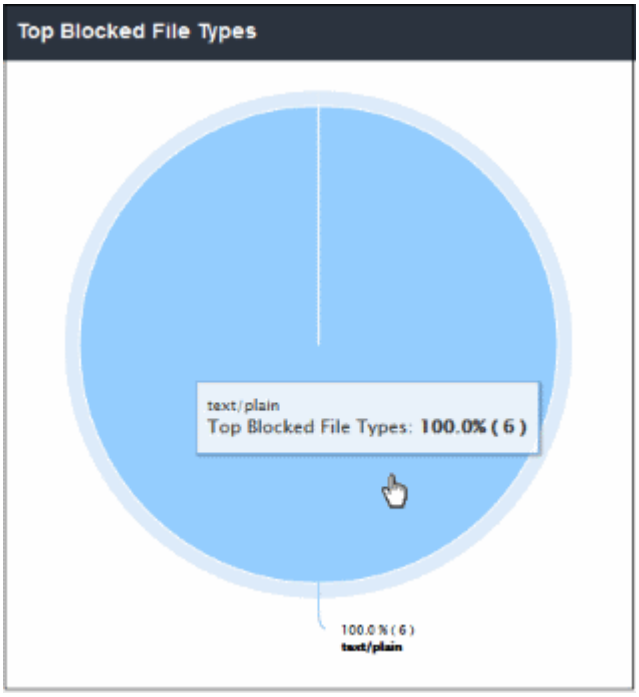
The users in your network who made the most website calls. The Y-axis value is a count of all HTTP requests made by a user. Each hit is counted separately, and each contributes to this total. This includes if the user visits different pages on the same website, or requests the same web-page multiple times. The count also includes requests made by the website itself for resources like images.



- Click a bar in the chart to view more a full log. See '**View Web Overview Dashboard Logs**' if you need more help with this.

Top Blocked File Types

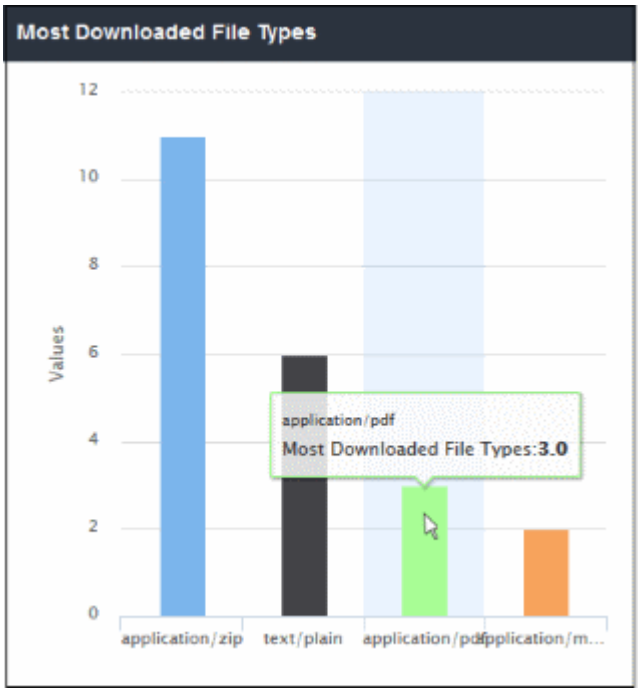
The 'Top Blocked File Types' chart displays the file types that were most blocked by SWG. The results are displayed for the top 10 categories. Place your mouse cursor over a sector to view further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays full details of the blocked file types. You can filter details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Most Downloaded File Types

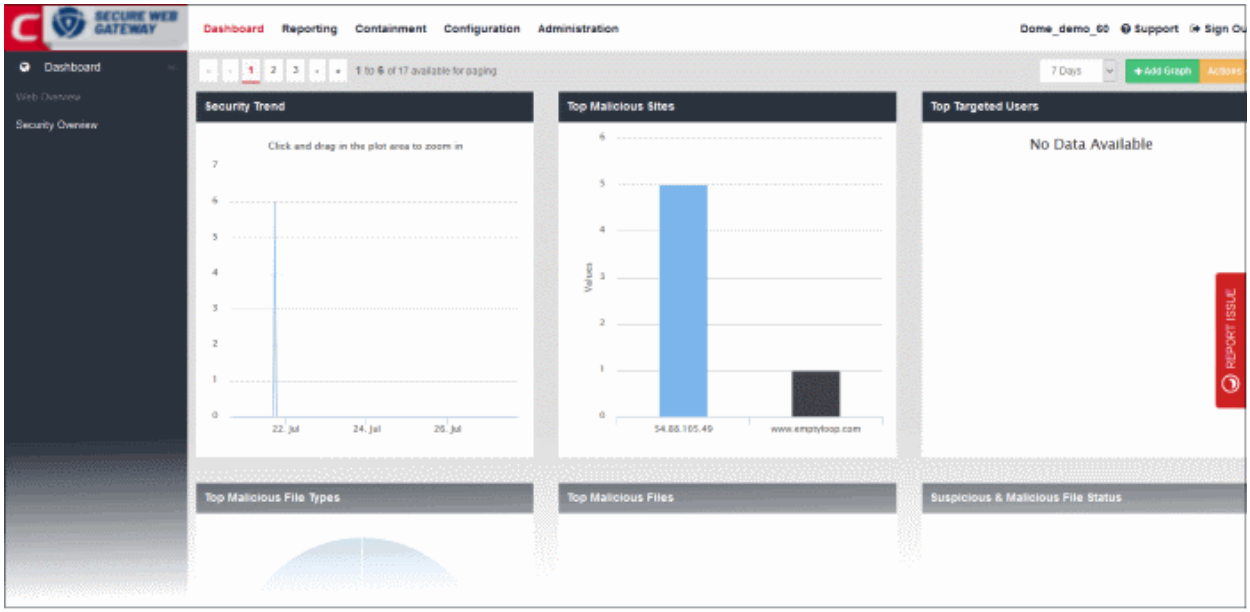
Shows the file types that were most often downloaded by users in the networks in your organization. The results are displayed for the top 10 file types. The X-axis displays the name of the file type and the Y-axis displays the number of file types that were downloaded. Placing your mouse cursor over a bar will display further details.



- Click a bar in the chart to open the 'View Logs' screen which contains more details. You can filter the details according to your needs. See '**View Web Overview Dashboard Logs**' for more details.

Security Overview

- To open the 'Security Overview' section, click 'Dashboard' then 'Security Overview' on the left.



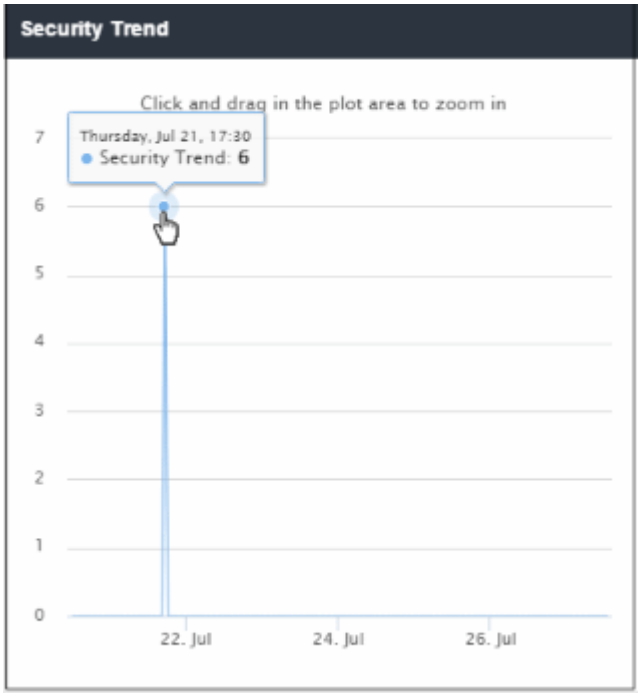
The 'Security Overview' dashboard section ships with a set of default tiles. Refer to the following for more details about each tile:

- **Security Trend**
- **Top Malicious Sites**
- **Top Targeted Users**
- **Top Malicious File Types**
- **Top Malicious Files**
- **Suspicious & Malicious File Status**
- **Top Sandboxed Files**
- **Wrapped Files**
- **Top Wrapped File Sources**
- **Executable File Downloaders**
- **Incidents Over Users**
- **Malicious Files**
- **Top Malicious File Sources**
- **Blacklisted Domains**
- **Top Blacklist Domain Access Sources**
- **Suspicious & Malicious Domains**
- **Top Suspicious & Malicious Access Sources**

Security Trend

The 'Security Trend' tile shows sites from which malicious files were blocked. The X-axis displays the date/time of the

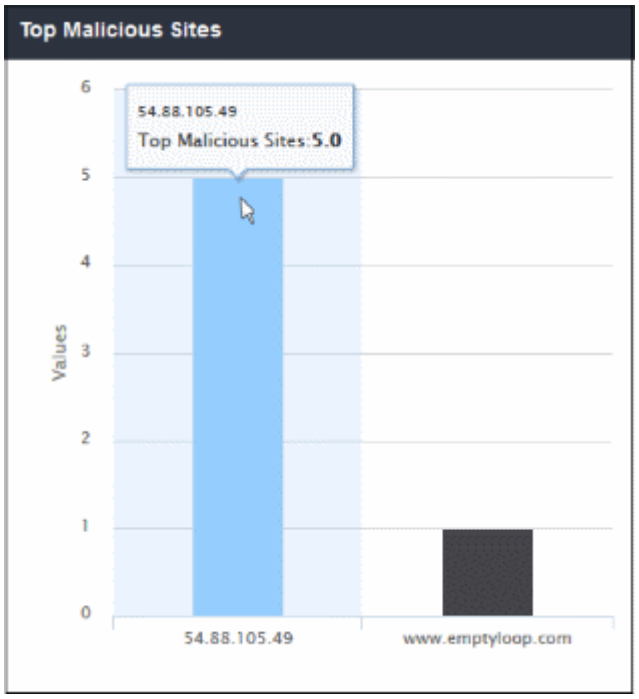
event and the Y-axis displays the number of blocked files. The results are displayed for the latest 5 events. Placing the mouse cursor over a point will display further details.



- To view full details for a particular period in the chart, click and drag to zoom the plot. Click 'Reset Zoom' to return to the full chart. Clicking on a particular point on the chart will open the 'View Logs' screen displaying full details of the sites, blocked file names, file hash and signature. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Malicious Sites

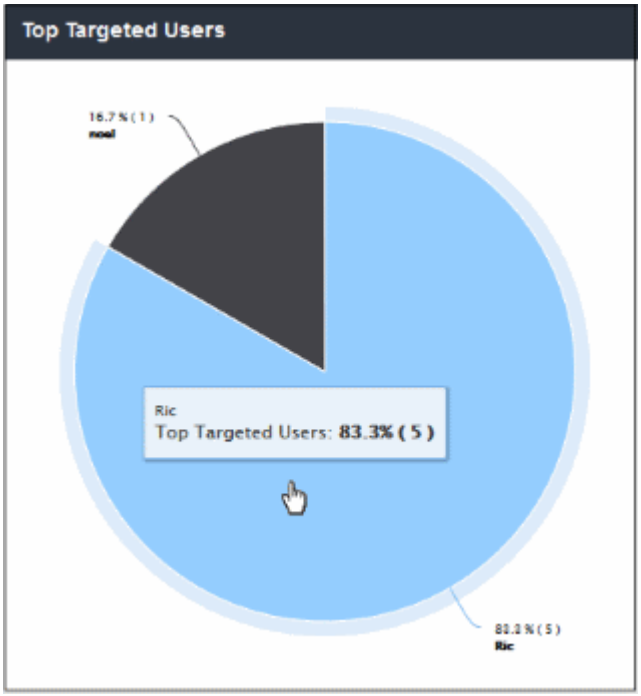
'Top Malicious Sites' shows which malicious sites were most often visited. The results are displayed for the top 10 malicious sites. The X-axis displays the name / IP of the malicious website and the Y-axis displays the number of malicious files that ware blocked for each site. Placing your mouse cursor over a bar will display further details.



- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the malicious sites. You can filter the details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Targeted Users

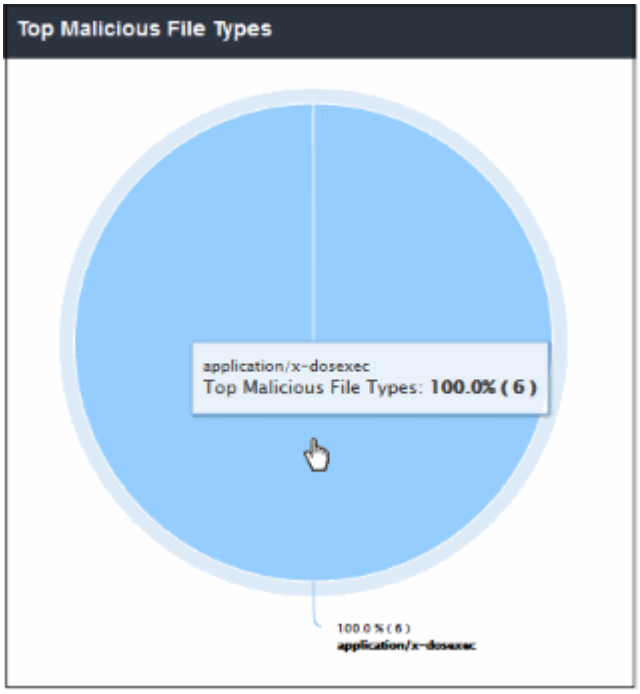
'Top Targeted Users' shows users who tried to download the highest quantities of malicious files. Placing your mouse cursor over a sector will display further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays full details of the top targeted users. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Malicious File Types

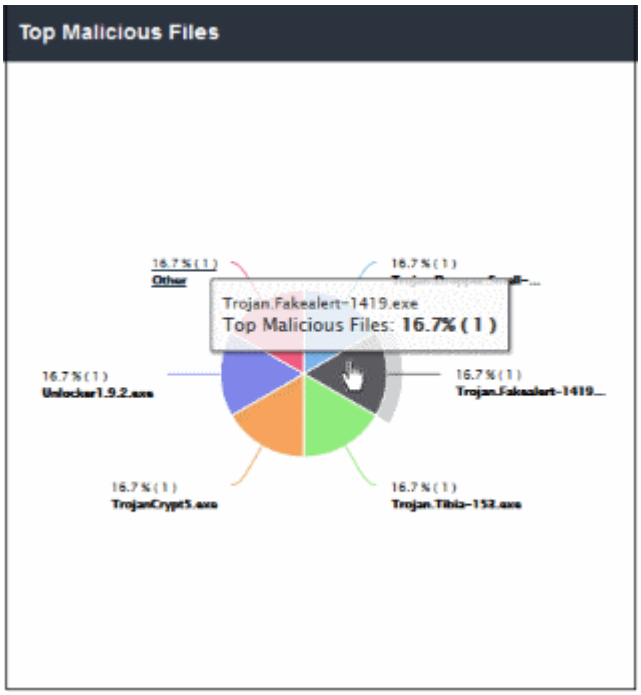
'Top Malicious File Types' shows which malicious file extensions were most often detected on your network. The results are displayed for the top 10 file types. Placing your mouse cursor over a sector will display further details.



- Clicking a particular sector on the chart will open the 'View Logs' screen which displays more details on these files. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Malicious Files

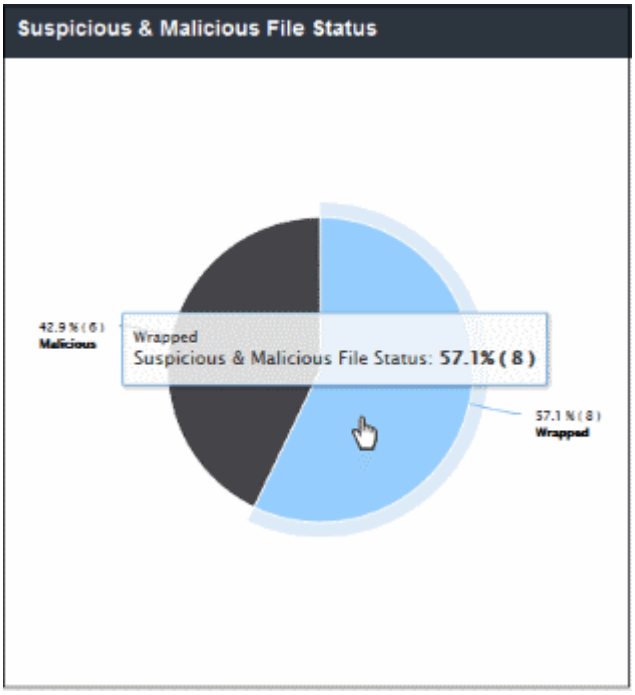
'Top Malicious Files' shows the names of those malicious files which were most often blocked by Comodo SWG. The results are displayed for the top 10 malicious files. Placing your mouse cursor over a sector will display further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays full details of top malicious files. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Suspicious & Malicious File Status

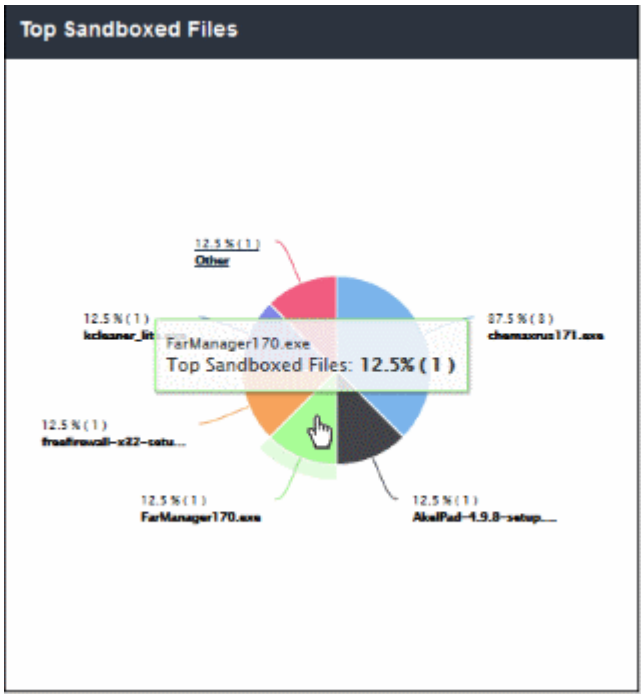
'Suspicious & Malicious File Status' shows malicious files which were blocked and files which were classified as suspicious and therefore sandboxed. The results are displayed for the top 10 file statuses. Placing your mouse cursor over a sector will display further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays the statuses of suspicious and malicious files. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Sandboxed Files

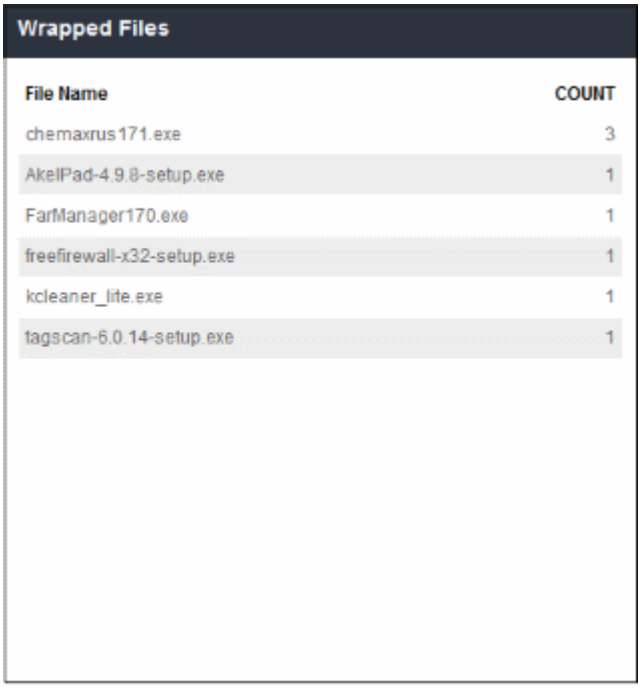
'Top Sandboxed Files' displays suspicious files which were most often placed in a secure sandbox environment. The results are displayed for the top 10 sandboxed files. Placing your mouse cursor over a sector will display further details.



- Clicking on a particular sector on the chart will open the 'View Logs' screen which displays the details of sandboxed files. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Wrapped Files

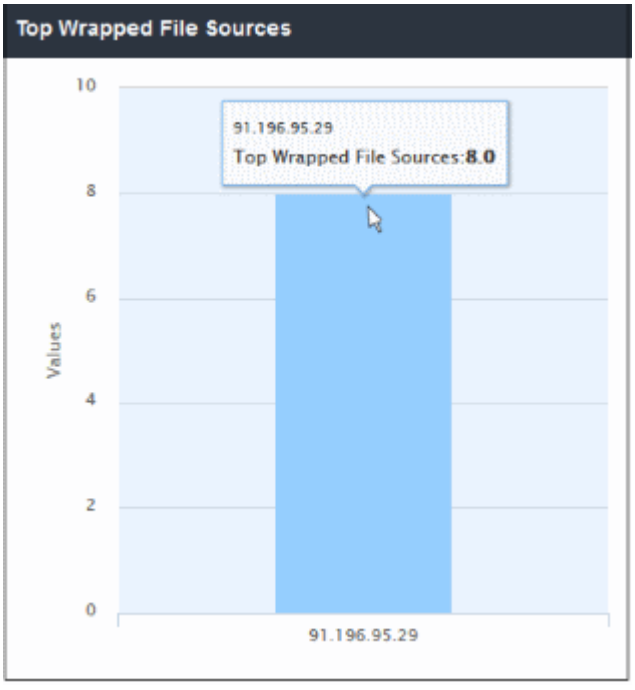
The details displayed here is same as explained in '**Top Sandboxed Files**' section, except here it is shown in tabular form for the top 50 results.



- Clicking on a particular row on the table will open the 'View Logs' screen which displays more details about sandboxed files. You can filter details according to your needs. See **View Security Overview Dashboard Logs**' for more details.

Top Wrapped File Sources

Shows which IP's were responsible for providing the most files which had to be sandboxed. The results are displayed for the top 10 file sources. Place your mouse cursor over a bar to view more information. The X-axis displays the source details and the Y-axis displays the number of files that are placed in sandbox.

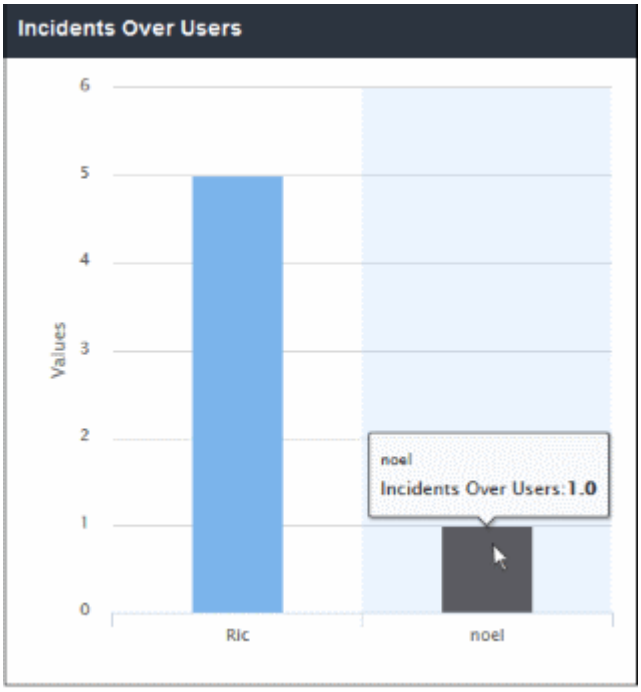


- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of sources from where the suspicious were downloaded. You can filter the details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Executable File Downloaders

'Executable File Downloaders' shows which users most often downloaded executable files from websites.

Incidents Over Users

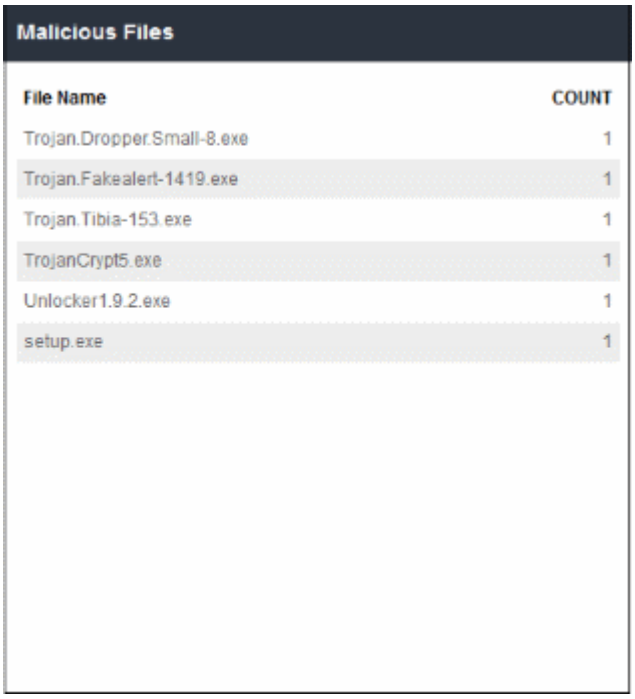


'Incidents Over Users' shows which users tried to download the most malicious files. This is same as the 'Top Targeted Users' tile. The results are displayed for the top 10 users. Placing your mouse cursor over a bar will display further details.

- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of the incidents by the user such as URL of the download site, file type and so on. You can filter the details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Malicious Files

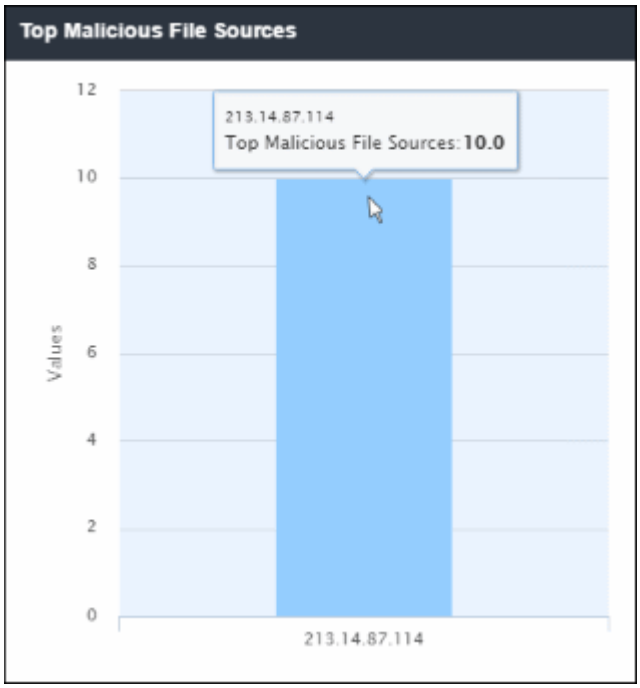
'Malicious Files' shows files that were determined as malicious and blocked by SWG. This is same as the 'Top Malicious' Files' tile, except here the details are provided in tabular form and displays results for the top 50 files.The URL of the web pages of the domain including port number.



- Clicking on a particular row on the table will open the 'View Logs' screen which shows more details about the malicious file. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Malicious File Sources

'Top Malicious File Sources' shows IP's which were responsible for providing the highest quantity of blocked, malicious files. The results are displayed for the top 10 file sources. Placing your mouse cursor over a bar will display further details. The X-axis displays the source details and the Y-axis displays the number of blocked files.



- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of sources from where the malicious files were tried to be downloaded. You can filter the details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

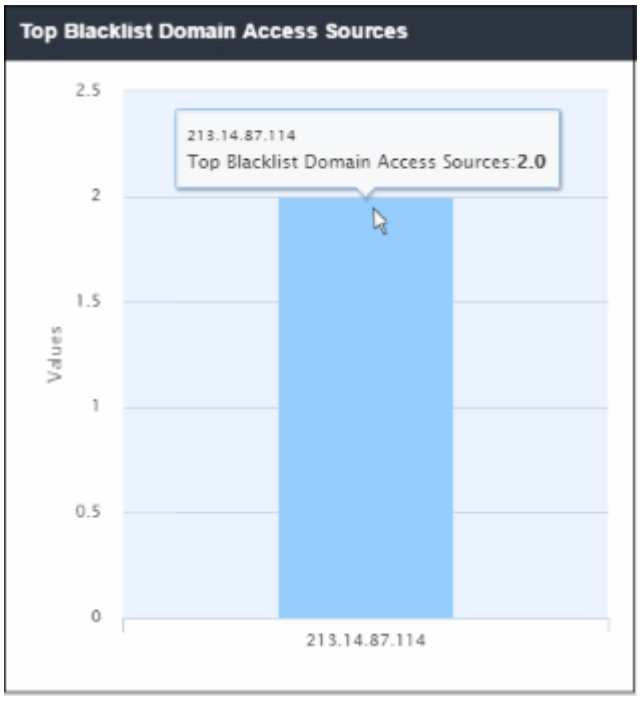
Blacklisted Domains

'Blacklisted Domains' shows the list of blacklisted domains that were added in Advanced Threat Protection settings from where users tried to download files. The table displays the results for the top 50 blacklisted domains.

- Clicking on a particular row on the table will open the 'View Logs' screen which displays the details of files that were tried to be downloaded. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Blacklist Domain Access Sources

'Top Blacklist Domain Access Sources' shows the IP details of sources that most often tried to download files from blacklisted domains. The results are displayed for the top 10 access sources. Placing your mouse cursor over a bar will display further details. The X-axis displays the source details and the Y-axis displays the number of blocked files.



- Clicking a particular bar on the chart will open the 'View Logs' screen displaying full details of sources from where the files were tried to be downloaded from blacklisted domains. You can filter the details according to

your needs. See '**View Security Overview Dashboard Logs**' for more details.

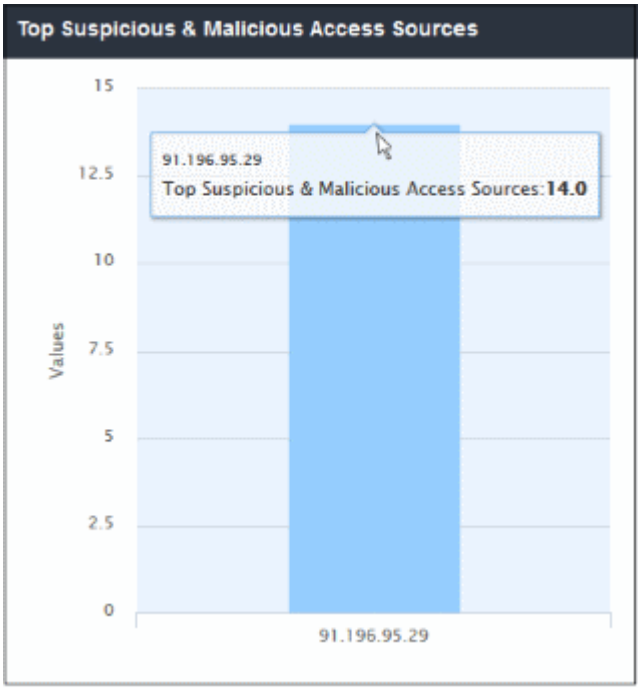
Suspicious & Malicious Domains

- Domains from which users most often attempted to download suspicious or malicious files
- The table displays the results for the top 50 domains.

- Click a particular row on the table to open the 'View Logs' screen. This displays details of the files that users attempted to download. You can filter details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

Top Suspicious & Malicious Access Sources

- The IP addresses which made the most attempts to download files from suspicious/malicious domains.
- The results are displayed for the top 10 sources. Placing your mouse cursor over a bar will display further details. The X-axis displays the source details and the Y-axis displays the number of blocked files.

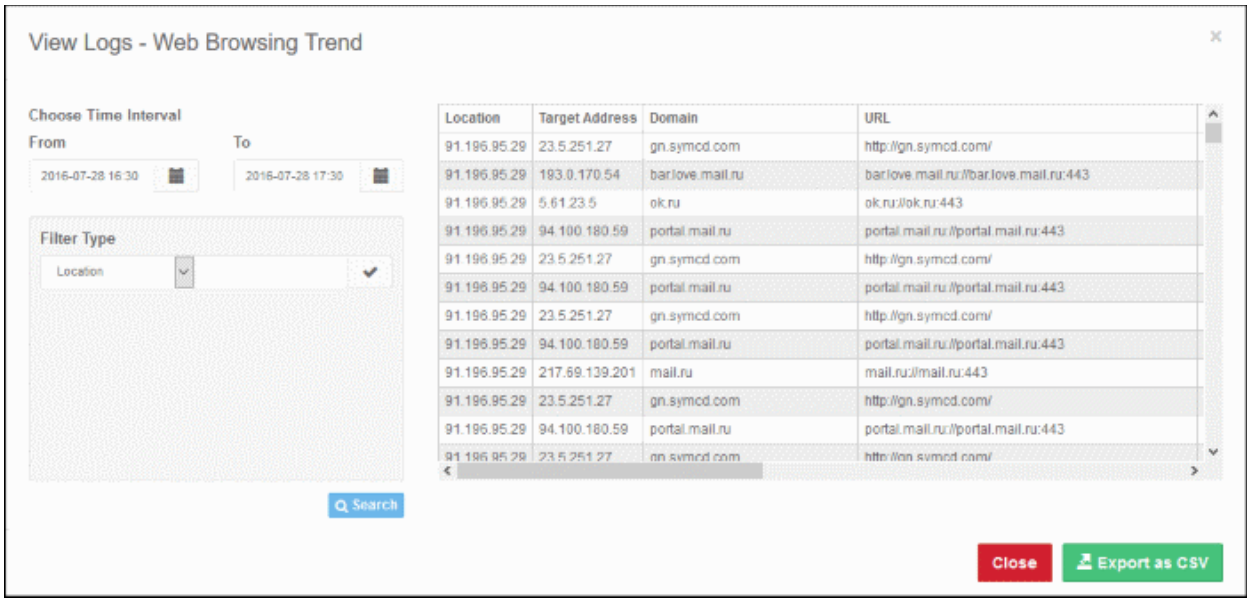


- Click a specific bar on the chart will open the 'View Logs' screen displaying full details of sources from where the files were tried to be downloaded from suspicious/malicious domains. You can filter the details according to your needs. See '**View Security Overview Dashboard Logs**' for more details.

View Web Overview Dashboard Logs

- Click a segment or bar in Web Overview dashboard chart to view more detailed information about the respective activity.

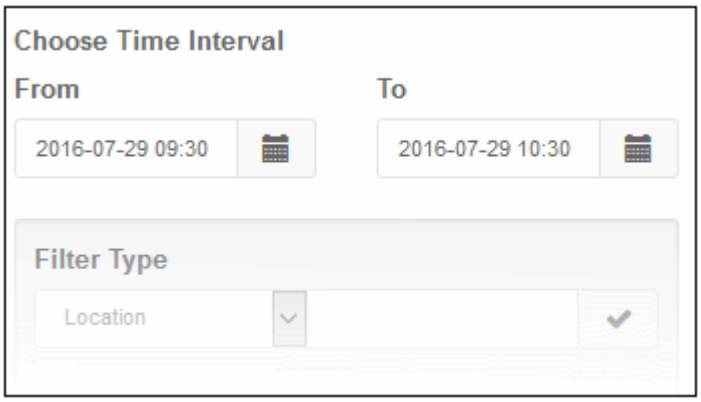
The log includes destination website, the network from which the event occurred, the website category, what action was taken and the reason for the action and more. The log view also allows you to choose the time period for which you want to view the logs. You can filter logs using the fields on the left. The example below shows the 'Web Browsing' log:



View Web Overview Dashboard Logs - Table of Column Descriptions	
Column Header	**Description**
Time	Date and time the log was generated for the event.
Location	The IP of the network from which the traffic originated.
Target Address	The IP address of the destination site.
Domain	The destination domain name.
URL	The URL of the web pages of the domain including port number.
Status	Action taken by SWG, whether allowed or blocked.
Message	The reason for the action taken, for example if the web site belongs to an allowed category.
User	The name of the end user from whose endpoint the traffic originated.
Country	The name of the country where the website is hosted.
Category	The category of the website determined by SWG.
Sub-category	The sub-category of the website as determined by SWG.
Internal IP	The local IP of the endpoint.
Computer Name	The name of the endpoint from which the traffic originated.

Selecting time interval

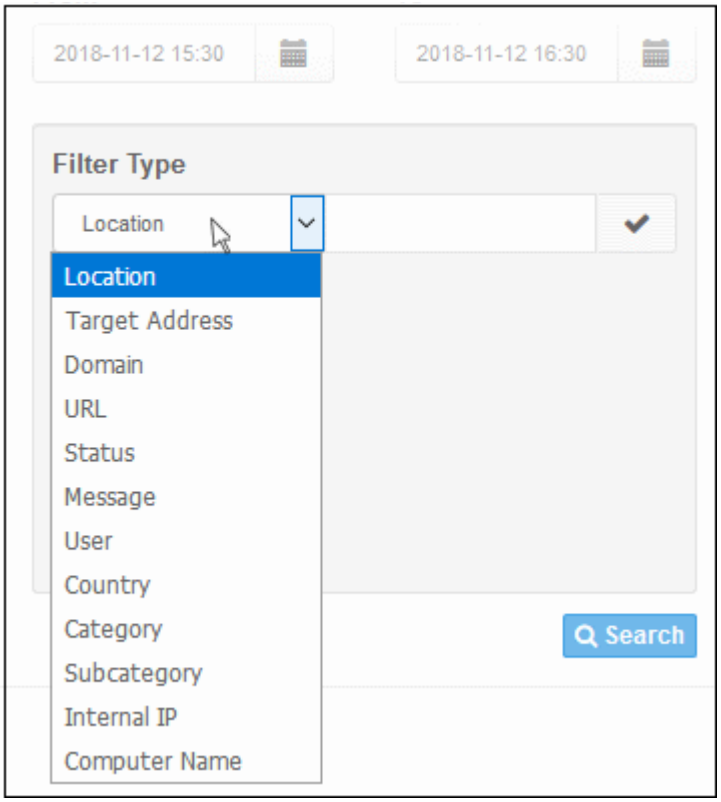
The log is displayed for the area at which you clicked on the graph. You can change the date and time for the log view from the 'Choose Time Interval' section.



- To change the period, click the calendar icon and select the 'From' and 'To' dates or enter the period directly in the fields.
- To change the time, enter the 'From' and 'To' time in the respective fields beside the date.

Filtering option

The 'Filter Type' section allows you to filter logs as required. You search logs by a single criteria or group them for more specific results.

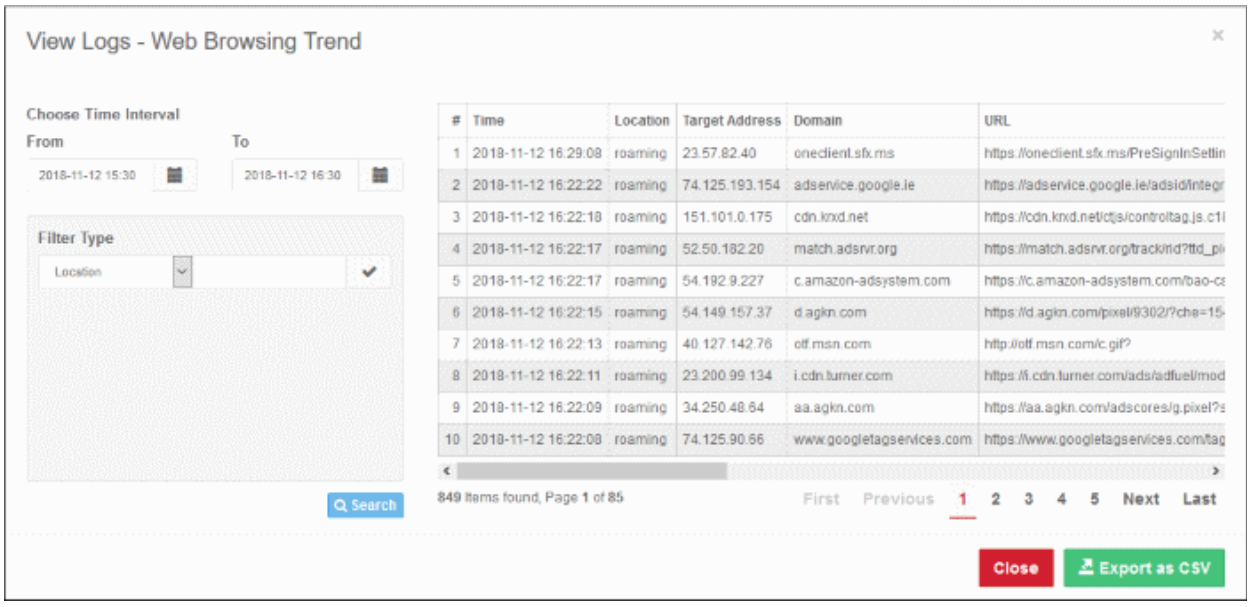


The filtering types available are: Location, Target Address, Domain, URL, Status, Message, User, Country, Category, Subcategory, Internal IP and Computer Name.

- To filter the log according to a type, select it from the 'Filter Type' drop-down, enter the relevant search text and click the check mark to run the search. The filtering type will be added and displayed.

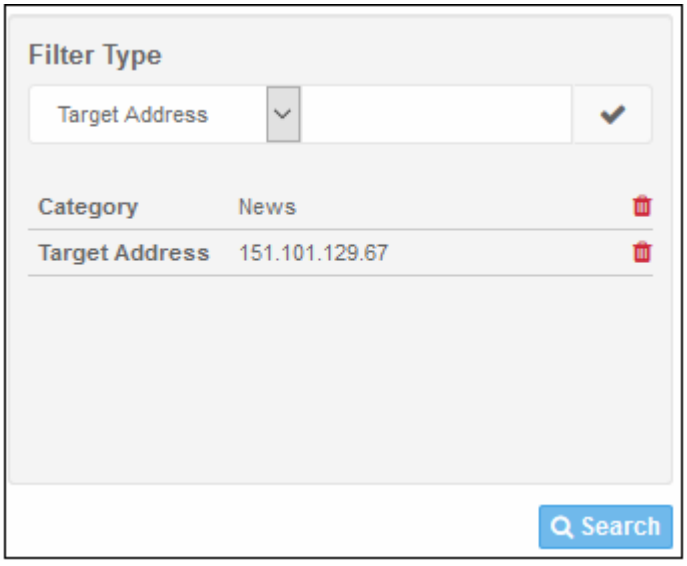
- Click the 'Search' button below to filter the log according to the entered criteria.

The log data for the entered filter criteria will be displayed:



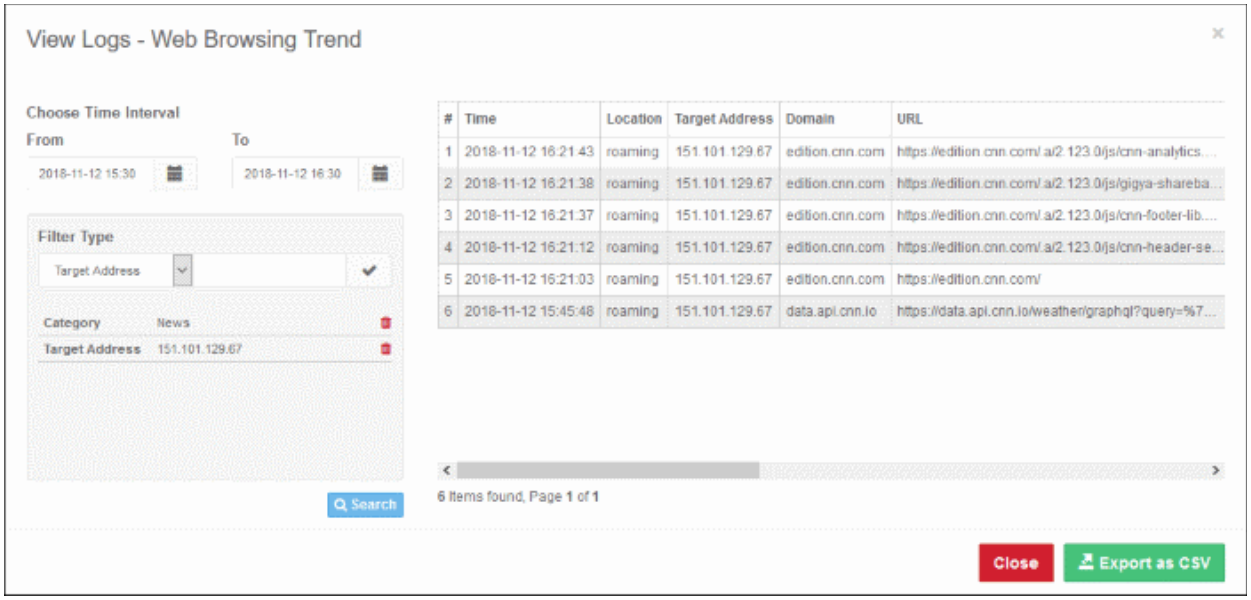
You can also group filters for more detailed search.

- To filter the log by multiple criteria, select the filtering types one by one, enter the relevant search criteria and click the check mark beside it.



- Click the 'Search' button below to filter the log according to the entered criteria.

