COMODO
Creating Trust Online®

COMODO DOME
FIREWALL CENTRAL MANAGER

Comodo **Dome Firewall Central Manager**

Software Version 1.5

Quick Start Guide

Guide Version 1.5.071619

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Dome Firewall Central Manager - Quick Start Guide

This tutorial explains how to setup Comodo Dome Firewall Central Manager then enroll firewall devices for central management.

The guide will take you through the following processes:

- **Step 1 - Setup Firewall Central Manager and login to console**
- **Step 2 - Integrate Dome Firewall Central Manager with Comodo One / Comodo Dragon / ITarian** (Optional)
- **Step 3 - Add Organizations**
- **Step 4 - Enroll firewall devices and assign them to organizations**
- **Step 5 - Configure network connections for firewall devices** (Optional)
- **Step 6 - Create Firewall Policy**

Step 1 - Setup Firewall Central Manager and Login to Console

The trial version of Dome Firewall Central Manager covers unlimited users for one year. The license can be upgraded at anytime for continued usage.

There are two ways to sign-up for a central manager license:

- **New customers** - Sign-up for a free license at **https://cdome.comodo.com/firewall**.
- **Comodo One / Comodo Dragon / ITarian customers** - Sign-up for a free license at **Comodo One** / **Comodo Dragon** / **ITarian** portal
    - Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
    - Click 'Store' then go to the firewall central manager tile.
    - Click the 'Free' button to begin setup.
    - After adding to Comodo One / Comodo Dragon / ITarian portal, you can open it by clicking 'Applications' > 'Dome Firewall Central Manager'. See **Step 2 - Integrate Dome Firewall Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

After sign up, there are two modes in which you can setup central manager:

- **Virtual Appliance** - Download the setup file and install central manager as a virtual appliance on your local network
- **Cloud Mode** - Comodo will host your central manager instance on our secure cloud servers

Virtual Appliance

- The virtual appliance setup file is available in two formats:
    - **.OVA File**
    - **.ISO File**

Install from OVA File

- Download the .ova file from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewallcm.ova**.
    - Alternatively, download the .ova from the final instructions dialog when adding CM to your Comodo One / Comodo Dragon / ITarian account.

- Import the virtual appliance into VMs such as Virtualbox or Vmware.
- Assign a public IP address to the virtual appliance
- Once installed, you can access the central manager console at https://<IP address of the virtual appliance>
    - UN = 'admin', password = 'comodo' (both without quotes). You should change the password after first login.

Install from ISO File

- Download the .iso file from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewallcm.iso**.
- Create a Ubuntu virtual machine on a VM such as Virtualbox or Vmware.
- Install central manager from the .iso file
- Assign a public IP address to the virtual appliance
- Once installed, you can access the central manager console at https://<IP address of the virtual appliance>
    - UN = 'admin', password = 'comodo' (both without quotes). You should change the password after first login.

Cloud Version

- Contact Comodo at **provisiondome@comodo.com** with your license key to setup the service.
- Once setup, we will send you the address where the service is hosted.
- You can access your central manager instance at the address provided.
- The default username is 'admin' and password is 'comodo' (without quotes). You can change these credentials anytime after your first login.

Tip: Comodo One / Comodo Dragon / ITarian customers can integrate the central manager appliance with their portal accounts. See **Step 2 - Integrate Dome Firewall Central Manager with Comodo One / Comodo Dragon / ITarian** for guidance on this.

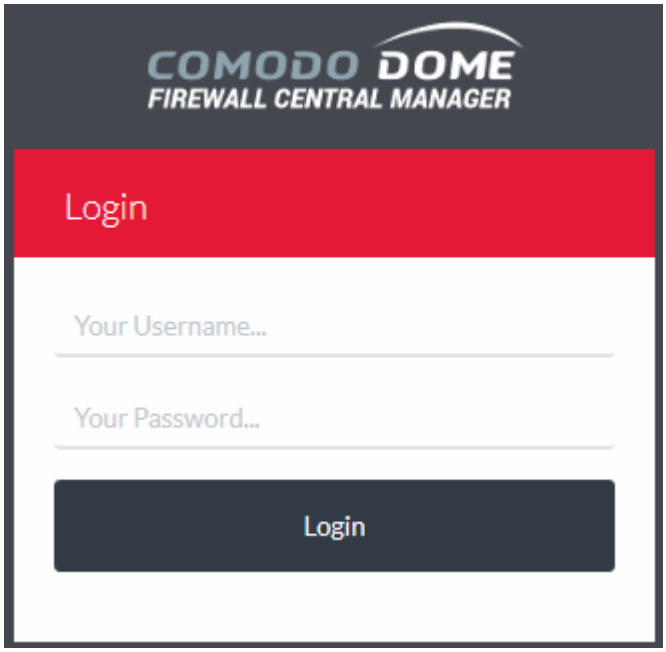
Login to the Console

Dome Firewall Stand-alone Customers

Once setup, you can login to the Dome Firewall Central Manager admin console using any web browser.

- Enter the URL or https://<*ip address of the central manager*>:8000 in the address bar of the browser

The login screen will be displayed.



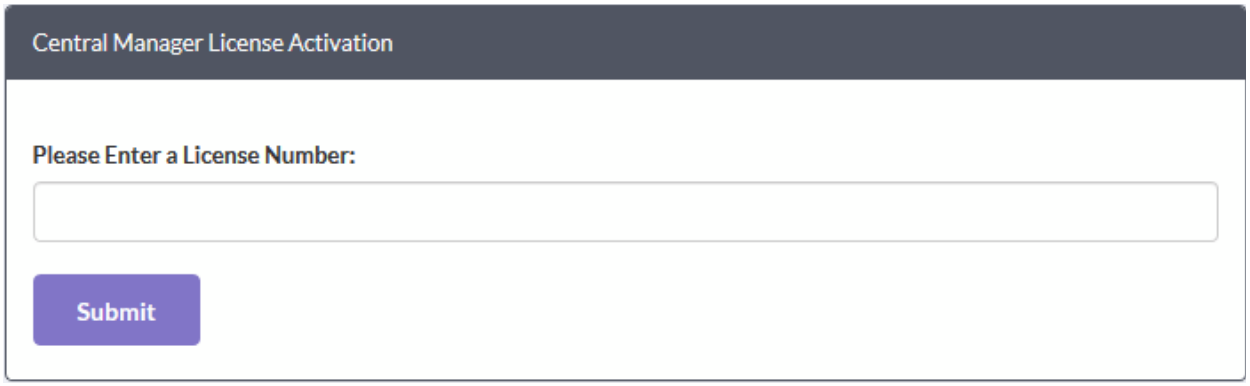
You can login with the default credentials:

Username = admin

Password = comodo

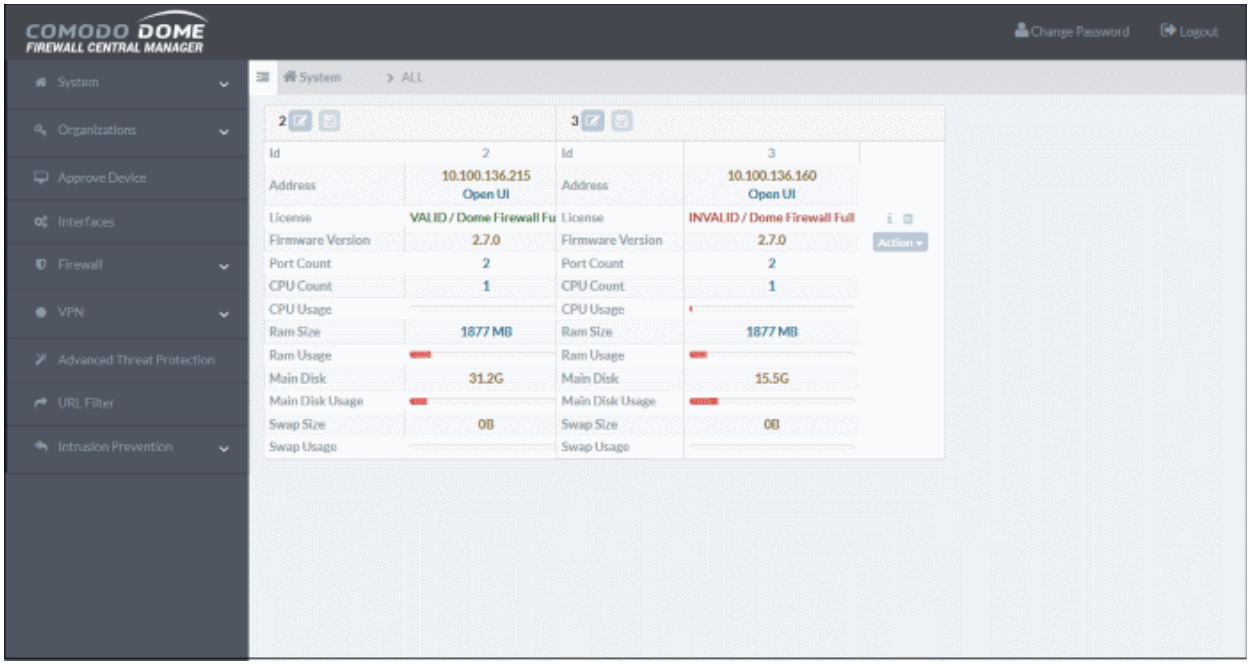
After first login, Dome Firewall Central Manager requires that you change the default password. Please choose a strong password that contains a mix of upper and lower case letters, numbers and special characters. We also recommend regularly changing your password as a best security practice.

- If you have setup central manager as a virtual appliance, you will be asked to enter the license key on your first login:



- Enter your license key and click 'Submit'.

The interface will open at the dashboard by default:



- After you have enrolled firewall devices, each device will be shown as a tile on the dashboard.
- Each tile displays hardware, software and licensing details about the device.
- The 'Open UI' link lets you login to the firewall itself to perform actions like backup data, edit network configuration and configure SSH access.
- You can also edit the name of the device and remove a device from the dashboard.
- Click 'Please select an organization or device' to filter which devices are shown on the dashboard.

Comodo One / Comodo Dragon / ITarian Customers

There are two ways to access the management console:

- Stand-alone console
  - Paste your login URL into the address bar of the browser. The URL is of the format: https://<given *ip address of the central manager*>
  - Login with the default credentials:
  - Username = admin
  - Password = comodo
  - You can change these credentials anytime after your first login. Click 'Change Password' at the top-right of the interface.
- Comodo One / Comodo Dragon / ITarian portal
  - You can integrate central manager with your Comodo One / Comodo Dragon / ITarian account. Doing so will let you access central manager from your portal. See **Step 2 - Integrate Dome Firewall Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.
  - After integration, login to your portal account and click 'Applications' > 'Dome Firewall Central Manager'.

Step 2 - Integrate Dome Firewall Central Manager with Comodo One / Comodo Dragon / ITarian portal (Optional)

Comodo One / Comodo Dragon / ITarian customers can integrate Central Manager with their portal account. Once integrated, you can access CM from the portal by clicking 'Applications' > 'Dome Central Manager'.

- **Dome Firewall Central Manager Virtual Appliance** - Integrating CM virtual appliance with Comodo One /

Comodo Dragon / ITarian portal involves two steps:

- **Enable SSO in the virtual appliance**
- **Add the IP Address of your CM installation as Dome Service URL for Dome Firewall Central Manager to your Comodo One / Comodo Dragon / ITarian account.**

- **Dome Firewall Central Manager Cloud Mode** -
- Single Sign-on (SSO) is enabled by default in the cloud version.
- You need to add the address of your CM instance as the 'Dome Service URL' to connect CM to your Comodo One / Comodo Dragon / ITarian account.
- See **Configure Dome Service URL in your Comodo One / Comodo Dragon / ITarian account.**

Enable SSO in the virtual appliance

Note: Ensure that you have assigned a public IP address to the virtual appliance

- Login to the root account of the Linux virtual machine with default credentials:

  username = root

  password = comodo
- Open the settings file of the central manager at /home/ubuntu/central-manager/centralmgr/settings.py using an editor.
- Scroll down to the 'cONE SSO settings' area

```
        'rest_framework.authentication.SessionAuthentication',
    )
}

# Honor the 'X-Forwarded-Proto' header for request.is_secure()
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')

# Allow all host headers
ALLOWED_HOSTS = ['*']

#AUTH_USER_MODEL = 'authentication.Account'

#License
WEB_API_LOGIN = "utm_web_api"
CAM_PATH_TO_CONNECT = "accounts.comodo.com"
CAM_PORT_TO_CONNECT = 443
CAM_SERVICE_PATH = "/signup_service/check_license_key"
SECRET_PHASE = "cwrcxdvgamknndmo"

# cOne SSO
SSO = 0  # 0 for casual login
SSO_TOKEN_CHECK_IP = 'one.comodo.com'
SSO_TOKEN_CHECK_PORT = 80
SSO_TOKEN_CHECK_SSL_PORT = 443
SSO_TOKEN_CHECK_URI = '/ir'
SSO_EMAIL_CHECK_IP = 'one.comodo.com'
SSO_EMAIL_CHECK_URI = '/app/auth'
SSO_EMAIL_CHECK_PORT = 80
SSO_EMAIL_CHECK_SSL_PORT = 443
SSO_REDIRECT_PREFIX = 'https://one.comodo.com/app/?token='
SSO_REDIRECT_POSTFIX = '#/licensed-applications/dome_firewall_central_manager'
SSO_TOKENLESS_REDIRECT_URL = 'https://one.comodo.com/app/#/licensed-applications/dome_firewall_centr
al_manager'
SSO_API_KEY = 'DOMEFWCMAK'
SSO_SSL_ENABLED = 1
SSO_TOKEN_PATH = '/etc/cm_sso_token.txt'
```

