COMODO
Creating Trust Online®

COMODO DOME
FIREWALL CENTRAL MANAGER

Comodo **Dome Firewall Central Manager**

Software Version 1.5

Administrator Guide

Guide Version 1.5.071619

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

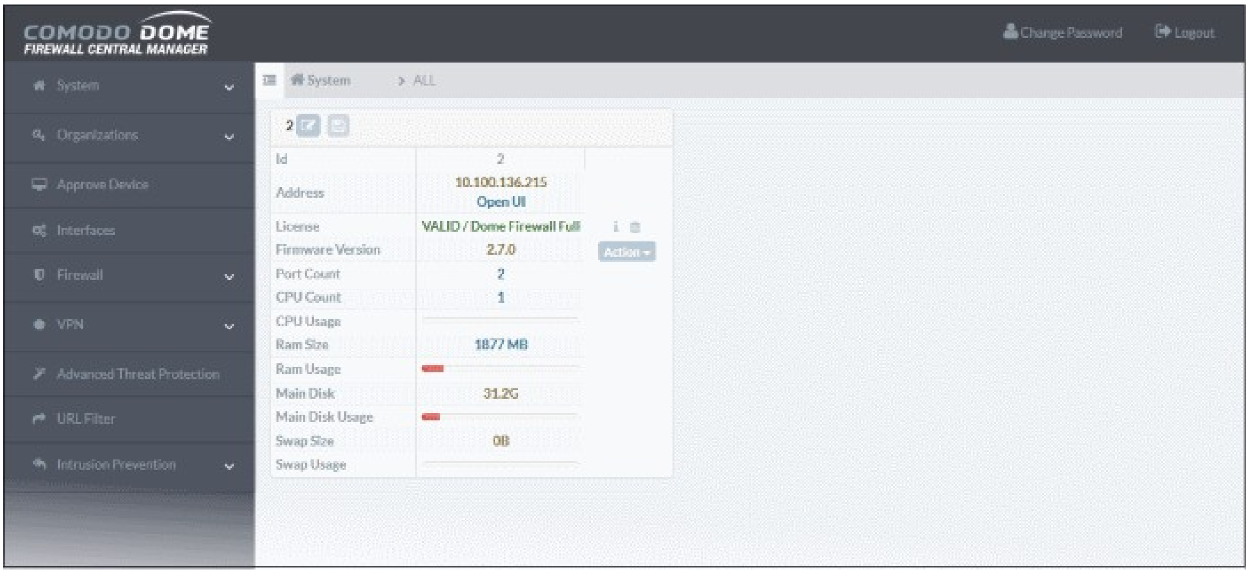
1 Introduction to Dome Firewall Central Manager

Comodo Dome Firewall Central Manager allows network admins to remotely manage multiple firewall devices from a single, centralized console.

- Import firewall devices belonging to different organizations for collective management.
- Connects to firewall devices even if they are behind Network Address Translation (NAT).
- Configure network zone interfaces, port connections, firewall rules, SNAT/DNAT rules and more for managed devices.
- Rules and profiles can be applied to individual devices or to all devices belonging to an organization.

The central manager is available in two modes:

- Virtual Appliance - Install firewall central manager as a VM on your network
- Cloud Mode - The solution will be hosted on Comodo servers



Id	2
Address	10.100.136.215 Open UI
License	VALID / Dome Firewall Full
Firmware Version	2.7.0
Port Count	2
CPU Count	1
CPU Usage	
Ram Size	1877 MB
Ram Usage	
Main Disk	31.2G
Main Disk Usage	
Swap Size	0B
Swap Usage	

Guide Structure

This guide will take you through the configuration and use of Comodo Dome Firewall Central Manager.

1.1 Sign-up for Firewall Central Manager License

The trial license is free and covers unlimited users for one year. The license can be upgraded at anytime for continued usage.

There are two ways you can sign up for Firewall Central Manager:

- **Get Central Manager as a standalone application**
    - Login to your Comodo account at **https://accounts.comodo.com/login**. Register for free if you don't yet have an account
    - Click 'My Account' > 'Sign up to Comodo Dome'.
    - Select 'Dome Firewall Central Manager (Free)' in the product drop-down.

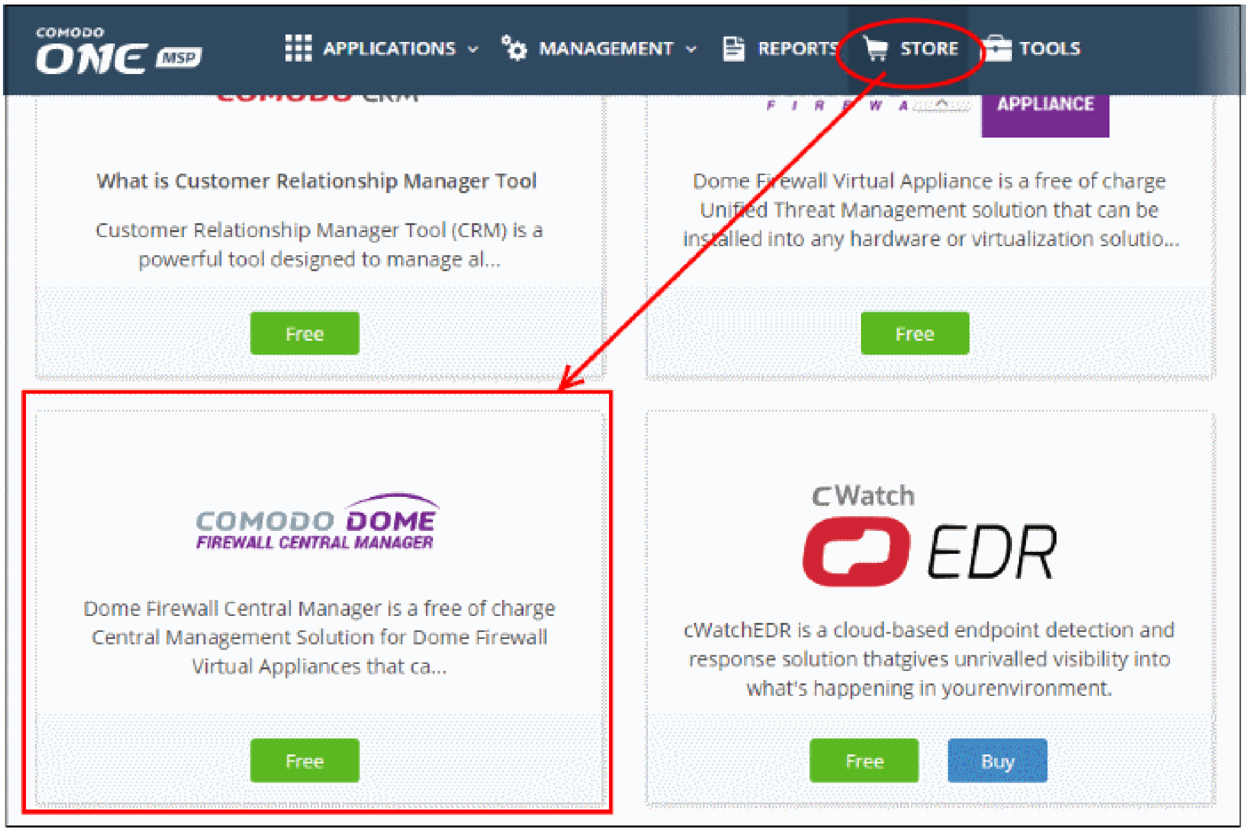
    - Complete the application form. You will receive your license key via email.
- **Comodo One / Comodo Dragon / ITarian customers**
    - Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
    - Click 'Store' then go to the firewall central manager tile.
    - Click the 'Free' button to begin setup.
    - After adding to your portal account, you can open it by clicking 'Applications' > 'Dome Firewall Central Manager'. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

Dome Firewall Central Manager Stand-alone Customers

- Visit **https://accounts.comodo.com/login**
- Login if you have an account or create new Comodo account
- Click 'Sign Up to Comodo Dome Service'
- Select 'Dome Firewall Central Manager' in the 'Comodo Sign-up Page' section
- In the 'Customer Information' section, select whether you are an existing Comodo customer or not and complete the form.
- Read the EULA fully, select 'I accept the Terms and Conditions' check box and click 'Continue'
- The product purchase confirmation page will be shown.
- You will receive an order acknowledgment mail which also contains subscription ID and license key.
- Next, see **Setup Dome Firewall Central Manager**' to download the setup file and install it.

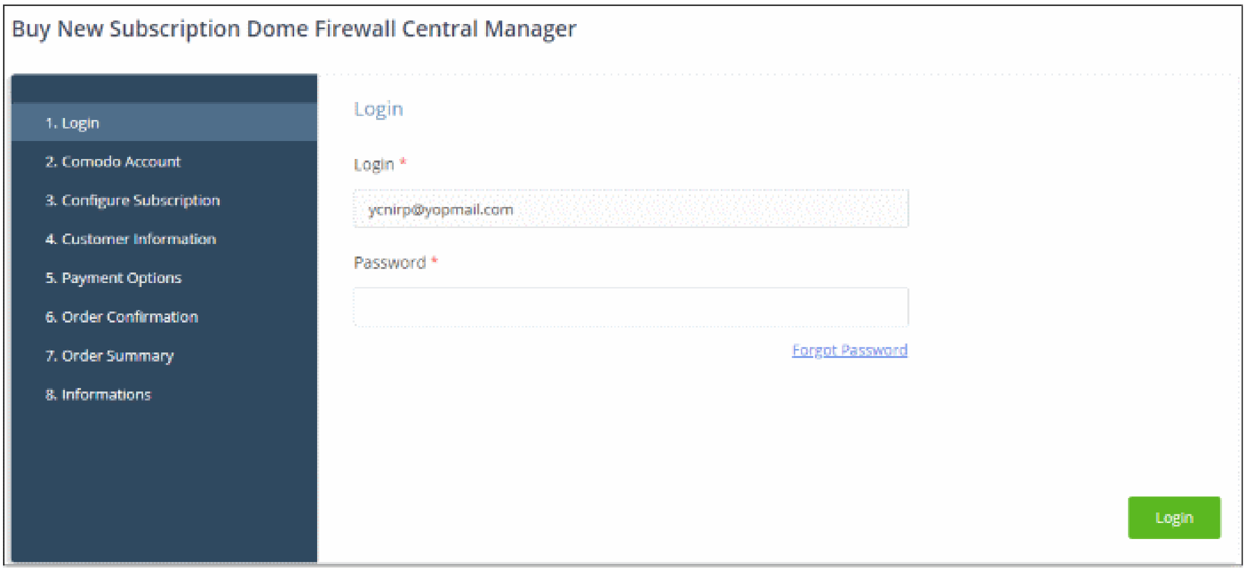
Comodo One / Comodo Dragon / ITarian MSP and Enterprise Customers

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account.
    - The process of adding is same for Comodo One, Comodo Dragon and ITarian platforms. The following tutorial explains how to add Firewall Central Manager to Comodo One platform.
- Click the 'Store' link on the top-navigation


COMODO ONE MSP
APPLICATIONS
MANAGEMENT
REPORTS
STORE
TOOLS
What is Customer Relationship Manager Tool
Customer Relationship Manager Tool (CRM) is a powerful tool designed to manage al...
Free
APPLIANCE
Dome Firewall Virtual Appliance is a free of charge Unified Threat Management solution that can be installed into any hardware or virtualization solutio...
Free
COMODO DOME
FIREWALL CENTRAL MANAGER
Dome Firewall Central Manager is a free of charge Central Management Solution for Dome Firewall Virtual Appliances that ca...
Free
CWatch EDR
cWatchEDR is a cloud-based endpoint detection and response solution thatgives unrivalled visibility into what's happening in yourenvironment.
Free
Buy

- Locate the 'Dome Firewall Central Manager' tile and click the 'Free' button.

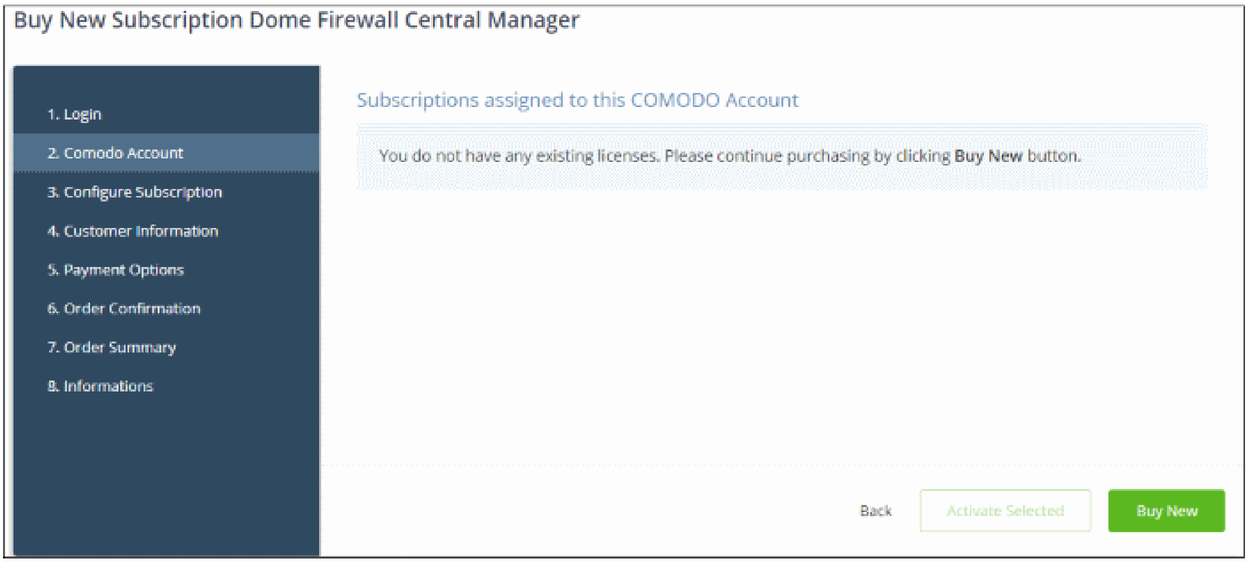
You will be taken to the product subscription page:



Buy New Subscription Dome Firewall Central Manager

Your login username will be pre-populated and cannot be changed.

- Enter your Comodo One account password and click 'Login'.
- The next step allows you purchase a new license or activate an existing license:

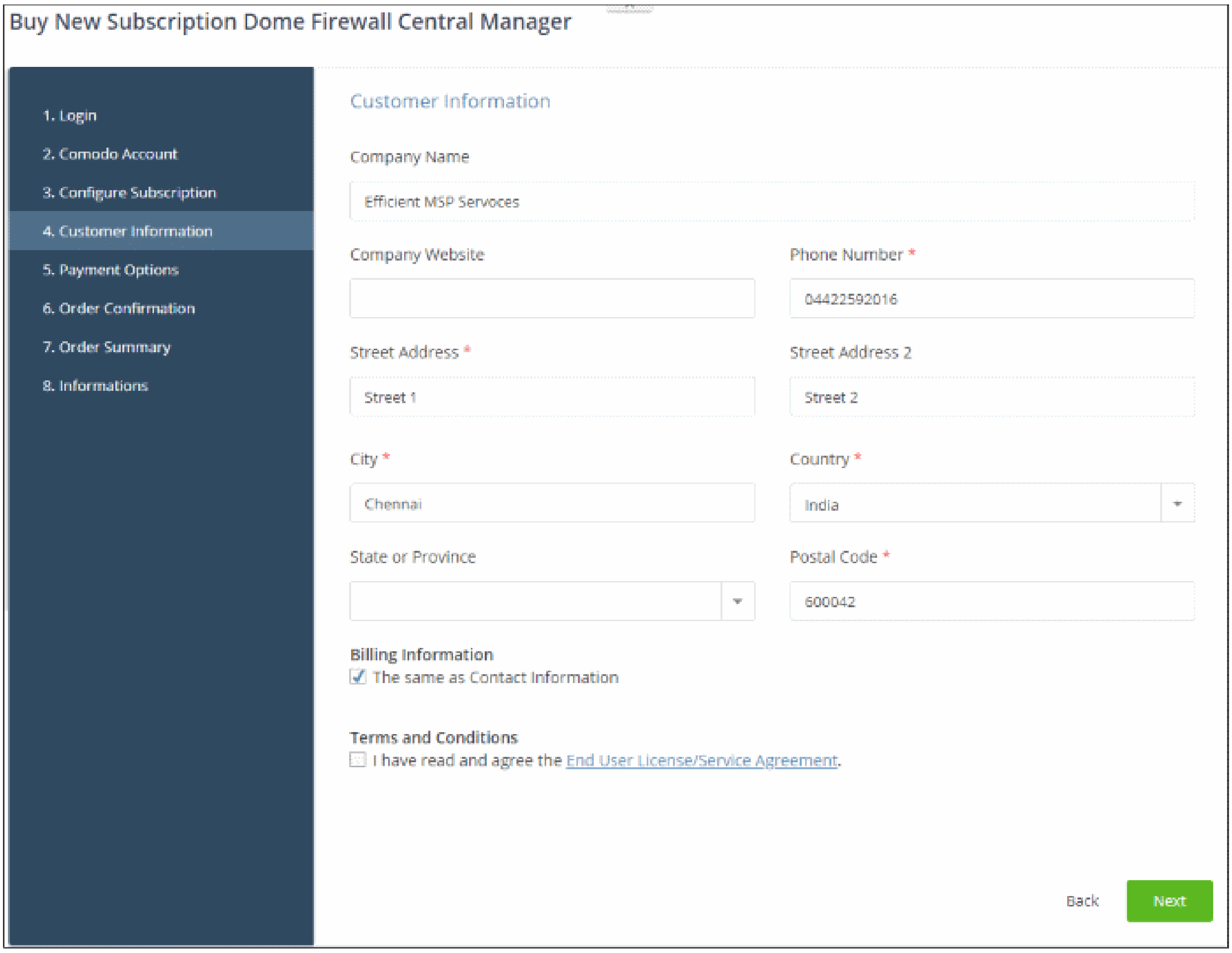


Buy New Subscription Dome Firewall Central Manager

Subscriptions assigned to this COMODO Account

You do not have any existing licenses. Please continue purchasing by clicking **Buy New** button.

- Click 'Buy Now' to purchase a new license



Buy New Subscription Dome Firewall Central Manager

Customer Information

Company Name: Efficient MSP Servoces

Company Website:

Phone Number *: 04422592016

Street Address *: Street 1

Street Address 2: Street 2

City *: Chennai

Country *: India

State or Province:

Postal Code *: 600042

Billing Information

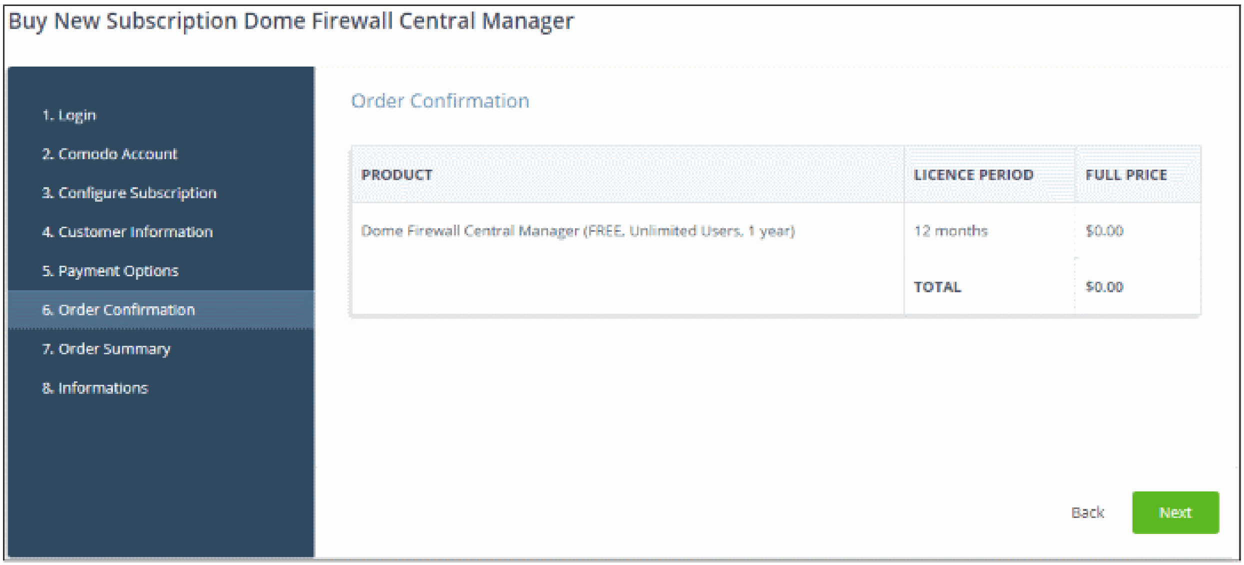
☑ The same as Contact Information

Terms and Conditions

☐ I have read and agree the End User License/Service Agreement.

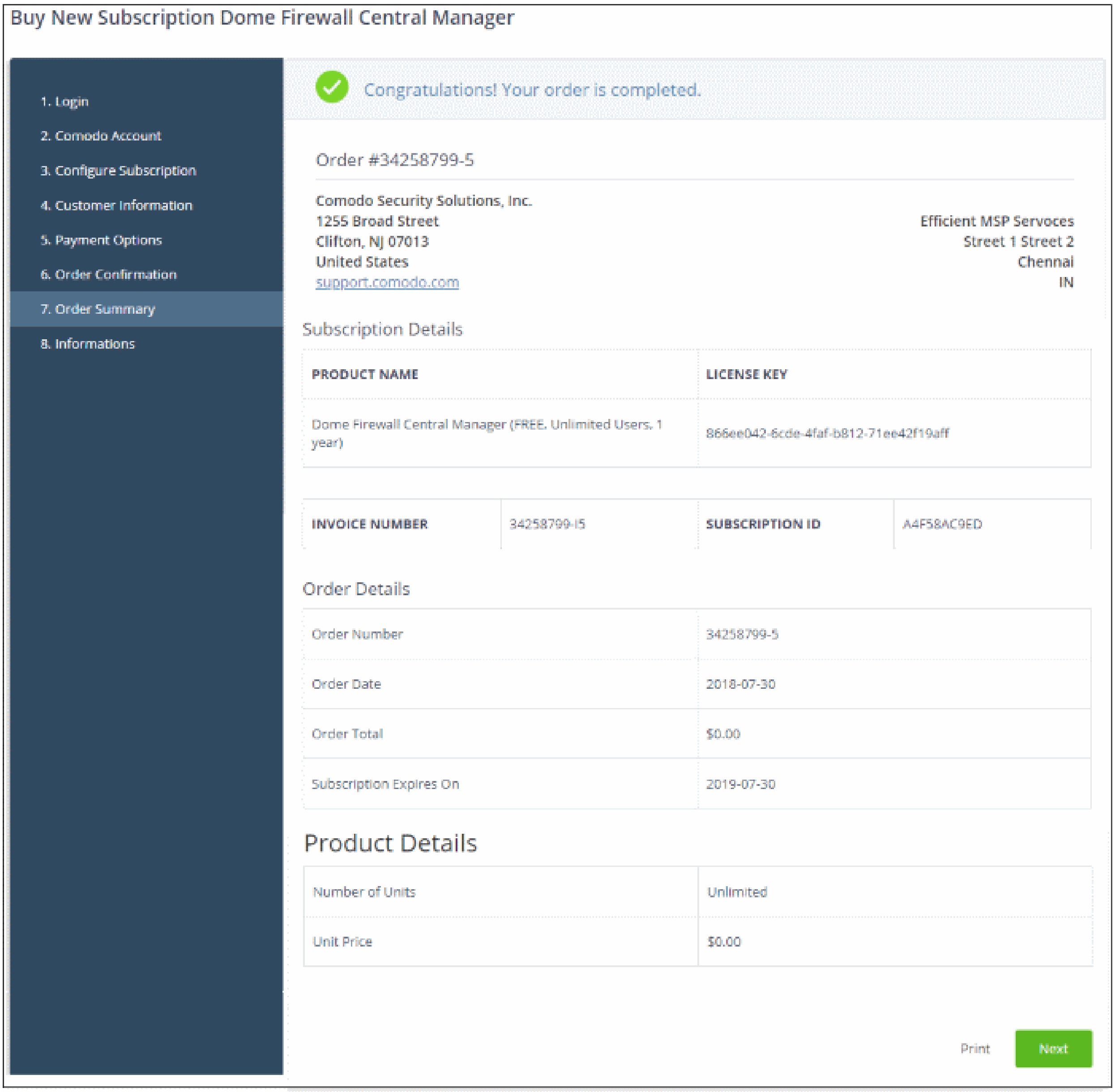
- Enter your company name, website and address details in the 'Customer Information' section. Read the EULA fully, agree to the terms & conditions and click 'Next':

Next, review your order details and click 'Next to confirm:



PRODUCT	LICENCE PERIOD	FULL PRICE
Dome Firewall Central Manager (FREE, Unlimited Users, 1 year)	12 months	$0.00
	TOTAL	$0.00

- You will see a order confirmation screen after your order has been successfully processed:



Buy New Subscription Dome Firewall Central Manager

✓ Congratulations! Your order is completed.

Order #34258799-5

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
support.comodo.com

Efficient MSP Servoces
Street 1 Street 2
Chennai
IN

Subscription Details

PRODUCT NAME	LICENSE KEY
Dome Firewall Central Manager (FREE, Unlimited Users, 1 year)	866ee042-6cde-4faf-b812-71ee42f19aff

INVOICE NUMBER	34258799-I5	SUBSCRIPTION ID	A4F58AC9ED

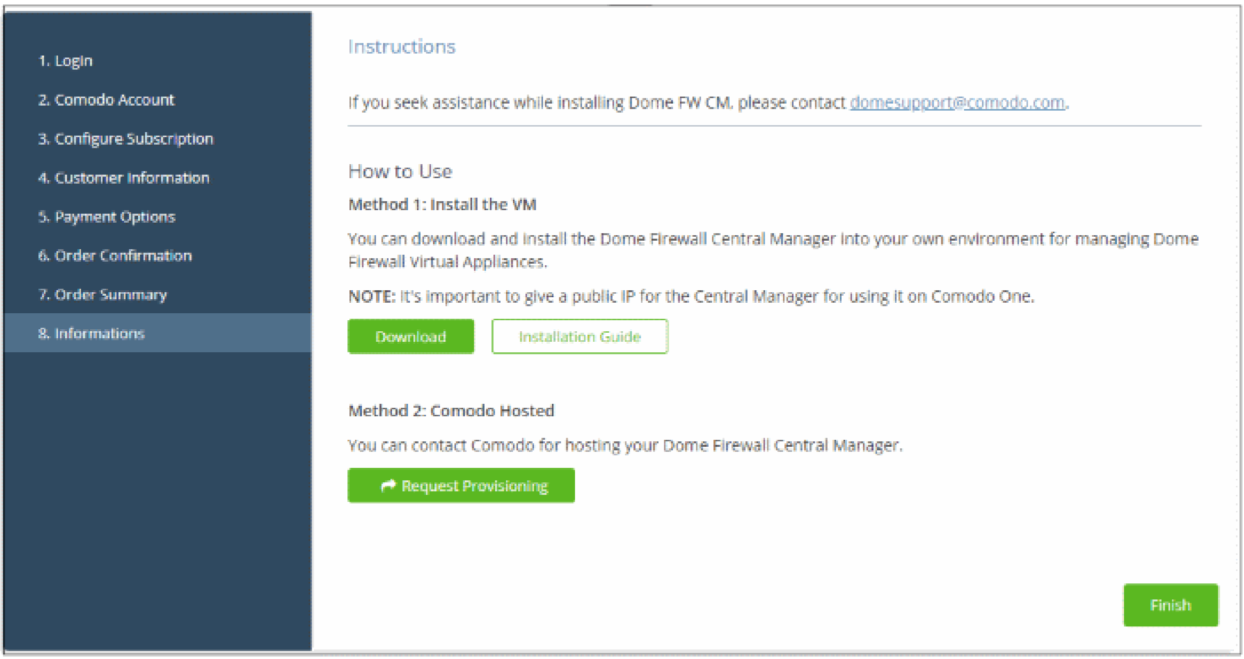
Order Details

Order Number	34258799-5
Order Date	2018-07-30
Order Total	$0.00
Subscription Expires On	2019-07-30

Product Details

Number of Units	Unlimited
Unit Price	$0.00

- Click 'Next' to move onto the instructions page. This provides help to setup Comodo Dome Firewall Central Manager on your network.



Instructions

If you seek assistance while installing Dome FW CM, please contact domesupport@comodo.com.

How to Use

Method 1: Install the VM

You can download and install the Dome Firewall Central Manager into your own environment for managing Dome Firewall Virtual Appliances.

NOTE: It's important to give a public IP for the Central Manager for using it on Comodo One.

Method 2: Comodo Hosted

You can contact Comodo for hosting your Dome Firewall Central Manager.

- There are two ways that you can setup Dome Firewall Central Manager:
  - **On premises** – Download the .ova setup file and install as explained in the **next section**. After installing CM in your environment, you can integrate it with your portal platform if required. **Click here** for help to integrate CM with C1 / Comodo Dragon (CD) / ITarian.
  - **Hosted** – Comodo will host Central Manager for you. Click 'Request Provisioning'. You will receive an email from Comodo containing the URL of your instance. This hosted service URL has to be configured in 'C1 / CD / ITarian' > 'Management' > 'Applications' > 'Dome Firewall Central Manager' and entered in the 'Settings' tab. **Click here** for more details.
- Click 'Finish' to return to the C1 Dashboard.
- Your license will be activated. You will also receive a confirmation email for your order.

1.2 Setup Dome Firewall Central Manager

There are two ways to set up Comodo Dome Firewall Central Manager:

- **Virtual Appliance**
- **Cloud Mode**

Virtual Appliance

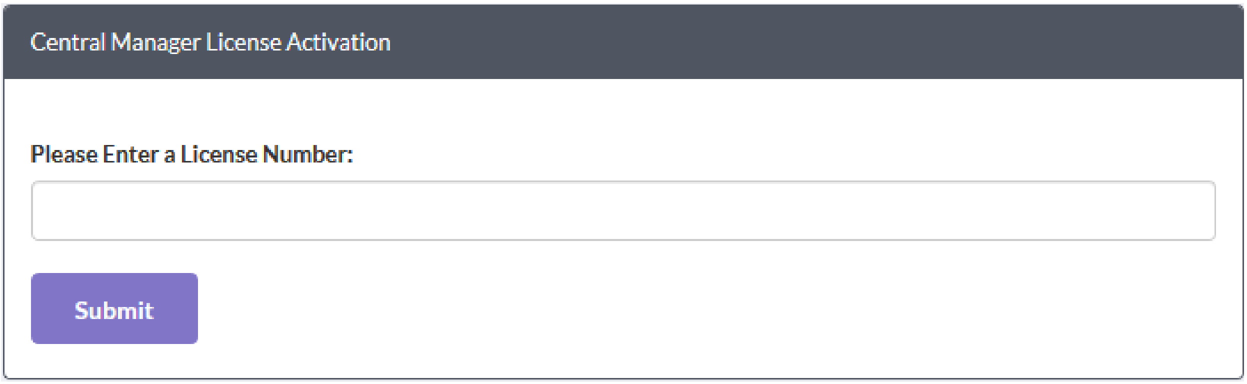
- The virtual appliance setup file is available in two formats:
  - **.OVA File**
  - **.ISO File**

Installation from OVA File

- Download the .ova file for Comodo Dome Firewall Central Manager from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewallcm.ova** or from the final instructions dialog while **adding CM to your C1 / Comodo Dragon / ITarian account**.
- Import the virtual appliance into VMs such as Virtualbox and 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 these credentials

after first login.

- You will be asked to enter a license key after first login:



Central Manager License Activation

Please Enter a License Number:

- Enter your license key and click 'Submit'.

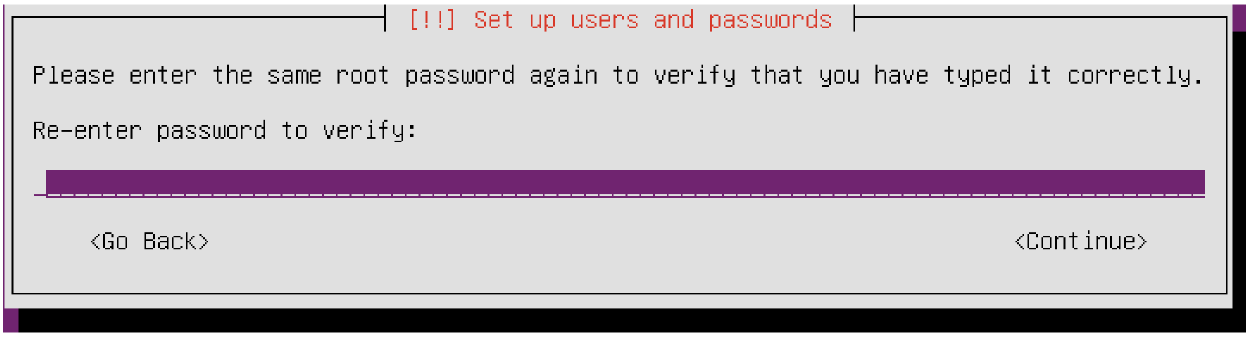
Tip: Comodo One / Comodo Dragon / ITarian customers can integrate the central manager appliance with their portal accounts. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

-

Installation from ISO File

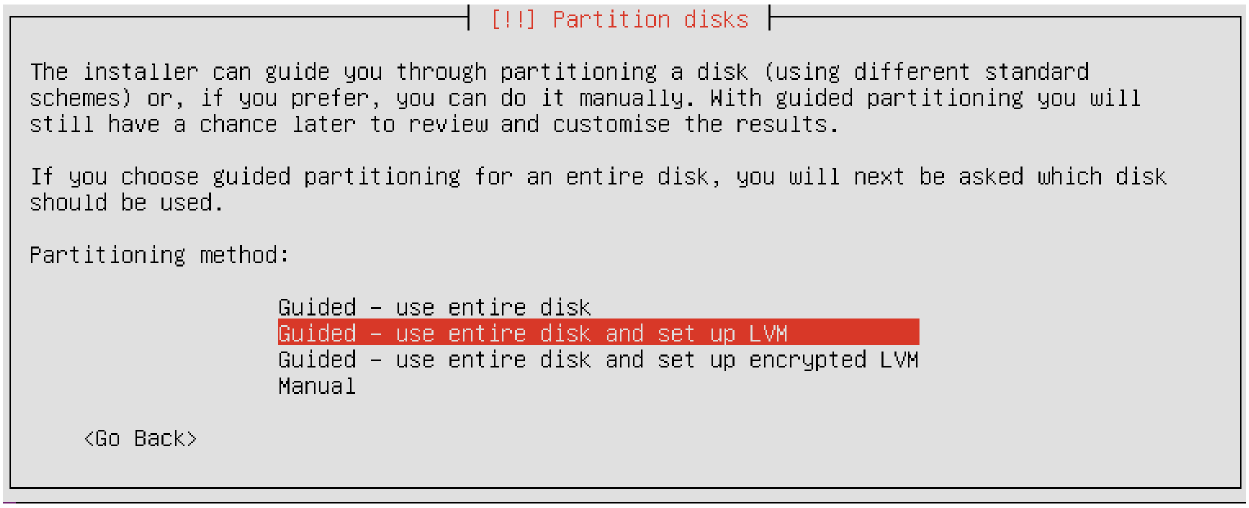
Central manager is available as an .iso which can be copied to usb and installed on bare-metal appliances.

- Download the .iso file from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewallcm.iso**.
- Create a Ubuntu virtual machine and start installation of the virtual appliance from the .iso file
  - Follow the installation wizard, select your installation language, country and keyboard layout



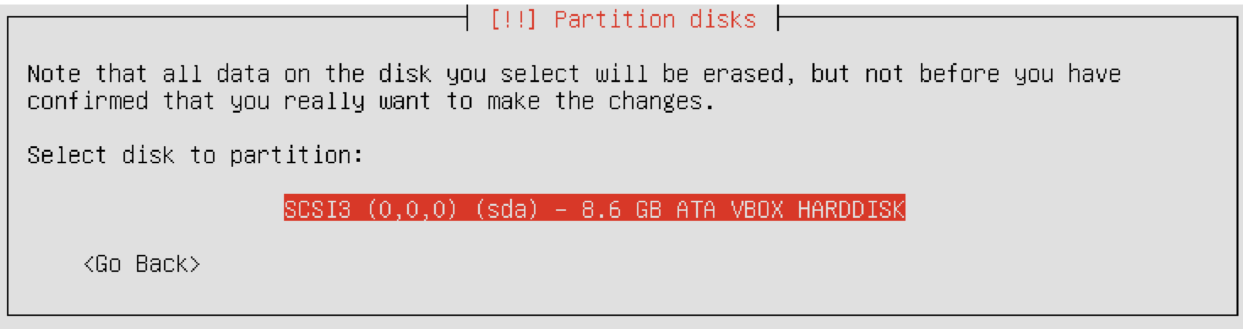
```
[!!] Set up users and passwords

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:
```

  - Enter the root password as 'comodo' (without quotes) when asked and continue.
  - Choose 'Guided - use entire disk and setup LVM' in the partition step



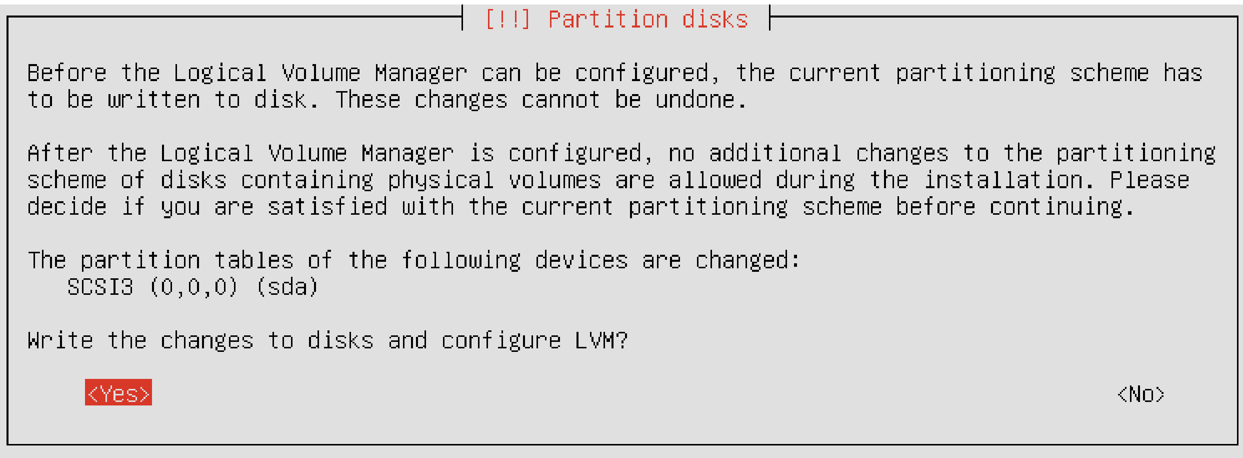
```
[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:

                    Guided - use entire disk
                    Guided - use entire disk and set up LVM
                    Guided - use entire disk and set up encrypted LVM
                    Manual

    <Go Back>
```

- Select the disk to be partitioned



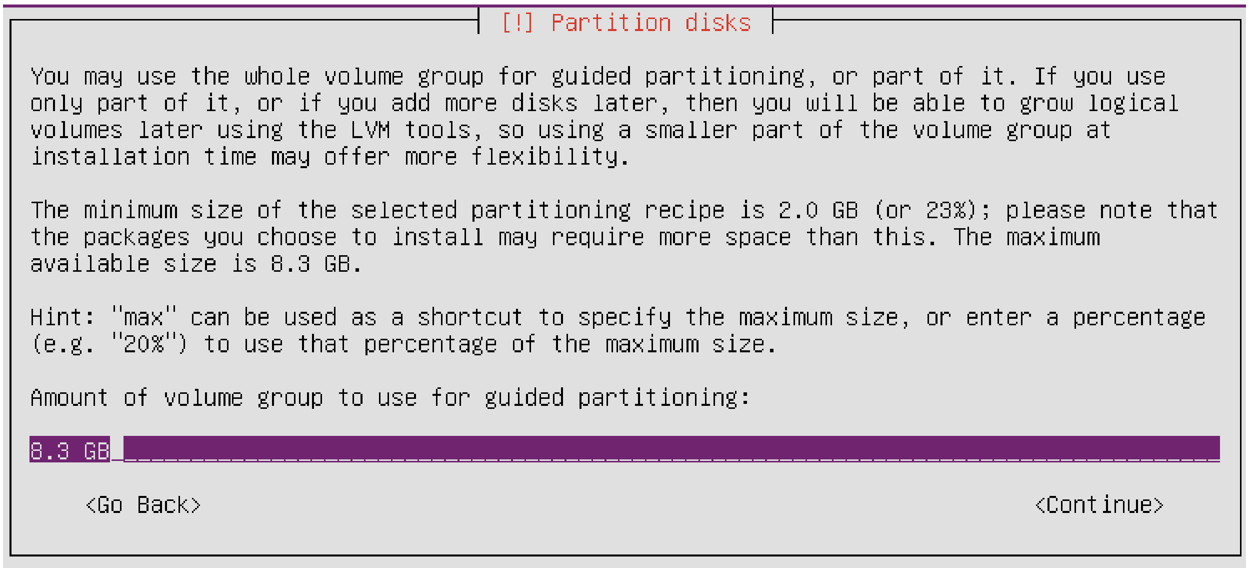
```
[!!] Partition disks

Note that all data on the disk you select will be erased, but not before you have
confirmed that you really want to make the changes.

Select disk to partition:

                    SCSI3 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK

    <Go Back>
```

- Select 'Yes' to 'Write the changes to disks and configure LVM'



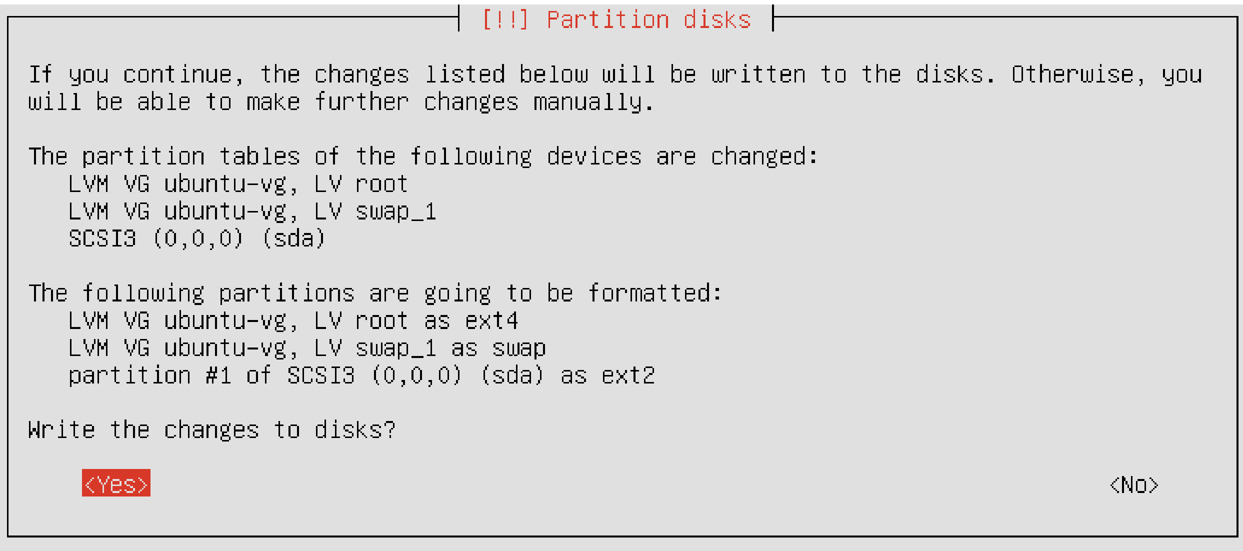
```
[!!] Partition disks

Before the Logical Volume Manager can be configured, the current partitioning scheme has
to be written to disk. These changes cannot be undone.

After the Logical Volume Manager is configured, no additional changes to the partitioning
scheme of disks containing physical volumes are allowed during the installation. Please
decide if you are satisfied with the current partitioning scheme before continuing.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

Write the changes to disks and configure LVM?

    <Yes>                                                                       <No>
```