The log data for the entered filter criteria will be displayed:

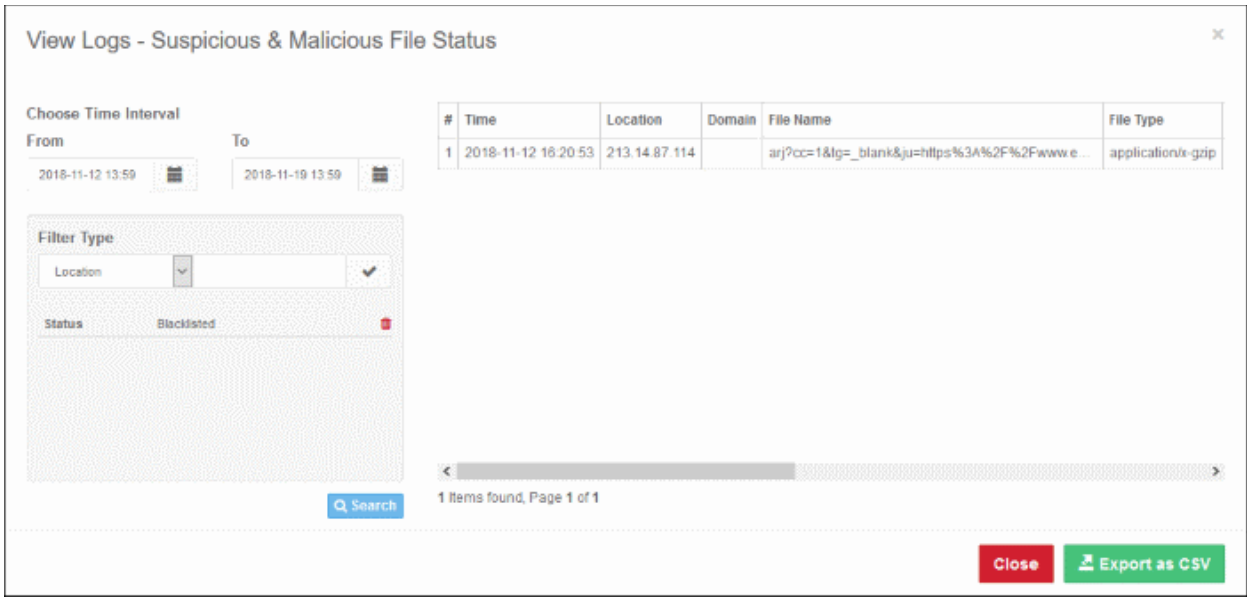


- Click 'Export as CSV' to save the log in CSV format for future reference.
- To view all the entries again, delete the filter types by clicking the trash can icon beside them and clicking the 'Search' button again.
- Click 'Close' to return to 'Dashboard'

View Security Overview Dashboard Logs

- Click a segment, bar or a table row in a Security Overview dashboard chart to view more detailed information about the activity.

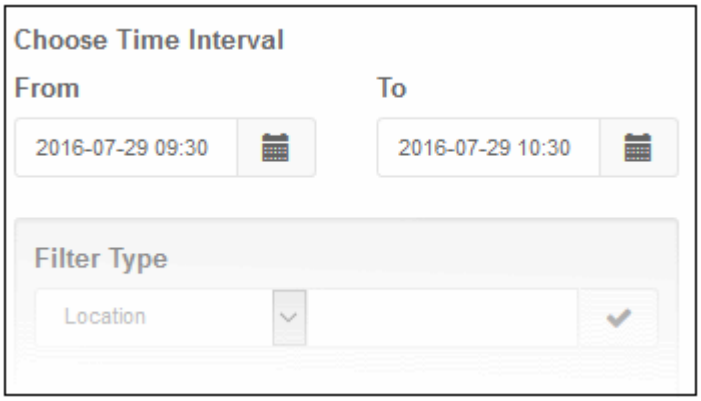
The log includes IP of network from which the event occurred, the domain name, file name, file type and more. The log view also allows you to choose the time period for which you want to view the logs. You can filter logs using the fields on the left. The example below shows the 'Suspicious & Malicious File Status' log:



View Security Overview Dashboard Logs - Table of Column Descriptions	
Column Header	**Description**
Time	Date and time the log was generated for the event.
Location	The IP of the network from which the traffic originated.
Domain	The destination domain name.
File Name	The name of the file that was attempted to be downloaded.
File Type	The extension type of the malicious/suspicious file.
URL	The URL of the web pages of the domain including IP details
File Hash (SHA1)	The SHA1 hash value of the file.
User	The name of the end user from whose endpoint the file was attempted to be downloaded.
Status	Action taken by SWG, whether blacklisted or wrapped (contained).
Internal IP	The local IP address of the endpoint.
Computer Name	The name of the endpoint from which the traffic originated.

Selecting time interval

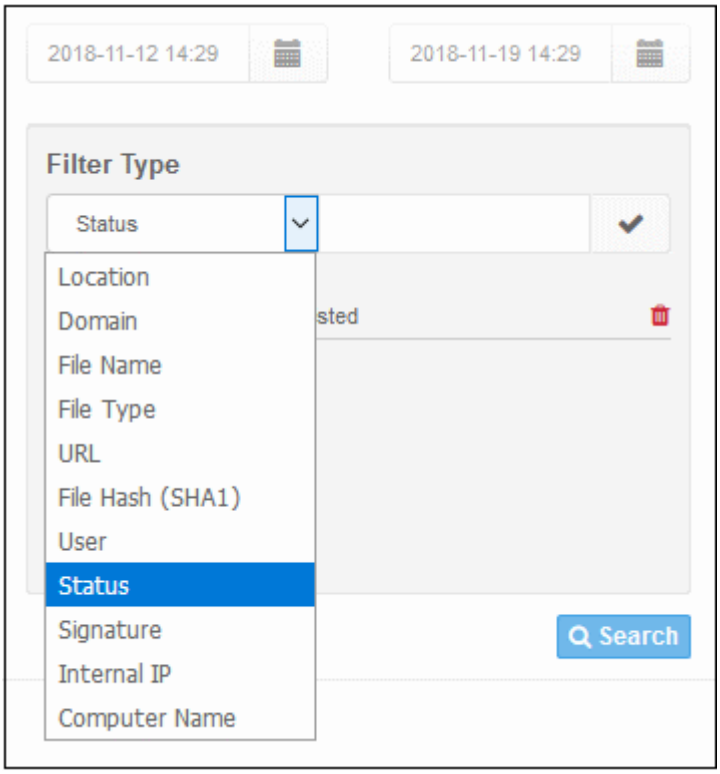
The log is displayed for the area at which you clicked on the graph. You can change the date and time for the log view from the 'Choose Time Interval' section.



- To change the period, click the calendar icon and select the 'From' and 'To' dates or enter the period directly in the fields.
- To change the time, enter the 'From' and 'To' time in the respective fields beside the date.

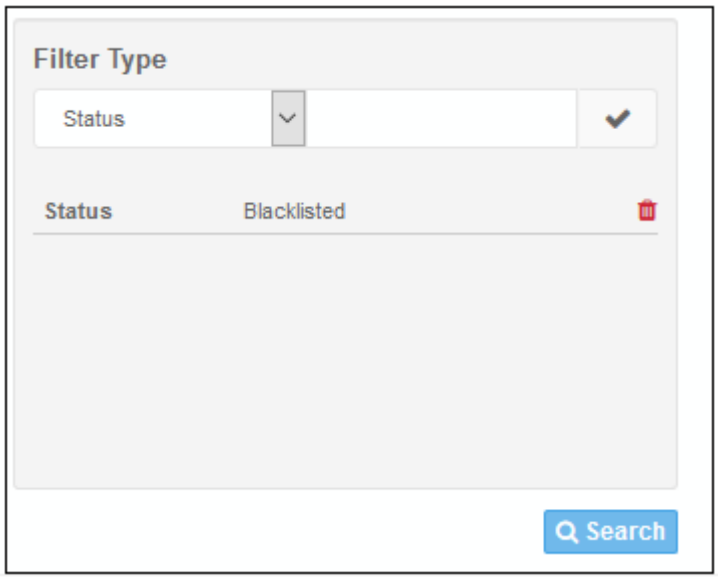
Filtering option

The 'Filter Type' section allows you to filter logs as required. You search logs by a single criteria or group them for more specific results.

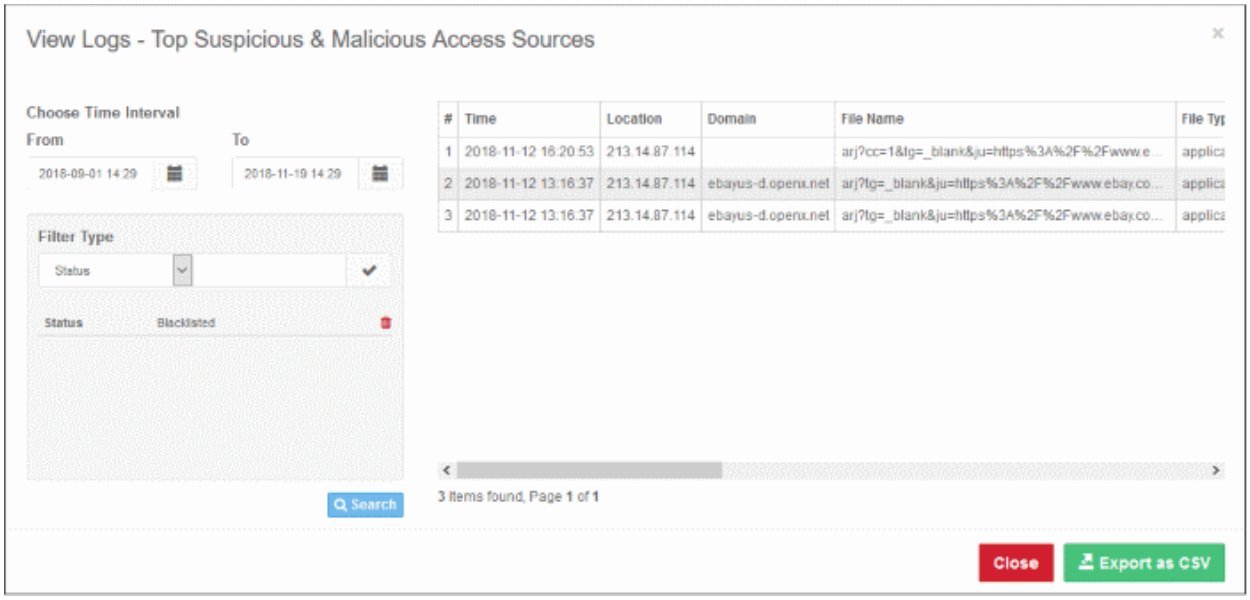


The filtering types available are: Location, Domain, File Name, File Type, URL, File Hash (SHA1), User, Status, Signature, Internal IP and Computer Name.

- To filter the log according to a type, select it from the 'Filter Type' drop-down, enter the relevant search text and click the check mark to run the search. The filtering type will be added and displayed.



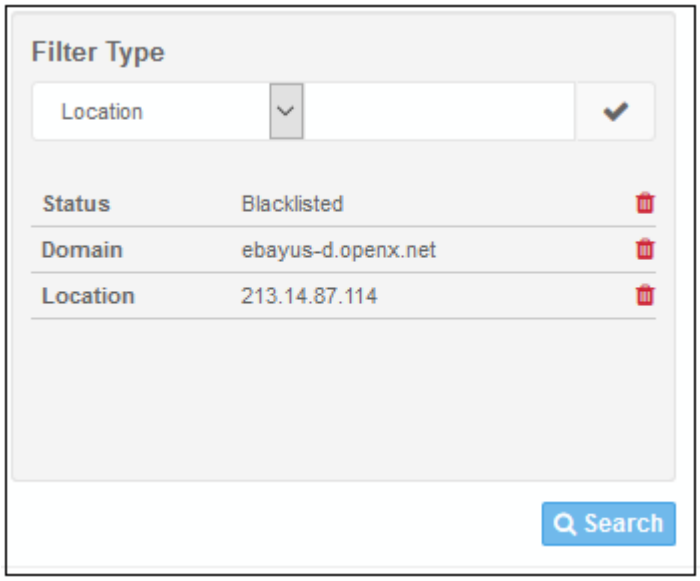
- Click the 'Search' button below to filter the log according to the entered criteria.



The log data for the entered filter criteria will be displayed:

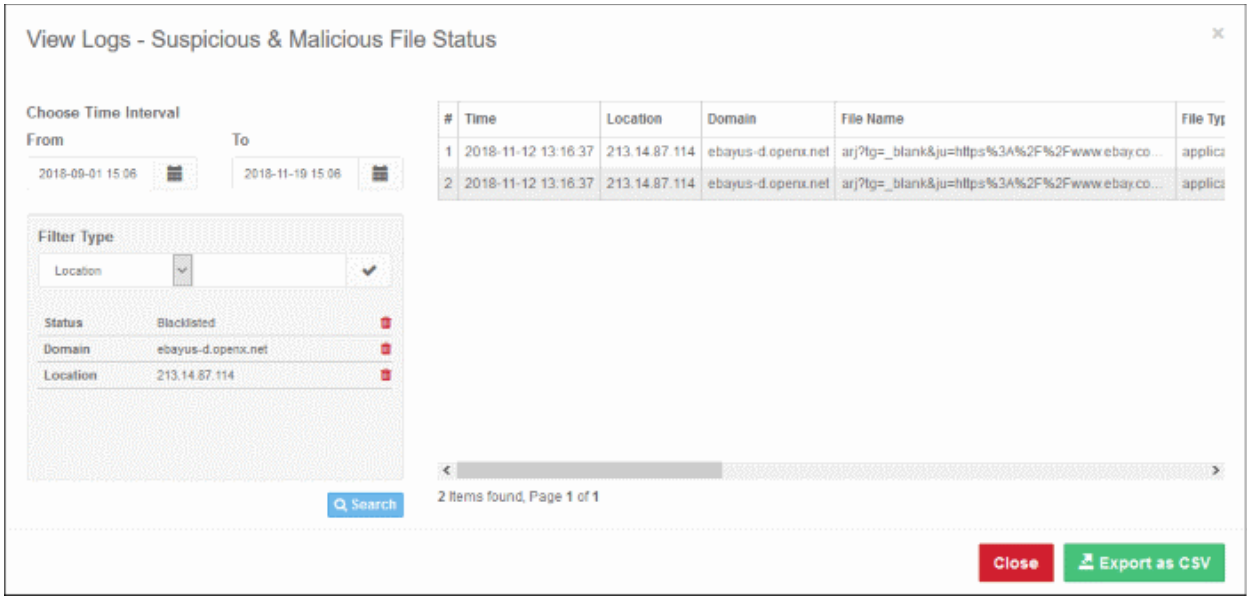
You can also group filters for more detailed search.

- To filter the log by multiple criteria, select the filtering types one by one, enter the relevant search criteria and click the check mark beside it.



- Click the 'Search' button below to filter the log according to the entered criteria.

The log data for the entered filter criteria will be displayed:

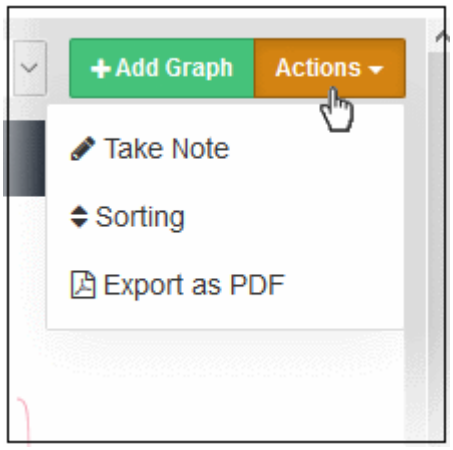


- Click 'Export as CSV' to save the log in CSV format for future reference.
- To view all the entries again, delete the filter types by clicking the trash can icon beside them and clicking the 'Search' button again.
- Click 'Close' to return to 'Dashboard'

Taking notes, sorting and exporting

The 'Actions' button on the top right of the dashboard allows you to create notes, re-order the dashboard tile layout and export the dashboard to PDF.

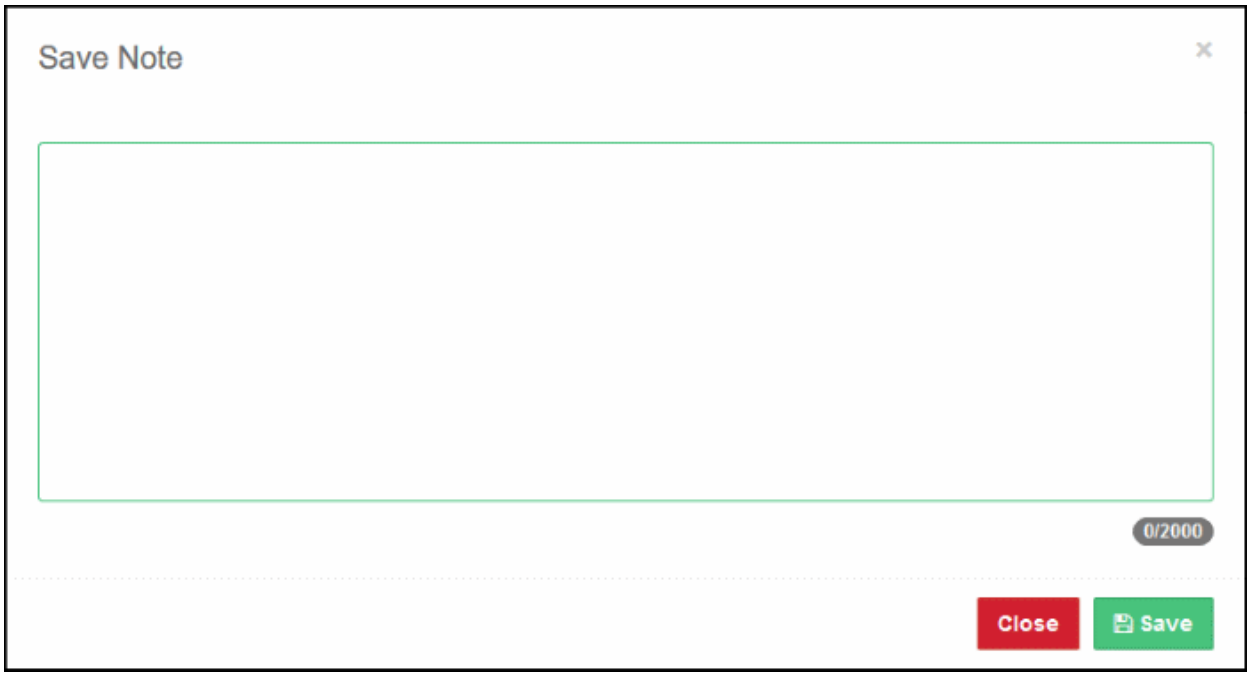
- Click the 'Actions' button on the top right



Keep a note in the dashboard

- Click 'Take Note'

The 'Save Note' dialog will be displayed. You can enter a maximum of 2000 characters in the note.



- Please note you can record only one note. After a note is saved, the drop-down for the note under 'Actions' will be displayed as 'Show Note'.
- To edit the note, click 'Show Note' under 'Actions', edit according to your requirements and click 'Save'.
- To remove a note, click 'Show Note' under 'Actions', delete the contents in the note and click 'Save'

Re-order the dashboard tile layout

- Click 'Sorting' under 'Actions'

The 'Sorting' dialog will be displayed. The tiles displayed depends on the dashboard type selected, either Web Overview or Security Overview. The following shows the Security Overview tiles.

Each tile's current position is indicated by a number at the right of each tile.

- To re-order the layout, click, drag and place the bar as per your requirements.
- Click 'Save'.

The layout of the dashboard tiles will be changed. Please note that you can also re-order the custom tiles that you have added. See '**Customizing the Dashboard**' to know about how to create new tiles.

Export the dashboard as PDF

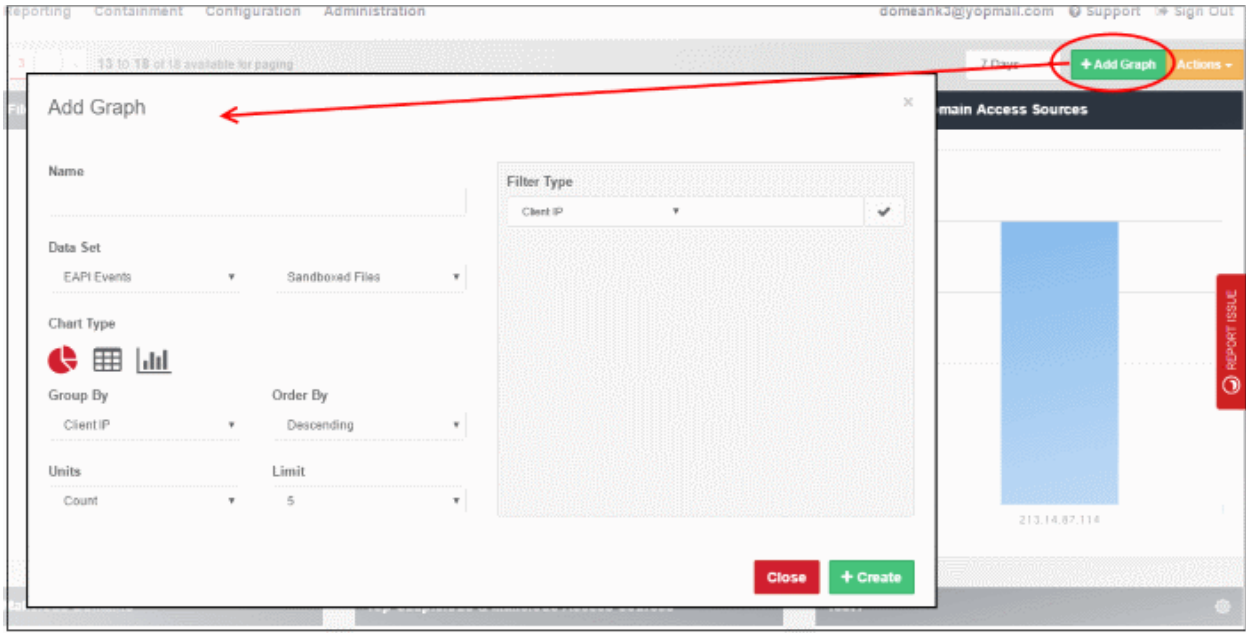
- Click 'Export as PDF' under 'Actions'

The export process will be begin and the dashboard will be stored in PDF format for your future reference.

3.1 Customize the Dashboard

The default tiles in the dashboards cannot be edited or deleted. However, you can create new dashboard tiles according to your requirements. Once created, custom dashboard tiles will be available along with the default tiles. Custom tiles can be edited and removed if no longer needed.

Click 'Dashboard' > 'Add Graph' to create a new tile:

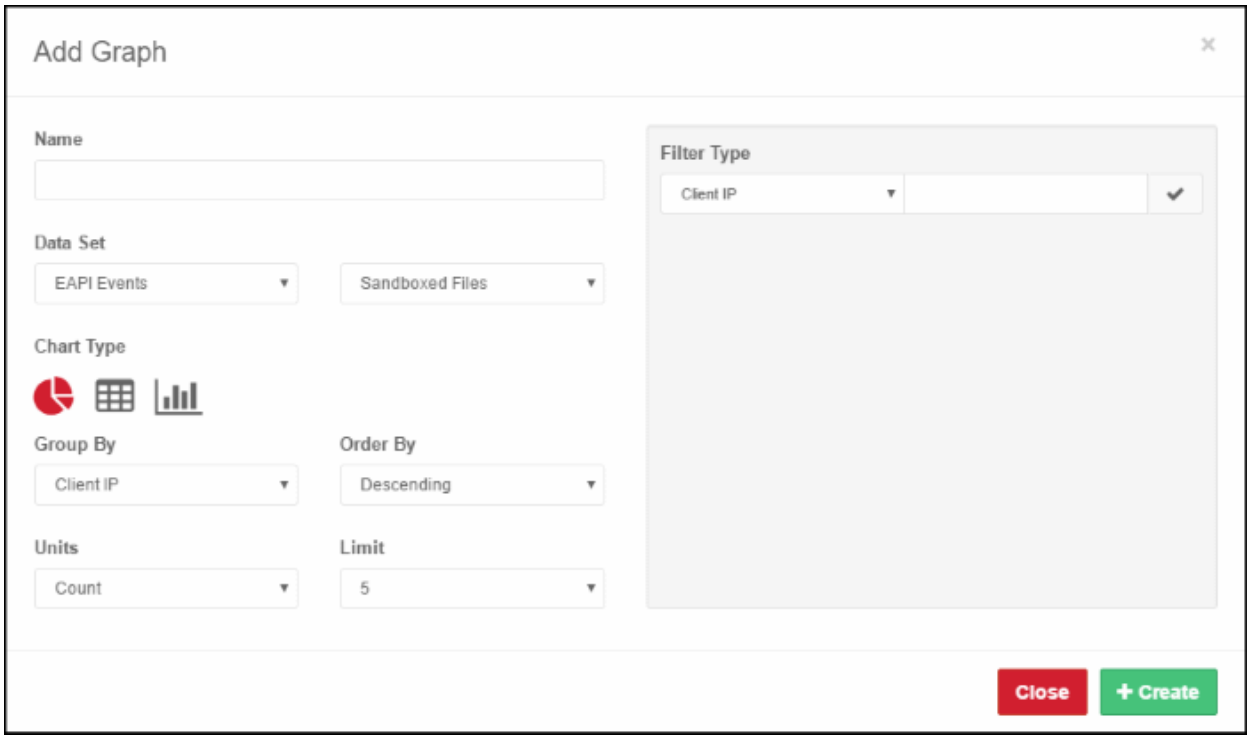


Add Graph Dialog - Table of Column Descriptions	
Parameter	**Description**
Name	The label of your custom tile.
Data Set	Allows you to select the data set and relevant data type to create the custom tile. The data sets available are: • EAPI Events (Data from endpoints that has contained file running) • Security Events (Data related to security policies) • Web Access Events (Data related to web content policies) The data category available in the second drop-down depends on the selected event type in the first drop-down.
Chart Type	Select the chart type. The options are pie chart, bar chart and table.
Group By	Select the parameter by which data in the tile should be organized. The available parameters depend on the selected event type. For 'EAPI Events', the options available are: Client IP, SHA1 and File Name. For 'Security Events' the options are: Location, Domain, File Name, File Type, URL, File

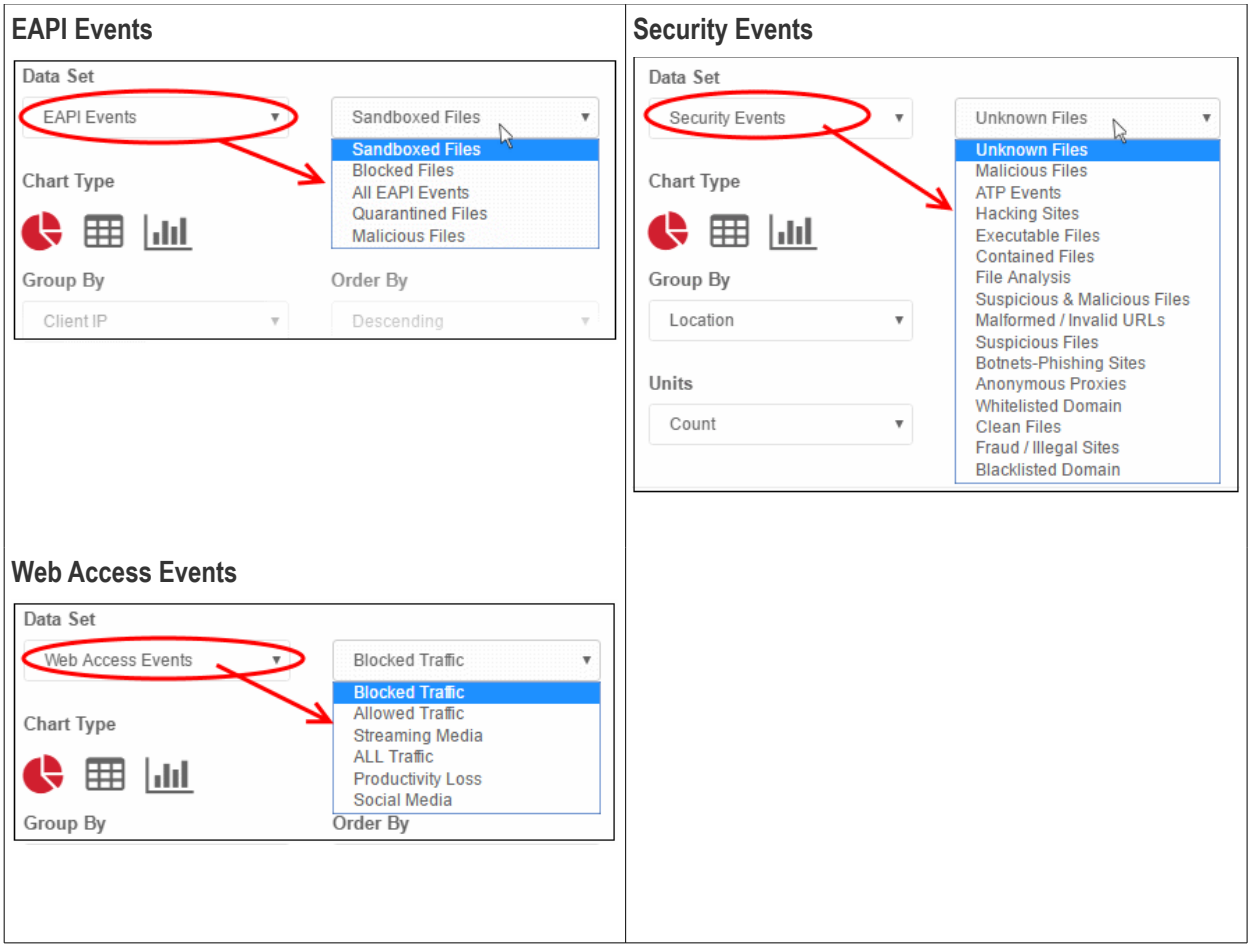
	Hash (SHA1), User and Signature. For 'Web Access Events', the options are: Location, Target Address, Domain, URL, Status, Message, User, Category, Subcategory and Country.
Order By	Select whether the data in the tile should be in ascending or descending order.
Units	Indicates the unit of 'Limit' number.
Limit	Allows you to select how many 'Group By' parameters should be displayed in the chart. For example, if you have selected 'Web Access Events' and 'Blocked Traffic' as the 'Data Set', 'Category' in 'Group By', 'Descending' in 'Order By' and '5' in 'Limit', then the chart will display the five top blocked websites by category in descending order (highest number to lowest number of blocked websites).
Filter Type	Allows you to add filters to get more detailed log data. The filter types depend on the selected event type in the first drop-down.
Create Button	Click this button to add the configured tile to dashboard.
Close Button	Allows you to close the 'Add Graph' dialog.

Create a new custom dashboard tile

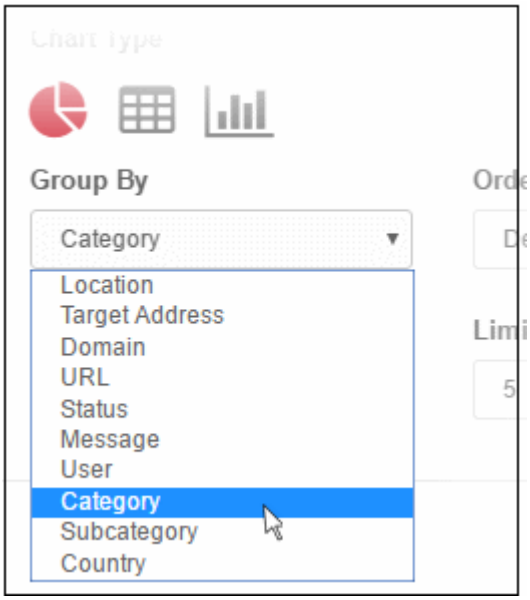
- Click the 'Add Graph' button



- **Name** - Enter an appropriate name for the custom dashboard tile
- **Data Set** - In the first drop-down, select event type. From the second drop-down, select the data category that you want use in the custom tile. The data category varies according to the event type.

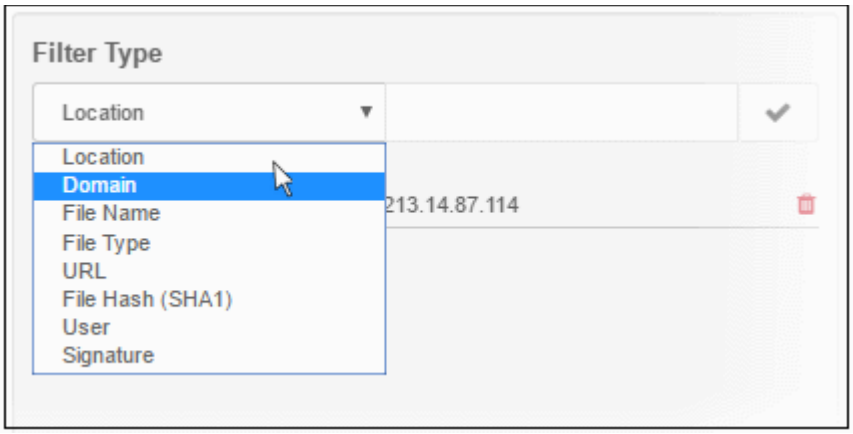


- **Chart Type** - Select the type of chart for the custom tile. The options available are pie chart, table and bar chart. The selected type will be highlighted in red.
- **Group By** - Select the parameter by which the chosen data set should be grouped.



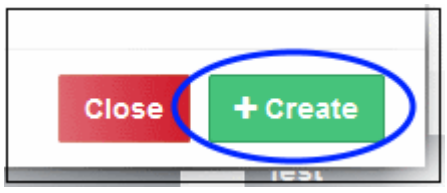
For example to view blocked websites in all networks by category, select 'Web Access Events' and 'Blocked Traffic' in 'Data Set' and 'Category' in 'Group By'.

- **Order By** - Select whether the data should be in ascending or descending order depending on the quantity specified in the 'Limit drop-down. For example, if you select '5' in Limit for 'Blocked Traffic' then 'Grouped By' as 'Category' and 'Order By' as 'Descending', then the chart will display the top 5 blocked categories from highest to lowest.
- **Units** - Select 'Count'. This is the unit for 'Limit' value.
- **Limit** - Choose the number of selected parameters in Data Set and Group By that should be displayed in the chart either from the top or bottom depending on the selection in 'Order By'. You can select from '5' to '50' from the drop-down.
- **Filter Type** - You can further filter the data to be displayed in the custom tile by adding filters here. For example, select 'Location' from the drop-down and enter the IP of the network in the next field and click the check mark button. The chart will display the data pertaining to that network only. The filters available depends on the data event selected in the first drop-down under 'Data Set'.

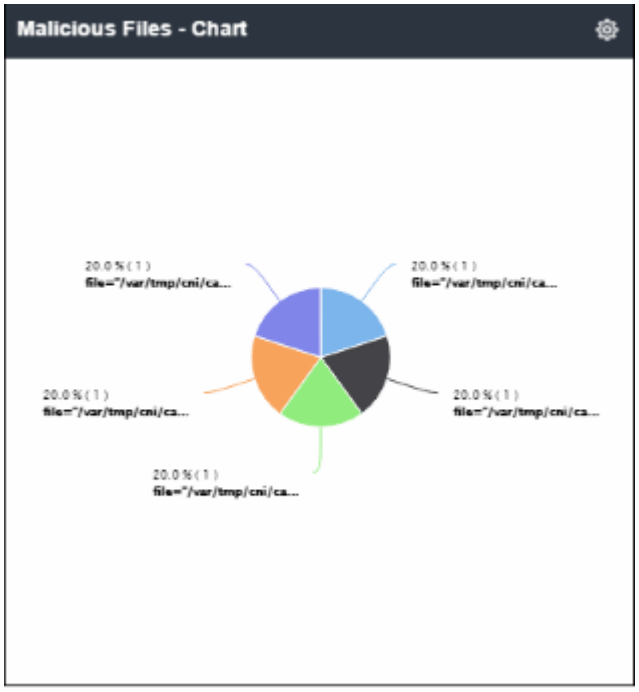


- You can add multiple filters to display drilled down data as per your requirement.

- To remove a filter, click the trash can icon beside it.
- Click the 'Create' button at the bottom of 'Add Graph' dialog after entering/selecting all the parameters.

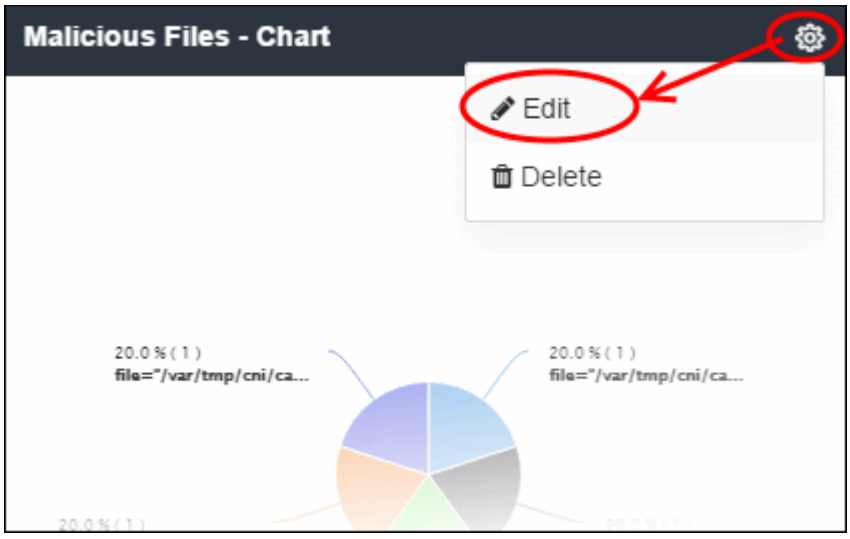


The custom tile will be created and added to the dashboard. The following example shows a custom pie chart tile added to display top 5 suspicious and malicious files detected and grouped by signature for all networks.

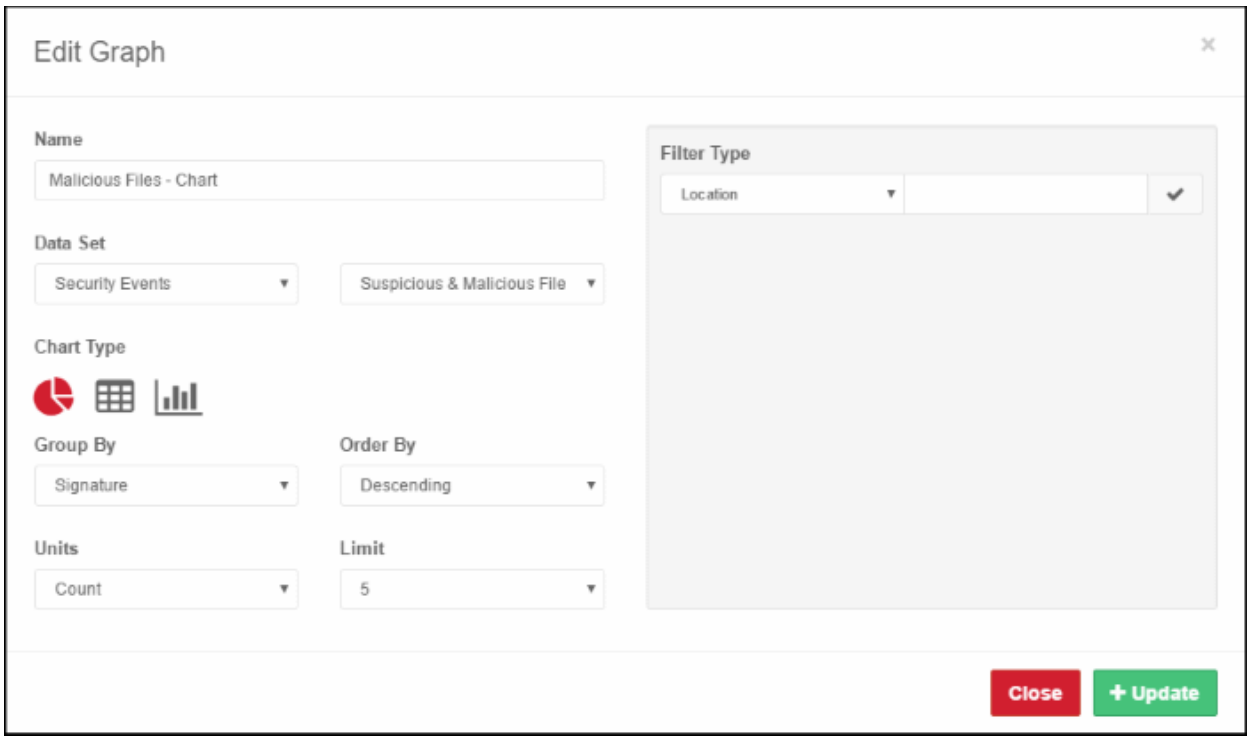


Edit a custom dashboard tile

- Click the settings icon at the top right of the custom tile and click 'Edit'. Please note the setting icon will be available only for custom tiles.



The 'Edit Graph' dialog will be displayed:

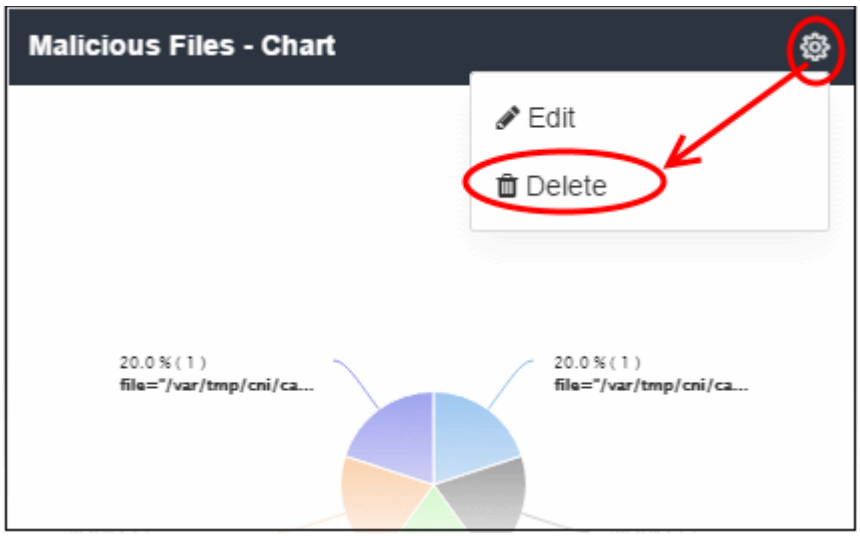


- Update the parameters as required. The process is similar to creating a new custom tile as explained **above**.
- Click the 'Update' button after editing the details.

The updated tile will be displayed in the dashboard.

Delete a custom dashboard tile

- Click the settings icon at the top right of the custom tile and click 'Delete'. Please note the setting icon will be available only for custom tiles.



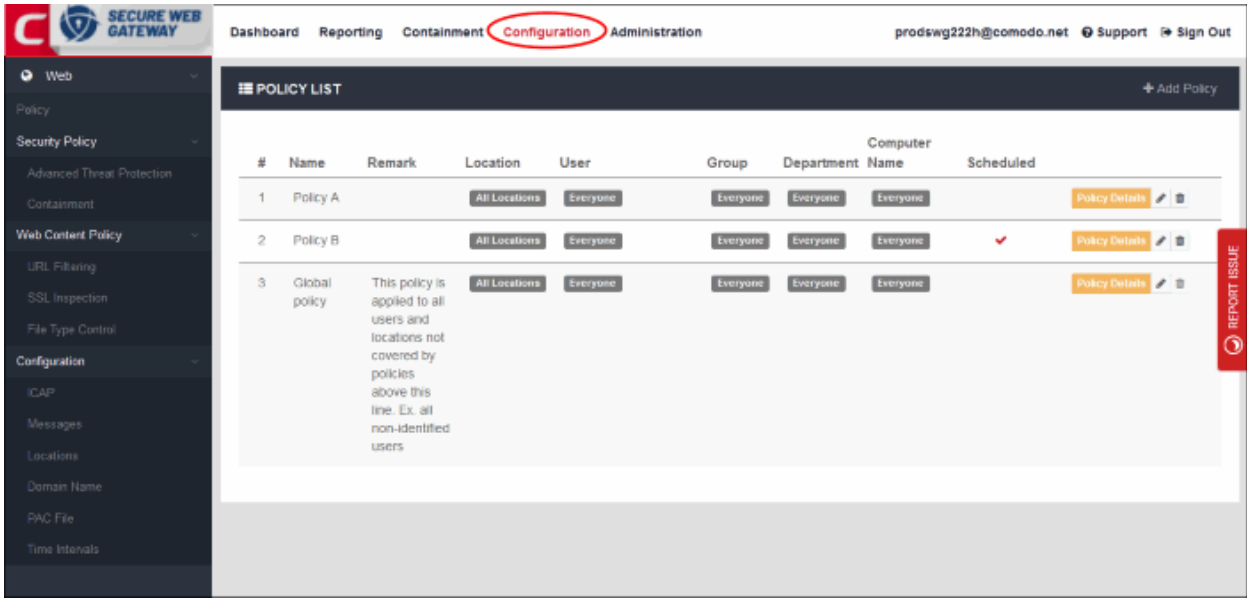
A confirmation dialog will be displayed.

- Click 'OK' to confirm removal of the tile from the dashboard.

4 Configure Comodo Secure Web Gateway

The 'Configuration' section lets you connect networks to Comodo SWG configure and deploy policies, and create SWG messages.

- Click 'Configuration' on the top-menu to open this area:



Please see the following for more details:

- **Connect your Network / Devices to Comodo Secure Web Gateway**
- **Configure SWG Messages**
- **Manage Policies**
- **Apply Policies to Networks**

4.1 Connect your Network / Devices to Comodo Secure Web Gateway

- You need to route your endpoint and network traffic through Comodo Secure Web Gateway (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 then you can just install the SWG agent on devices and deploy user 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 SWG will not function correctly and your network will not be able to connect to the internet. See '**Manage Trusted Networks**' for more details.

- 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.

4.1.1 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 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 Proxy' field, enter SWG IP <X.X.X.X> or Domain name and port number as 19080
- In the 'SSL Proxy' field, enter SWG IP <X.X.X.X> or Domain name and port number as 19443
- In the 'No Proxy for:' box 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 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 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.
- 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 SWG will not function correctly and your network will not be able to connect to the internet. See '**Manage Trusted Networks**' for more details.

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

4.1.2 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 Secure Web Gateway (SWG).
- 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 SWG is the upstream proxy.

1. Basic Chaining

Bluecoat > SWG

In this scenario, Bluecoat Proxy SG is forwarding requests to 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 'Forwarding' > '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: 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: 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 SWG will not function correctly. Your network will also not be able to connect to the internet.
- See '**Manage Trusted Networks**' for more details.
- 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.

4.1.3 Traffic Forwarding via Internet Content Adaptation Protocol (ICAP)

- Similar to the proxy chain scenario as explained in the **previous section**, ICAP integration is required when there is another ICAP client in the customer network.
- Like the chain scenario, traffic first comes to the network device and communicates with Comodo Secure Web Gateway (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.

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

Click 'Configuration' > 'Configuration' on the left then 'ICAP' to view the 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. '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 (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 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. Select 'ICAP' for user authentication and traffic forwarding.
  - 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 '**Manage Trusted Networks**' for more details.
- 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.

4.1.4 Traffic Forwarding via SWG Agent

Another method of forwarding traffic from endpoints to Comodo Secure Web Gateway (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. However, these devices can also be used in a protected network. **Network location** based policies will be applied to such devices.