- Set the SSO flag to1
- Save the 'Settings' file

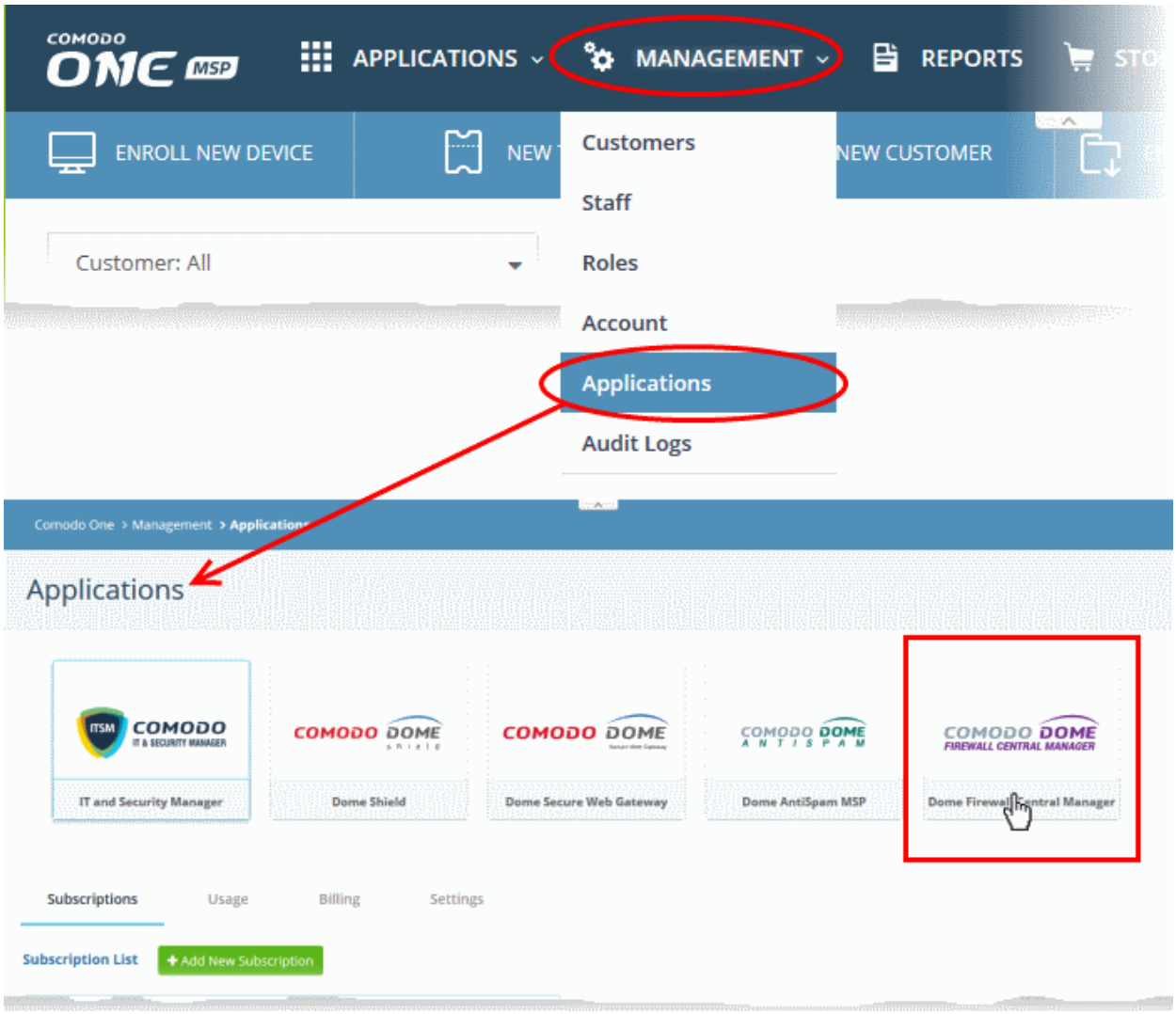
- Restart the apache service using the Sudo command: *sudo apache2ctl restart*

SSO with your portal is enabled in your Central Manager appliance.

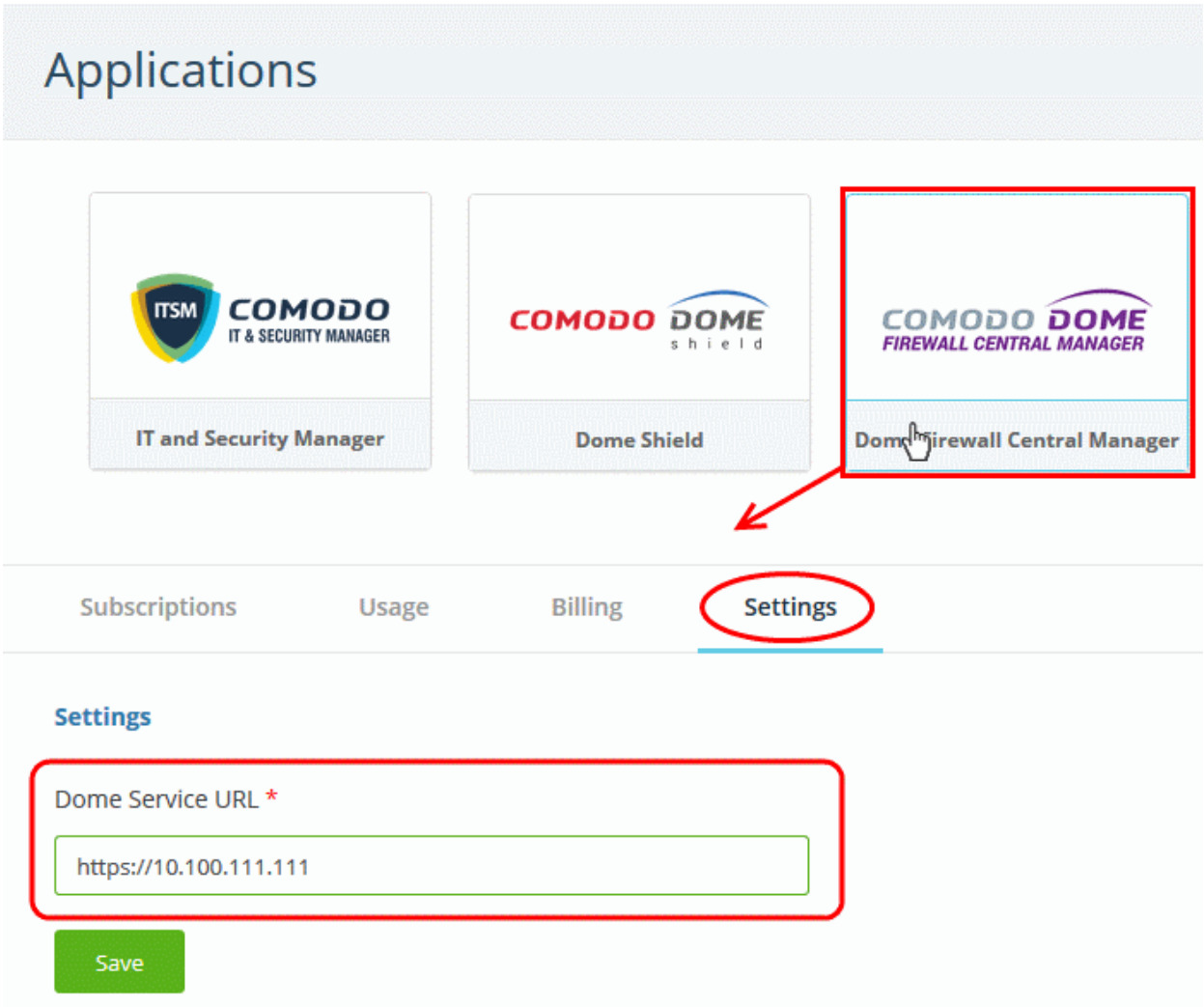
Configure Dome Service URL in your Comodo One / Comodo Dragon / ITarian account

You need to add the address of your CM instance as the 'Dome Service URL ':

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Manage' > 'Applications' from the top to open the Application Management screen. (Comodo One portal is shown below as an example)



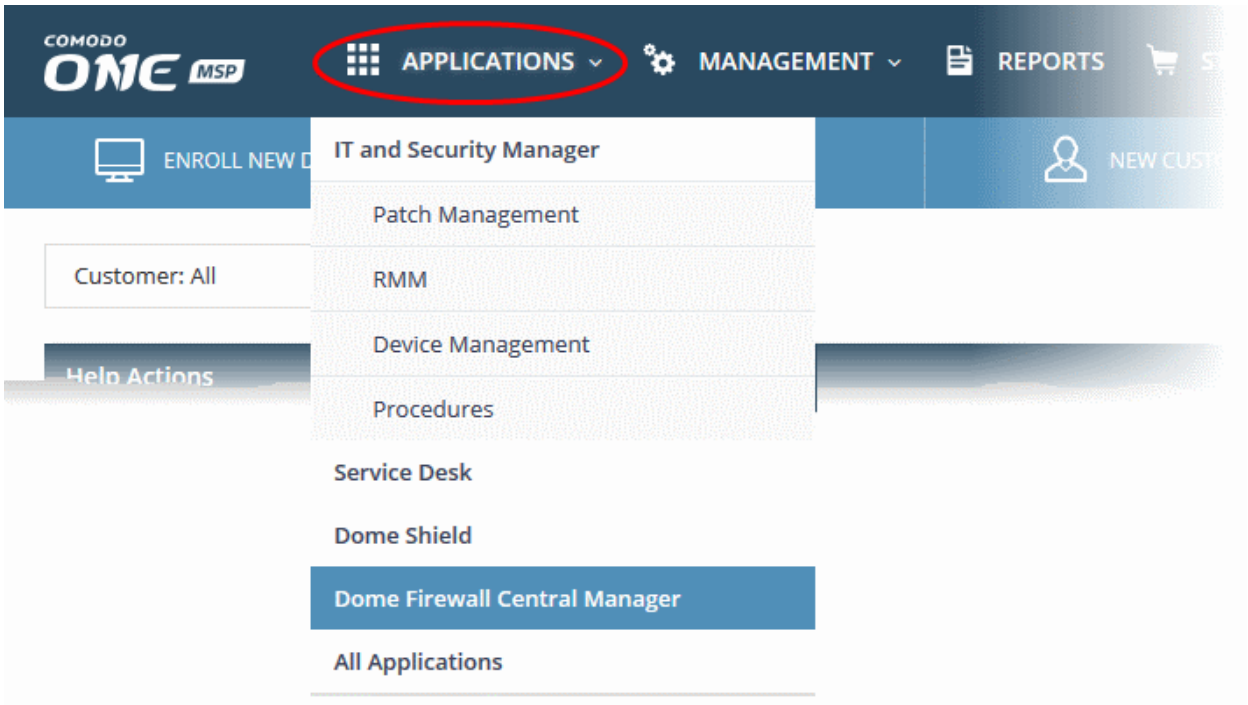
- Click the 'Dome Firewall Central Manager' tile
- Select the 'Settings' tab in the bottom pane



- Enter the address of your Dome Firewall Central Manager instance in the Dome Service URL text box and click 'Save'.

Your Firewall Central Manager appliance is now integrated with your Comodo One / CD / ITarian account. You can login to your Central Manager console from your portal.

- You can access CM from your portal as follows:
  - Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
  - Click 'Applications' > 'Dome Firewall Central Manager'



Central manager will open at the dashboard in a new tab.

Step 3 - Add Organizations

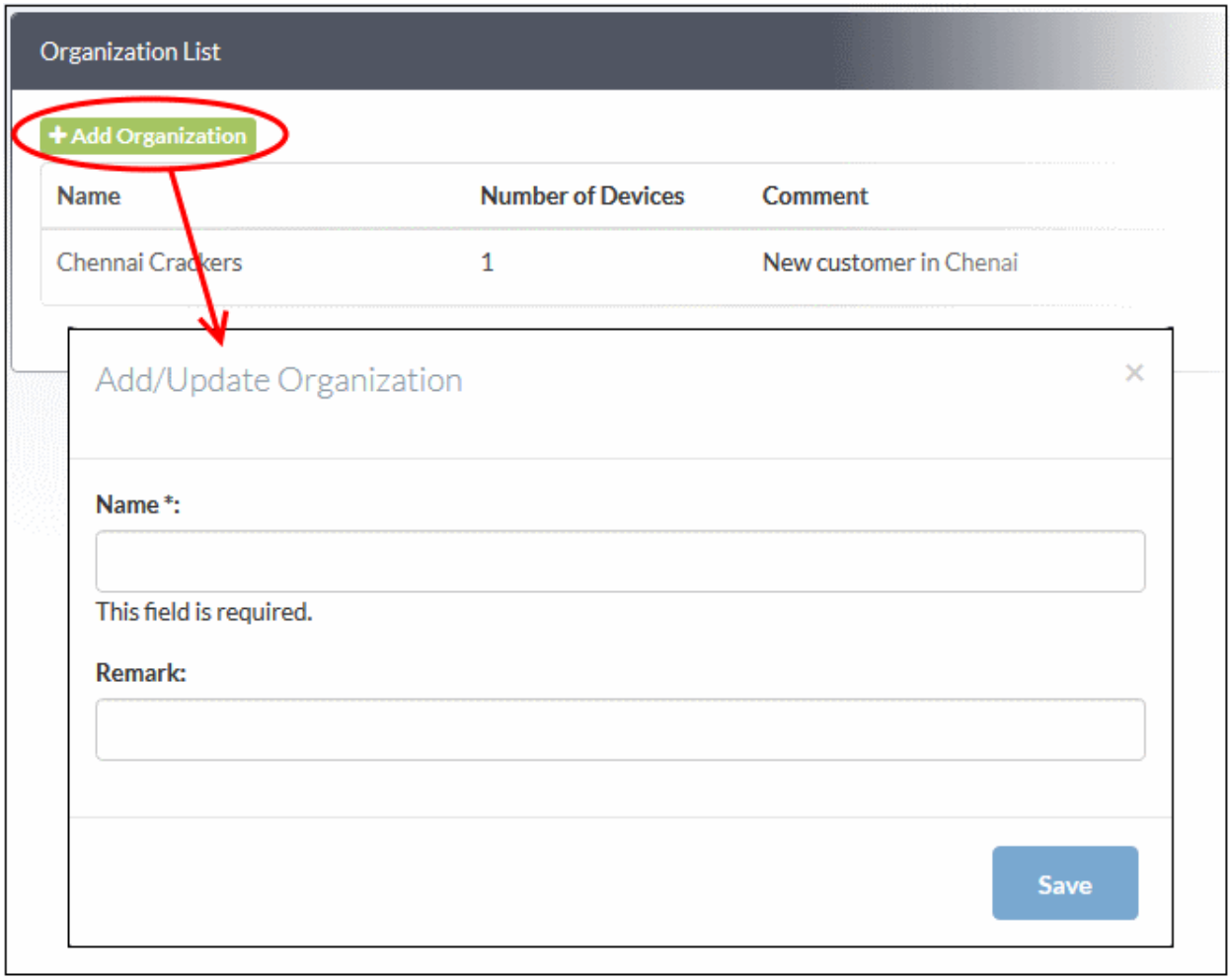
- Each firewall device you enroll to the central manager needs to be assigned to an organization. Doing so will allow you to collectively manage and apply policies to all devices in the organization.