- Select the disk partition size



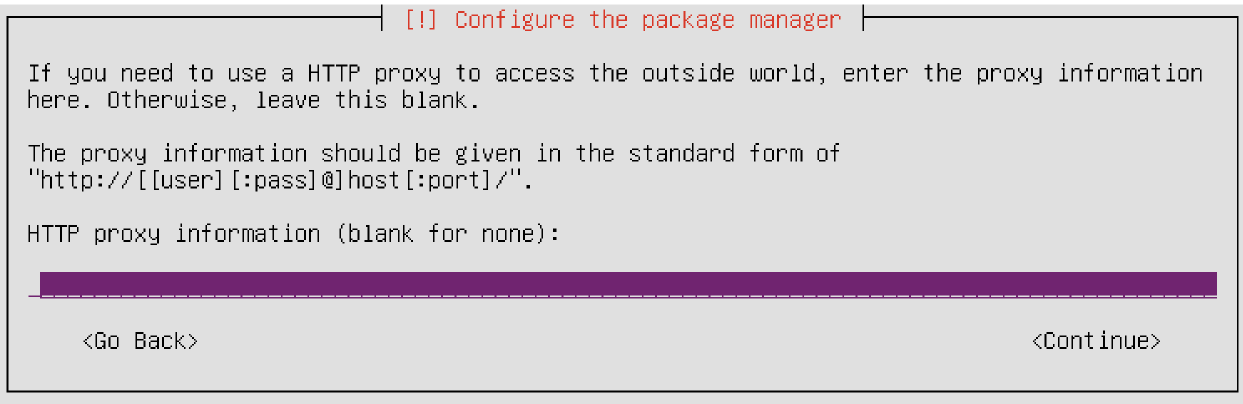
```
[!] Partition disks

You may use the whole volume group for guided partitioning, or part of it. If you use
only part of it, or if you add more disks later, then you will be able to grow logical
volumes later using the LVM tools, so using a smaller part of the volume group at
installation time may offer more flexibility.

The minimum size of the selected partitioning recipe is 2.0 GB (or 23%); please note that
the packages you choose to install may require more space than this. The maximum
available size is 8.3 GB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage
(e.g. "20%") to use that percentage of the maximum size.

Amount of volume group to use for guided partitioning:

8.3 GB

    <Go Back>                                                          <Continue>
```

- Select 'Yes' for 'Write the changes to disks?':



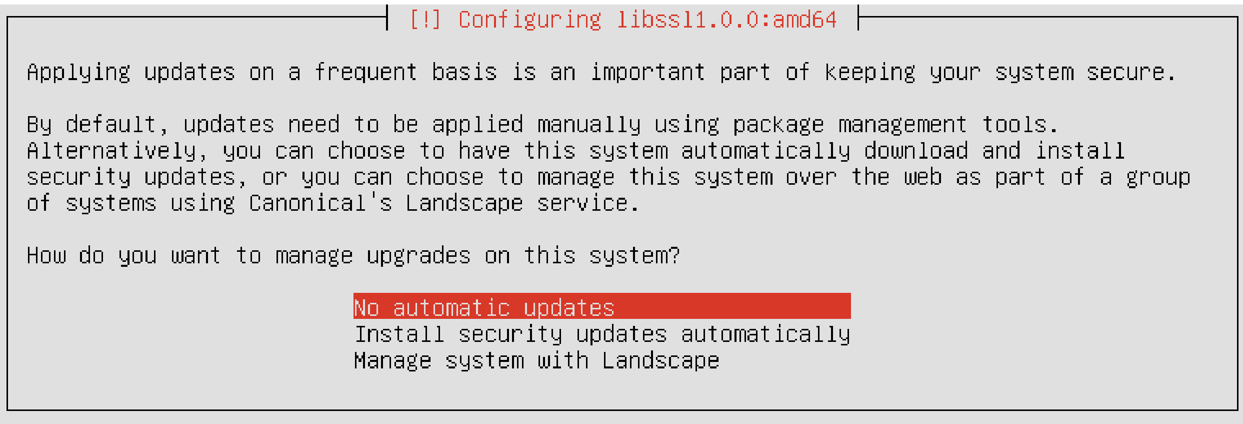
```
[!!] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you
will be able to make further changes manually.

The partition tables of the following devices are changed:
   LVM VG ubuntu-vg, LV root
   LVM VG ubuntu-vg, LV swap_1
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   LVM VG ubuntu-vg, LV root as ext4
   LVM VG ubuntu-vg, LV swap_1 as swap
   partition #1 of SCSI3 (0,0,0) (sda) as ext2

Write the changes to disks?

    <Yes>                                                                 <No>
```

- Continue the setup
- Enter the IP address of your proxy server if you are using one on your network. If not, leave the field blank and choose 'Continue':



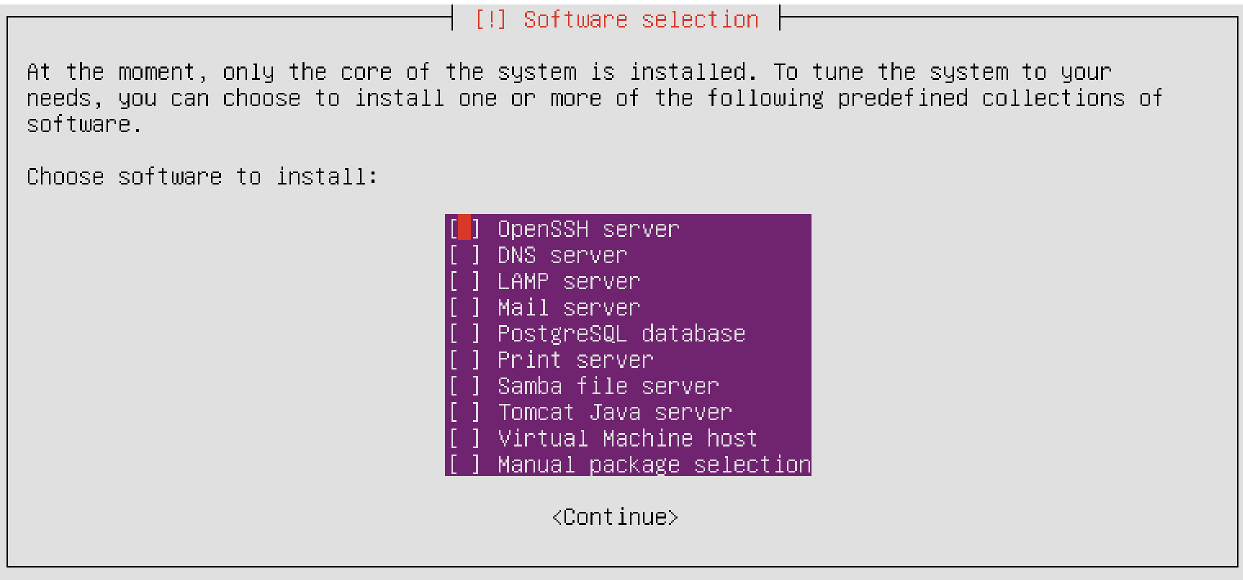
```
[!] Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information
here. Otherwise, leave this blank.

The proxy information should be given in the standard form of
"http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):



    <Go Back>                                                          <Continue>
```

The installation will begin. Once complete, please choose how you wish to handle updates:



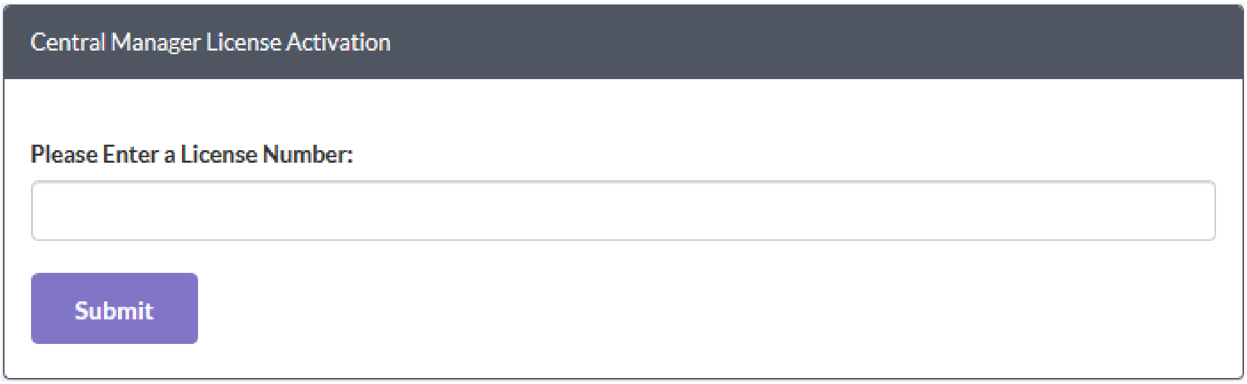
```
                    [!] Configuring libssl1.0.0:amd64

 Applying updates on a frequent basis is an important part of keeping your system secure.

 By default, updates need to be applied manually using package management tools.
 Alternatively, you can choose to have this system automatically download and install
 security updates, or you can choose to manage this system over the web as part of a group
 of systems using Canonical's Landscape service.

 How do you want to manage upgrades on this system?

                          No automatic updates
                          Install security updates automatically
                          Manage system with Landscape
```

  - Select your preferred option and continue onto the package selection screen:



```
                         [!] Software selection

 At the moment, only the core of the system is installed. To tune the system to your
 needs, you can choose to install one or more of the following predefined collections of
 software.

 Choose software to install:

                                 [ ] OpenSSH server
                                 [ ] DNS server
                                 [ ] LAMP server
                                 [ ] Mail server
                                 [ ] PostgreSQL database
                                 [ ] Print server
                                 [ ] Samba file server
                                 [ ] Tomcat Java server
                                 [ ] Virtual Machine host
                                 [ ] Manual package selection

                                         <Continue>
```

  - Select 'OpenSSH Server' then continue. Use the Space bar to select the option.
  - The appliance will restart when installation is complete..
- Assign a public IP address to the virtual appliance
- Once installed, you can access the Dome Firewall Central Manager console at the URL https://<IP Address of the virtual appliance>
  - UN = 'admin', password = 'comodo' (both without quotes). You should change these credentials after first login.
- You will be asked to enter the license key on your first login:



Central Manager License Activation

Please Enter a License Number:

  - Enter your license key and click 'Submit'.

Tip: Comodo One / Comodo Dragon / ITarian customers can integrate the central manager appliance with their portal accounts. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

Cloud Version

- Contact Comodo at **provisiondome@comodo.com** with your license key to setup the service.
- After setup, we will inform you of the IP address or domain on which the service is hosted
- The way you login to the console depends on how you purchased your license:
    - **Stand-alone Customers** - You can access your central manager instance at the address provided to you. For example, https://<given I P address>
        - UN = 'admin', password = 'comodo' (both without quotes). You should change these credentials after first login.
    - **Comodo One, Comodo Dragon and ITarian MSP/Enterprise Customers -** you can integrate your central manager appliance to your portal account. You can access the central manager administrative console directly from your portal. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

1.3 Integrate Central Manager with Comodo One / Comodo Dragon / ITarian

Comodo Dome Firewall Central Manager can be integrated with your Comodo One / Comodo Dragon (CD) / ITarian account. Once integrated, you can access CM from portal by clicking 'Applications' > 'Dome Central Manager'.

The following sections explain how to integrate different versions of CM to C1 / CD / ITarian:

- **Dome Firewall Central Manager Virtual Appliance**
- **Dome Firewall Central Manager Cloud Mode**

Dome Firewall Central Manager Virtual Appliance

Single Sign-on (SSO) from C1, CD and ITarian is not enabled by default in the virtual appliance version. Integrating CM virtual appliance with your portal involves two steps:

- **Step 1 - Enable SSO in the virtual appliance**
- **Step 2 - Add the IP Address of your CM installation as Dome Service URL for Dome Firewall Central Manager to your Comodo One / CD / ITarian account.**

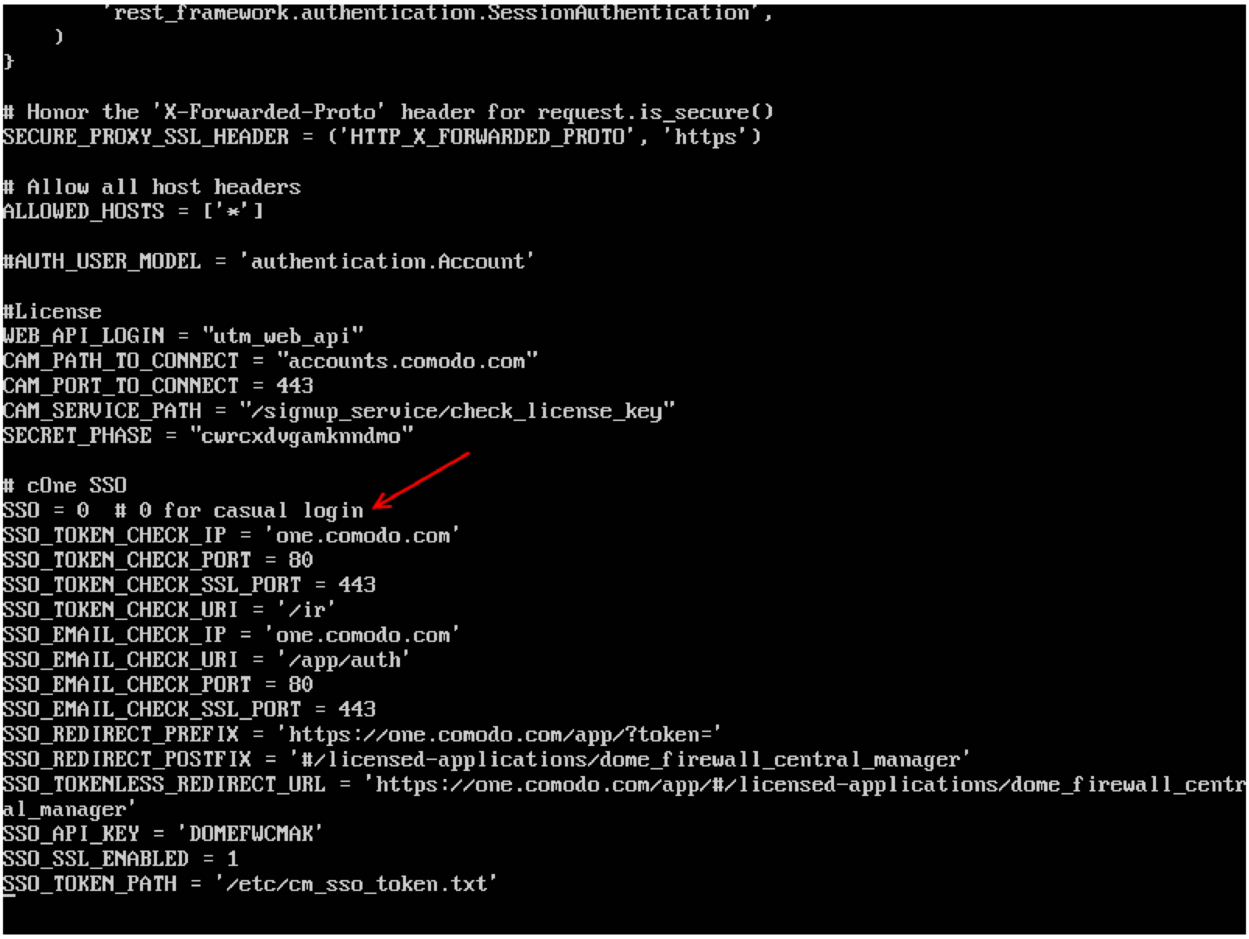
Step 1 - Enable SSO in the virtual appliance