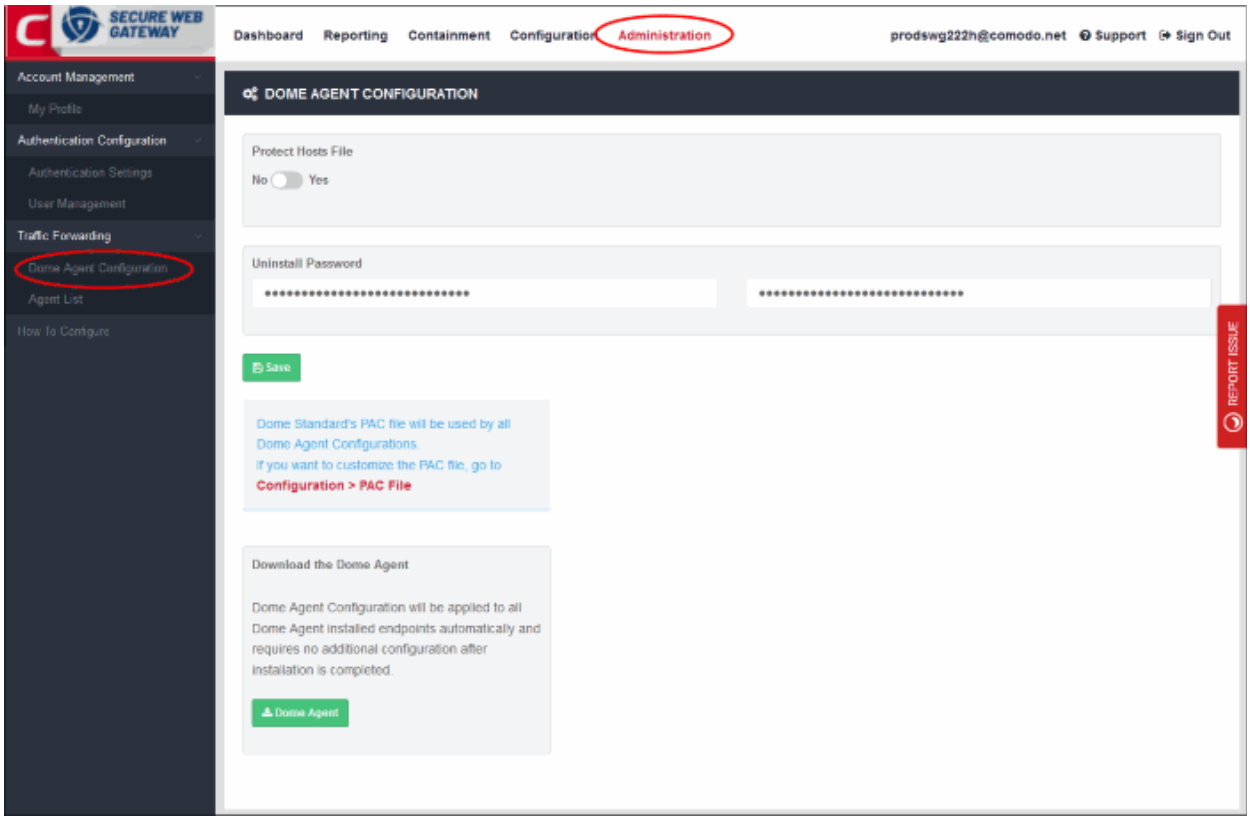
- Supports user specific policies deployment.
- Supports computer specific policies deployment
- There is no need to select any authentication and traffic forwarding option on the 'Locations' interface.
- See '**Connect your Roaming Devices to Comodo Secure Web Gateway**' for information about how to 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.

4.2 Connect your Roaming Devices to Comodo Secure Web Gateway

- Click 'Administration' > 'Traffic Forwarding' > 'SWG Agent Configuration'

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:

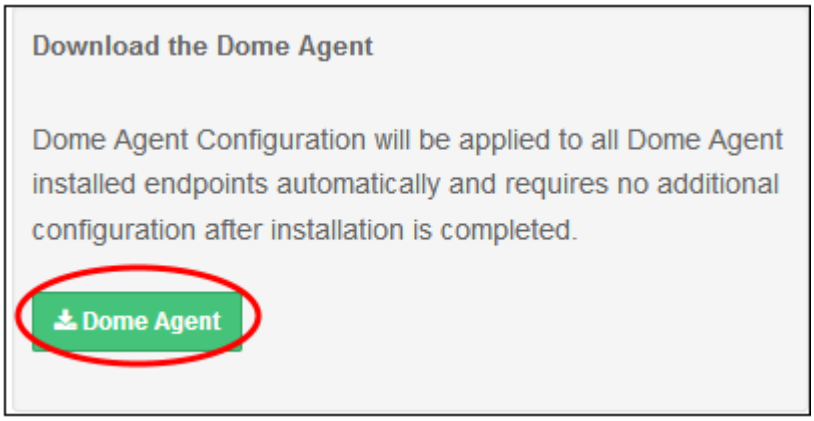


- **Protect Hosts File** - Determines whether a user can access non-public, internal domains.
  - For example, if you have added an internal domain to the 'Hosts' file, then 'SWG' proxy cannot resolve it since it is not available publicly.
  - The default setting is 'No'. If you select 'Yes', the internal 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 section.

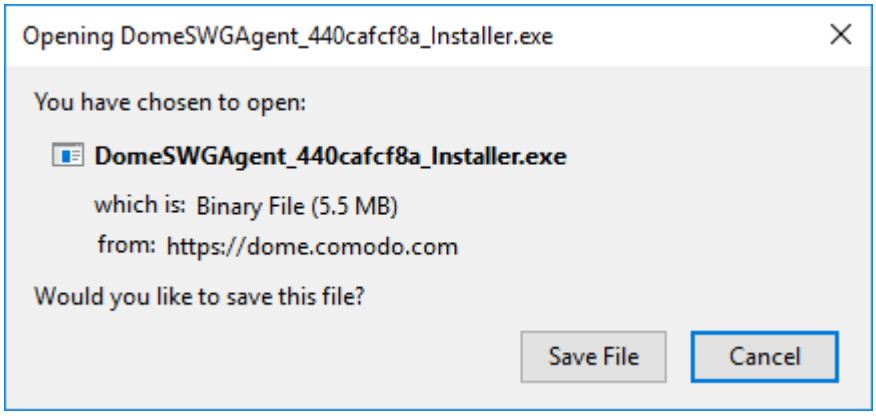
- Click 'Save' to apply the settings to the agent.

Download the SWG Agent

- Click the 'SWG Agent' button:



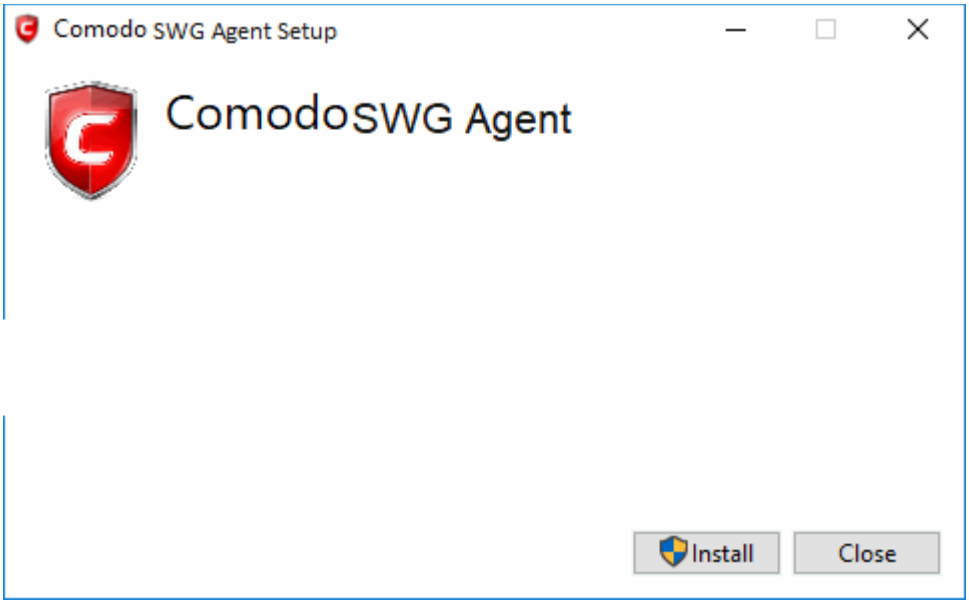
Click 'Save File' in the download dialog:



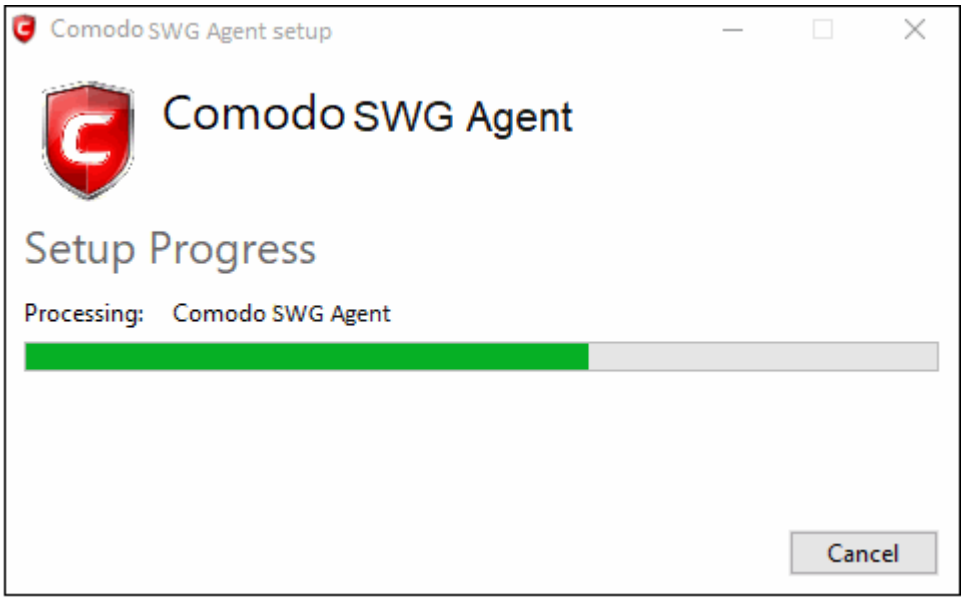
- Copy the agent to all roaming devices you want to protect.

Install the agent

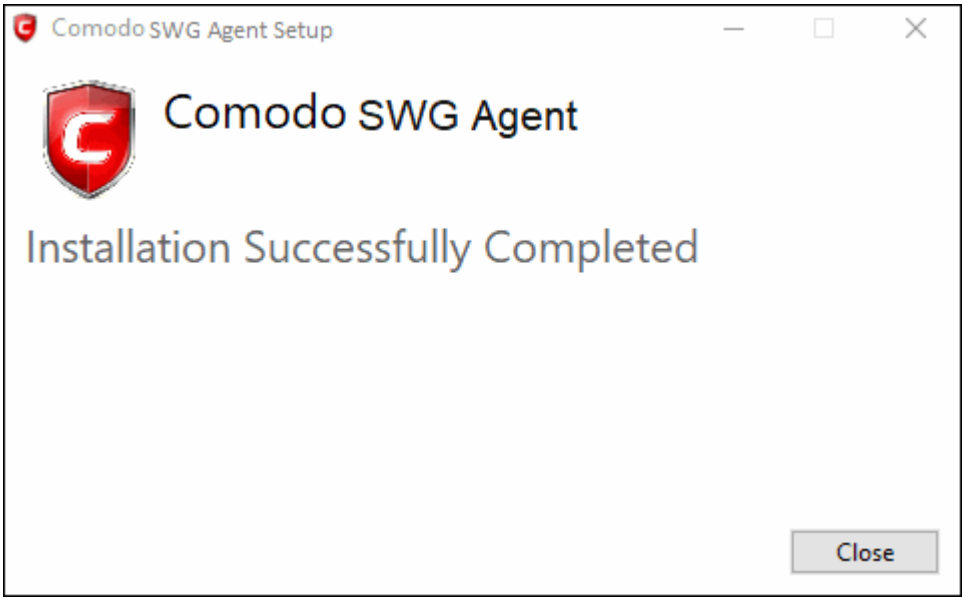
- Run the agent setup file



- Click 'Install'



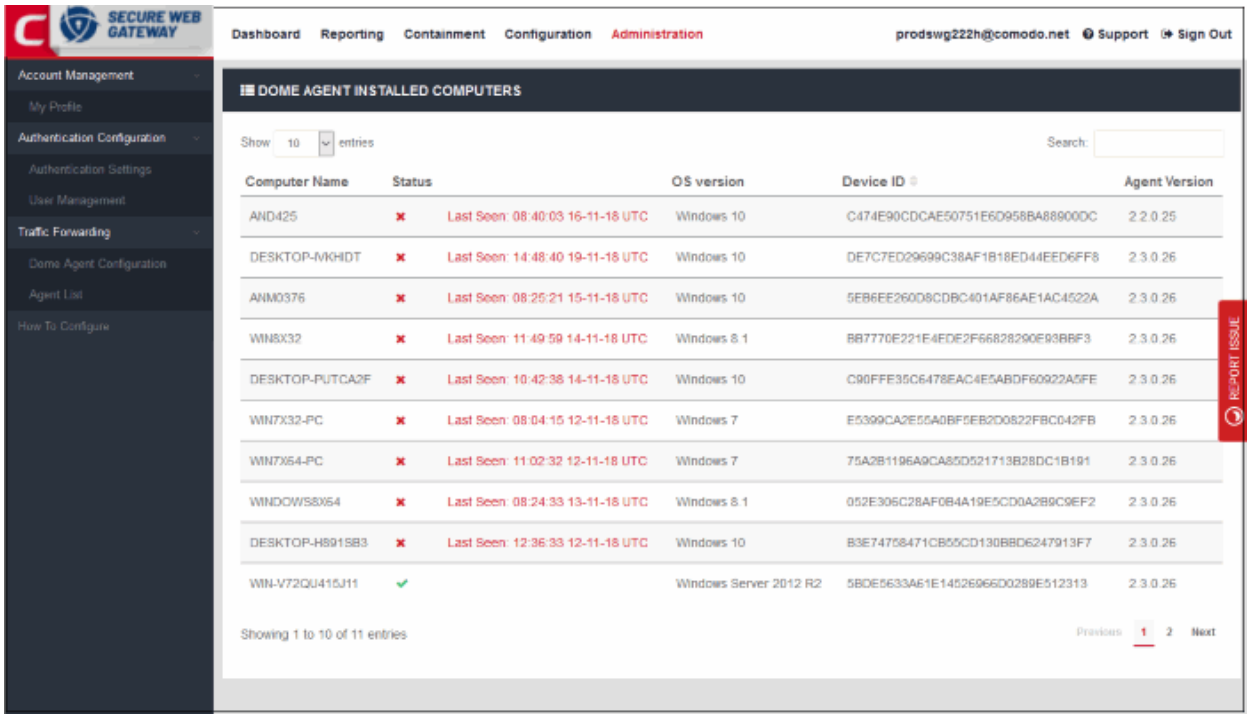
- Click 'Close' after the agent installation is complete.



- 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.
- Any specific policies for roaming users will be applied to the device. If none exist then then the default 'Global Policy' is applied. See '**Manage Policies**' and '**Apply Policies to Networks**' for more details.
- 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.

4.2.1 View Enrolled Roaming Devices

- Click 'Administration' > 'Traffic Forwarding' > 'Agent List'
- The agent list screen shows all devices on which you have installed the SWG agent.
  - See previous section, '**Connect your Roaming Devices to Comodo Secure Web Gateway**', if you need help to install the agent.



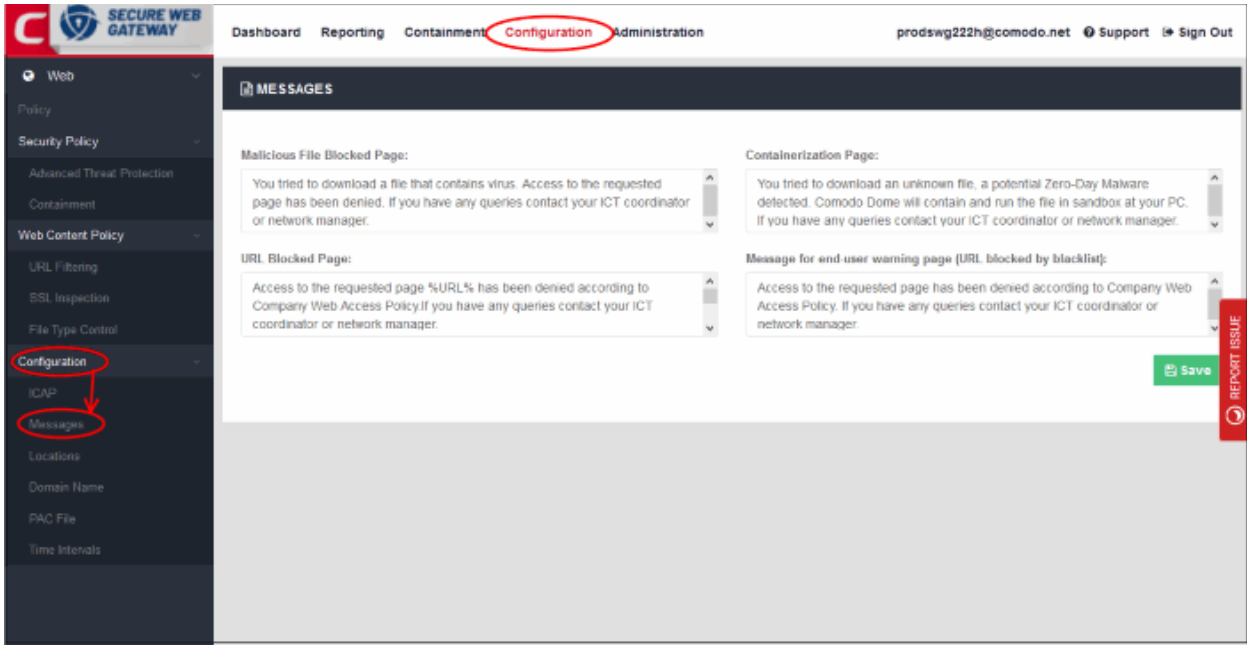
SWG Agent Installed Computers- Table of Column Descriptions	
Column Header	**Description**
Computer Name	The label of the roaming device.
Status	Shows whether the device is connected to SWG or not. The most recent connection time is shown for offline devices.
OS version	The operating system of the device.
Device ID	The unique identification number generated by the agent for the device.
Agent Version	Version number of SWG agent.

- Use the search box at top-right to filter by computer name or device ID.

4.3 Configure Comodo Secure Web Gateway Messages

'Messages' are warnings that are shown to users when the device security policy is breached.

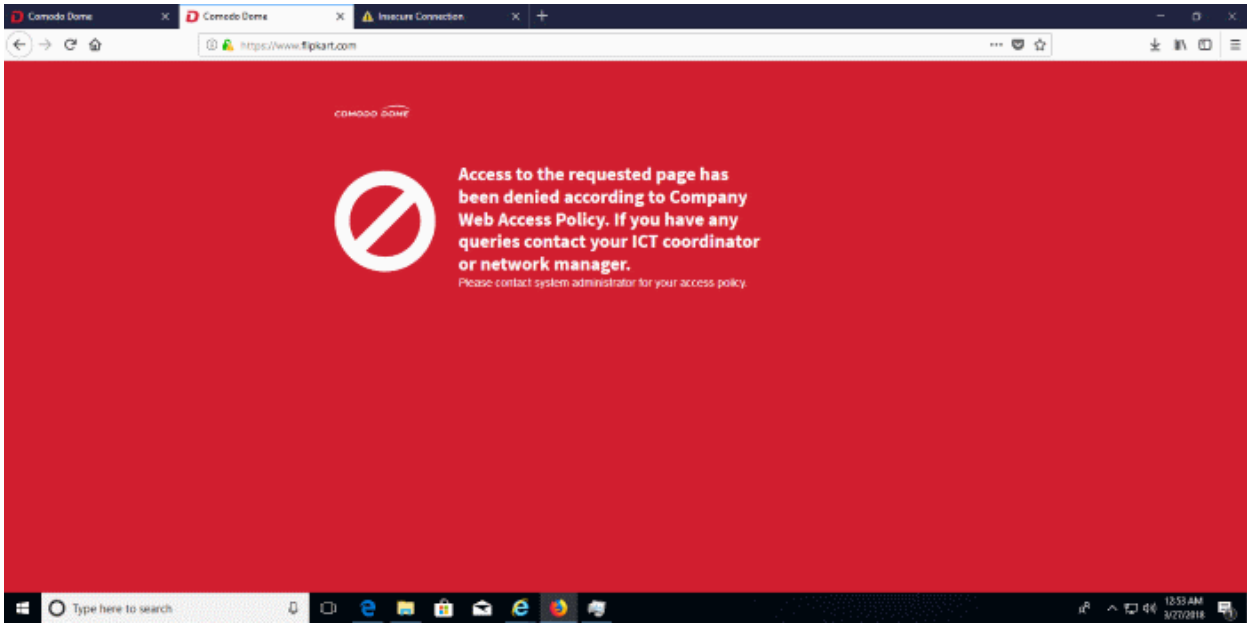
- Click 'Configuration' > 'Configuration' > 'Messages' to open the 'Messages' interface.



Comodo Secure Web Gateway ships with the following warnings and messages:

- **Malicious File Blocked Page** – Shown when a user tries to download an executable file from a blacklisted domain configured in the **Advanced Threat Protection** interface.
- **URL Blocked Page** - Shown when users visit a site in a blocked **category**. Blocked categories are specified in URL filtering rules.
- **Containerization Page** - Shown when a user downloads an unknown file to inform them that the file will be run inside the sandbox.
- **Message for end-user warning page (URL blocked by blacklist)** - Shown when a user visits a website that has been **blacklisted in a URL filtering profile**.

You can easily edit these messages should you wish. Click 'Save' to apply your changes. The following message is an example of URL blacklist policy breach:



4.4 Configure Domain Name

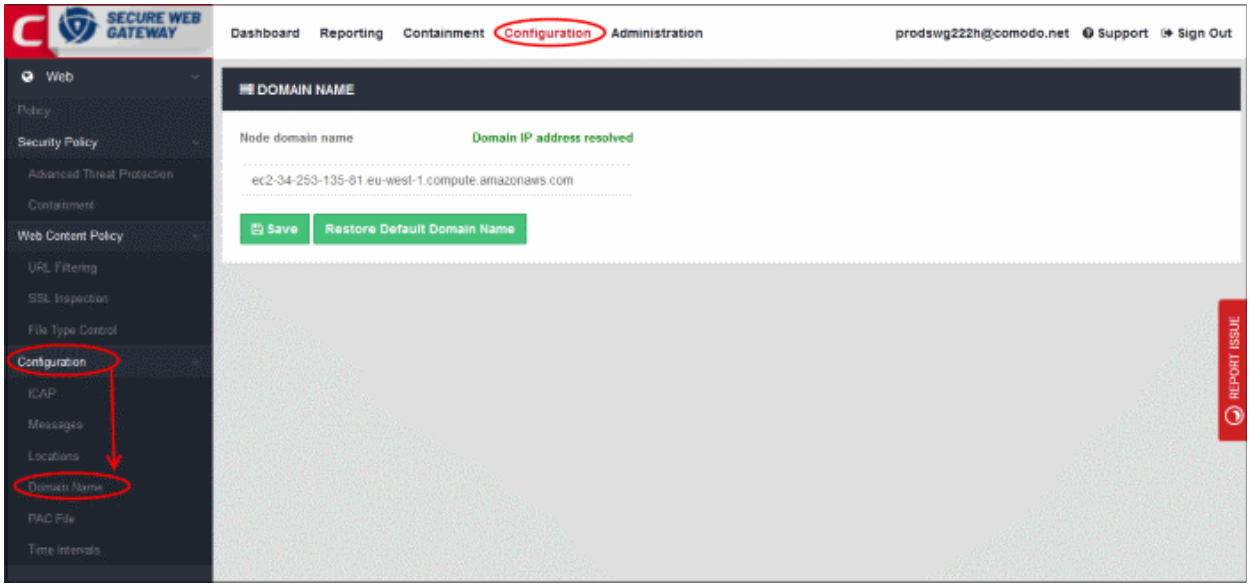
- Click 'Configuration' > 'Configuration' > 'Domain Name'

Add your own domain as a Comodo Secure Web Gateway (SWG) node so you can easily manage domain names. For example:

- You have your own domain
- Register a sub-domain for SWG node use
- Point this sub-domain's DNS record to Comodo SWG so that it resolves to the node's IP address
- After the DNS record becomes active (it may take few minutes to 72 hours), update the node domain name with your subdomain name

Change the node domain name

- Click 'Configuration' > 'Configuration' > 'Domain Name' to open the interface.



- Node domain name – The SWG node domain configured in Amazon AWS for your account
- To change the node domain, enter the sub-domain details that you have configured as explained above
- Click 'Save'
- Click 'Restore Default Domain Name' to update to the default node domain name

4.5 Configure PAC File for Exclusions

- Click 'Configuration' > 'Configuration' > 'PAC File' to download the PAC file.

A proxy auto-config (PAC) file determines which proxy servers a browser or client should use to access a given URL.

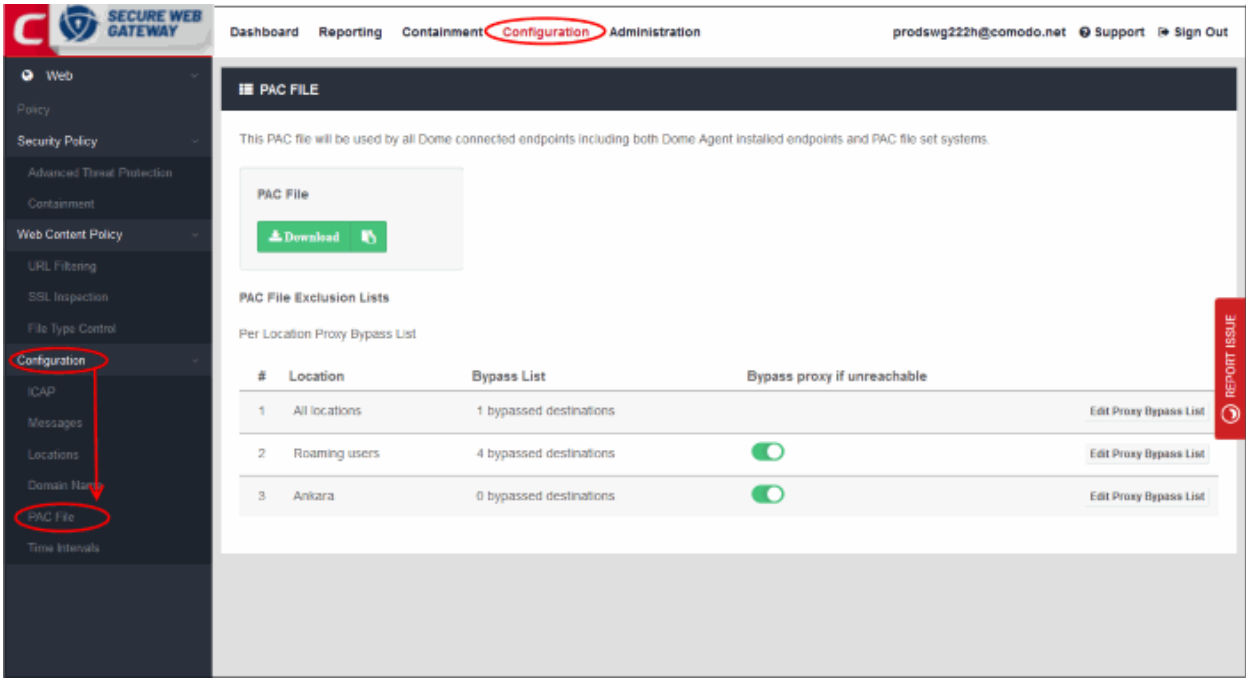
- Your Comodo SWG node domain URL is automatically configured in the PAC file so it acts as the proxy server.
- If you add your own sub-domain as explained in the '**Configure Domain Name**' section, then this will be configured in the PAC file. This automatically resolves to the SWG node IP address.
- You can configure exclusions (domains, IPs and networks) that can be reached directly without using the Comodo SWG proxy server. You can define different exclusions for each location and roaming agent.
- You have the option to bypass the proxy if the connection to SWG is lost, so users can access the internet

directly.

- Click 'Administration' > 'How to Configure' > 'Set as Proxy' > 'PAC' to find the URL of the PAC file.

Exclude network locations

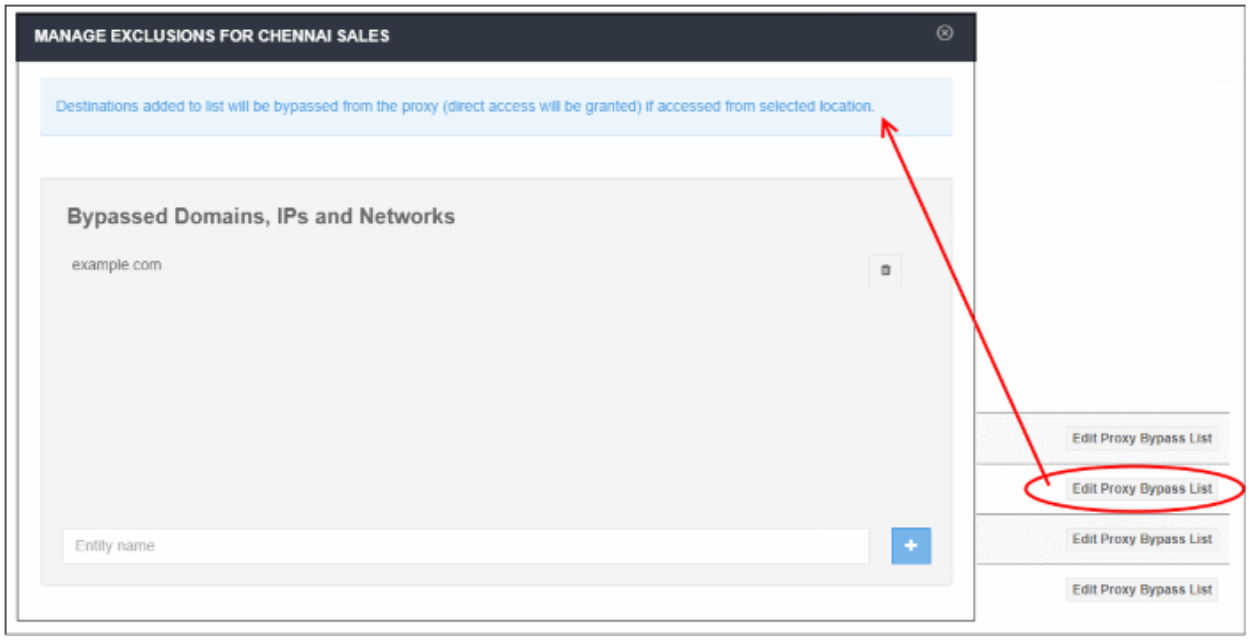
- Click 'Configuration' > 'Configuration' > 'PAC File'



PAC File Exclusions List - Table of Column Descriptions	
Column Header	**Description**
Location	Trusted networks. 'All locations' and 'Roaming Users' are shown by default. You can add more locations as required. See '**Manage Trusted Networks**' for help to add trusted networks.
Bypass List	Number of destinations added to the exclusion list for the network.
Bypass proxy if unreachable	Choose whether users should connect to the internet directly if the connection to SWG gateway is lost. • If enabled, endpoints in the location will make direct connections to the internet if SWG gateway is unreachable.
Edit Proxy Bypass List	Manage the exclusions list. See '**Manage Exclusions**' for more information.

Manage Exclusions

- Click 'Edit Proxy Bypass List' in the row of the network to which you want to add / remove exclusions.



Add a destination to the exclusions list

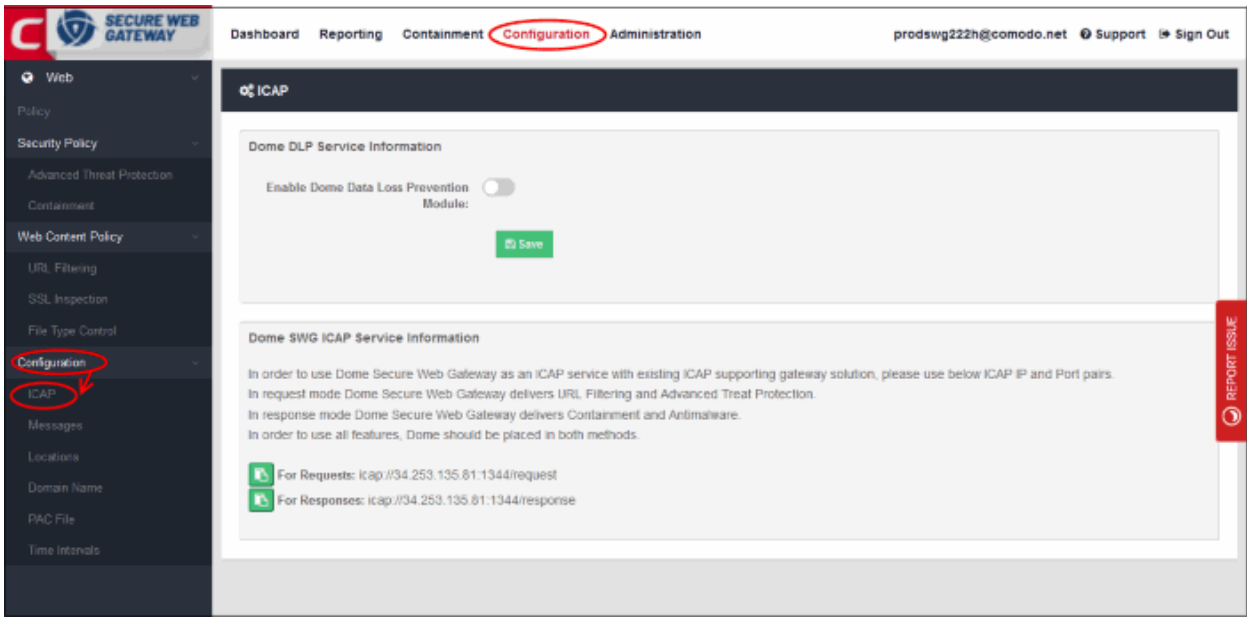
- Enter a valid domain name, IP or network in CIDR format in the 'Entity name' field. Click the '+' button.
- You can use wildcards with domain names. For example, *.mydomain.com
- The destination will be added to the list

Remove destination from the exclusions list

- Click the trash can icon beside an entry
- Click 'OK' in the confirmation dialog to remove the entry

4.6 Configure Data Loss Prevention and View ICAP Service Information

- Click 'Configuration' > 'Configuration' > 'ICAP' to open this interface.
- Comodo Secure Web Gateway (SWG) can provide its security features as an Internet Content Adaptation Protocol (ICAP) service to other ICAP supporting solutions.
  - This interface contains the IP and port details required to use SWG as an ICAP service.
- You can also integrate Comodo Data Loss Prevention (DLP) with Comodo SWG to monitor and protect confidential information on your network.



- **Configure Comodo DLP Service**
- **View Comodo SWG ICAP Service Information**

Configure Comodo DLP Service

Use the switch to enable or disable the DLP service.

Prerequisites to using the service:

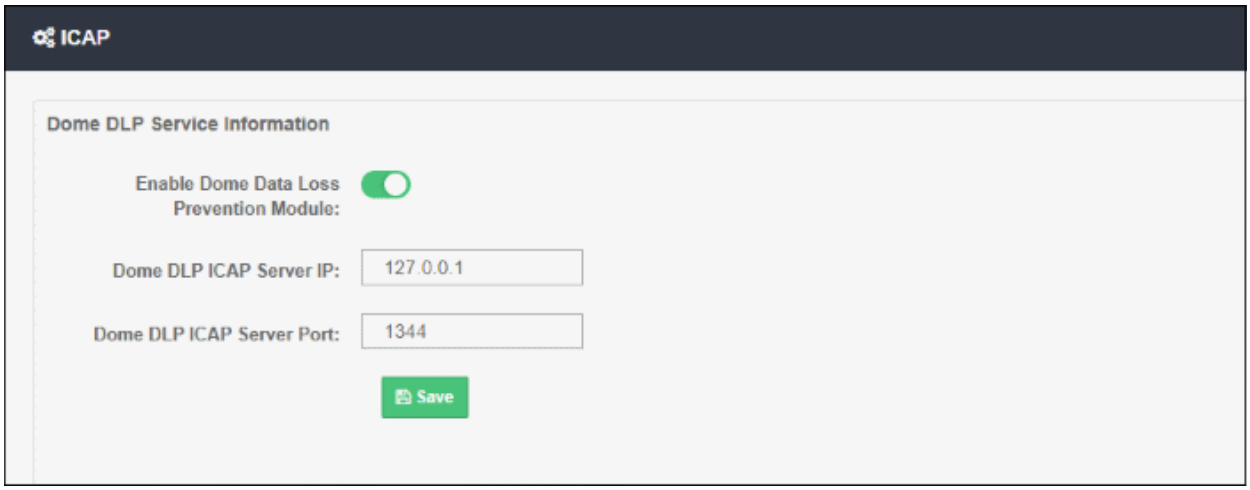
- Traffic forwarding should have been set up. **Click here** for more information about traffic forwarding methods.
- You should have a valid Comodo Data Leak Prevention (DLP) license. **Click here** for help to install / subscribe for DLP.

How DLP integration works:

- Traffic flows to SWG via the proxy.
- SWG communicates with the DLP module and implements DLP rules on the traffic. Here is a simplified traffic flow:
  - Endpoint > Comodo SWG > Comodo DLP > Comodo SWG > Internet
  - Internet > Comodo SWG > Comodo DLP > Comodo SWG > Endpoint
- If the requests / responses comply with your DLP policy then the traffic is allowed. Likewise, the traffic is blocked if the request violates your DLP policy.
- The result is that both SWG and DLP policies are applied to your traffic.

Configure the Comodo DLP service

- Move the 'Enable Comodo Data Loss Prevention Module' switch to the right:



- Comodo DLP ICAP Server IP – Comodo DLP service IP. Default = 127.0.0.1
- Comodo DLP ICAP Server Port – DLP port number. Default = 1344

- Click 'Save' for your changes to take effect.

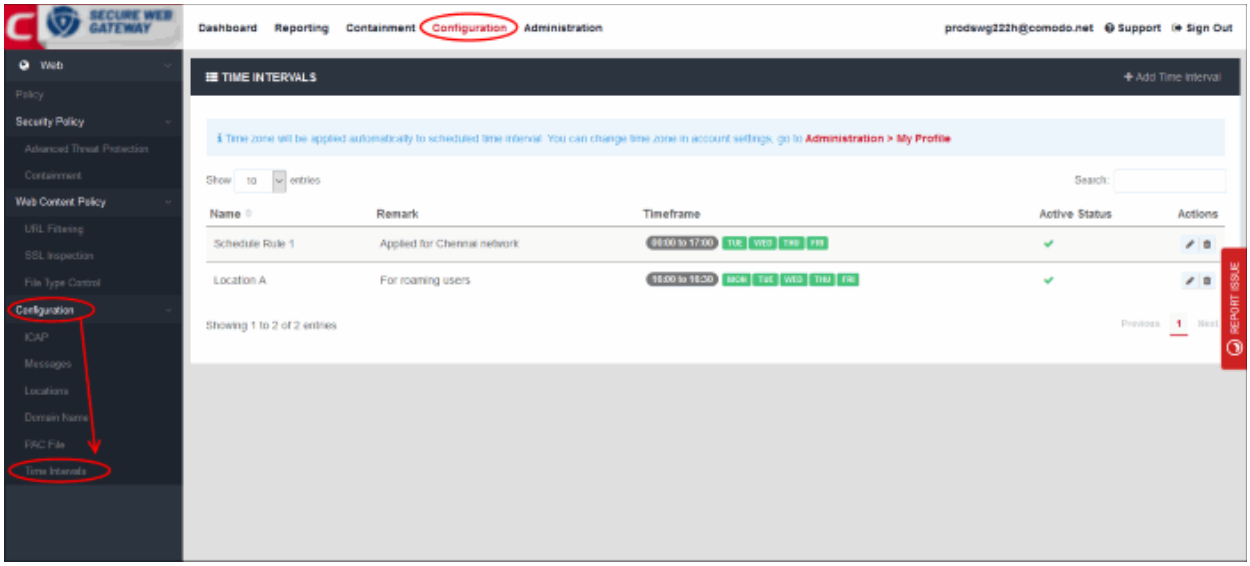
Please contact us at **domesupport@comodo.com** if you have any issues connecting endpoints / networks to Comodo SWG and Comodo DLP.

View Comodo SWG ICAP Service Information

The lower section shows the request and response details needed to configure SWG to work with another ICAP service. **Click here** for more information about how to do this.

4.7 Configure Policy Time-Schedules

- Click 'Configuration' > 'Configuration' > 'Time Intervals'
- You can configure Comodo Secure Web Gateway (SWG) to activate a policy only at specific times. This interface lets you create the schedules which you then add to a policy.
  - See '**Apply Policies to Networks**' if you need help to configure and apply a policy.
- The time zone used is as set in '**Administration**' > '**My Profile**'



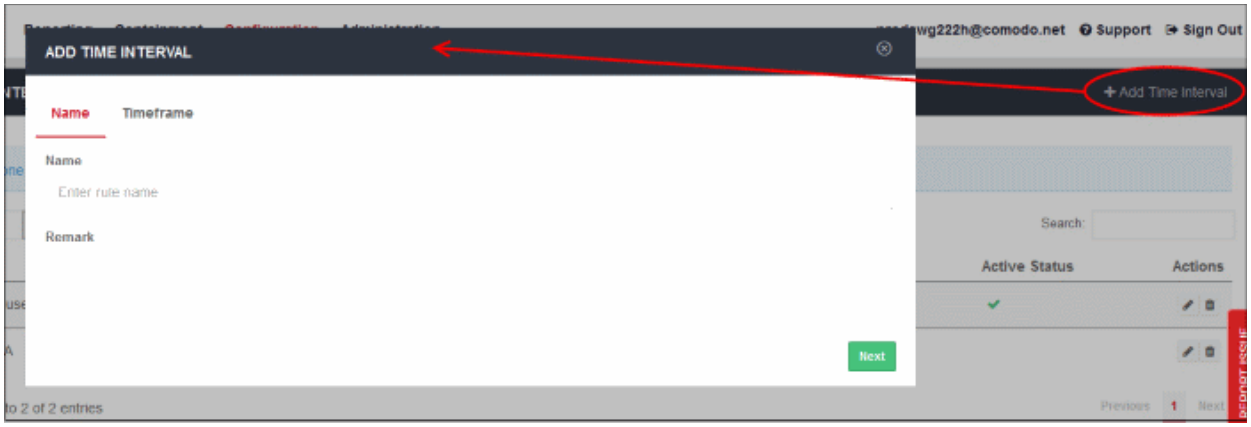
Time Intervals - Table of Column Descriptions	
Column Header	**Description**
Name	Schedule label.
Remark	Short description of the schedule.
Timeframe	The times when a policy is active under this schedule.
Active Status	Whether or not the schedule is currently active. This status also applies to any policies 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.

The interface allows you to:

- **Create a new time schedule**
- **Edit a schedule**
- **Delete a schedule**

Create a new time schedule

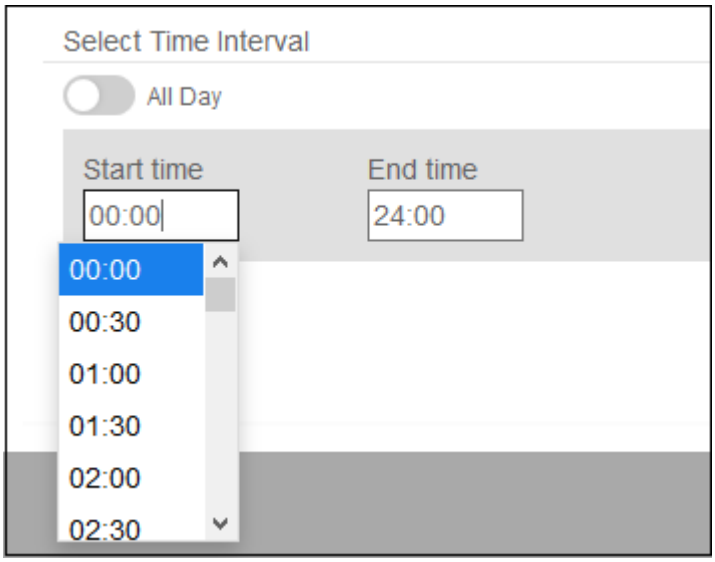
- Click 'Add Time Interval' at top-right



- 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

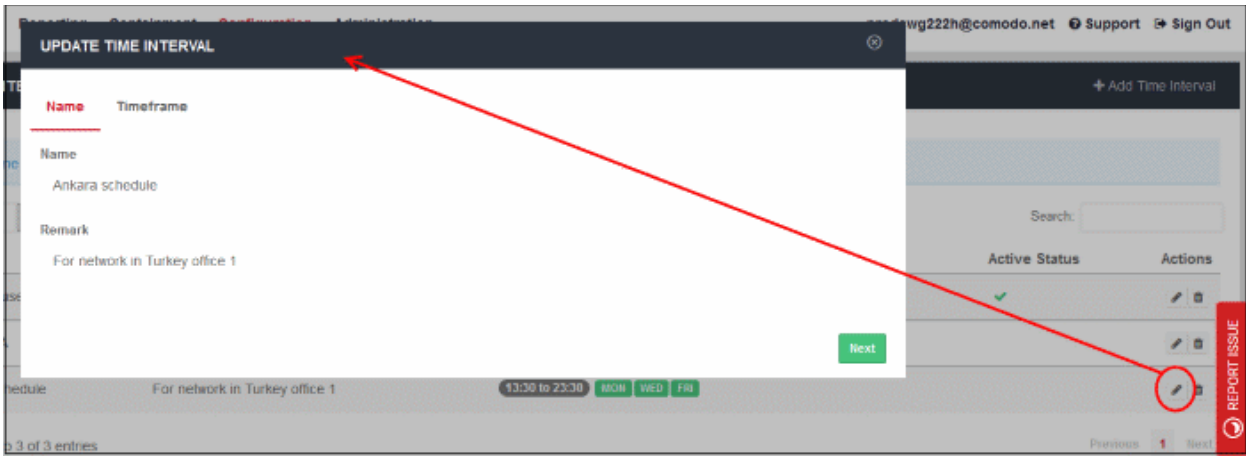


- Select the time period from the 'Start time' and 'End time' drop-downs. The schedule will be active for the configured period for the scheduled days.
- Click 'Create' when done.