Notes:

- Your C1 / CD / ITarian 'Organizations' are NOT imported into Comodo firewall central manager.
- You must add organizations separately in firewall central manager. You may, of course, use the same organization names for identification purposes.

To add organizations

- Click 'Organizations' > 'Organizations' on the left
- Click 'Add Organization' at the top-left of the interface



Complete the following items in the add organizations dialog:

- Name - The name of the customer organization you want add. You can make this match the name of a C1 / CD / ITarian organization if you prefer.
- Remark – Description of, or comments about, the organization

- Click 'Save' to add the organization.

The new organization will be shown in the organization list. You can now assign devices to the organization. Firewall policies which are applied to an organization will take effect on all devices in the organization.

- Repeat the process to add more organizations.

Step 4 - Enroll Firewall Devices and Assign them to Organizations

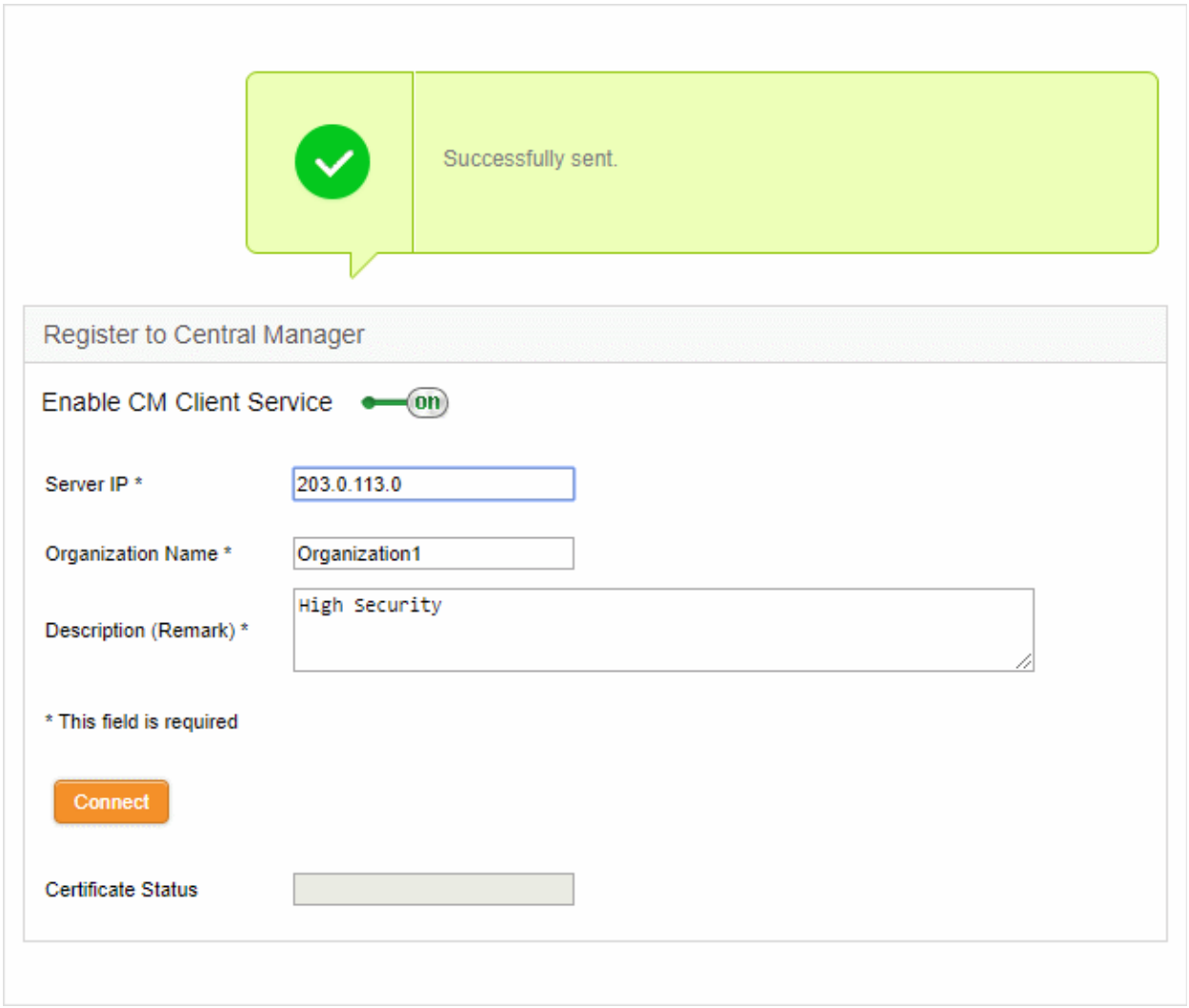
- Assigning multiple devices to an organization allows you to collectively manage and update them.

To connect a Dome Firewall Device to the central manager

- Login to the firewall device at https://<*ip address of the dome firewall device*>:10443
- Click 'System' > 'Central Management'
- Switch 'Enable CM Client Service' to 'ON'
- Enter the parameters required to connect the firewall to the central manager
  - Server IP - The IP address of the DFW Central Manager interface

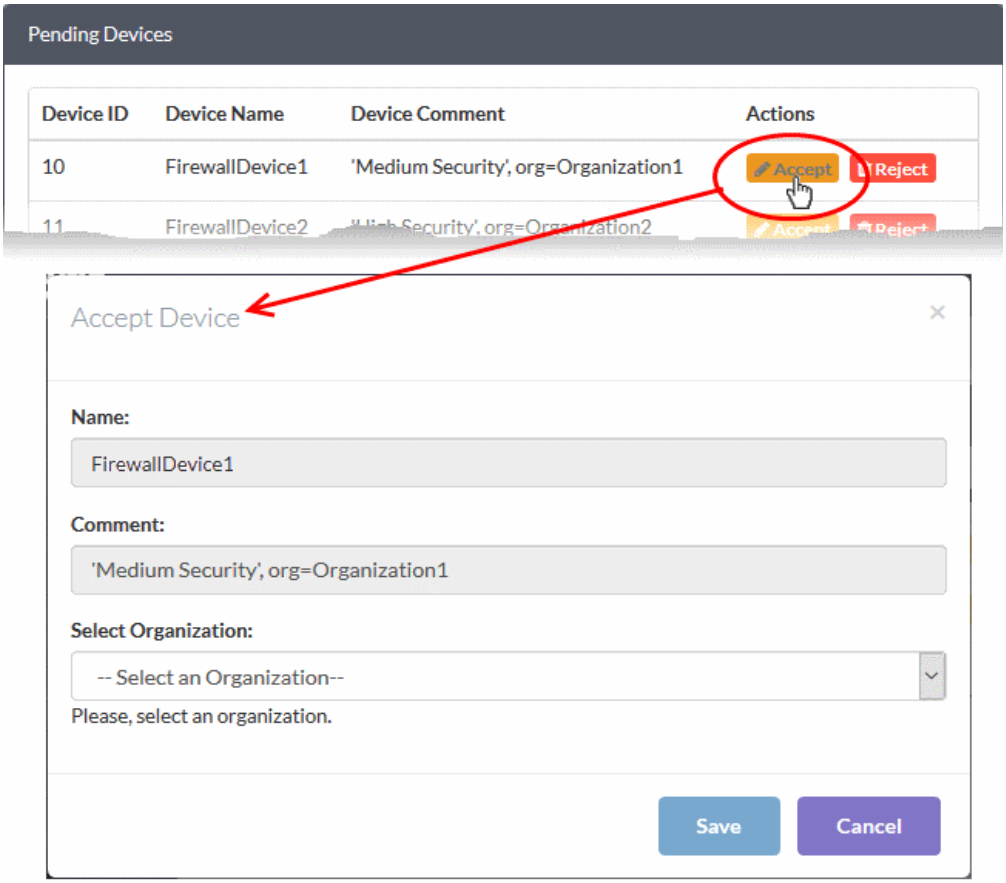
- Organization Name - The name of the organization to which you want the device to belong. You can create organizations by logging into central manager and clicking 'Organizations' > 'Organizations' > 'Add Organization'.
- Description (Remark)* - Enter any comments you wish to leave about the device

- Click 'Connect'



The device will attempt to connect to Dome Firewall Central Manager. After a successful connection is made you will need to approve the device:

- Login to the DFW Central Manager console
- Click 'Approve Device' on the left.
- The 'Pending Device' interface shows all devices awaiting approval.
- Click 'Accept' next to the device you wish to approve. This will open the 'Accept Device' dialog.



- You have the option to change the device organization if required.
- Click 'Save' to approve the device and assign it to an organization.
- Repeat the process to approve and import more devices.

Step 5 - Configure Network Connections for Firewall Devices (Optional)

- A firewall device should have network adapter ports to connect to different network zones.
- By default, port 1 on the FW device is automatically configured for LAN with IP 192.168.0.15.
- The number of ports shown in the CM network configuration screen depends on the number of adapters on the FW device. These ports are shown as Port 2, Port 3, Port 4 etc.
- If required, you can define new interfaces for different network zones in central manager. You can then configure ports on the firewall device to connect to the new interfaces.

In brief:

- Ports and zones configured on the FW device will be imported to CM when the device is enrolled. Example zones are LAN, WIFI, Internet.
  - Click 'System' > 'Dashboard' > select the device > 'Action' > 'Network Configurations' to view imported network settings and zone configurations.
- You can define new interfaces (zones) for the ports in CM for a FW device.
  - Click 'Interfaces' on the left, then 'Add Zone'.
  - Define a new zone (such as LAN, WIFI, Internet) and click 'Save'.
  - Next, click 'System' > 'Dashboard' > select the device > 'Action' > 'Network Configurations'
  - Click the drop-down in the 'Actions' column beside a port that you want to configure and select the zone. The zone options include imported zones and configured zones in CM. Zones added for

organizations will be prefixed with 'O' and for devices with 'D'.

- Click 'Save'. The new network interface configuration for the port will be updated on the FW device.

To add new network zone interfaces

- Click 'Interfaces' on the left
- Select an organization or device from the drop-down in the title bar (next to the word 'Interfaces')
  - Select an organization to manage interfaces for all devices belonging to the organization
  - Select an individual device to manage the interfaces for a specific device

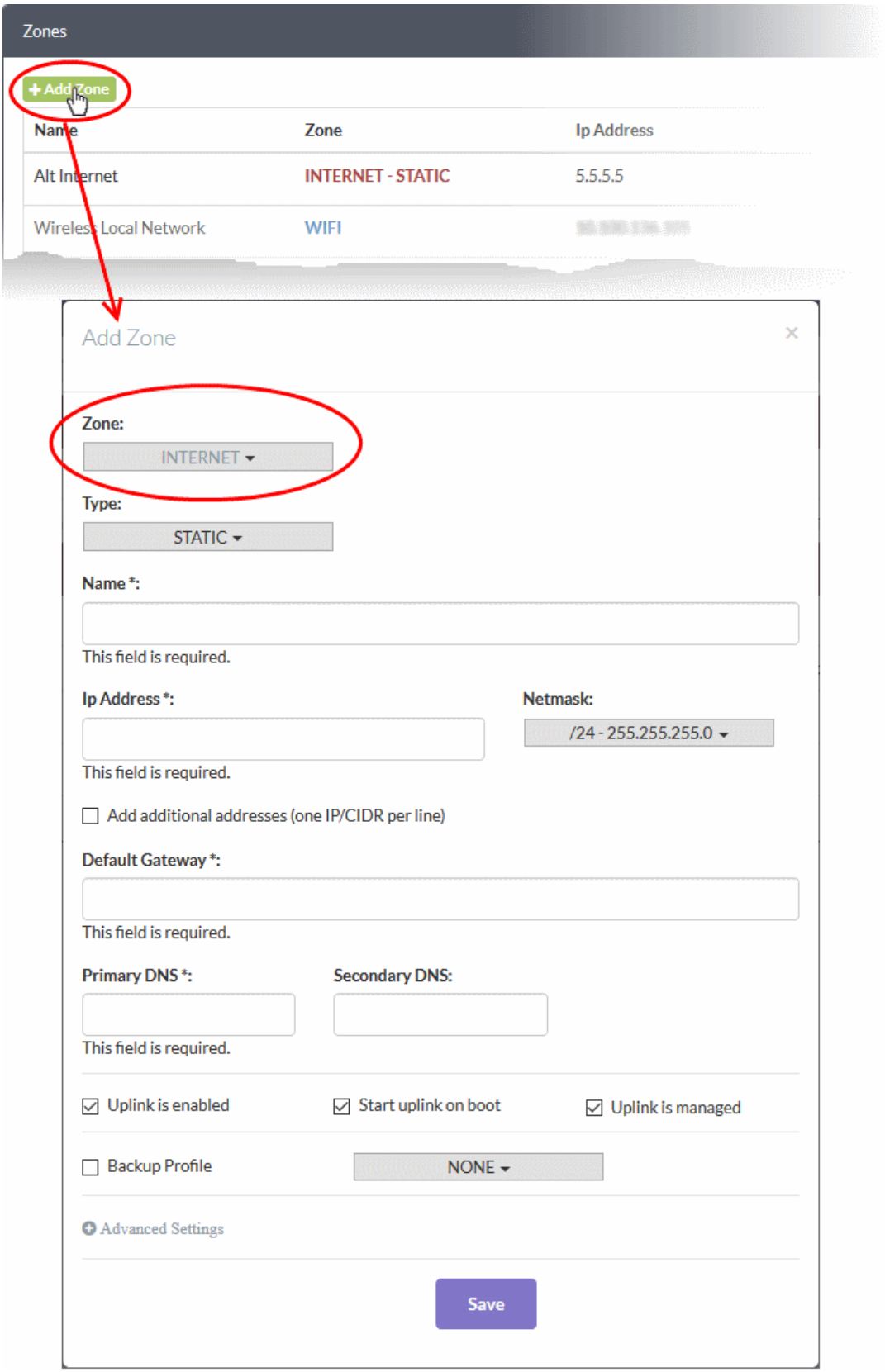
The 'Zones' screen shows all the interfaces created for the selected organization/device.