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'
```

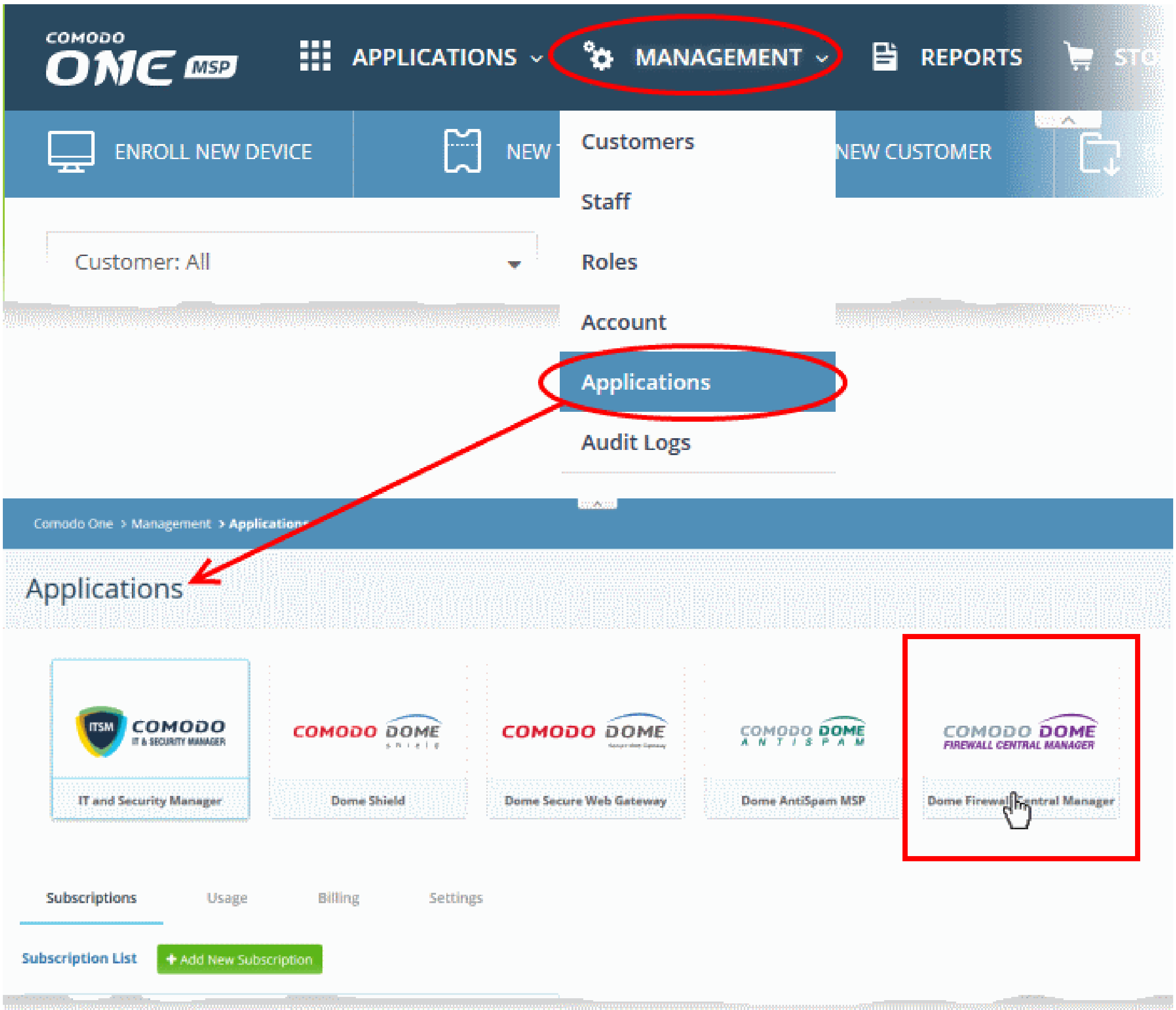
- Set the SSO flag to1
- Save the 'Settings' file
- Restart the apache service using the Sudo command: *sudo apache2ctl restart*

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

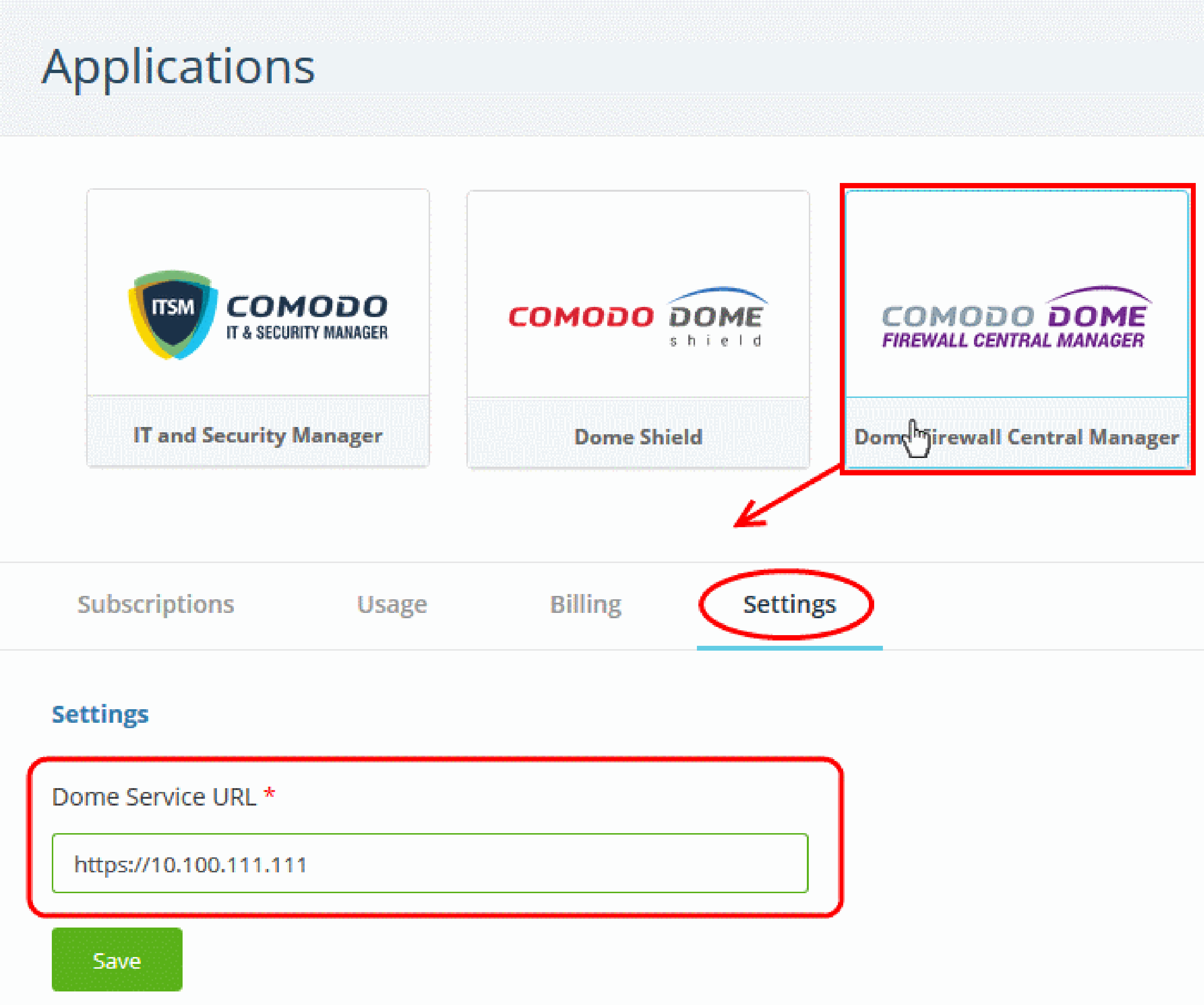
Step 2 - Add Dome Service URL for Dome Firewall Central Manager to your Comodo One / CD / ITarian account

You need to add the IP Address of your appliance as Dome Service URL for Dome Firewall Central Manager to your portal account.

- 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



Settings

Dome Service URL *

https://10.100.111.111

- Enter the IP address of your appliance (in the form https://<given IP Address>) in the Dome Service URL text box and click 'Save'.

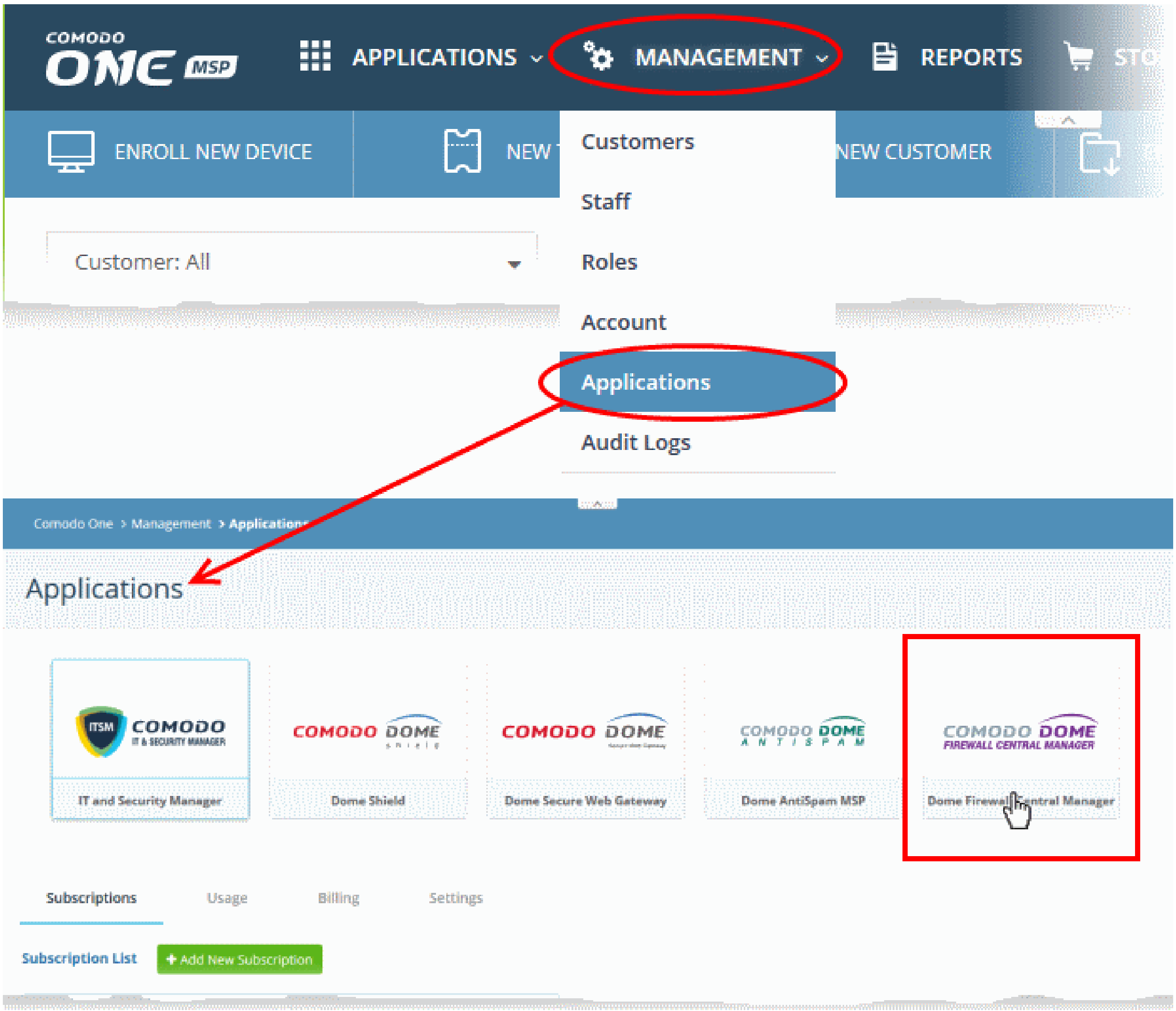
Your Firewall Central Manager appliance is now integrated with your Comodo One / CD / ITarian account. You can login to your Central Manager console from your portal.

Dome Firewall Central Manager Cloud Mode

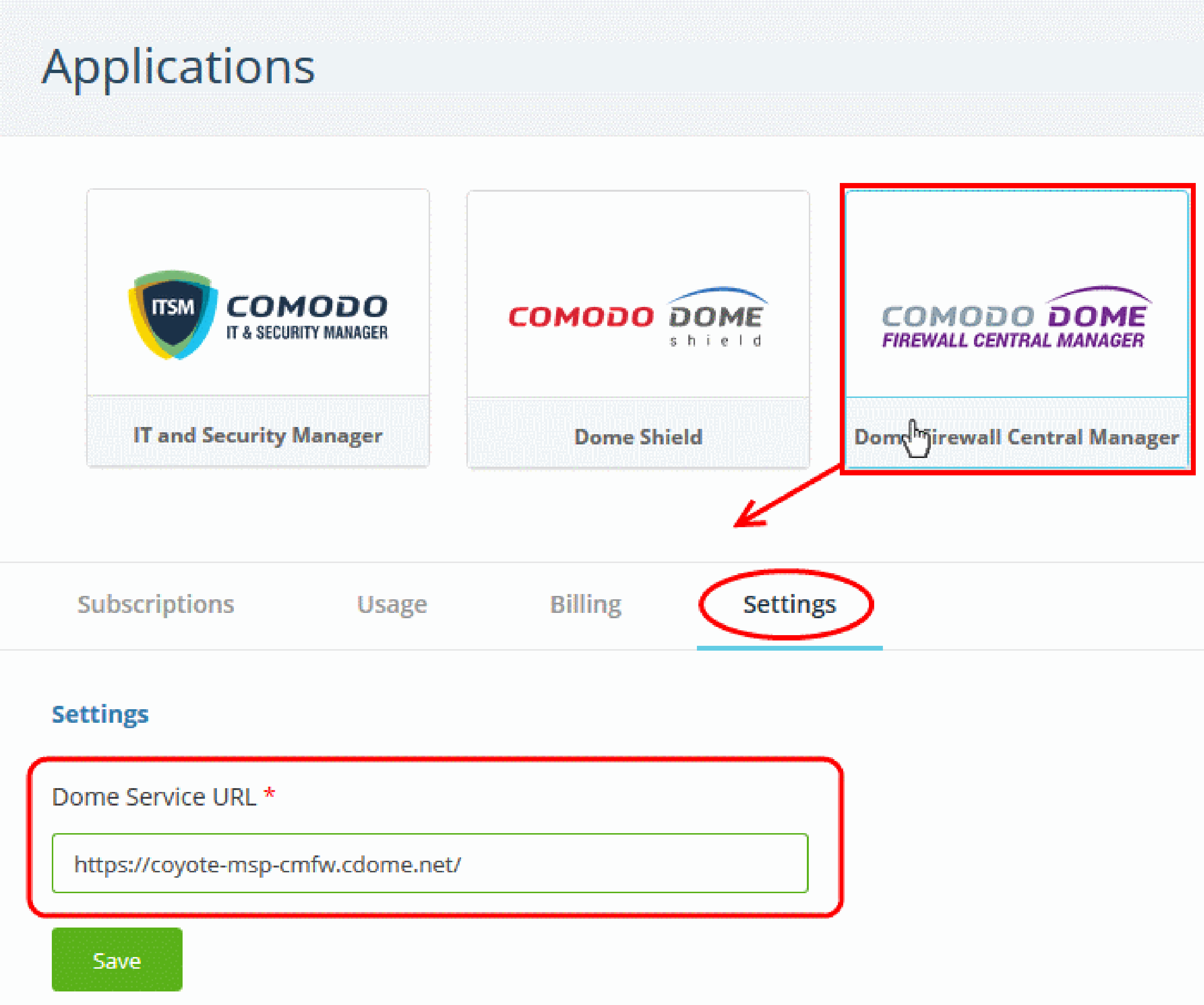
Single Sign-on (SSO) is enabled by default in the cloud version. You need to add your CM access URL or the IP address as Dome Service URL for Dome Firewall Central Manager to your portal account.

To integrate your Cloud CM to Comodo One, Comodo Dragon or ITarian account

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



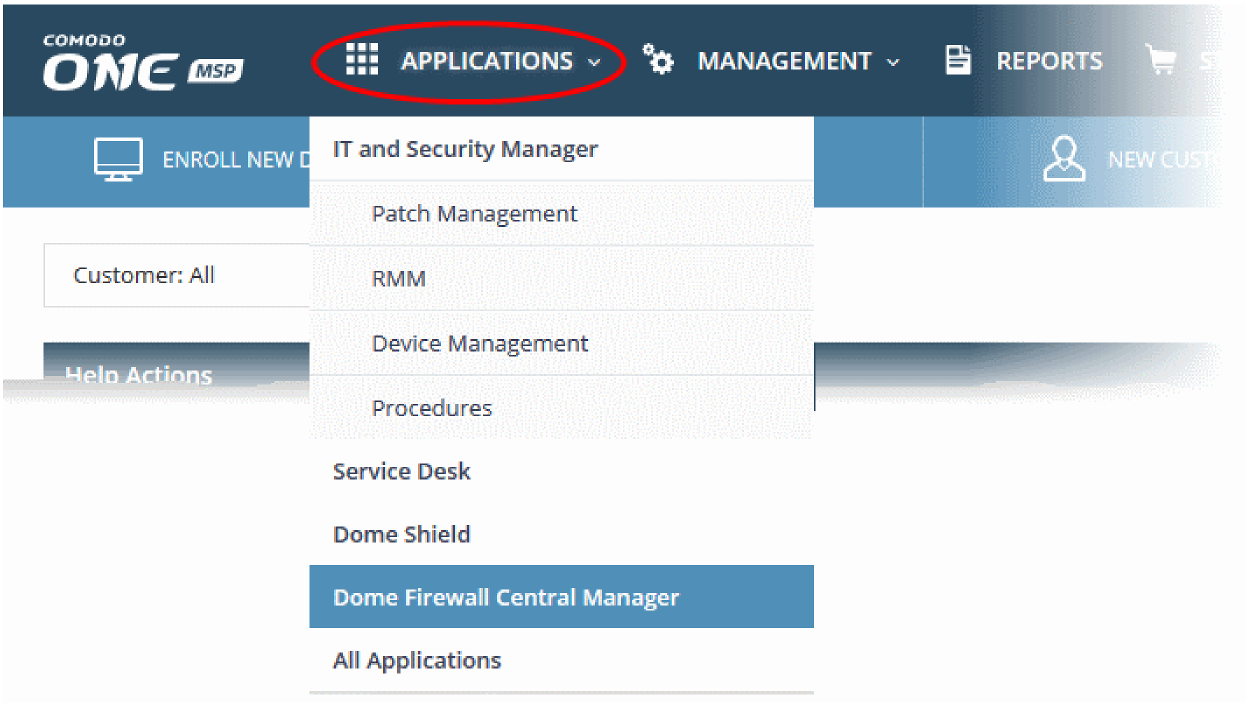
- Click the 'Dome Firewall Central Manager' tile
- Select the 'Settings' tab in the bottom pane



Dome Service URL *

https://coyote-msp-cmfw.cdome.net/

- Enter the given domain or IP address (Format = https://<given IP Address>) in the Dome Service URL text box and click 'Save'.
- Dome Firewall Central Manager is now integrated with your portal account.
- You can access CM from your portal as follows:
  - Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
  - Click 'Applications' > 'Dome Firewall Central Manager'



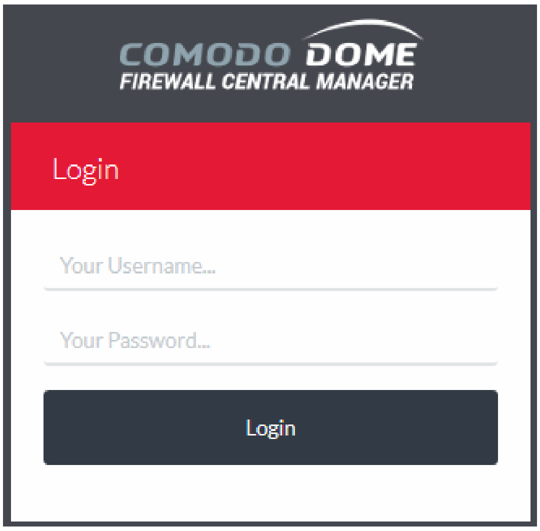
Central manager will open at the dashboard in a new tab.

1.4 Login to the Admin Console

Dome Firewall Stand-alone Customers

Once setup, you can login to the central manager admin console using any web browser.

- Paste the IP address of your instance into any browser. Format = https://<given IP address>.
- Login with the following default credentials:
  - Username = admin
  - Password = comodo



- You can change the default password after first login. 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. See **Change Password** for more details.

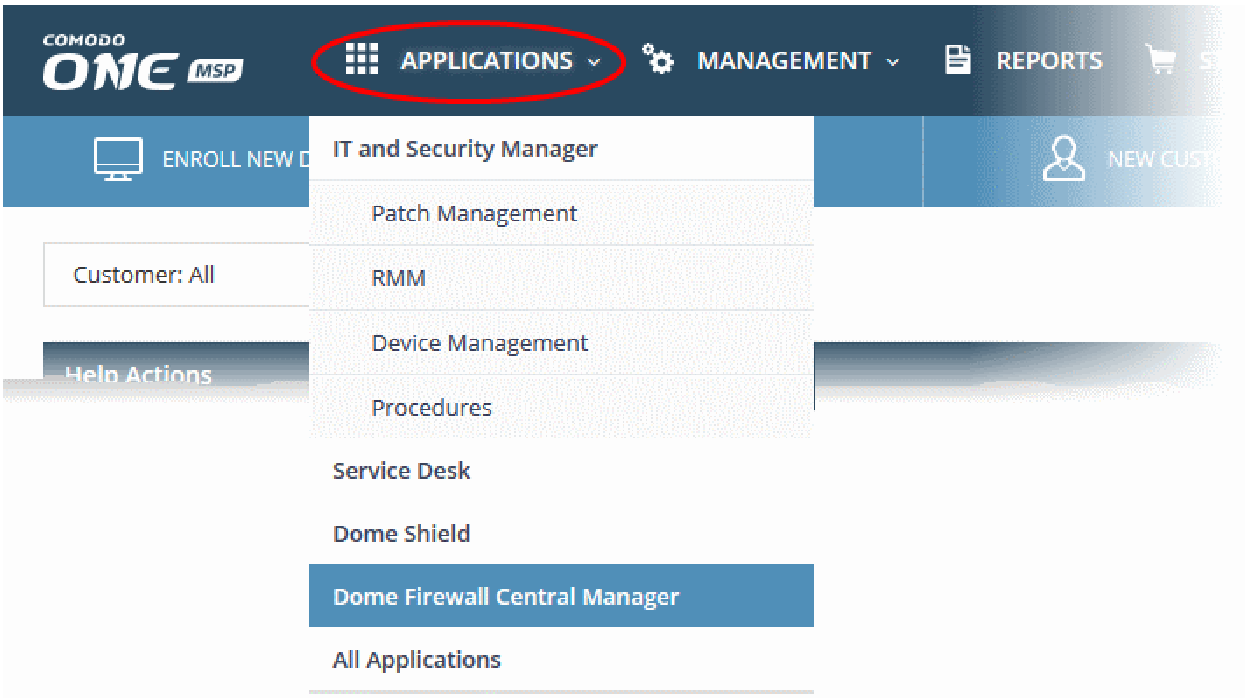
Comodo One / Comodo Dragon / ITarian MSP and Enterprise Customers

You can login to the administrative console in two ways:

- Login to stand-alone Central Manager Console
  - Enter the given URL or https://<given *ip address of the central manager*> in the address bar of the browser
  - Use the default credentials:

    Username = admin

    Password = comodo
  - You can change these credentials anytime after your first login. See **Change Password** for more details
- Comodo One/ CD / ITarian Console – You can integrate your Dome Firewall Central Manager to your portal and access the administrative console from it. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.
  - After integration, you can access the administrative console at anytime by clicking 'Applications' > 'Dome Firewall Central Manager' from your portal console.



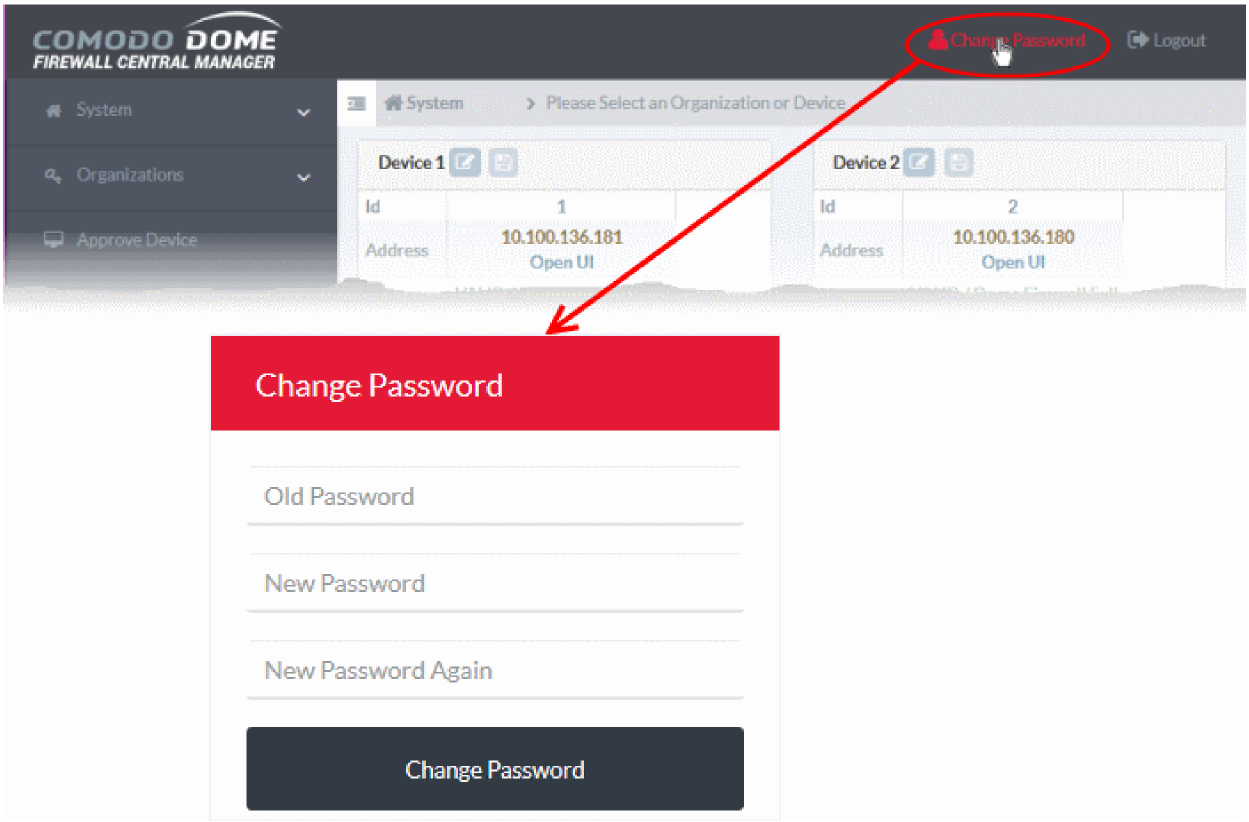
1.5 Change Password

The 'Change Password' option at the top right allows you to change your login password at any time.

Note: The change password option will be available only for stand-alone Central Manager Console. You cannot change the password for central manager console accessed through C1 / CD / ITarian portal.

To change your login password for Dome Firewall Central Manager

- Click 'Change Password' at the top right



The 'Change Password' dialog will appear.

- Enter your existing password in the 'Old Password' field
- Enter a new password in the 'New Password' field and re-enter it for confirmation n the 'New Password Again' field. The new password should be of minimum eight characters length. Choose a strong password that contains a mix of upper and lower case letters, numbers and special characters

Tip: We also recommend regularly changing your password as a best security practice.

- Click 'Change Password'

Your password will be changed. You should use your new password from your net login.

1.6 Add Organizations

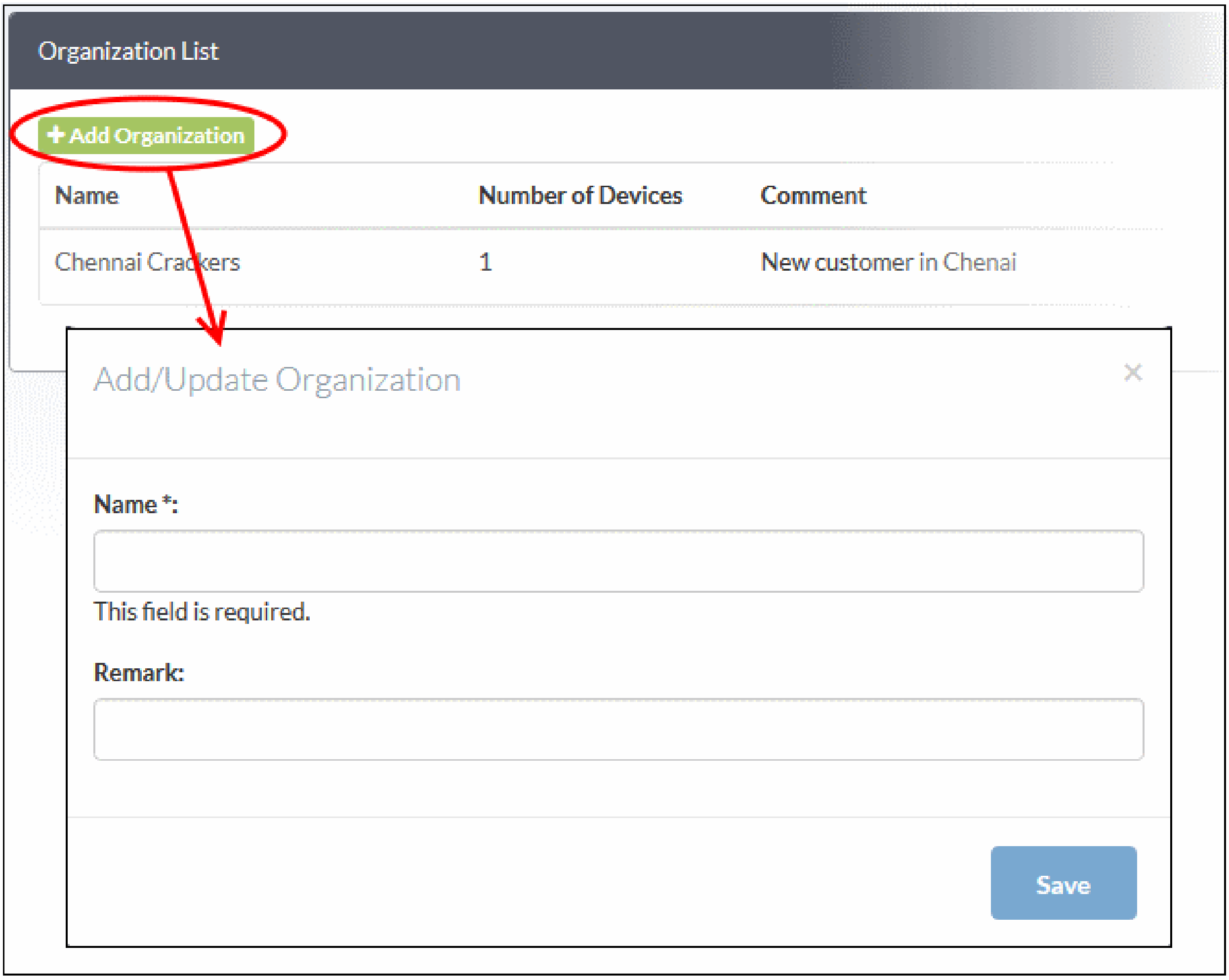
- Each firewall device you enroll to the central manager needs to be assigned to an organization. Doing so will allow you to collectively manage and apply policies to all devices in the organization.

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



Organization List

Name	Number of Devices	Comment
Chennai Crackers	1	New customer in Chenai

Add/Update Organization

Name *:

This field is required.

Remark:

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.

- Repeat the process to add more organizations.

1.7 Enroll Dome Firewall Devices

- Dome Firewall devices have a built-in client which communicates with the central manager. This allows the device to receive commands from the manager and apply them to the firewall.
- Dome Firewall virtual appliances behind Network Address Translation (NAT) can also be enrolled to the central manager. The manager will communicate with the appliance through the NAT IP address.
- Note – Existing configurations (policies, objects etc) will not be imported with the FW device. We recommend you remove these from the device before importing then configure them again in central manager.

Enrolling firewall devices to Central Manager takes two steps:

- **Connect the device to Dome Firewall Central Manager**
- **Approve the device and assign it to an organization**

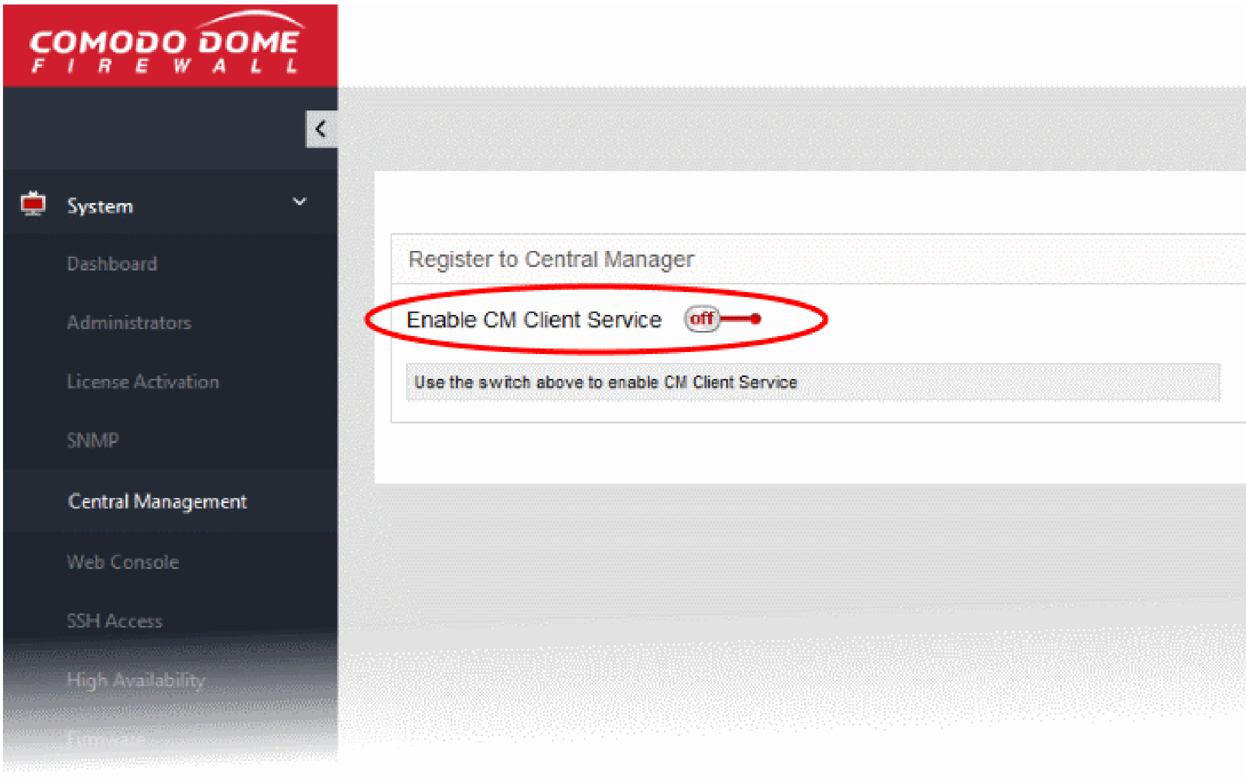
See the following for more details:

Step1: Connect the firewall device to Dome firewall Central Manager

- Login to the firewall device at https://<ip address of the Dome firewall device>:10443

The 'Comodo Dome Firewall' interface will open.

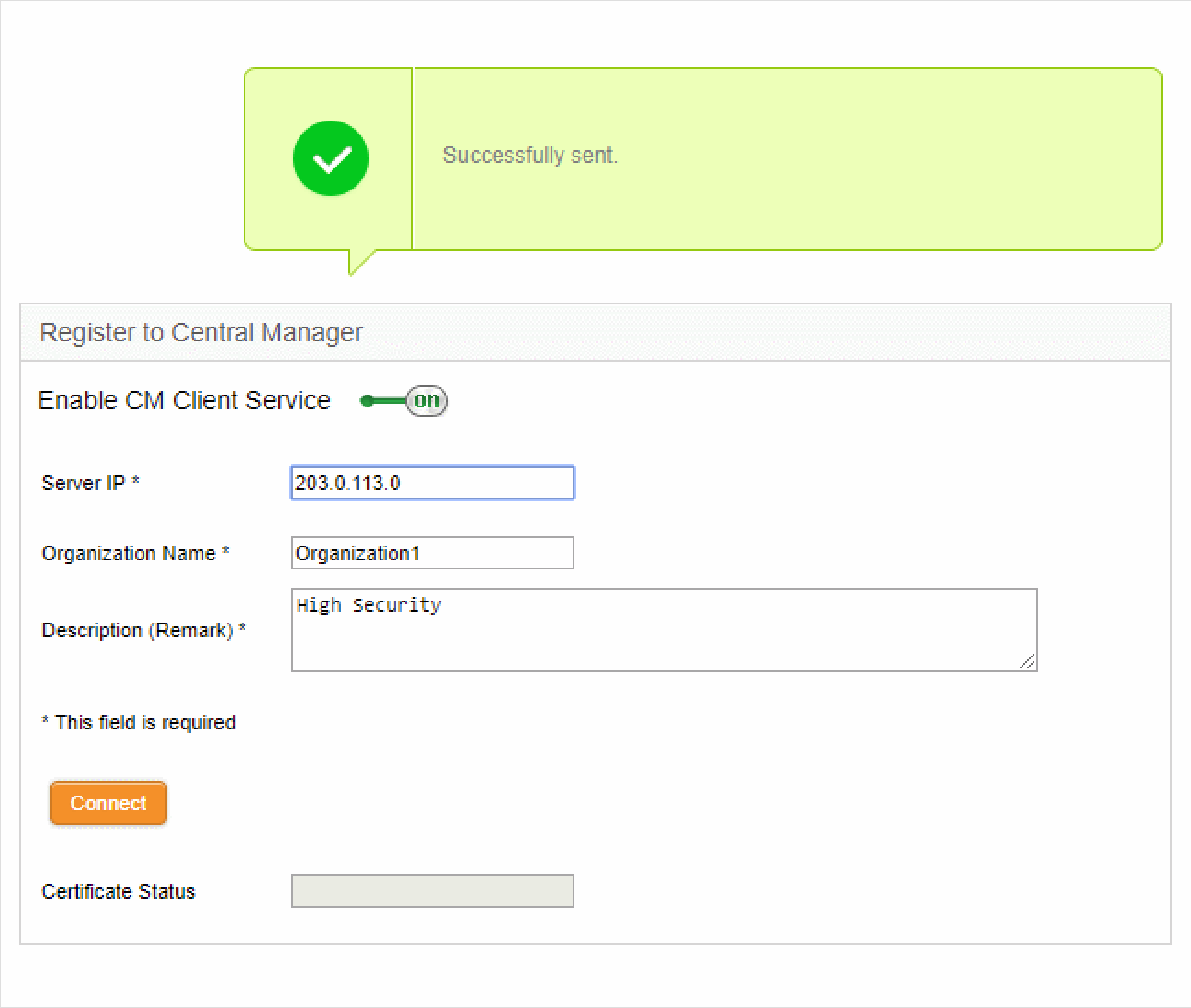
- Click 'System' > 'Central Management'
- Switch 'Enable CM Client Service' to 'ON':



Enable CM Client Service

Use the switch above to enable CM Client Service

- Enter the parameters required to connect the firewall to Dome central manager
  - Server IP - Enter the IP address of the DFW Central Manager interface
  - Organization Name - Enter the name of the organization to which you want the device to belong. You can create organizations by logging into the central manager and clicking 'Organizations' > 'Organizations' > 'Add Organization'.
  - Description (Remark)* - Enter any comments you wish to leave about the device
- Click 'Connect'



Successfully sent.

Register to Central Manager

Enable CM Client Service: on

Server IP *: 203.0.113.0

Organization Name *: Organization1

Description (Remark) *: High Security

* This field is required

Certificate Status:

The device will be successfully connected to Dome Firewall Central Manager.

Next, the administrator needs to approve the device in order to complete the import process.

Step 2 : Approve the Dome Firewall Device

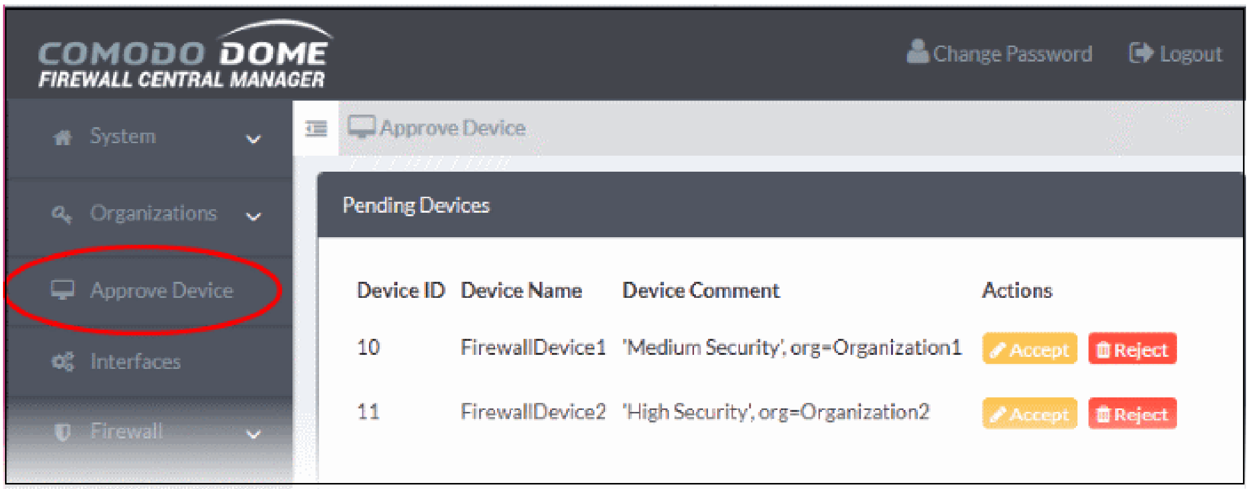
- Newly enrolled devices must be approved by the central manager admin before they can be imported. These devices are listed in the 'Approve Device' interface.
- The 'Approve Device' interface lets you approve devices and assign them to an organization

To approve a device:

- Make sure you have connected the device as explained in step 1 above.
- Login to the DFW Central Manager console.

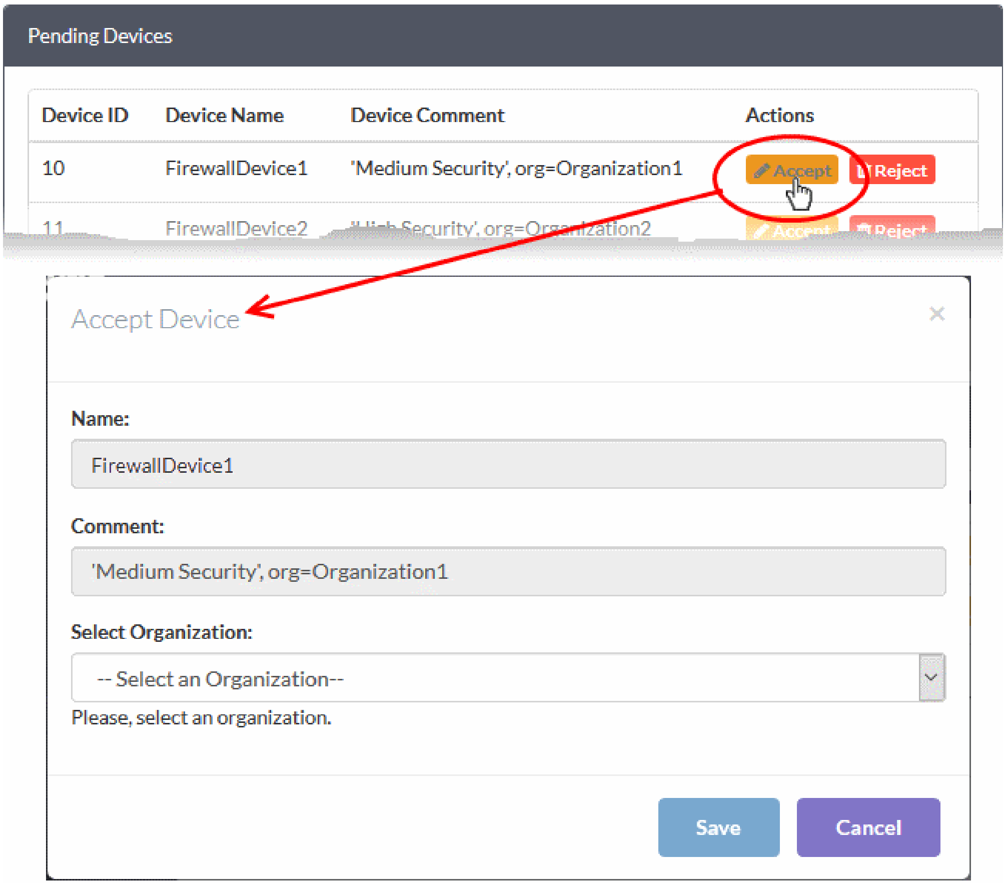
After logging in,

- Click 'Approve Device' on the left.



Device ID	Device Name	Device Comment	Actions
10	FirewallDevice1	'Medium Security', org=Organization1	Accept Reject
11	FirewallDevice2	'High Security', org=Organization2	Accept Reject

- 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.



Device ID	Device Name	Device Comment	Actions
10	FirewallDevice1	'Medium Security', org=Organization1	Accept Reject
11	FirewallDevice2	'High Security', org=Organization2	Accept Reject

Name: FirewallDevice1

Comment: 'Medium Security', org=Organization1

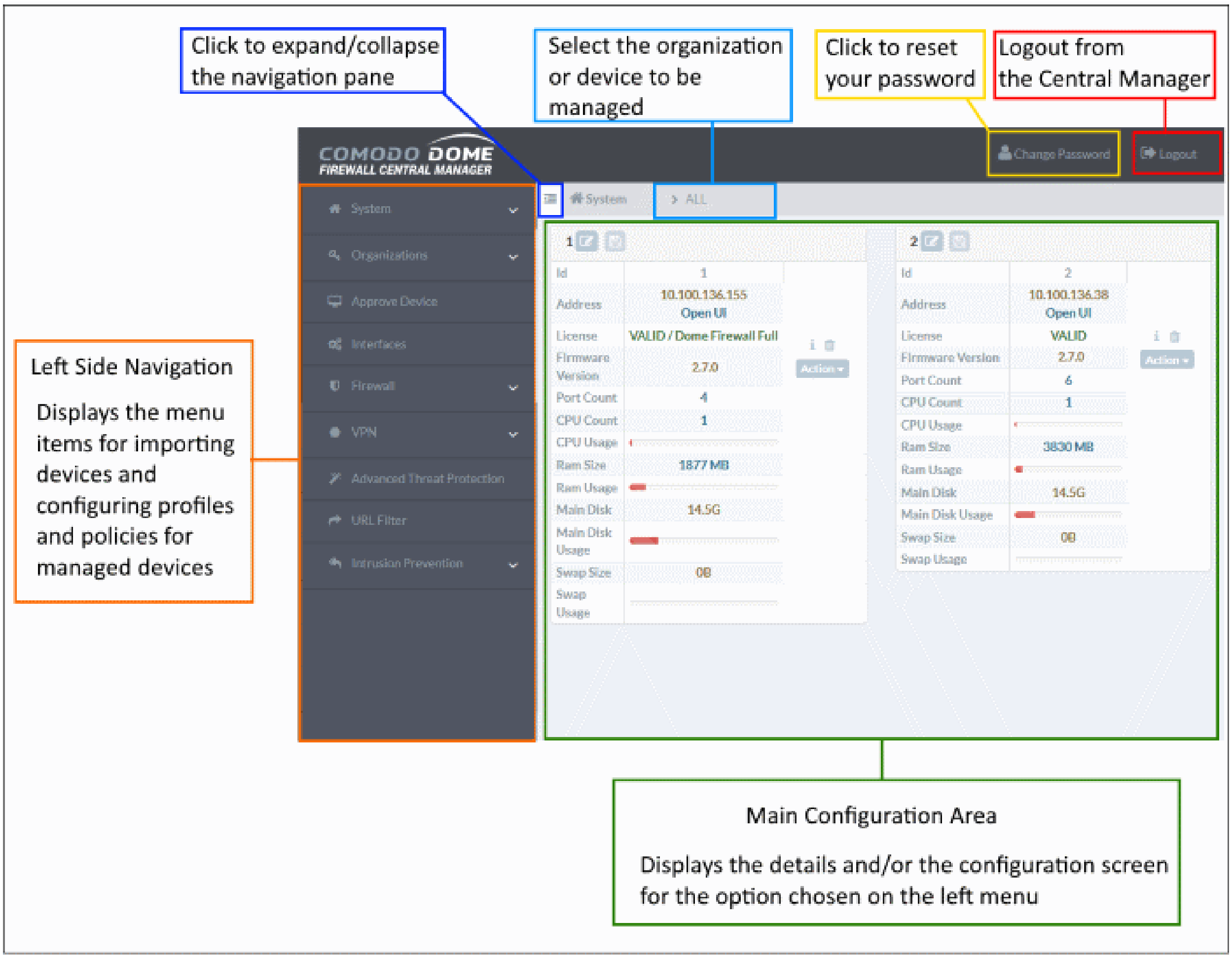
Select Organization: -- Select an Organization--

Please, select an organization.

- Name - The device label. The name is pre-populated and cannot be edited. Please note that you can change the name of a device from the dashboard after device enrollment.
- Comment - Brief description and organization details entered when enrolling the device. This field is pre-populated and not editable
- Select Organization - Choose the organization to which the device should be assigned. See **Add Organizations** if you have not yet added an organization.

2 The Main Interface

The admin console has a modular interface which lets you easily manage all aspects of your firewall policies:



Click to expand/collapse the navigation pane

Select the organization or device to be managed

Click to reset your password

Logout from the Central Manager

Left Side Navigation

Displays the menu items for importing devices and configuring profiles and policies for managed devices

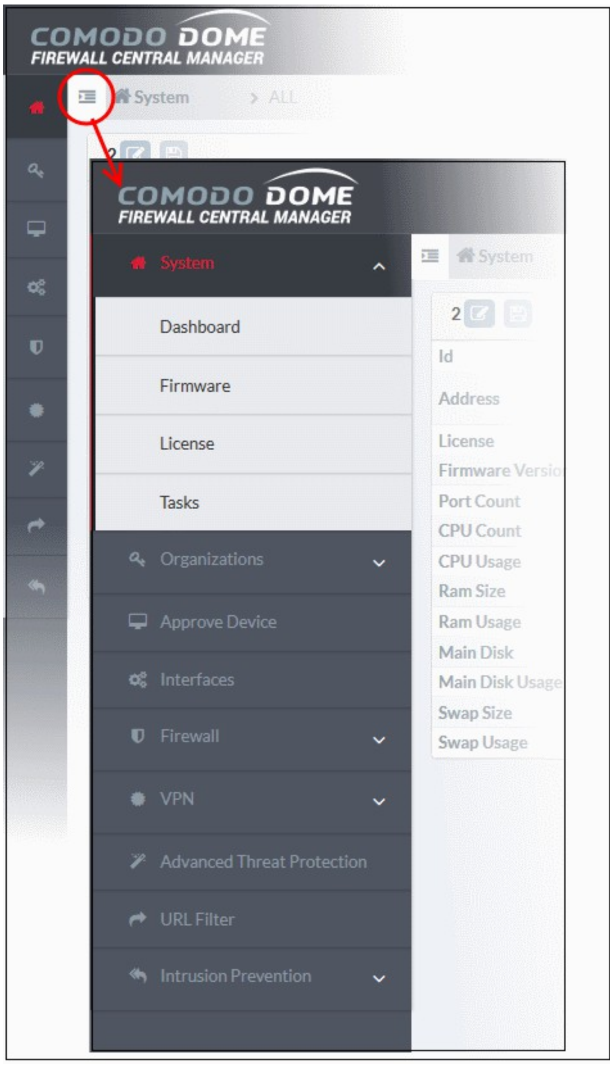
Main Configuration Area

Displays the details and/or the configuration screen for the option chosen on the left menu

Id	1
Address	10.100.136.155 Open UI
License	VALID / Dome Firewall Full
Firmware Version	2.7.0
Port Count	4
CPU Count	1
CPU Usage	
Ram Size	1877 MB
Ram Usage	
Main Disk	14.5G
Main Disk Usage	
Swap Size	0B
Swap Usage	

Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	6
CPU Count	1
CPU Usage	
Ram Size	3830 MB
Ram Usage	
Main Disk	14.5G
Main Disk Usage	
Swap Size	0B
Swap Usage	

All modules can be accessed using the links in the left-hand menu. The following table is a quick overview of the modules:



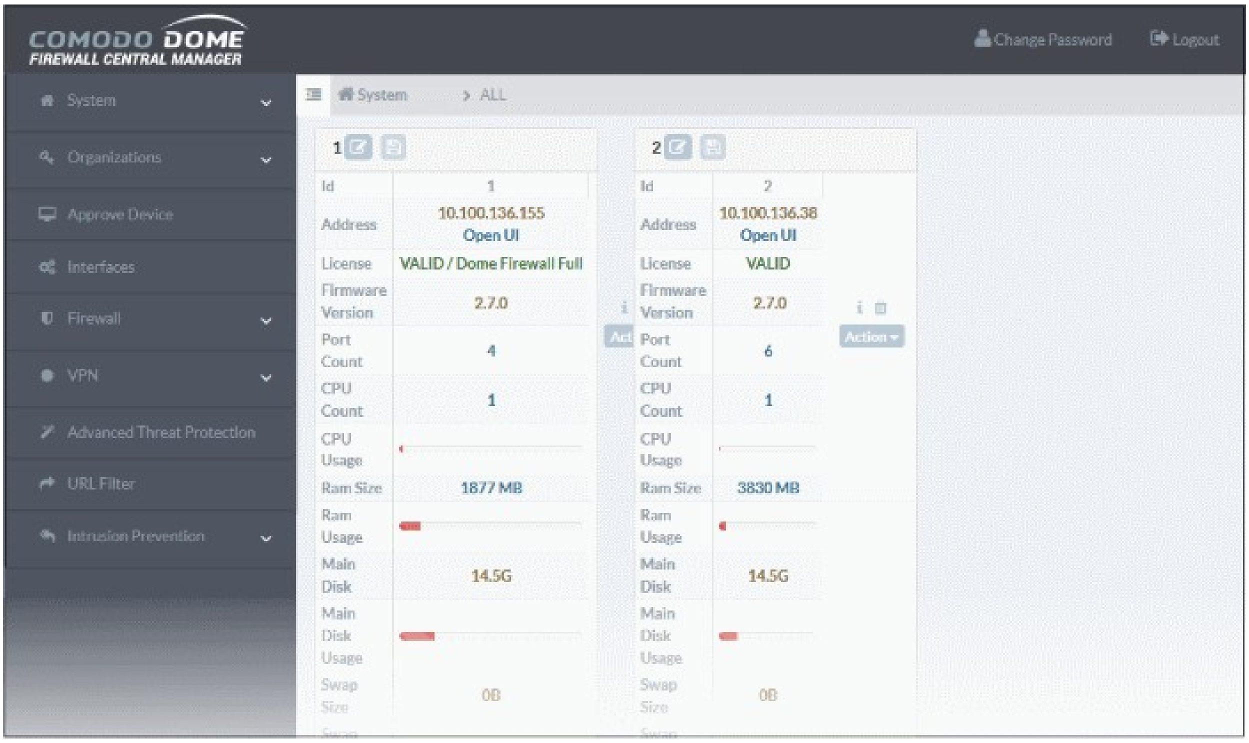
- **System** - View dashboard, manage enrolled firewall devices, update firmware, activate CM license, view and re-apply management tasks and more.
- **Organizations** - View and manage customer organizations for whom you manage firewall devices and activate firewall device licenses.
- **Approve Device** - Accept and import enrolled new devices and assign them respective organizations.
- **Interfaces** - Configure network zone interfaces for connection to different ports of managed firewall devices.
- **Firewall** - Configure firewall policy rules for managed devices, create security profiles for use in policy rules and more.
- **VPN** - Configure IPsec-based VPN tunnels and L2TP servers. Manage IPSec / L2TP users.
- **Advanced Threat Protection** - Configure default ATP profiles for managed organizations and devices for use in firewall policy rules applied to them.
- **URL Filter** - Configure web filtering profiles for use in firewall policy rules for managed organizations and devices.
- **Intrusion Prevention** - Configure default profiles for Intrusion Prevention and application detection for use in firewall rules applied to managed organizations and devices.

3 The Dashboard

The dashboard shows information about firewall devices which have been added to the central manager.

- Click 'System' > 'Dashboard' on the left to access the dashboard
- Each tile contains info about a specific device.
- The 'Open UI' link lets you login to the firewall directly. You can 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.

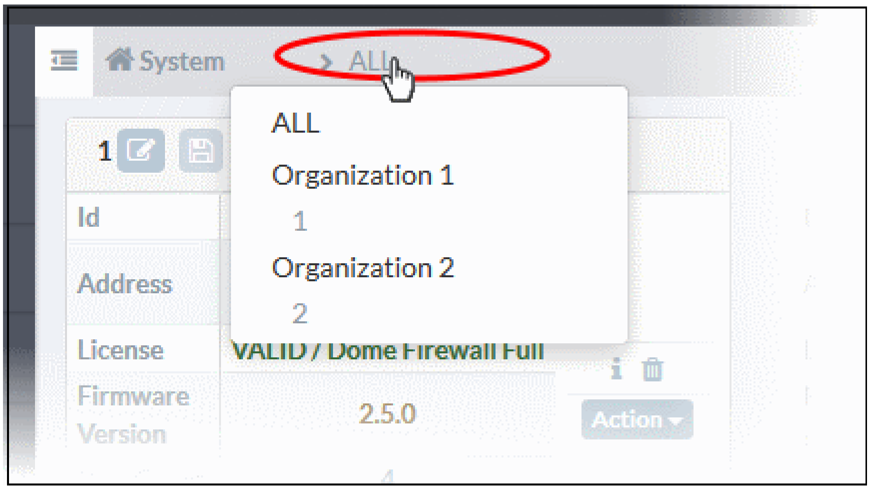
The dashboard is shown by default whenever you login to the admin interface.



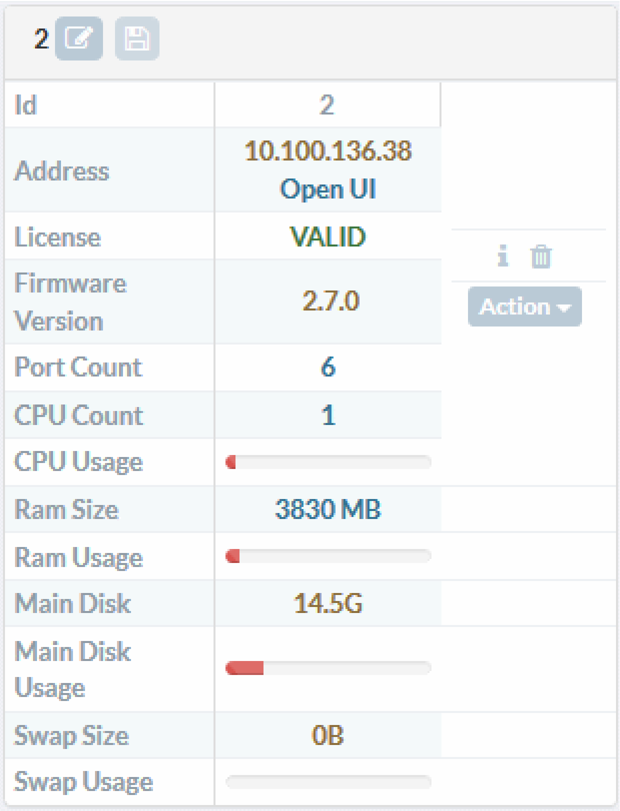
	1	2
Id	1	2
Address	10.100.136.155 Open UI	10.100.136.38 Open UI
License	VALID / Dome Firewall Full	VALID
Firmware Version	2.7.0	2.7.0
Port Count	4	6
CPU Count	1	1
CPU Usage		
Ram Size	1877 MB	3830 MB
Ram Usage		
Main Disk	14.5G	14.5G
Main Disk Usage		
Swap Size	0B	0B

The dashboard shows the last viewed firewall devices after logging in. Use the filter at the top to view only devices which belong to a specific organization.

- Click the filter at the header and select an organization.



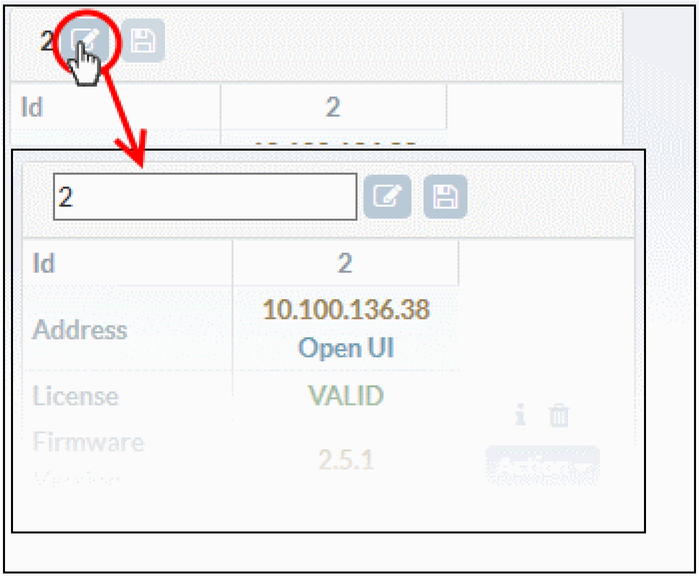
Each tile shows device identification/location/license and hardware/software details. There are also shortcuts to view complete details on various parameters, execute device tasks and more.



2

Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	6
CPU Count	1
CPU Usage	
Ram Size	3830 MB
Ram Usage	
Main Disk	14.5G
Main Disk Usage	
Swap Size	0B
Swap Usage	

Device Details - Table of Parameters	
Parameter	**Description**
ID	The identification number assigned to the firewall device by the central manager
Address	The IP address of the device. • If the device is behind Network Address Translation (NAT), the NAT address of the device is shown. • Click 'Open UI' to login to the firewall console See **Access Admin Console of a Firewall Device** for more details.
License	Displays the license type of the device and its status, whether valid or expired.
Firmware Version	The firmware version number of the firewall device, You can update the firmware from the central manager if required. See **Update Firmware Version** for more details.
Port Count	Number of network interfaces connected to the firewall.
CPU Count	Number of processor resources in the firewall device
CPU Usage	The usage of the CPU resources. In a multi-processor device, the cumulative load on all CPU's is indicated.
RAM size	The size of the system memory in the firewall device.
RAM Usage	Shows the amount of system memory currently used.
Main Disk	Shows the size of root partition of the disk drive in the firewall appliance.

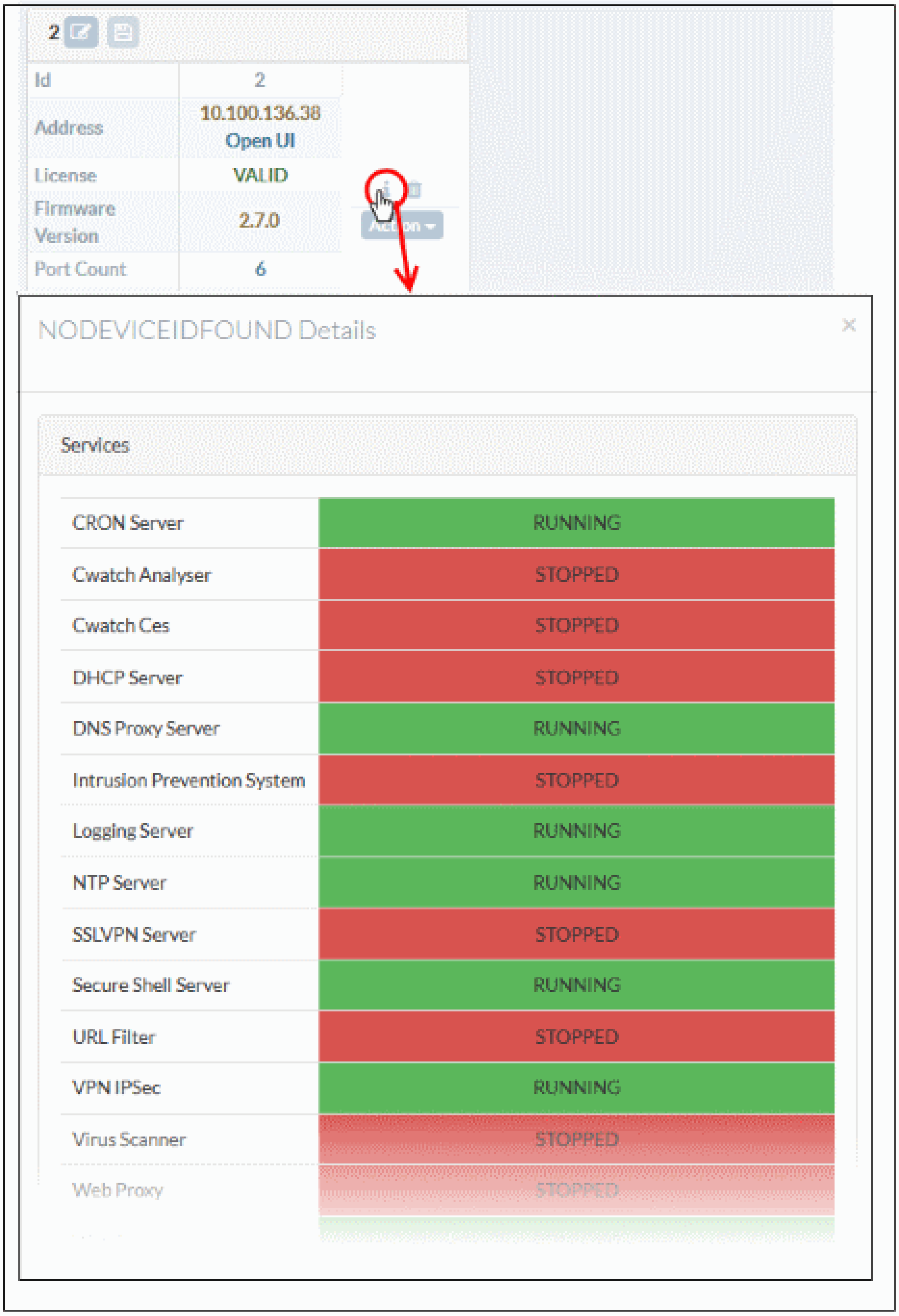
Main Disk Usage	Shows the current usage of the root partition of the hard disk in the firewall device. The disk usage should not exceed 95%.
Swap Size	Shows the size of memory dedicated for swapping services/processes in the firewall device.
Swap Usage	Shows the current usage of the swap memory. The average swap usage will be below 20%, if not all the services are used all the time.
Control Buttons	
Edit and Save	Allow you to change the name of the device as identified in the dashboard. • Click the 'Edit' button to open the edit field  2 Id 2 2 Id 2 Address 10.100.136.38 Open UI License VALID Firmware Version 2.5.1 Action • Enter a new name for the device • Click the 'Save' button for the new name to take effect
Information i	Shows the details on currently running services and disk usage on the firewall device. See **View Details of a Firewall Device** for more details.