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

Edit a schedule

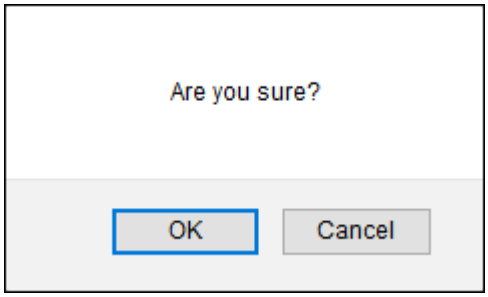
- Click the 'Edit' button beside the schedule to update it



- Updating a schedule is similar to creating a new schedule explained **above**.

Delete a schedule

- Click the trash can icon beside a schedule to remove it from the list



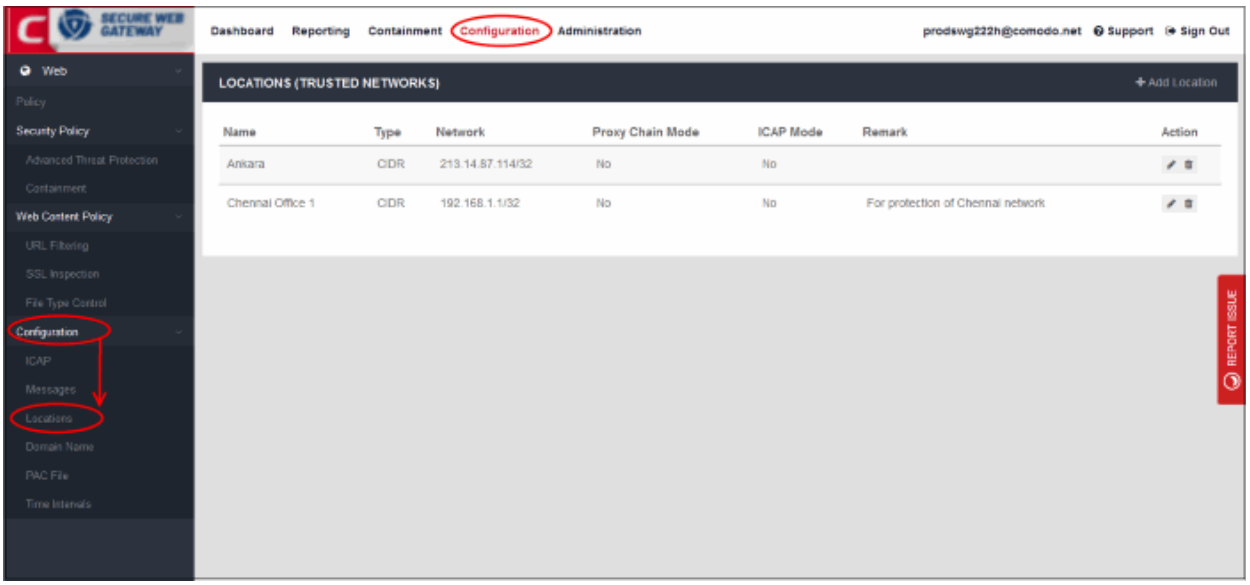
- Click 'OK' to confirm

Note – When a schedule is removed, it will be removed from the policies also.

5 Manage Trusted Networks

- Click 'Configuration' > 'Configuration' > 'Locations' to open the trusted networks interface
- After **Connect your Network to Comodo Secure Web Gateway,** the next step is to add a 'Trusted Network'. 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. See '**Apply Policies to Networks**' section for more details.
- This section explains how to add and manage networks in the 'Locations (Trusted Networks)' interface.

Note – You must have added some users before you can apply policies to users. See '**User Management**' and '**Apply Policies to Networks**' for more details.



Locations (Trusted Networks) - Table of Column Descriptions	
Column Header	**Description**
Name	Identifying label of the trusted location.
Type	Addressing architecture. Can be CIDR or FQDN.
Network	Public IP address of the network, or the fully qualified domain name.
Proxy Chain Mode	Yes - Proxy chain mode authentication and traffic forwarding is enabled.
ICAP Mode	Yes – SWG is set as a provider of ICAP services to another ICAP solution. See **https://help.comodo.com/topic-436-1-842-10781-Traffic-Forwarding-via-Internet-Content-Adaptation-Protocol-(ICAP).html** if you need more information on ICAP mode.
Remark	Comments provided for the location

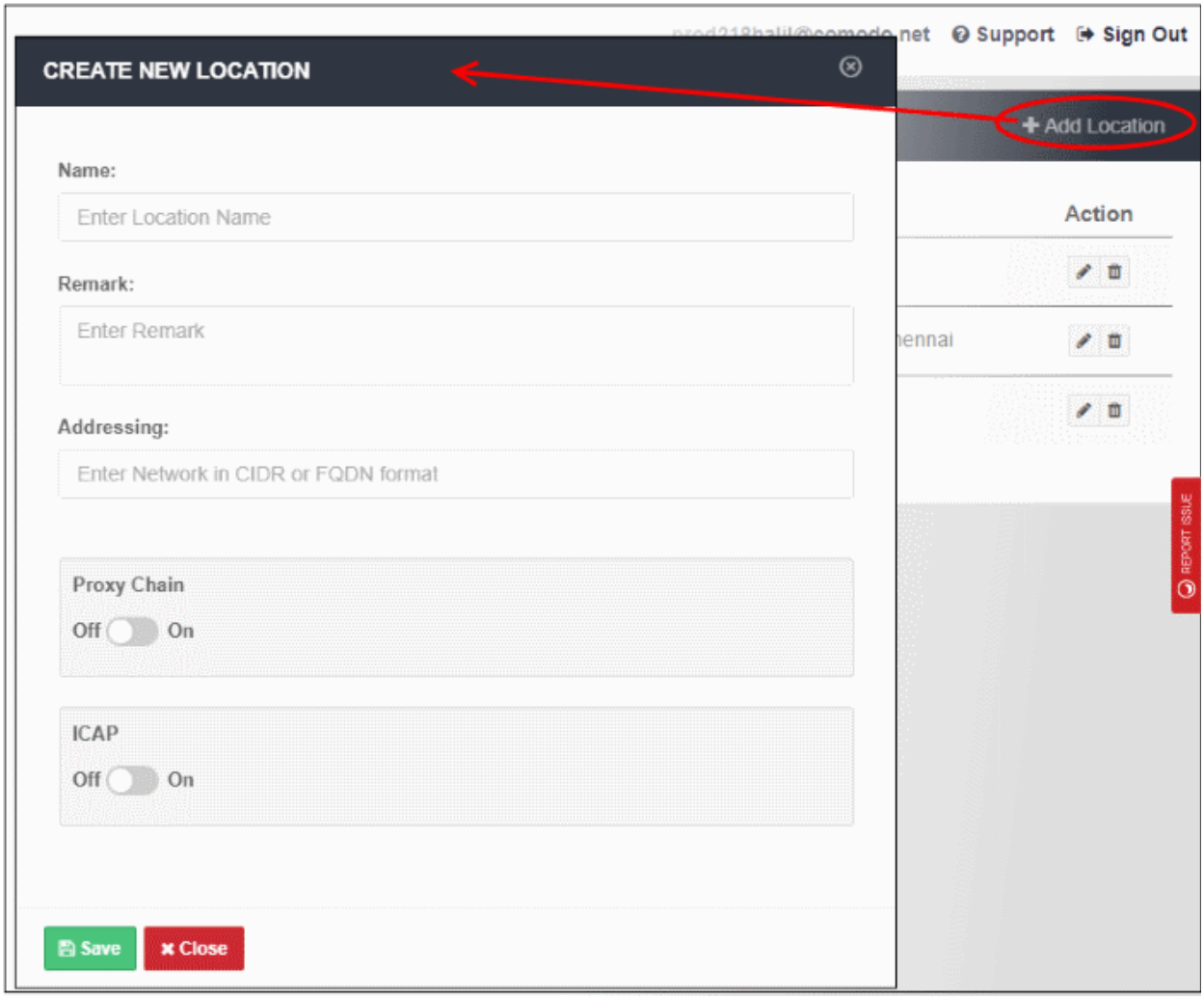
Actions	You can edit and / or delete a location. If you delete a location, the policies applied to that location are also removed.

The interface allows you to:

- **Add a new location**
- **Edit a location**
- **Delete a location**

Add a new 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.

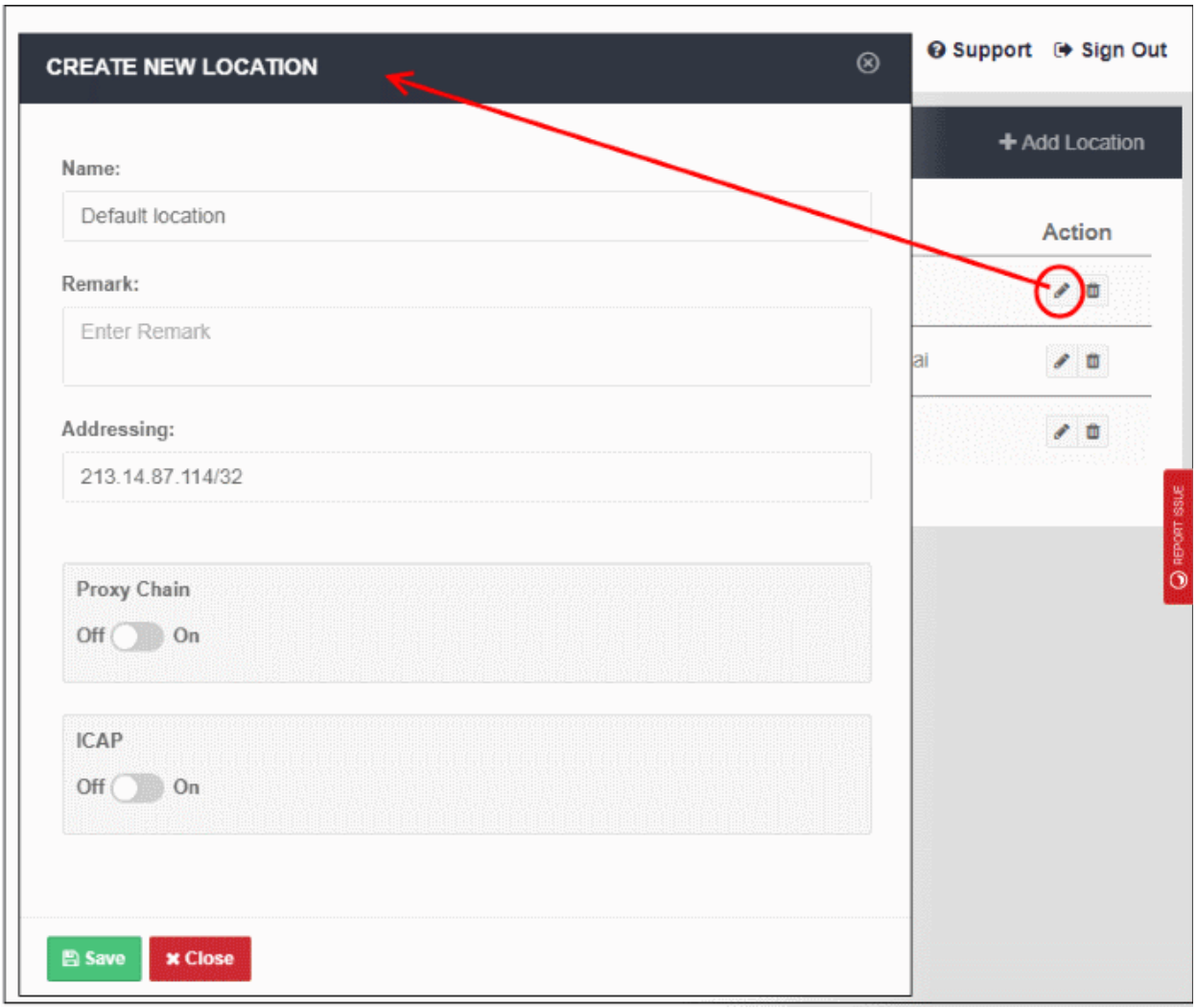
- See '**User Management**' and '**Configure User Authentication Settings**' for more information.

- 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.

Edit a location

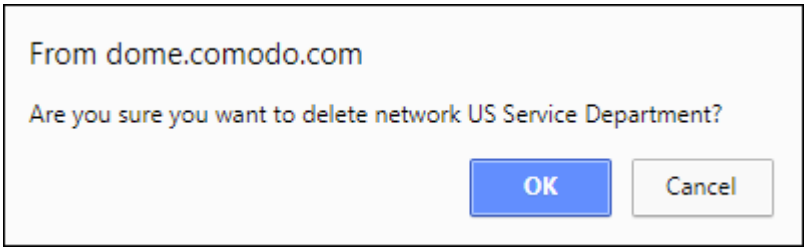
- Click the 'Edit' icon beside the location that you want to update:



- Update the details as required. The procedure is same as explained in the '**Add**' section above.
- Click 'Save' to apply your changes.

Delete a location

- Click the trash can icon beside the location that you want to delete under the Actions column.



- Click 'OK' to confirm removal of the location

Please note that if you remove a location, all applied policies to that location and related users/group/department will no longer be applicable. Also make sure to alter your LAN settings in order to connect to the internet.

6 Manage Policies

- Click 'Configuration' > 'Policy'
- Policies let you apply specific web-filtering and threat-prevention rules to trusted locations.
- You need to configure policy targets and components ***before*** you configure a policy.
  - Targets - Users/locations/departments.
  - Components – Components are security policy, web-content policy and schedule.
- Click 'Add Policy' to open the new policy wizard. The interface has three tabs:
    - **Name** – Select the priority of the policy and create a policy label. Policies are prioritized top-to-bottom according to this list. In the event of a conflict between policies, Comodo Secure Web Gateway (SWG) will implement the setting in the policy nearer the top of this list. You can change the priority of a policy by clicking 'Edit' > 'Policy Order'
    - **Select Objects** – These are the targets of the policy. The targets can be any combination of locations, users, user-groups, departments or computers.
      - Click 'Configuration' > 'Locations' to **add and manage locations** (trusted networks)
      - Click 'Administration' > 'User Management' to **add/manage users, user-groups, departments and computers**
    - **Apply Policy** – This is where you add the policy components from the 'Security Policy', 'Web Content Policy' areas and 'Time Intervals' shown in the left-menu:

  Security Policy components

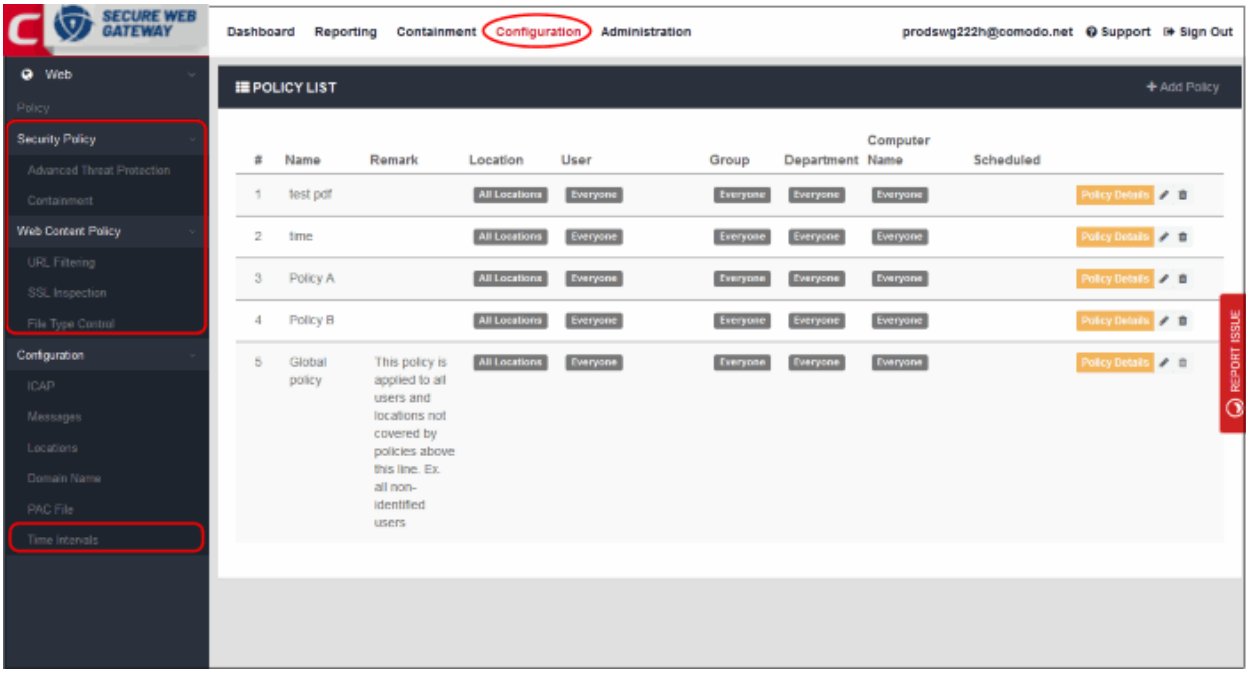
  - ***Advanced Threat Protection*** - Comodo Secure Web Gateway ships with a default security policy to block all web threats. You can create exceptions to advanced threat protection which will be applied to your policy. See '**Configure Advanced Threat Protection Settings**' for more information.
  - ***Containment*** - All unknown applications and processes are automatically run in a secure, virtual environment on a user's endpoint. The 'containment' component lets you define what type of files should be contained. You can also specify the maximum size and depth of archive files which Comodo SWG should attempt to scan. See '**Configure Containerization Settings**' for more information.

  Web Content Policy components

  - ***URL Filtering*** - Configure which website categories should be allowed or blocked. You can also create your own domain whitelist or blacklist. See '**Manage URL Filtering Policies**' for more information.
  - ***SSL Inspection*** - Configure whether or not Comodo SWG should check that websites use an SSL certificate from a trusted certificate authority. You can also download and install the SWG root certificate, which is required if you wish to decrypt and scan files from https sites. See '**Configure SSL Inspection Setting**' for more details.
  - ***File Type Control*** - Configure which file types Comodo SWG should prevent users from downloading. You can fine-tune this restriction by website category. See '**Manage File Type Control Rules**' for more information.

  Time Interval (Policy schedule time)

  - ***Time Interval*** – Set the times that the policy is active. You can create a schedule in 'Configuration' > 'Time Intervals'. You can then add the schedule to a policy. See '**Configure Policy-Time-Schedules**' for more information.
- You can create and apply your policy after configuring your targets and policy components. See '**Apply Policies to Networks**' for more details.
- The policy component interfaces are shown in the red box in the screenshot below:



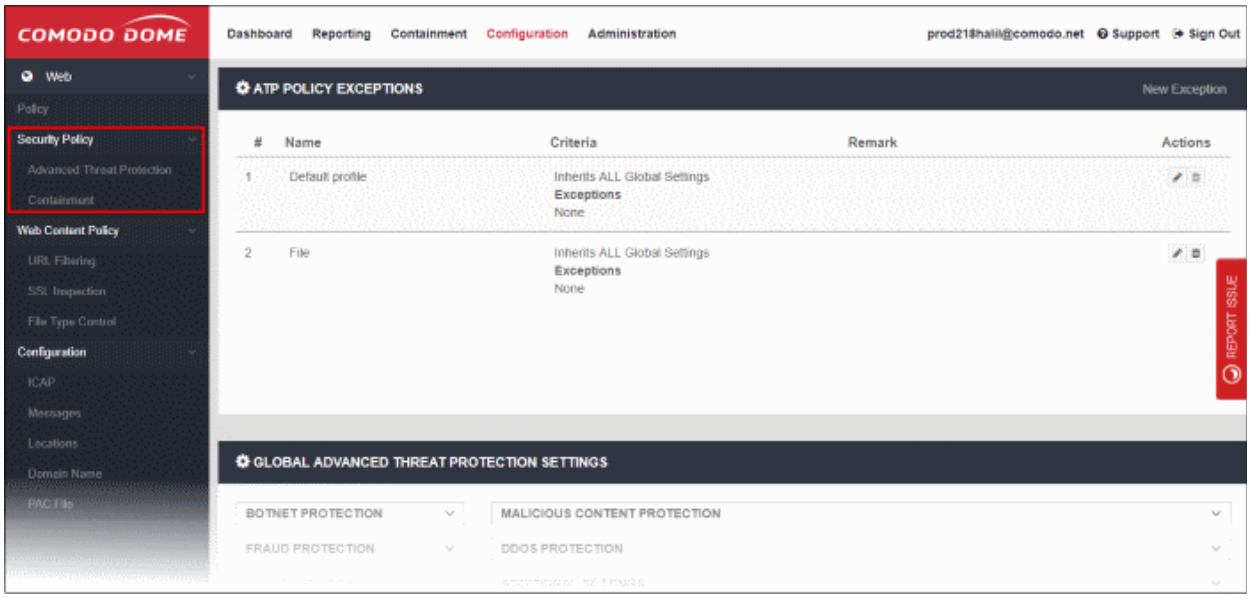
Click on the following links for more details:

- **Security Policy**
- **Web Content Policy**

6.1 Security Policy

Comodo maintains a huge blacklist of harmful websites which is split into several threat categories. This list is continually updated and is used by Comodo Secure Web Gateway (SWG) to implement security rules on networks.

- By default, SWG will block access to blacklisted websites. This is because the default profile deployed to managed endpoints / networks is set to 'Block'.
- These settings are configured in 'Global Advanced Threat Protection Settings' ('Configuration' > 'Security Policy' > 'Advanced Threat Protection' > 'Global Advanced Threat Protection Settings'). A default profile with these settings is automatically deployed to managed endpoints / networks.
- If you alter the Global ATP settings, the ATP policy will be updated for all protected networks. You can, however, create exceptions which can be deployed to specific endpoints / networks as required.
- The security policy area also allows you to configure containment settings (sandboxing of unknown files).



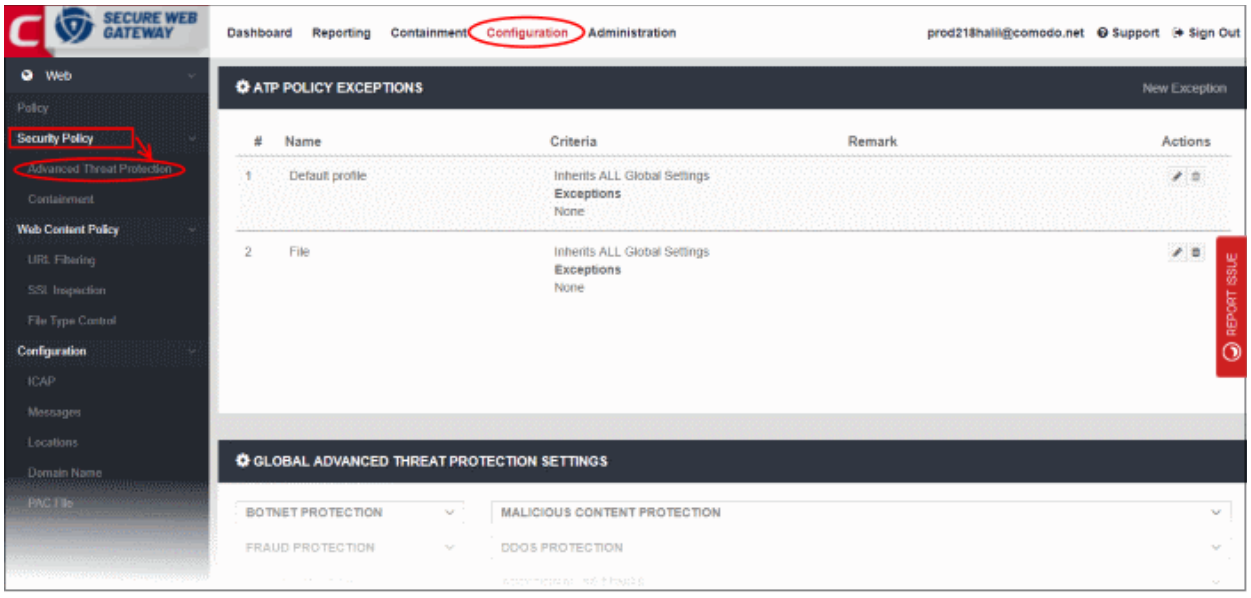
Click on the following links for more details:

- **Configure Advanced Threat Protection Settings**
- **Configure Containerization Settings**

6.1.1 Configure Advanced Threat Protection Settings

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

Comodo Secure Web Gateway (SWG) ships with a default security policy configured to block all web threats. This policy is deployed onto roaming devices / networks immediately after their enrollment and cannot be deleted. However, as your requirements demand, you can create exceptions and deploy these to networks / roaming devices as required.



The interface is divided into four sections:

- **ATP Policy Exceptions**
- **Global Advanced Threat Protection Settings**

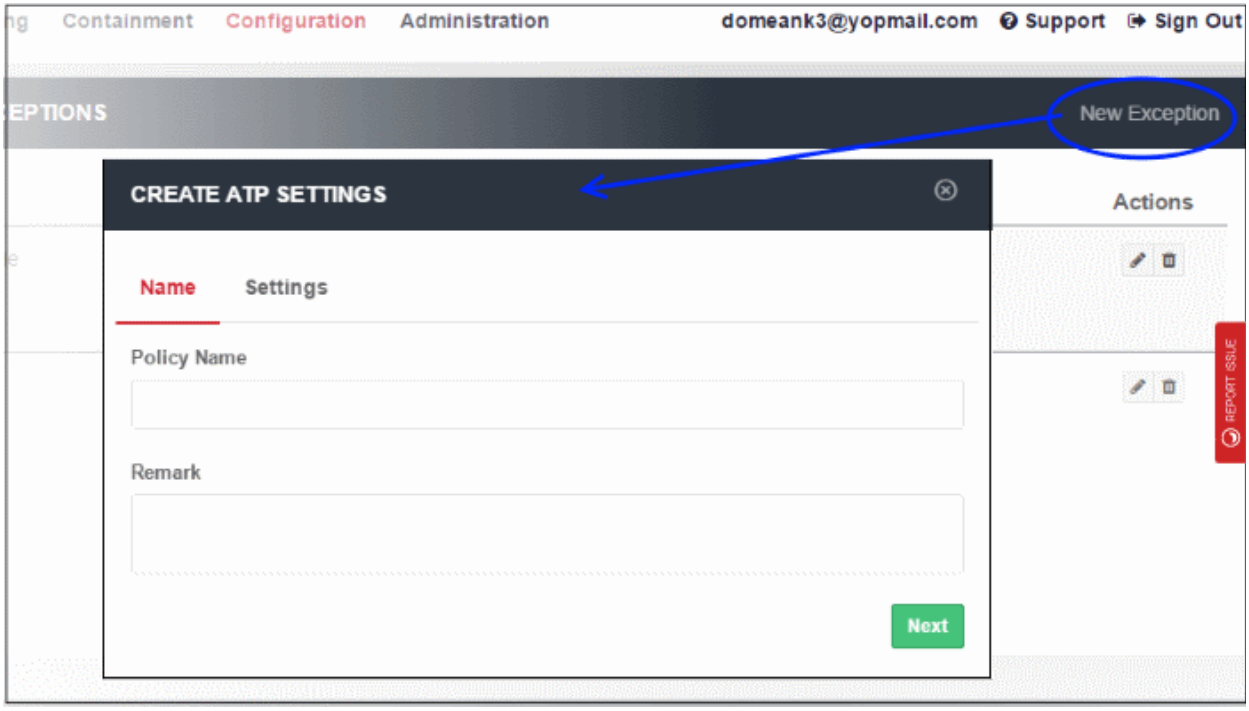
- **Global Blocked Files List**
- **Blocked Country List**

ATP Policy Exceptions

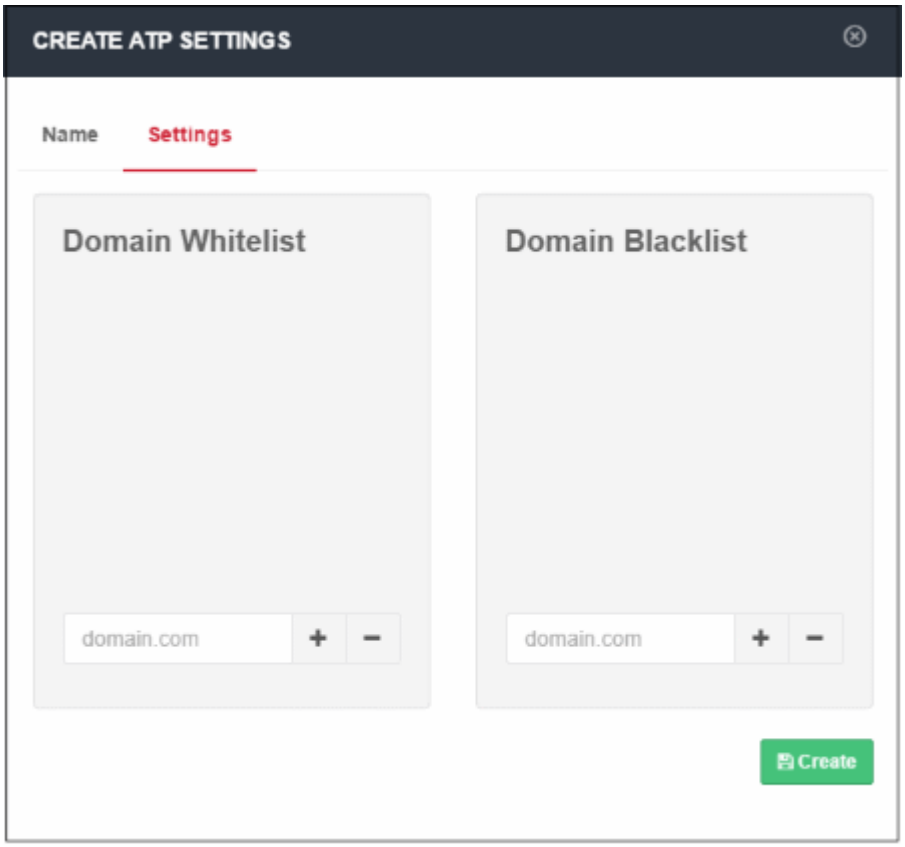
Allows you to specify domains will should ignored by the Advanced Threat Prevention system.

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



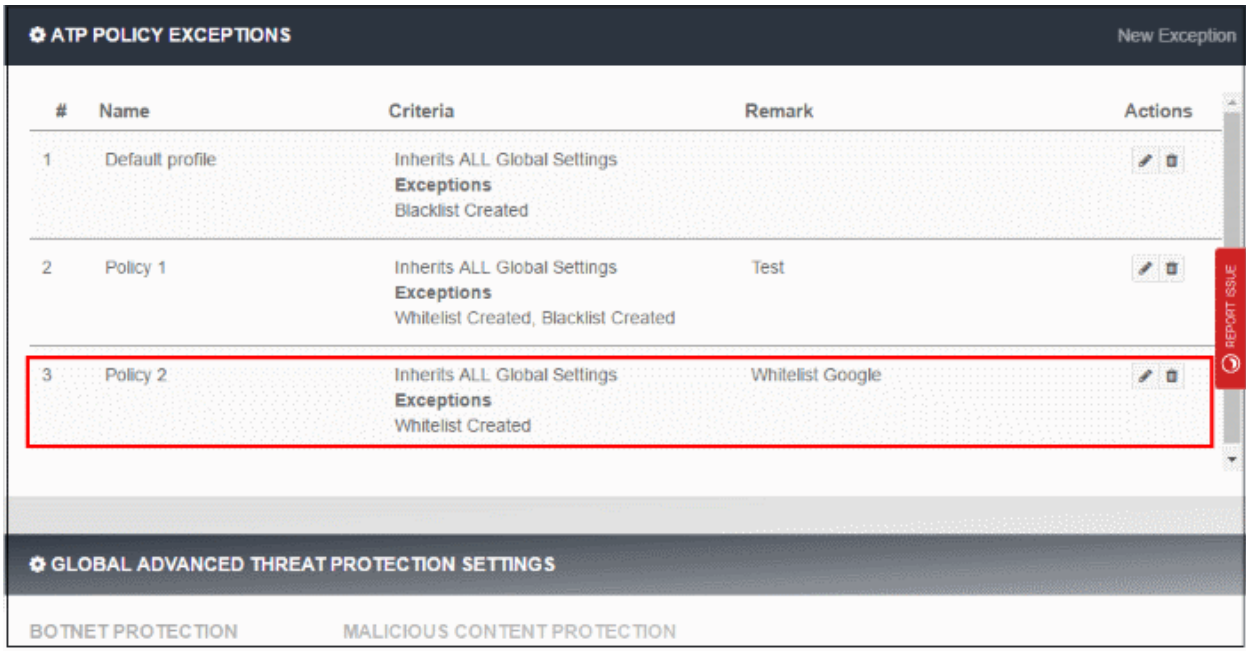
- Policy Name - Enter a descriptive label for the ATP exception.
- Remark - Enter any comments you wish to add about the exception.
- Click 'Next' to proceed or 'Settings' if you wish to specify domain whitelist and blacklist.



- 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.

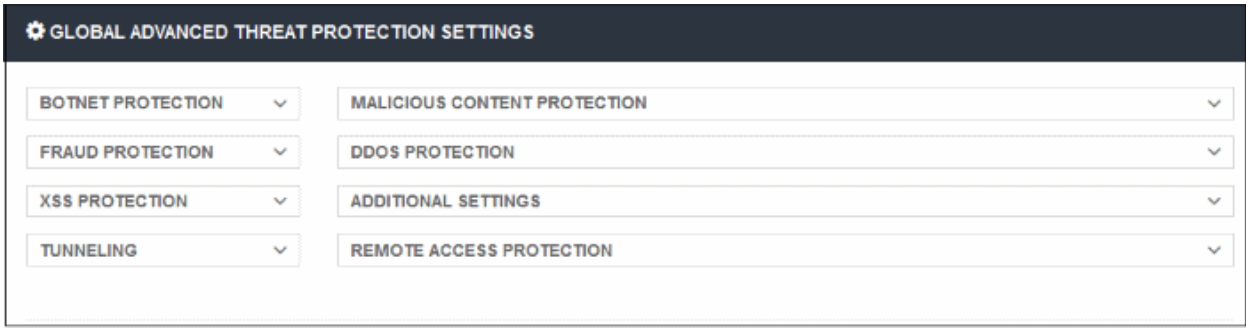


This new ATP policy will be available for selection when creating / editing a SWG policy. See '**Apply Policies to Network**' for more details.

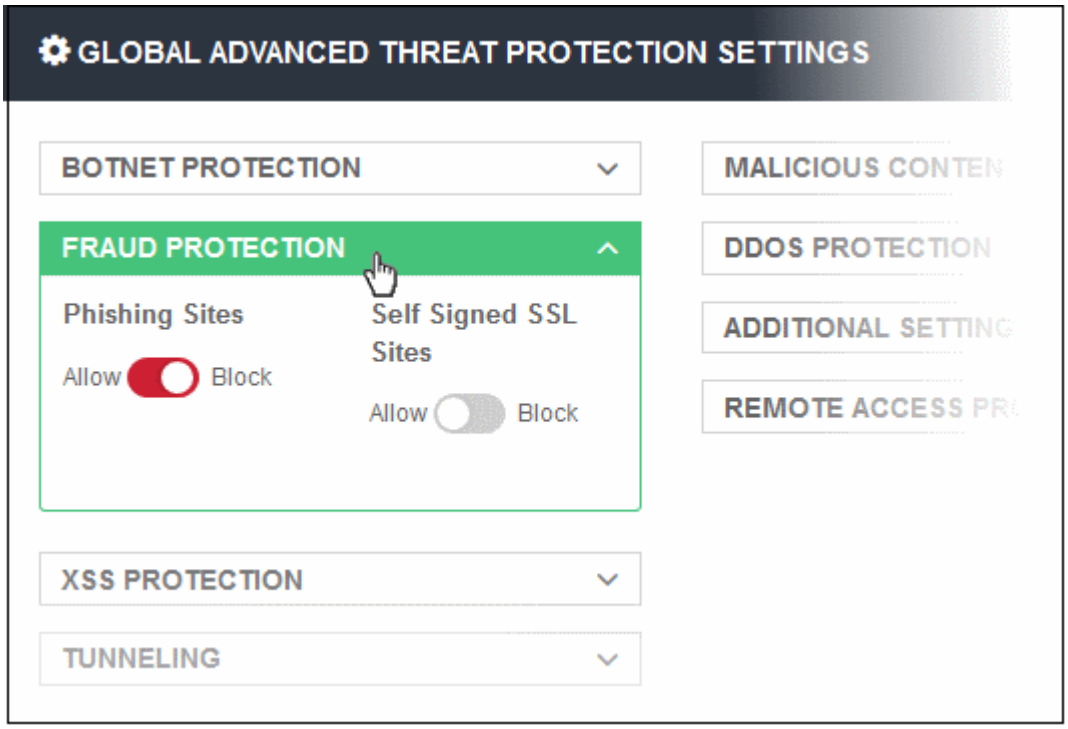
Global Advanced Threat Protection Settings

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.

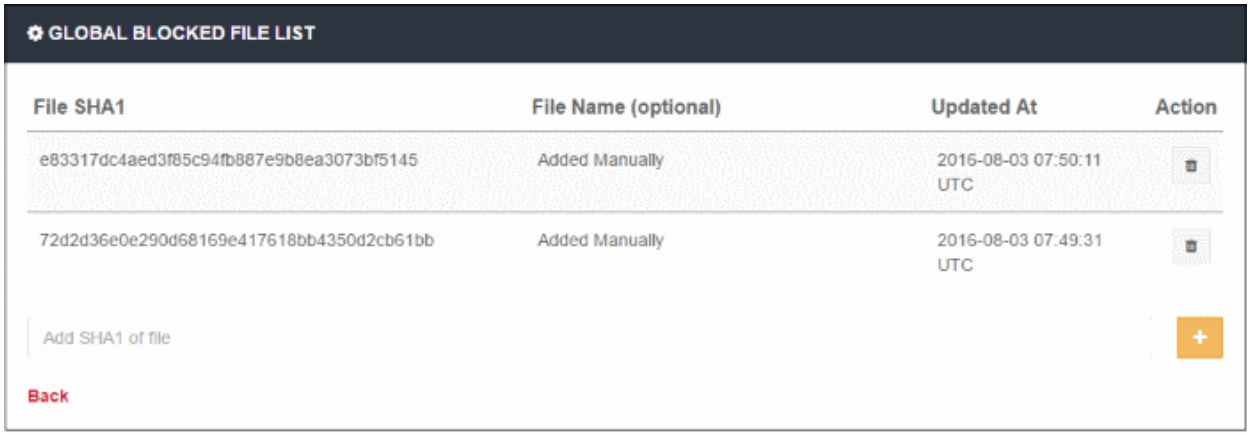


- The setting will be applied globally, to all protected domains and endpoints.
- You can create a policy with exceptions which you can to deploy to a particular network or endpoint. See '**ATP Policy Exceptions**' to find out how to add exceptions to the global settings.

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.



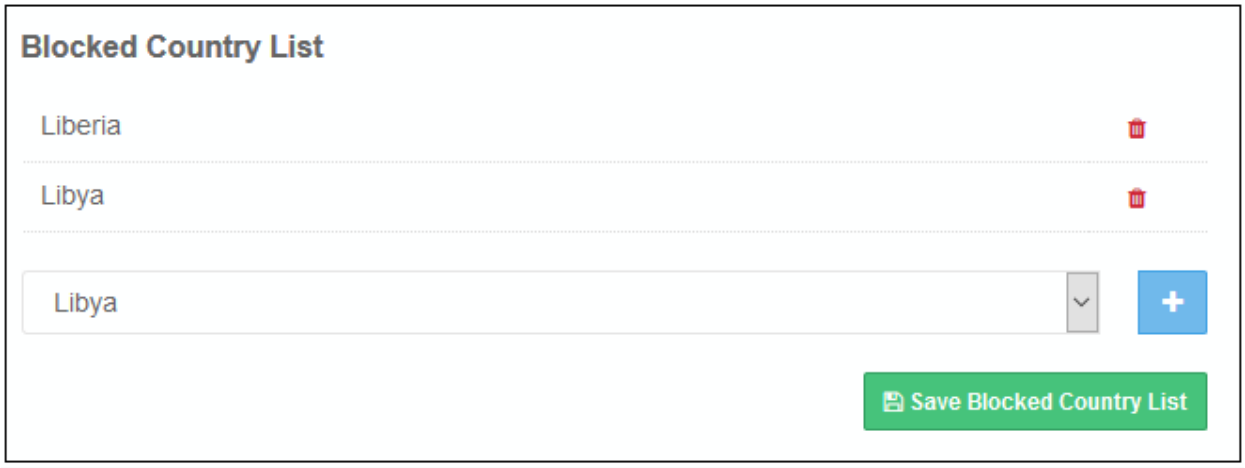
The list of SHA1 hash values already uploaded will be displayed.

- 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.

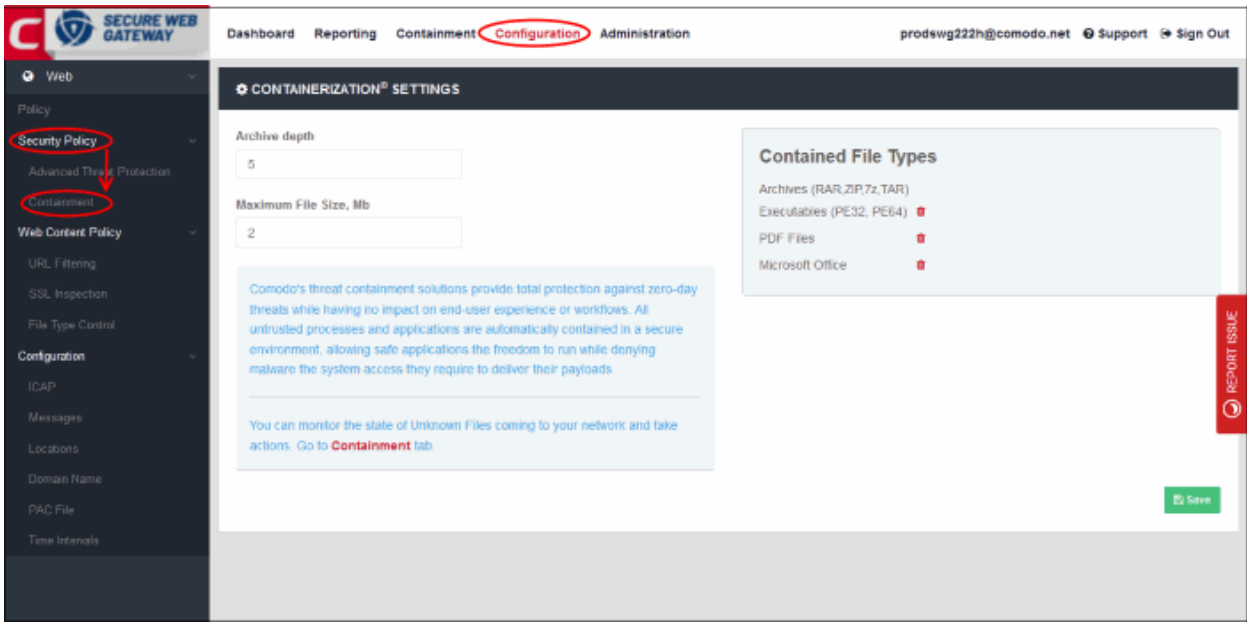


- Select the country from the drop-down and click the '+' button
- Click 'Save Blocked Country List' to save your changes
- To remove a country from the list, click the trash can icon beside it.

6.1.2 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'.



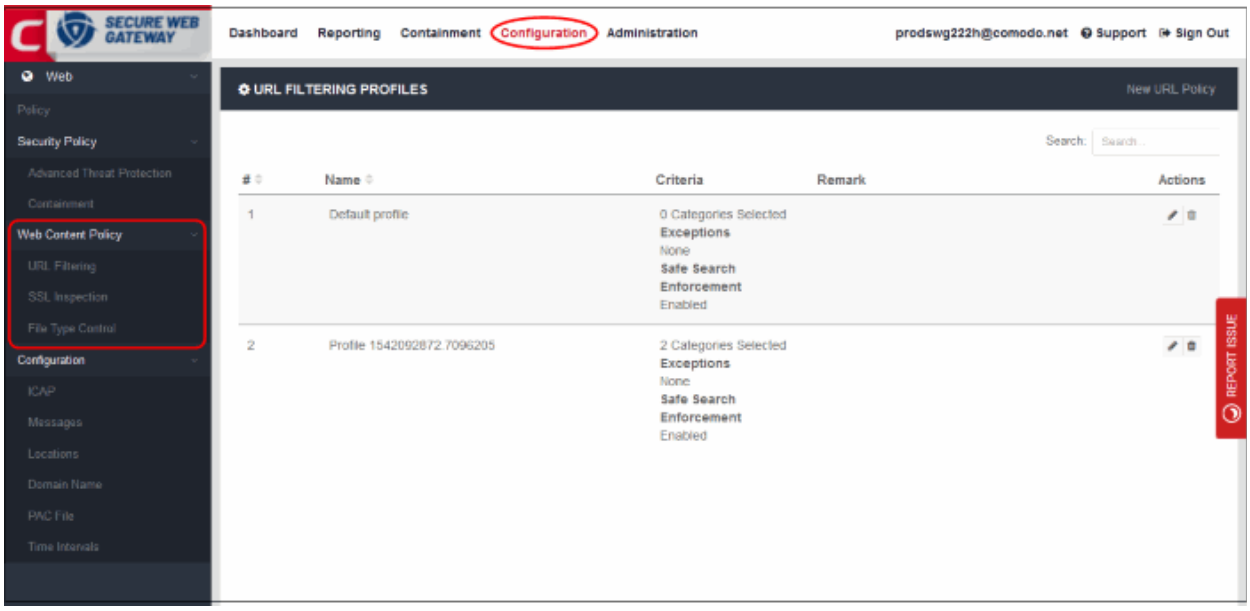
- Archive Depth - Maximum level the archive files will be unpacked to check for file within archive files. Enter the value till which the zip files will be checked. If the archive depth is more than the provided value, the files inside the exceeded layer will not be checked. For example, if the value 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 Comodo 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.