The following sections explain how to configure network zone interfaces:

- **Add untrusted external network zones for connecting to the internet (e.g. WAN)**
- **Add trusted internal network zone interfaces (e.g. LAN, DMZ, WiFi)**

Add untrusted external network zones for connecting to the internet (e.g. WAN)

- Click the 'Add Zone' button at the top-left of the 'Zones' screen
- Select 'Internet' from the 'Zone' drop-down



- Type - Choose the interface type through which the firewall device will connect to the internet. Options are:
  - STATIC - The external network interface is in a LAN and has a fixed IP address and netmask. An example is a router in which the DFW device is assigned a fixed IP address.
  - DHCP - The external network interface receives its network configuration through dynamic host control protocol (DHCP) from a local server, router, or modem.
  - PPPoE - The external interface is connected to an ADSL modem through an ethernet cable. Select

this option only if the modem uses the Point-to-Point Protocol over Ethernet (PPPoE) to connect to the service provider.

- Configure the parameters for the selected interface type

Device Settings

- Name - Enter a label to identify the interface
- IP Address - The address that will be assigned to the interface
- Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)
- Add additional addresses - Enable this box if you wish to add additional IP address(es)/netmask(s) to the interface.
- Default gateway - Enter the IP address of the gateway through which the firewall connects to the internet
- DNS Settings - Enter the IP addresses/hostnames of the primary and secondary DNS servers you wish to use.

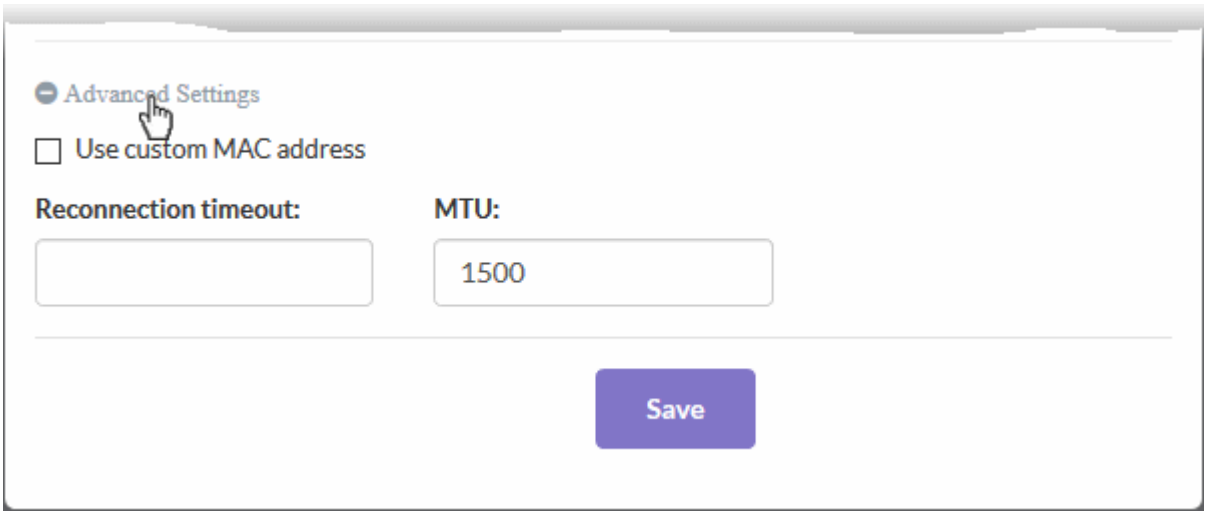
Uplink Settings

- Uplink is Enabled - The uplink will be activated after you click 'Save'. Deselect this if you don't want to enable the uplink device at this time. You can enable the uplink later by editing the interface from the dashboard of the firewall device console.
- Start uplink on boot - The uplink will start automatically on every restart of the DFW device. Deselect this checkbox if you want to manually start the uplink when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details displayed in the firewall dashboard. Deselect this option if you do not want the uplink details to be shown in the dashboard.
- Backup Profile - Select if you want to specify an alternate uplink connection which will become active in the event this one fails. Choose the alternative uplink from the drop-down.

Advanced Settings:

The 'Advanced Settings' pane lets you specify the MAC address and the Maximum Transmission Unit (MTU) of data packets for the interface. These settings are optional.

- Click the 'Advanced Settings' link if you need to specify custom values for these fields



- Use custom MAC address - The firewall will automatically detect the MAC address of the network adapter port and will populate it in the MAC address column. Enable 'Use custom MAC address' if you need to override and replace the default MAC address of the external interface. Enter the MAC address in the text box that appears below the checkbox.

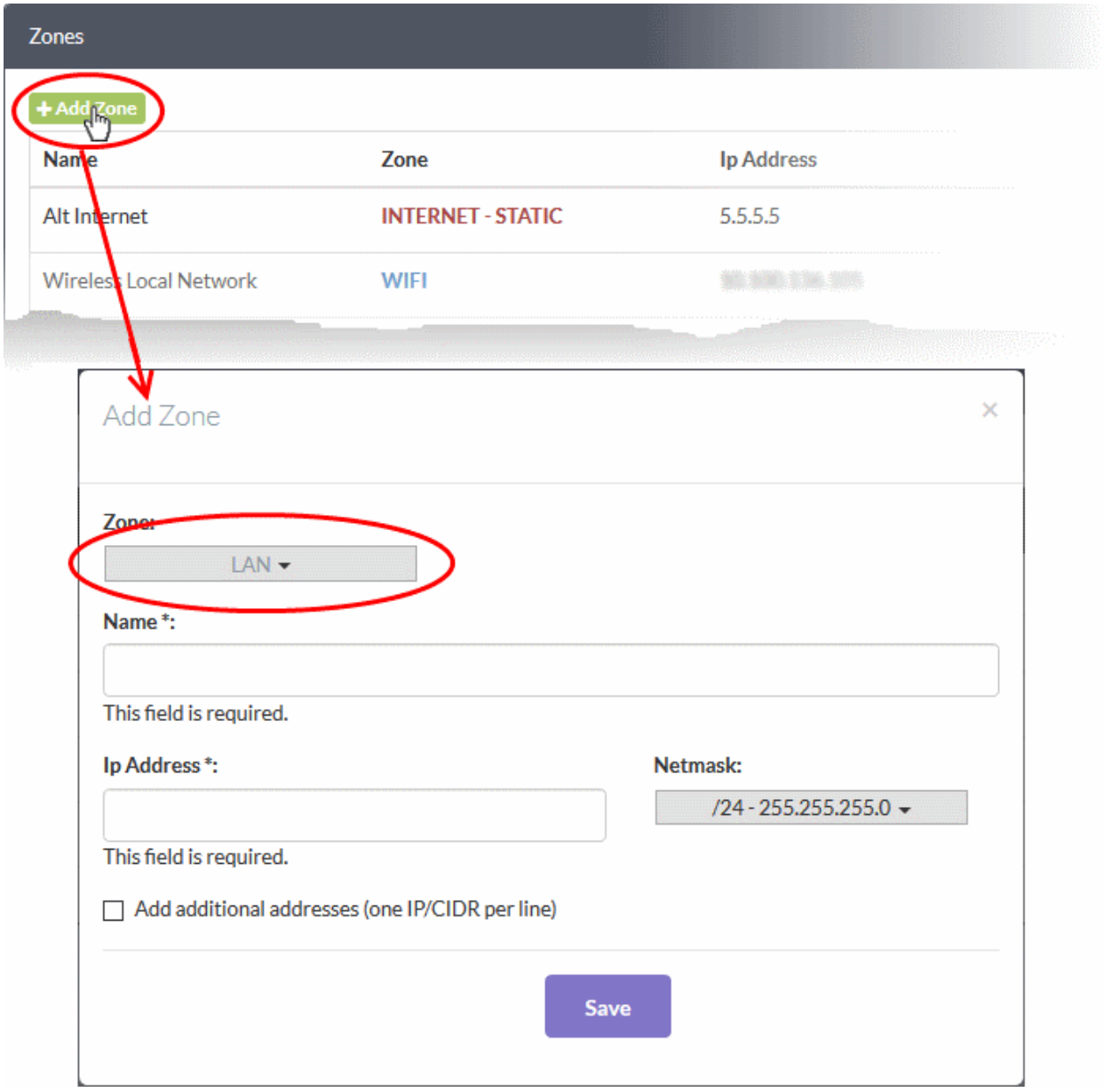
- Reconnection timeout - Specify the maximum period in seconds that the uplink should attempt to reconnect in the event of a connection failure. The connection timeout period depends on the ISP configuration. If you are unsure, leave this field blank.
- MTU - Enter the Maximum Transmission Unit (MTU) of the data packets that can be sent over the network.

- Click 'Save'.

The interface will be added to the list.

Add trusted internal network zone interfaces (e.g. LAN, DMZ, WiFi)

- Click the 'Add Zone' button at the top-left of the 'Zones' screen.
- Select 'LAN', 'WIFI' or 'DMZ' from the 'Zone' drop-down as required.



- Configure the following for the internal network zone:
  - Name - Enter a label to identify the interface.
  - IP Address - Enter the IP address of the interface as pre-configured in the network
  - Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)

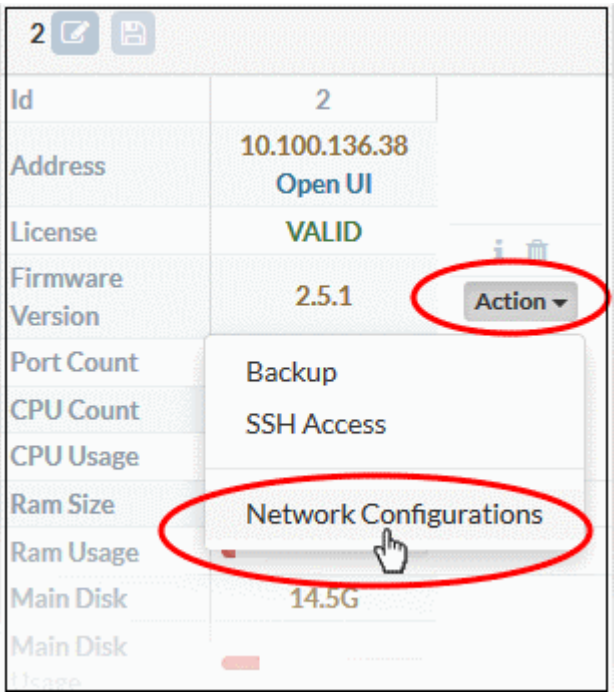
- Add additional addresses - Enable to add additional IP address(es)/netmask(s) to the interface. Enter the additional address(es)/netmask(s) one per line in the text box that appears.

- Click 'Save'.

The interface will be added to the list.

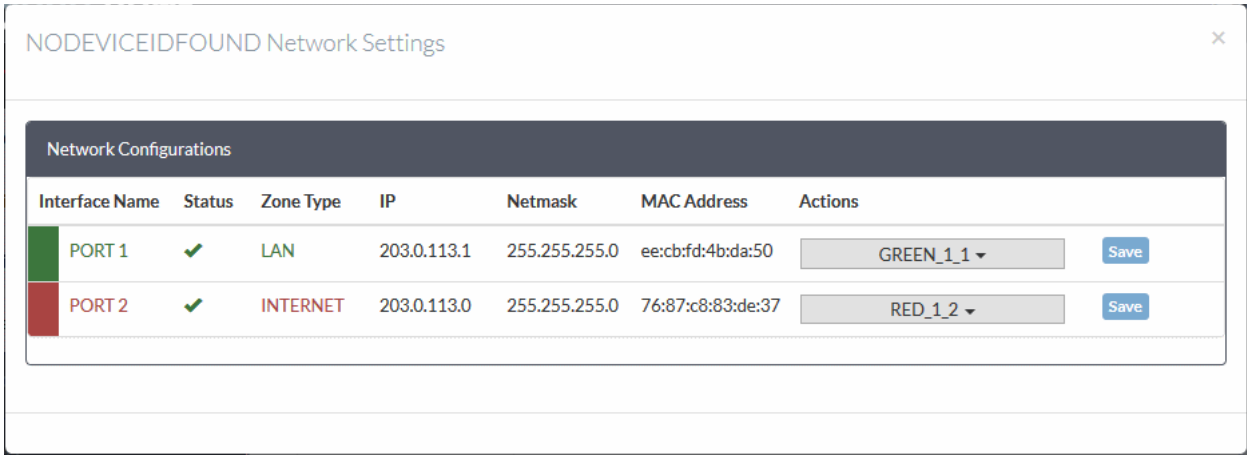
To view and manage the network connections for a device

- Click 'System' on the left then select 'Dashboard' to open the dashboard
- Click the 'Actions' button on the tile of the device

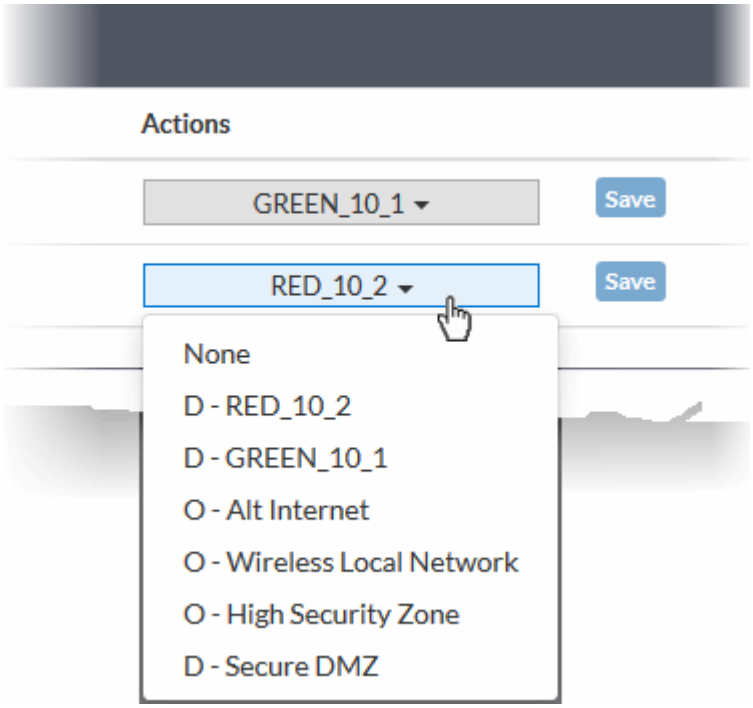


- Choose 'Network Configurations' from the options

The 'Network Settings' dialog for the device will appear.