Trash Can	Removes the firewall device from management.
Action Action ▾	Contains options to execute important configuration changes in the firewall device. See **Quick Actions on a Firewall Device** for more details.

3.1 View Details of a Firewall Device

The dashboard lets you view a list of currently running services, disk usage and the kernel version of a managed firewall device.

To view the details

- Click 'System' on the left then select 'Dashboard'
- Click the information icon i on the tile of the device



Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	6

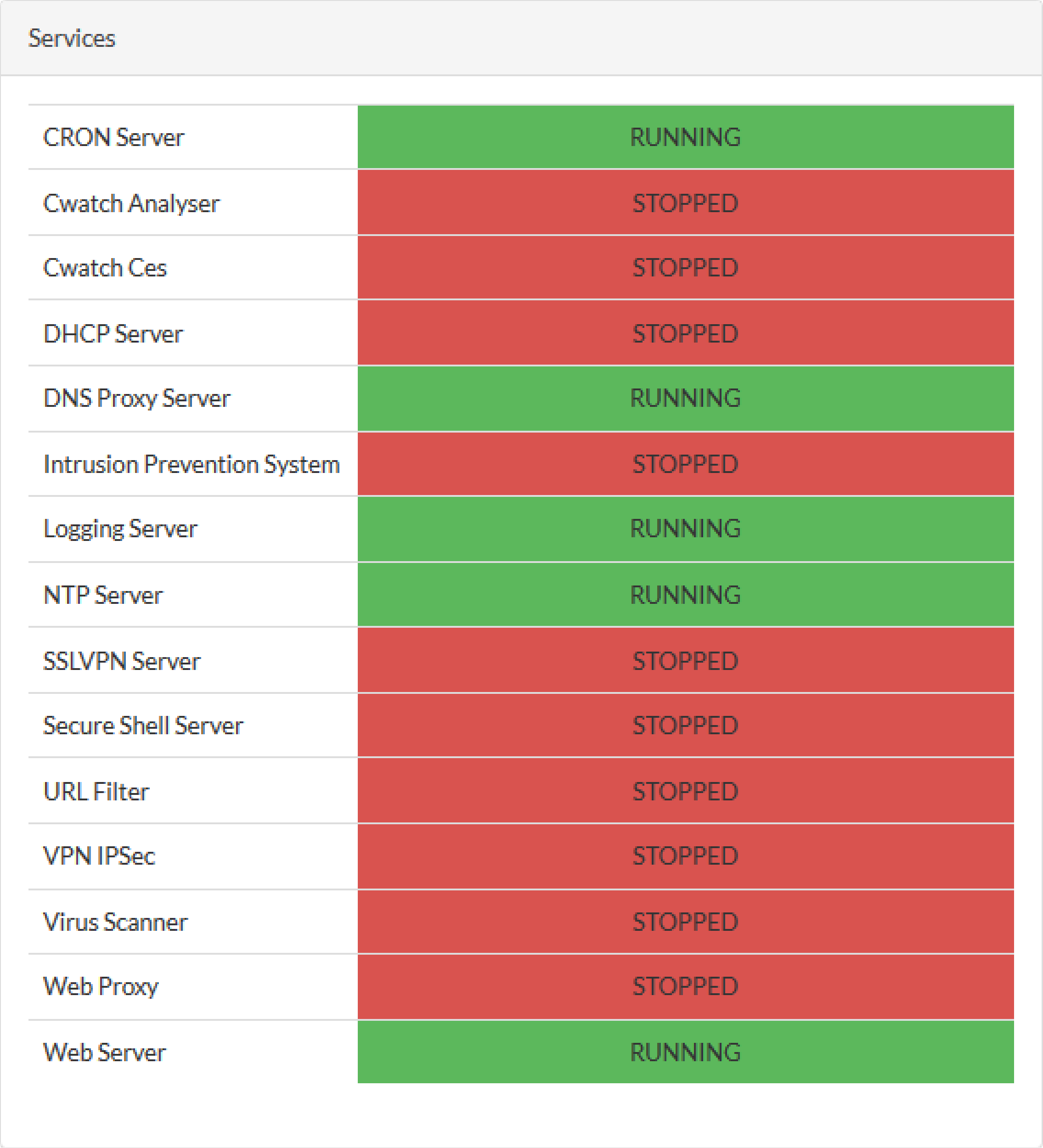
NODEVICEIDFOUND Details

Services

CRON Server	RUNNING
Cwatch Analyser	STOPPED
Cwatch Ces	STOPPED
DHCP Server	STOPPED
DNS Proxy Server	RUNNING
Intrusion Prevention System	STOPPED
Logging Server	RUNNING
NTP Server	RUNNING
SSLVPN Server	STOPPED
Secure Shell Server	RUNNING
URL Filter	STOPPED
VPN IPSec	RUNNING
Virus Scanner	STOPPED
Web Proxy	STOPPED

The details pane contains three areas:

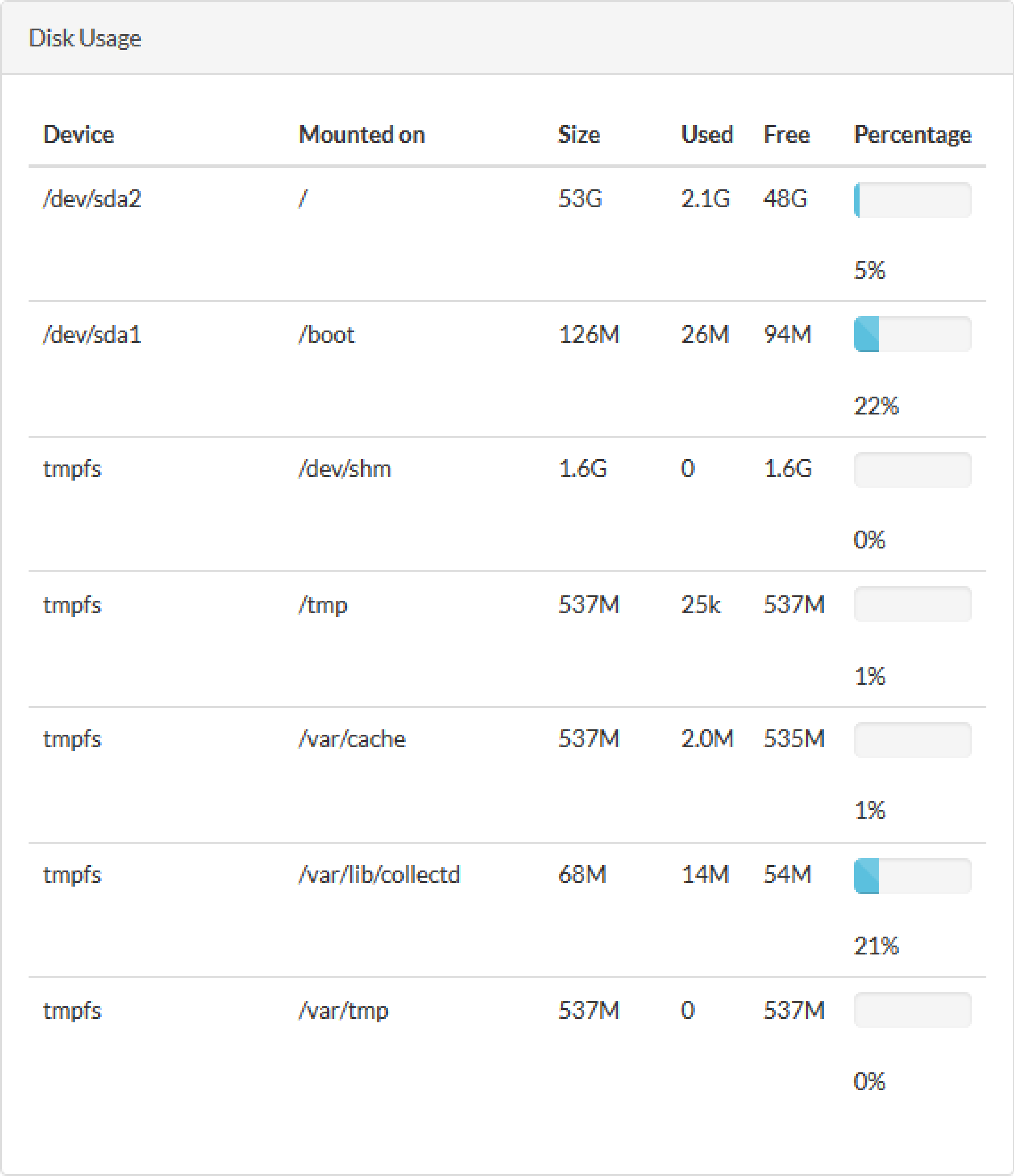
- **Services -** Shows a list of services that are currently loaded to the firewall device and their current running status. A service may be stopped if the corresponding daemon or script is not enabled. An example is shown below:



Services

CRON Server	RUNNING
Cwatch Analyser	STOPPED
Cwatch Ces	STOPPED
DHCP Server	STOPPED
DNS Proxy Server	RUNNING
Intrusion Prevention System	STOPPED
Logging Server	RUNNING
NTP Server	RUNNING
SSLVPN Server	STOPPED
Secure Shell Server	STOPPED
URL Filter	STOPPED
VPN IPSec	STOPPED
Virus Scanner	STOPPED
Web Proxy	STOPPED
Web Server	RUNNING

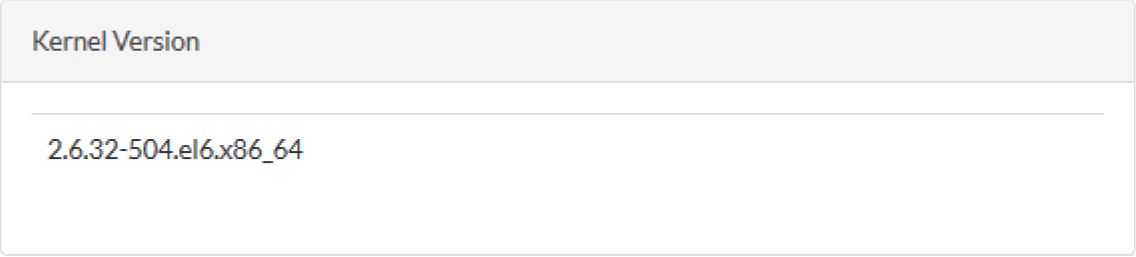
- **Disk Usage -** Shows the hard disk drives/ partitions mounted on the firewall device, their mount path and the space of each disk partition similar to the output of Linux Disk Free (df) command. An example is shown below:



Disk Usage

Device	Mounted on	Size	Used	Free	Percentage
/dev/sda2	/	53G	2.1G	48G	5%
/dev/sda1	/boot	126M	26M	94M	22%
tmpfs	/dev/shm	1.6G	0	1.6G	0%
tmpfs	/tmp	537M	25k	537M	1%
tmpfs	/var/cache	537M	2.0M	535M	1%
tmpfs	/var/lib/collectd	68M	14M	54M	21%
tmpfs	/var/tmp	537M	0	537M	0%

- **Kernel Version -** Shows the version number of the kernel currently used by the firewall device. An example is shown below:



Kernel Version

2.6.32-504.el6.x86_64

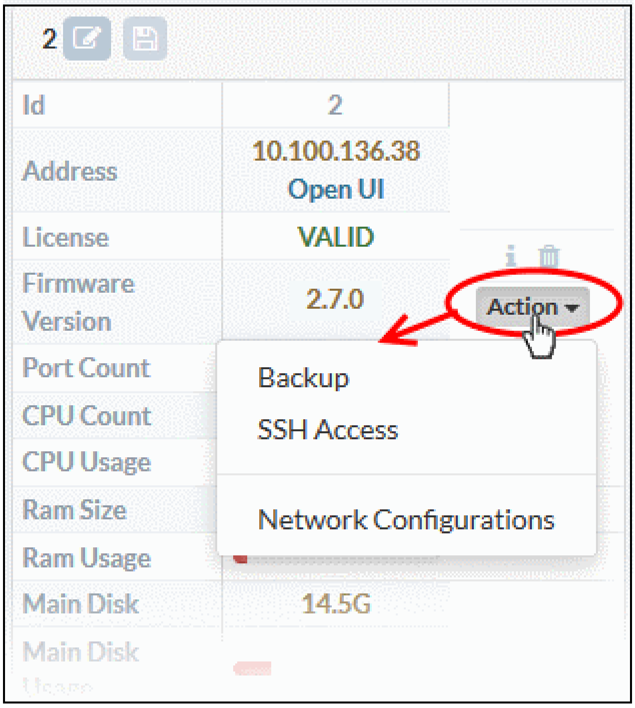
3.2 Quick Actions on a Firewall Device

The 'Action' button on a device tile contains links to important configuration interfaces for the device.

To perform quick actions on a device

- Click 'System' on the left then select 'Dashboard'
- Click the 'Actions' button on the tile of a device

You can configure the following from this menu:



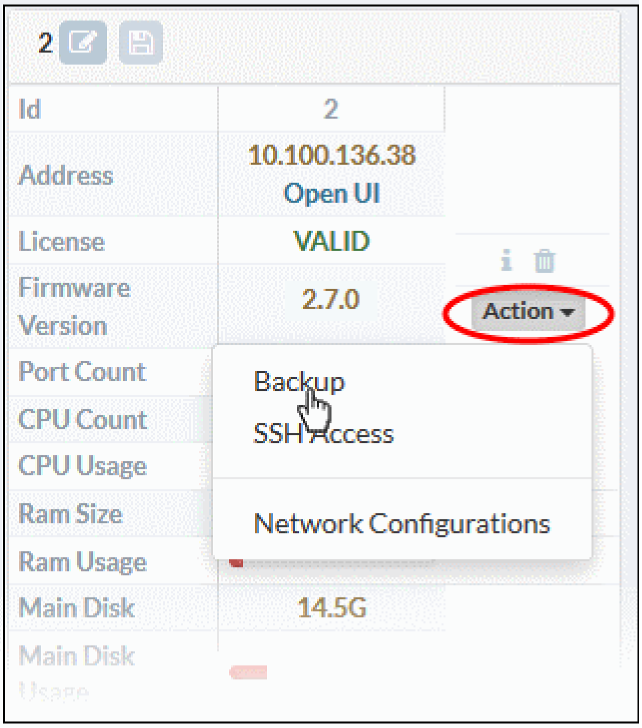
- Backup - Make a copy of the firewall configuration and logs. Restore the device from a saved backup. See **Backup/Restore a Firewall Device** for more details.
- SSH Access - Configure secure shell access to the device. See **Configure SSH Access** for more details.
- Network Configurations - Setup network zone connections to different ports of the device. See **Network Configuration** for more details

3.2.1 Backup/Restore a Firewall Device

- Dome Central Manager allows you to backup the current state of a firewall device at any time. Each backup includes device configuration settings and database dumps.
- The backups are stored on the firewall device itself.
- You can restore the firewall from any saved backup by clicking the 'Restore' button.

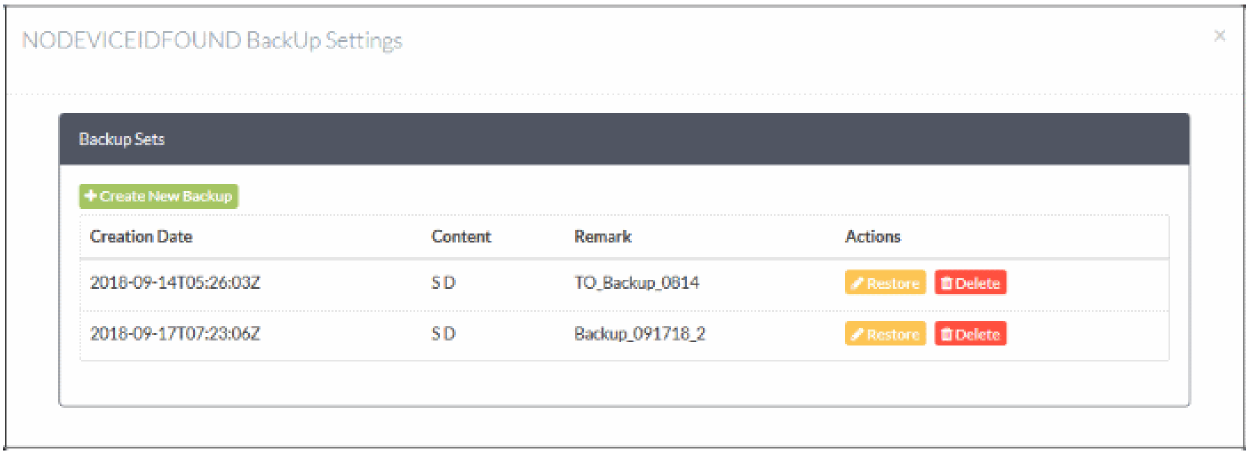
To manage backup and restore operations of a device

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



Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	
CPU Count	
CPU Usage	
Ram Size	
Ram Usage	
Main Disk	14.5G
Main Disk Usage	

- Select 'Backup' from the options



NODEVICEIDFOUND BackUp Settings

Backup Sets

Creation Date	Content	Remark	Actions
2018-09-14T05:26:03Z	S D	TO_Backup_0814	Restore Delete
2018-09-17T07:23:06Z	S D	Backup_091718_2	Restore Delete

The backup settings interface lists any previously created backups and allows you to create a new backup.

- The list only shows backup sets created via the central manager interface. Backups created on the firewall device itself are not listed.

<table>
<tr><th colspan="2">Backup Sets - Column Descriptions</th></tr>
<tr><th>Column Header</th><th>Description</th></tr>
<tr><td>Creation date</td><td>Date and time at which the backup was created.</td></tr>
<tr><td>Content</td><td>Shows the components of the backup
<table>
<tr><th>Character</th><th>Expansion</th><th>Description</th></tr>
<tr><td>D</td><td>Database dumps</td><td>Contains database dumps</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>S</td><td>Settings</td><td>Contains configurations and settings</td></tr></table></td></tr>
<tr><td>Remark</td><td>Comments entered by the administrator during backup creation</td></tr>
<tr><td>Actions</td><td>Restore - Restores the firewall using this backup
Delete - Deletes the backup</td></tr>
</table>

The following sections explain backup tasks in more detail:

- **Create a backup**
- **Rollback a firewall device to a previous time point**

Create a Backup

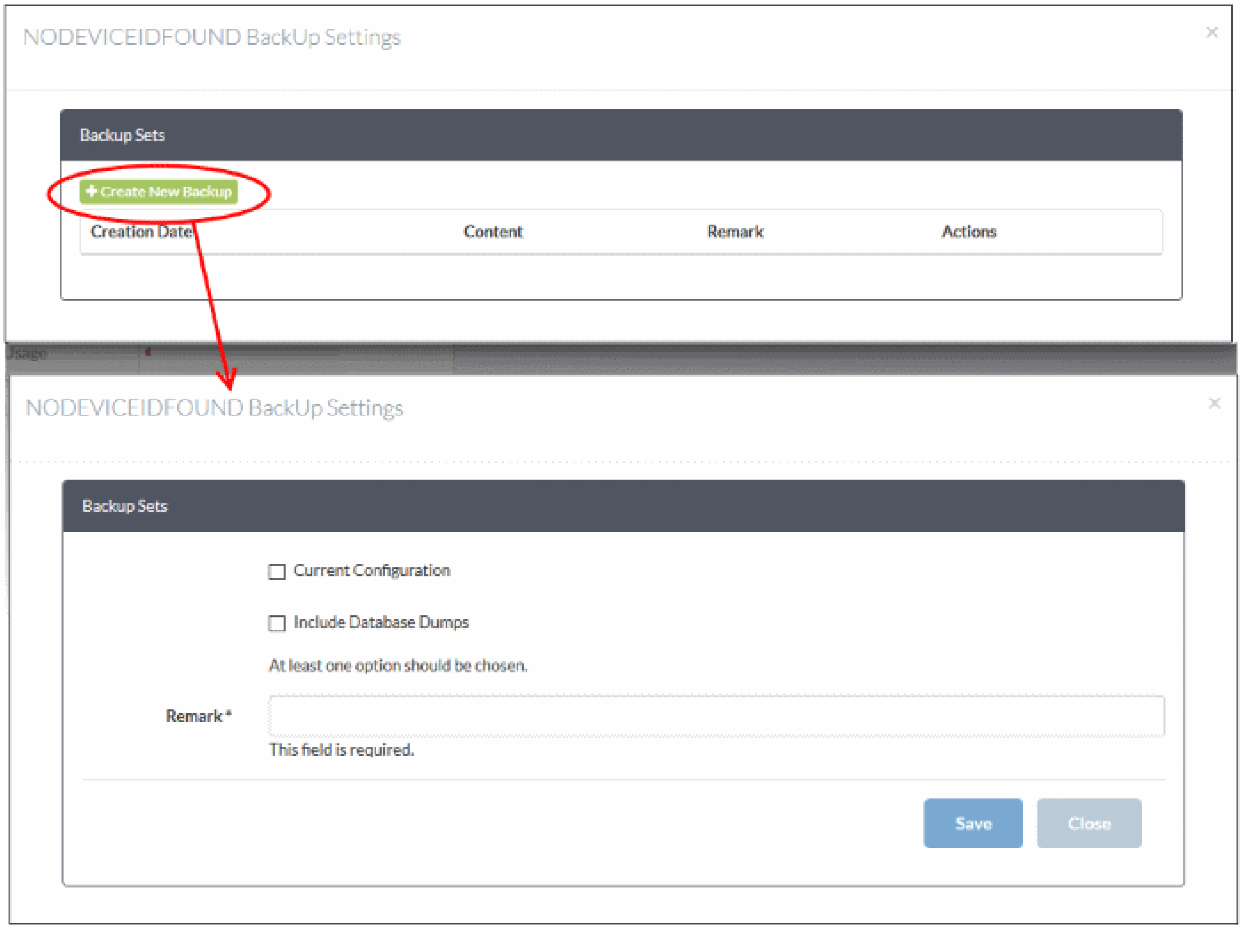
- You can backup the configuration and database dumps of a managed firewall at any time.
- For example, you may wish to do this before making a critical configuration change.
- Backups are stored locally on the firewall device. You can restore devices from a backup as required.

To create a backup of a device

- Click 'System' on the left then select 'Dashboard'
- Click the 'Actions' button on the tile of the device and choose 'Backup'

The backup settings interface will open.

- Click the 'Create New Backup' button



NODEVICEIDFOUND BackUp Settings

Backup Sets

Creation Date	Content	Remark	Actions

NODEVICEIDFOUND BackUp Settings

Backup Sets

□ Current Configuration

□ Include Database Dumps

At least one option should be chosen.

Remark *

This field is required.

- Choose the components you want to include in the backup:
  - Current configuration - Will backup all current firewall settings.
  - Include database dumps - Adds firewall database content and logs to the backup.
- Enter a short description or comment for the backup in the text box. This description will appear in the 'Remark' column in the list of backup archives.
- Click 'Save'.

A command to create the backup will be sent to the device. Once the backup has been created and stored on the device, it will be listed in the 'Backup Sets' interface.

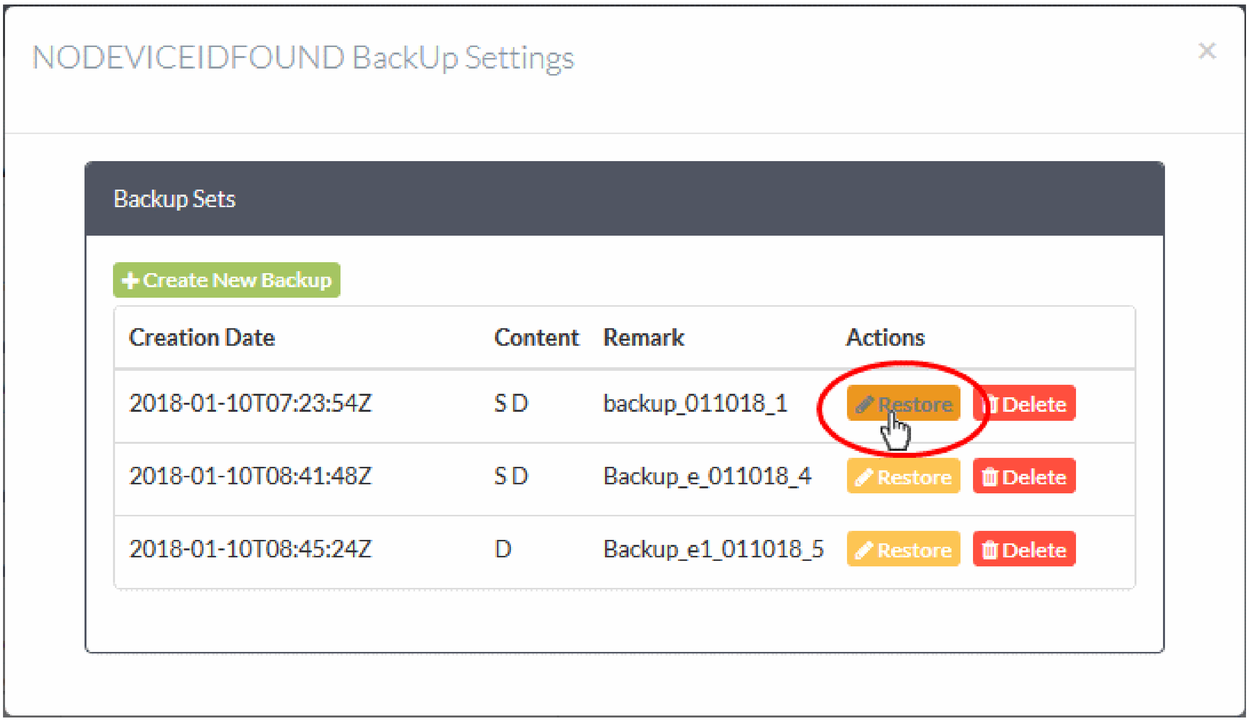
Rollback a Firewall Device to a Previous Time Point

Backup archives allow you to rollback a firewall to a previous state if you encounter issues with your current configuration. The firewall will automatically restart after you have restored from a backup.

To restore a backup

- Click 'System' on the left then select 'Dashboard'
- Click the 'Actions' button on the tile of the device and choose 'Backup'

The backup settings interface will open with a list of available archives:



NODEVICEIDFOUND BackUp Settings

Backup Sets

Creation Date	Content	Remark	Actions
2018-01-10T07:23:54Z	S D	backup_011018_1	Restore Delete
2018-01-10T08:41:48Z	S D	Backup_e_011018_4	Restore Delete
2018-01-10T08:45:24Z	D	Backup_e1_011018_5	Restore Delete

- Click the 'Restore' button Restore in the row of the required backup archive.
- After the restore operation is complete, the device will restart with the configuration as per the backup contents.

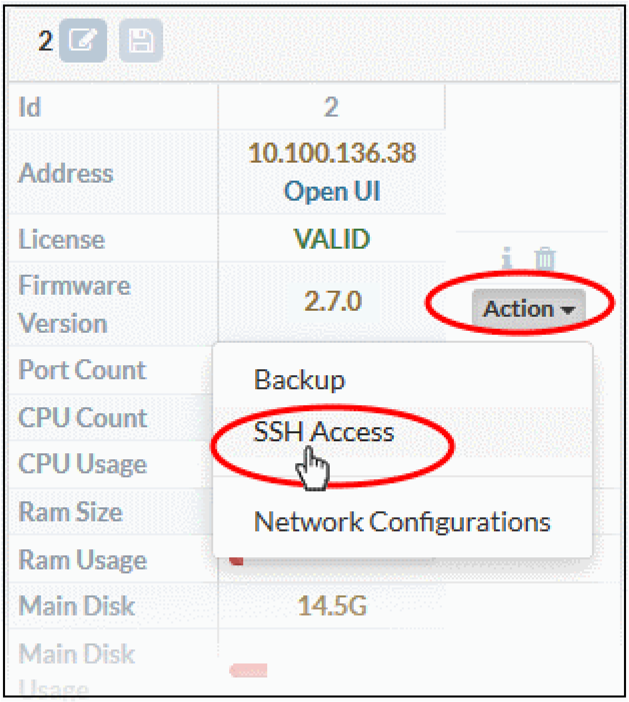
3.2.2 Configure SSH Access for a Firewall Device

- SSH connections let you provide access to managed firewalls from clients in external networks.

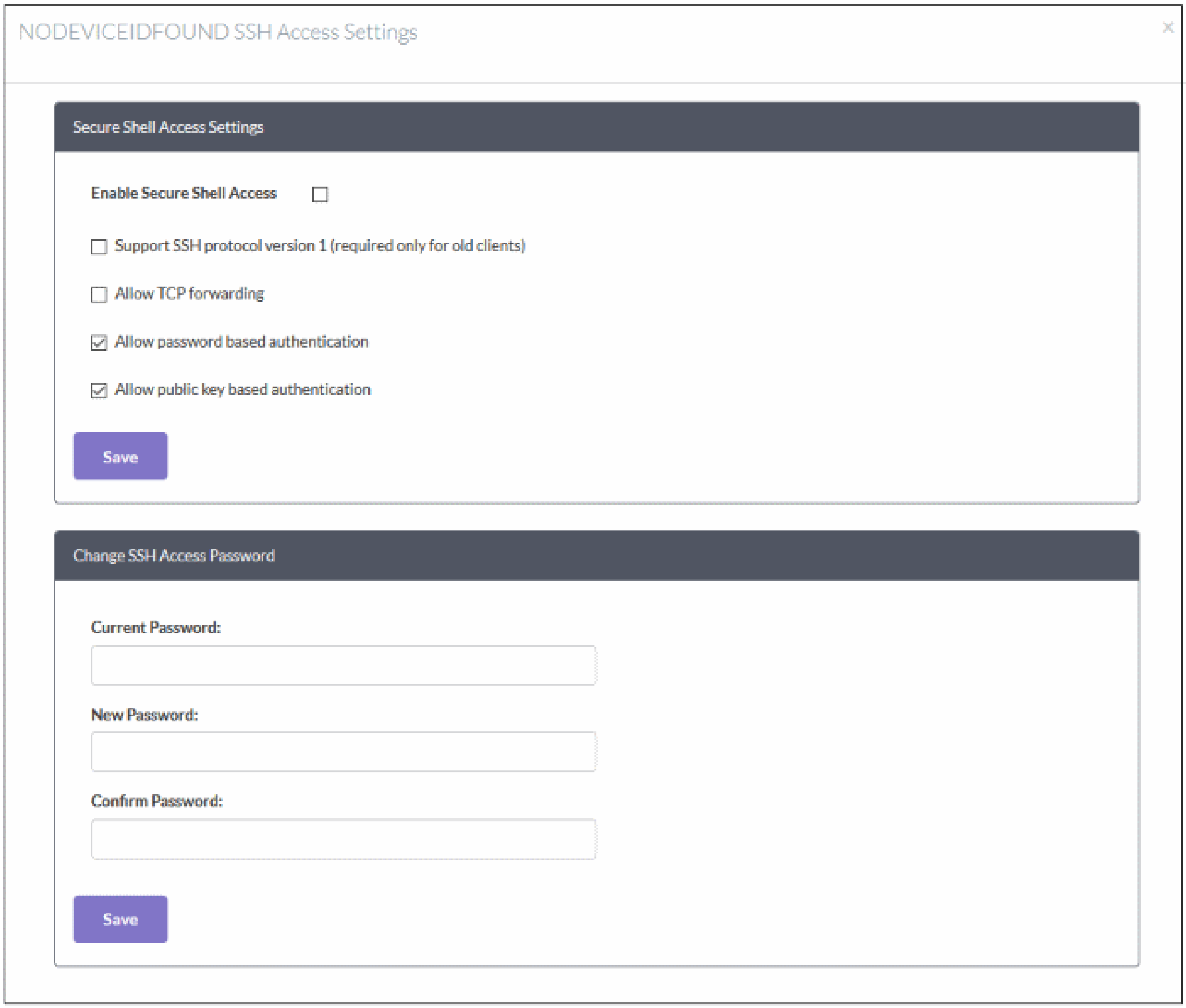
Note: SSH grants access to important information and configuration data which are inaccessible via Dome Firewall's GUI interfaces. Administrators should provide SSH access and authorization with caution.

To enable and configure SSH access for a firewall device

- Click 'System' on the left then select 'Dashboard'
- Click the 'Actions' button on the tile of the device
- Choose 'SSH Access' from the options



The 'SSH Access Settings' dialog for the device will appear.



NODEVICEIDFOUND SSH Access Settings

Secure Shell Access Settings

Enable Secure Shell Access □

□ Support SSH protocol version 1 (required only for old clients)

□ Allow TCP forwarding

☑ Allow password based authentication

☑ Allow public key based authentication

Change SSH Access Password

Current Password:

New Password:

Confirm Password:

Secure Shell Access Settings - Table of Parameters	
Forrn Element	**Description**
Enable Secure Shell Access	Allow or deny SSH access to the firewall device.
Support SSH protocol version 1 (required only for old clients)	Select this option only if you are using old SSH client that do not support the newer versions of the SSH protocol.
Allow TCP forwarding	Select this option to allow other protocols like TCP to tunnel through SSH.
Allow password based authentication	Select this option if you plan to use password authentication for admins who login to the management console over SSH.
Allow public key based authentication	Select this option if you plan to use public key type authentication for admins who login to the management console over SSH.. As a prerequisite, The public keys need to be added to the file /root/.ssh/authorized_keys.

- Select the required options and click 'Save' for your settings to be applied to the device.

Change SSH Access Password - Table of Parameters	
Forrn Element	**Description**
You can change the password for SSH access from external network.	
Current Password	Enter the currently used password for the administrator account to login to the shell for administration.
New Password: and Confirm Password	Enter the new password to replace the current password and re-enter the same in the 'Confirm Password' field. Note: The new password should be at least eight characters long and could not be easily guessed. They should contain a mixture of upper and lower case letters, numbers and special characters.

- Enter the old and new passwords and click 'Save'.

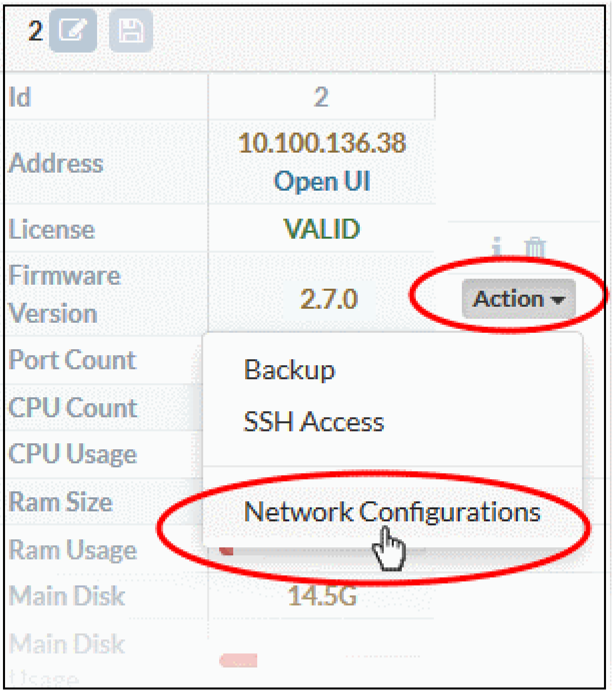
Your settings will be applied to the device.

3.2.3 Network Configuration

- 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 configuration screen depends on the number of adapters on the FW device. These ports will be shown as Port 2, Port 3, Port 4 etc.
- The central manager console lets you view and manage the connection used by each device port.
  - For help to add interfaces, see Add Interfaces.

To view and manage the network connections

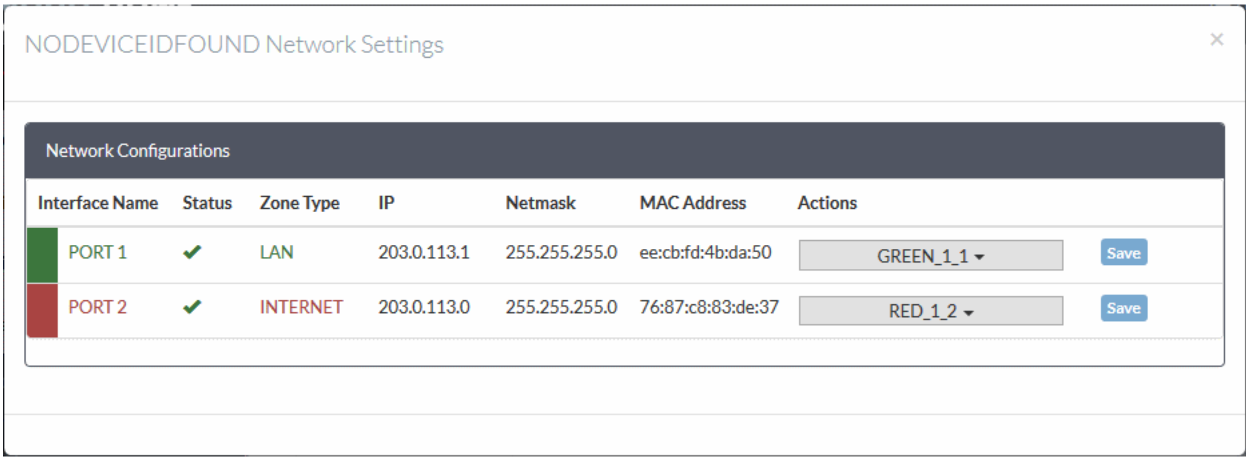
- Click 'System' on the left then select 'Dashboard'
- Click the 'Actions' button on the tile of the device



Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	
CPU Count	
CPU Usage	
Ram Size	
Ram Usage	
Main Disk	14.5G
Main Disk Usage	

- Choose 'Network Configurations' from the options

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



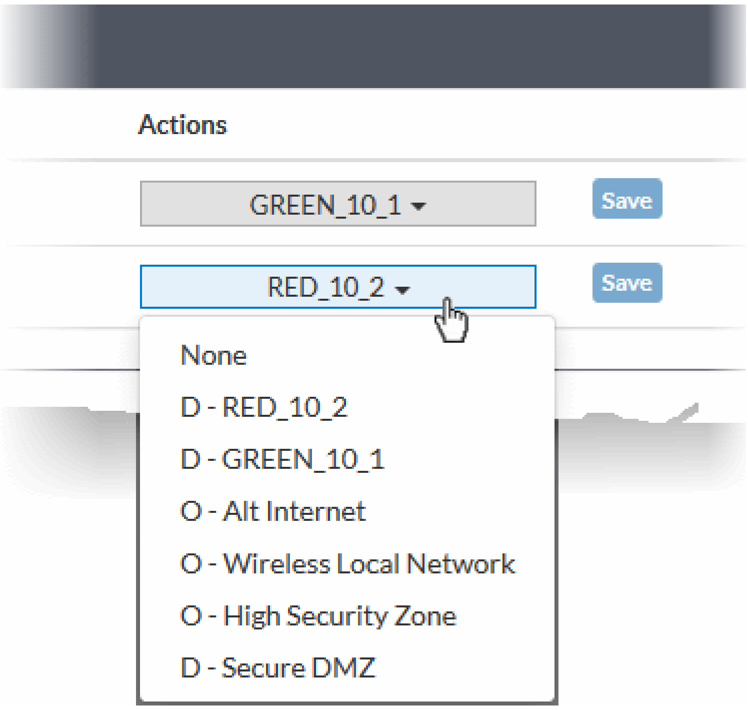
NODEVICEIDFOUND Network Settings

Network Configurations

Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions	
🟩 PORT 1	✓	LAN	203.0.113.1	255.255.255.0	ee:cb:fd:4b:da:50	GREEN_1_1 ▾	Save
🟥 PORT 2	✓	INTERNET	203.0.113.0	255.255.255.0	76:87:c8:83:de:37	RED_1_2 ▾	Save

Network Configurations - Column Descriptions	
Column Header	**Description**
Interface Name	Name of the Dome Firewall port. The font color indicates the type of network zone to which the port is connected. Red - External networks, like WAN, for internet connection Yellow - DMZ zone Green - Local Area Network to which workstations are connected Blue - Wi-Fi network
Status	Link status of the network zone interface. The status can be one of the following: Green Tick - Link is active Red Cross - The link is not active Question Mark - No information about the link from the device driver

Network Configurations - Column Descriptions

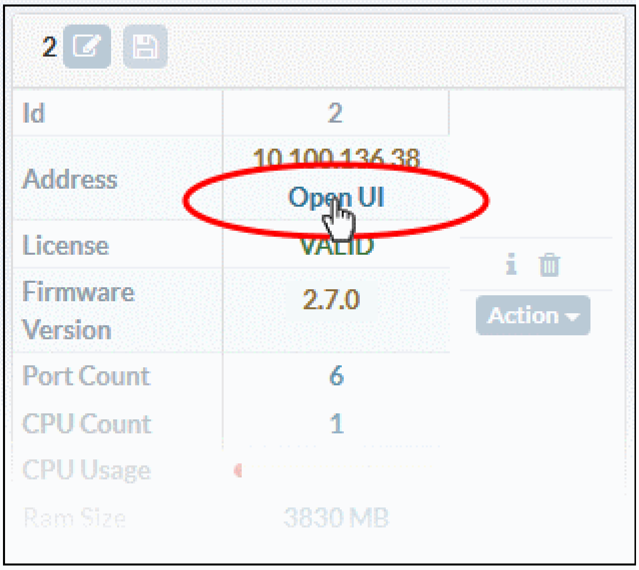
Column Header	Description
Zone Type	The network zone type of the interface. The network zone can be one of the following: • Internet • LAN • Wi-Fi • DMZ
IP	The IP address of the network zone interface connected to the port.
Netmask	The netmask of the network zone connected through the interface
MAC Address	The Media Access Control (MAC) address of the interface
Actions	Displays the name of the network zone interface currently connected to the port. You can change the interface by selecting an option from the drop-down.  Actions GREEN_10_1 Save RED_10_2 Save None D - RED_10_2 D - GREEN_10_1 O - Alt Internet O - Wireless Local Network O - High Security Zone D - Secure DMZ The drop-down will display the interfaces defined at the firewall device and the central manager. • Select the interface and click 'Save' **Notes:** • The interfaces can be added for organizations/devices to the central manager from the 'Interfaces' screen. See **Add Interfaces** for more details. • The interfaces defined for an organization will be available for all devices of that organization (with a prefix 'O' in the interface name) • The interfaces defined for an individual firewall device will be available only for that device. (with a prefix 'D' in the interface name)

3.3 Access Admin Console of a Firewall Device

You can remotely access the admin console of a managed firewall from the central manager interface.

To open the administrative web console of a managed firewall device

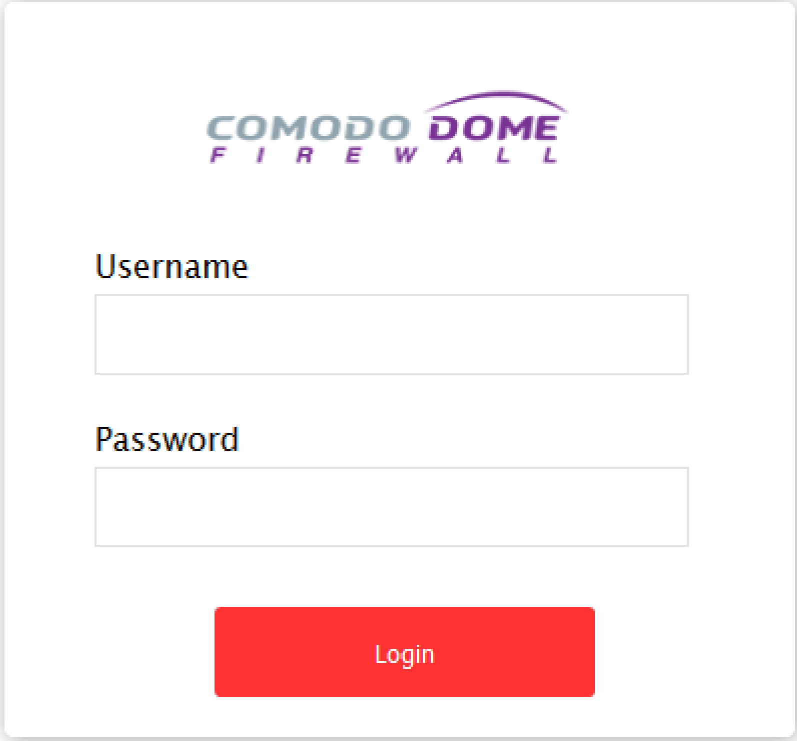
- Click 'System' in the left-hand menu then select 'Dashboard'
- Click the 'Open UI' link in the 'Address' field on the tile of the device



2

Id	2
Address	10.100.136.38 Open UI
License	VALID
Firmware Version	2.7.0
Port Count	6
CPU Count	1
CPU Usage	
Ram Size	3830 MB

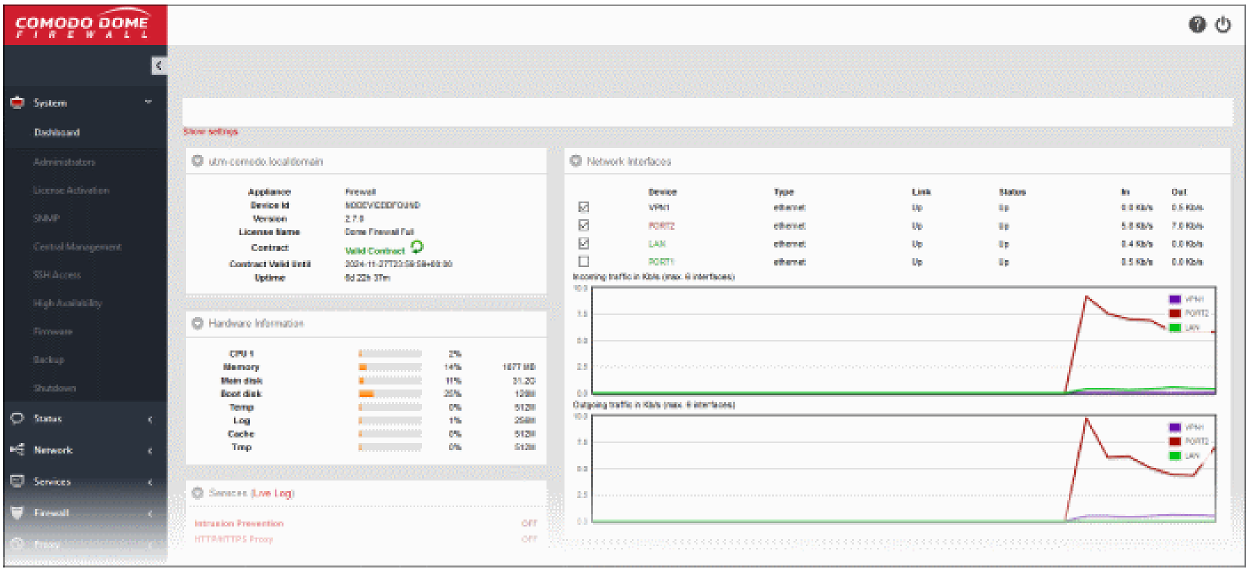
Enter the username and password for the firewall device :



Username

Password

The device admin console will open:



utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.7.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2024-11-27T23:59:59+00:00
Uptime	6d 22h 37m

Hardware Information

CPU 1	2%	
Memory	14%	1677 MB
Main disk	11%	31.2G
Boot disk	25%	128M
Temp	0%	512M
Log	1%	256M
Cache	0%	512M
Tmp	0%	512M

Services (Live Log)

Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

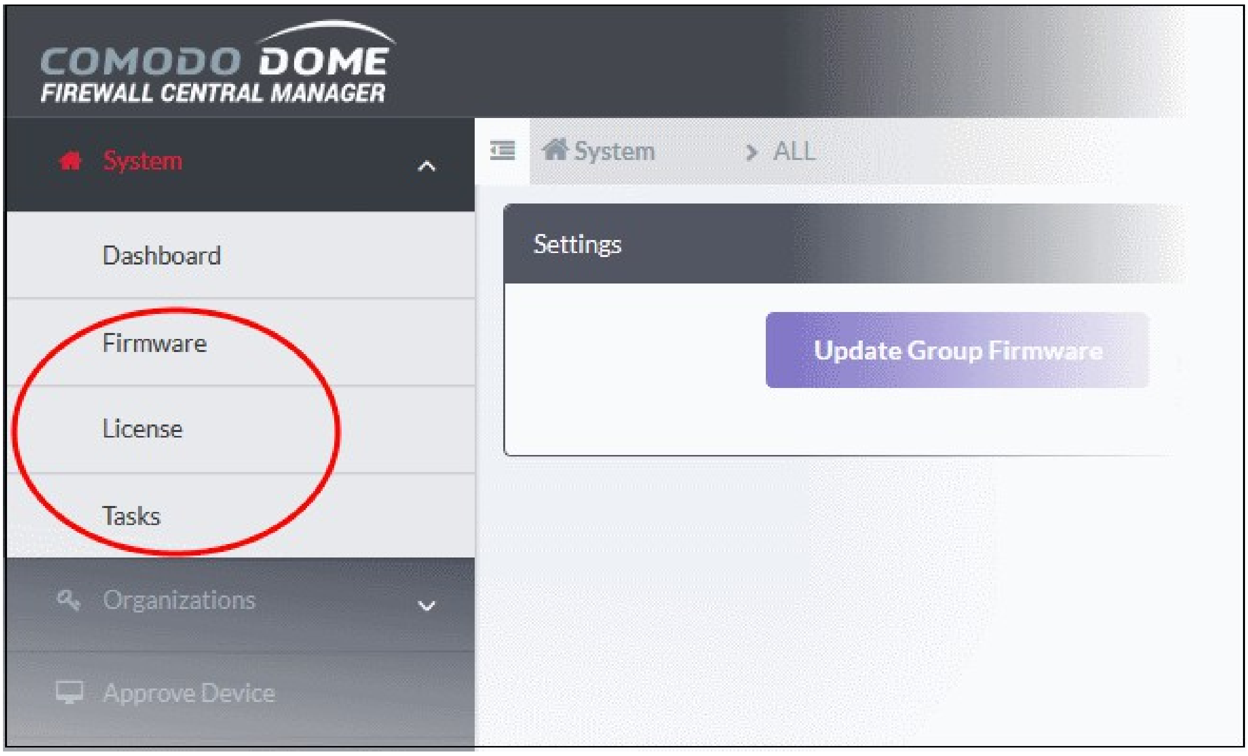
Network Interfaces

	Device	Type	Link	Status	In	Out
☑	VPN1	ethernet	Up	Up	0.0 Kb/s	0.5 Kb/s
☑	PORT2	ethernet	Up	Up	5.0 Kb/s	7.0 Kb/s
☑	LAN	ethernet	Up	Up	0.4 Kb/s	0.0 Kb/s
□	PORT1	ethernet	Up	Up	0.5 Kb/s	0.0 Kb/s

- You can configure the remote firewall as required.