6.2 Web Content Policy

There are three elements in a web content policy:

- **URL Filtering** - Configure which categories of website should be allowed or blocked. You can also create your own domain whitelist or blacklist.
- **SSL Inspection** - Check whether the sites visited by your users have a trusted SSL certificate installed. You can allow or block the connection if they do not. Enable decryption and scanning of encrypted traffic in order to apply Comodo Secure Web Gateway policies.
- **File Type Control** - Restrict which file types can be downloaded by your users. Block downloads of specific file extensions from sites in specific categories.

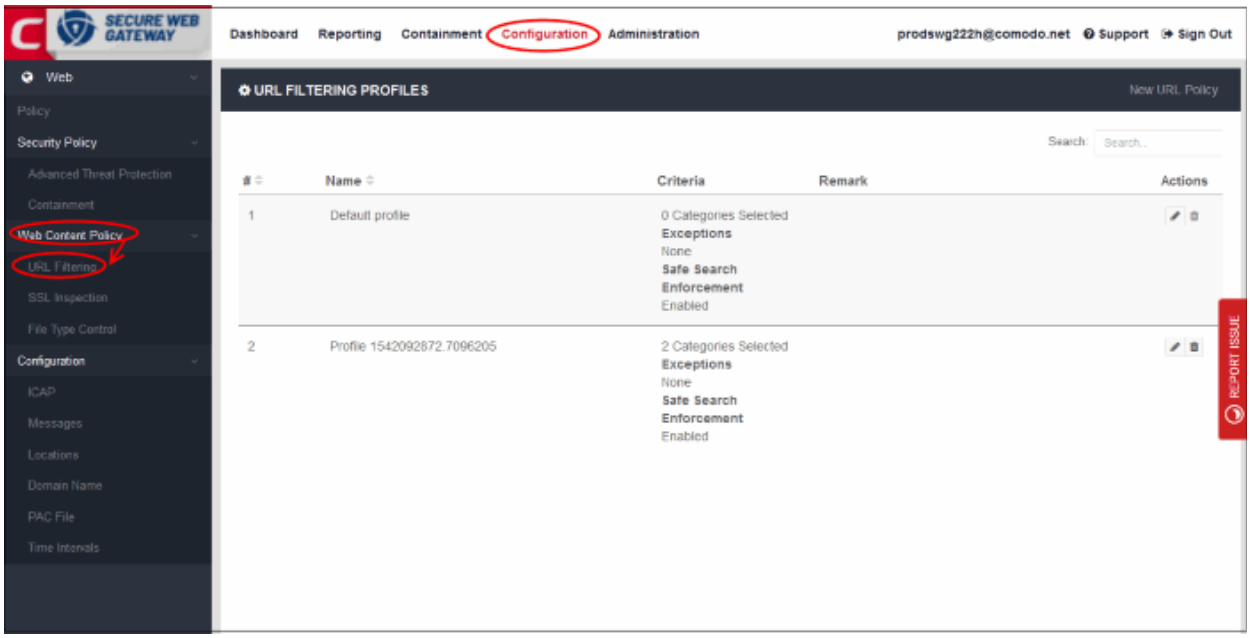


Click on the following for more details:

- **Manage URL Filtering Policies**
- **Configure SSL Inspection Setting**
- **Manage File Type Control Rules**

6.2.1 Manage URL Filtering Policies

- Click 'Configuration' > 'Web Content Policy' > 'URL Filtering'
- URL filtering policies let you block or allow access to websites of a certain type.
- You can add multiple website categories to a single profile.
- You can also define your own domain whitelist and blacklist.
- Whitelists and blacklists over-rule category rules. For example, if you block the 'News' category but add cnn.com to the whitelist, then your users can access cnn.com but cannot access any other news site.



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.

Search option

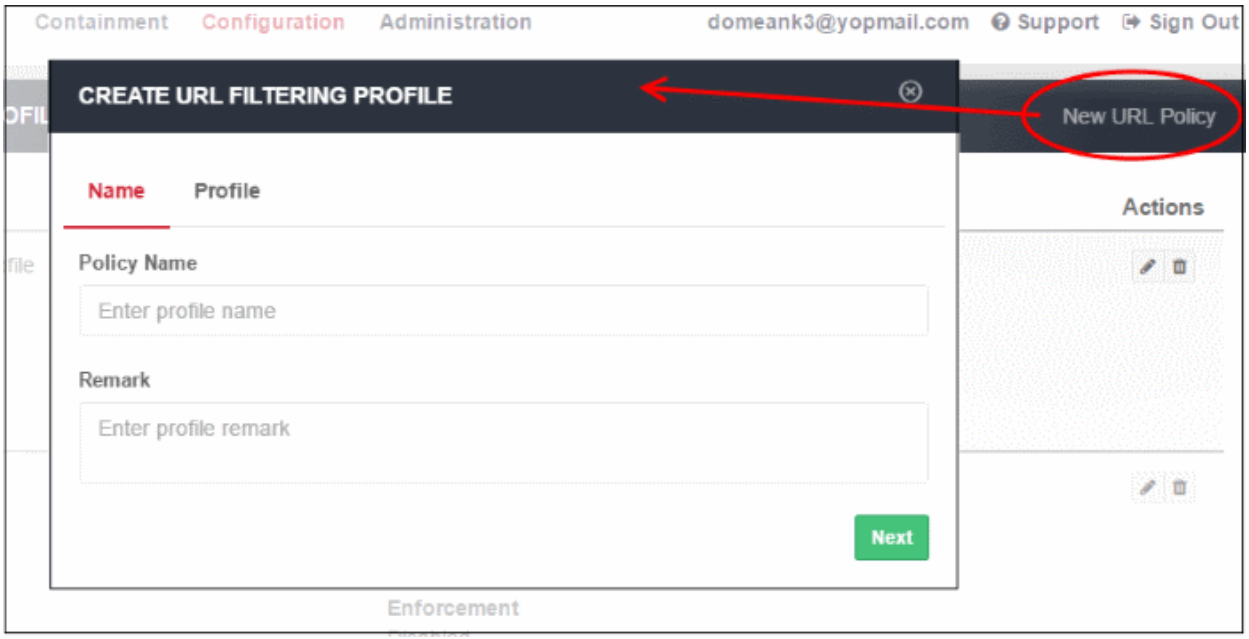
- Enter the search parameters fully or partly in the 'Search' field. The screen will display the matching results.

The interface allows you to:

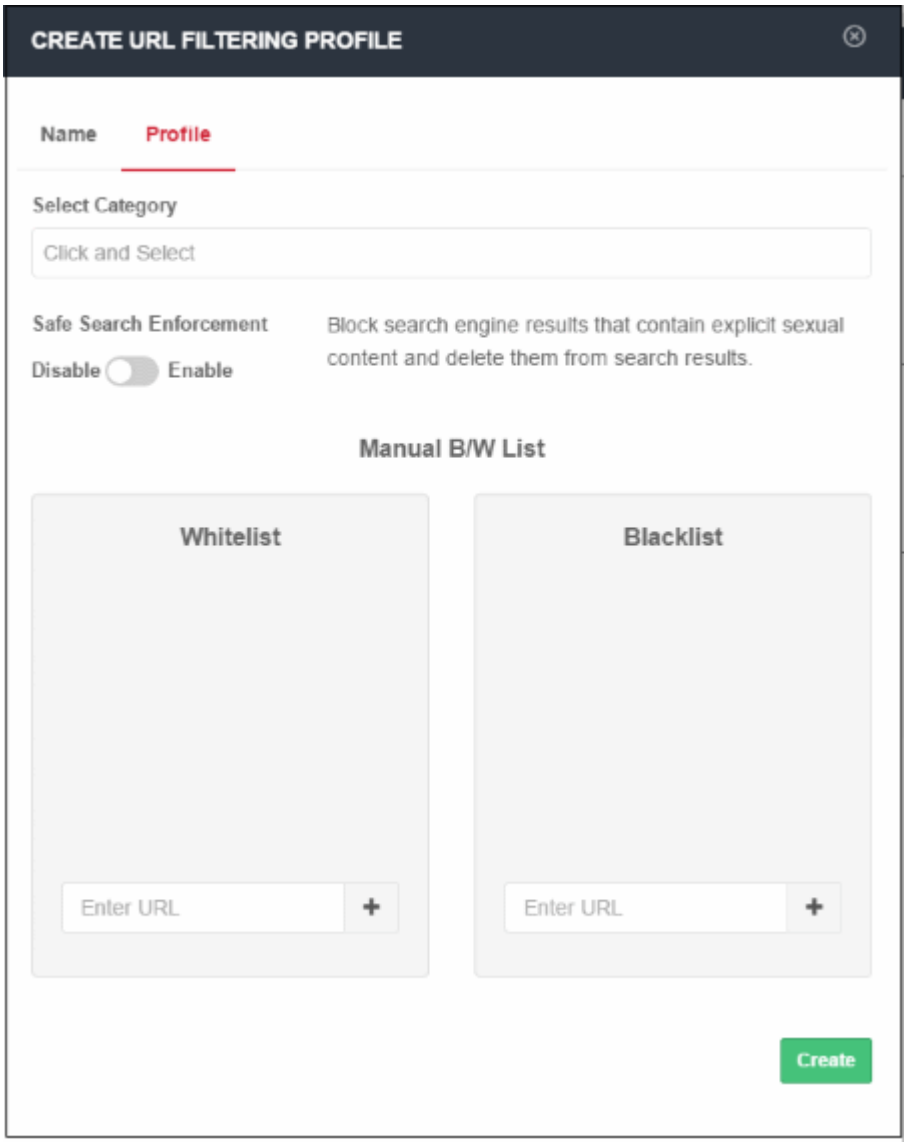
- **Create a new URL policy**
- **Edit an URL policy**
- **Delete an URL policy**

Create a new URL policy

- Click 'New URL Policy' at top-right

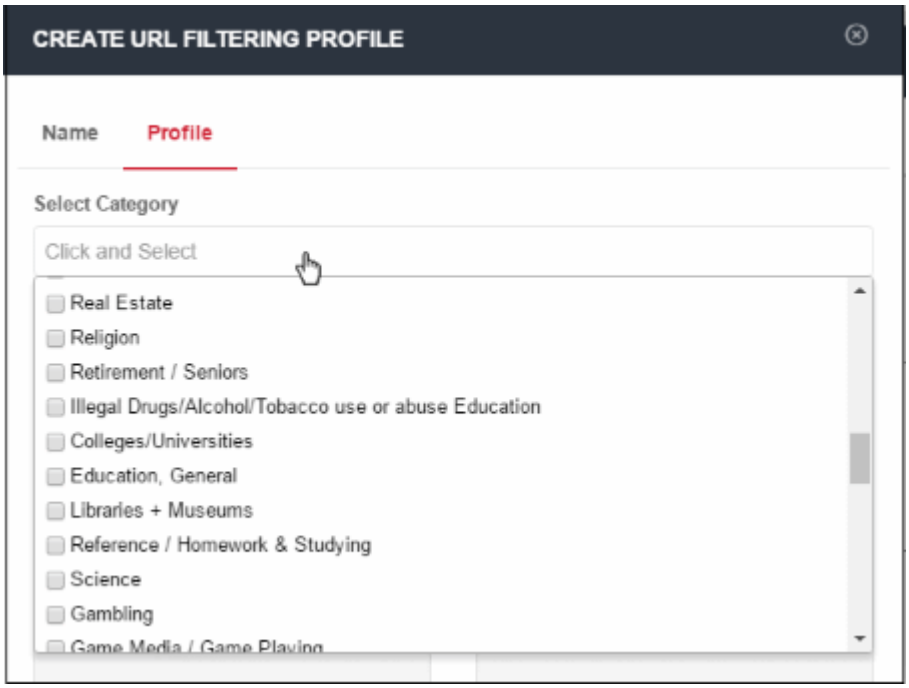


- Name
  - Policy Name – Create a label for the URL filtering profile.
  - Remark – Add helpful comments about the profile.
- Click 'Next' or 'Profile' to specify categories:

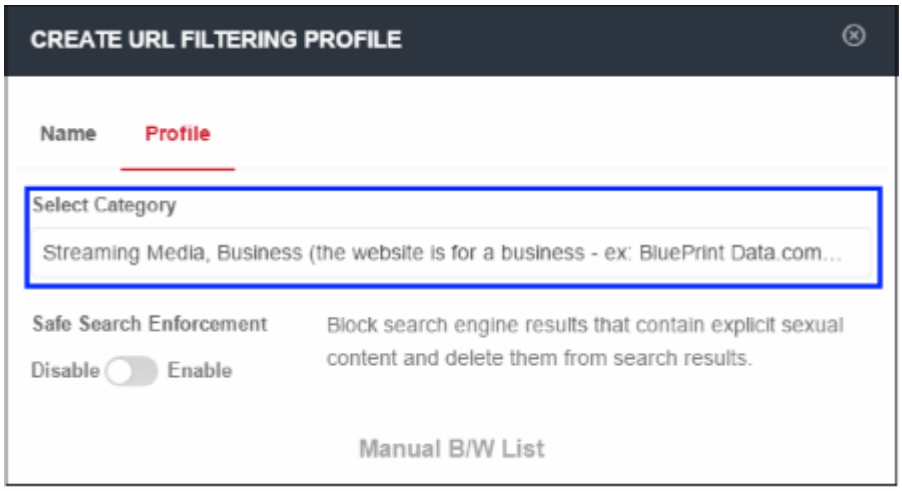


Category

- 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.

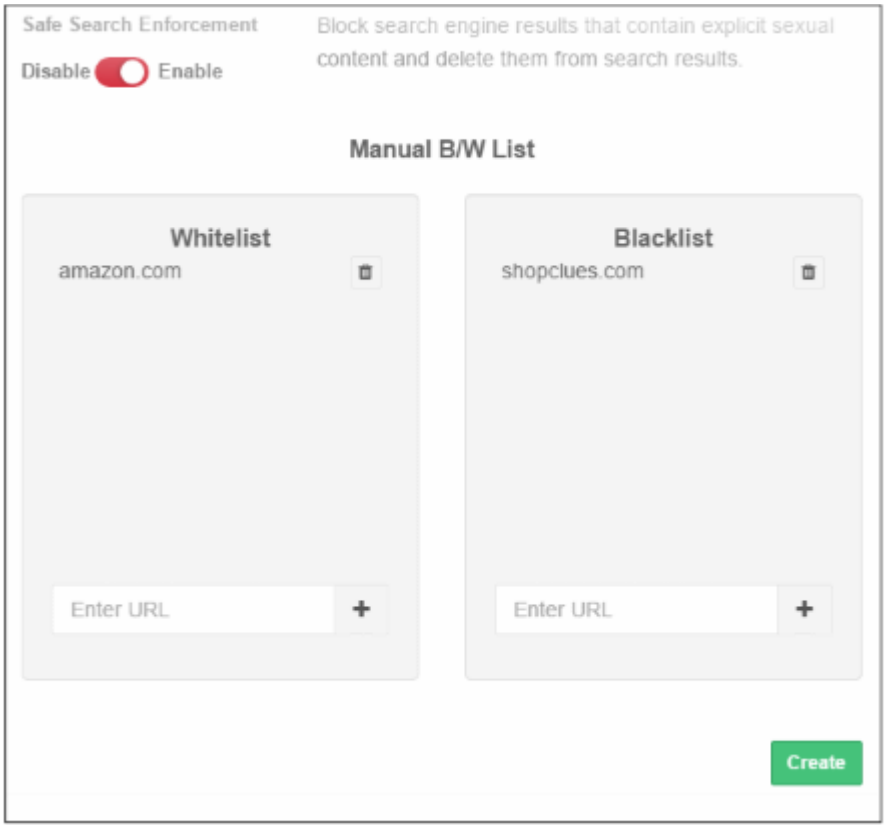
Safe Search Enforcement

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**' in the '**Configuring Advanced Threat Protection Settings**' section for more details.

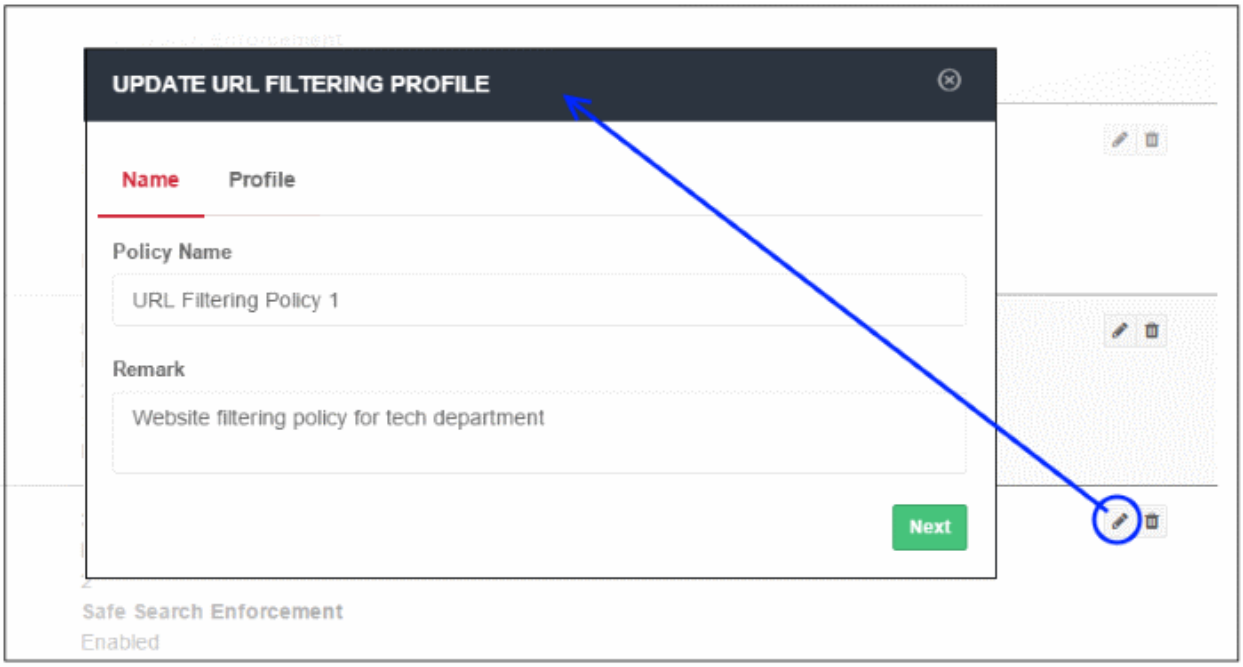


  - Whitelist - Add domains that you want to exempt from SWG URL filtering rules. Please note the list here takes priority over the category setting. Make sure the sites that are whitelisted are safe. Click the '+' button after entering the domain name in the field. To remove a domain name, click the trash 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 to Networks**' for more details.

Edit an URL policy

- To update an URL filtering policy, click the edit button beside the rule



The 'Update URL Filtering Profile' dialog will be displayed. Modify the name, remark, category selection and/or B / W list per your requirements.

- Click the 'Save' button

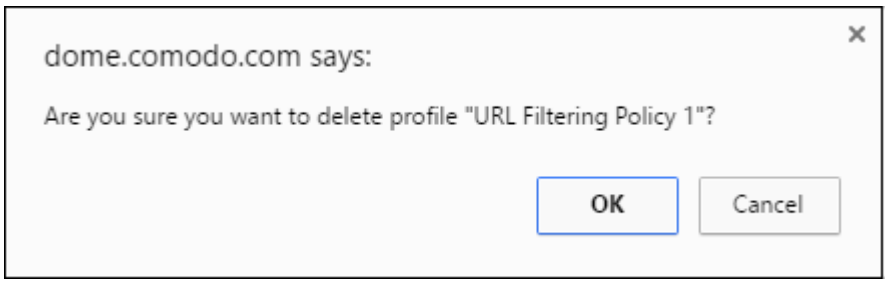
Please note that the profiles containing the rule will also be updated according to the new settings and name.

Delete an URL policy

If a URL policy is deleted, the default URL filtering policy will be applied to endpoints / networks.

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

A confirmation dialog will be displayed.



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

6.2.2 Configure SSL Inspection Settings

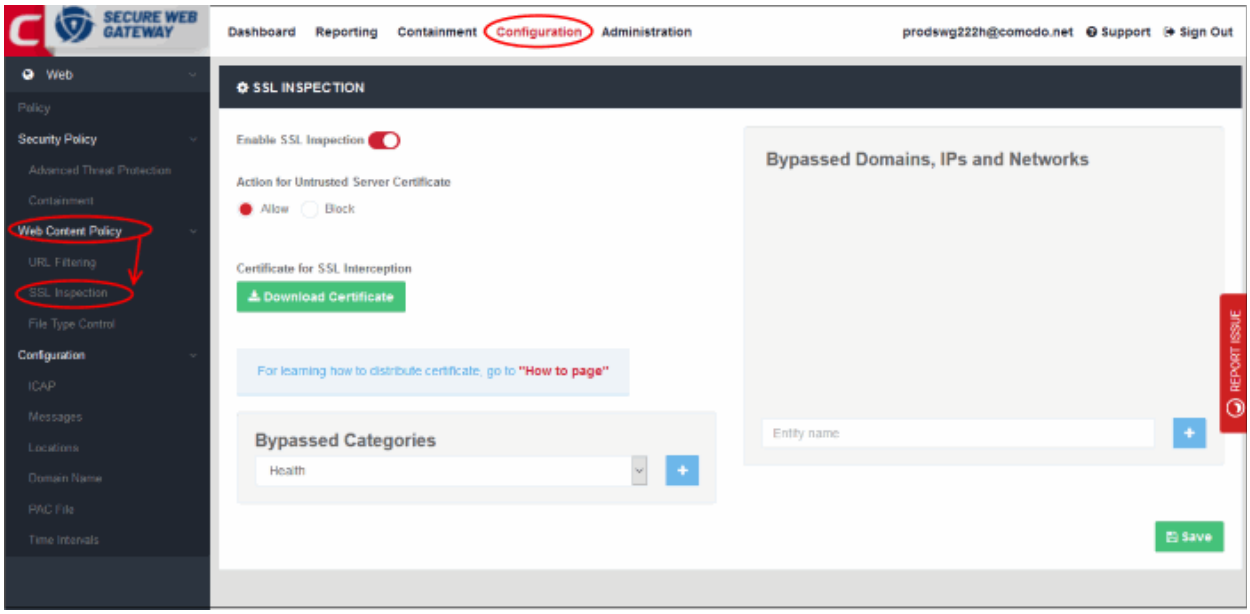
- Click 'Configuration' > 'Web Content Policy' > 'SSL Inspection' to view this interface.

The 'SSL Inspection' area lets you:

- Specify whether Comodo Secure Web Gateway (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

Contact Comodo at **domesupport@comodo.com** to specify website categories to bypass Comodo Secure Web Gateway filtering engine and allow users to access websites in these categories directly.



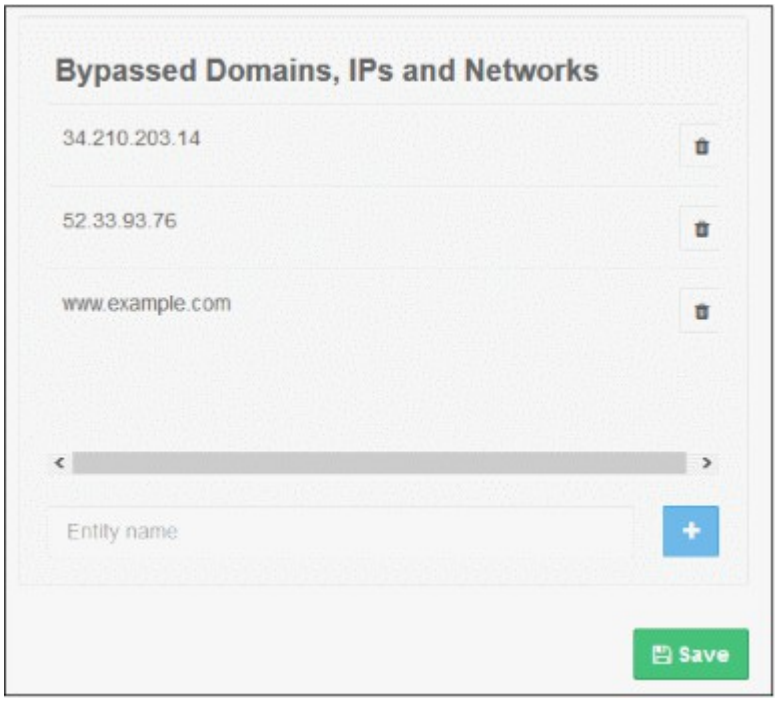
Enable SSL Inspection

- 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.

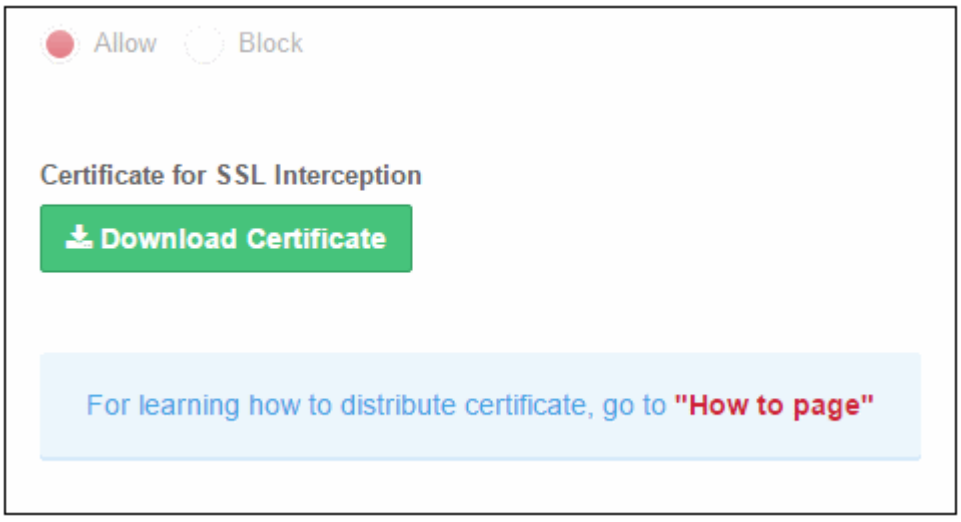
- Enter the URL of a website, domain, domain name with wildcard, IP or network in CIDR format in the field and click the '+' button. Repeat the process to add more exceptions.



- 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 SWG certificate in order to decrypt and apply policy to HTTPS websites.
- Once the certificate is installed, 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 get Comodo SWG to generate a certificate for you, or you can upload an existing certificate.
  - 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.

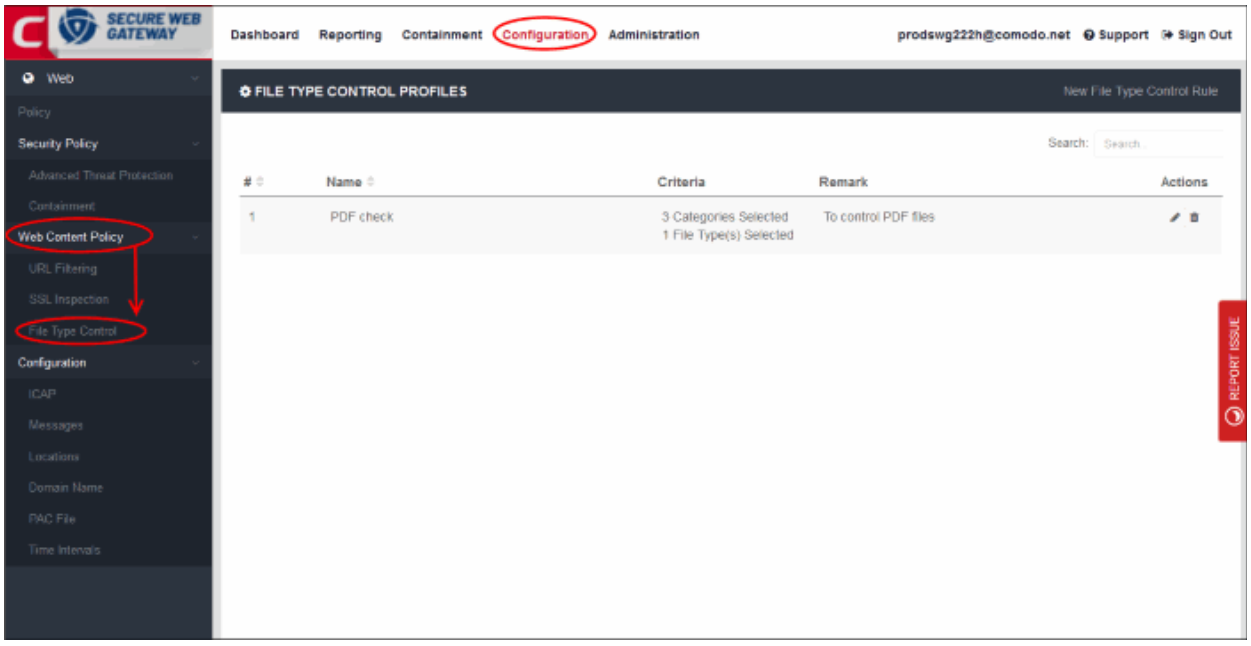
- Upload Combined PEM File – To use your own SSL certificate, click 'Browse...' , select the certificate then click 'Upload'.
- Click 'Download Certificate'. Follow the instructions under 'Browsers' / 'Windows Group Policy" for help to install the certificate.

Bypassed Categories

The list of bypassed categories is provided by Comodo. Sites in bypassed categories are not subject to 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.

6.2.3 Manage File Type Control Rules

- 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.

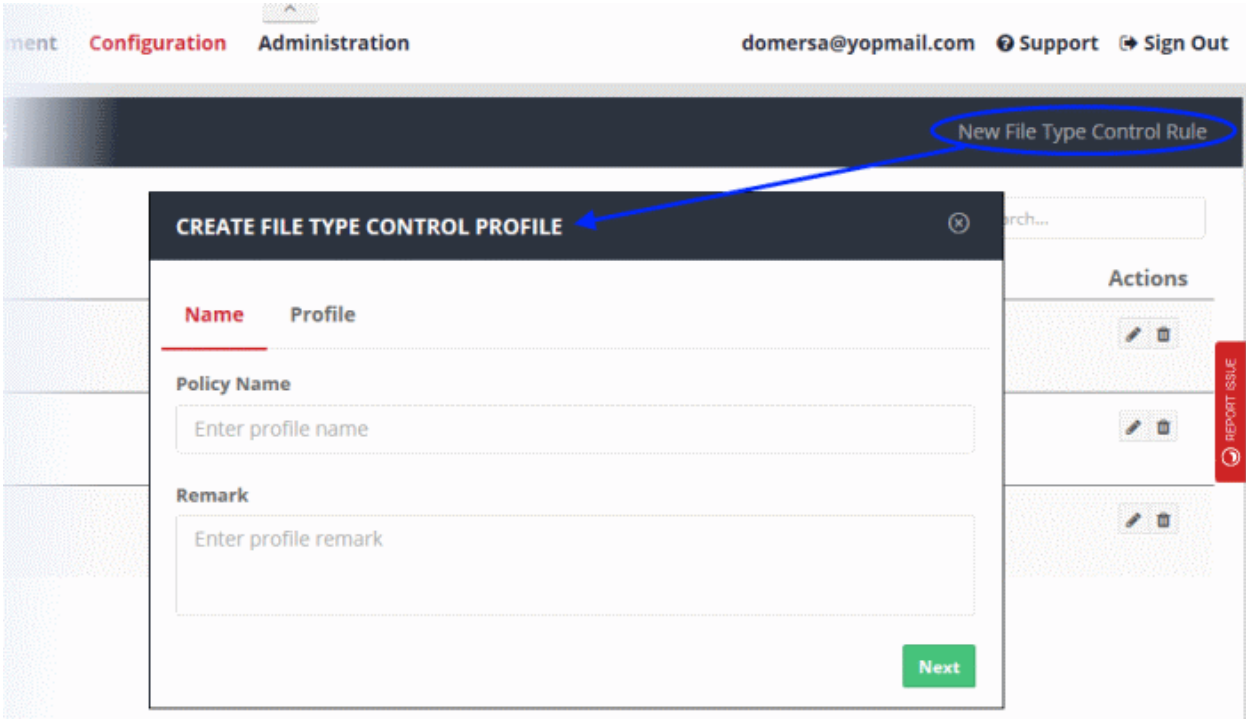
The search box at top-right lets you search for terms in the '#', 'name', 'criteria' and 'remark' columns.

The interface allows you to:

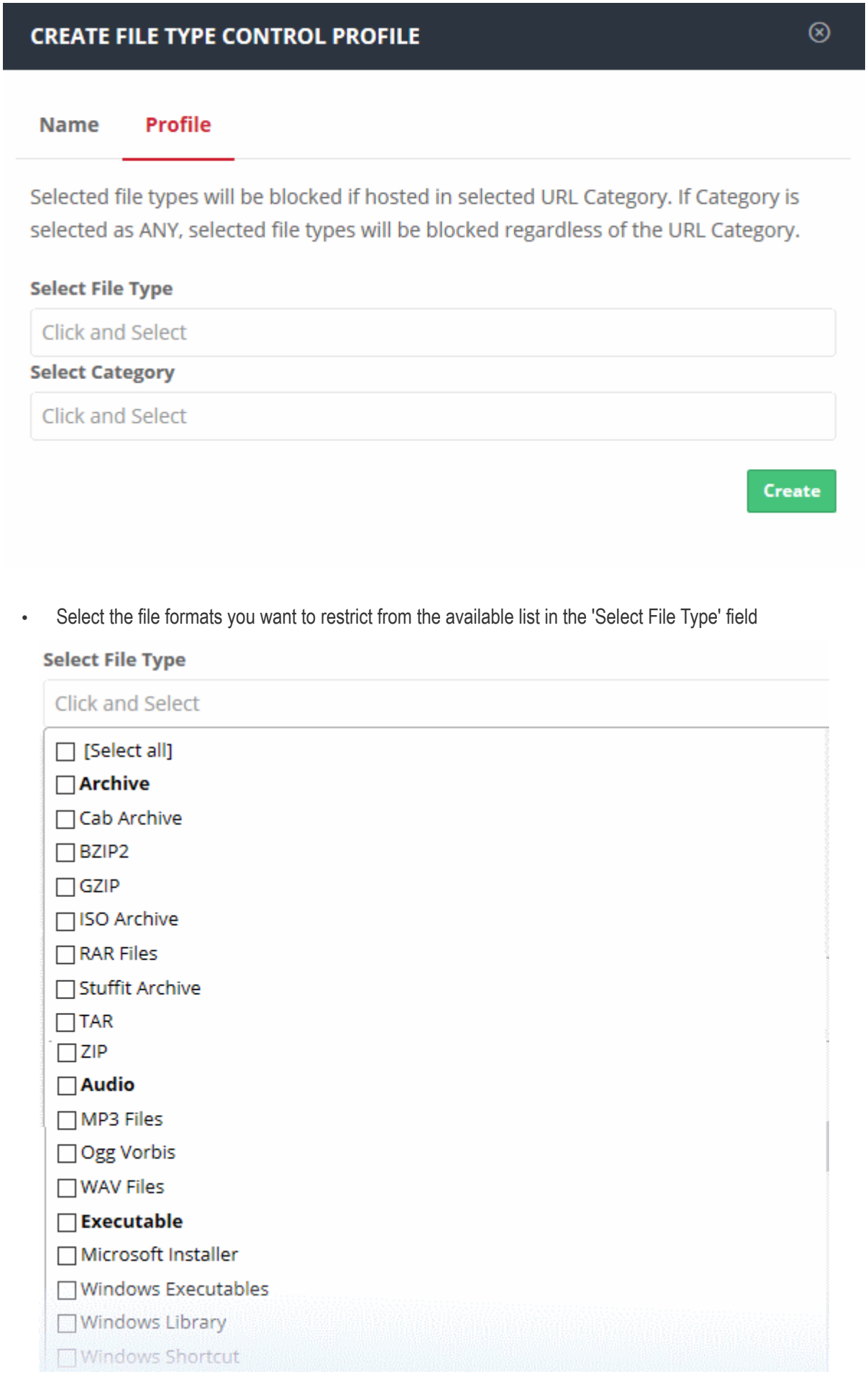
- **Create a new File Type Control rule**
- **Edit a File Type Control rule**
- **Delete a File Type Control rule**

Create a new File Type Control Rule

- Click 'New File Type Control Rule' at the top-right

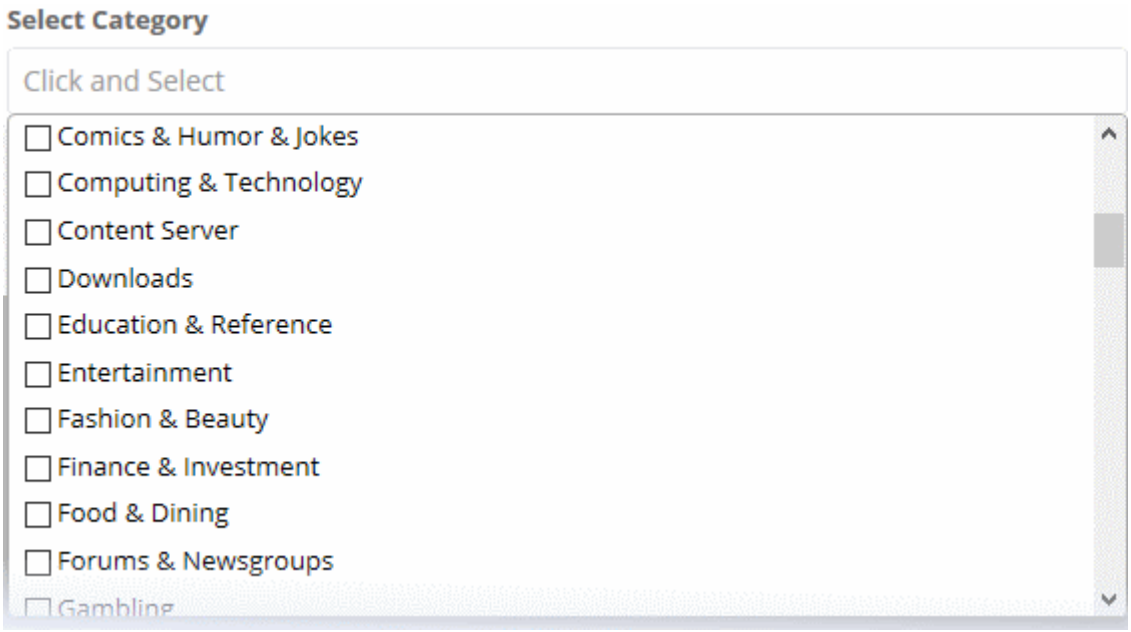


- Name:
  - Policy Name – Create a label to identify the policy.
  - Remark – Add comments to describe the policy.
- Click 'Next' or 'Profile' to specify file types and categories:



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

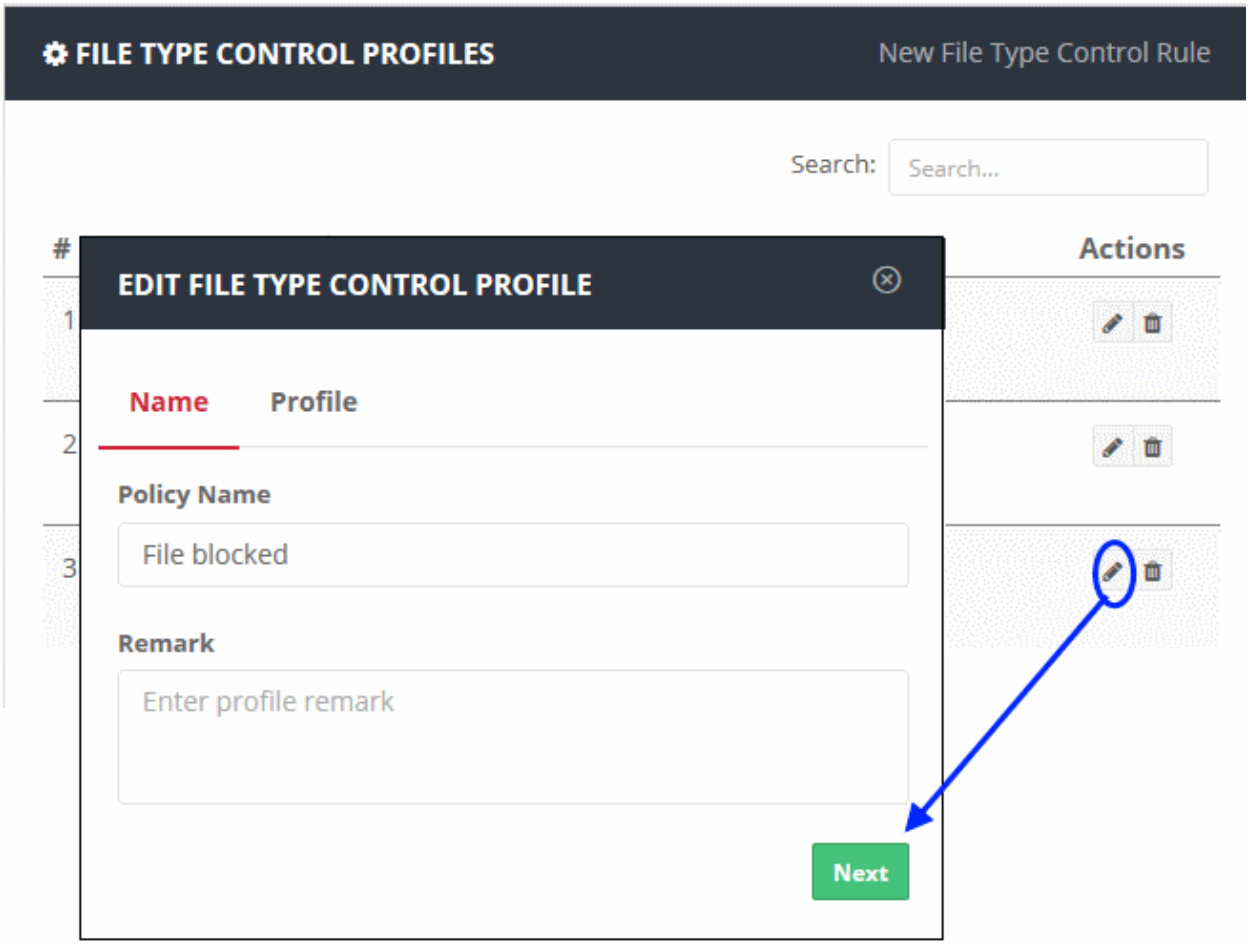
- Select the category of websites from where you want to the selected file types to be blocked.



- Click 'Create'

Edit a File Type Control Rule

- To update a file type control policy, click the edit button beside the rule



The 'Edit File Type Control Profile' dialog will be displayed. Modify the name, remark, file type and category selection as per your requirements.

- Click the 'Save' button

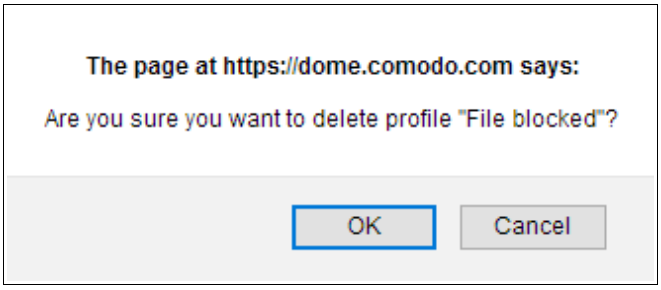
Please note that the profiles containing the rule will also be updated according to the new settings and name.

Delete a File Type Control Rule

If a file type restriction rule is deleted, it will be removed from any policies in which it is present.

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

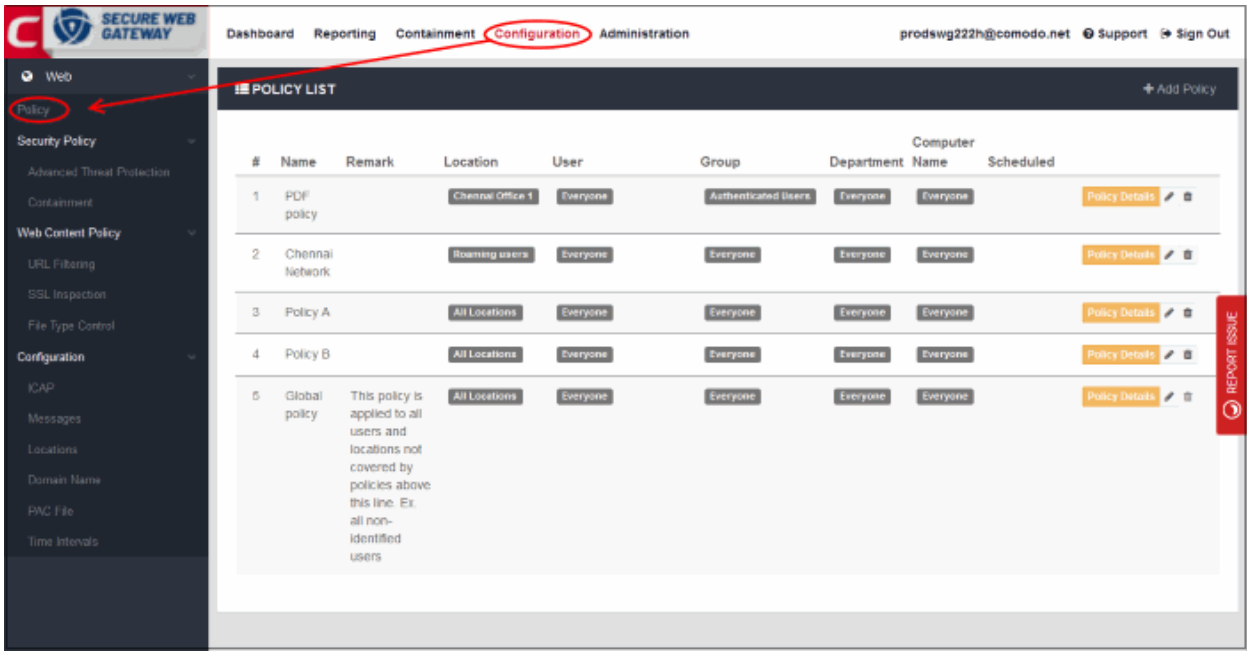
A confirmation dialog will be displayed.