- Use the drop-down in the 'Actions' column to select the interface (zone) for each port in the firewall device
  - Organization interfaces are prefixed 'O', and are available for all devices in the organization
  - Individual interfaces are prefixed 'D' and are available only for a specific device
- Click 'Save'.



Step 6 - Create Firewall Policy

Central manager lets you configure firewall policies for all devices in an organization and for individual devices. You can also create rules for source network address translation (SNAT), destination network address translation (DNAT), system access and more.

- Note - Existing FW

Each Dome firewall has a policy which manages traffic flowing in and out of the network. A policy is constructed from a series of firewall rules that are imposed on different types of traffic.

- Incoming traffic - Traffic from external network zones to hosts in the internal network zone
- Outgoing traffic - Traffic from hosts to the external network zone
- Inter-zone traffic - Traffic between network zones connected to the firewall device
- VPN traffic - Traffic from users connected to internal zones via virtual private network (VPN).

Each Firewall rule contains three components:

- General Settings - Specify source and destination addresses and the service/protocol of packets to be intercepted by the rule. You can select firewall address objects/groups as 'source' and 'destination' addresses. See **Create Firewall Address Objects** for help to create firewall address objects.
- Web Protection - Enable or disable URL filtering, Advanced Threat Protection (ATP) and SSL Interception. You can also choose pre-configured profiles for them. See **Manage ATP Profile** and **Create URL Filter Profiles** for help to create these profiles.
- Content Flow Check - Enable or disable Intrusion Prevention and Application Detection settings for the rule.

You can create different rules for different configurations for each of these components. The rules will be applied to the inbound and outbound packets in order.

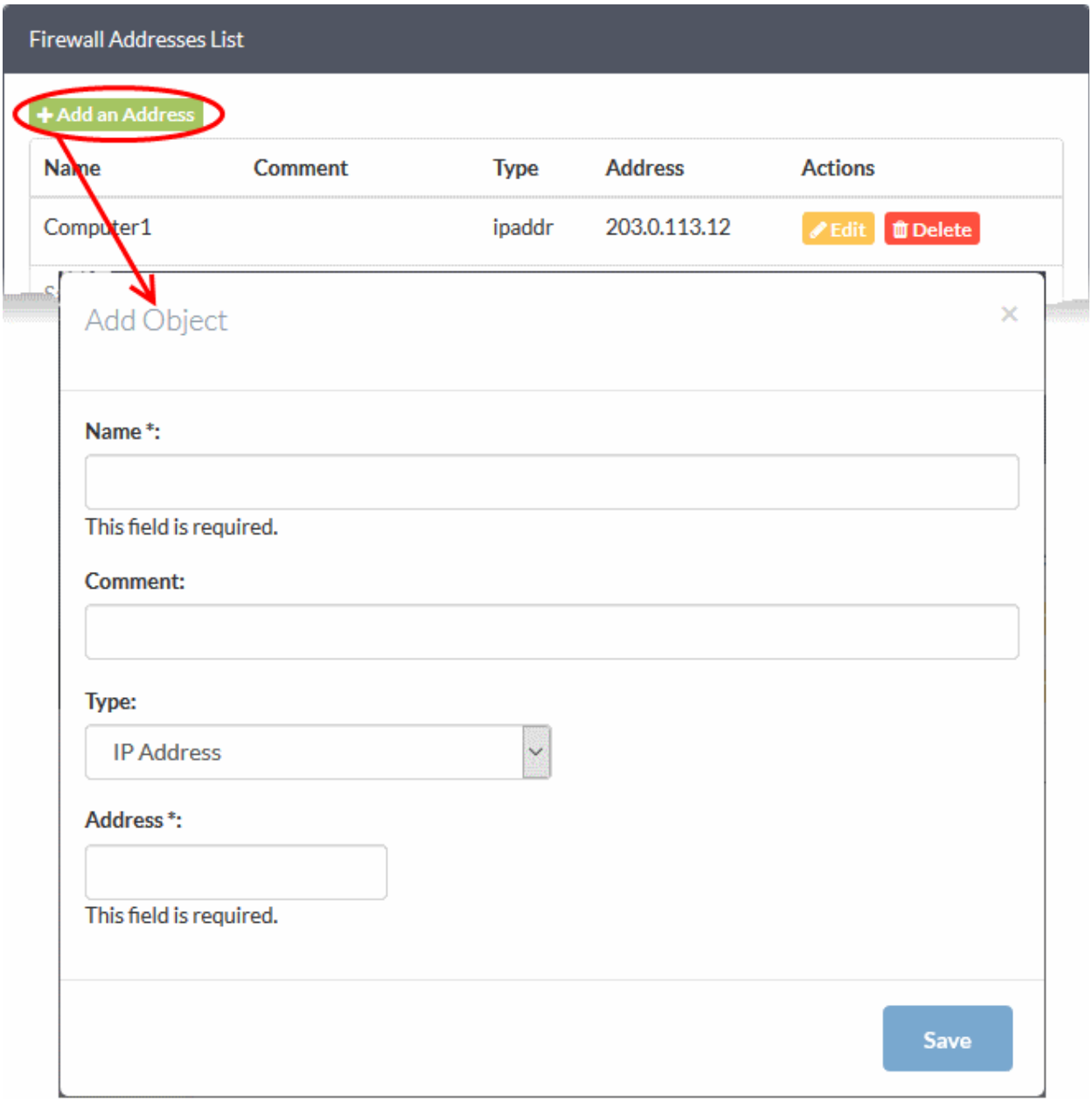
- Before creating a firewall policy, you must first create firewall address objects, an advanced threat protection (ATP) profile, URL filters, and an intrusion prevention profile.
- Once done, these objects and profiles can be used in firewall, source network address translation (SNAT)

and system access rules.

- **Firewall Address Objects**
- **Firewall Address Object Groups (Optional)**
- **ATP Profiles**
- **URL Filter Profiles**
- **Intrusion Prevention Profile**
- **Configure Firewall Policy**

Create Firewall Address Objects

- An address object is reference to a set of IP addresses in a specific organization / device. These objects can be used in firewall rules.
- Click 'Firewall' > 'Firewall Addresses' in the left-hand menu
- Select an organization or individual device from the drop-down above the list (next to the word 'Firewall')
    - Select an organization object to manage addresses for all devices in the organization
    - Select an individual object under an organization to manage addresses for a single device
- Click the 'Add an address' button
- The 'Add Object' dialog will open:

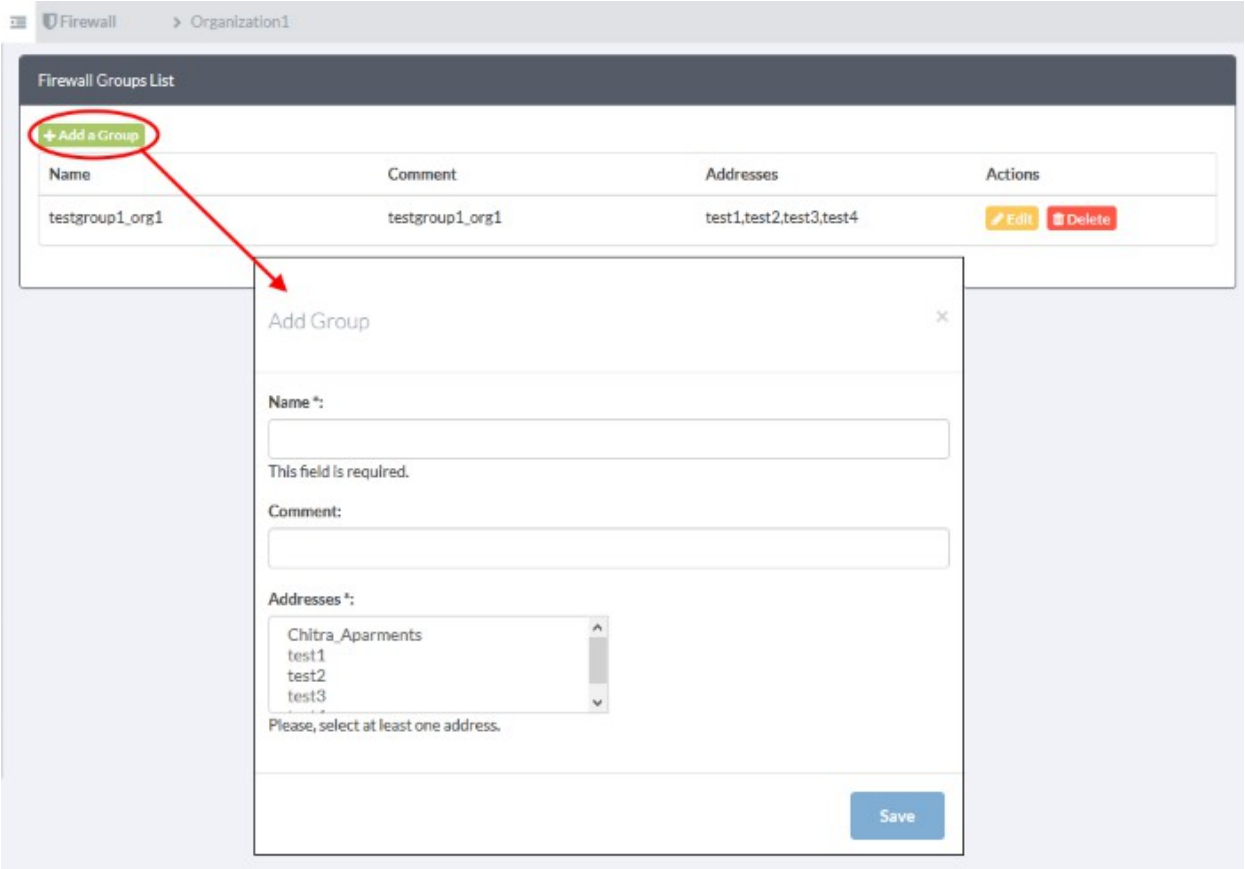


- Enter parameters for the new object:
  - Name - Specify a label for the object (15 characters max). Ideally this should help identify the host(s) included in the object.
  - Comment - Enter a short description of the object.
  - Type - The type of address object you wish to create. The options are:
    - Subnet - The object will describe an entire sub-network of computers. Enter the subnet address in the 'Address' field.
    - IP address - Select this if a single host will be covered by the object. Enter the IP address in the 'Address' field.
    - IP range - The object will refer to hosts on an entire range of IP addresses. Enter the IP range in the 'Address' field.
- Click 'Save'. The new address object will be added to the list.

Create Firewall Address Object Groups (Optional)

- Firewall object groups consist of one or more IP address objects. Object groups can be created for organizations or devices.

- Click 'Firewall' > 'Firewall Groups' in the left-hand menu
- Select an organization or individual device from the drop-down above the list (next to the word 'Firewall')
  - Select an organization object to manage groups for all devices in the organization
  - Select an individual object under an organization to manage groups for a single device
- Click 'Add a Group' at the top-left. The 'Add Group' dialog will open:



- Enter the parameters for the new object:
  - Name - Specify a label for the group (15 characters max)
  - Comment - Enter a short description of the group.
  - Address - Select the address objects that should be included in the group.
- Click 'Save'. The new group will be added to the list.

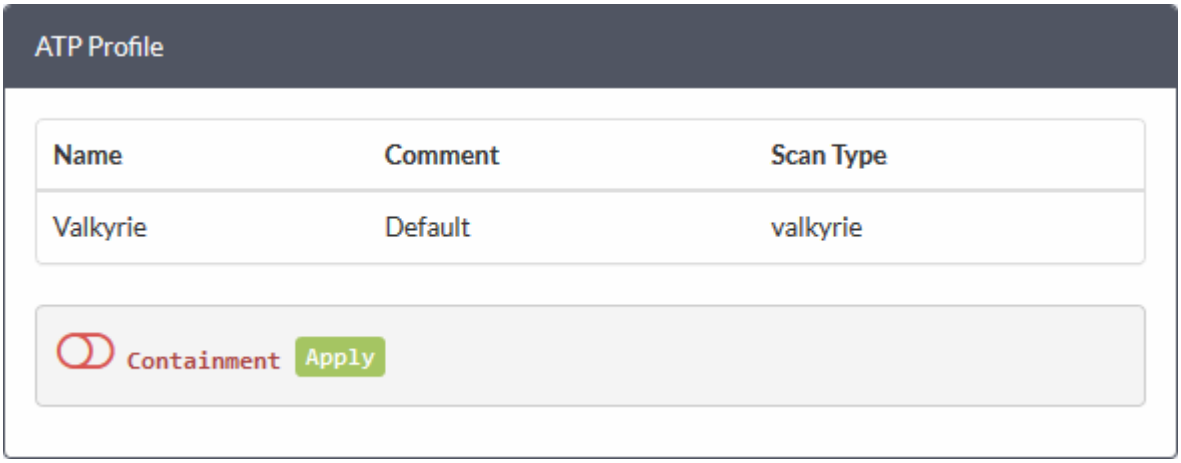
Manage ATP Profile

- Advanced Threat Protection (ATP) safeguards networks against malware, hack attempts, data breaches and more.
- ATP intercepts files downloaded from websites or email attachments and uses a combination of antivirus scans, behavior analysis and blacklist checks to quickly block threats.
- Default ATP Profiles can be created for organizations and individual devices
- The settings you save in the default profile will be applied to all rules in your firewall policy that have 'Advanced Threat Protection' enabled.