- See Dome Firewall guide at **https://help.comodo.com/topic-451-1-936-12755-Introduction-to-Comodo-Dome-Firewall---Virtual-Appliance.html** for help to configure and manage a firewall device.

4 Manage System Status and General Configuration

The 'System' menu lets you update the firmware of managed firewalls, view and upgrade licenses, and view tasks executed by the central manager on managed firewalls.



See the following sections for more details:

- **Update Firmware Version**
- **View and Upgrade Central Manager License**
- **View Management Tasks**

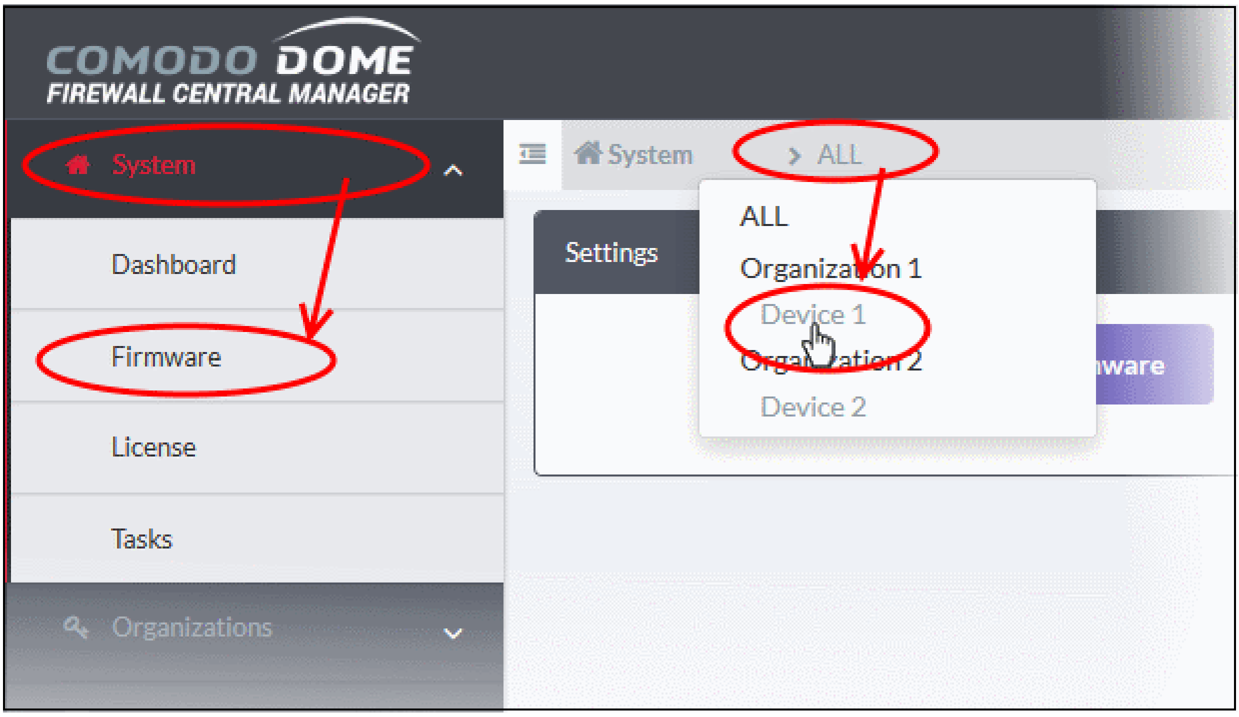
4.1 Update Firmware Version

The firmware settings interface allows you to:

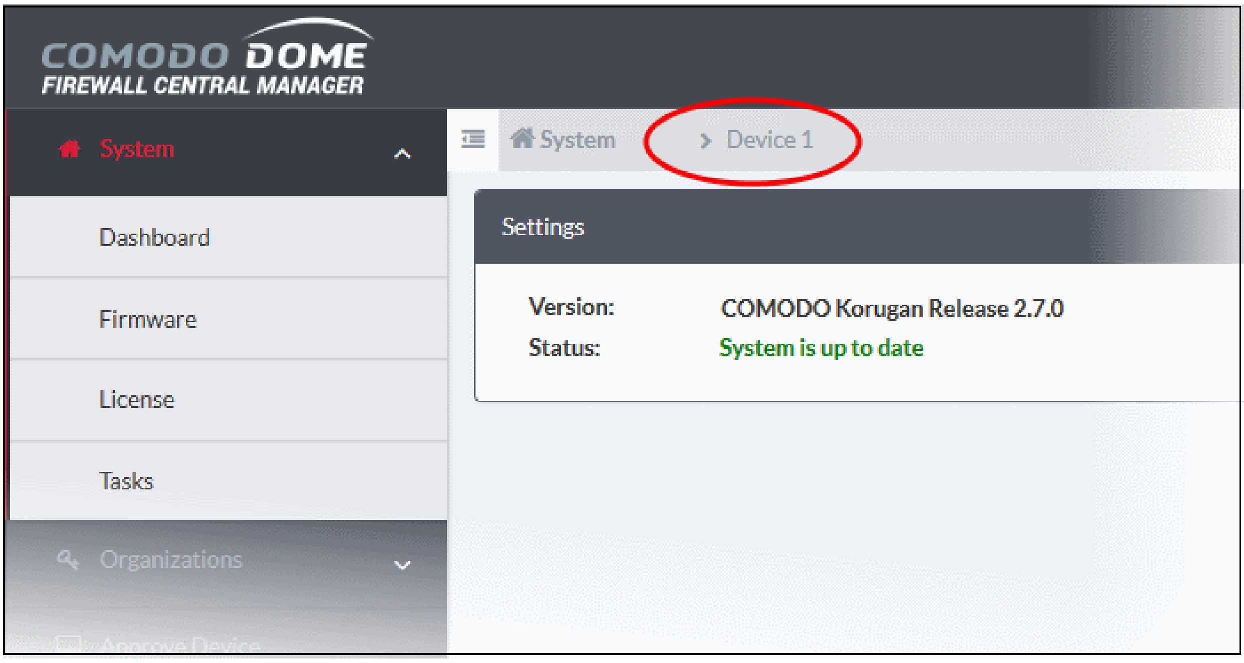
- View firmware version installed on each firewall device and update the firmware if required.
- Send an update command to every device, or only to devices associated with a specific organization. All devices with older firmware versions will be updated.

To view and update firmware on individual devices

- Click 'System' on the left then select 'Firmware'
- Select the 'Device' under the required 'Organization' from the drop-down at the title bar



The details of the currently installed firmware on the selected device will appear in the right pane.



Version: COMODO Korugan Release 2.7.0

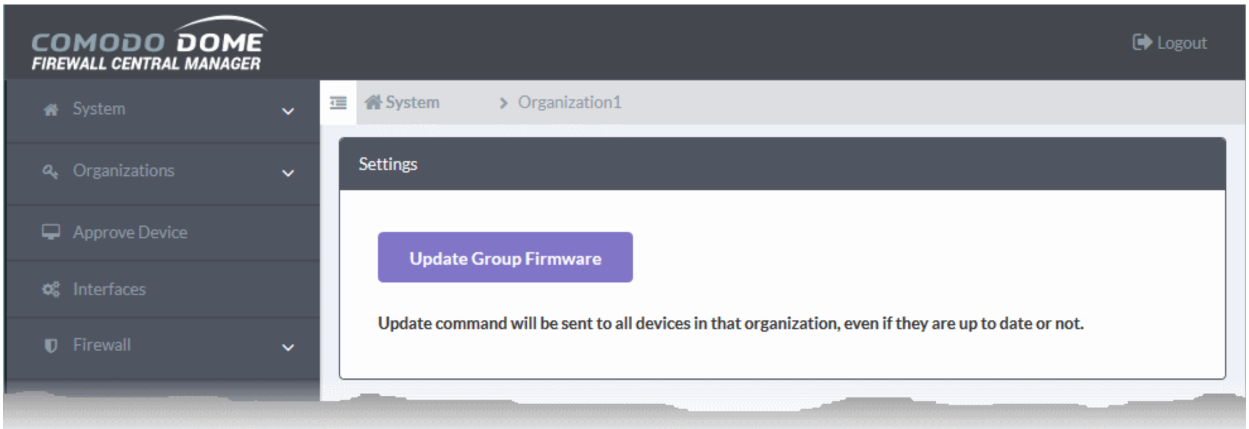
Status: System is up to date

- **Version** - Shows the version number of the Comodo Dome Firewall Firmware installed on the selected device.
- **Status** - Indicates whether your firmware is up-to-date. If it indicates 'System must be updated', you can initiate the update process by clicking the 'Update Firmware' button. The firmware will be automatically downloaded and installed.

To upgrade the firmware version on a group of firewall devices

- Click 'System' on the left then select 'Firmware'
- Select the group of devices to be updated
    - Select 'ALL' from the drop-down at the title bar to update firmware on all managed devices at-once.

- Select the 'Organization' from the drop-down at the title bar to update only group of devices belonging to the organization.



Update command will be sent to all devices in that organization, even if they are up to date or not.

- Click the 'Update Group Firmware' button
- The command can be sent to all devices in the group at once.
- On receiving the command, devices with an older version of Dome Firewall firmware will automatically download and install the latest version.

4.2 View and Upgrade Central Manager License

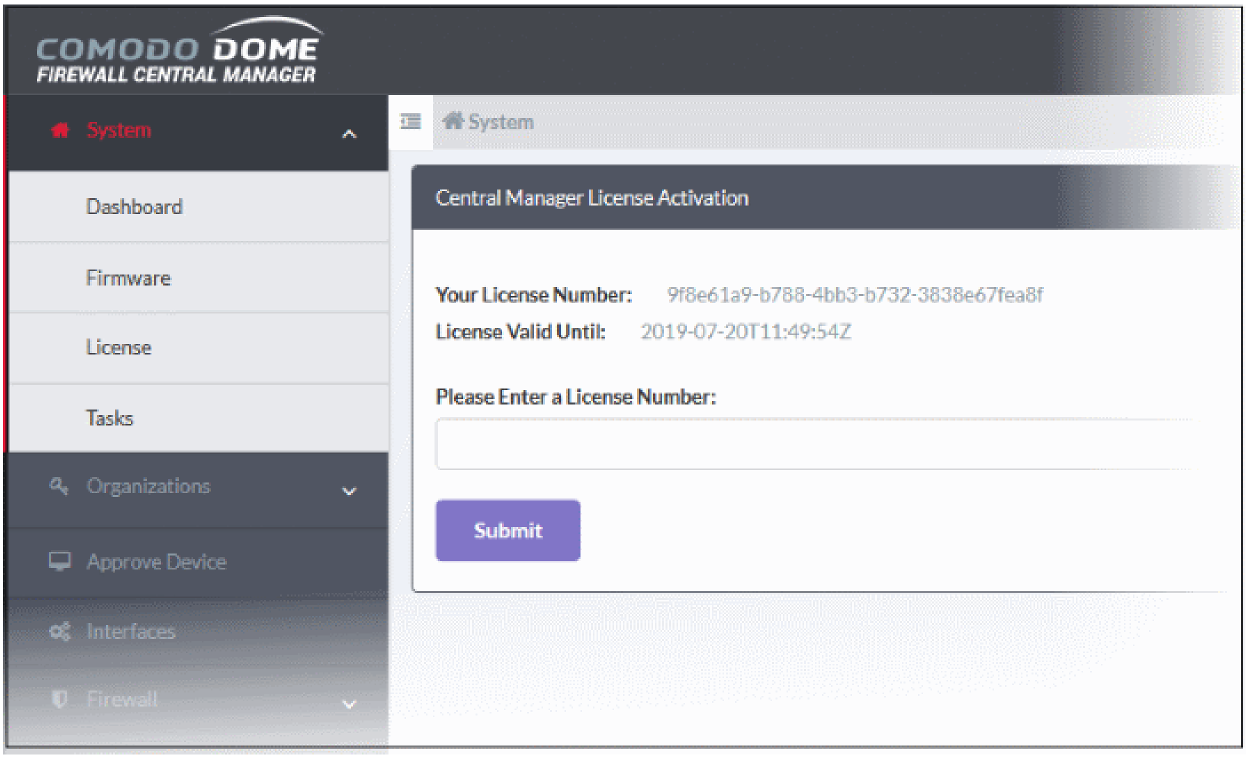
You can view and upgrade your license when it is nearing expiry from the 'Central Manager License Activation' interface.

Note: New licenses can be purchased from the Comodo One / Comodo Dragon / ITarian console or Comodo Accounts Manager. For more details, see **Sign-up for Firewall Central Manager License**.

To view and manage licenses

- Click 'System' on the left then select 'License'

The 'Central Manager License Activation' interface will open, with your existing license details.



Central Manager License Activation

Your License Number: 9f8e61a9-b788-4bb3-b732-3838e67fea8f

License Valid Until: 2019-07-20T11:49:54Z

Please Enter a License Number:

The right pane shows your current Dome Firewall CM license key and its expiry date.

- To upgrade or renew you license, paste the new license key in the text box under 'Please Enter a License Number' and click 'Submit'.
- The license will be verified and if found valid, it will be activated.

4.3 View Management Tasks

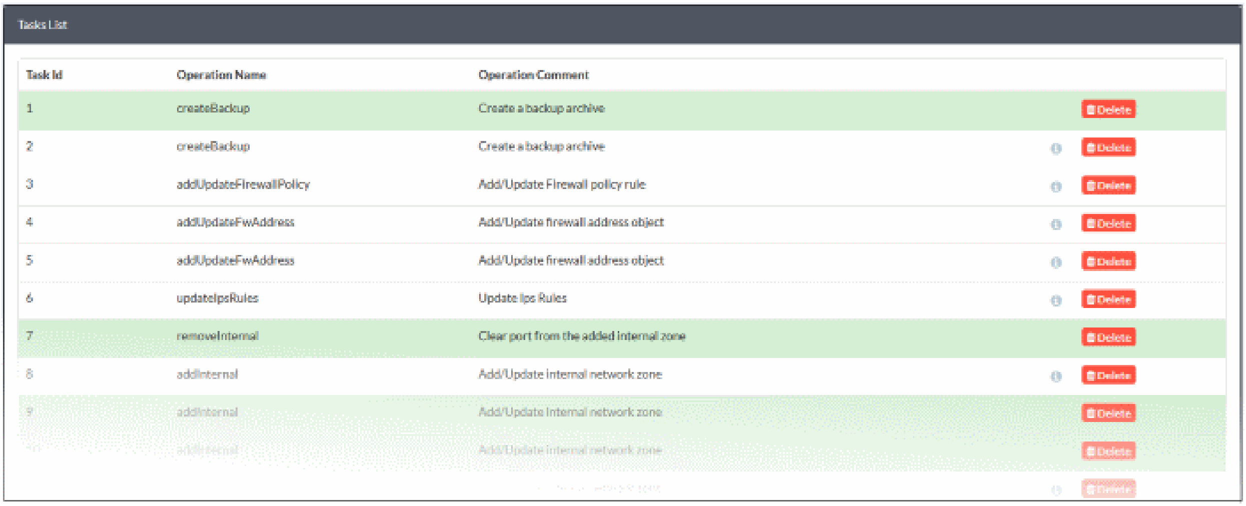
The 'Tasks List' interface shows configuration and management actions executed by the central manager on managed devices.

- Central Manager first executes a test (or dry run) of each action on target devices.
- The action is only committed to a device if the test run is successful.
- You can view error messages in the information dialog of the action.

To view the list of actions

- Click 'System' on the left then select 'Tasks'

The 'Tasks List' will open on the right pane.



Tasks List

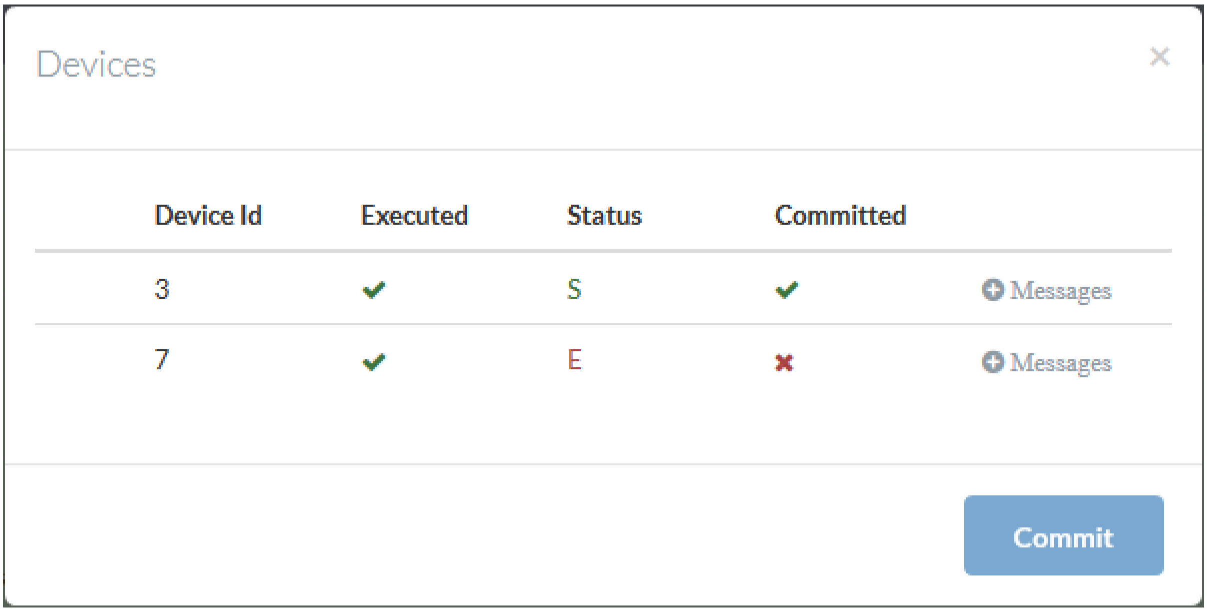
Task Id	Operation Name	Operation Comment		
1	createBackup	Create a backup archive		Delete
2	createBackup	Create a backup archive	ⓘ	Delete
3	addUpdateFirewallPolicy	Add/Update Firewall policy rule	ⓘ	Delete
4	addUpdateFwAddress	Add/Update firewall address object	ⓘ	Delete
5	addUpdateFwAddress	Add/Update firewall address object	ⓘ	Delete
6	updateIpsRules	Update Ips Rules	ⓘ	Delete
7	removeInternal	Clear port from the added internal zone		Delete
8	addInternal	Add/Update internal network zone	ⓘ	Delete
9	addInternal	Add/Update Internal network zone		Delete
10	addInternal	Add/Update internal network zone		Delete

- Green background - Actions that passed the test run on all target devices and successfully committed on those devices.
- White background - Actions that failed the test run on some of the target devices and hence not committed on those devices.. You can recommit these actions to be applied on those devices bypassing the test run. See **Manually Committing Actions on Selected Devices** for more details.

Tasks List - Column Descriptions		
Column Header		**Description**
Task ID		The identification number assigned to the action by Central Manager
Operation Name		Indicates the action executed
Operation Comment		A short description of the action
Controls	Info ⓘ	Clicking the Info icon opens the list of devices on which the action was applied and executed. You can view the status of execution and recommit the action pending on some devices. See **View Details of an Action** for more details.
	Delete	Removes the entry from the list. See **Remove Tasks from Tasks List** for more details.

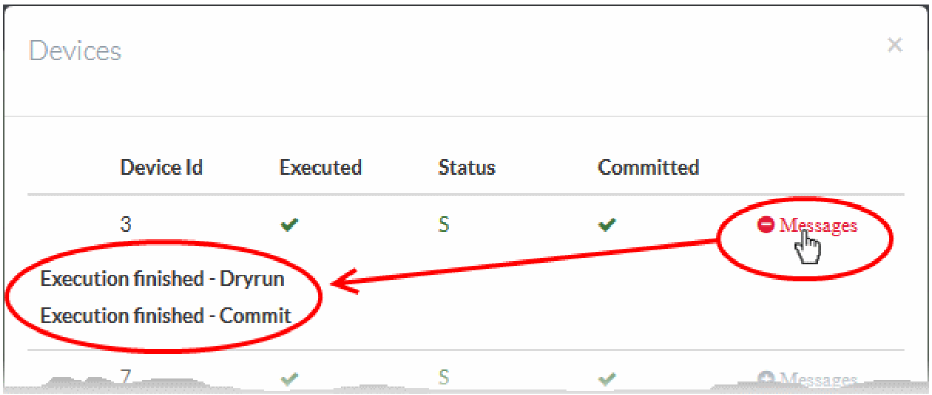
View Details of an Action

- Click the information icon ⓘ to open the list of devices on which the action was applied and their statuses



Devices

Device Id	Executed	Status	Committed	
3	✓	S	✓	Messages
7	✓	E	✗	Messages

Devices List - Column Descriptions		
Column Header		**Description**
Device Id		The identification number assigned to the firewall device by the central manager
Executed		Indicates whether the action was executed a test run on the device
Status		Indicates whether the action passed/failed the test run on the device • S - Successfully executed • E - An error occurred during test run. You can view the error message by clicking the Messages link at the right end of the row.
Committed		Indicates whether the action was successfully applied and completed on the device
Controls	Messages	Click the 'Messages' link to view the error/success messages generated during the test run and the commitment of the action.  Devices Device Id / Executed / Status / Committed 3 ✓ S ✓ Messages Execution finished - Dryrun Execution finished - Commit 7 ✓ S ✓ Messages

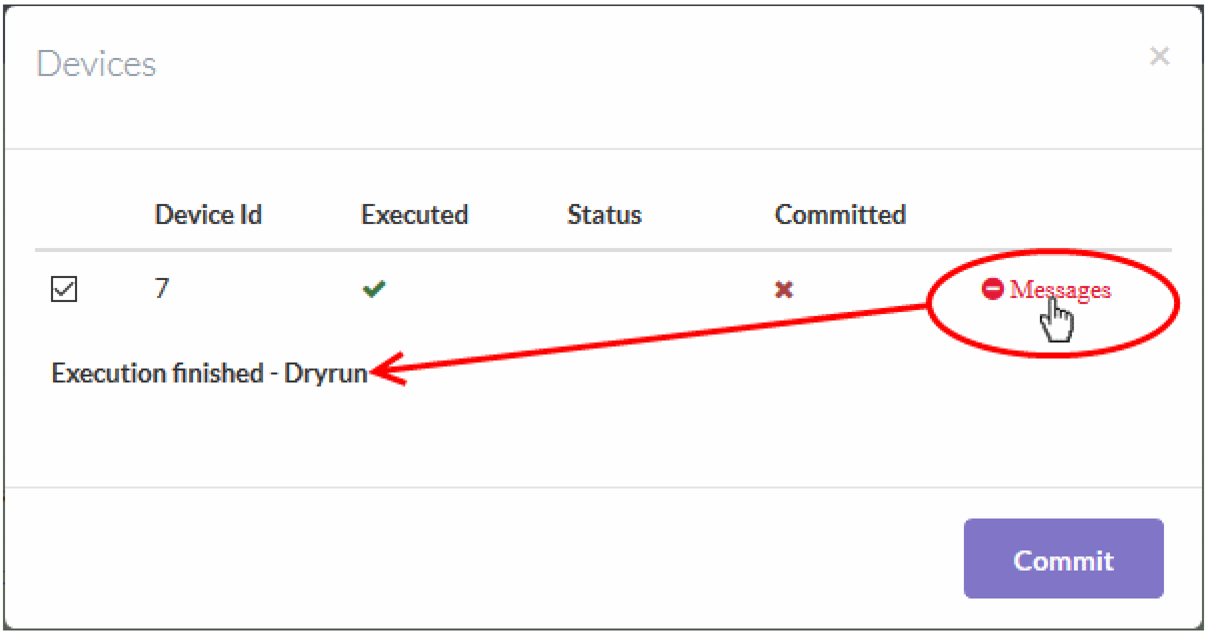
Manually Committing Actions on Selected Devices

The actions that were not completed on all/some devices are displayed with white background in the 'Tasks List' interface. You can reapply the action to those device(s).

- You should first read and analyze the error message generated at the end of the test run
- If the error occurred can be ignored and the action can be applied, you can recommit the action

To re-apply an action on a device

- Click the information icon ℹ in the row of an action with white background to open the list of devices
- Click the 'Messages' link in the row of device on which the action was not completed



Devices

	Device Id	Executed	Status	Committed	
☑	7	✓		✗	Messages

Execution finished - Dryrun

- Analyze message to check the status/error occurred
- Click 'Commit' to re-apply the action

The action will be completed on the device without executing the test run again.

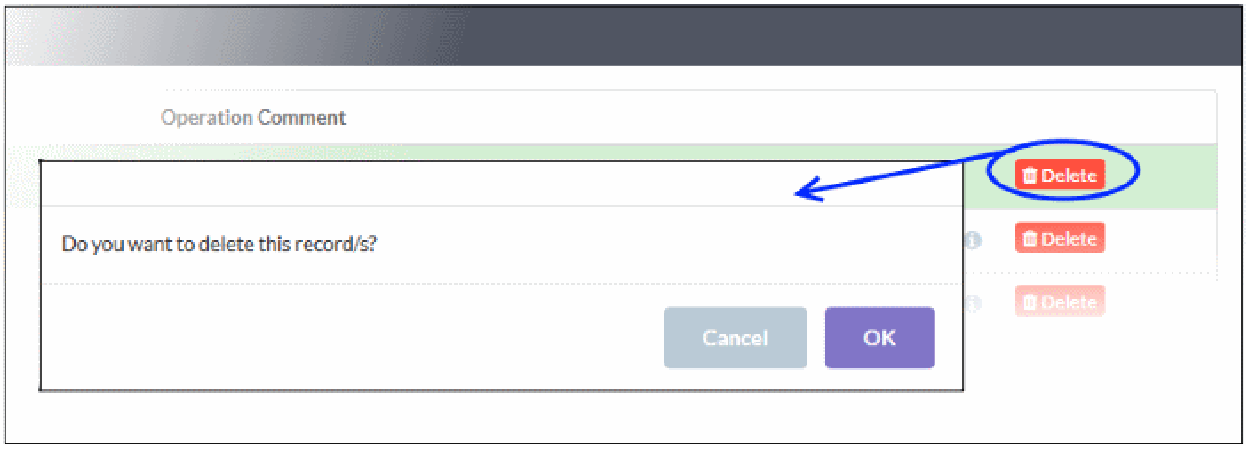
Remove Tasks from Tasks List

You can remove the unwanted and completed action entries from the tasks list.

To remove individual entries

- Click the 'Delete' button at the right end of a row

A confirmation dialog will appear.



Operation Comment

Do you want to delete this record/s?

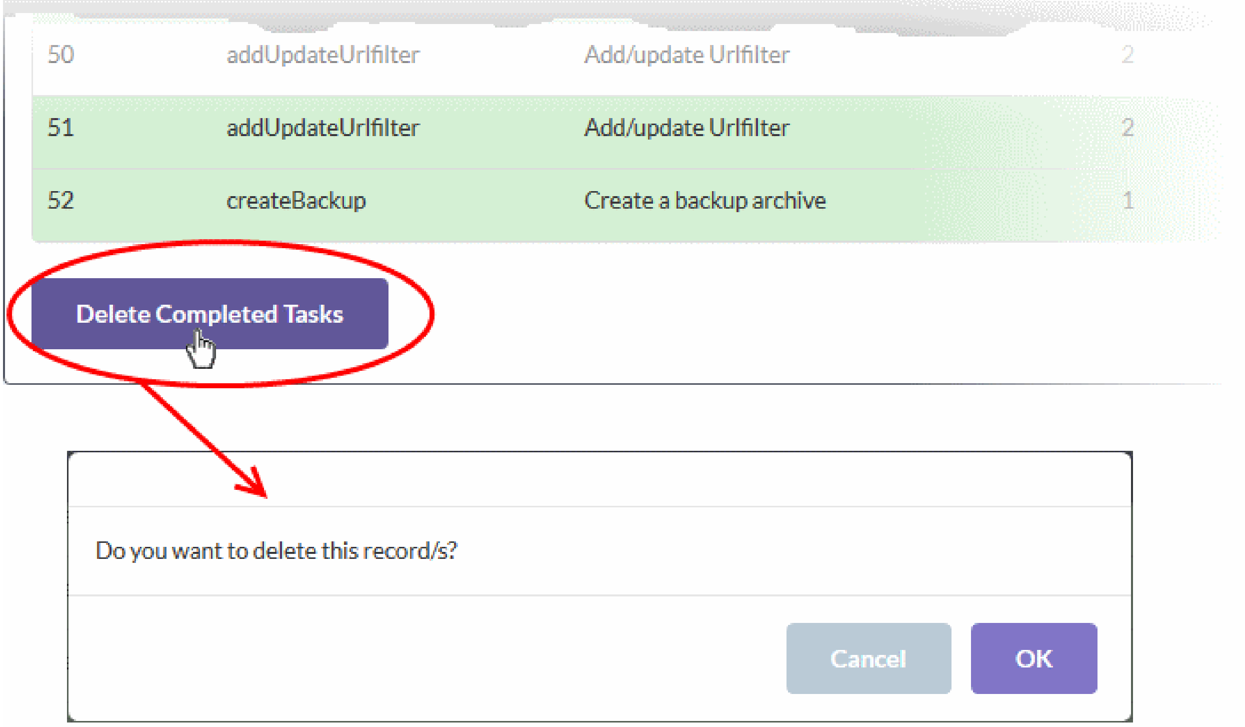
- Click 'OK'

The entry will be removed from the list

- Repeat the process to remove more entries

To remove all completed actions at-once

- Click the 'Delete Completed Tasks' button at the bottom of the 'Tasks List'



50	addUpdateUrlfilter	Add/update Urlfilter	2
51	addUpdateUrlfilter	Add/update Urlfilter	2
52	createBackup	Create a backup archive	1

Do you want to delete this record/s?

- Click 'OK' in the confirmation dialog

All completed actions will be removed from the list.

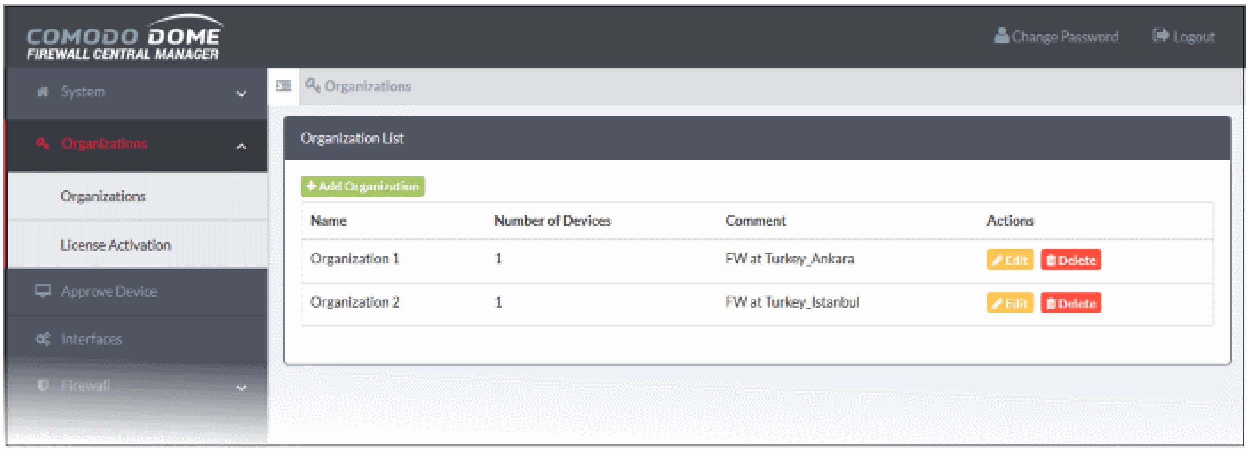
5 Customer Management

An organization is a customer entity, usually a company or business for whom you manage firewall devices.

You can add organizations to the central manager and enroll firewall devices for them.

- Firewall devices can be enrolled by specifying the central manager server address in the firewall's management console. See **Enroll Dome Firewall Devices** for more details.
- Once enrolled, a firewall device has to be approved and assigned to an organization from the central manager console. See **Approve Firewall Device Enrollment** for more details.
- Devices assigned to an organization can be managed as a device group. You can configure firewall policies, Advanced Threat Protection (ATP), URL filters and more for each device/device group.

The 'Organizations' menu lets you add and manage organizations and activate licenses for the managed devices.



Name	Number of Devices	Comment	Actions
Organization 1	1	FW at Turkey_Ankara	Edit Delete
Organization 2	1	FW at Turkey_Istanbul	Edit Delete

See the following sections for more details:

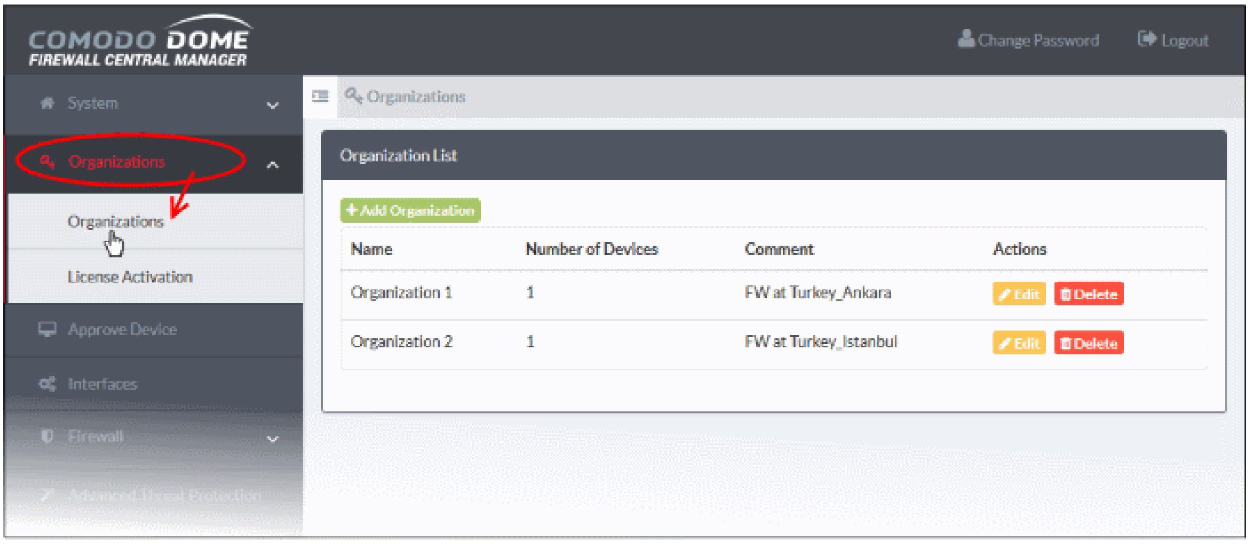
- **Manage Organizations**
- **Activate Firewall Licenses**

5.1 Manage Organizations

- Click 'Organizations' on the left then select 'Organizations'
- This area lets you add and update customer organizations for whom you manage firewall devices.
- After adding an organization, you can assign devices to it in the 'Approve Device' interface.

Note:

- Comodo One / Comodo Dragon / ITarian organizations are NOT imported into Comodo firewall central manager.
- You must add organizations separately to the firewall central manager. You may, of course, use the same organization names to make identification easier.



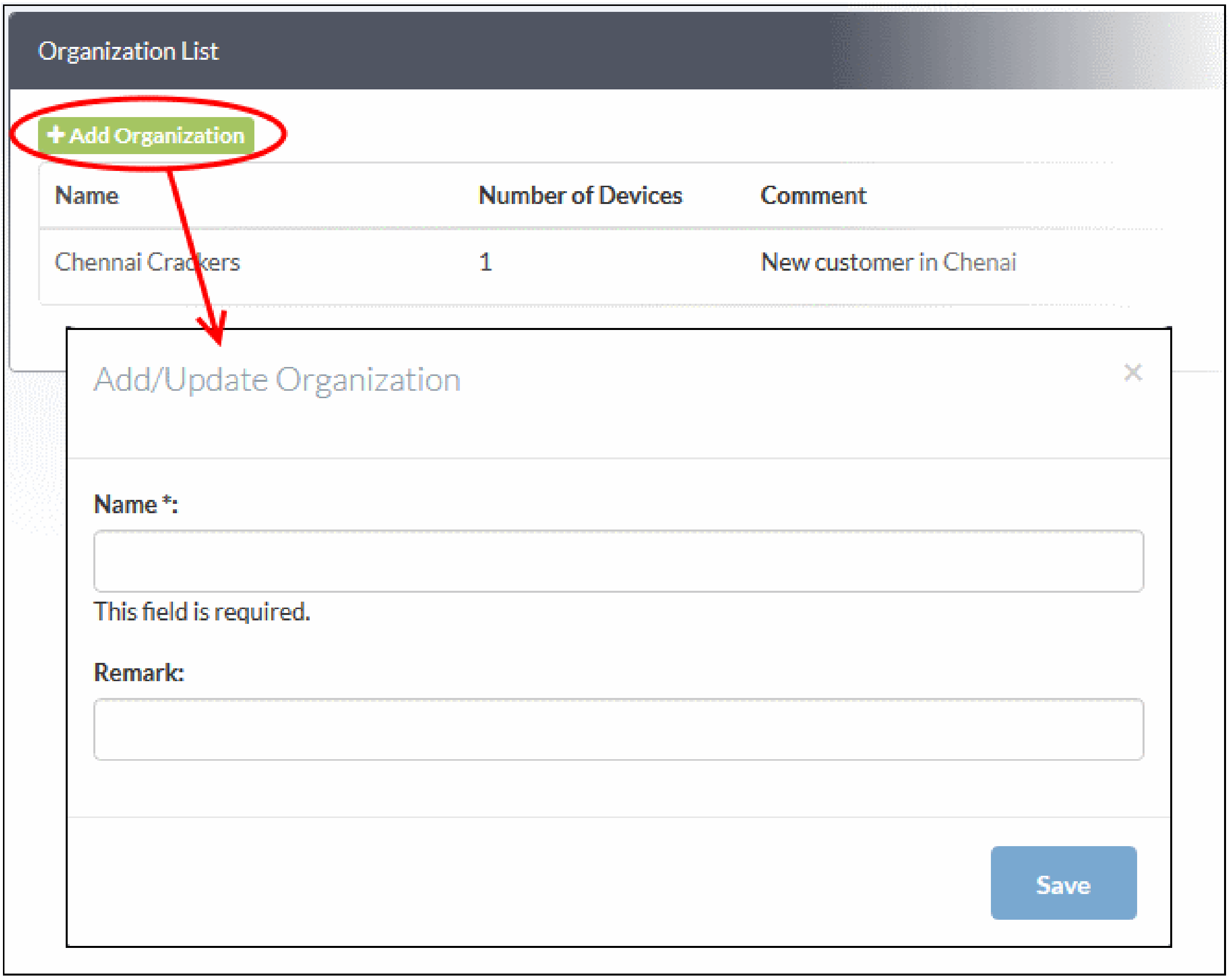
Name	Number of Devices	Comment	Actions
Organization 1	1	FW at Turkey_Ankara	Edit Delete
Organization 2	1	FW at Turkey_Istanbul	Edit Delete

Organization List - Column Descriptions		
Column Header		**Description**
Name		The name of the organization / company
Number of Devices		The number of devices enrolled and assigned to the organization.
Comment		A brief description of the organization entered as remark when creating/editing the organization.
Actions	Edit	Modify organization details.
	Delete	Remove an organization from central manager

Add Organizations

- Click 'Organizations' > 'Organizations' on the left

- Click 'Add Organization' on the top left of the interface



Organization List

Name	Number of Devices	Comment
Chennai Crackers	1	New customer in Chenai

Add/Update Organization

Name *:

This field is required.

Remark:

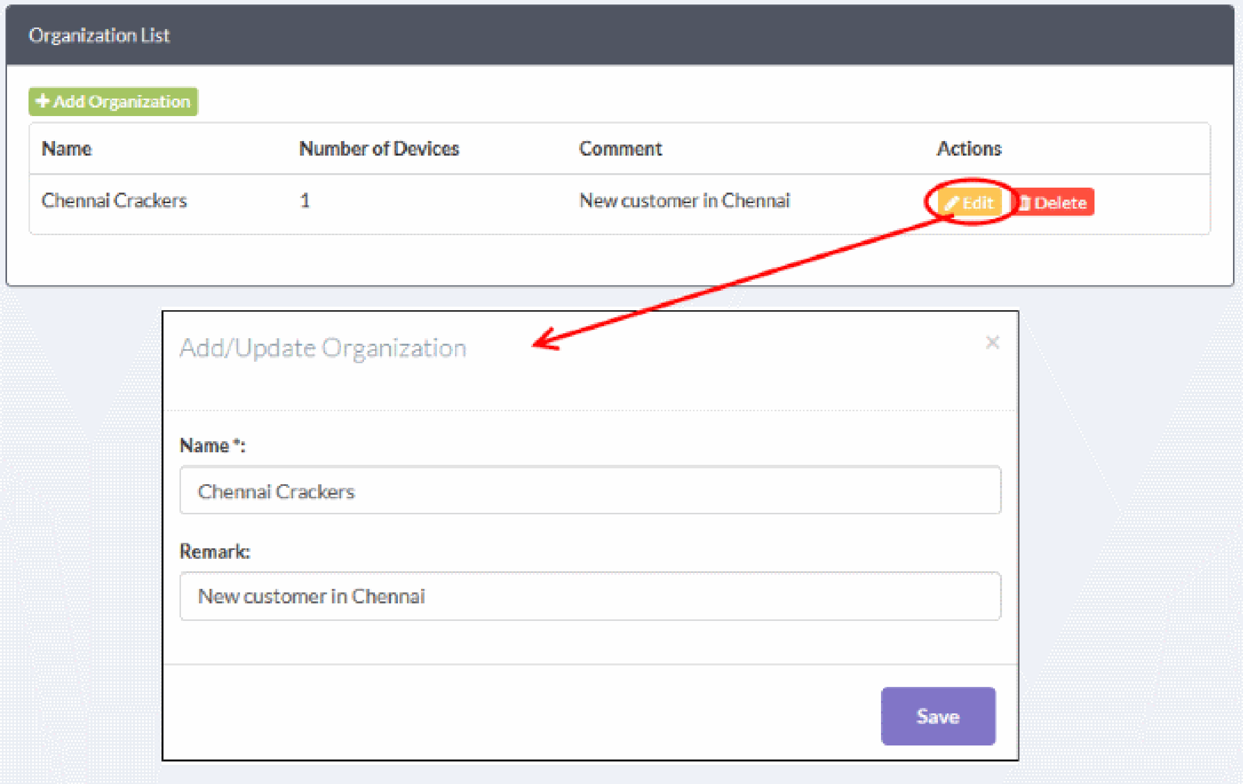
Complete the following items:

- Name - Name of the customer organization you want to enroll
- Remark - Short description of, or comments about, the organization
- Click 'Save' to add the organization.

You can now assign devices to the organization.

Edit an Organization

- Click the 'Edit' button in the row of an organization to edit its name and description



Organization List

Name	Number of Devices	Comment	Actions
Chennai Crackers	1	New customer in Chennai	Edit Delete

Add/Update Organization

Name *: Chennai Crackers

Remark: New customer in Chennai

- Update as required and click 'Save'.

Remove an Organization

- Click the 'Delete' button in the row of an organization

The organization will be removed from the list. Please note that any devices under the organization will also be removed.

5.2 Activate Firewall Licenses

Dome Firewall Central Manager lets you activate licenses for firewall devices belonging to different organizations.

- You need to purchase and activate a Dome Firewall (DFW) license for each device you wish to manage.
- Licenses can be purchased from Comodo Accounts Manager (CAM) at **https://accounts.comodo.com** or from your Comodo One / Comodo Dragon / ITarian account.

Comodo Account Manager

- Sign in to your Comodo Accounts Manager (CAM) account at **https://accounts.comdoo.com**. Please create an account if you do not yet have one.
- Click 'Sign up to Comodo Dome', choose a DFW license type and complete the purchase process.
- An order confirmation mail with DFW license details will be sent to your registered email address.

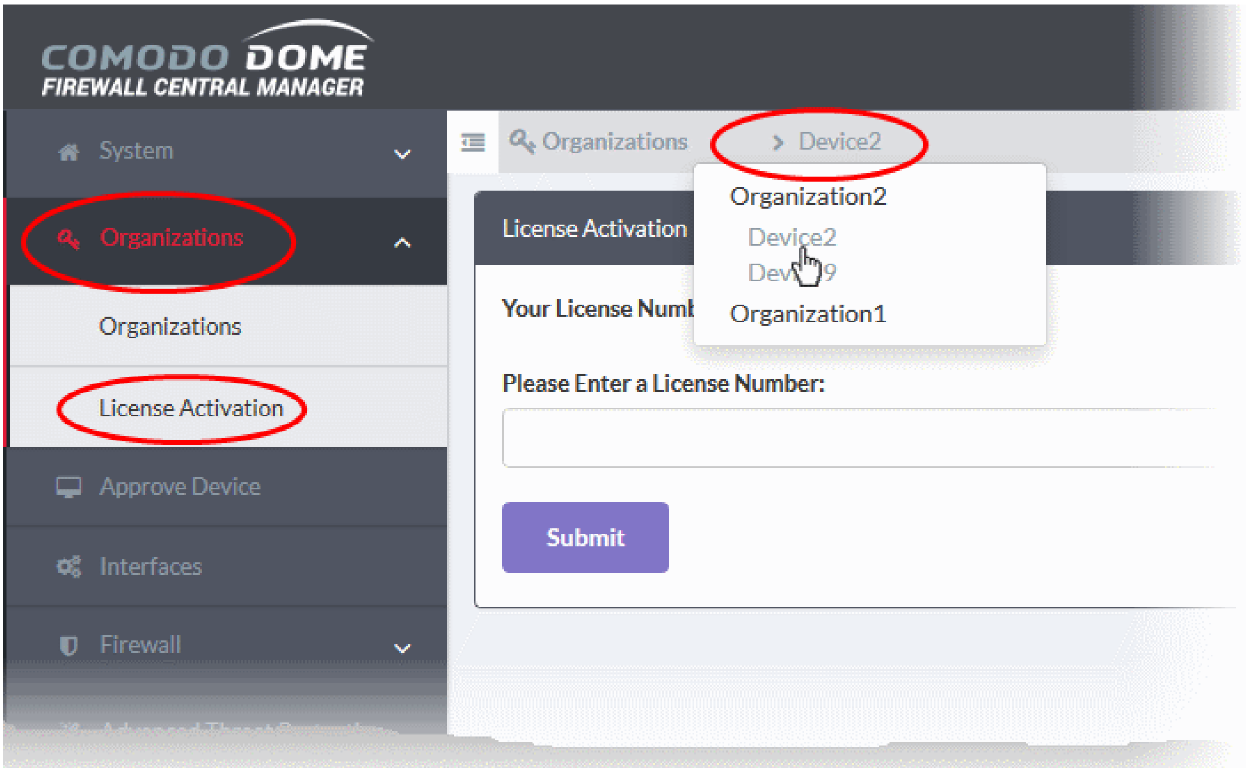
Comodo One / Comodo Dragon / ITarian Console

- 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 your portal account, you can open it by clicking 'Applications' > 'Dome Firewall Central

Manager'. See **Integrate Central Manager with Comodo One / Comodo Dragon / ITarian** for more details.

To activate firewall licenses

- Click 'Organizations' on the left then choose 'License Activation'



- Select the device from the drop-down on the title bar

If the device already has an active license, the license key will be displayed.

- Enter the new license key in the text box under 'Please Enter a License Number' and click 'Submit'

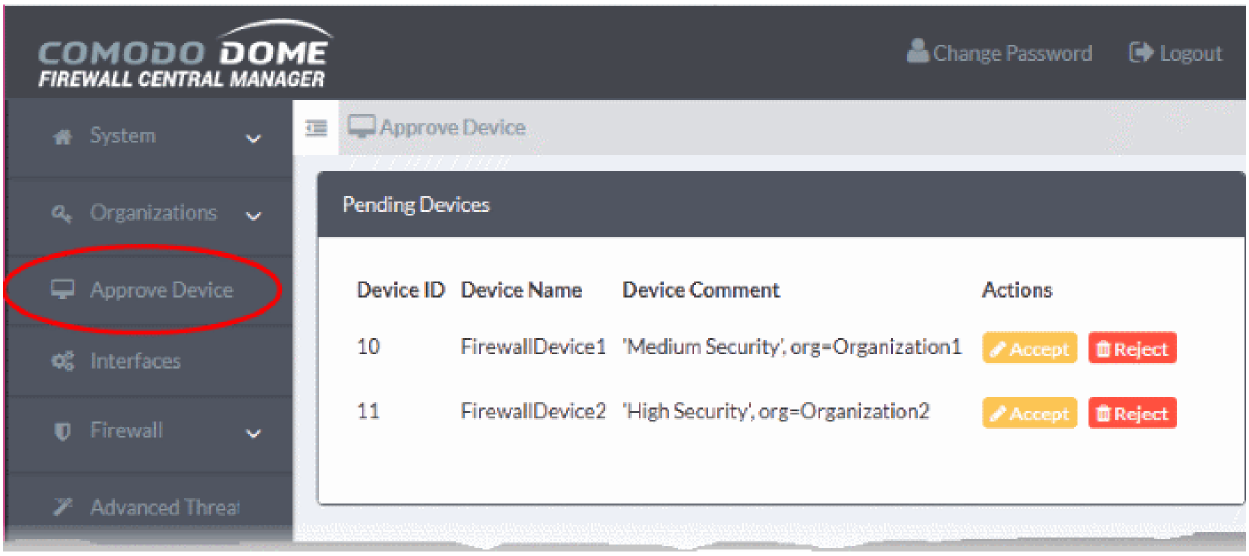
After the license key has been verified, your DFW license will be activated.

6 Approve Firewall Device Enrollment

- Firewall devices must be approved by an admin before they can be imported
  - See **Enroll Dome Firewall Devices** if you need help to add a firewall.
- The 'Approve Device' interface lets you approve devices and assign them to organizations.

Note: You must have added an organization before you can assign devices to it. See **Manage Organizations** for help with this.

- Click 'Approve Device' on the left



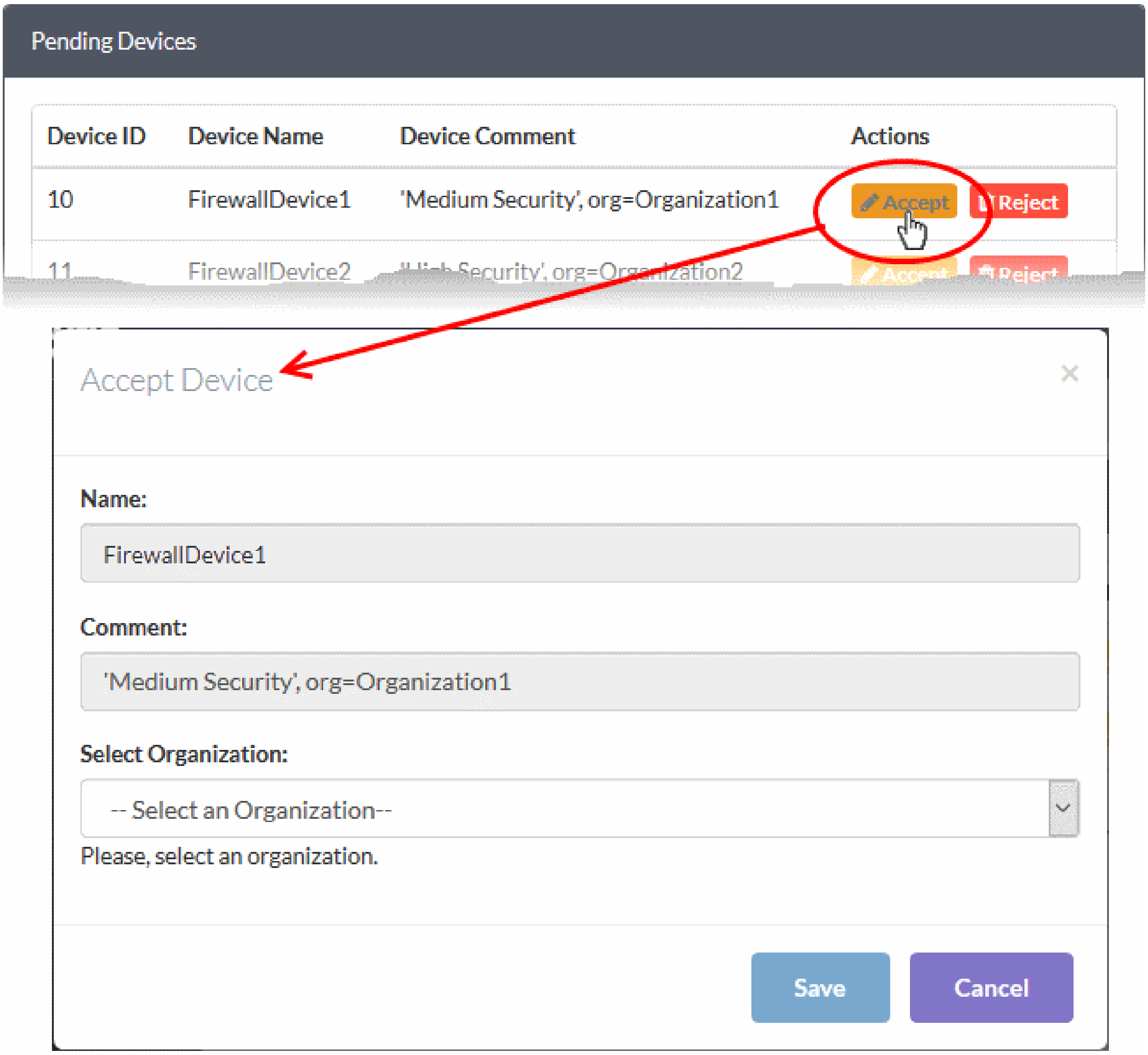
Device ID	Device Name	Device Comment	Actions
10	FirewallDevice1	'Medium Security', org=Organization1	Accept Reject
11	FirewallDevice2	'High Security', org=Organization2	Accept Reject

The interface lists all devices which are pending approval.

Pending Devices - Column Descriptions		
Column Header		**Description**
Device ID		The identification number assigned to the firewall device by Dome Firewall Central Manager
Device Name		The device label
Device Comment		A brief description of the device and details of its organization. This can be written when enrolling or editing the device.