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

7 Apply Policies to Networks

- Click 'Configuration' > 'Policy' to open the policy list.
- After enrolling networks as explained in '**Connect your Network / Devices to Comodo Secure Web Gateway**', the default global policy is applied to your endpoints.
- 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.
  - Note 1: To apply user specific policies, you must enable user authentication.
  - Note 2: To apply computer specific policies, you must select 'Hosted DB' as user authentication method.
    - Click 'Administration' > 'User Management' to add users/groups/departments/computers. See '**User Management**' for help
    - Click 'Administration' > 'Authentication Settings' to configure user authentication. See '**Configure User Authentication Settings**' for help



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. See '**Manage Users**' to learn how to add end users.
Location	The name of the network location to which the policy is applied. See '**Manage Trusted Networks**' for details on how to add Comodo SWG-connected networks / roaming users.
Group	The name of the group to which the policy is applied. See '**Manage User Groups**' for more information.
Department	The name of the department to which the policy is applied. See '**Manage Departments**' for more information.
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**. See '**Manage Computers**' for more information.
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 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

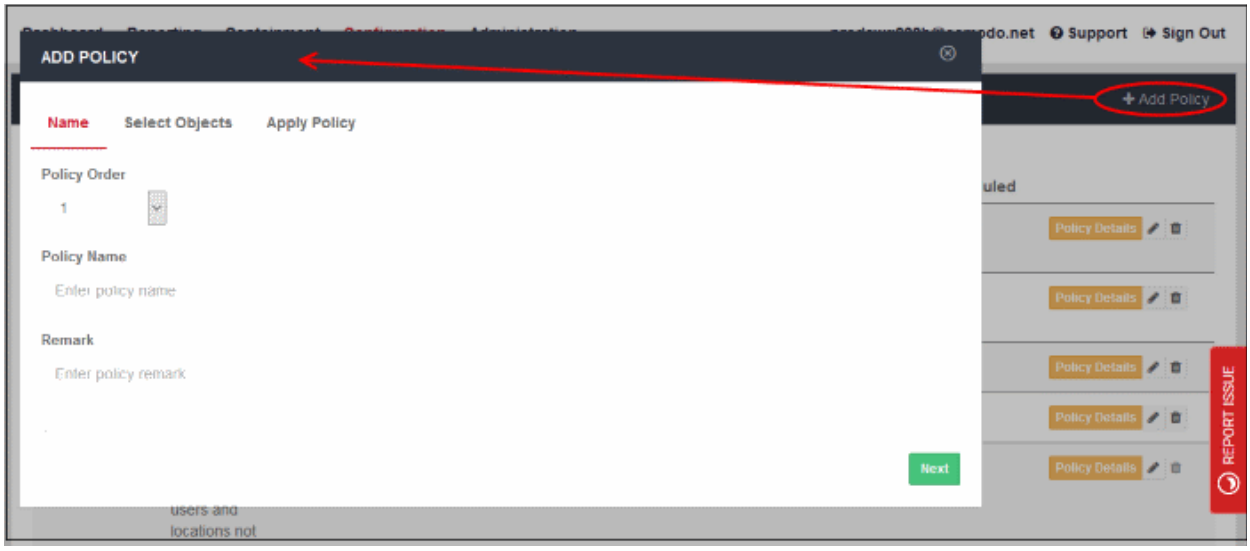
- Give policies which target a specific audience a higher rank than policies which cover large user bases. This is to ensure your targeted policies are not over-ruled by the policy above it. The 'All locations' and 'All Users' settings will over-rule every corresponding object below them if the policy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

The interface allows you to:

- **Add a new policy**
- **Edit a policy**
- **View policy details**
- **Delete a policy**

Add a new policy

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



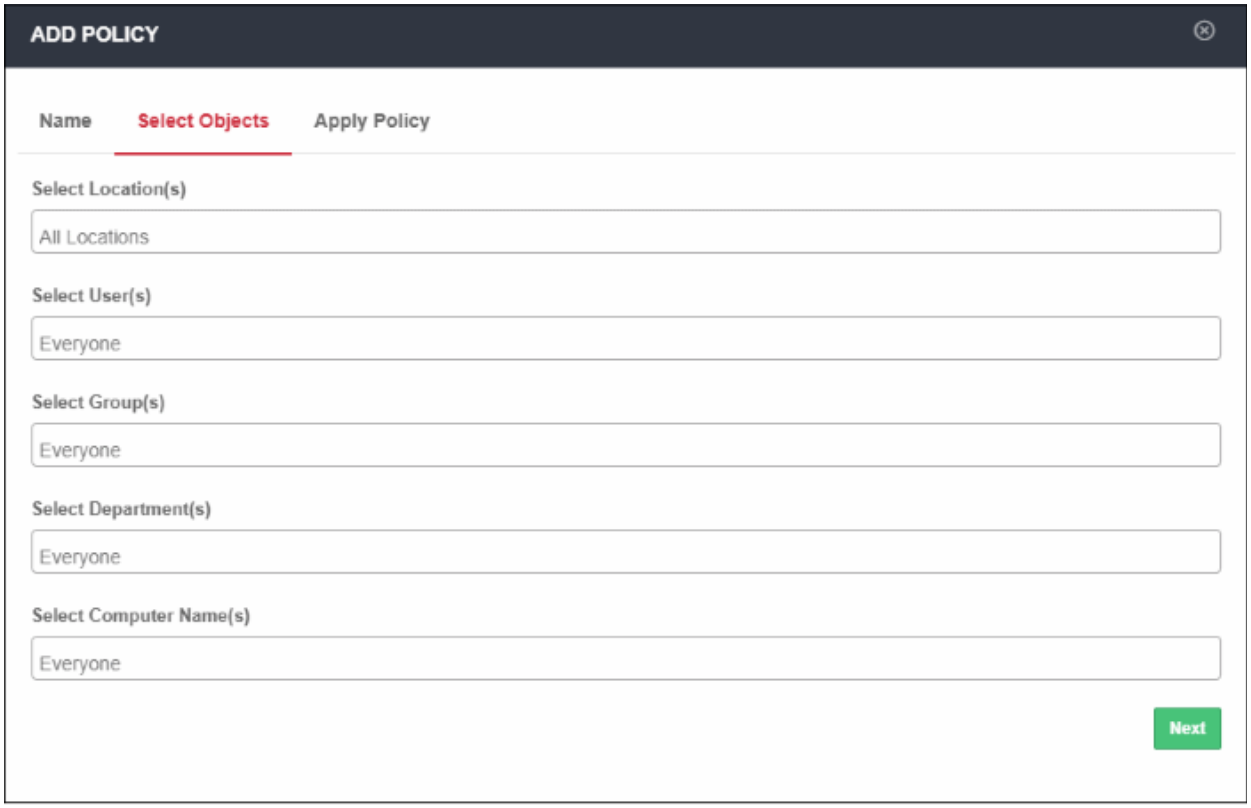
Step 1 - Policy Details

- 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.

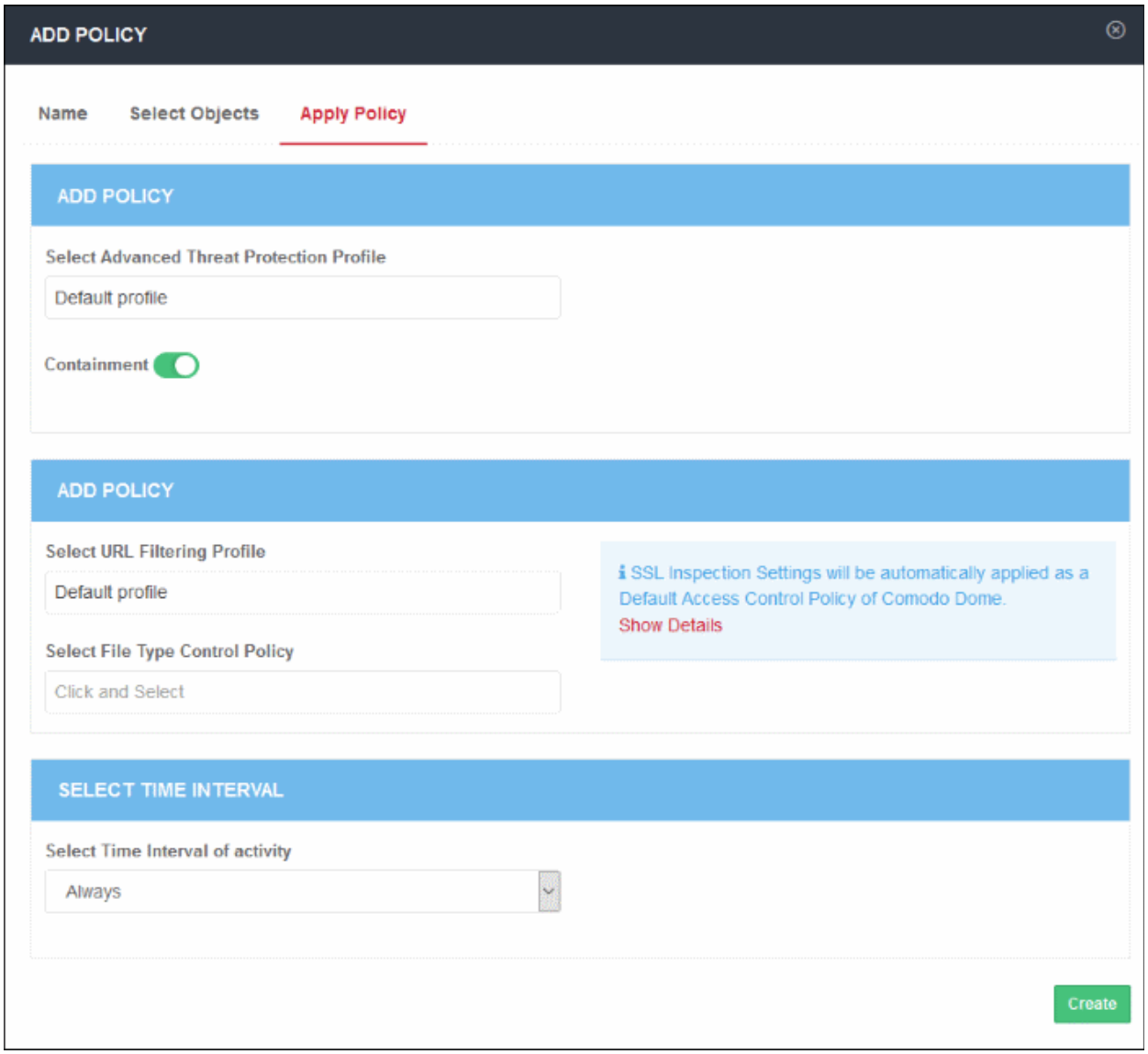


- **Location** - Select the required trusted network from the list. 'All Locations' is selected by default. You can add networks in the **Locations** area ('Administration' > 'Locations').
- **User** - Select the required users from the list. 'Everyone' is selected by default. You can add users in the **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. See '**Configure Containerization Settings**' for more details. Containment is enabled by default.

Add Access Control Profile

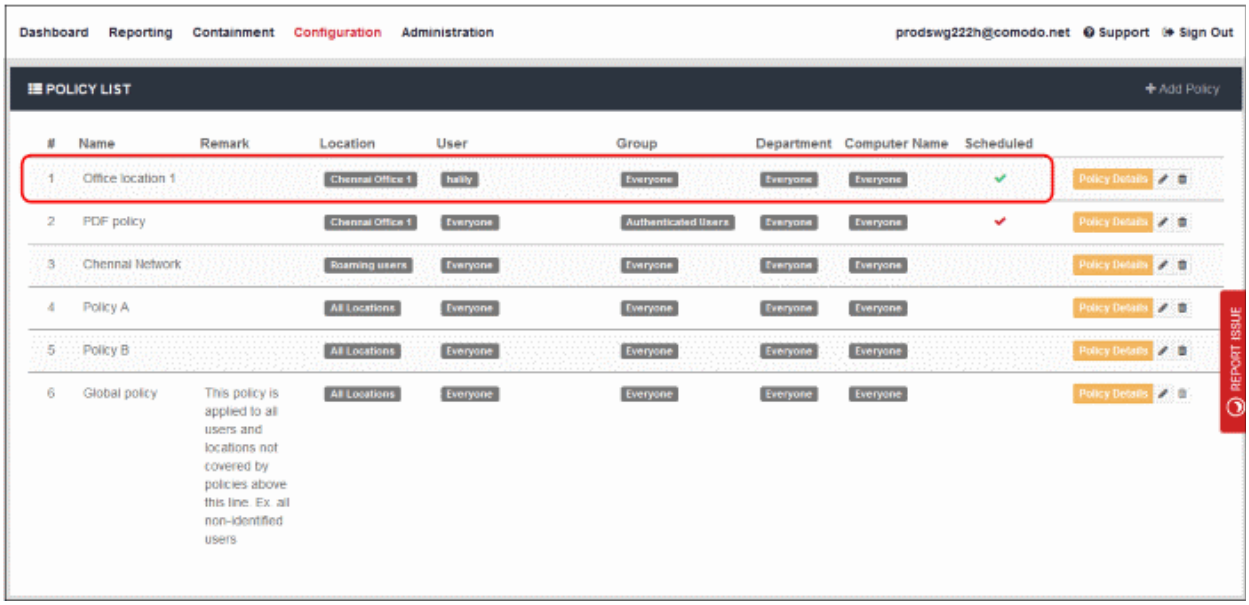
- Select URL Filtering Profile - The default profile will be selected. The drop-down will display the URL filtering profiles that are available in **URL Filtering** section. Select the appropriate URL filtering profile from the list.
- SSL Inspection Settings - Allows you to configure how Comodo SWG 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. See '**Configure SSL Inspection Settings**' for more details.
- File Type Control Policy - Displays file download restriction rules that were created in 'Configuration' > 'Web Content Policy' > 'File Type Control'. See **File Type Control Rules** for more about this area. 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.

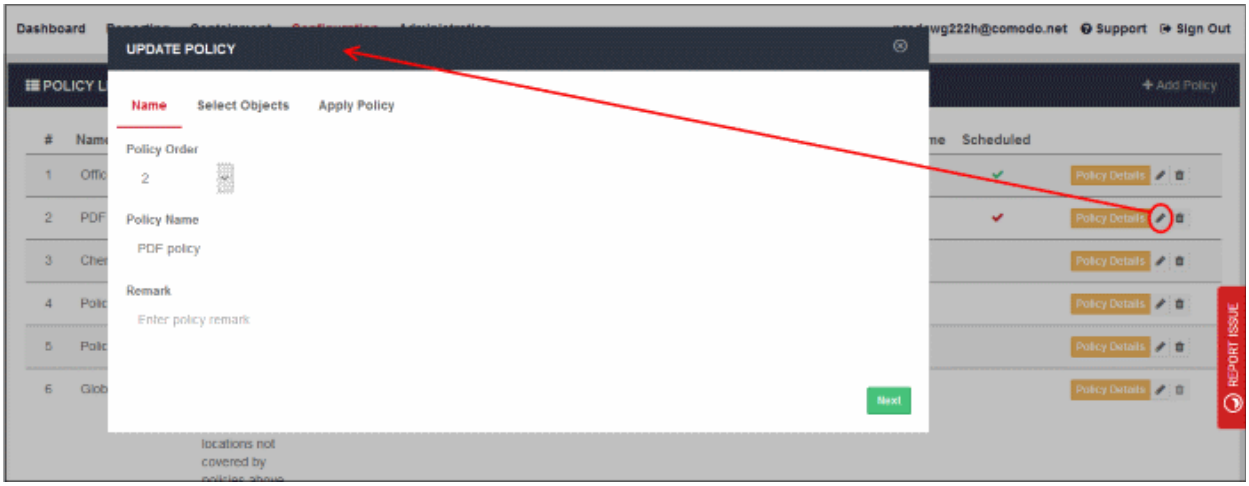
The drop-down lists the schedules that you have configured in Configuration' > 'Configuration' > 'Time Intervals'. See '**Configure Policy Time-Schedules**' for more information about pre defined schedules'. Select the schedule from the drop-down list. Note – Make sure to place a scheduled policy above a non scheduled policy.

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



Edit a policy

- To update a policy, click the edit icon beside it. The 'Update Policy' dialog will be displayed.

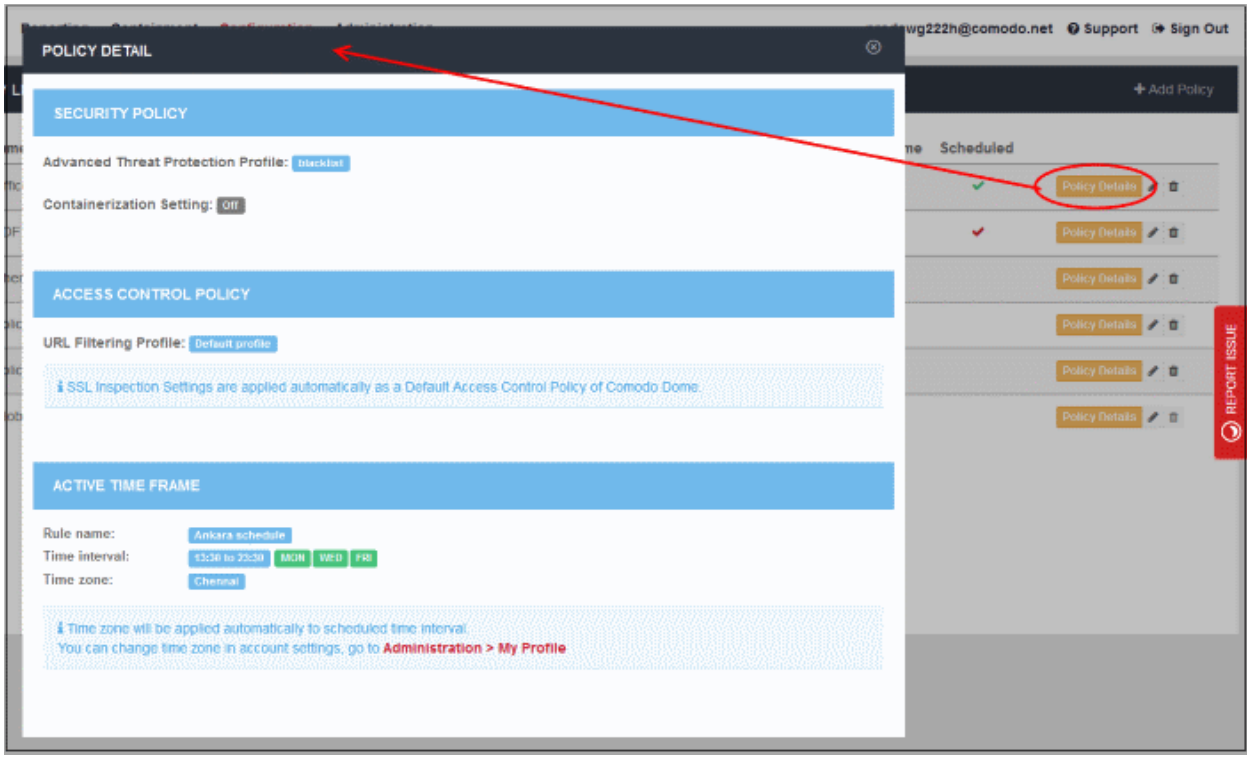


- Edit the name and other parameters as required. The process is similar to adding a policy as explained **above**.

Click 'Save' after modifying the policy. The policy will be updated for users to whom it is deployed.

View policy details

- To view the details of a policy, click 'Policy Details' beside it. The 'Policy Detail' dialog will be displayed.

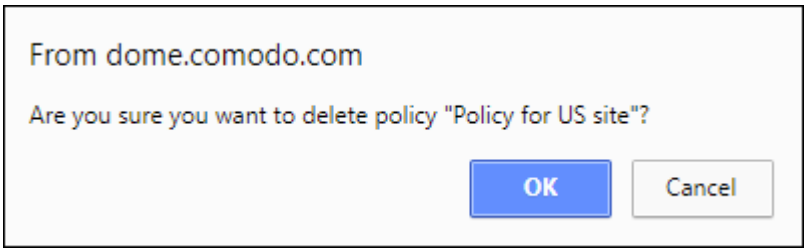


The 'Policy Details' dialog displays the details of profiles that are added for security and access control policy including containerization and SSL inspection settings.

- Click the 'X' mark at the top right to close the dialog.

Delete a policy

- Click the trash icon beside a policy that you want to remove from the list. Please note you cannot remove the default Global policy.



- Click 'OK' to confirm

When a policy is removed, Comodo SWG will deploy other applicable policies for the affected users. If no other policy is applicable, then the default global policy will be deployed.

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

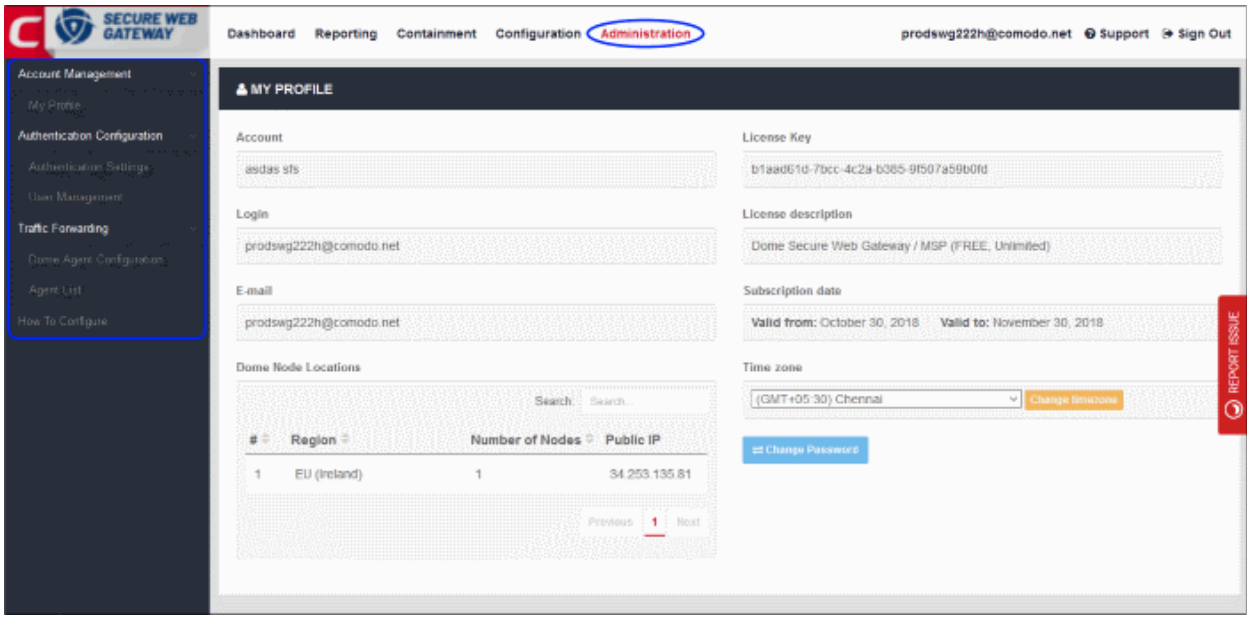
- Another user Angel is out of trusted location - Policy 2 will be applied since it matches the current location (Roaming) and other objects are 'Everyone', which includes Angel.

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'.

8 Administration

- Click 'Administration' in the top-navigation to open this area.
- The administration area lets you add users, configure user authentication and create new groups/departments. After adding users here, you can deploy policies to them in 'Configuration' > 'Policies'
- You can also download and install the SWG agent to protect users outside the network. This includes road-warriors whose IP changes dynamically. Devices with the agent can be viewed in 'Administration' > 'Traffic Forwarding' > 'Agent List'. See '**Connect your Roaming Devices to Comodo Secure Web Gateway**' for help to add roaming devices.
- You can also view details about your account such as license key, login and more.
- Click 'Administration' in the top-menu to open this area.

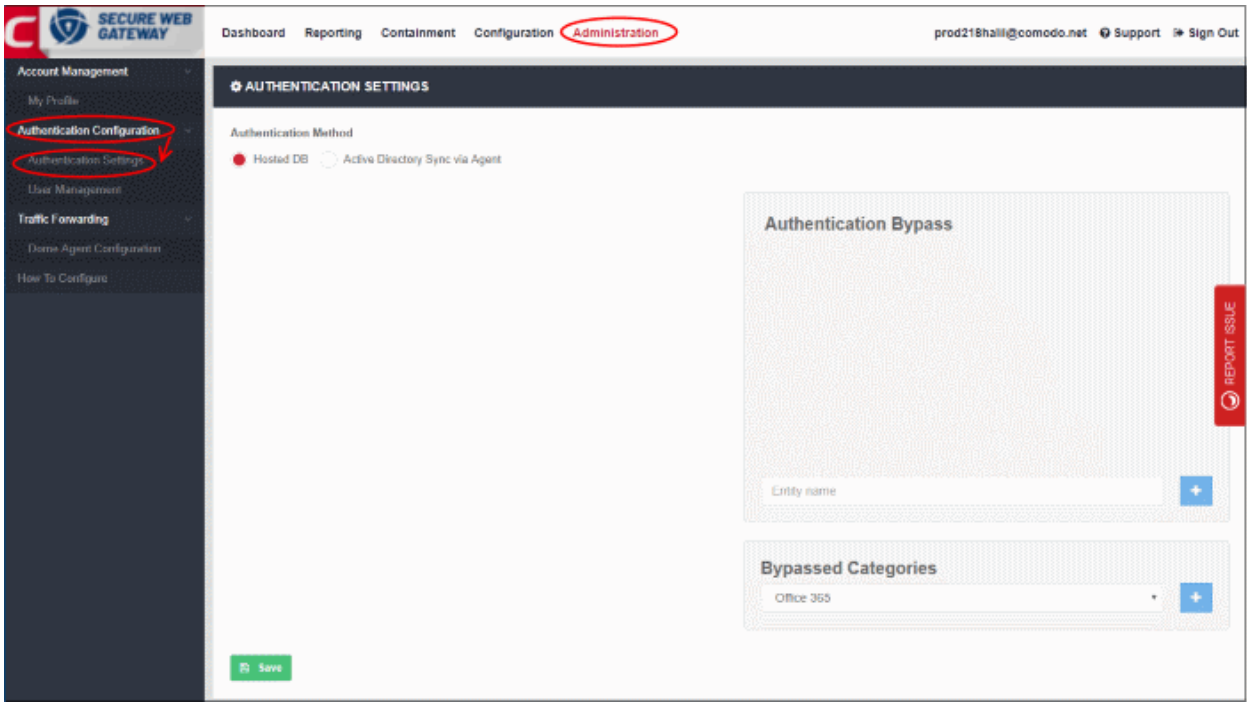


The following sections explain more about:

- **User Authentication Settings**
- **User Management**
- **My Profile**

8.1 Configure User Authentication Settings

- Click 'Administration' > 'Authentication Configuration' > 'Authentication Settings' to open this interface.
- You have to choose a user authentication method in order to deploy user-specific policies.
- There are two methods available - 'Hosted DB' and 'Active Directory'. You can select only one authentication method per account.
- After **connecting your networks** to Comodo Secure Web Gateway and adding them to 'Locations', the default security and URL filtering polices will be applied to all endpoints in your networks.
- 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 '**User Management**' if you need help with this.



Authentication Method

- 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 as explained in **Connect your Network to Comodo Secure Web Gateway**.
- 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

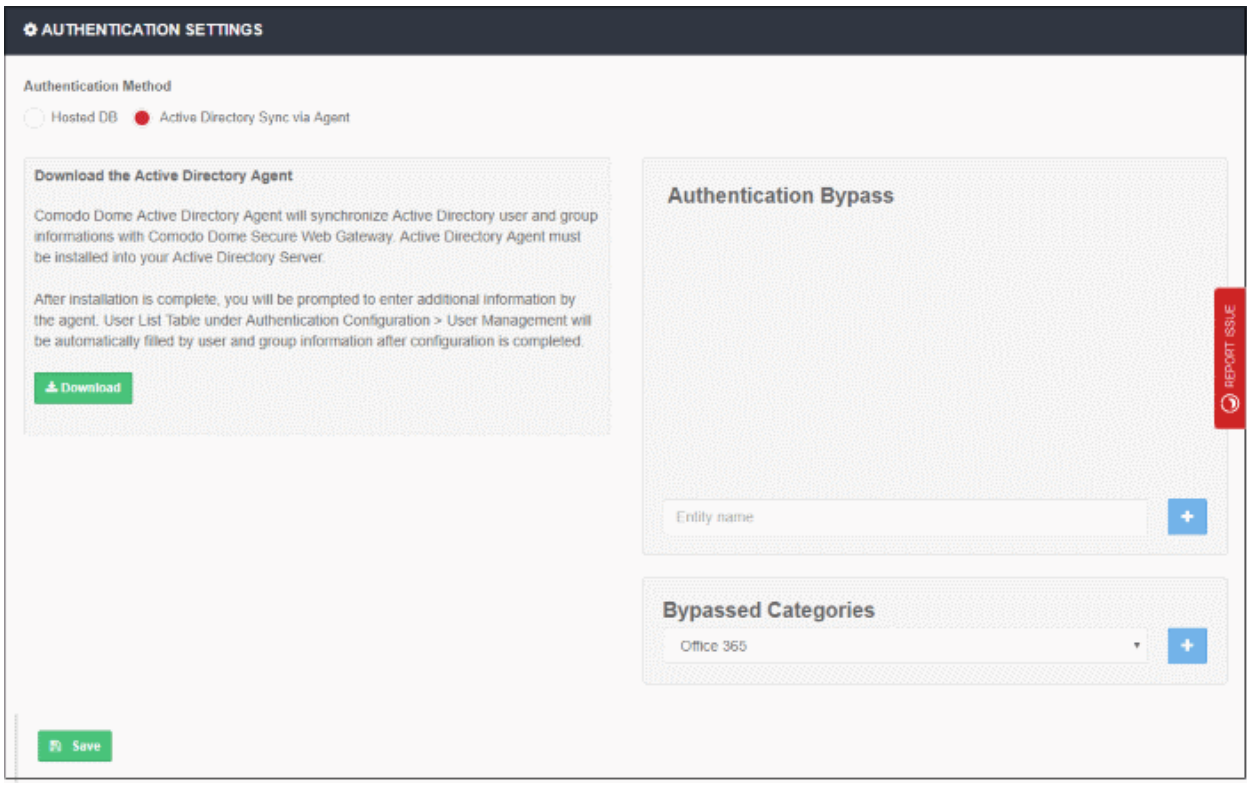
A user database hosted on SWG will be used for authentication and identification. You will need to provide additional

details including group and department in the 'Add User' dialog. End users will have to provide the credentials when the browser asks for basic authentication.

Active Directory

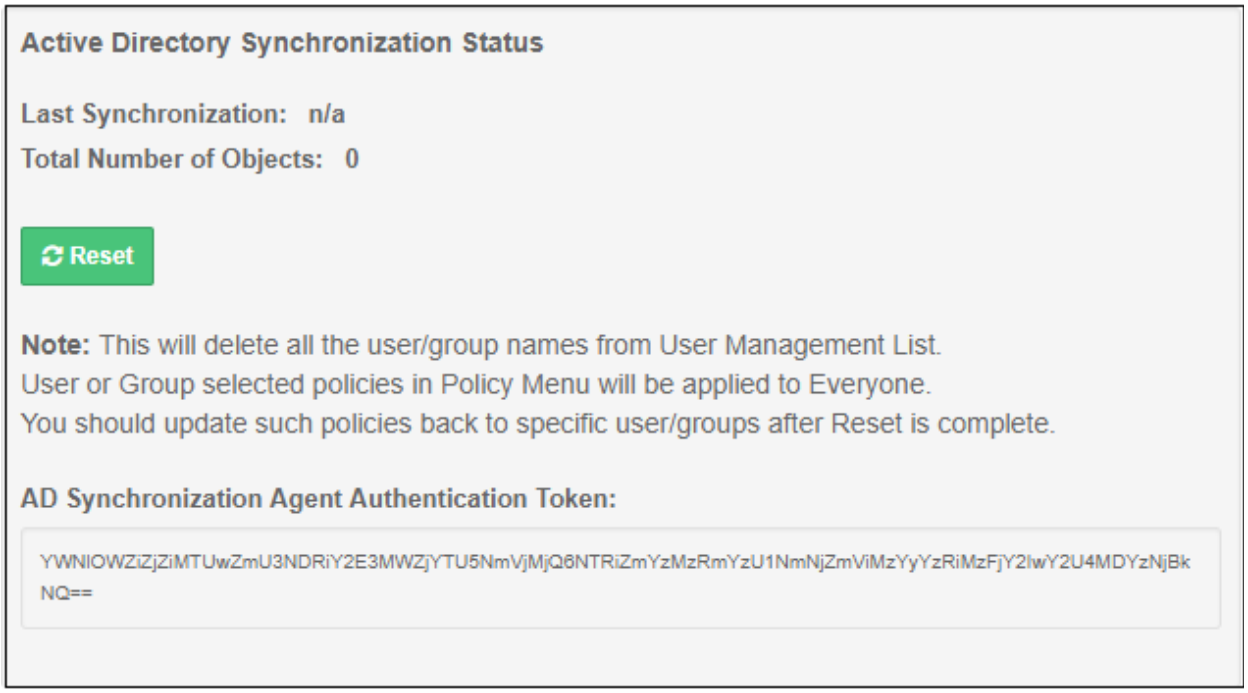
Users are authenticated using Active Directory. To use this method, you need to download the SWG AD agent and install it in your AD server. After installation and configuration, AD users and groups will be automatically enrolled to SWG and be visible under 'User Management'.

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



- Click 'Download'
- The agent setup file will be downloaded to your default location
- Next, click 'Save'

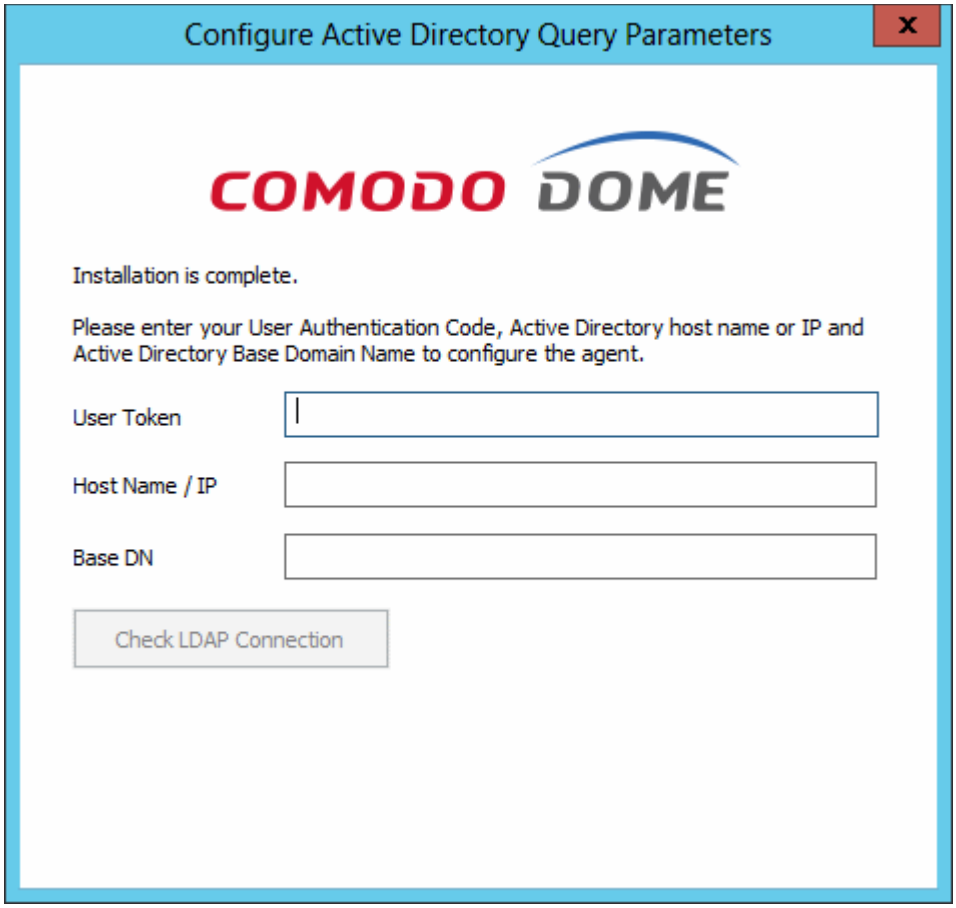
A unique AD sync agent authentication token will be generated.



- 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 Comodo SWG AD agent

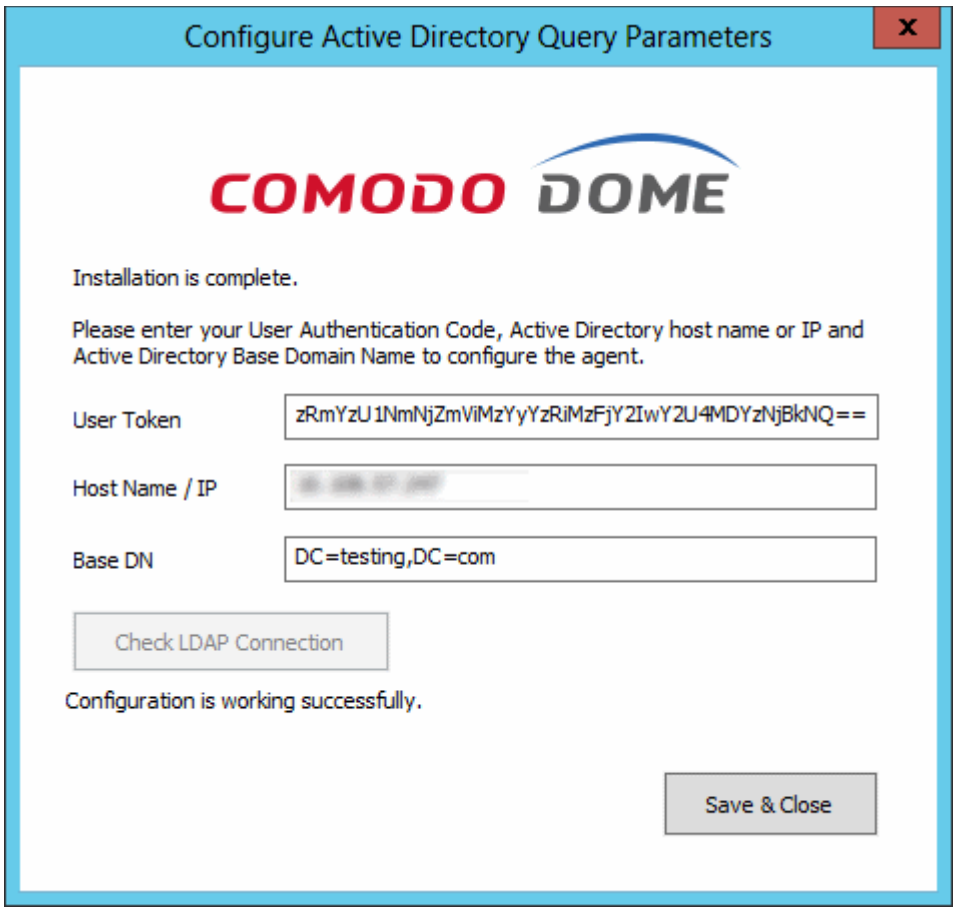
- Run the setup file and complete the AD connection details form:



- 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

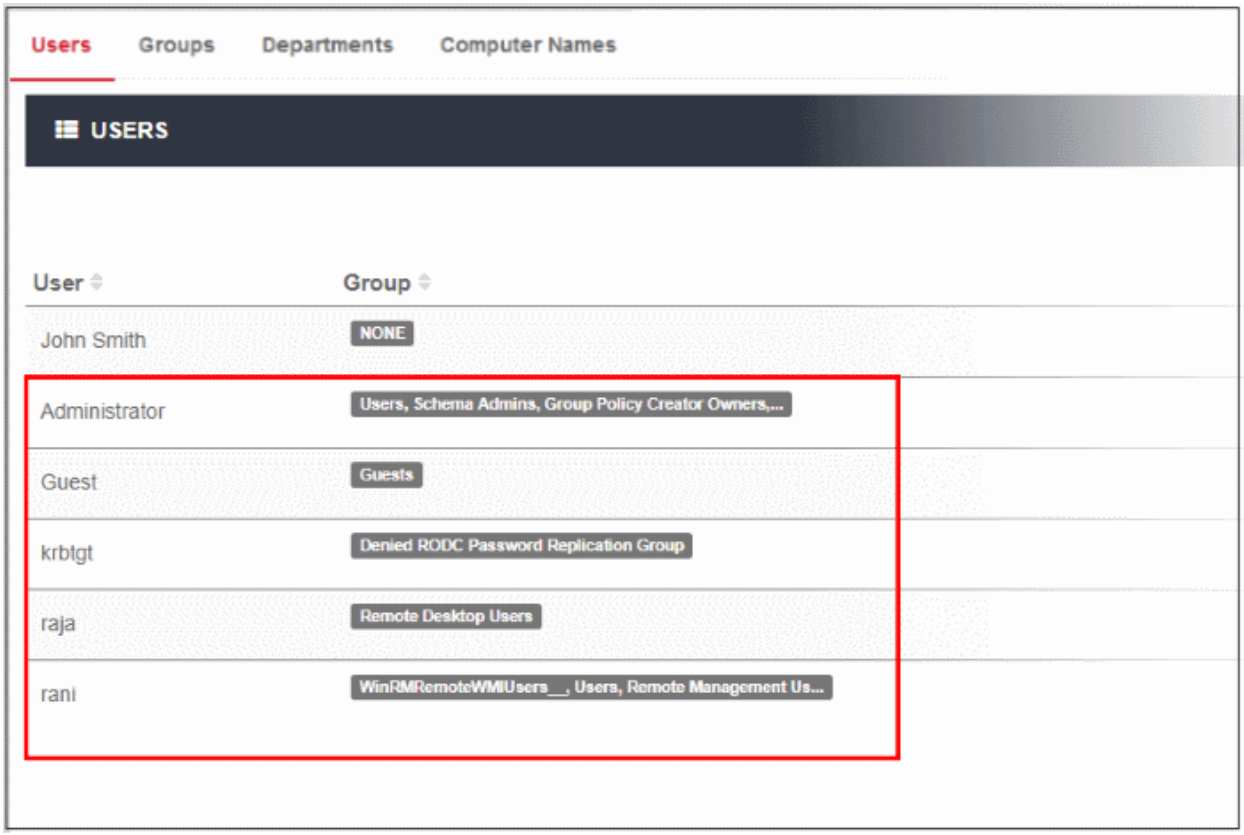
You will see the following dialog after a successful connection:



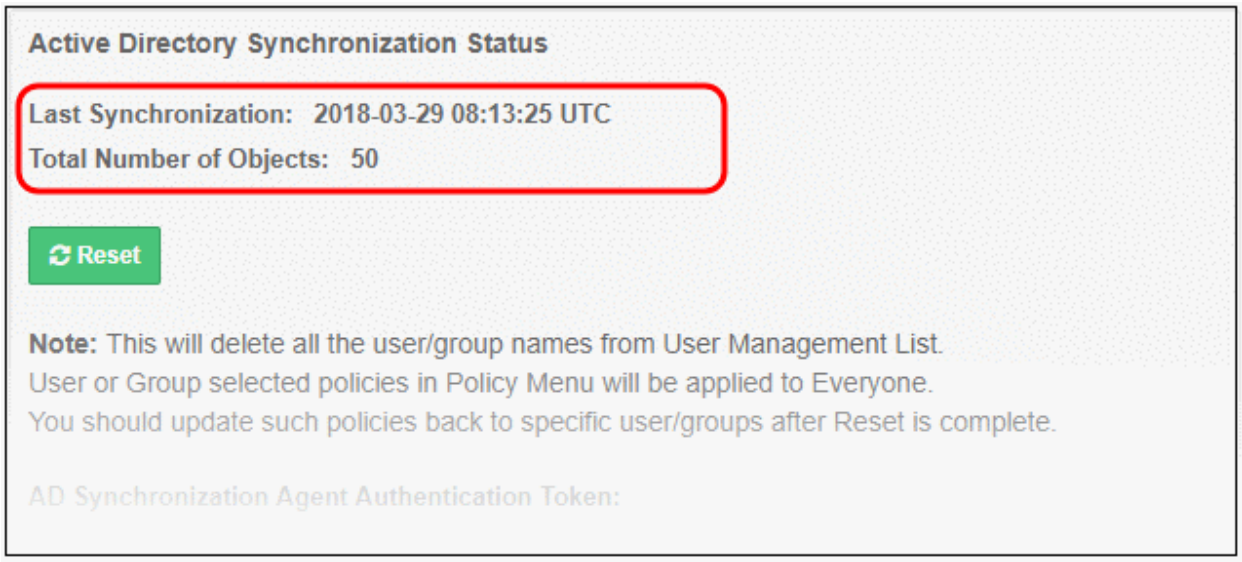
- Click 'Save & Close'

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.



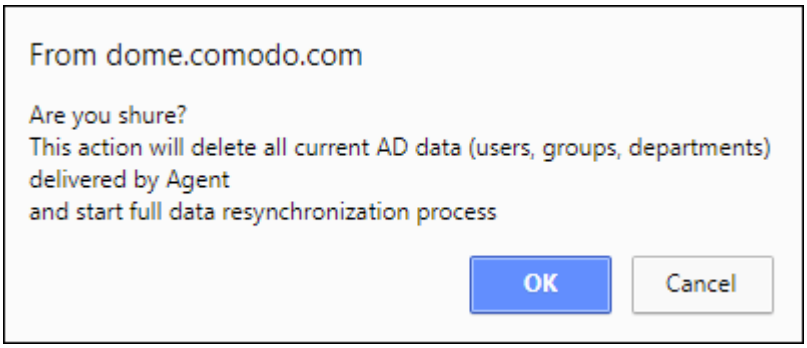
The AD agent will initiate subsequent synchronizations every 3 hours automatically.