To configure an ATP profile for an organization or device

- Click 'Advanced Threat Protection' on the left.
- Select an organization or device from the drop-down above the list (next to the words 'Advanced Threat Protection')

- Select an organization to manage the ATP profile for all devices in the organization
- Select an individual device to manage the ATP profile for that single device



- Containment - Enable or disable automatic containment (sandboxing) of unknown files on endpoints.
- Click 'Apply' to save the profile.

Create URL Filter Profiles

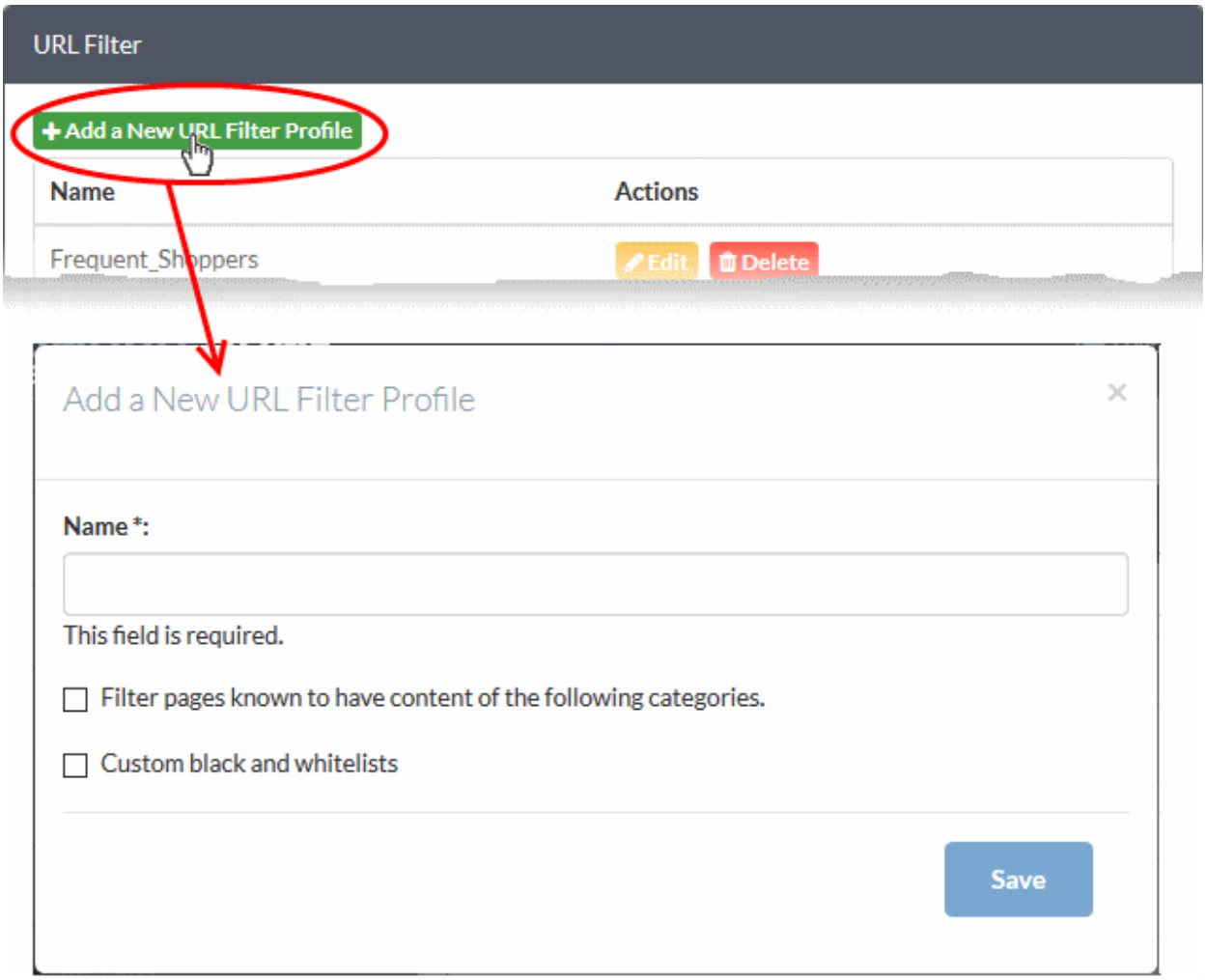
A URL filter profile lets you control which sites can be accessed by users on your network. There are two types of filters:

- Content categories - Web pages with content which falls into a selected category will be automatically blocked
- URL Whitelist/Blacklist – Users can access whitelisted addresses. Blacklisted addresses will be blocked. These lists are often used to create exceptions for sites blocked (or allowed) by content categories.

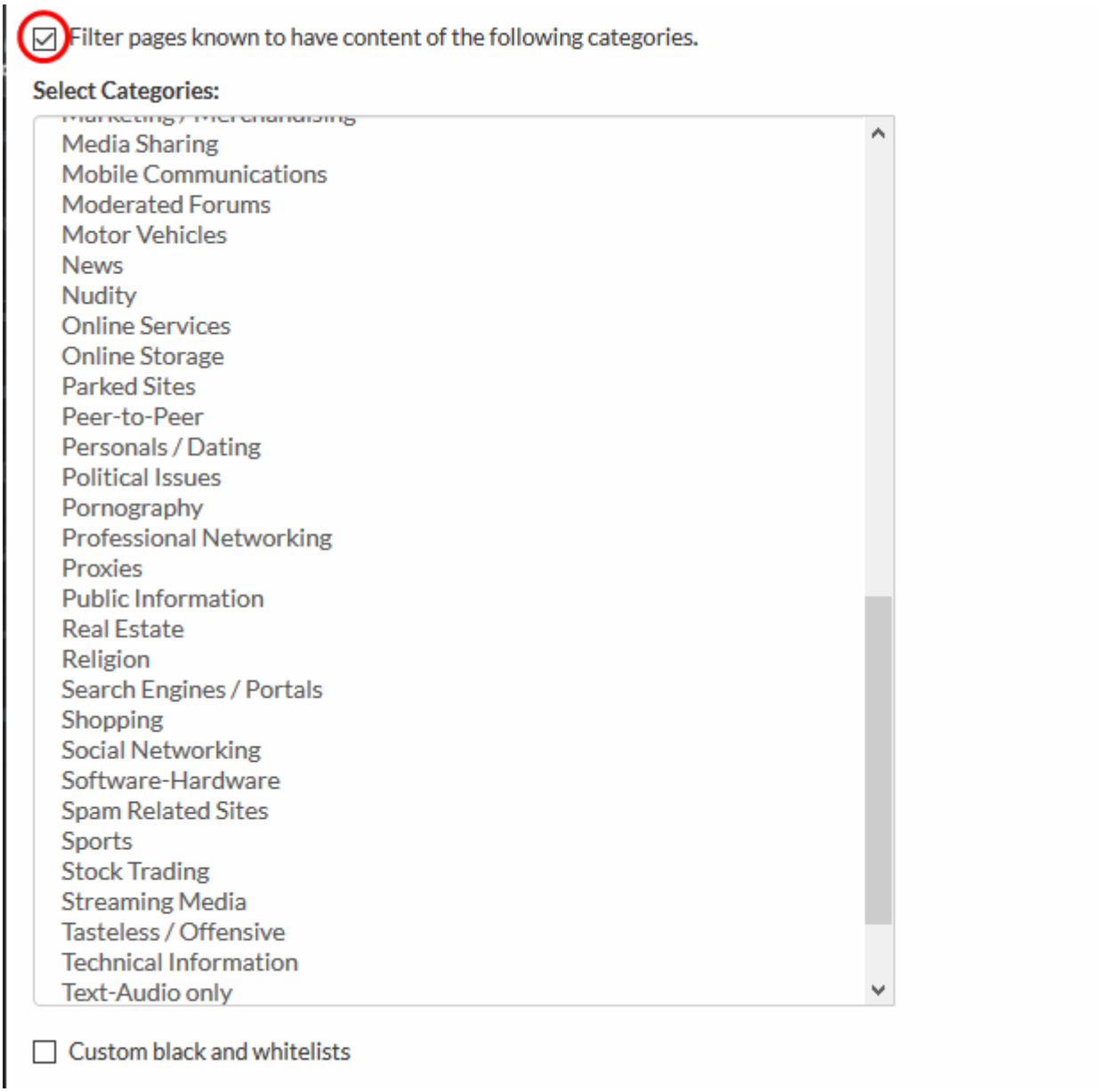
A profile can feature a combination of categories and white/blacklists. Profiles can be added to firewall rules created for an organization or device.

To create a URL filtering profile

- Click 'URL Filter' on the left
- Select an organization or device from the drop-down above the list (next to the words 'URL Filter')
  - Select an organization to add a filter profile for all devices belonging to an organization
  - Select an individual device to add a filter profile for a single device
- Click the 'Add a New URL Filter Profile' button:



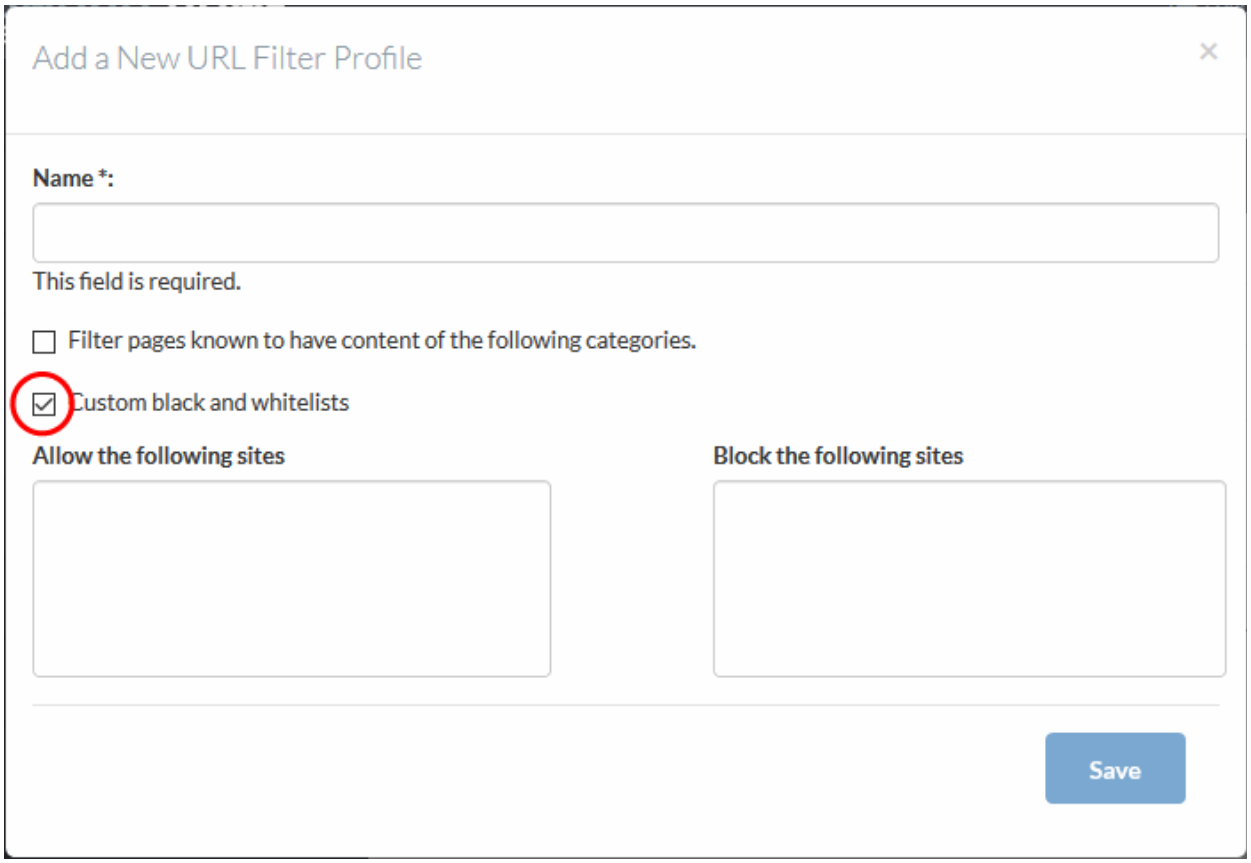
- Create a name for the profile. Ideally this should identify the network to which the profile will apply.
- **Filter pages known to have content of the following categories** - Specify content types which should be blocked by the profile.



- Click on each category you wish to block.

Tip: Hold down the 'CTRL' key while clicking to select multiple items.

- **Custom black and whitelists** - Type the URLs of specific websites you wish to block or allow in the boxes provided:



Note:

- URLs should be of the format 'example.com'. Do NOT include the protocol (http:// or https://) at the start of the address.
- Wildcard characters are allowed. For example, '*.example.com' will also cover all sub-domains of 'example.com'.

- Click 'Save' to add the profile to the list.
- Repeat the process to add more URL filter profiles.