Actions	Accept	Authorize the device enrollment. See **To approve a device enrollment** for more details.
	Reject	Decline the device enrollment.

To approve a device enrollment

- Click the 'Accept' button in the row of the device to be approved



Pending Devices

Device ID	Device Name	Device Comment	Actions
10	FirewallDevice1	'Medium Security', org=Organization1	Accept Reject
11	FirewallDevice2	'High Security', org=Organization2	Accept Reject

Accept Device

Name: FirewallDevice1

Comment: 'Medium Security', org=Organization1

Select Organization: -- Select an Organization--

Please, select an organization.

The 'Accept Device' dialog will appear.

- **Name -** The device label. The name is pre-populated and cannot be edited from this dialog. You can, however, change the name of a device from the dashboard after it has been enrolled. See **The Dashboard** for more details.
- **Comment -** Brief description and organization details entered when enrolling the device. This field is pre-populated and cannot be edited.
- **Select Organization -** Choose the customer to which the device should be assigned. See **Manage Organizations** if you need help to add an organization to CM.

- Click 'Save' to approve the device and assign it to an organization.

The device will be imported to the central manager and become available for management.

- Repeat the process to approve and add more devices.

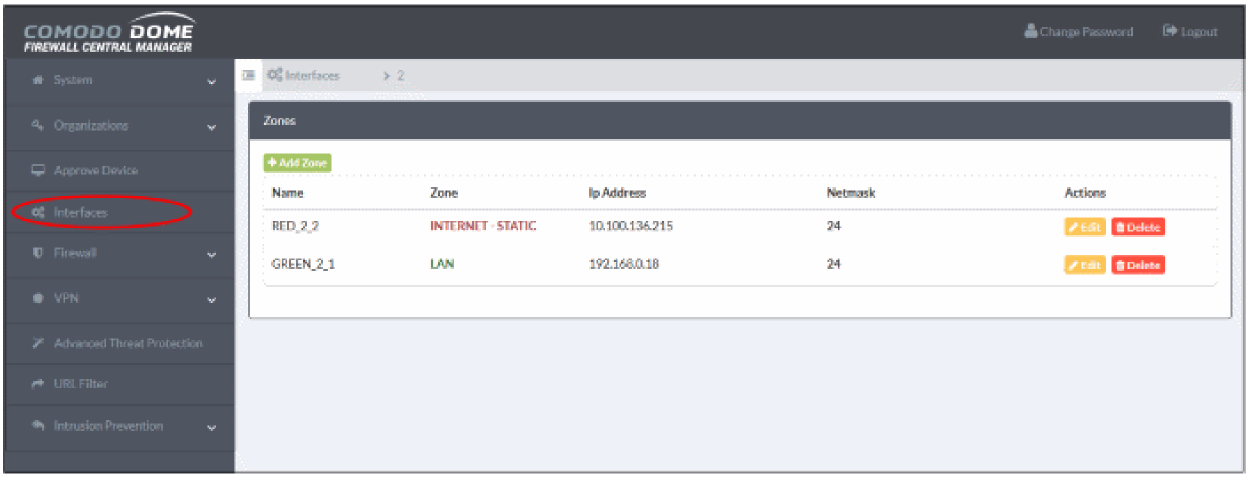
7 Add Interfaces

The 'Interfaces' area lets you add and edit interfaces which connect to different network zones. You can also add fail-over uplinks for groups of devices or individual devices.

- The 'Interfaces' screen is the only place you can add network zone interfaces to organizations and individual devices.
- Network and interface configurations are also imported when you add a firewall to central manager.
  - Click 'Dashboard' > select the device > Click 'Actions' > 'Network Configuration' in the device tile to view its network settings
- Central manager interfaces can be assigned to the ports of a device from the dashboard.
  - Click 'Actions' > 'Network Configurations' in the device tile
  - Select the interface from the 'Actions' drop-down in the row of the port
  - See **Network Configuration** if you need more details
- Interfaces added to an organization will be available for all devices assigned to that organization. (These device names will have a prefix 'O' in the 'Actions' drop-down).
- Interfaces added to an individual device will be available only for that specific device. (These device names will have a prefix 'D' in the 'Actions' drop-down)

To add and manage network zone interfaces

- Click 'Interfaces' on the left
- Select the organization/device from the drop-down in the title bar
  - Select an organization to manage the interfaces for all of devices belonging to the organization
  - Select an individual device under an organization to manage the interfaces for a specific device



Name	Zone	Ip Address	Netmask	Actions
RED_2_2	INTERNET - STATIC	10.100.136.215	24	Edit Delete
GREEN_2_1	LAN	192.168.0.18	24	Edit Delete

The screen shows a list of network zone interfaces configured for the selected organization or device.

Zones - Column Descriptions	
Column Header	**Description**
Name	The label of the network zone interface.
Zone	The type of network zone interface. The network zone can be one of the following: • Internet • LAN

		• Wi-Fi • DMZ
Ip Address		The address of the interface.
Netmask		The netmask of the network zone connected through the interface.
Actions	Edit	Edit the connection settings of the interface.
	Delete	Disconnects the interface and clears the port.

The following sections explain how to configure network zone interfaces:

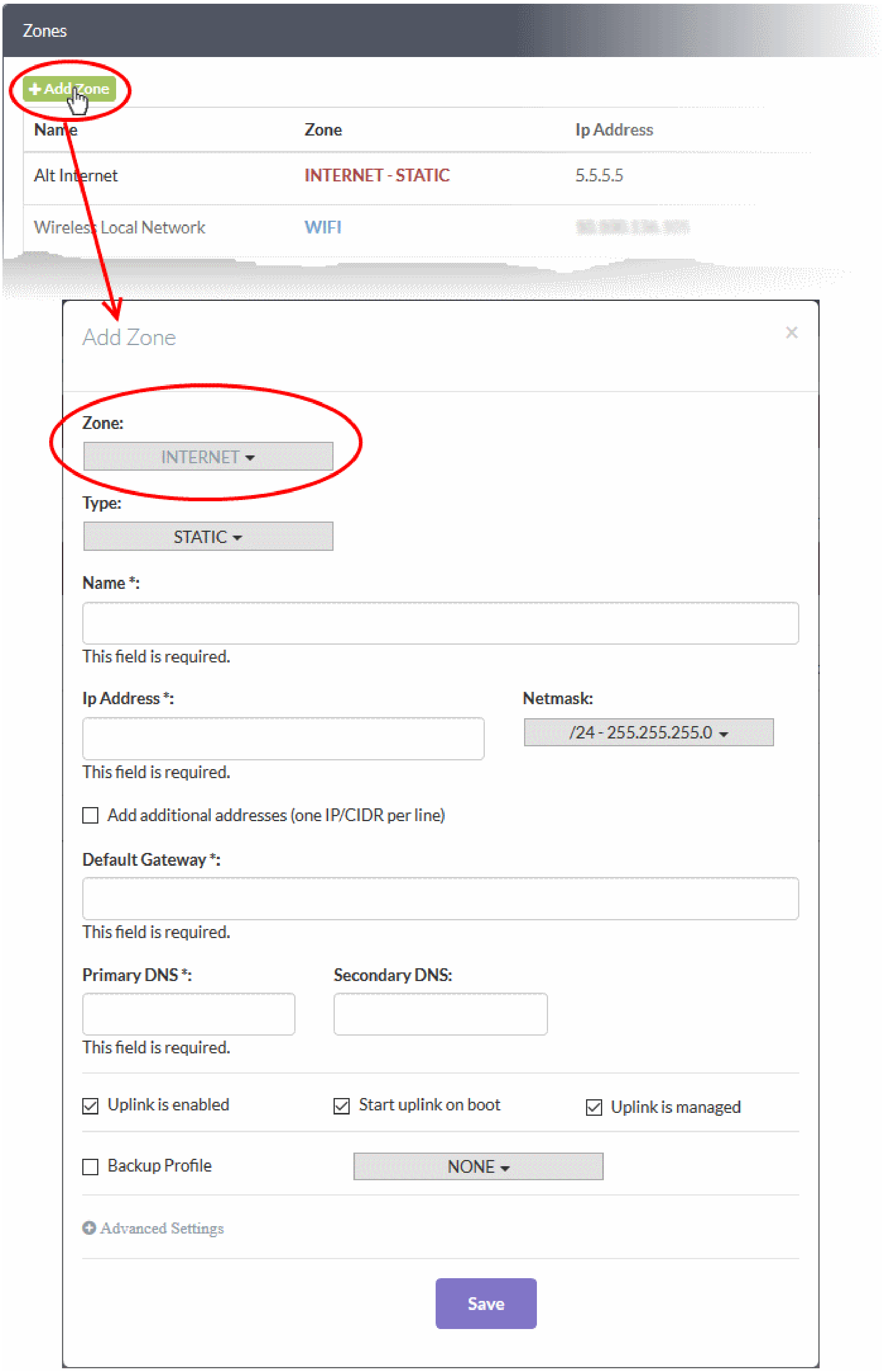
- **Add untrusted external network zones like WAN for connecting to the internet**
- **Add trusted internal network zones like LAN, DMZ and Wi-Fi interfaces**

Add untrusted external network zones like WAN for connecting to the internet

- Click 'Add Zone' at the top-left of the 'Zones' screen

The 'Add Zone' dialog will appear.

- Select 'Internet' from the 'Zone' drop-down



Zones

+ Add Zone

Name	Zone	Ip Address
Alt Internet	INTERNET - STATIC	5.5.5.5
Wireless Local Network	WIFI	[redacted]

Add Zone

Zone: INTERNET

Type: STATIC

Name *:

This field is required.

Ip Address *:

This field is required.

Netmask: /24 - 255.255.255.0

□ Add additional addresses (one IP/CIDR per line)

Default Gateway *:

This field is required.

Primary DNS *:

This field is required.

Secondary DNS:

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

□ Backup Profile NONE

Advanced Settings

Save

- Type - Choose the interface type through which the FW device will connect to the internet. The available 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.

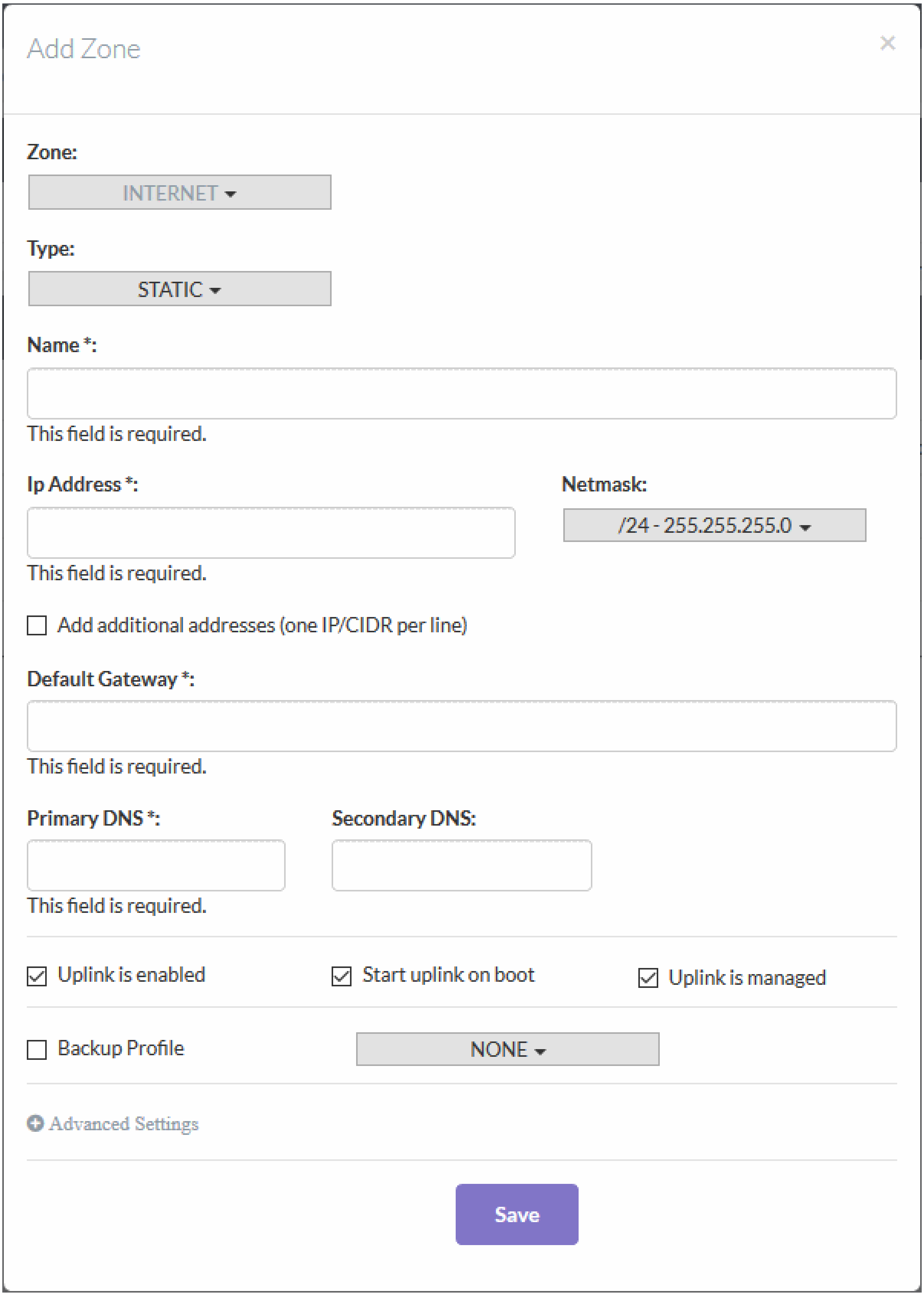
- PPPoE - The external interface is connected to an ADSL modem through an ethernet cable. Select this option only if the modem uses the Point-to-Point Protocol over Ethernet (PPPoE) to connect to the service provider.

The following sections explain configuration of each interface type:

- **STATIC**
- **PPPoE**
- **DHCP**

STATIC

- Select 'STATIC' from the 'Type' drop-down
- Configure the following for the external network zone



Add Zone

Zone:

INTERNET ▾

Type:

STATIC ▾

Name *:

This field is required.

Ip Address *:

This field is required.

Netmask:

/24 - 255.255.255.0 ▾

□ Add additional addresses (one IP/CIDR per line)

Default Gateway *:

This field is required.

Primary DNS *:

This field is required.

Secondary DNS:

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

□ Backup Profile NONE ▾

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.

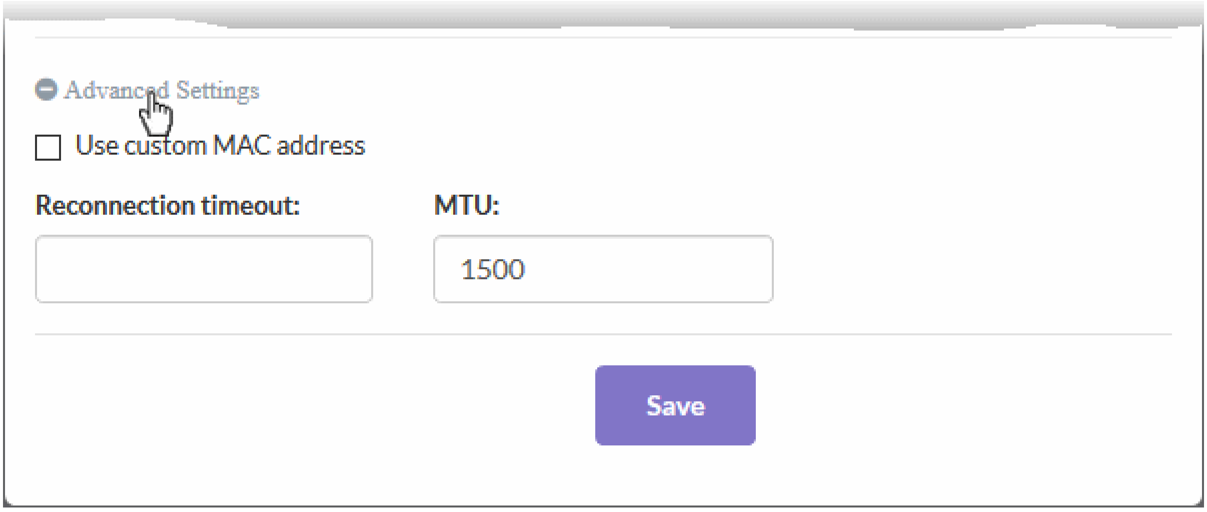
Uplink Settings

- 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. You can change the uplink to managed at any time by enabling the 'Managed' checkbox beside the uplink 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

Reconnection timeout:

MTU: 1500

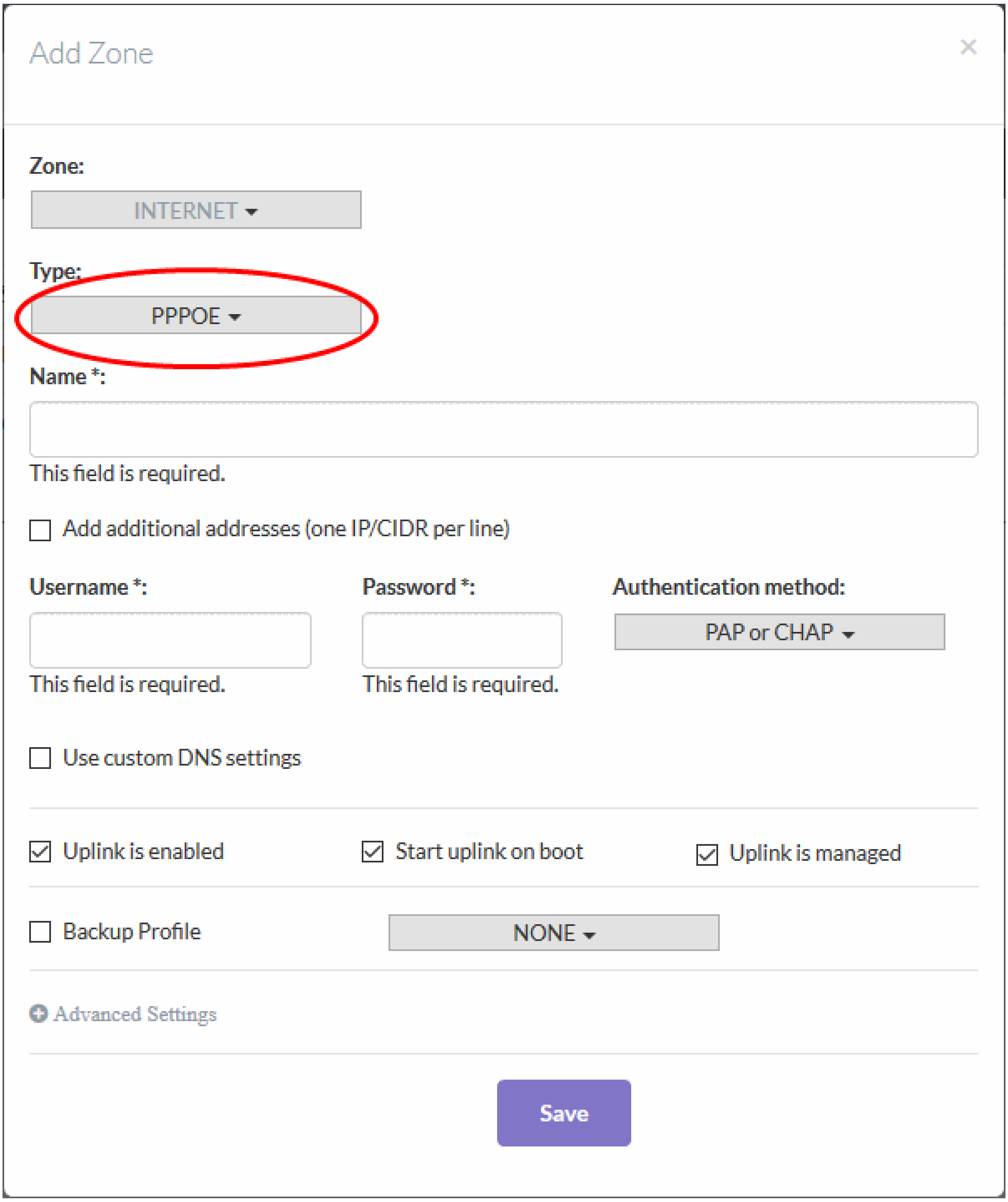
- Use custom MAC address – The firewall will automatically detect the MAC address of the network adapter port and will populate it in the MAC address column. Enable 'Use custom MAC address' if you need to override and replace the default MAC address of the external interface. Enter the MAC address in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

Tip: You can edit a network zone interface at any time by click the 'Edit' button in the row of the interface.

PPPoE

- Select 'PPPoE' from the 'Type' drop-down
- Configure the following for the external network zone with PPPoE interface



Add Zone

Zone: INTERNET

Type: PPPOE

Name *:

This field is required.

☐ Add additional addresses (one IP/CIDR per line)

Username *: This field is required.

Password *: This field is required.

Authentication method: PAP or CHAP

☐ Use custom DNS settings

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

☐ Backup Profile NONE

Device Settings

- Name - Enter a label to identify the interface.
- 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.
- Username - Enter the login username for the internet connection as provided by the Internet Service Provider (ISP)
- Password - Enter the login password as provided by the ISP
- Authentication Method - Choose the method of authentication used by your ISP for your device to

connect to internet. The options available are: Password Authentication Protocol (PAP); Challenge Handshake Authentication Protocol (CHAP); or both. If you are not sure, choose 'PAP or CHAP' (Default).

- Use Custom DNS Settings - Specify your preferred DNS servers. Enable this checkbox and enter the IP address/hostname of your primary and secondary DNS servers. DNS servers will be automatically assigned if you do not enable this option.

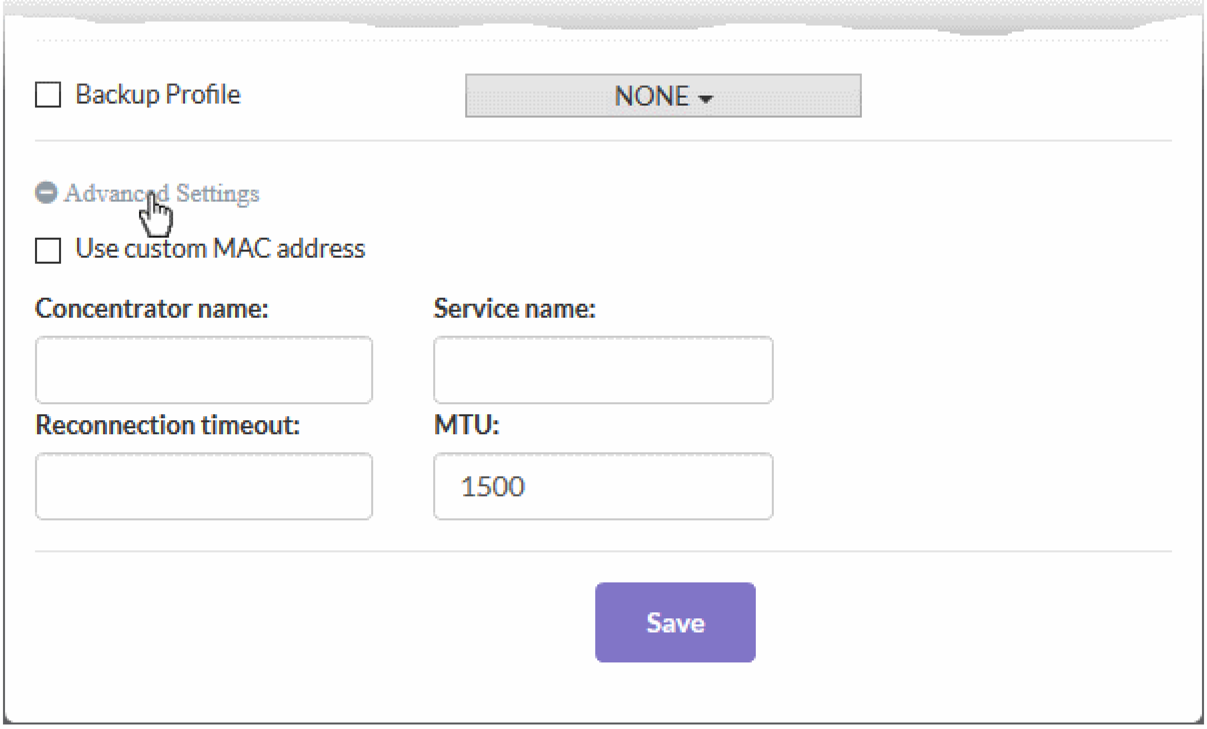
Uplink Settings

- Uplink is Enabled - The uplink will be activated immediately after it is created. 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 or from the dashboard of the firewall device console.
- Start uplink on boot - The uplink will start automatically after every restart of the firewall device. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details displayed in the firewall console dashboard. Deselect this option if you do not want uplink details to be shown in the dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the dashboard.
- Backup Profile - Select if you want to specify an alternate uplink connection to be activated in the event this uplink fails. Choose the alternative device from the drop-down.
- Additional Link check hosts - In the event of a connection failure, the uplink will attempt to reconnect after a time period set by your ISP. If you want the virtual appliance to check whether the uplink has connected successfully, you can try to ping known hosts in an external network. Enabling this option will reveal a text field where you should enter a list of one or more perpetually reachable IP addresses or hostnames. One of the hosts could be your ISP's DNS server or gateway.

Advanced Settings:

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

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



□ Backup Profile NONE ▾

Advanced Settings

□ Use custom MAC address

Concentrator name:

Service name:

Reconnection timeout:

MTU: 1500

- 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.

- Concentrator name - Enter the identifier of the remote access concentrator setup by your service provider (Optional, usually not needed).
- Service Name - Enter the name of your ISP (Optional, usually not needed).
- 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 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.

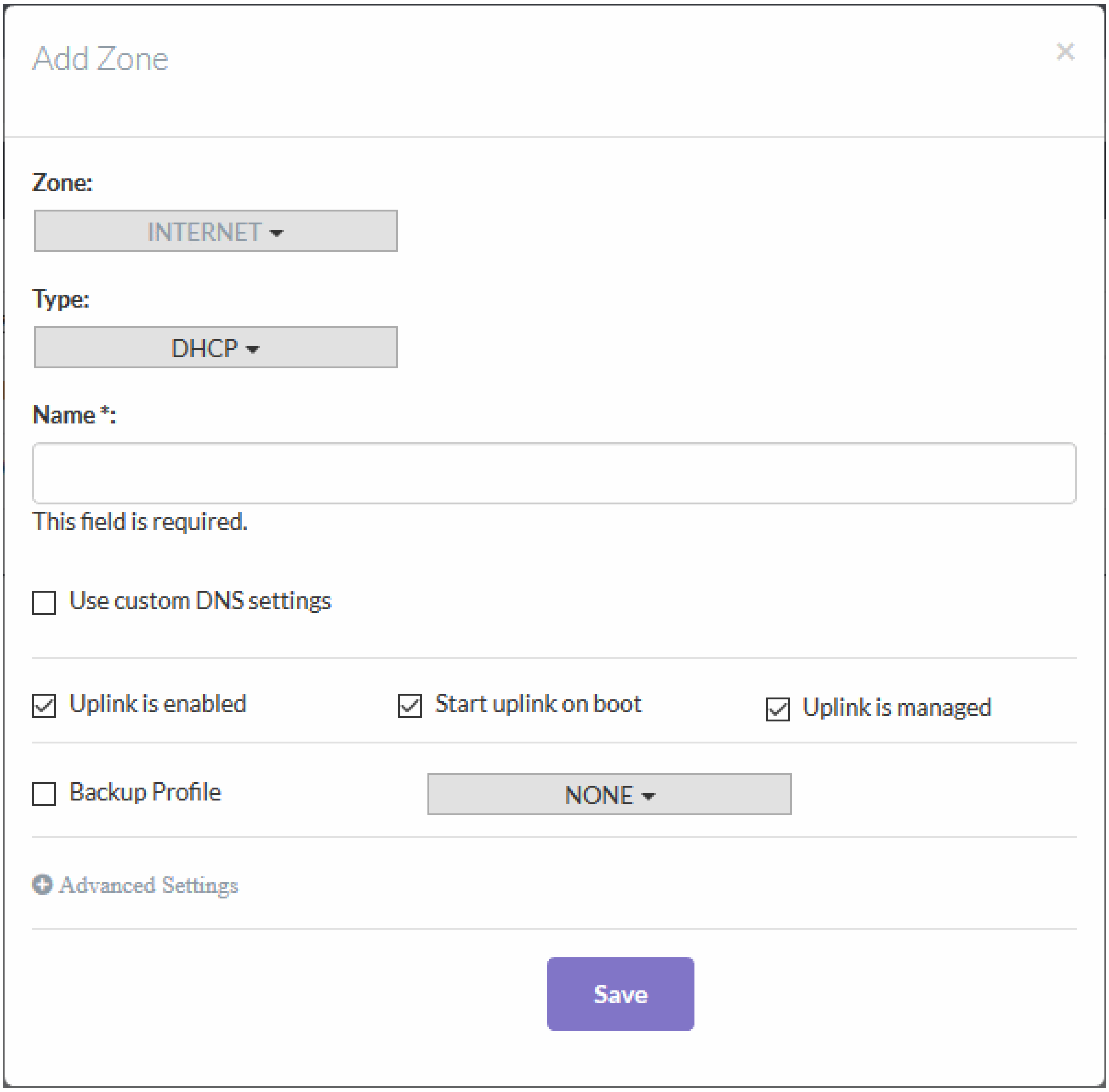
- Click 'Save'.

The interface will be added to the list.

Tip: You can edit the network zone interface e.g. for changing selected parameters like network range of a zone, at any time depending on changes in the network. Click the 'Edit' button in the row of the device, make the changes and save the changes.

DHCP

- Select 'DHCP' from the 'Type' drop-down



Add Zone

Zone: INTERNET

Type: DHCP

Name *:

This field is required.

☐ Use custom DNS settings

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

☐ Backup Profile NONE

- Configure the following for the external network zone with Ethernet DHCP interface

  Device Settings

  - Name - Enter a label to identify the interface.
  - Use Custom DNS Settings - Specify your preferred DNS servers. Enable this checkbox and enter the IP address/hostname of your primary and secondary DNS servers. DNS servers will be automatically assigned if you do not enable this option.

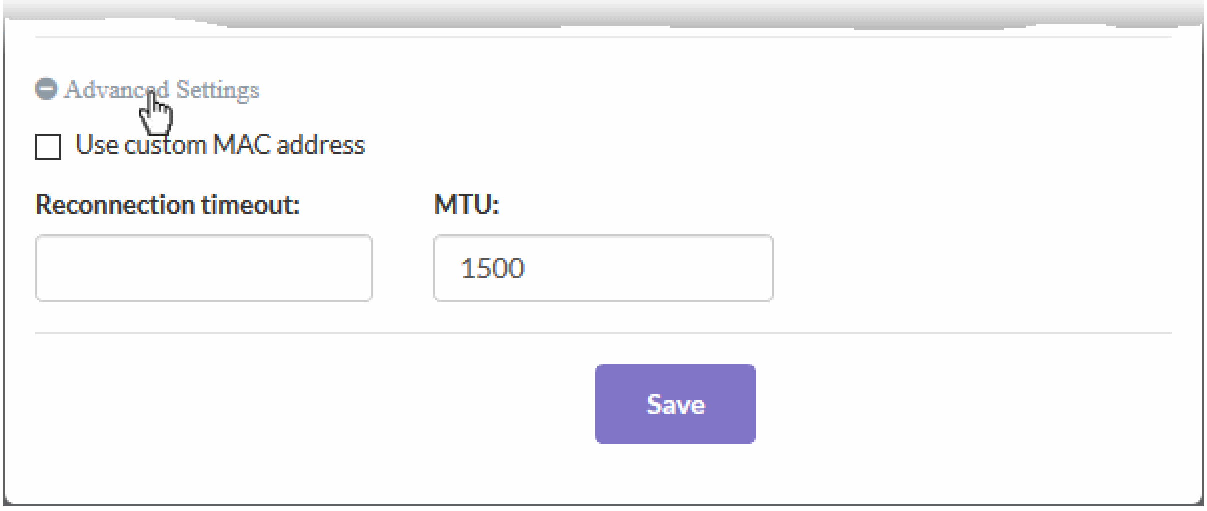
  Uplink Settings

  - Uplink is Enabled - The uplink will be activated immediately after it is created. 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 or from the dashboard of the firewall device console.
  - Start uplink on boot - The uplink will start automatically after every restart of the firewall device. Deselect this checkbox if you want to manually start the uplink only when required.
  - Uplink is managed - The uplink will be managed by Dome Firewall and its details displayed in the firewall console dashboard. Deselect this option if you do not want uplink details to be shown in the dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the dashboard.
  - Backup Profile - Select if you want to specify an alternate uplink connection to be activated in the event this uplink fails. Choose the alternative device from the drop-down.
  - Additional Link check hosts - In the event of a connection failure, the uplink will attempt to reconnect after a time period set by your ISP. If you want the virtual appliance to check whether the uplink has connected successfully, you can try to ping known hosts in an external network. Enabling this option will reveal a text field where you should enter a list of one or more perpetually reachable IP addresses or hostnames. One of the hosts could be your ISP's DNS server or gateway.

  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

Reconnection timeout:

MTU: 1500

  - 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.

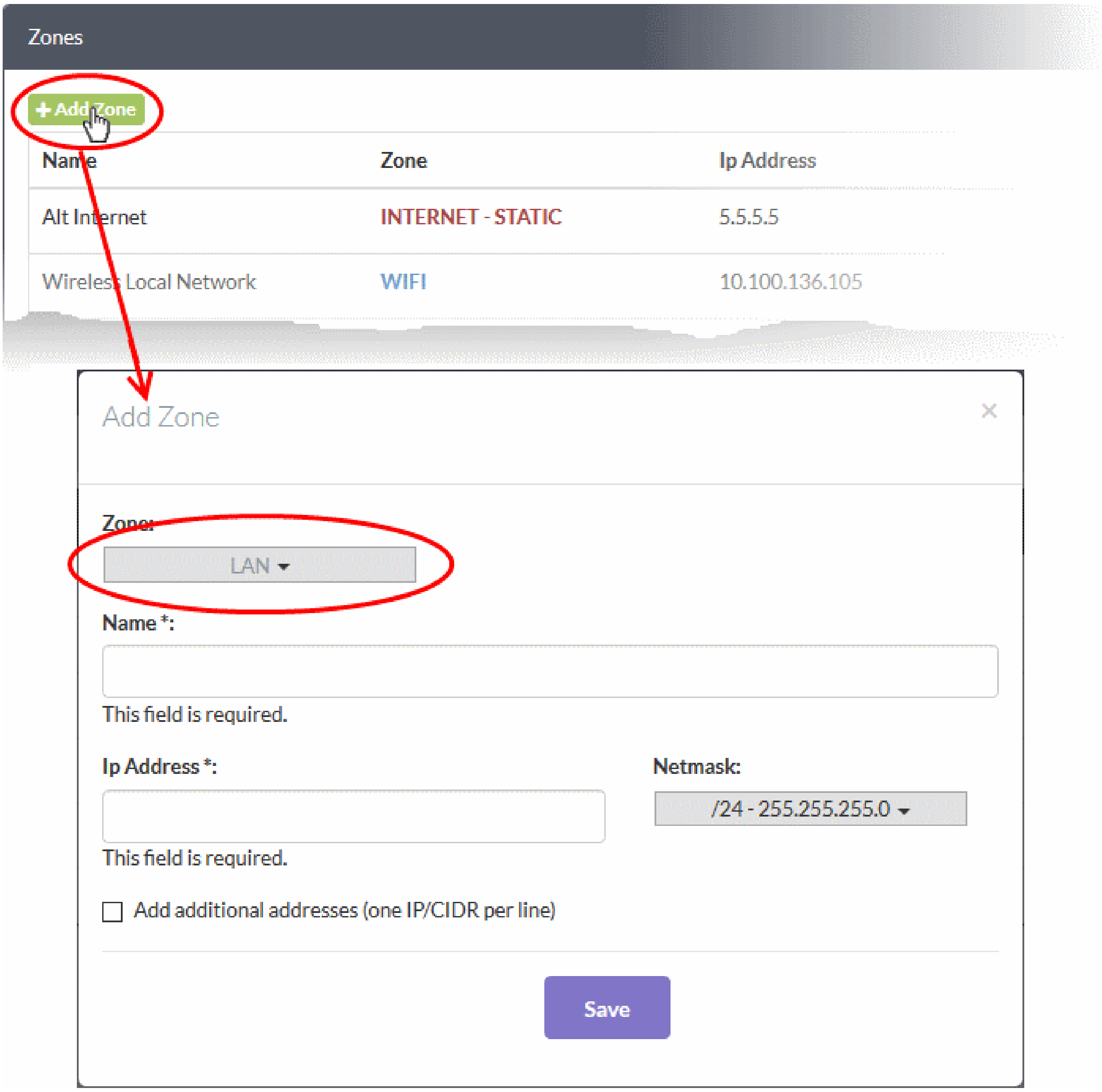
Tip: You can edit a network zone interface at any time by click the 'Edit' button in the row of the interface.

Add trusted internal network zones like LAN, DMZ and Wi-Fi interfaces

- Click 'Add Zone' at the top-left of the 'Zones' screen.

The 'Add Zone' dialog will appear.

- Select 'LAN', 'WIFI' or 'DMZ' from the 'Zone' drop-down as required.



Zones

+ Add Zone

Name	Zone	Ip Address
Alt Internet	INTERNET - STATIC	5.5.5.5
Wireless Local Network	WIFI	10.100.136.105

Add Zone ×

Zone: LAN

Name *:

This field is required.

Ip Address *:

This field is required.

Netmask: /24 - 255.255.255.0

□ Add additional addresses (one IP/CIDR per line)

Save

- 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)

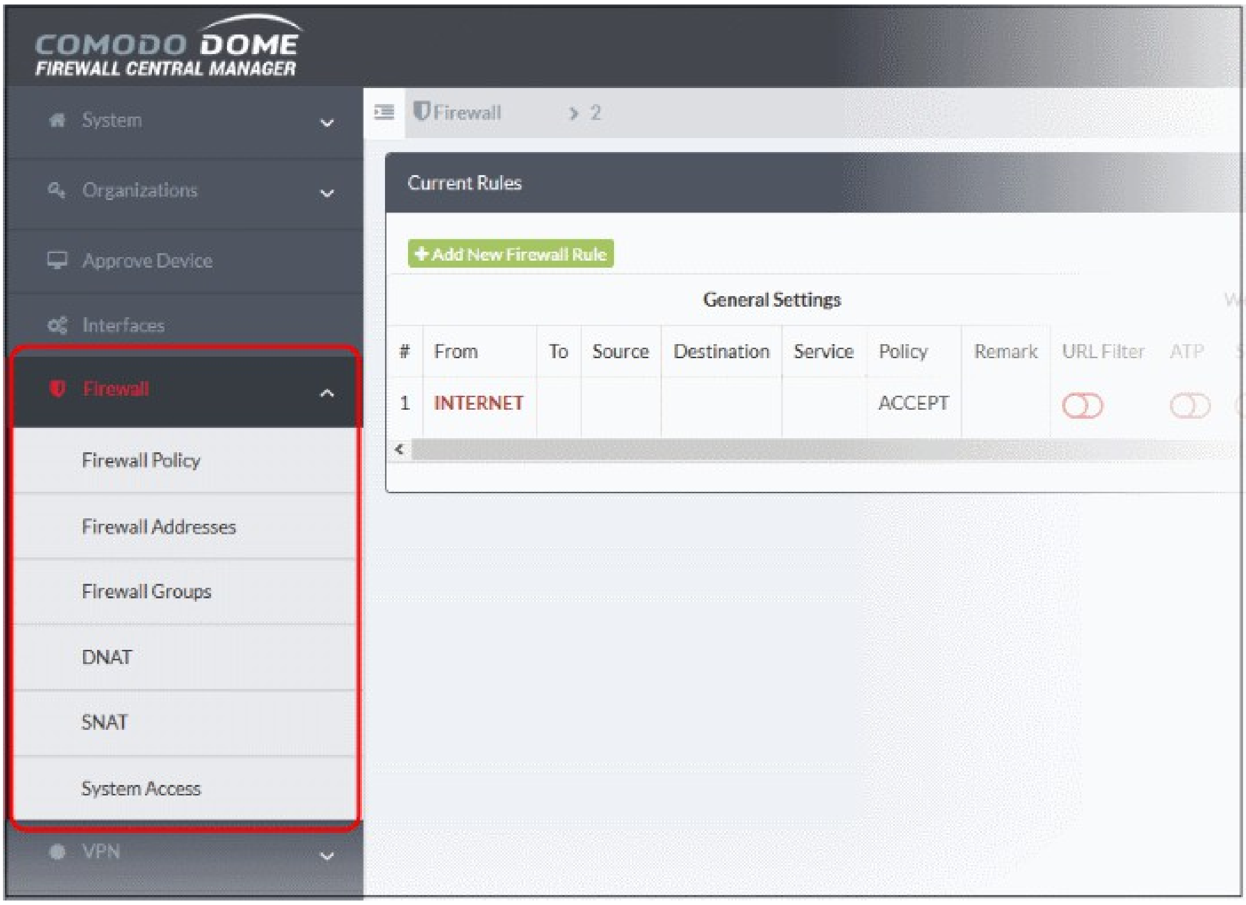
  - Add additional addresses - Enable to add additional IP address(es)/netmask(s) to the interface. Enter the additional address(es)/netmask(s) one per line in the text box that appears.
- Click 'Save'.

The interface will be added to the list.

Tip: You can edit a network zone interface at any time by click the 'Edit' button in the row of the interface.

8 Firewall Management

The 'Firewall' menu lets you configure firewall policies for organizations and individual devices. You can also create rules for source network address translation (SNAT), destination network address translation (DNAT), system access and more.



Current Rules

General Settings									
#	From	To	Source	Destination	Service	Policy	Remark	URL Filter	ATP
1	INTERNET					ACCEPT		○	○

The menu contains the following options:

- **Firewall Policy** - Add and manage firewall rules for polices applied to a device or organization. See **Configure Firewall Policy Rules** for more details.
- **Firewall Addresses** - Create firewall address objects covering specific IP addresses, IP ranges or network masks. Once created, these objects can be called as the source and destination addresses when creating firewall rules, DNAT rules, SNAT rules and system access rules. See **Manage Firewall Address Objects** for more details.
- **Firewall Groups** - Create groups of firewall address objects to further streamline policy and rule creation. See **Manage Firewall Object Groups** for more details.
- **DNAT** - Create rules for Destination Network Address Translation (DNAT) on incoming traffic. DNAT rules