- Last Synchronization – Indicates the date and time of last synchronization with the LDAP server
- Total Number of Objects – The number of users and groups enrolled to SWG via AD

Reset Synchronization

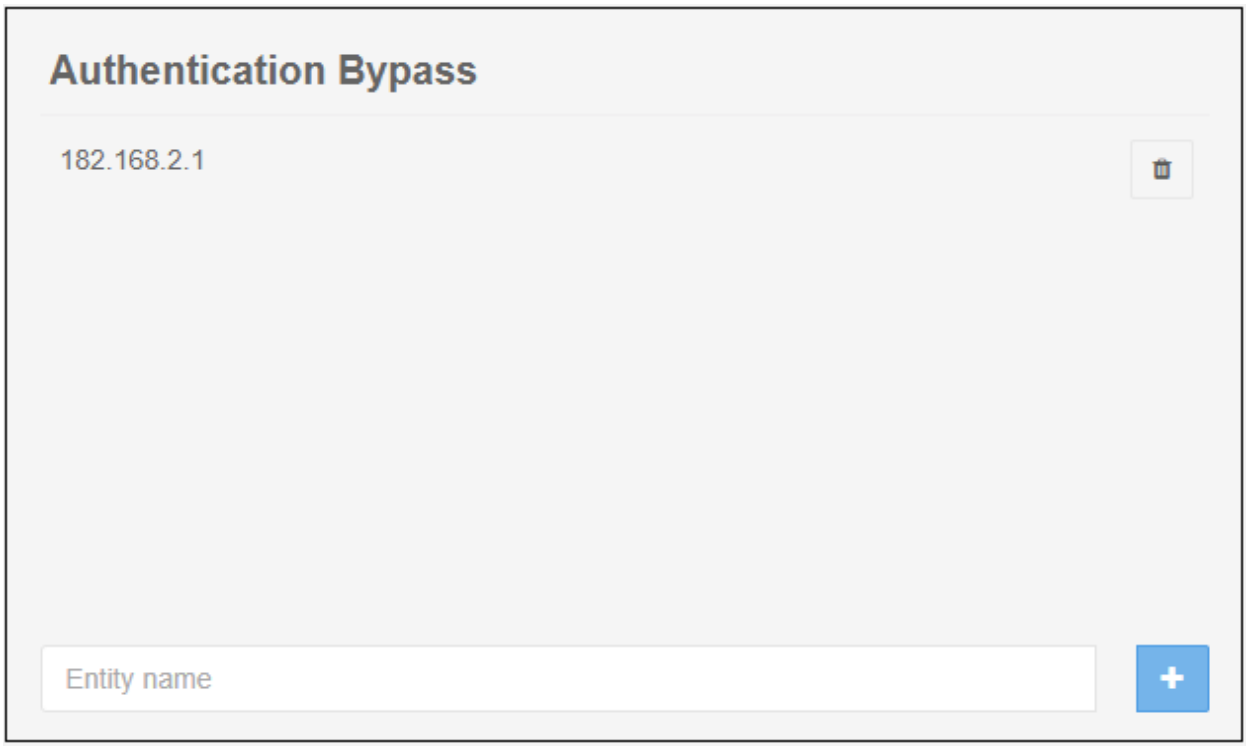
- Click 'Reset'



- 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

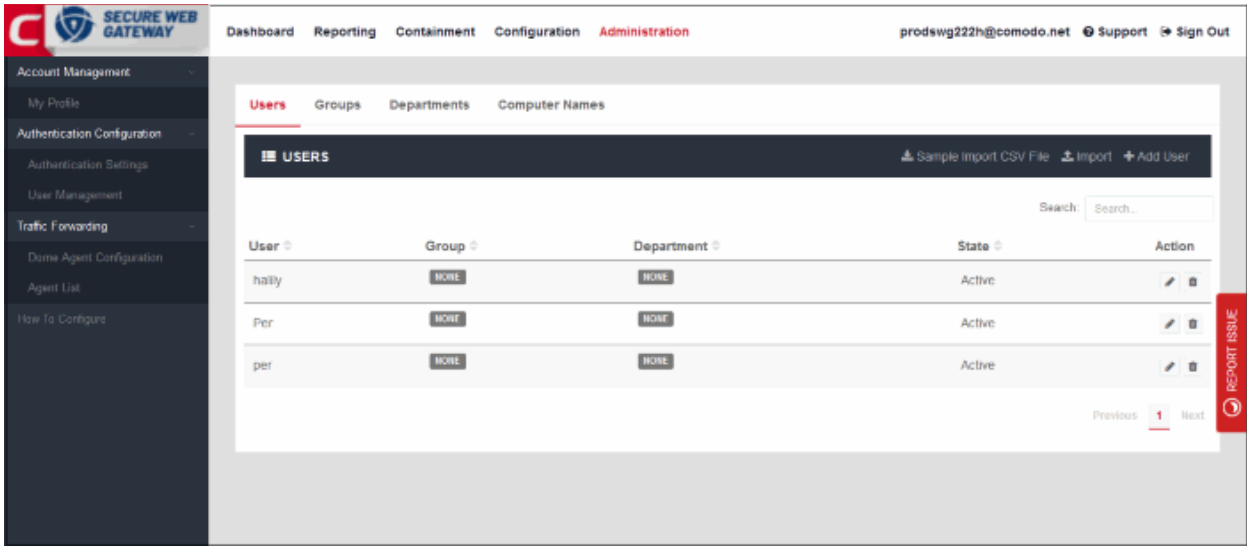
Bypassed Categories

- 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. 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

8.2 User Management

- Click 'Administration' > 'User Management' to open this area.
- The 'User Management' section lets you add individual users and bulk import users from .csv. You can also assign users to a group or department.
- Once created, you can add users, groups or departments to a policy (click 'Configuration' in the top-menu to **configure policy**).
- You can also add computer names in order to deploy policies for specific endpoints. Note: SWG agent must be installed on the endpoints.



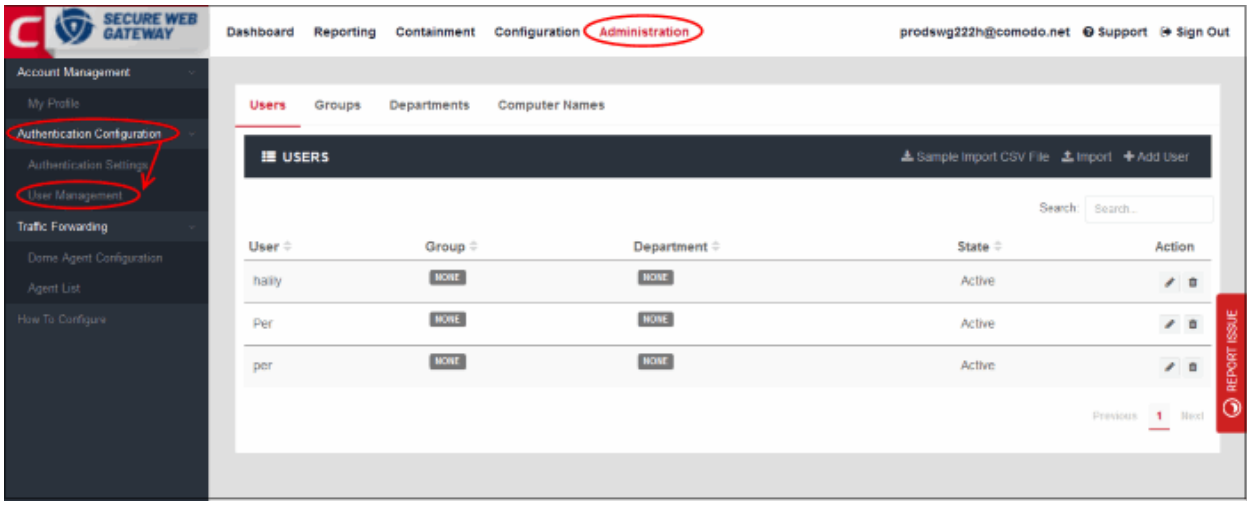
From this interface you can:

- **Manage Users**
- **Manage Groups**

- **Manage Departments**
- **Manage Computers**

8.2.1 Manage Users

- Click 'Administration' > 'Authentication Configuration' > 'User Management' to open this interface.
- The 'Users' interface lets you add end-users in order to apply user-specific policies.
- User-based policy is supported by the SWG agent, proxy chain and ICAP traffic forwarding methods.
- You can import users in bulk from a CSV file.
- The 'Add User' dialog depends on the type of **end user authentication type selected**.
  - If 'Active Directory' is configured then only the user name needs to be completed.
- 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 prevail.
  - Click 'Configuration' > 'Policy' > 'Edit' > 'Policy Order' to change the priority of a policy. See '**Apply Policies to Network**' section for more details.



The 'Users' interface allows you to:

- **Add a new user**
- **Import users from a CSV file**
- **Edit an existing user**
- **Delete a user**

Note – You can also enroll users by syncing with Active Directory:

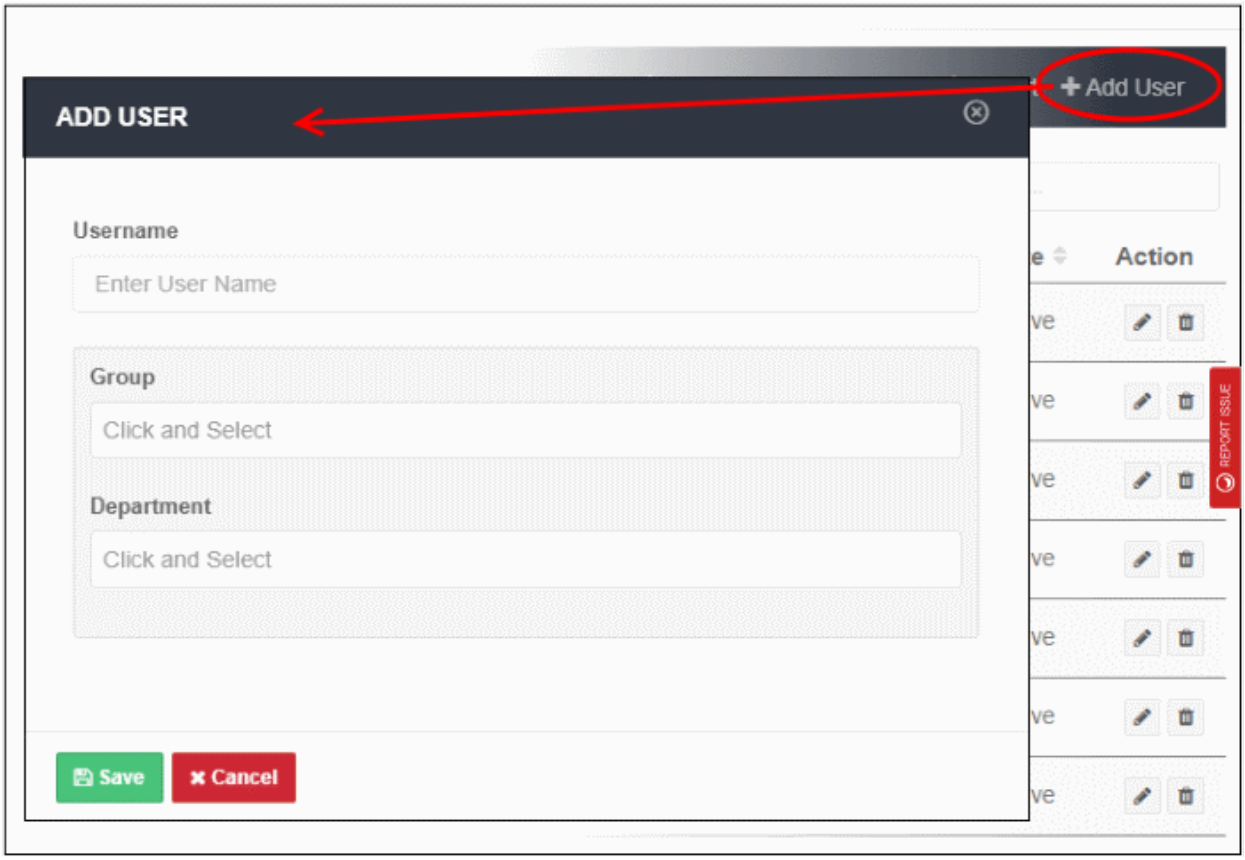
Sync via Active Directory

- 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 SWG and will be visible under 'User Management'.
- The SWG agent will automatically synchronize with AD every 3 hours.
- This method is explained in '**Active Directory**'

Add a new user

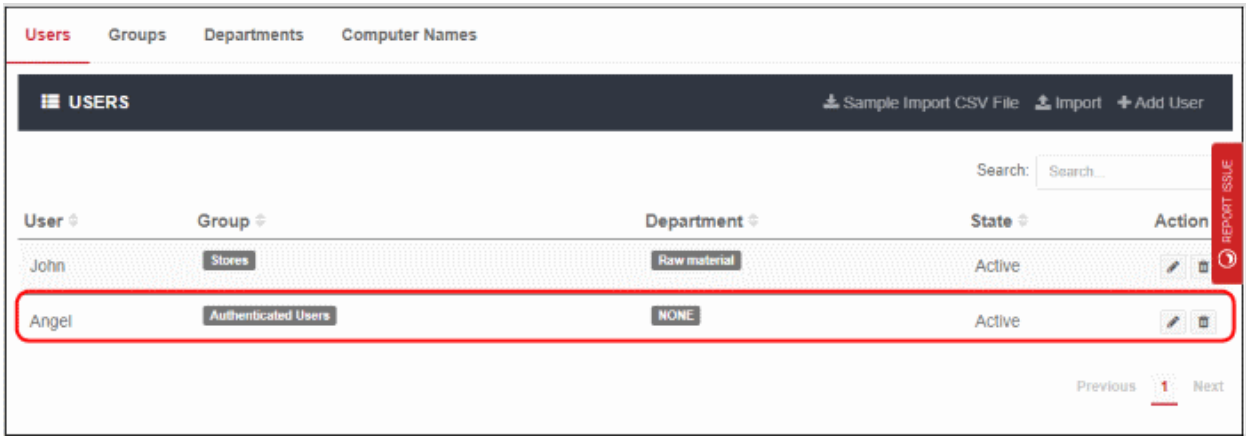
- Click 'Users' and then 'Add User' at top-right

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. The groups added in the 'Groups' interface will be listed here. See '**Manage Groups**' for details.
- **Department** - Relevant only if 'Hosted DB' is selected in '**Authentication Settings**' interface. Click in the field and select the appropriate department for the user. The departments added in the 'Departments' interface will be listed here. See '**Manage Departments**' for details.
- Click 'Save' when done

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



You can now apply policies to this user according to your requirements. Make sure 'User Authentication' is selected in the 'Locations' interface. See '**Apply Policies to Networks**' to learn more about deploying polices.

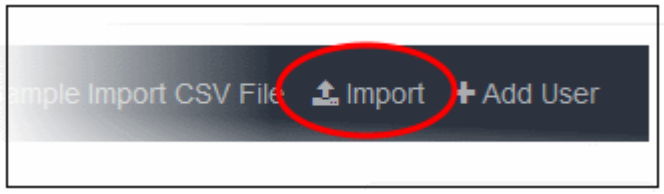
Import users from a CSV file

Comodo SWG allows you to add users in bulk 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.

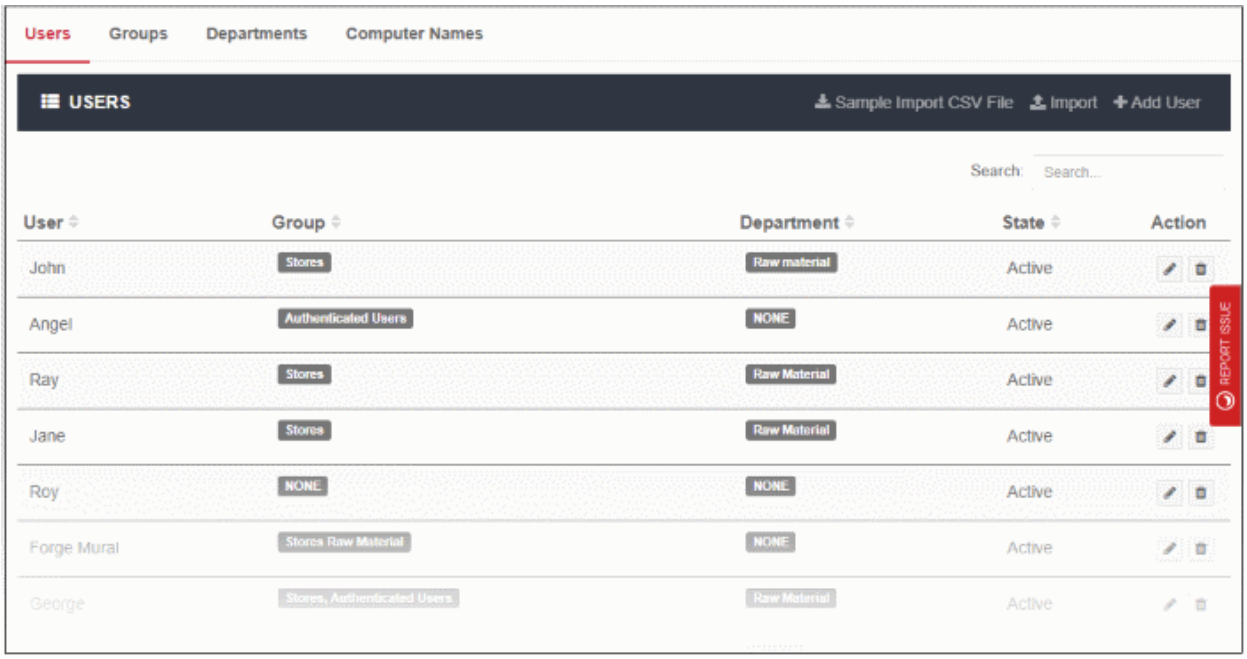
Import users from a CSV file

- Click 'Import' at the top



- Navigate to the CSV file location, select the file and click 'Open'

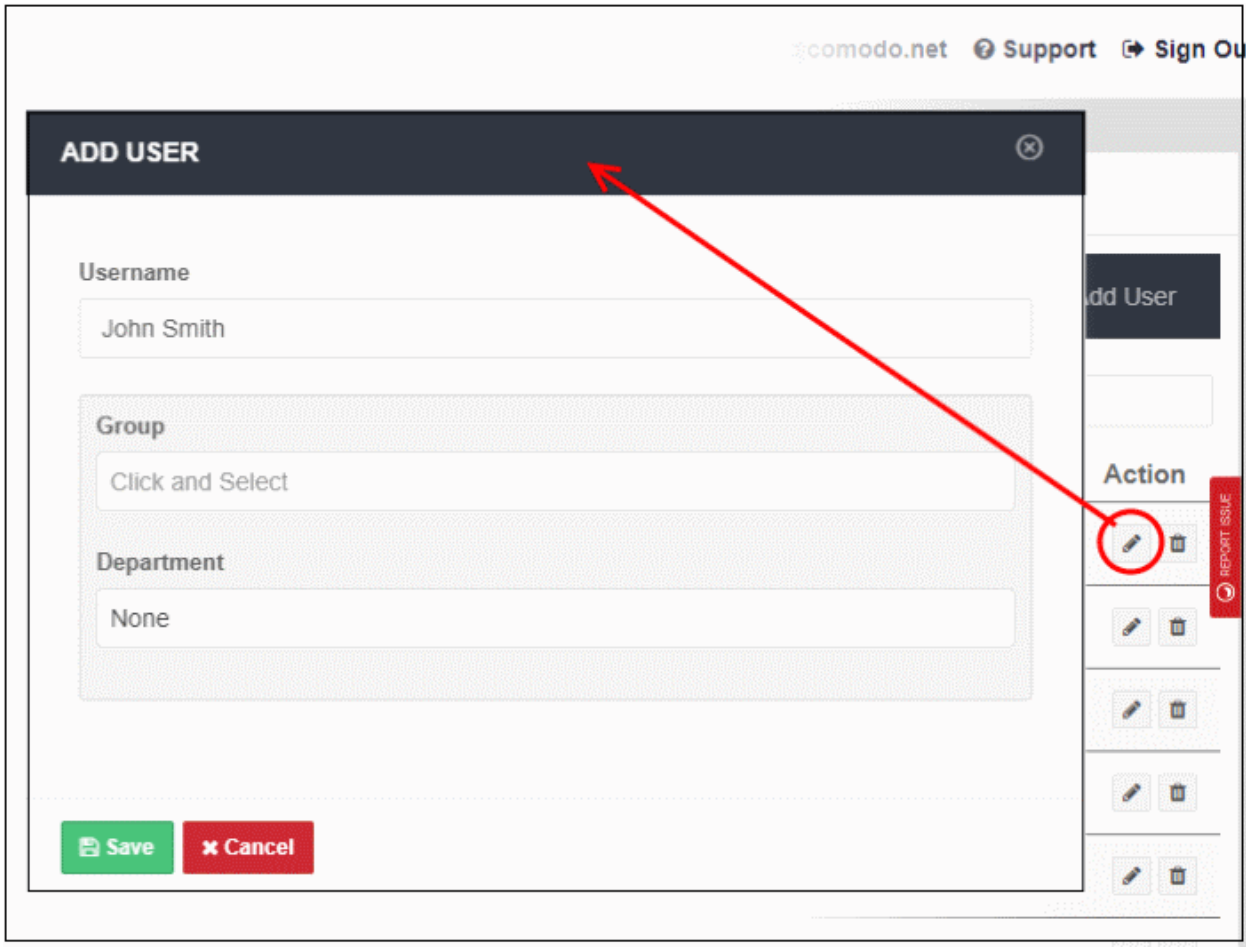
The 'Users' will be imported and displayed in the list.



You can now apply policies to this user according to your requirements. Make sure 'User Authentication' is selected in the 'Locations' interface. See '**Apply Policies to Networks**' to learn more about deploying polices.

Edit an existing user

- Click the edit icon beside the user



- Update the details as required. The process is similar to adding a user explained above. Please note that

you cannot change the username.

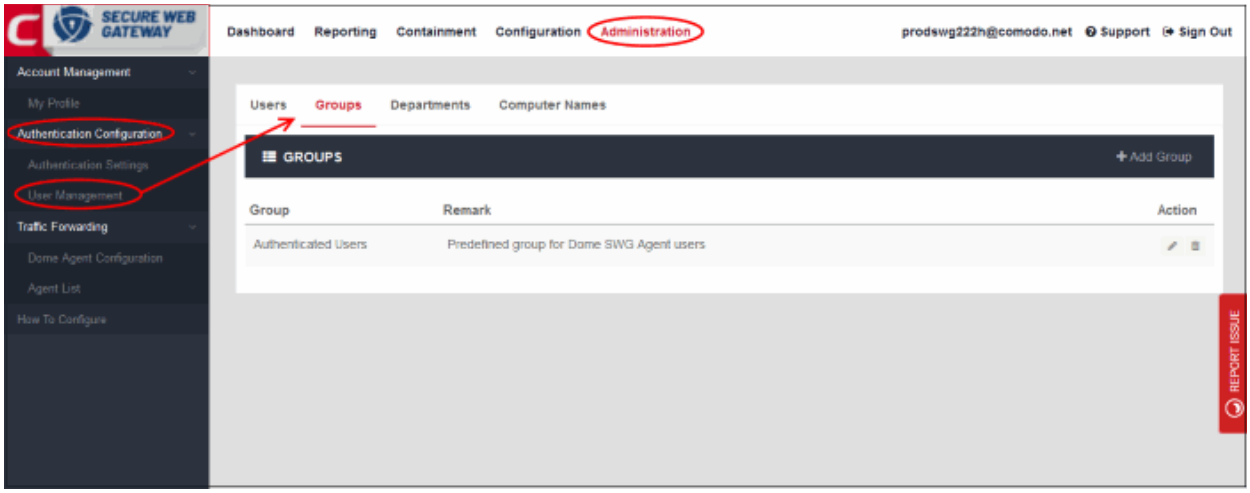
- Click 'Save' to apply your changes.

Delete a user

- Click the trash can icon beside the user that you want to remove from the list. Note – You cannot delete a user that is assigned a policy.
- Click 'OK' in the confirmation dialog

8.2.2 Manage User Groups

- Click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Groups' to open this interface.
- The 'Groups' interface lets you create groups and add users to them. You can then add the group to a policy in the 'Policy' area ('Configuration' > 'Policy')
- You can apply multiple policies to any group.
  - Policies are prioritized top-to-bottom according to the list in 'Configuration' > 'Policy'.
  - In the event of a conflict between policies over a setting, the setting in the policy nearer the top will prevail.
  - You can change priority in the 'Policy Order' drop-down when editing a policy:
    - Click 'Configuration' > 'Policy'
    - Locate the policy whose priority you want to change and click the 'Edit' button on the right.
    - Choose the priority with the 'Priority Order' drop-down. See '**Apply Policies to Network**' section for more details.



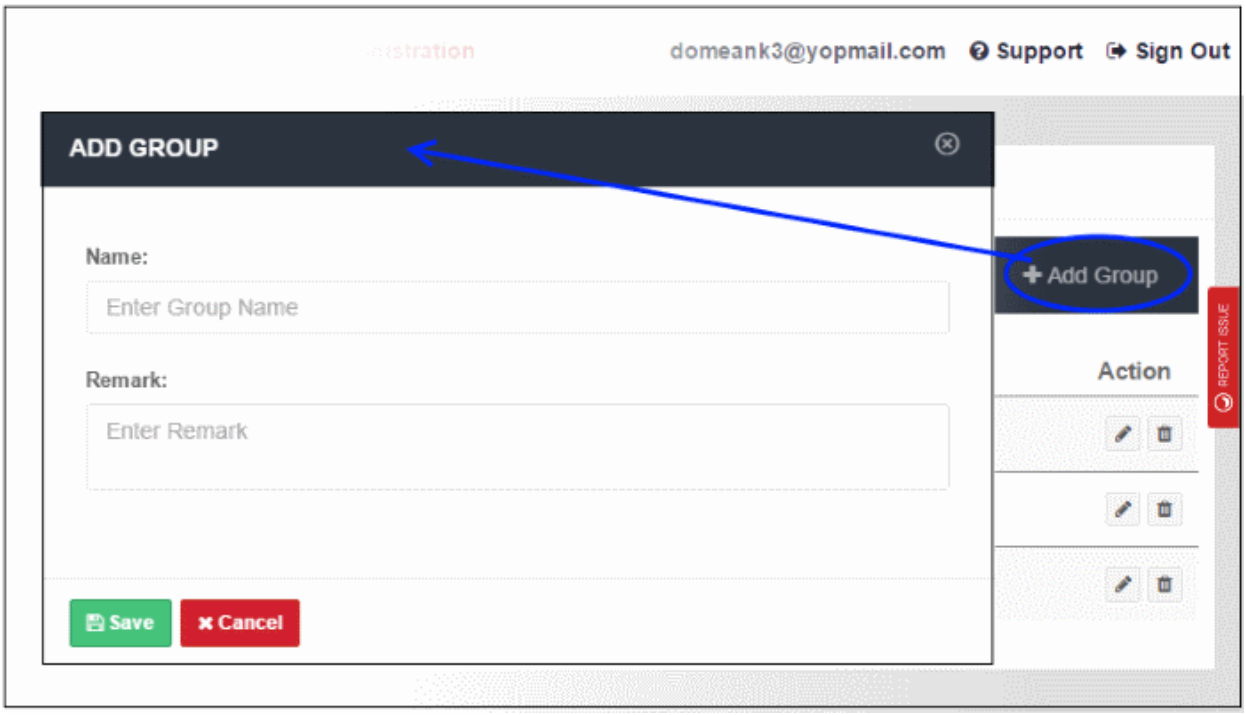
From the 'Groups' interface, you can:

- **Add a group**
- **Edit a group**
- **Delete a group**

Add a group

- Click 'Groups' and then 'Add Group' on top right

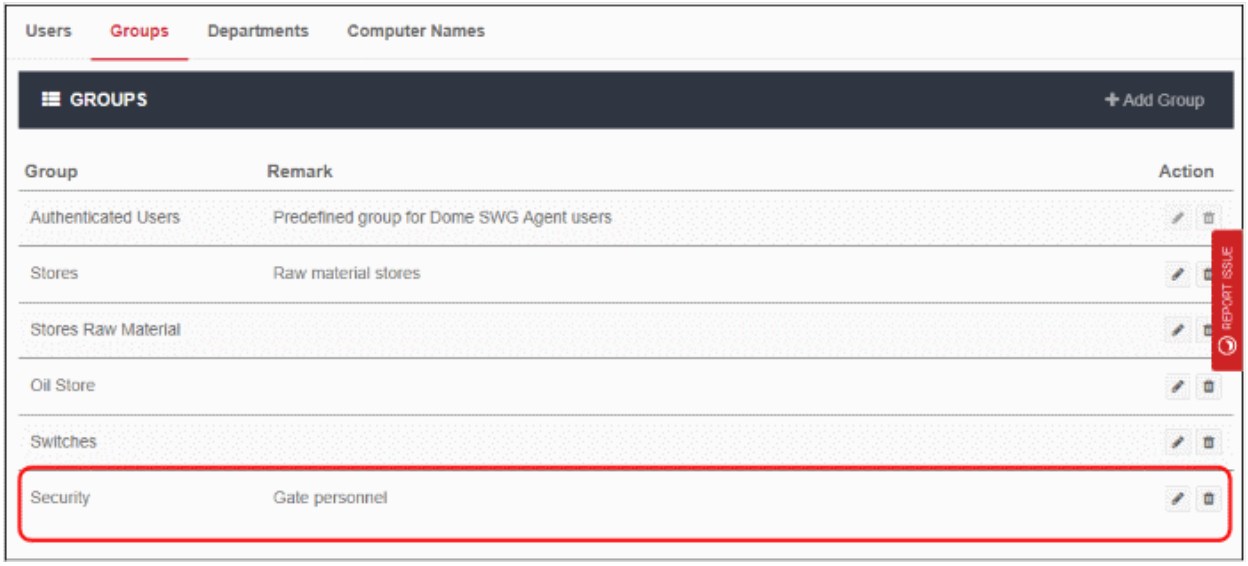
The 'Add Group' dialog will be displayed:



- **Name** - Enter a label for the group in the field
- **Remark** - Provide appropriate comments for the group

- Click 'Save'

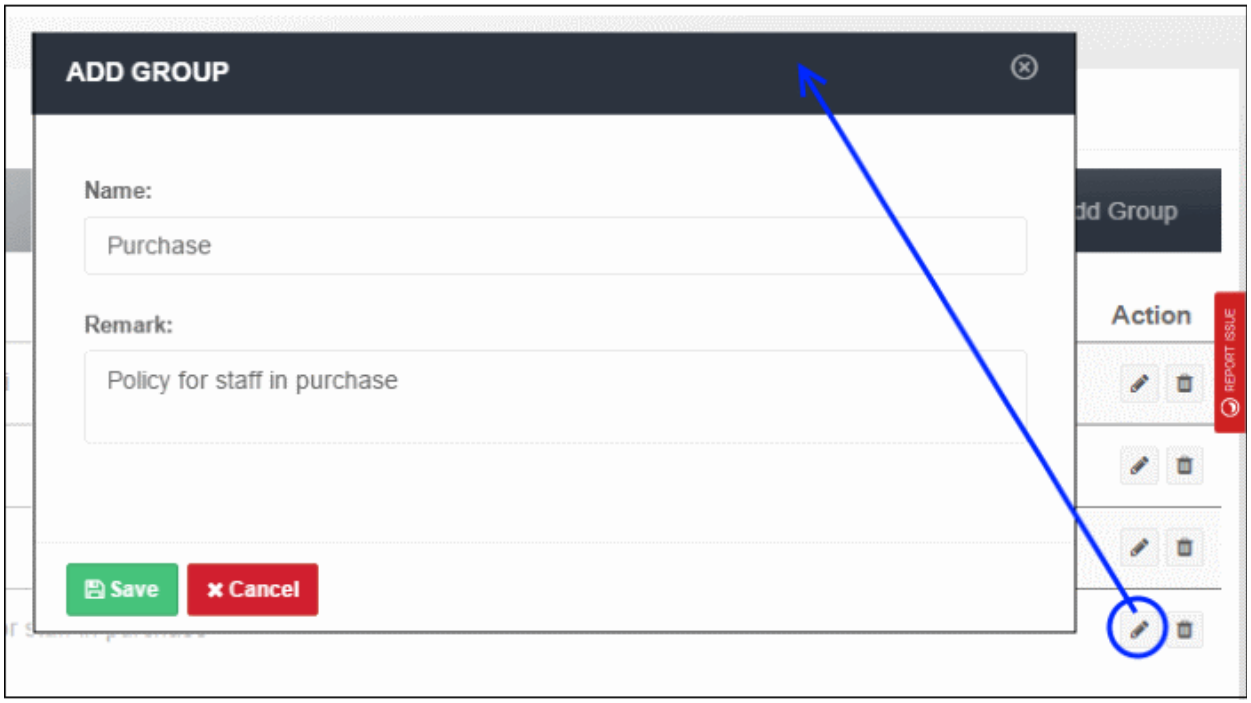
The new group will be added and displayed:



The group now can be deployed policy according to your requirement. See '**Apply Policies to Networks**' to know how to deploy polices.

Edit a group

- Click the edit icon beside the group



- Update the details as required. The process is similar to adding a group explained above.
- Click 'Save' to apply your changes.

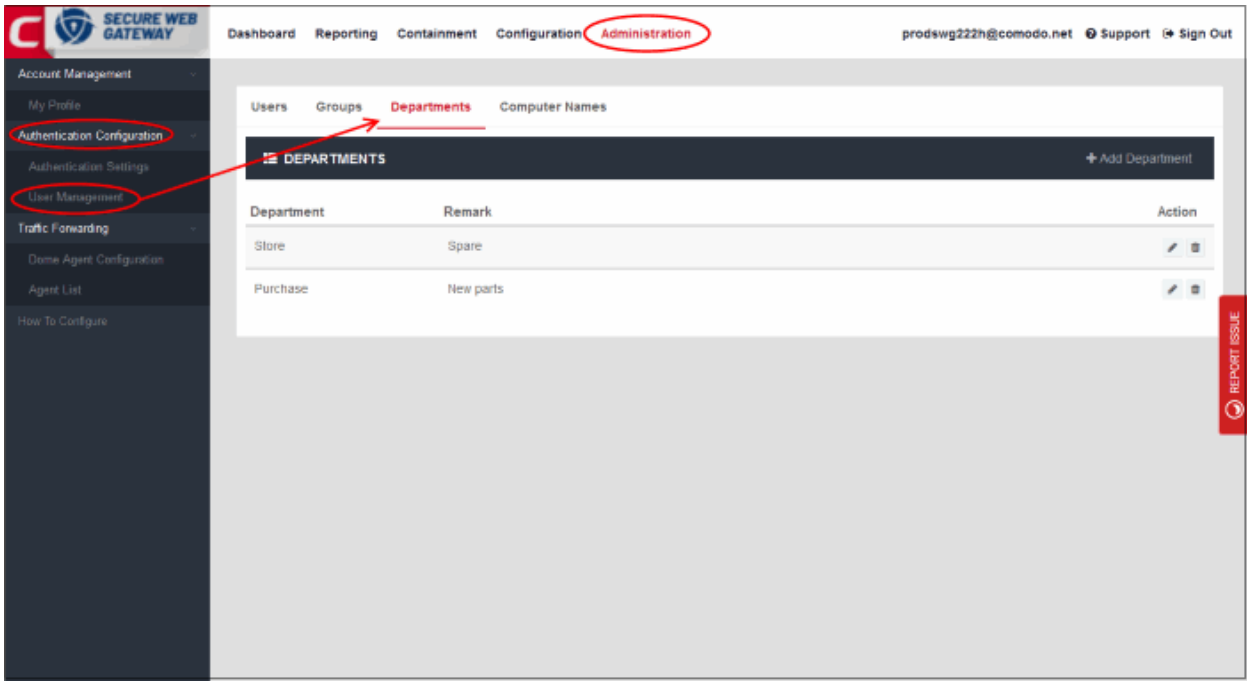
If the group is applied any policies, the changes done here will also be reflected in the **Policy List** interface.

Delete a group

- Click the trash can icon beside the group that you want to remove from the list. Note – You cannot delete a group that is assigned a policy.
- Click 'OK' in the confirmation dialog

8.2.3 Manage Departments

- Click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Departments' to open this interface
- The 'Departments' area lets you create departments and add users to them. You can then add the department to a policy in the 'Policy' area ('Configuration' > 'Policy')
- Department specific policy can be deployed.
  - 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 policy priority in the 'Policy Order' drop-down when editing a policy:
    - Click 'Configuration' > 'Policy'
    - Locate the policy whose priority you want to change and click the 'Edit' button on the right.
    - Choose the priority with the 'Priority Order' drop-down. See '**Apply Policies to Network**' section for more details.



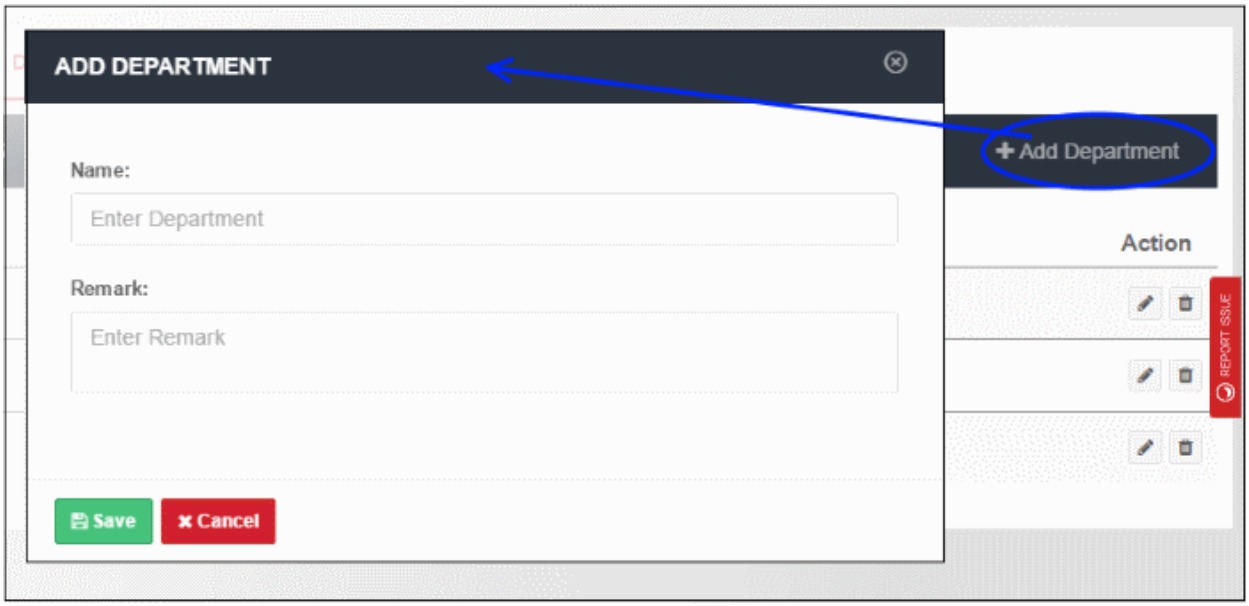
From the 'Departments' interface, you can:

- **Add a department**
- **Edit a department**
- **Delete a department**

Add a department

- Click 'Departments' and then 'Add Department' at top-right

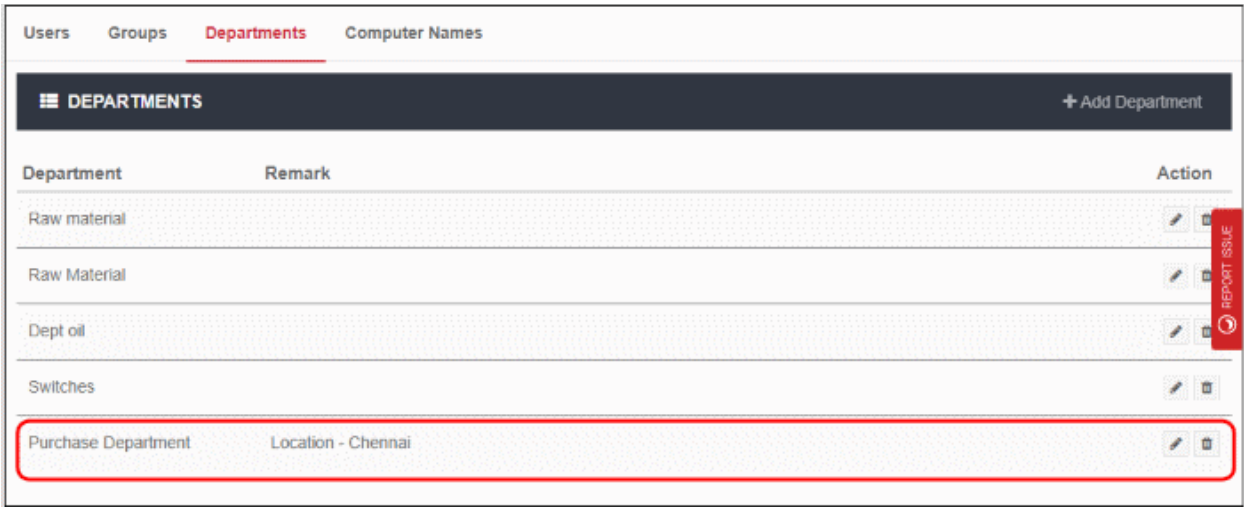
The 'Add Department' dialog will be displayed:



- **Name** - Enter a label for the department
- **Remark** - Provide appropriate comments for the department

- Click 'Save'

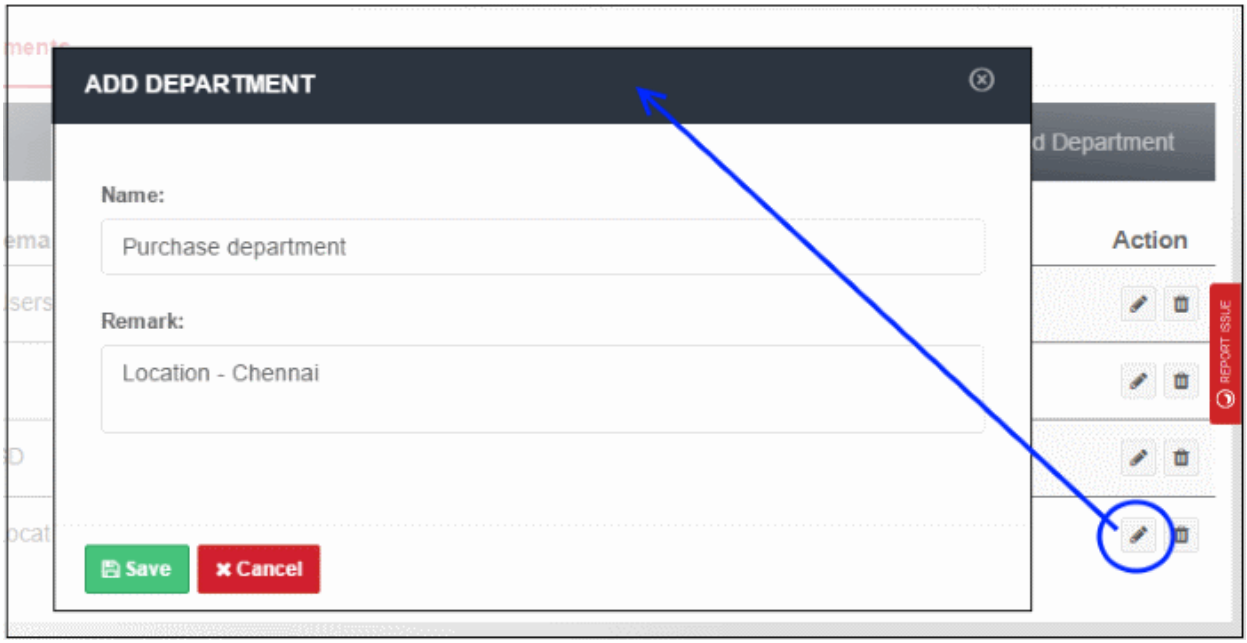
The new department will be added:



You can now apply policies to the department as required. See '**Apply Policies to Networks**' to for help with this.

Edit a department

- Click the edit icon beside the department



- Update the details as required. The process is similar to adding a department explained above.
- Click 'Save' to apply your changes.

If the department is applied any policies, the changes done here will also be reflected in the **Policy List** interface.

Delete a department

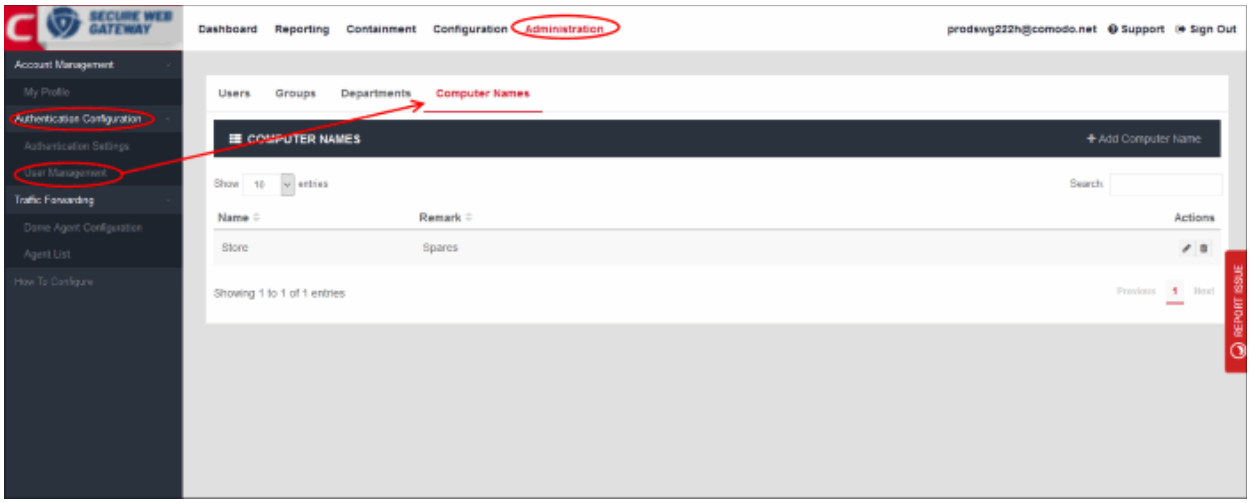
- Click the trash can icon beside the department that you want to remove from the list. Note – You cannot

delete a department that is assigned a policy.

- Click 'OK' in the confirmation dialog

8.2.4 Manage Computers

- Click 'Administration' > 'Authentication Configuration' > 'User Management' > 'Computer Names'
- The 'Computer Names' area lets you add endpoints to Comodo SWG. You can then include the endpoints in a policy ('Configuration' > 'Policy')
  - Note – 'Computer Names' is only visible if you selected 'Hosted DB' method for user authentication. Click 'Administration' > 'Authentication Configuration' > 'Authentication Settings' to view/change this setting. **Click here** for more information about user authentication methods.
- 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 policy priority in the 'Policy Order' drop-down when editing a policy:
  - Click 'Configuration' > 'Policy'
  - Locate the policy whose priority you want to change and click the 'Edit' button on the right.
  - Choose the priority with the 'Priority Order' drop-down. See '**Apply Policies to Network**' section for more details.