Manage Intrusion Prevention Profile

- Comodo Dome Firewall uses 'Snort', a state-of-the-art network intrusion prevention and detection system (IDS/IPS) directly built-in to its IP tables.
- Snort employs signature, protocol, and anomaly-based inspection of incoming traffic to detect and block intrusion attempts.
- Snort uses IPS 'rulesets'. Each ruleset contains a number of ips and application rules to identify applications that generate traffic on your network.
- Application identification rulesets intercept traffic from web based applications and allow or block data packets from them.
- All rule sets are constantly updated to confront emerging network intrusion techniques.
- The settings you save in the default profile will be applied to all rules in your firewall policy that have the 'default' intrusion prevention profile enabled.

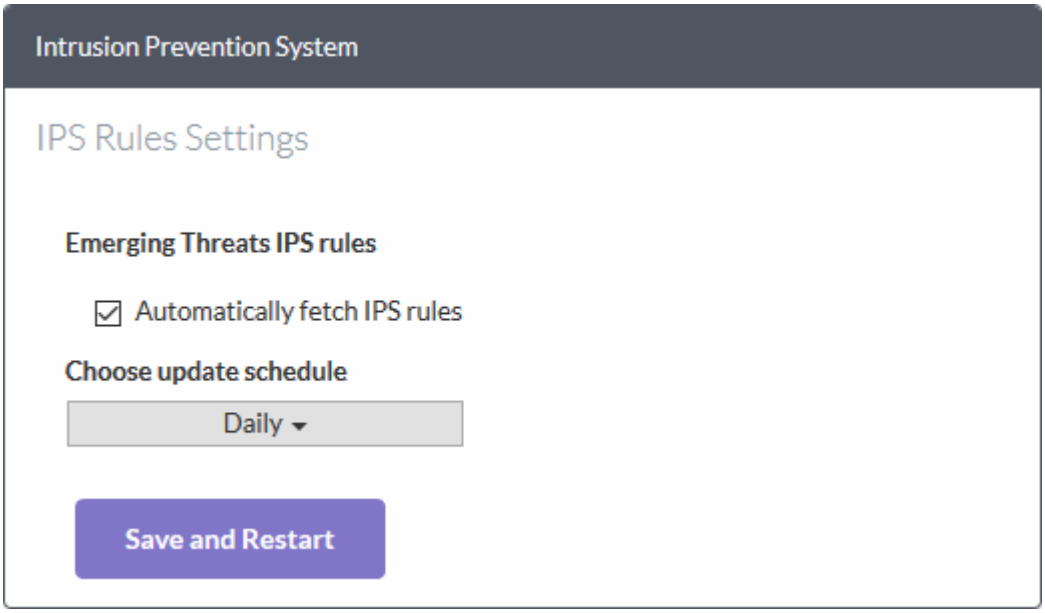
There are three components of an intrusion prevention profile:

- **Rules update schedule**
- **IPS Rulesets**

- **Application Identification Rulesets**

Configure Rules Update Schedule

- Click 'Intrusion Prevention' on the left and choose 'IPS Settings'
- Select an organization or device from the drop-down above the list (next to the words 'Intrusion Prevention')
  - Select an organization to manage the IPS ruleset update schedule for all devices in the organization
  - Select an individual device to manage the IPS ruleset update schedule for that single device.



  - **Automatically fetch IPS rules** - If enabled, Dome Firewall will download and install ruleset updates at the schedule you choose.
  - Choose update schedule - Select the interval for automatic updates. The available options are:
    - Hourly
    - Daily (***Default***)
    - Weekly
    - Monthly
- Click 'Save and Restart'

Your settings will be saved. The devices in which the profile is already in effect will be restarted for the changes to take effect.

Configure IPS Rulesets

You can enable/disable IPS rulesets and configure them to allow or block data packets as required.

To configure IPS Rulesets

- Click 'Intrusion Prevention' on the left and choose 'IPS Rules'
- Select an organization or device from the drop-down above the list (next to the words 'Intrusion Prevention')
  - Select an organization to manage the IPS rulesets for all devices in the organization
  - Select an individual device to manage the IPS rulesets for that single device.

Enable/Disable rulesets

Rulesets can be enabled or disabled individually or collectively:

- Enable a single ruleset - Click the icon in the 'Actions' column
- Disable a single ruleset - Click the icon in the 'Actions' column
- Multiple rulesets - Select rulesets using the check-boxes on the left. Click the 'Enable' or 'Disable' button as required.
- Any changes will be saved to the default profile and immediately applied to devices on which the profile is active.

Rule actions

Rule actions are the responses you want the firewall to take if the conditions of a rule are met. There are two options:

- Alert – Will allow the packet to pass and will generate an alert. An alert policy is indicated by a yellow triangle in the 'Actions' column -
- Drop – Will block the data packet without generating an alert. A drop policy is indicated by a shield icon in the 'Actions' column -
- Any changes will be saved to the default profile and immediately applied to devices on which the profile is active.

Configure Application Identification Rulesets

- Application identification rules intercept traffic from web apps and allow or block packets according to your preference.

To configure Application Identification Rulesets

- Click 'Intrusion Prevention' >'Application Identification'
- Select an organization or device from the drop-down above the list (next to the words 'Intrusion Prevention')
    - Select an organization to manage the application identification rulesets for all devices in the organization
    - Select an individual device to manage the application identification rulesets for that single device.

Enable/Disable rulesets

Rulesets can be enabled or disabled individually or collectively:

- Enable a single ruleset - Click the icon in the 'Actions' column
- Disable a single ruleset - Click the icon in the 'Actions' column
- Multiple rulesets - Select rulesets using the check-boxes on the left. Click the 'Enable' or 'Disable' button as required.
- Any changes will be saved to the default profile and immediately applied to devices on which the profile is active.

Rule actions

Rule actions are the responses you want the firewall to take if the conditions of a rule are met. There are two options:

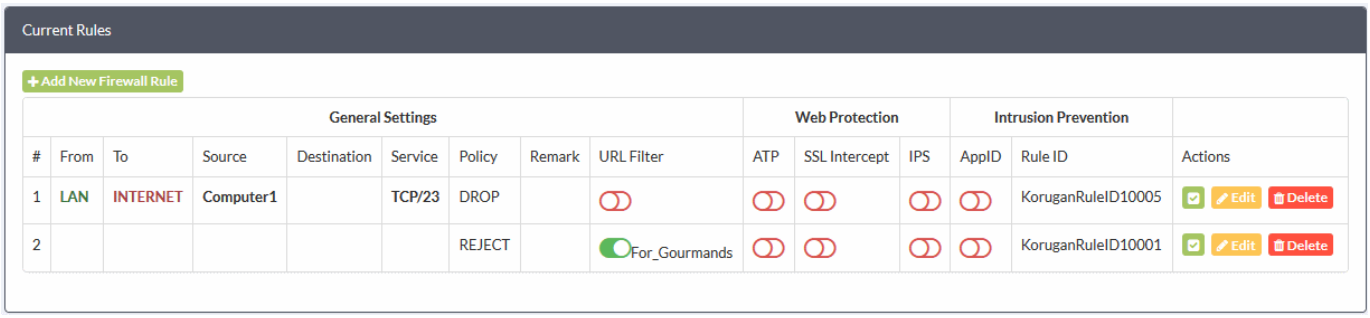
- Alert – Will allow the packet to pass and will generate an alert. An alert policy is indicated by a yellow triangle in the 'Actions' column -
- Drop – Will block the data packet without generating an alert. A drop policy is indicated by a shield icon in the 'Actions' column -
- Any changes will be saved to the default profile and immediately applied to devices on which the profile is active.

Configure Firewall Policy

Each organization or device should have a firewall policy applied to it. A policy consists of a series of firewall rules that are imposed on different types of traffic.

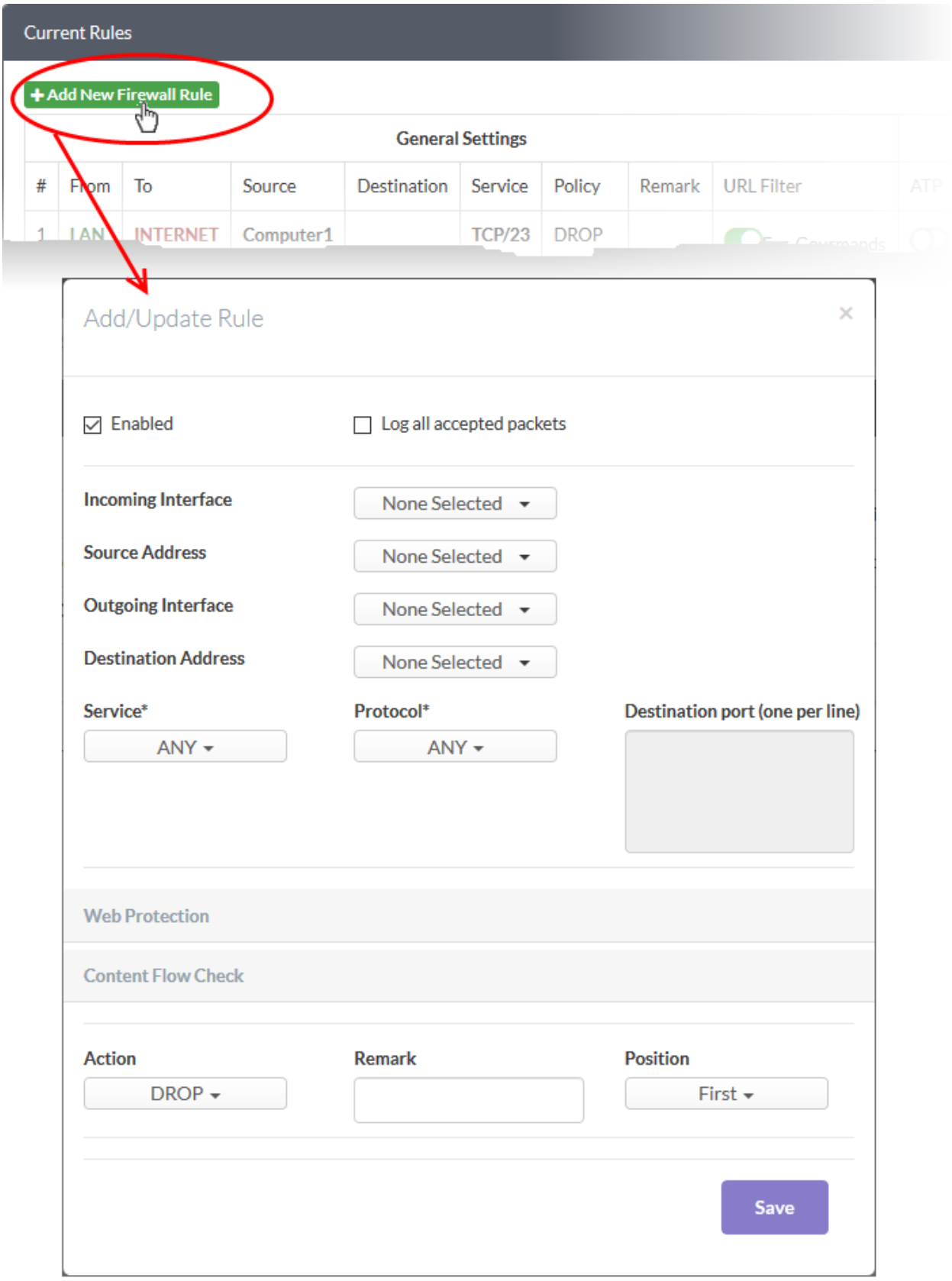
- Click 'Firewall' on the left and choose 'Firewall Policy'
- Select an organization or device from the drop-down in the title bar (next to the word 'Firewall')
  - Select an organization to manage the firewall policy/rules for all devices belonging to the organization
  - Select an individual device to manage the firewall policy/rules for a specific device

The 'Current Rules' pane shows all rules in the policy. You can edit these rules and create/remove rules.



To add a rule to a policy

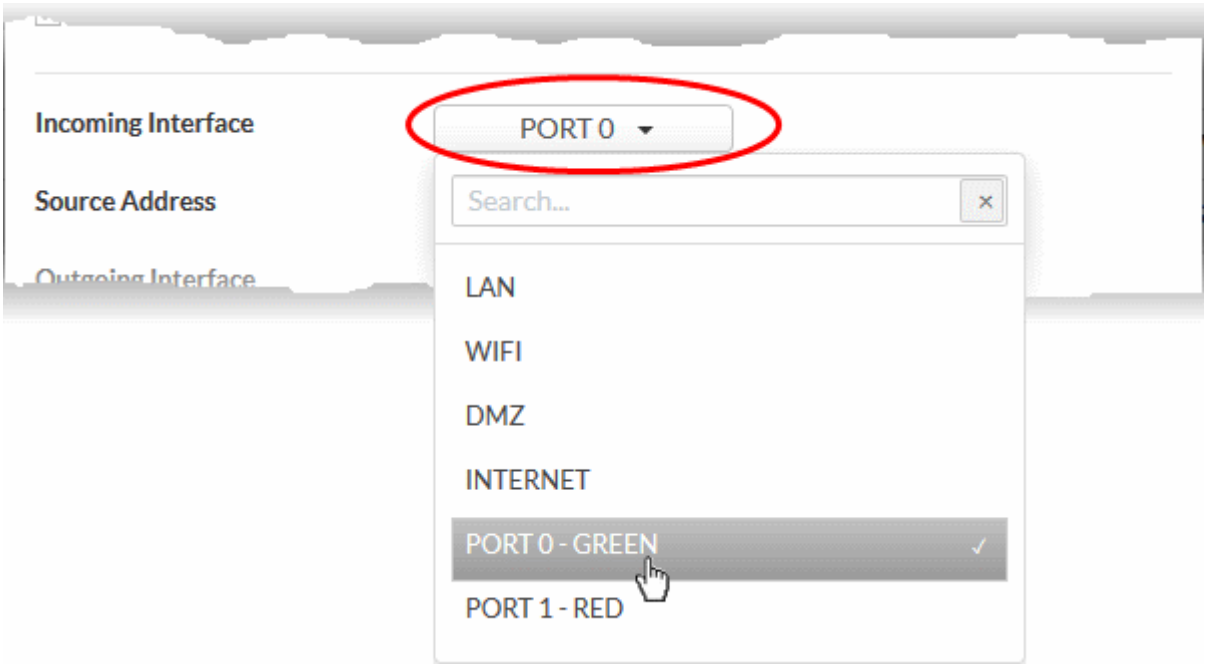
- Click 'Add New Firewall Rule' at the top-left of the 'Current Rules' interface



General Settings:

- **Enabled** - Enable or disable the firewall rule.
- **Log all accepted packets** - Enable to create a record of all packets allowed by the rule. You can view the logs from the respective firewall admin console. See **https://help.comodo.com/topic-436-1-912-11997-Viewing-Logs.html** for more details.