can be used to limit access from untrusted external networks to the hosts in the network infrastructure. See **Configure Destination Network Address Translation Rules** for more details.

- **SNAT** - Create Source Network Address Translation (SNAT) rules for outbound traffic. SNAT rules can be used to configure the source IP address in the outgoing packets from a host/server in a network. See **Configure Source Network Address Translation Rules** for more details.
- **System Access** - Create rules to regulate access to the firewall device by hosts in internal and external networks. See **Configure System Access Rules** for more details.

8.1 Configure Firewall Policy Rules

Each Comodo Dome Firewall has a policy which manages traffic flowing in and out of the network. The policy is constructed from a series of firewall rules that are created and imposed for different types of data traffic.

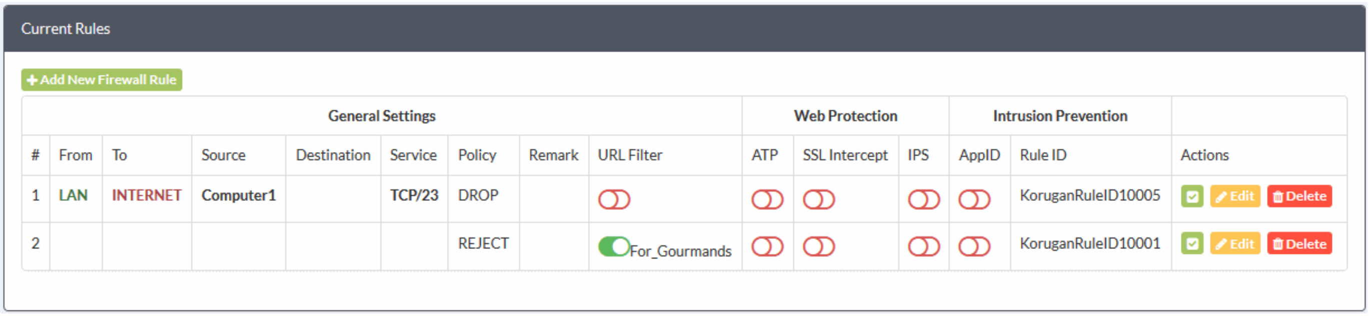
- Incoming traffic - Traffic from external network zones to specified hosts in the internal network zone
- Outgoing traffic - Traffic from hosts to the external network zone
- Inter-zone traffic - Traffic between network zones connected to the firewall device
- VPN traffic - Traffic from users connected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

The 'Firewall Policy' interface lets you create and manage rules for policies which are applied to organizations and individual firewall devices. An organization policy will apply to all firewall devices belonging to that organization.

- Note - Existing FW policies will not be imported with the device. We recommend you remove these from the device before importing then configure them again from central manager.

To configure firewall policy

- Click 'Firewall' on the left and choose 'Firewall Policy'
- Select the organization/device from the drop-down in the title bar
    - Select an organization to manage policy/rules for all devices in that organization
    - Select an individual device under an organization to manage policy/rules for a single device.



Current Rules

General Settings									Web Protection		Intrusion Prevention			
#	From	To	Source	Destination	Service	Policy	Remark	URL Filter	ATP	SSL Intercept	IPS	AppID	Rule ID	Actions
1	LAN	INTERNET	Computer1		TCP/23	DROP		○	○	○	○	○	KoruganRuleID10005	✓ Edit Delete
2						REJECT		● For_Gourmands	○	○	○	○	KoruganRuleID10001	✓ Edit Delete

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

Policy Firewall Rules Table - Column Descriptions		
Category	**Column**	**Description**
General Settings	#	Serial number of the rule.
	From	The interface or network zone from which the traffic originates.
	To	The interface or network zone to which the traffic is directed.
	Source	The firewall object or object group which contains the addresses of the host(s) from which traffic originates.

	Destination	The firewall object or object group which contains the addresses of the host(s) to which traffic is sent.
	Service	Protocol and port that will be used by traffic affected by this rule.
	Policy	Indicates the action taken on the data packets intercepted by the rule
	Remark	A short description of the rule
Web Protection	URL Filter	Whether or not the 'Web Filter' security profile is enabled for the rule. If enabled you will see the name of the profile.
	Advanced Threat Protection	Whether or not the 'Advanced Threat Protection' component is enabled for the rule.
	SSL Intercept	Whether or not the 'HTTPS Intercept Web Filter security profile' is enabled for the rule. If enabled you will see the name of the profile.
Intrusion Prevention	IPS	Whether or not the 'Intrusion Protection System (IPS)' security profile is enabled for the rule.
	AppID	Whether or not the the 'Application Filter' rule is enabled for the policy.
	Rule ID	Identity number of the rule. This is determined by the order in which the rules were created for the device/organization. Traffic is allowed or denied based on the first matching rule in ascending order of ID numbers. This is regardless of the order of the rules as shown in the table.
	Actions	Controls for managing the rule. ☑ - Enable or disable the rule ✎ Edit - Modify the rule. The 'Edit' interface is similar to the 'Policy Firewall Rule Editor' interface used to create new rules. See **Add Firewall Rules** for more details. 🗑 Delete - Removes the rule.

Add Firewall Rules

Firewall rules contain three components:

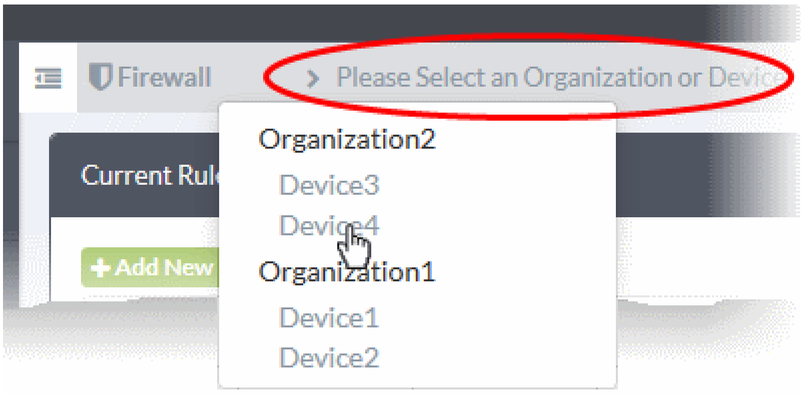
- General Settings - Specify source and destination addresses and the service/protocol of packets to be intercepted by the rule. You can specify the firewall address objects and object groups as source and destination addresses. See **Manage Firewall Address Objects** for more details on adding firewall 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 Advanced Threat Protection Profiles** and **Manage URL and Content Filtering 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.

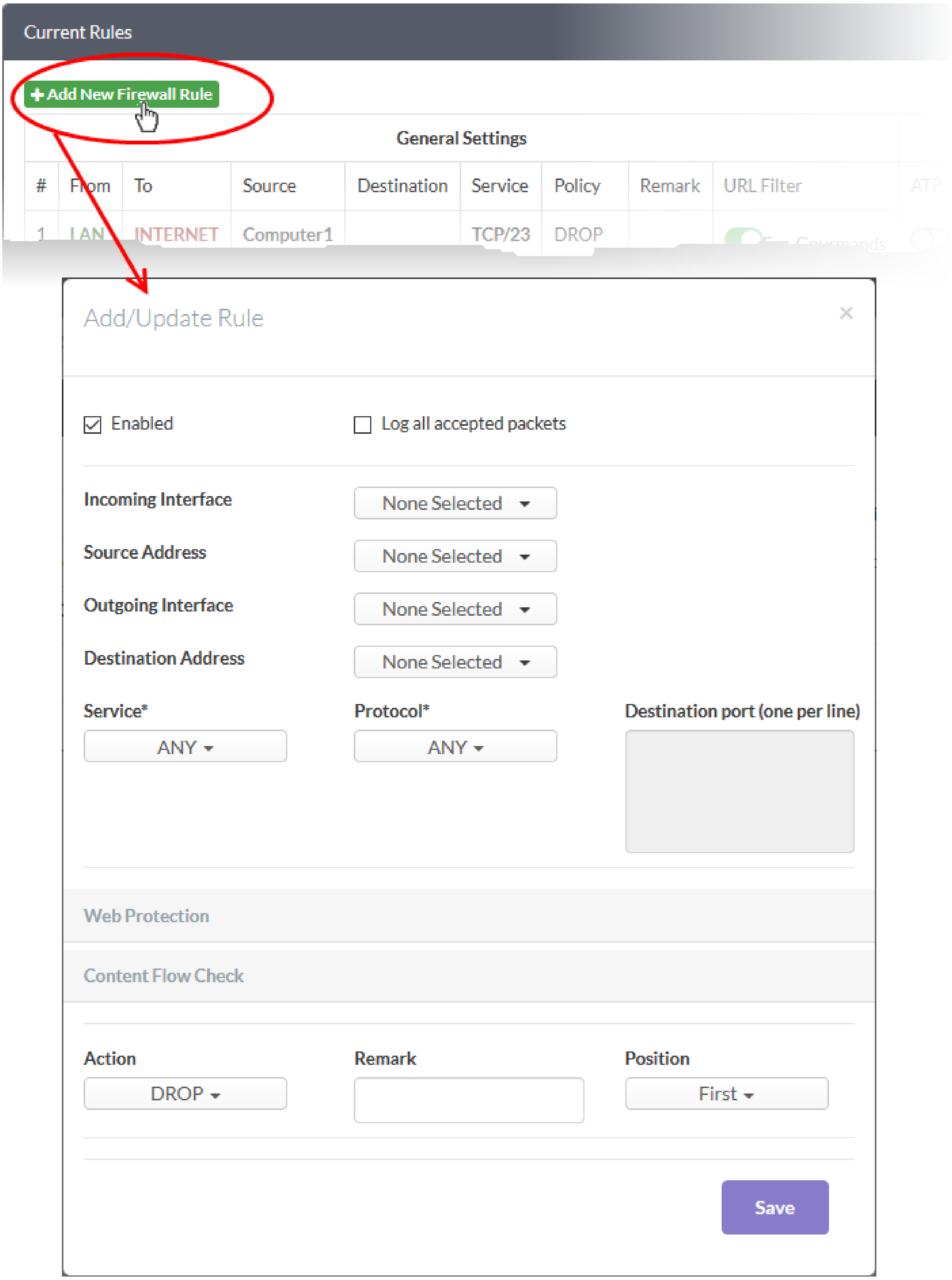
To add a rule to an existing organization a device policy

- Click 'Firewall' on the left and choose 'Firewall Policy'
- Select the organization/device from the drop-down in the title bar

- Select an organization if you wish to manage policy rules for all devices in the organization
- Select an individual device to manage policy rules for a particular device



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



Current Rules

+ Add New Firewall Rule

General Settings									
#	From	To	Source	Destination	Service	Policy	Remark	URL Filter	ATP
1	LAN	INTERNET	Computer1		TCP/23	DROP			

Add/Update Rule

☑ Enabled

□ Log all accepted packets

Incoming Interface	None Selected
Source Address	None Selected
Outgoing Interface	None Selected
Destination Address	None Selected

Service*: ANY

Protocol*: ANY

Destination port (one per line)

Web Protection

Content Flow Check

Action: DROP

Remark

Position: First

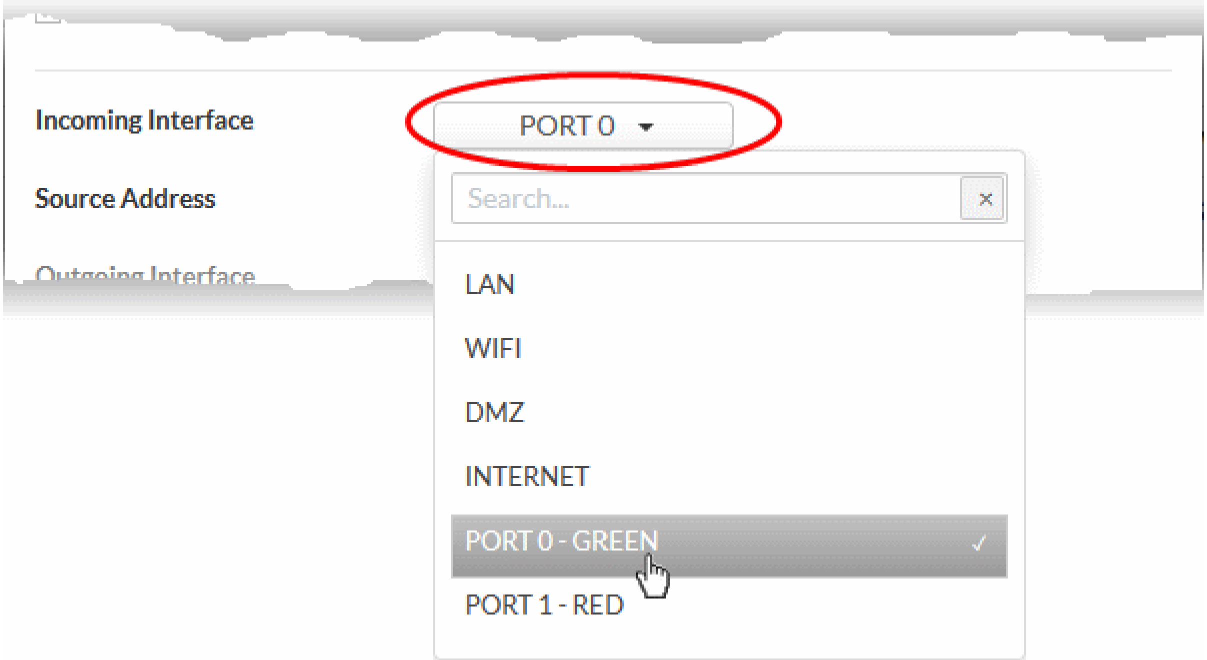
Save

General Settings:

- **Enabled** - Enable or disable the firewall rule. You can also enable/disable the rule from the 'Current Rules' interface.
- **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 administrative console. See **https://help.comodo.com/topic-451-1-936-**

12765-View-Logs.html for more details.

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

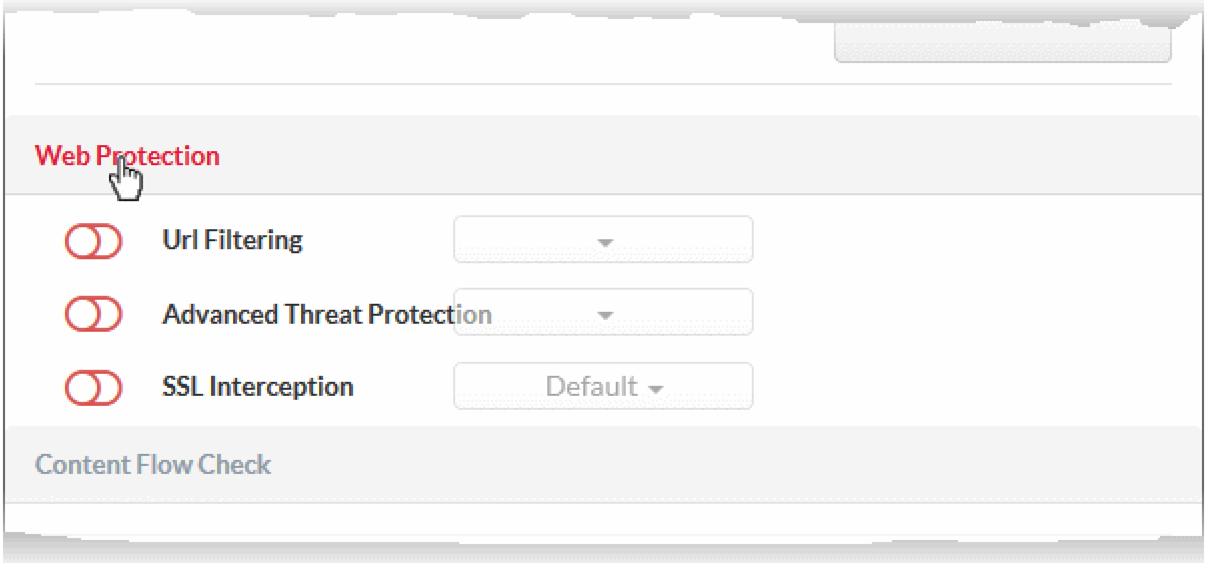


  - You can select more than one interface for the rule
  - Use the 'Search' box to search for a specific interface

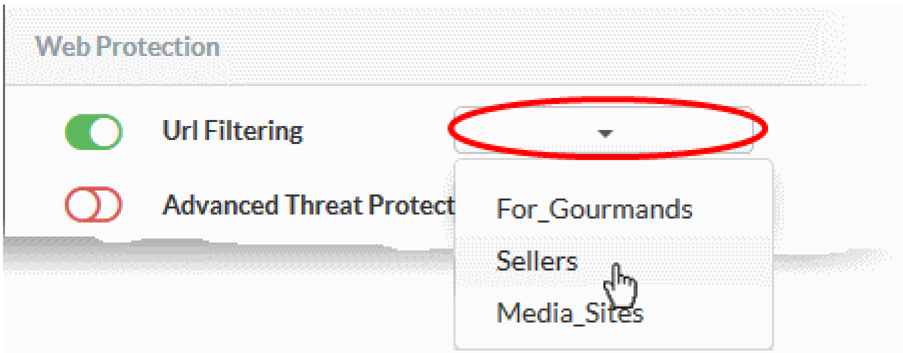
- **Source Address -** Choose the firewall address object or group from which traffic originates. Please note that only the firewall address objects and object groups created for the selected organization/device will be available in the drop-down. See **Manage Firewall Address Objects** for guidance 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

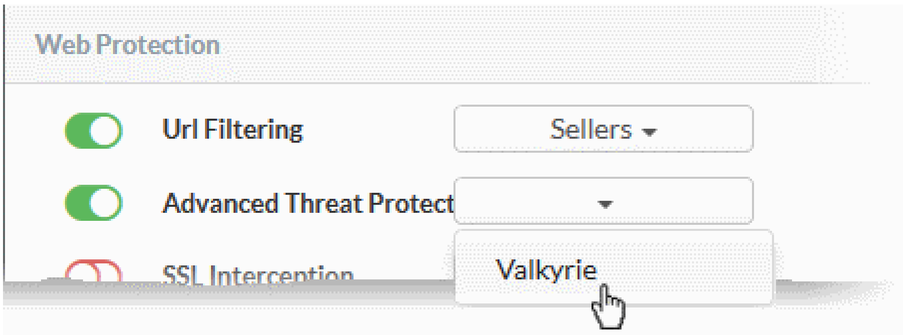
- Click 'Web Protection' to open the security features for web protection:



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



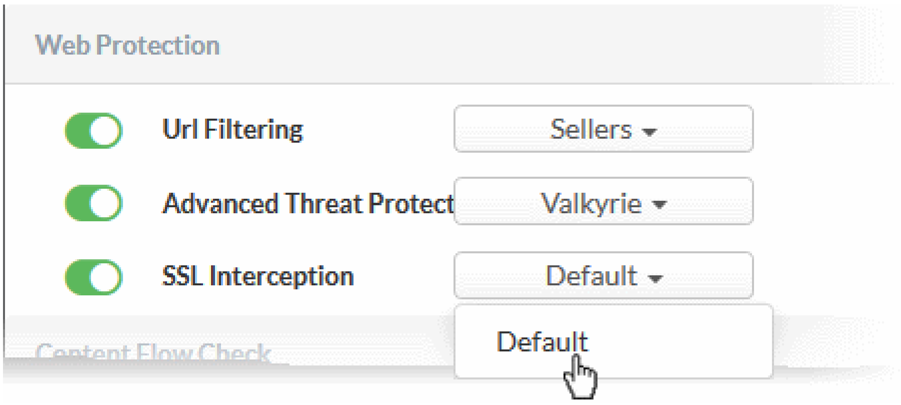
    - URL filtering profiles can be added for organizations/devices from the 'URL Filter' interface. See **Manage URL and Content Filtering Profiles** for more details.
    - Profiles defined for an organization can only be applied to devices which belong to the organization. If you apply it to the organization itself, the profile will pertain 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 ATP default profile can be managed for the organization/device from the 'Advanced

Threat Protection' > 'Profiles' interface. See **Manage Advanced Threat Protection Profile** for guidance on this.

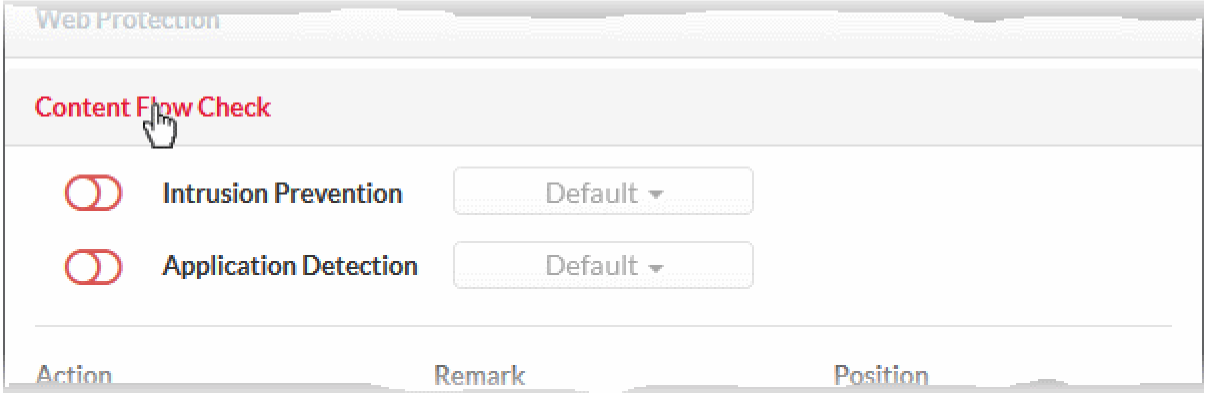
- **SSL Interception -** Enable or disable analysis of encrypted traffic which is intercepted by the rule.
  - Move the switch to ON to enable SSL interception.
  - Select the default profile from the drop-down.



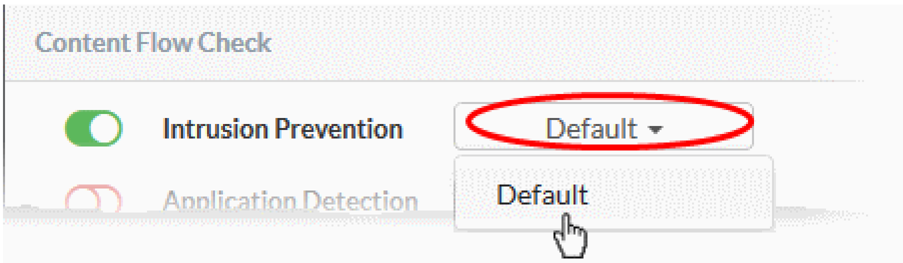
Selecting 'Default' will apply the HTTPS exceptions settings as configured in the firewall device. See the online help page **https://help.comodo.com/topic-436-1-912-12058-HTTPS-Proxy.html** for more details.

Content Flow Check Settings:

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



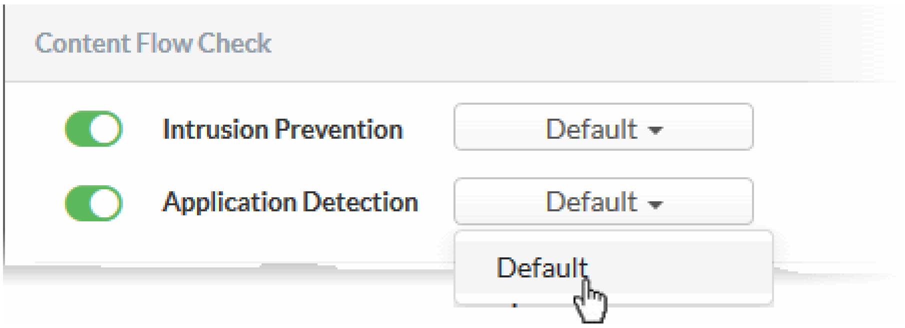
- **Intrusion Prevention -** Enable/disable Snort intrusion detection technology on traffic intercepted by the rule. See '**Intrusion Prevention**' for more details.
  - Move the switch to ON to enable intrusion prevention.
  - Select the default profile from the drop-down.



Selecting 'Default' will apply the rule settings configured in the 'Intrusion Prevention' interface. See '**Intrusion Prevention**' 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.



Content Flow Check

ON	Intrusion Prevention	Default
ON	Application Detection	Default

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

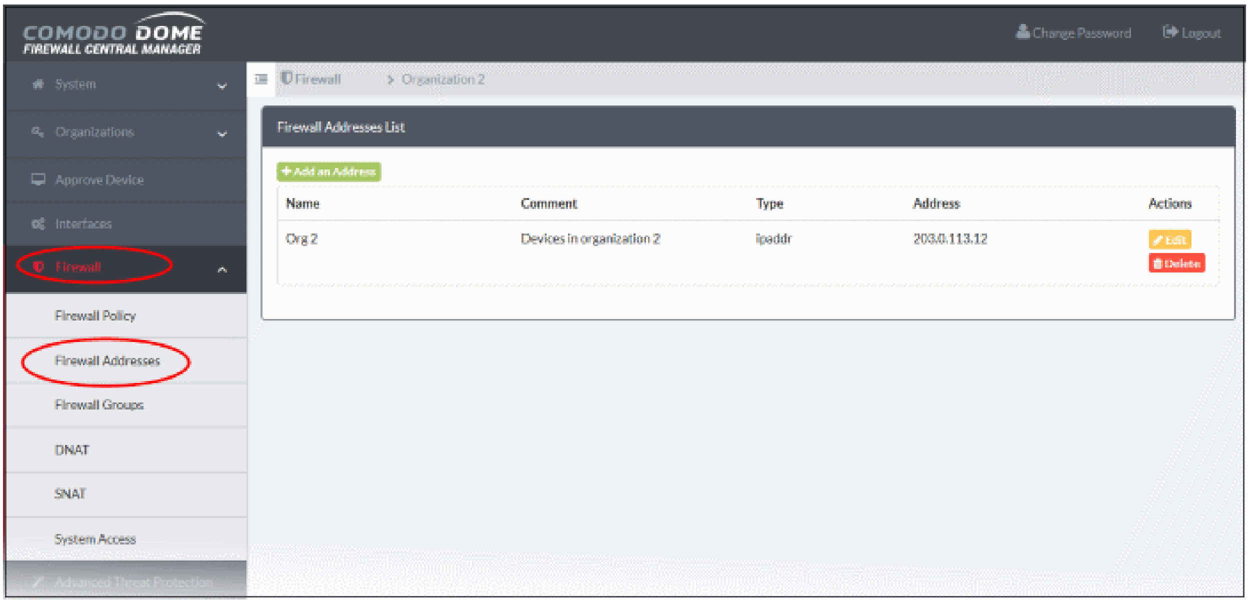
The rule will be applied to all target devices. You can view the view the application status and re-apply the rule if required from the 'Dashboard' > 'Tasks' interface. See **View Management Tasks** for more details.

8.2 Manage Firewall Address Objects

- An address object is reference to a set of IP addresses in a specific organization / device. These objects ca be used in firewall rules.
- An object is specific to an organization or firewall device.
  - Address objects added to an organization will be available for that organization's 'Source' and 'Destination' IP address drop down, which includes all devices assigned to that organization.
  - Address objects added for an individual device will be available only for that specific device's 'Source' and 'Destination' IP address drop down.
- You can also create firewall object groups to create rules for larger networks.
- You can create a wide range of rules for each firewall device.
- Note - Existing FW address objects will not be imported with the device. We recommend you remove these from the device before importing then configure them again from central manager.

To create and manage firewall address objects

- Click 'Firewall' > 'Firewall Addresses' on the left hand menu
- Select the organization to which the firewall device belongs, or the name of firewall device
  - 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



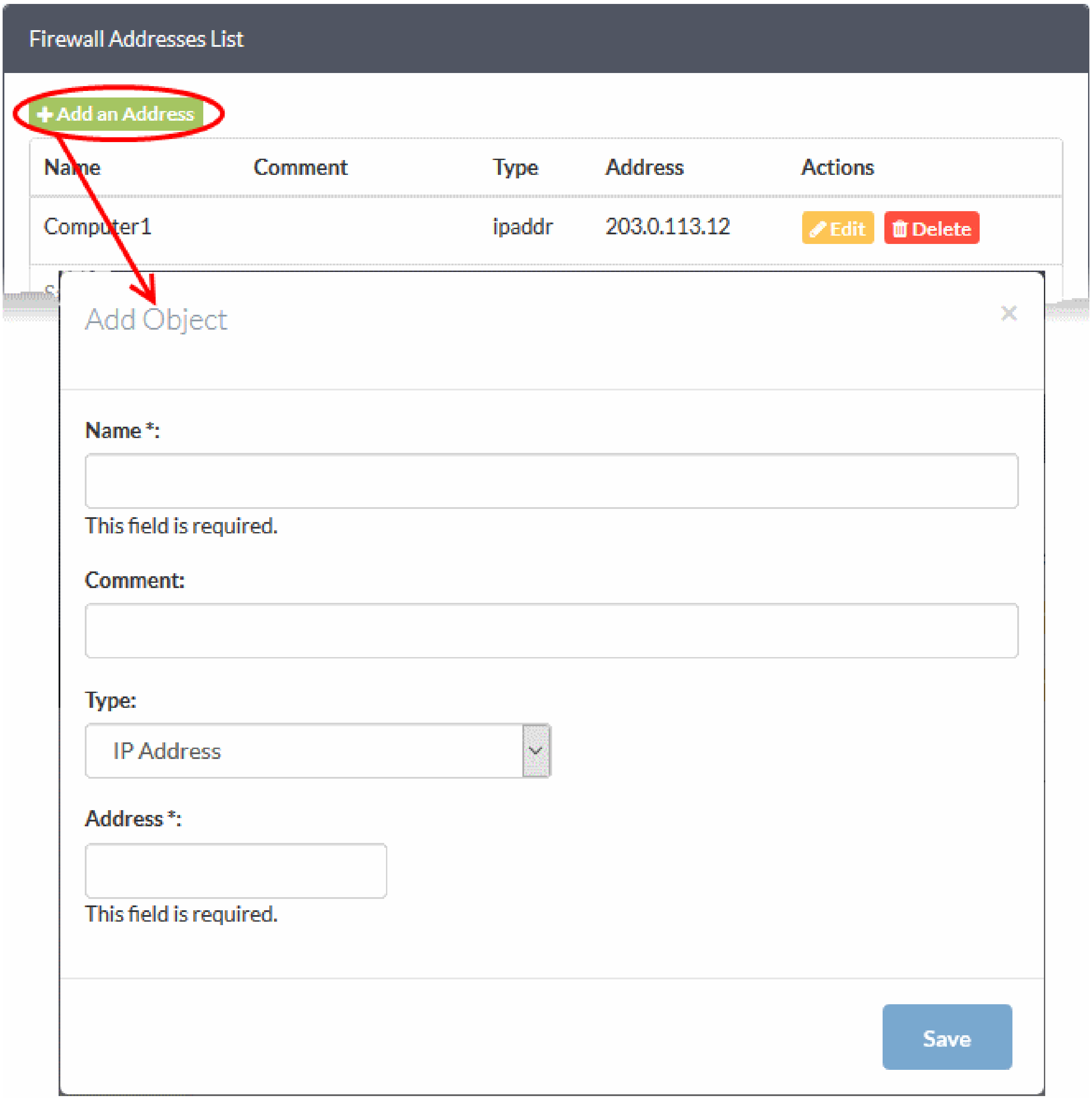
Name	Comment	Type	Address	Actions
Org 2	Devices in organization 2	ipaddr	203.0.113.12	Edit Delete

The 'Firewall Addresses' interface lists all firewall address objects added to Comodo Dome Firewall Central Manager. The objects can be added to specific devices or all devices that belong to a particular organization. The interface lets admins view, create and manage address objects.

Firewall Address List Table - Column Descriptions	
Column	**Description**
Name	Label of the firewall address object. The object name will become available for selection in the 'source' and 'destination' address fields when creating a 'Firewall Policy'.
Comment	A short description of the object
Type	Category of address. Can be IP address, IP address range, Subnet
Address	IP addresse(s) the host computer(s) contained in the object.
Actions	Displays controls for managing the object. Edit - Opens the 'Edit' interface so you can modify the parameters of the object. The edit interface is similar to the 'Add Object' interface Delete - Removes the object. **Note**: Objects which are currently referenced in a firewall rule or in a group cannot be removed. To delete an object, you must first remove it from all rules or groups in which it is included.

To create a new object

- Click 'Firewall' > 'Firewall Addresses' on the left
- Select the organization/device from the drop-down in the title bar
  - Select an organization to manage FW address objects for all devices in that organization
  - Select an individual device under an organization to manage FW address objects for a single device.
- Click 'Add an address' at the top-left
- The 'Add Object' dialog will open:


Firewall Addresses List

Name	Comment	Type	Address	Actions
Computer1		ipaddr	203.0.113.12	Edit Delete

Add Object

Name *:

This field is required.

Comment:

Type: IP Address

Address *:

This field is required.

- Enter the parameters for the new object as shown below:
    - Name - Specify a label for the object (15 characters max) representing the host(s) included in the object.
    - Comment - Enter a short description of the object.
    - Type - Select the type by which the hosts are to be referred in the object. The available options are:
        - Subnet - Select this if a sub network of computers is to be covered by the object and enter the sub network address
        - IP address - Select this if a single host is to be covered by the object and enter the IP address of the host
        - IP range - Select this if more than one host is to be covered by the object and enter the IP address range of the hosts
- Click 'Save'. The new address object will be added to the list.

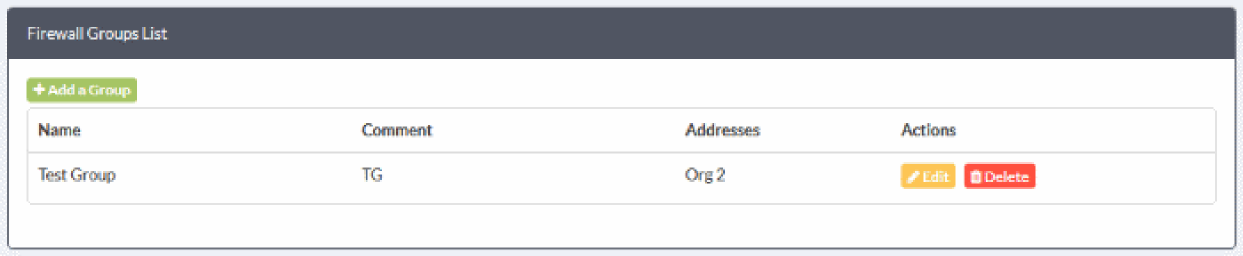
The object will be available for selection as a source or destination when creating a firewall rule. You can search for the object by typing the first few letters of the object name.

8.3 Manage Firewall Object Groups

- Firewall object groups consist of one or more IP address objects. Object groups can be created for organizations or devices.
- Administrators can reference object groups when creating and managing firewall rules.
- Object groups can be edited to change member objects. The change will be applied to all firewall rules which include the object group.
- Similar to address objects, object groups are specific to an organization or device.
- Address objects added for an individual device will be available only for that device's 'Source' and 'Destination' IP address drop down.
- Note - Existing FW group objects will not be imported with the device. We recommend you remove these from the device before importing then configure them again from central manager.

To create and manage firewall objects groups

- Click 'Firewall' > 'Firewall Groups' in the left-hand menu
- Select the organization/device on the top left of the interface
    - Select an organization to manage group objects for all devices in the organization
    - Select an individual device under an organization to manage group objects for a single device



Firewall Groups List

+ Add a Group

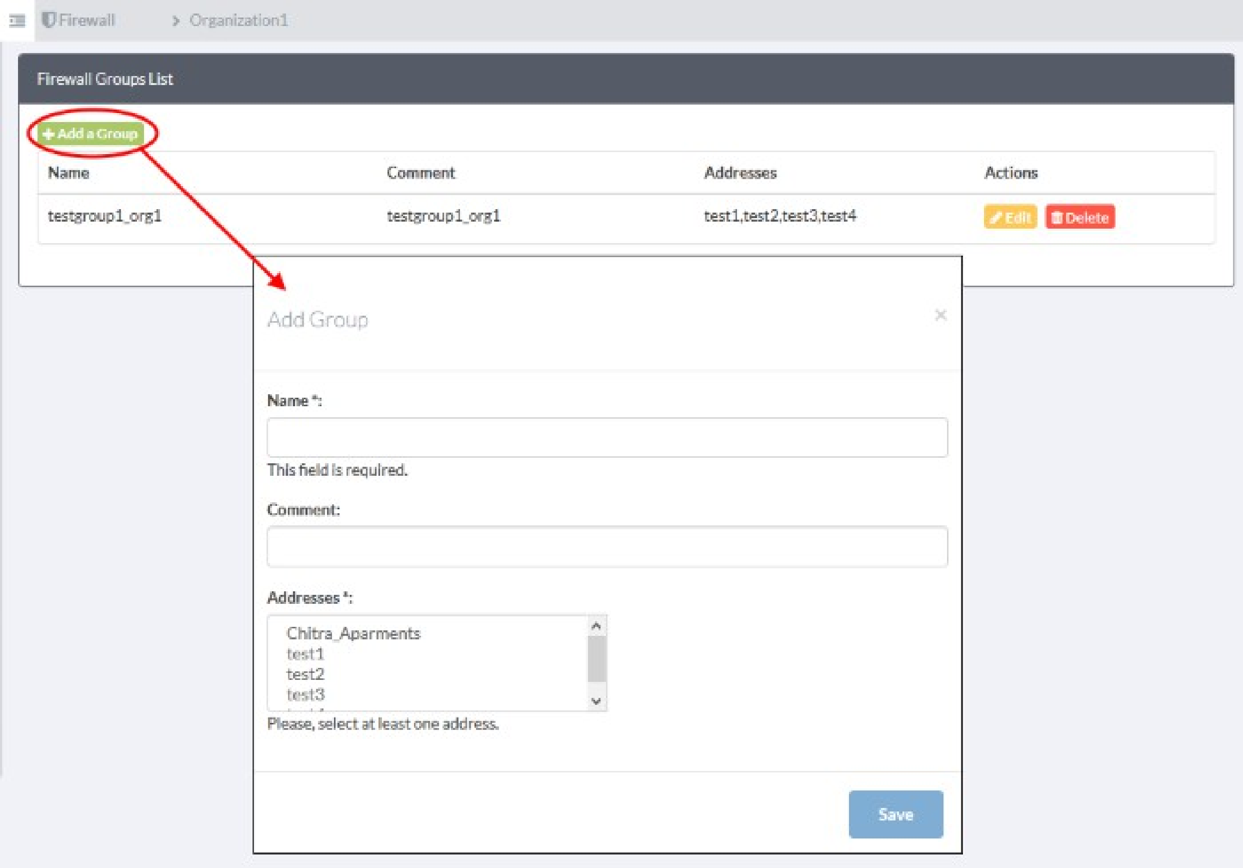
Name	Comment	Addresses	Actions
Test Group	TG	Org 2	Edit Delete

The 'Firewall Groups' list shows object groups added to specific devices / organizations. The interface allows you to view, create and manage objects groups. Groups in this list will be available when creating/managing new firewall policy.