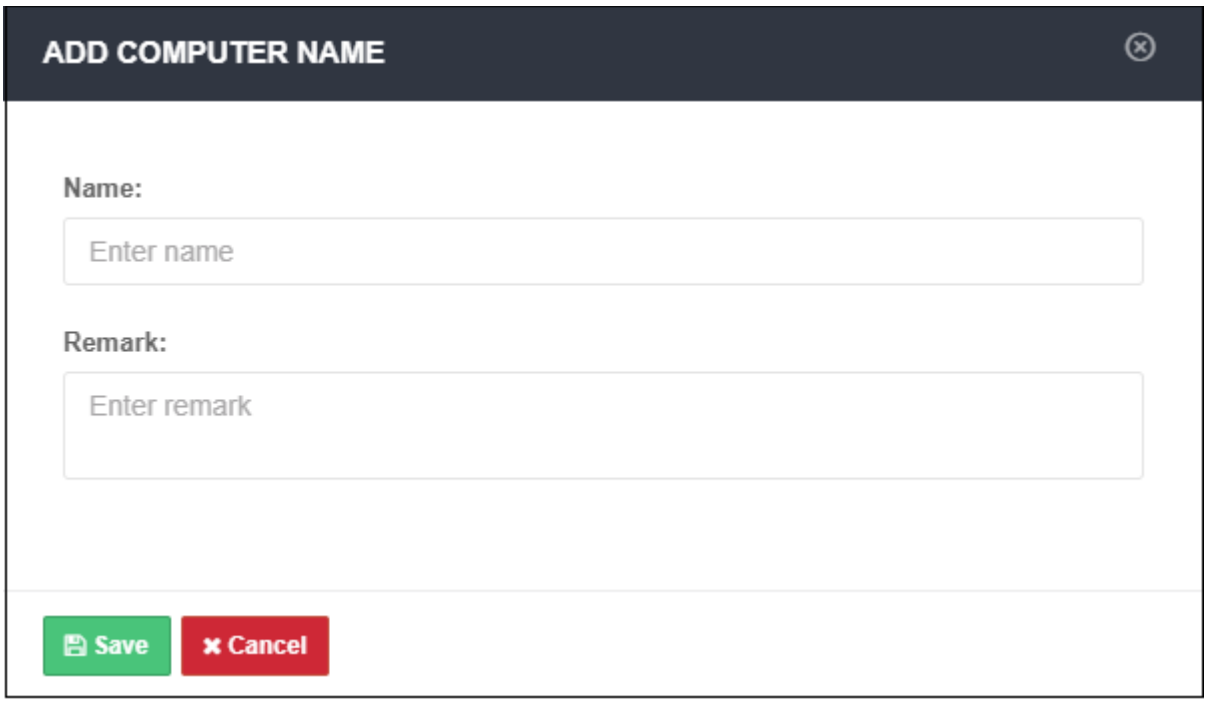


From the 'Computers Name' interface, you can:

- **Add a computer**
- **Edit computer details**
- **Delete a computer name**

Add a computer

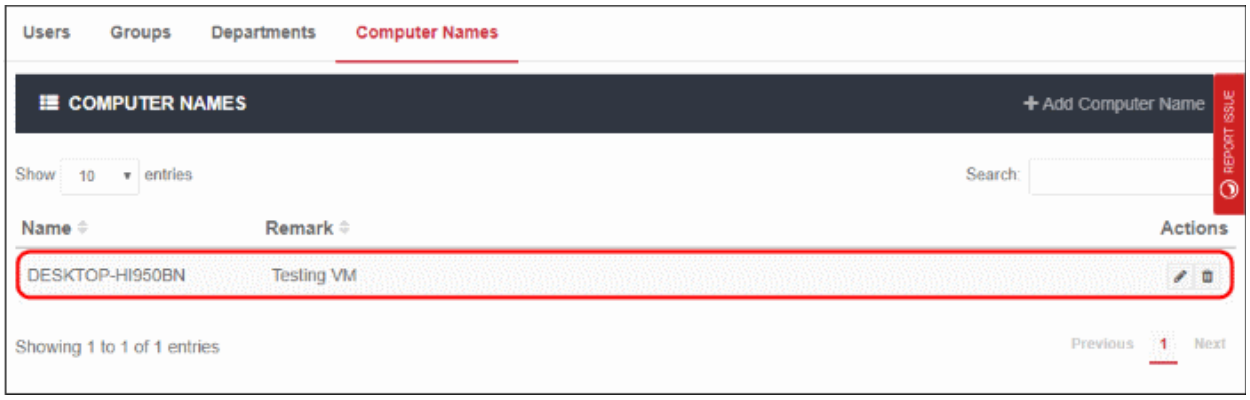
- Click 'Computer Names' then 'Add Computer Name' at top-right
- This opens the 'Add Computer Name' dialog:



- **Name** - Create a label for the computer
- **Remark** - Provide appropriate comments for the computer

- Click 'Save'

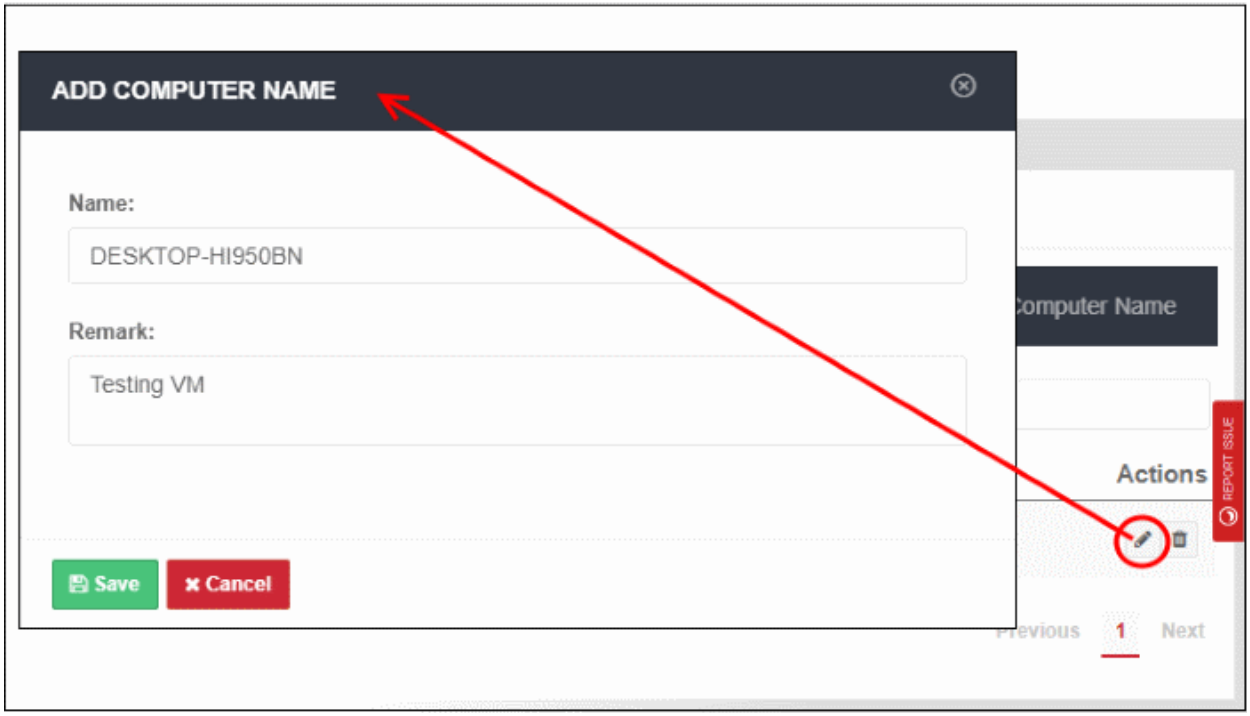
The computer is added to the computer names area:



You can now deploy policies to the endpoint as required. See '**Apply Policies to Networks**' to learn more.

Edit computer details

- Click the edit icon beside the computer name



- Update the details as required. The process is similar to adding a computer explained above.
- Click 'Save' to apply your changes.

If the computer is applied any policies, the changes done here will also be reflected in the **Policy List** interface.

Delete a computer

- Click the trash can icon beside the computer that you want to remove from the list. Note – you cannot delete a computer that has a policy assigned to it.
- Click 'OK' in the confirmation dialog.

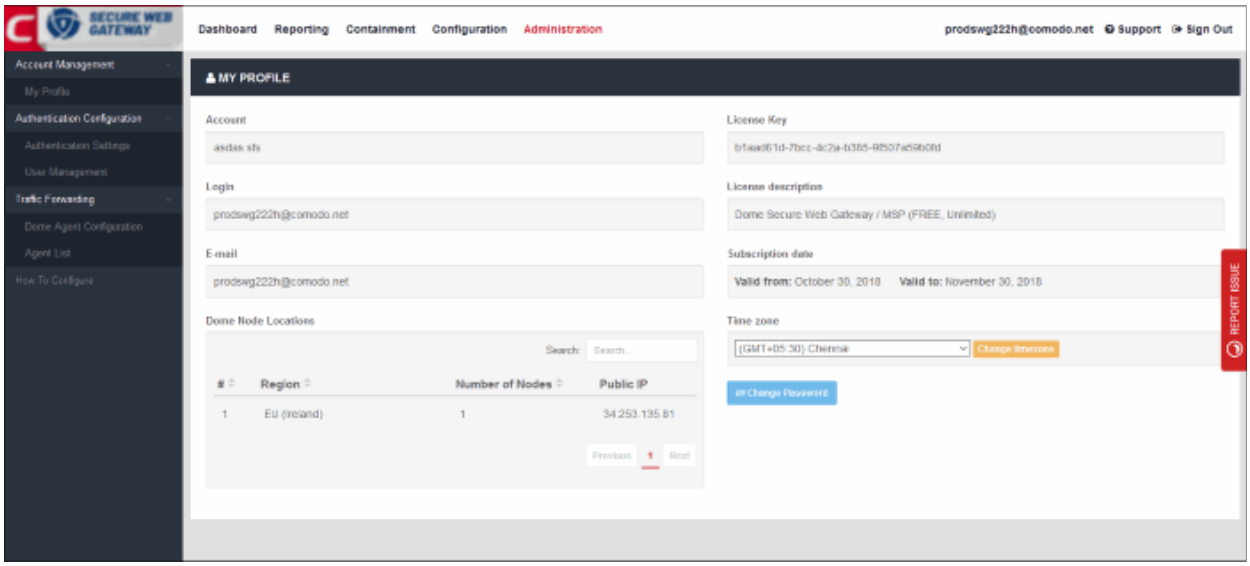
8.3 My Profile

The 'My Profile' screen lets you view details about your account. Details include account name, login, license key and more. You can also change the time zone and password from this interface.

Open the 'My Profile' screen

- Click 'Administration' > 'Account Management' > 'My Profile'

  OR
- Click your username at top-right



- **Account** - The name provided when purchasing Comodo Secure Web Gateway, or signing up for a Comodo account.
- **Login** - The user name to log into the account. This is the same as the email address provided during sign up.
- **Email** - The address provided at account sign-up.
- **License Key** - The activation code your for license.
- **License Description** - Number of networks/endpoints, users and license period.
- **Subscription Date** - License activation and expiry dates.

Time Zone

- Click the drop-down and select your preferred time zone.
- Click 'the Change timezone' button.

Change Password

- Click the 'Change Password' button at the bottom of the screen.

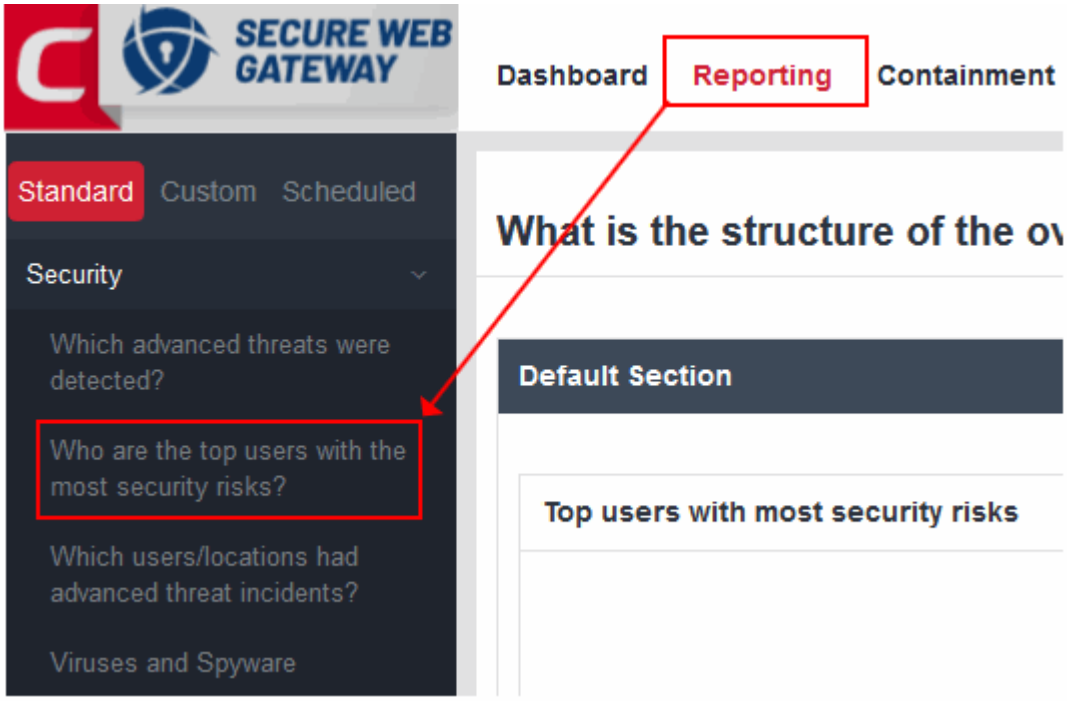
Note - Your Comodo Secure Web Gateway account is linked to your Comodo Accounts Manager (CAM) account at **https://accounts.comodo.com/**. You will be taken to that website to change your password.

Comodo SWG Node Locations

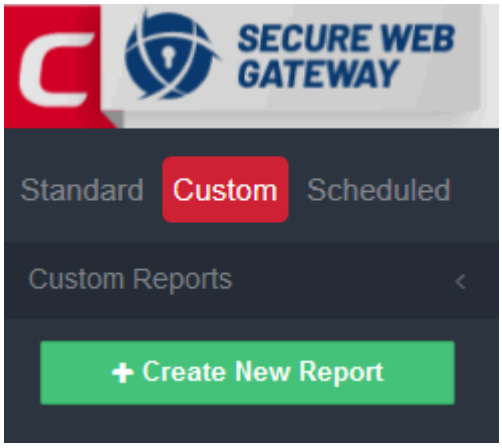
Shows the number of Comodo SWG nodes that you have configured for your account. Hosting multiple nodes in different locations balance the traffic to Comodo SWG. The configuration is done at first login after subscribing. Contact support at **domesupport@comodo.com** if you want to reconfigure the nodes.

9 Reports

Comodo Secure Web Gateway (SWG) 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' reports can be viewed by clicking the links presented on the left. The content of the report will be displayed in the main pane.
- The default period covered by the report is 7 days. This cannot be changed.
- You can create your own custom reports by clicking the 'Custom' button on the left:



- Comodo SWG ships with the following 'Standard' reports across the three categories of 'Security', 'User/Location Activity' and 'Web Activity':

Security Reports

- Advanced Threat Report
- Top Users with Most Security Risks Report
- Top Users with Advanced Threat Incidents Report
- Virus and Spyware Report
- Contained File List Report
- Top Attack Types Report

- Containerization Trend Report
- Top Users/Location with most Contained Files Report
- Top Malware Report
- Top Users/Locations with Virus and Spyware Incidents Report
- Productivity Loss Report

User / Location Activity Reports

- Locations with Most Blocked Traffic Reports
- Locations with Most Productivity Loss Reports
- Most URL Blocked Category Report
- Top Blocked Users and Locations Report
- Top Users Visited URL Categories Report
- User Browsing History Report
- Top Web Browsing Users Report
- Top Users with Most Productivity Loss Report

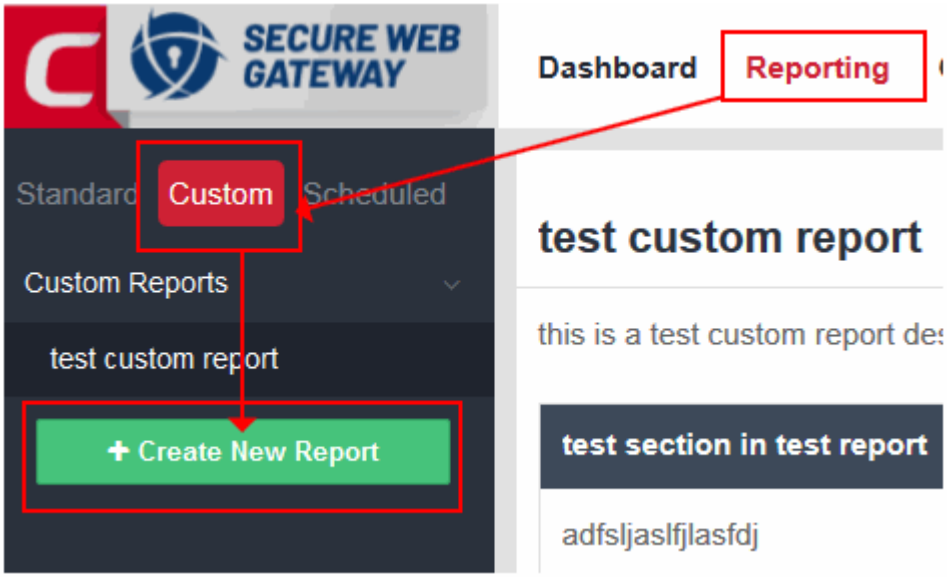
Web Activity Reports

- Top URL Categories Report
- Web Traffic Overview Report
- Top Blocked Web Traffic Overview Report

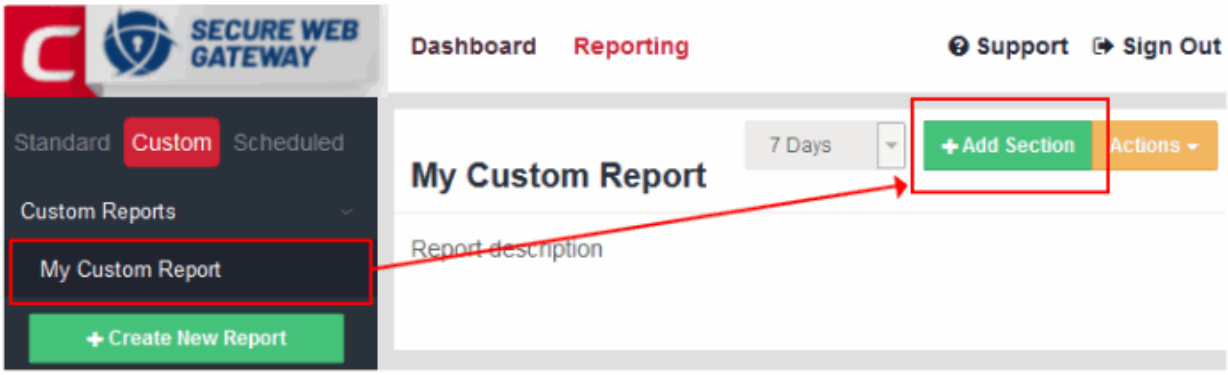
9.1 Custom Reports

Comodo Secure Web Gateway lets you construct reports specifically tailored to the needs of your organization.

- Click 'Reporting' > 'Custom' then '+ Create New Report'

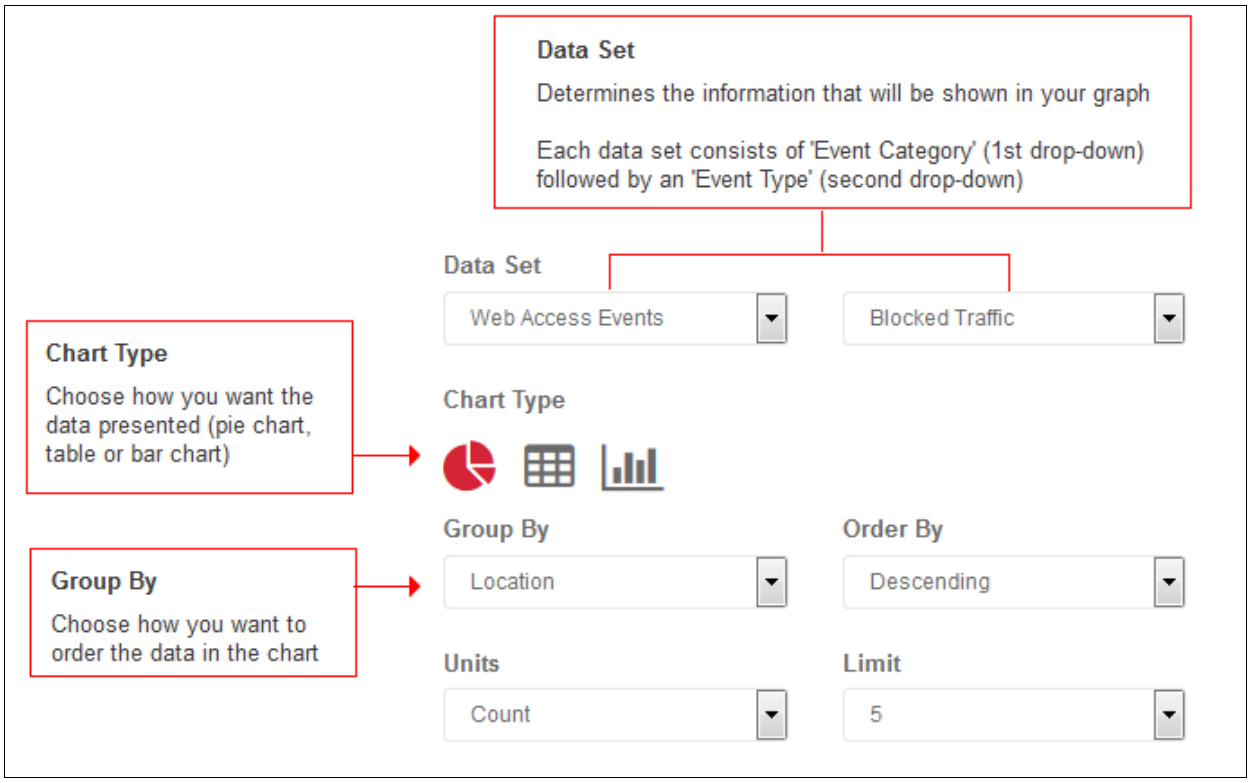


- In the 'Add Report' dialog, create a name and description for your report then click 'Save'
- Next, select your report on the left then click the 'Add New Section' button to begin specifying your data-set:



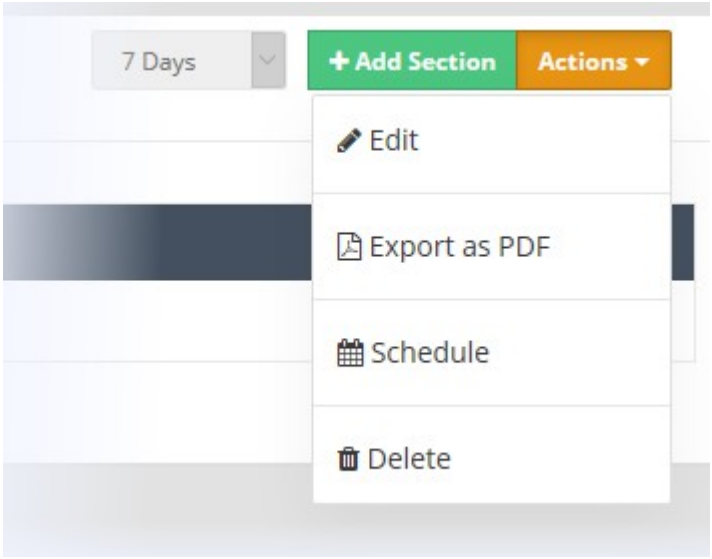
- A 'section' is a named area where you can group charts according to theme. You can add multiple charts to each section. For example, you can create sections to:
  - Cover multiple event types in a particular event category
  - Cover a specific event type (e.g. 'Blocked Traffic') with charts grouped by different parameters
  - Present a specific data set with graphs showing different filters (or multiple data sets with the same filter)
  - Any combination of charts that you require
- Create a name and description for your new section and click 'Save'.
- Next, click 'Add Graph' in your new section:

- The 'Add Graph' dialog allows you to construct your custom chart:



- The filters on the right allow you to further refine the data which is presented. For example, if you select 'Location', enter a network IP and click the check mark button then the chart will only display data pertaining to that network.

- The settings in the 'Add Graph' configuration screen are covered in more detail in **Customize the Dashboard**
- Repeat the process above to add more graphs and/or sections
- Click the 'Actions' drop down to schedule, edit, export or delete a custom report.

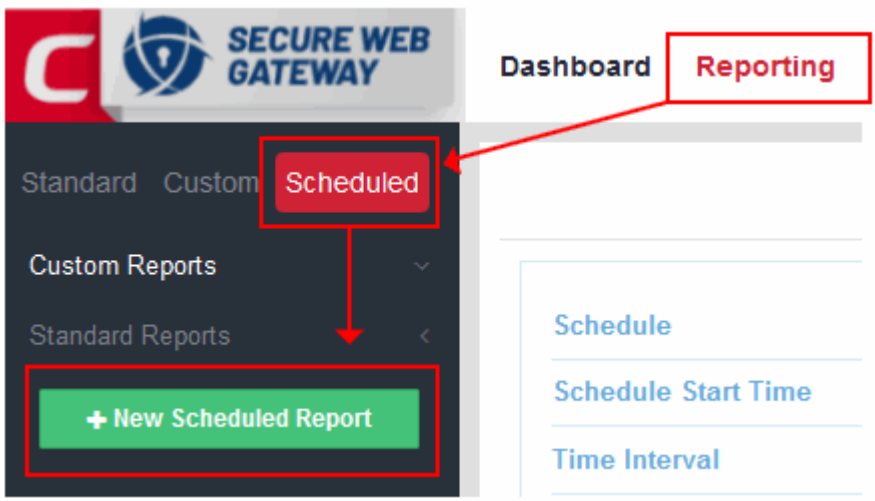


- Please note that you can schedule any type of report from the scheduled reports tab.

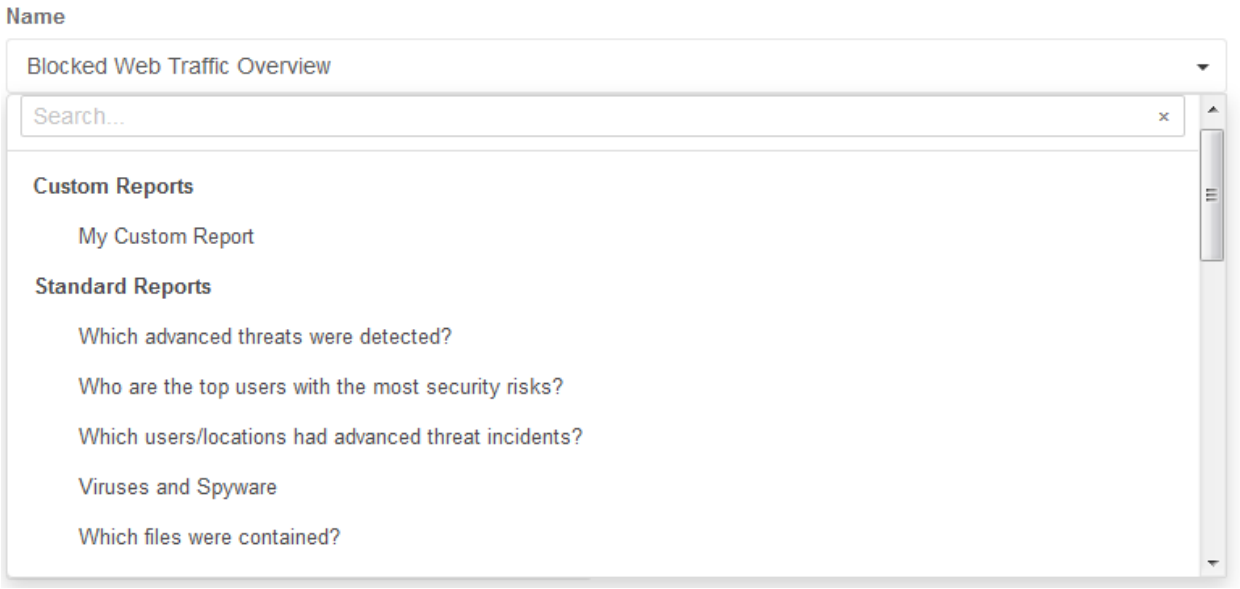
9.2 Scheduled Reports

Comodo Secure Web Gateway can automatically generate reports at specific times and email them to a list of recipients.

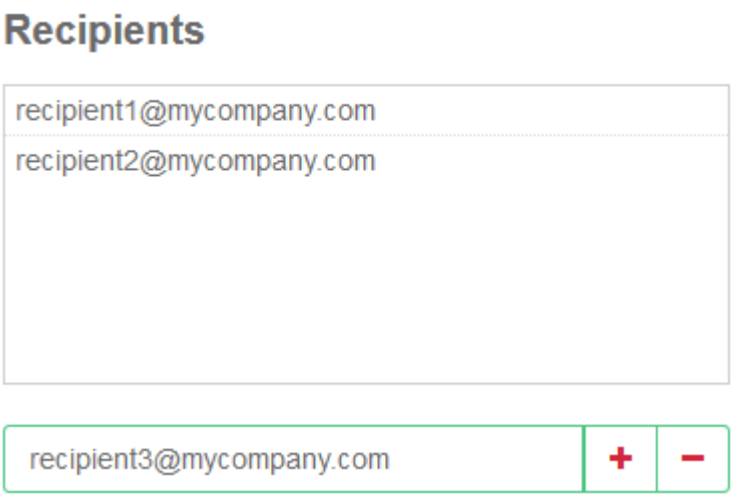
- Click 'Reporting' then click the 'Scheduled' button followed by 'New Scheduled Report':



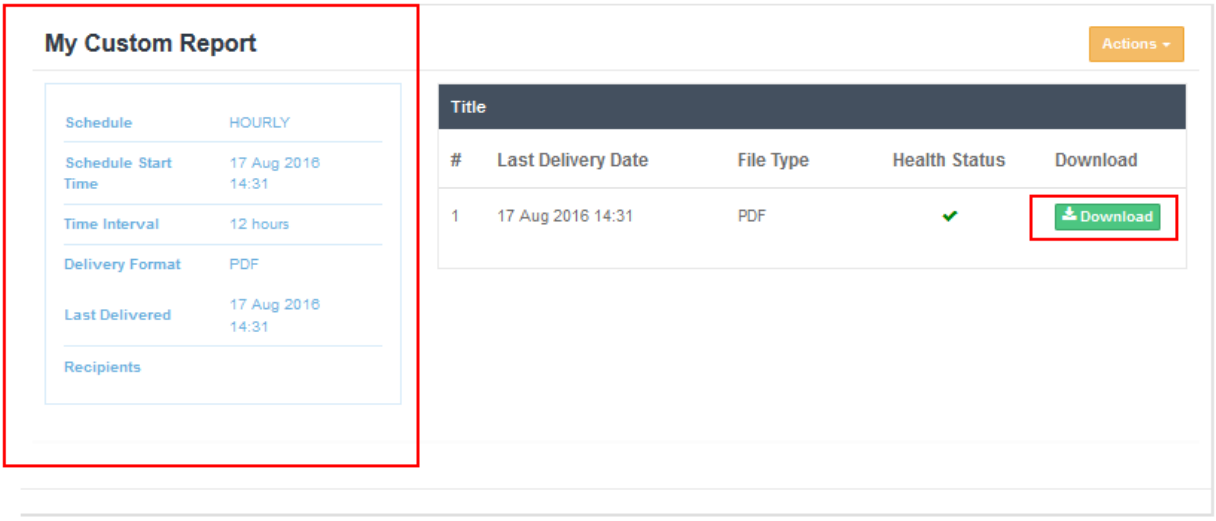
- In the 'Schedule Details' dialog, first pick the type of report you want to schedule. You can choose any standard or custom report:



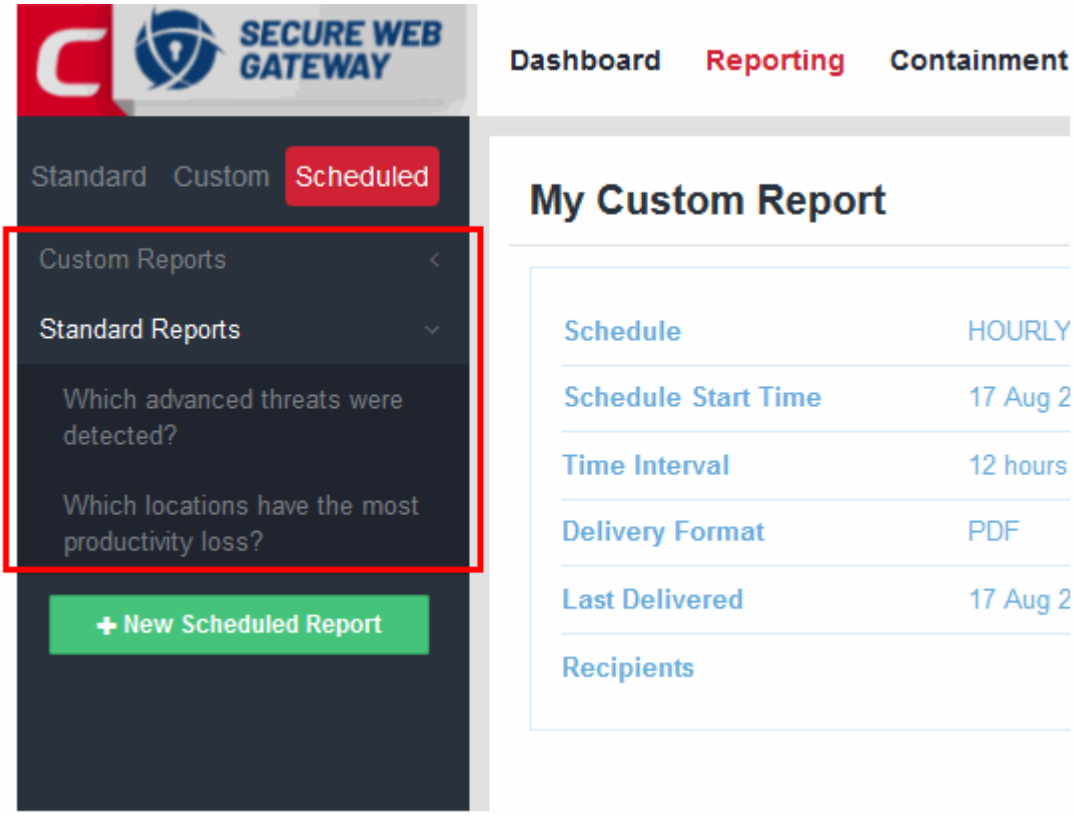
- Next, specify your schedule.
  - **Creation Time** - The time and date on which the first report should be generated. By default this is set at the current date and time.
  - **Schedule** - Choose whether you want the report to be generated and sent on an hourly, daily, weekly or monthly basis.
  - **Time interval** - Choose the period of time which should be covered by the report. For example, '3 days' will generate a report which covers data from the preceding 3 days.
- Finally, create your list of recipients by typing email addresses in the field provided. Use the '+' and '-' buttons to add or remove recipients as required:



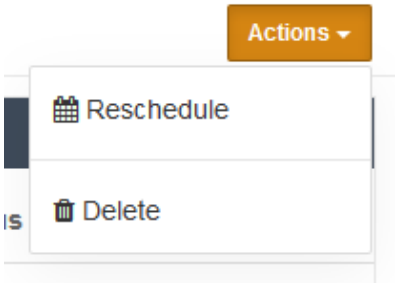
- Click 'Save' to implement your schedule. A summary of your scheduled report will be shown in the 'Scheduled Interface'. You can also download any delivered report by clicking the 'Download' button:



- All scheduled reports that you create will be listed in the left menu under the headings 'Custom Reports' and 'Standard Reports':

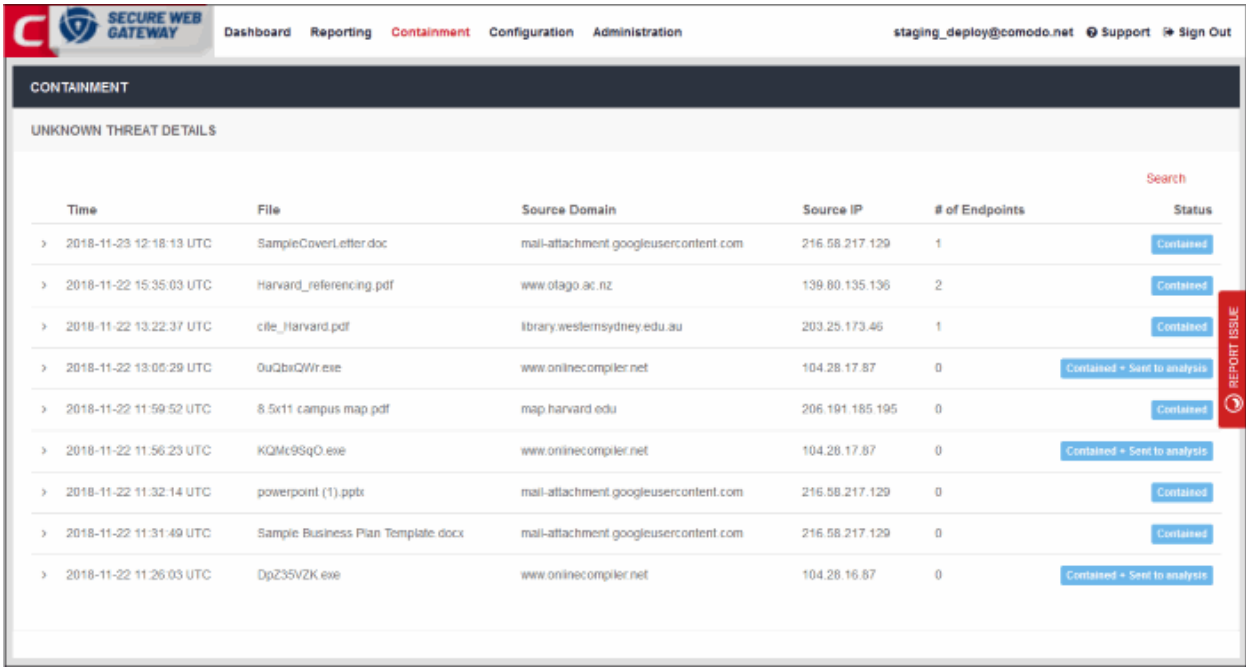


- The 'Actions' button on the upper-right allows you edit (reschedule) or delete reports as required:



10 Unknown Threat Statistics

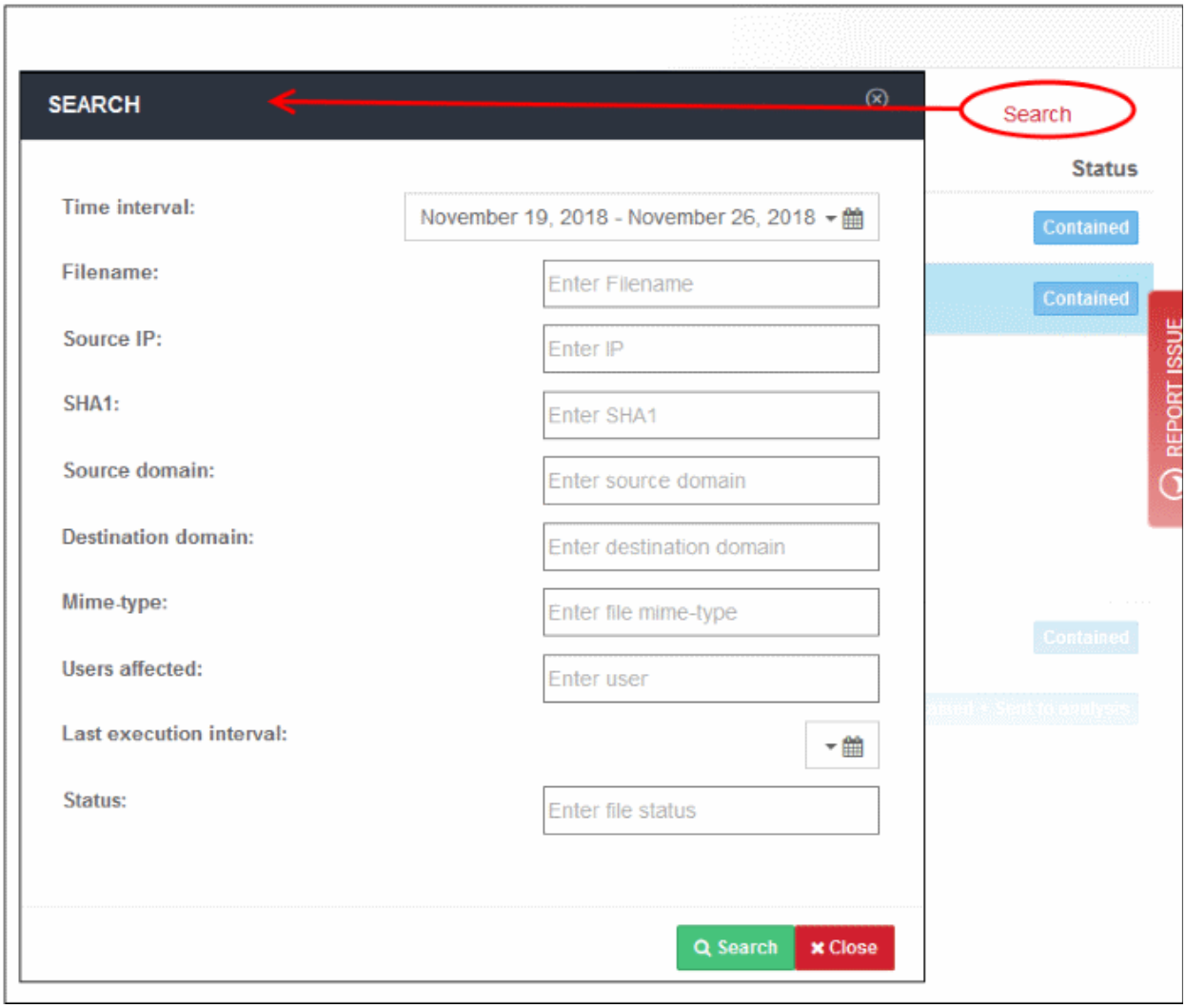
- Click 'Containment' in the top-menu to open the 'Unknown Threat Details' area.
- This area shows details about unknown files discovered on your network.
- Unknown files are automatically run in a secure environment called the 'Container'. While running in the container, unknown files cannot access operating system resources, the file system, other processes or user data.
- Simultaneously, unknown files are uploaded to Valkyrie for analysis to establish their trust level.



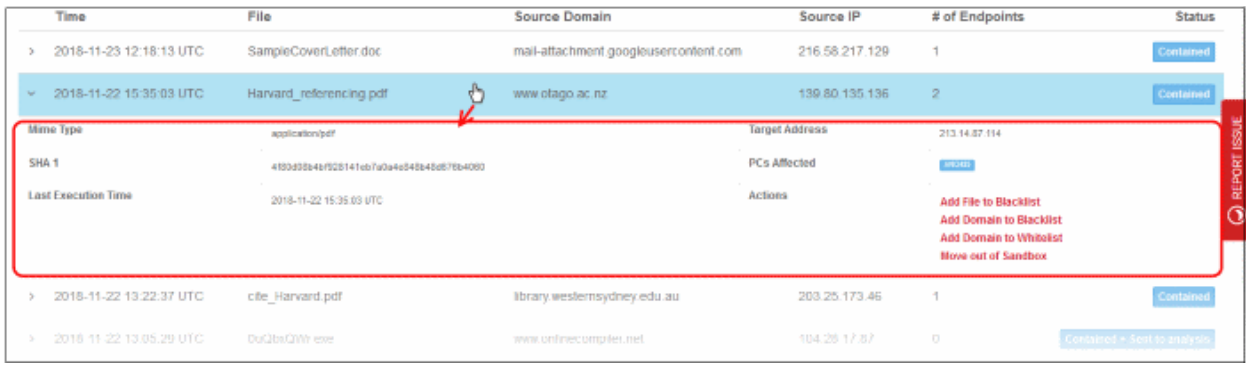
Unknow Threat Details - Table of Column Descriptions	
Column Header	**Description**
Time	Date and time the unknown file was detected
File	Name of the file, including file extension.
Source Domain	Website from which the file originated.
Source IP	IP address of the domain from which the file originated.

# of Endpoints	Number of endpoints on which the file was contained.
Status	Shows whether the file was contained, or contained + uploaded to Valkyrie for analysis. Valkyrie is Comodo's file analysis system. It runs a barrage of tests on unknown files to discover their behavior and assign them a trust rating.

The 'Search' button allows you to find specific files by numerous criteria:



Click a file row to view its details:



- MIME Type – File type
- SHA 1 – Hash value of the file
- Last Execution Time – The date and time the file was last run
- Target Address – The location network IP address the file was downloaded
- PCs Affected – The name of the affected computer(s)
- Actions – Click a link to categorize:
  - Add File to Blacklist – File is added to Global Blocked File List ('Configuration' > 'Advanced Threat Protection' > 'Global Blocked File List')
  - Add Domain to Blacklist - Domain is added to blacklist in the default profile of ATP on the Advanced Threat Protection Page ('Configuration' > 'Advanced Threat Protection' > 'Domain Blacklist')
  - Add Domain to Whitelist - Domain is added to whitelist in the default profile of ATP on the Advanced Threat Protection Page ('Configuration' > 'Advanced Threat Protection' > 'Domain Whitelist')
  - Move out of Sandbox - The file runs outside the container and will not be contained again.

Valkyrie

- You can view the status of unknown files you have submitted to Valkyrie at **https://valkyrie.comodo.com/**.
- You can login to Valkyrie with your Comodo SWG username and password.

More information about using Valkyrie can be found in the dedicated guide at **https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html**

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