- **Incoming Interface** - Choose the interface through which traffic is received. The drop-down shows the common and custom interfaces created for the selected organization or device.

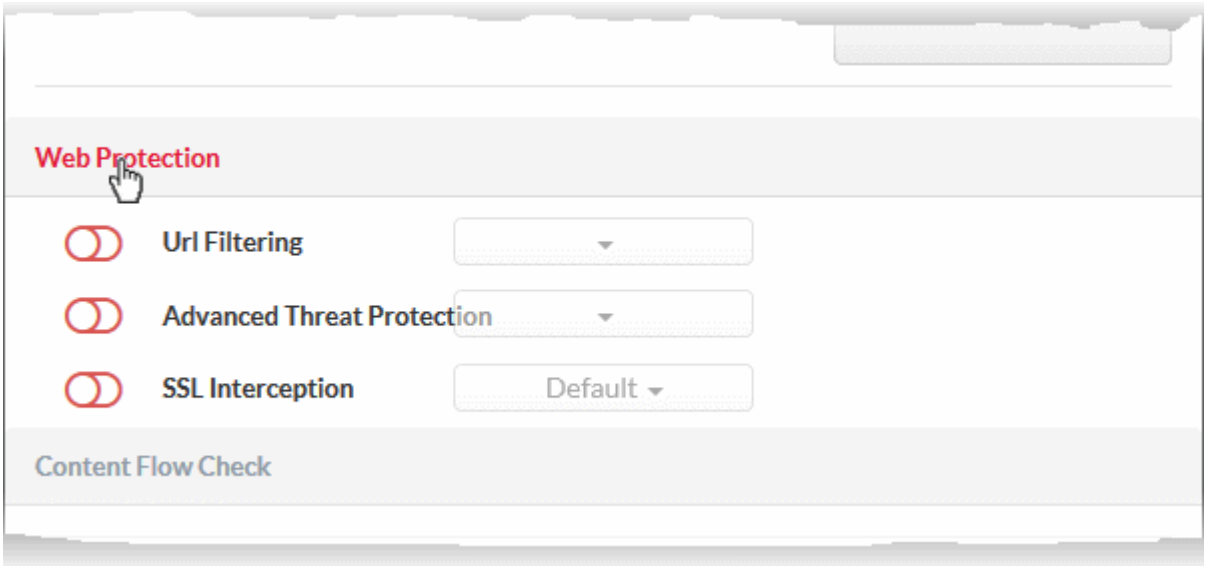


  - You can select more than one interface for the rule
  - Use the 'Search' box to search for a specific interface

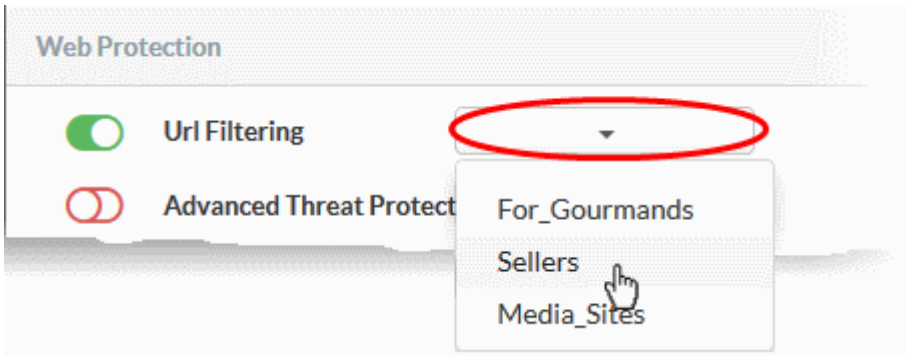
- **Source Address** - Choose the firewall address object or group from which traffic originates. Please note that only the firewall address objects and object groups created for the selected organization/device will be available in the drop-down. See **Create Firewall Address Objects** for guidance on creating firewall address objects.
- **Outgoing Interface** - Choose the interface through which the traffic is sent. The drop-down shows the common interfaces and the custom interfaces created for the selected organization or the device.
- **Destination Address** - Choose the firewall address object or group to which traffic is sent. Please note that only the firewall address objects and object groups created for the selected organization/device will be available in the drop-down.
- **Service** - Choose the type of service hosted by the source from the drop-down
- **Protocol** - Choose the protocol used by the service
- **Destination port** - Specify the destination port number(s) used by the service, one by one.

Web Protection Settings

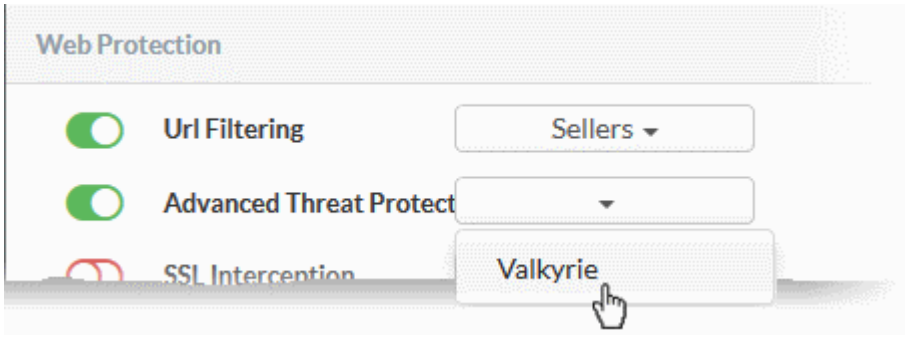
- Click 'Web Protection' to open the security features for web protection:



- **URL Filtering** - Enable or disable URL filtering profiles on traffic intercepted by the rule.
  - Move the switch to ON to enable URL filtering
  - Select the profile which specifies the sites you wish to block or allow from the drop-down:



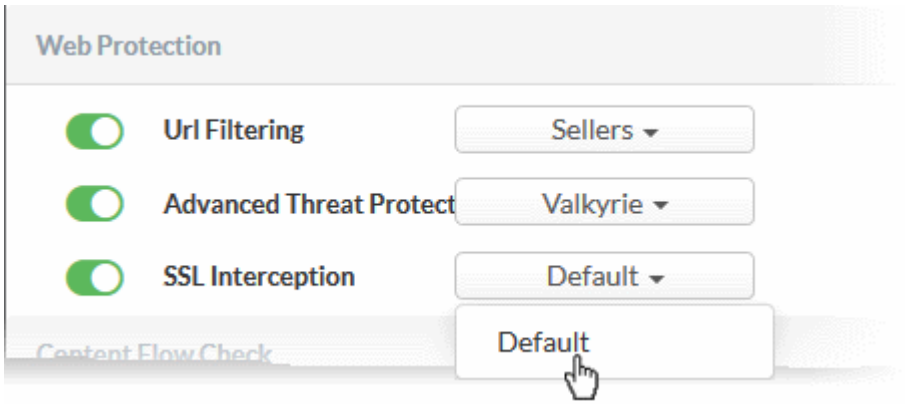
  - URL filtering profiles can be created for organizations/device in the 'URL Filter' interface (click 'URL filter' on the left). See **Create URL Filter Profiles** for more details.
  - Profiles defined for an organization can only be applied to devices which belong to the organization. If you apply it to the organization itself, the profile will apply to every device in the organization.
  - Profiles defined for an individual device will be available only for that device.
- **Advanced Threat Protection** - Enable or disable advanced threat protection (ATP) settings on traffic intercepted by the rule. You can choose the ATP profile you want to apply from the drop-down menu.
  - Move the switch to ON to enable ATP.
  - Select the ATP profile from the drop-down.



  - The default ATP profile can be managed for the organization/device from the 'Advanced

Threat Protection' interface. See **Manage ATP Profile** for guidance on this.

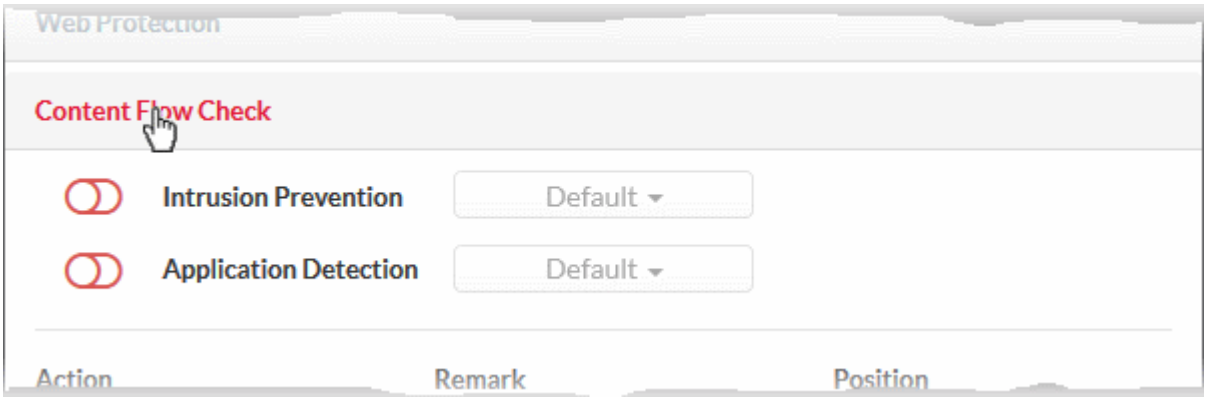
- **SSL Interception** - Enable or disable analysis of encrypted traffic which is intercepted by the rule.
  - Move the switch to ON to enable SSL interception.
  - Select the default profile from the drop-down.



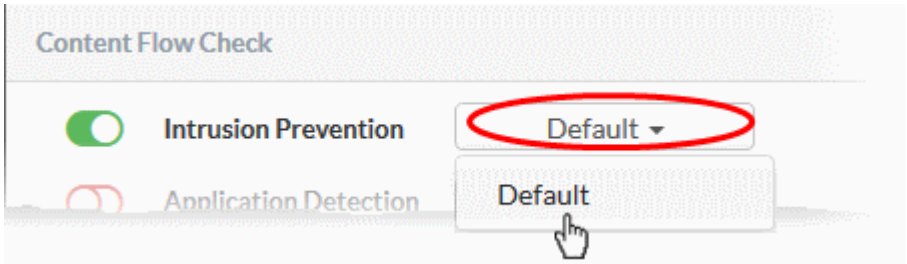
Selecting 'Default' will apply the HTTPS exception settings as configured on the firewall device itself. See **https://help.comodo.com/topic-436-1-912-12058-HTTPS-Proxy.html** for help with this.

Content Flow Check Settings:

- Click 'Content Flow Check' to configure these settings:



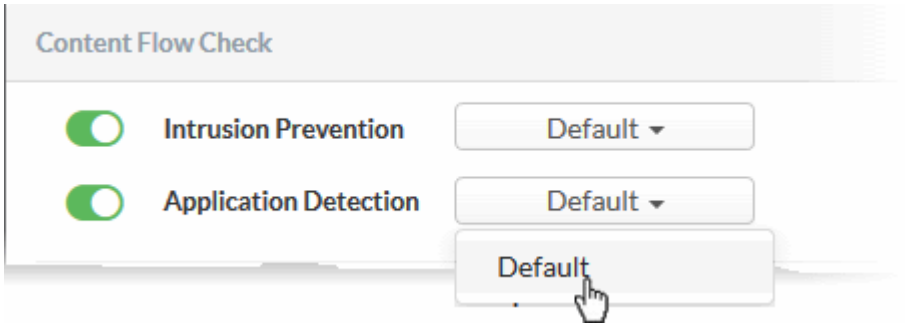
- **Intrusion Prevention** - Enable/disable Snort intrusion detection technology on traffic intercepted by the rule. See '**Intrusion Prevention**' for more details.
  - Move the switch to ON to enable intrusion prevention.
  - Select the default profile from the drop-down.



Selecting 'Default' will apply the rule settings configured in the 'Intrusion Prevention' default profile. See '**Manage Intrusion Prevention Profile**' for more details.

- **Application Detection** - Enable or disable application identification rules on traffic intercepted by the rule. Application ID rules allow you to track the activities of applications on your network, allowing you to attribute IPS events to applications.

- Move the switch to ON to enable application detection.
- Select the default profile from the drop-down.



Selecting 'Default' will apply the settings configured for the organization/device in the 'Intrusion Prevention > 'Application Identification' interface. See '**Configure Application Identification Rulesets**' for more details.

Actions

- **Action** - Specify whether packets matching the rule should be allowed or denied. The available options are:
  - Accept - The data packets will be allowed without filtering
  - Drop - The packets will be denied.
  - Reject - The packets will be rejected, and error packets will be sent in response
- **Remark** - Enter a short description of the rule. The description will appear in the 'Remark' column of the 'Rules' table.
- **Position** - Set the priority of the rule in the list of rules. The rules will be applied on the inbound and outbound traffic in the order they appear on the list.
- Click 'Save' to add the rule to central manager.

The rule will be applied to all target devices. You can view the view the application status and re-apply the rule if required from the 'Dashboard' > 'Tasks' interface. See the online help page at **https://help.comodo.com/topic-436-1-920-12377-View-Management-Tasks.html** for guidance on this.

- Repeat the process to add more firewall rules to the policy

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