Firewall Group List Table - Column Descriptions	
Column	**Description**
Name	Label for the firewall group. The group name will become available for selection in the 'source' and 'destination' address fields when creating a 'Firewall Policy'.
Comment	A short description of the object
Address	IP address(es) of host computer(s) contained in the object.
Actions	Controls for managing the group. Edit - Modify object settings. The Edit interface is similar to 'Add Group' interface. Delete - Removes the object. Note: Objects which are currently referenced in a firewall rule or in a group cannot be removed. To delete an group, you must first remove it from all rules or groups in which it is included.

To create a new group

- Click 'Firewall' > 'Firewall Groups' in the left-hand navigation
- Select the organization/device on the drop-down of the interface
- Click 'Add a Group' at the top-left. The 'Add Group' dialog will open:



Name	Comment	Addresses	Actions
testgroup1_org1	testgroup1_org1	test1,test2,test3,test4	Edit Delete

Name *:

This field is required.

Comment:

Addresses *:

Chitra_Aparments
test1
test2
test3

Please, select at least one address.

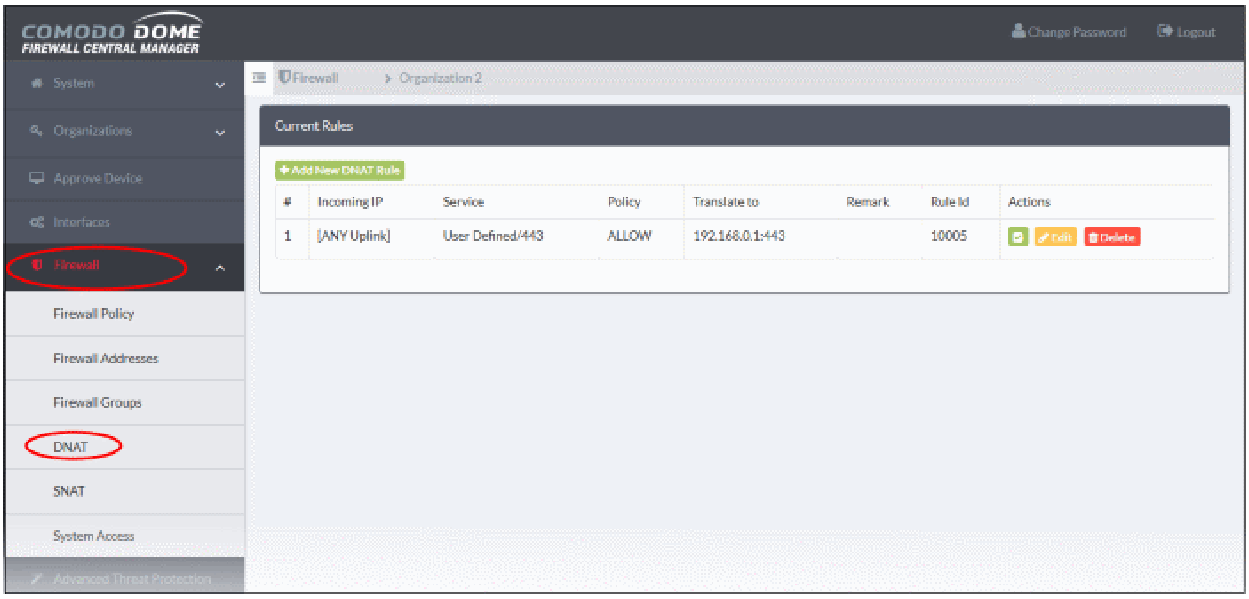
- Enter the parameters for the new object as shown below:
  - Name - Specify a label for the group (15 characters max)
  - Comment - Enter a short description of the group.
  - Address - Select the address objects that should be included in the group.
- Click 'Save'. The new group will be added to the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

8.4 Configure Destination Network Address Translation Rules

- Destination Network Address Translation (DNAT) is used to provide access to internal applications/devices from outside of the network.
  - For example, you can provide access to web, ftp, mail and other services that are located inside the network.
- The common use of DNAT is to redirect traffic sent to a public-facing IP to an internal IP / port.
- DNAT rules can be added for a device / organization
- Note - Existing FW DNAT rules will not be imported with the device. We recommend you remove these from the device before importing then configure them again from central manager.

To create and manage DNAT rules:

- Click 'Firewall' > 'DNAT' in the left-hand menu.

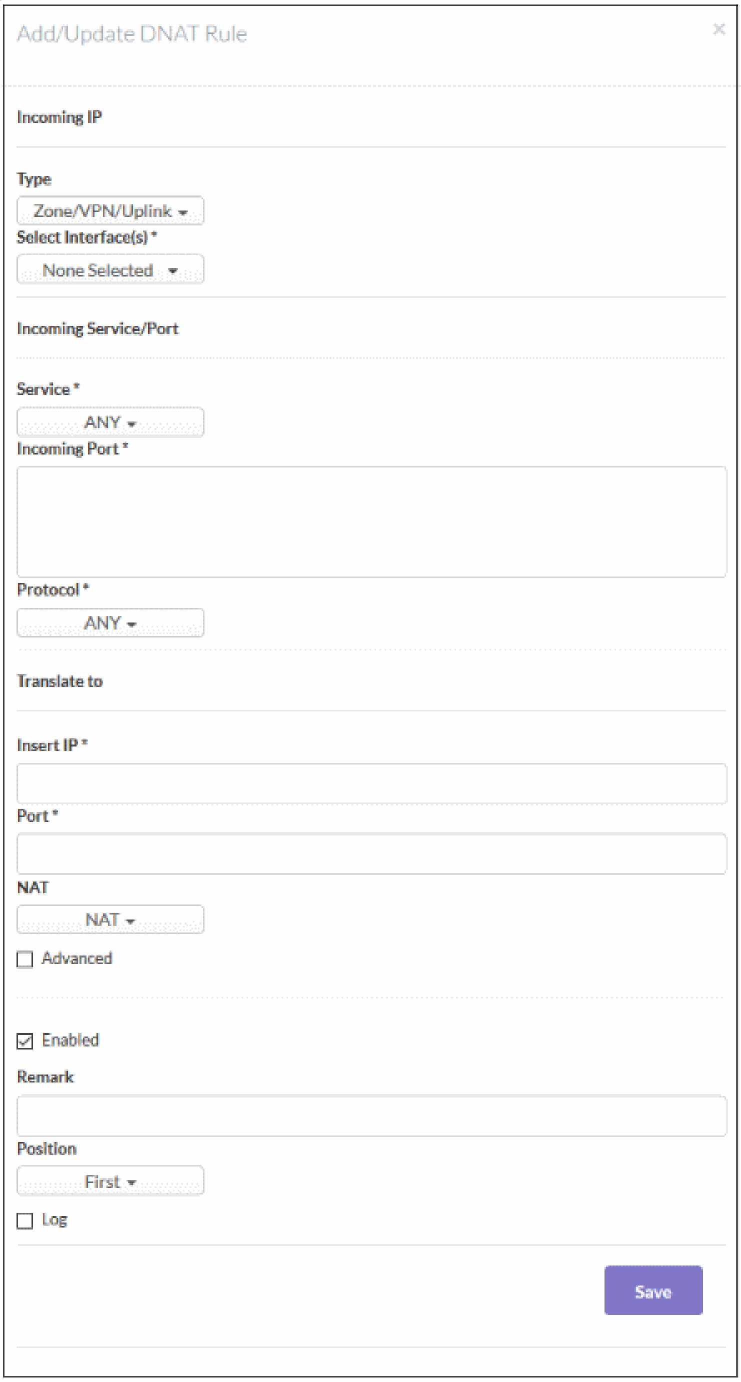


#	Incoming IP	Service	Policy	Translate to	Remark	Rule Id	Actions
1	[ANY Uplink]	User Defined/443	ALLOW	192.168.0.1:443		10005	☑ Edit Delete

DNAT Table - Column Descriptions	
Column	**Description**
#	Serial number of the rule
Incoming IP	The address that receives the traffic. This can be an internal network zone or an external network.
Service	The protocol and destination port used by the traffic
Policy	Whether traffic matching the rule should be allowed, denied or rejected
Translate to	The internal IP and port that the traffic should be forwarded to
Remark	Comments about the DNAT rule
Rule ID	ID number of the rule. Translation is applied by the first rule which meets the conditions of the traffic, regardless of any matching rules that follow.
Actions	Displays control buttons for managing the rule. ☑ - Enable or disable the rule. Edit - Modify the rule. The edit interface is similar to 'Add / Update DNAT Rule' interface. Delete - Removes the rule.

To create a DNAT rule

- Click 'Firewall' > 'DNAT' on the left
- Select the organization to which the device belongs or, alternatively, select an individual device.
- Click the 'Add New DNAT Rule' link at the top left.
- The 'Add / Update DNAT Rule' dialog will open.



Add/Update DNAT Rule

Incoming IP

Type: Zone/VPN/Uplink

Select Interface(s) *: None Selected

Incoming Service/Port

Service *: ANY

Incoming Port *

Protocol *: ANY

Translate to

Insert IP *

Port *

NAT: NAT

□ Advanced

☑ Enabled

Remark

Position: First

□ Log

- **Incoming IP -** Select the type of incoming source and specify the source in the text box below it. The options available are:
  - Zone/ VPN/ Uplink – The interfaces configured in the '**Interface Configuration**' screen will be available for selection. Select this option if the incoming source is a network zone or an Interface connected to the virtual appliance. Choose the network zone and/or the interface from the options listed in the text box. Press and hold the Ctrl key in the keyboard to choose multiple zones/interfaces.
  - Network/ IP/ Range - Select this option if the rule is to be applied to incoming traffic from a network IP or from a specific IP address or address range. Enter the IP address of the network(s) in CIDR notation or the specific IP address(es) or address range in the text box, as one entry per line.
  - SSL VPN User - Select this option if the rule is to be applied to traffic from VPN user(s) added to the network. Choose user(s) from the list of pre-registered users displayed in the textbox. Press and hold the Ctrl key in the keyboard to choose VPN users.
- **Incoming Service / Port -** Specify the service, protocol and incoming destination port for the rule.

- Service - Select the service type.
- Incoming port - Select the destination port for the service. Usually this field will be auto selected based on the service selected.
- Protocol - Select the protocol for the service. Usually this field will be auto selected based on the service selected.

- **Translate to –** Specify to which IP and port the incoming traffic should be forwarded to. Select whether network address translation should be performed or not.
  - Insert IP – Enter the IP to which the traffic should be forwarded to. Note – You have to specify a single IP only.
  - Port – Enter the port number / port range to which the incoming traffic should be forwarded to.
  - NAT – Select whether network address translation should be done or not. If you select 'Do not NAT', destination address translation will not be performed.
- **Advanced Mode -** Allow traffic from specific sources and choose whether traffic for a matching DNAT rule should be allowed, dropped or rejected.
  - Select the type of incoming source from the drop-down. Press and hold the Ctrl key in the keyboard to choose multiple sources.
  - Filter Policy – Select whether network packets from a matching rule should be allowed, dropped or rejected from the drop-down.
- **General Settings -** Configure the general settings to enable/disable, enter a short description and select a position for the rule in the list.
  - Enabled - Leave this checkbox selected if you want the rule to be activated upon creation.
  - Remark - Enter a short description for the rule. The description will appear in the remark column of the respective rules interface
  - Position - Set the priority for the rule in the list of rules in the respective rules interface. The rules are processed in the order they appear on the list.
  - Log - Select this checkbox if you want the packets allowed by the rule are to be logged.
- Click 'Save'. The new DNAT rule will be created and applied to the selected organization or device.

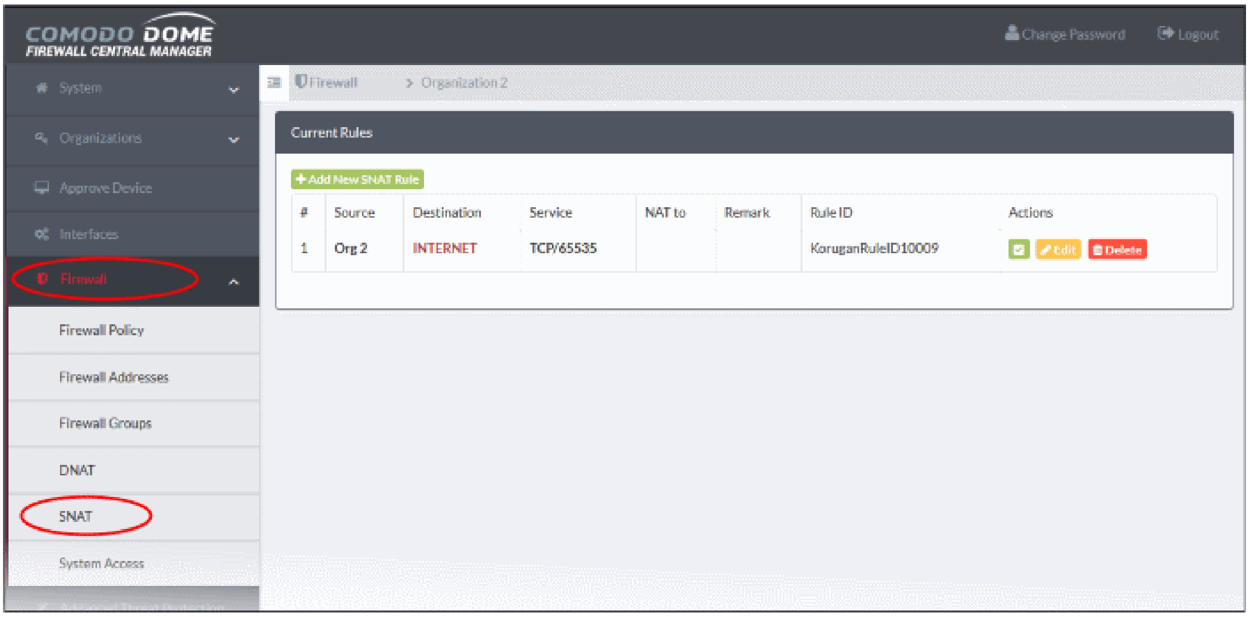
DNAT rule management activities are logged in System > Tasks. See '**View Management Tasks**' for more details.

8.5 Configure Source Network Address Translation Rules

- Source Network Address Translation (SNAT) is used when a private / internal host needs to connect to an public / external host.
  - For example, when an internal host is running a web or mail service and the outgoing packets should be from a public facing IP address.
- SNAT rules can be added for a device / organization
- Note – Existing SNAT rules will not be imported when you add a device. We recommend you remove them from the device before importing then configure them again from central manager.

To create and manage SNAT rules:

- Click 'Firewall' > 'SNAT' in the left-hand menu.



Current Rules

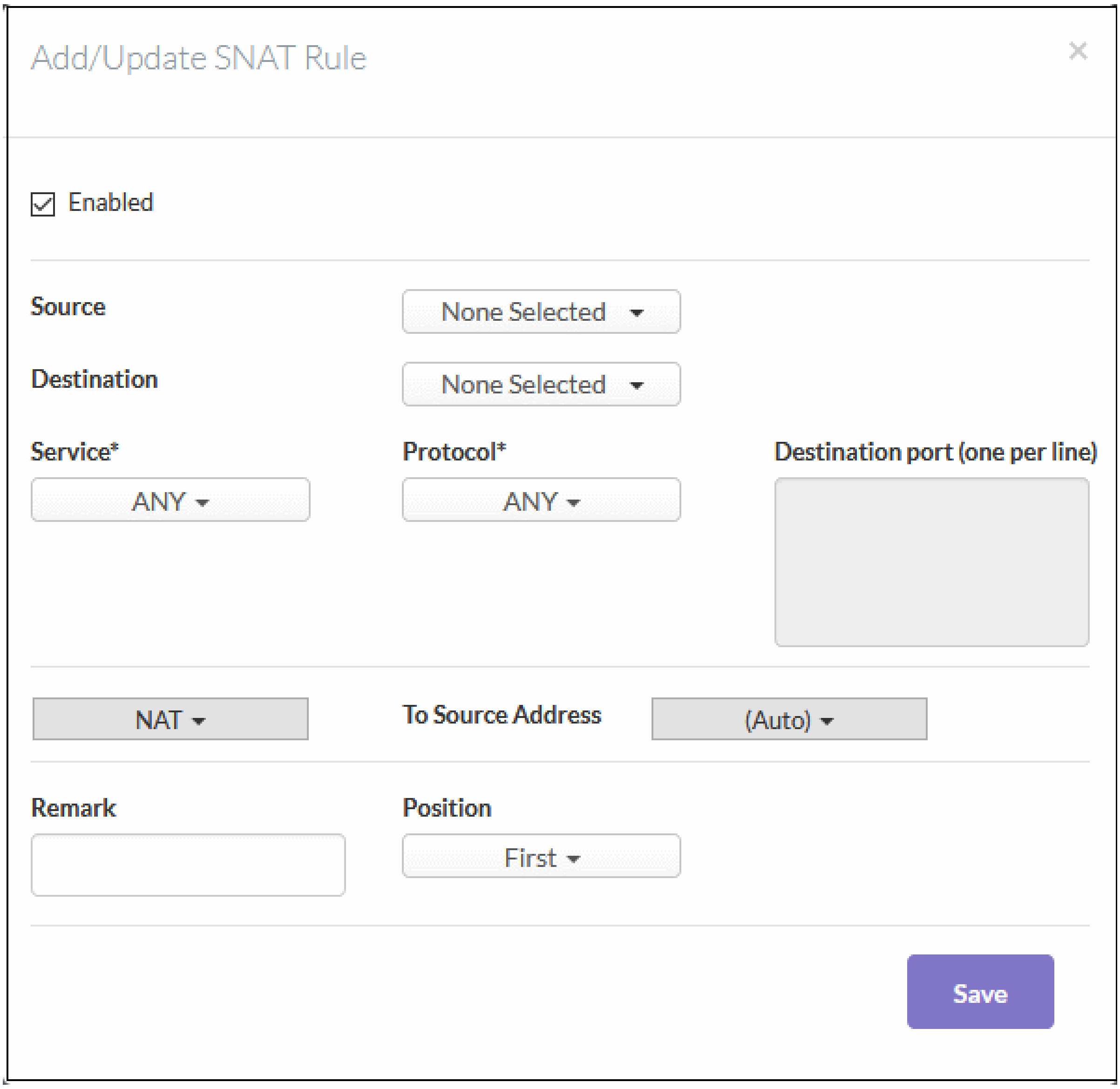
+ Add New SNAT Rule

#	Source	Destination	Service	NAT to	Remark	Rule ID	Actions
1	Org 2	INTERNET	TCP/65535			KoruganRuleID10009	☑ Edit Delete

SNAT Table - Column Descriptions	
Column	**Description**
#	ID number of the rule. Translation is applied based on the first matching rule in the list, regardless of other matching rules that follow.
Source	The firewall object containing the IP address, IP address range or subnet of the host(s) from which the traffic originates
Destination	The interface through which traffic is directed to the external network
Service	The protocol and port used by the traffic
NAT to	The address to which this traffic should be redirected
Remark	A short description of the rule
Rule ID	A unique identifier for the SNAT rule. This helps identify the rule in the back-end of the console.
Actions	Controls for managing the rule. ☑ - Enable or disable the rule. Edit - Edit rule parameters. The 'Edit' interface is similar to the 'Add/Update Rule' interface. Delete - Removes the rule.

To create an SNAT rule

- Click 'Firewall' > 'SNAT' on the left menu
- Click 'Add New SNAT Rule'. The 'Add/Update Rule' dialog will open:



Add/Update SNAT Rule

☑ Enabled

Source: None Selected

Destination: None Selected

Service*: ANY

Protocol*: ANY

Destination port (one per line)

NAT

To Source Address: (Auto)

Remark

Position: First

- **Enabled -** Leave this checkbox selected if you want the rule to be activated after saving.
- **Source –** Firewall Address object/object group from which traffic originates. Select the required object from the drop-down menu.
- **Destination –** Specify the interface / firewall address object / object group to which traffic is sent. See '**Manage Firewall Address Objects**' to find out how to create address objects.
- **Service / Protocol / Destination Port -** Select the type of service hosted by the source, its protocol and ports.
- **NAT -** Choose whether or not to apply network address translation. The options available are:
  - No NAT - Network Address Translation will not be applied
  - Map Network - All IPs from the source subnet will be statically mapped to another network of the same size. Specify the subnet to which the IPs are to be mapped in the textbox at the right.
  - NAT (to Source Address) - Traffic will be directed to the address you select from the 'To source address' drop-down.

General Settings:

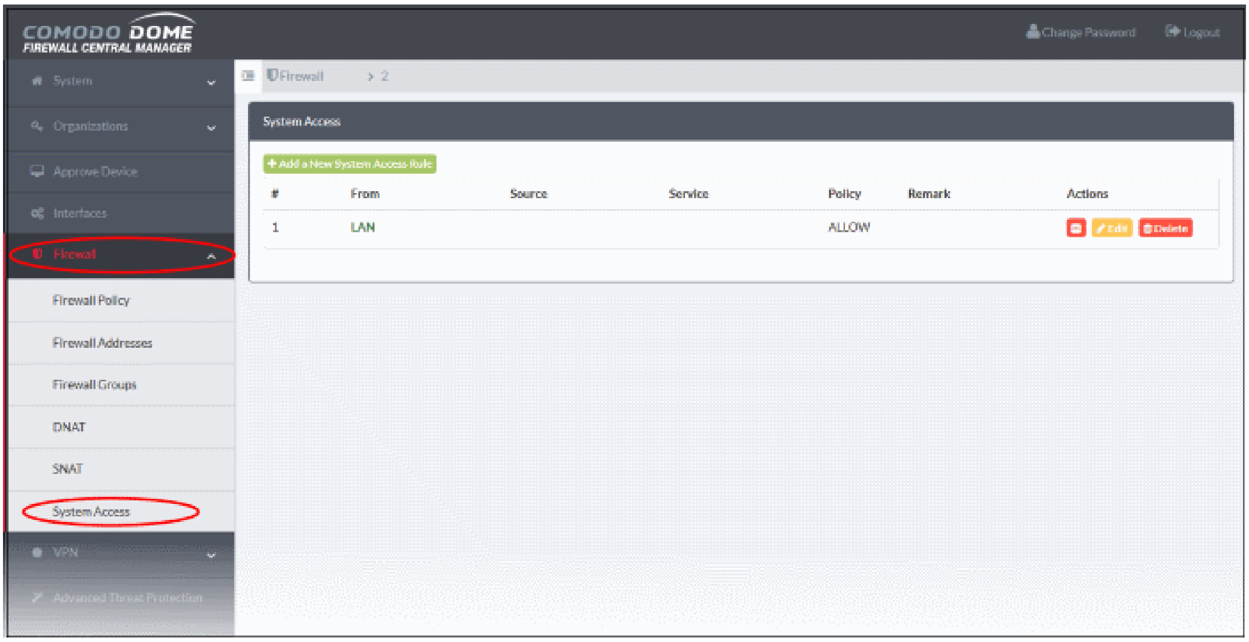
- **Remark -** Enter a short description of the rule (optional). The description will appear in the 'Remark' column of the respective rule
- **Position -** Set the priority of the rule among the rules listed in the rules interface. The rules are

processed in the order they appear on the list.

- Click 'Save'. The new SNAT rule will be created and applied to the selected organization or device.

8.6 Configure System Access Rules

- System access rules govern the rights that various hosts and zones have to access a firewall device.
- Click 'Firewall' > 'System Access' on the left to open the rules interface.
- Select a firewall device or organization from the gray bar above the table.
- The system access table shows all existing access rules for the organization or device, and allows you to add new rules.



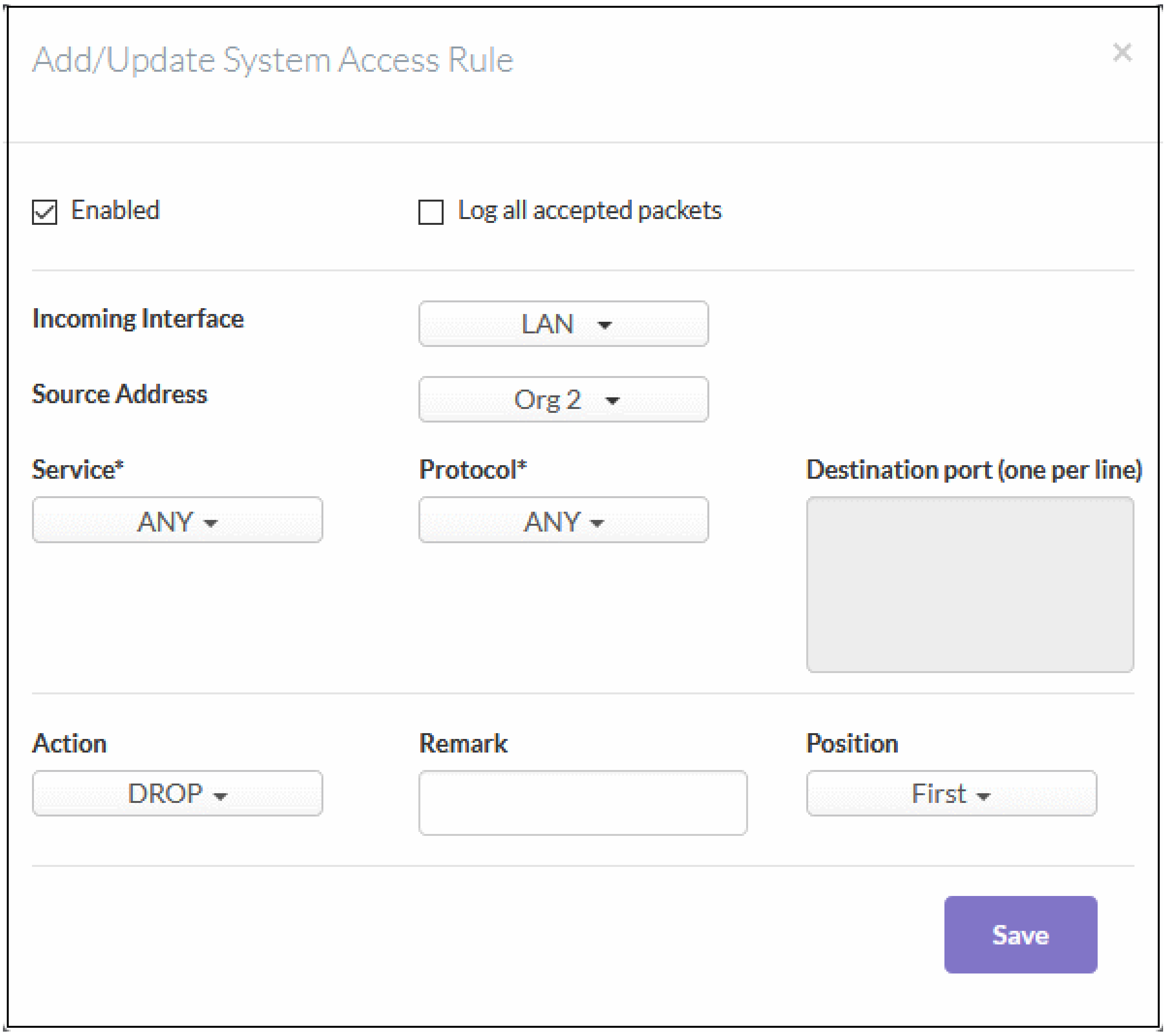
#	From	Source	Service	Policy	Remark	Actions
1	LAN			ALLOW		Edit Delete

System Access Rules Table - Column Descriptions	
Column	**Description**
#	ID number of the rule. A packet is allowed or denied based on the first matching rule in the list, regardless of other matching rules that follow.
From	The interface over which traffic is received. E.g. 'LAN', 'Internet', 'WiFi'.
Source	The firewall address object/object group from which traffic originates.
Service	The port and protocol used by traffic which will be affected by this rule.
Policy	Action taken on traffic affected by this rule.
Remark	A short description of the rule
Actions	Controls for managing the rule. ☑ - Enable or disable the rule. Edit - Edit rule parameters. The 'Edit' interface is similar to the 'Add/Update System Access Rule' interface.

	Delete - Removes the rule.

To create a new rule

- Click 'Firewall' > 'System Access' on the left
- Select a firewall device or organization from the gray bar above the table.
- Click the 'Add a New System Access Rule' link button. The rule configuration screen will open:



Add/Update System Access Rule

☑ Enabled

□ Log all accepted packets

Incoming Interface: LAN

Source Address: Org 2

Service*: ANY

Protocol*: ANY

Destination port (one per line)

Action: DROP

Remark

Position: First

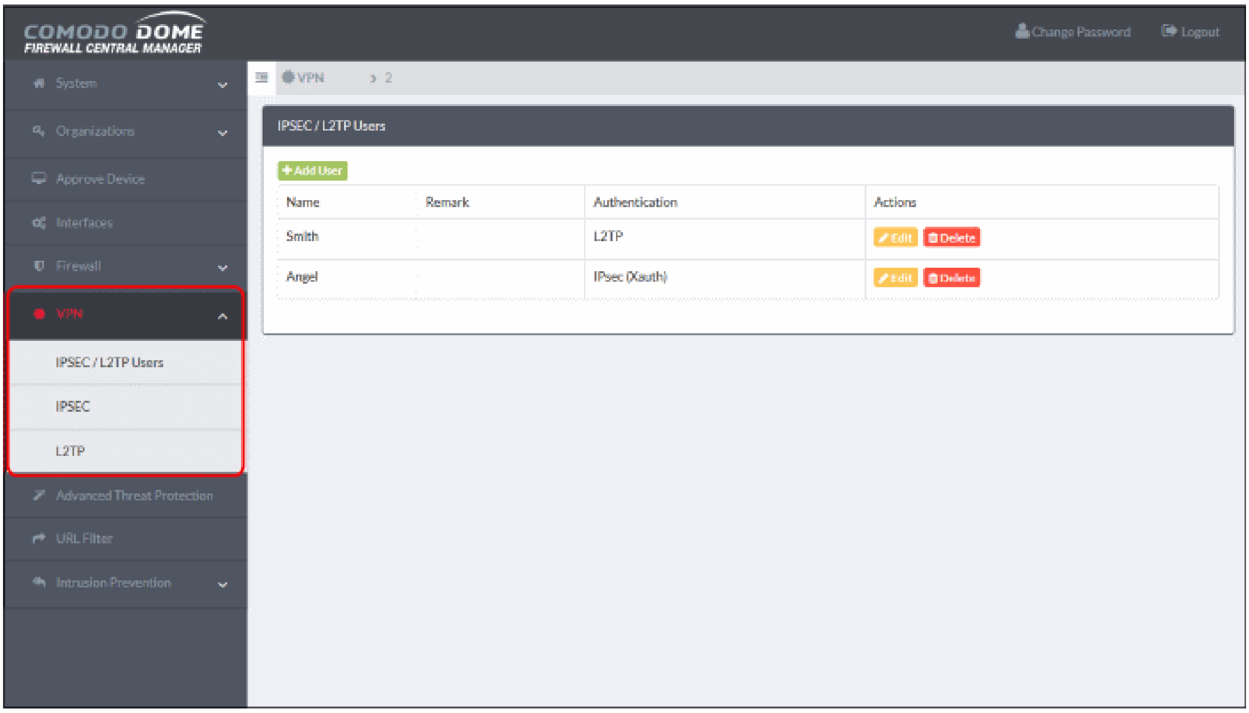
- **Enabled -** Leave selected if you want the rule to be activated immediately after saving. You can enable or disable the rule later in the rules list if required.
- **Log all accepted packets -** Enable to create a record of all data packets accepted by the rule.
- **Incoming Interface -** Select the interface from which traffic is received
- **Source Address -** The firewall address object/object group from which traffic originates.
- **Service/Protocol/Port-**
  - **Service -** Choose the service over which the traffic is sent. Selecting a service will auto-populate the 'Protocol' and 'Destination Port' fields. You can, of course, edit the port fields if required.
  - **Protocol -** Choose the protocol used by the service. Selecting a protocol will change the 'Service' to 'User defined'. Assuming a match on incoming interface and source address, the rule will affect all traffic using the chosen protocol regardless of service type.
  - **Destination port -** Specify the destination port(s) of the service one by one.

- **Action -** Specify whether packets matching the rule should be allowed or denied. The options available 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 (optional)
  - **Position -** Set the priority for the rule in the list of rules in the respective rules interface. The rules in the IP tables are processed in the order that appears on the list.
- Click 'Save'. The new system access rule will be created and applied to the selected organization or device.

9 Configure Virtual Private Network Settings

The VPN section lets you configure IPSec and L2TP settings, and add IPSec / L2TP end-users for managed firewalls.

- IPSec / L2TP Users – Add and manage end-users.
- IPsec - Configure and connect network and clients to Dome Firewall.
- L2TP Server – DFW acts as a L2TP server to connect remote L2TP clients to local zones via IPSec VPN tunnel.



Name	Remark	Authentication	Actions
Smith		L2TP	Edit Delete
Angel		IPsec (Xauth)	Edit Delete

The following sections provide detailed descriptions of different VPN services and their configuration:

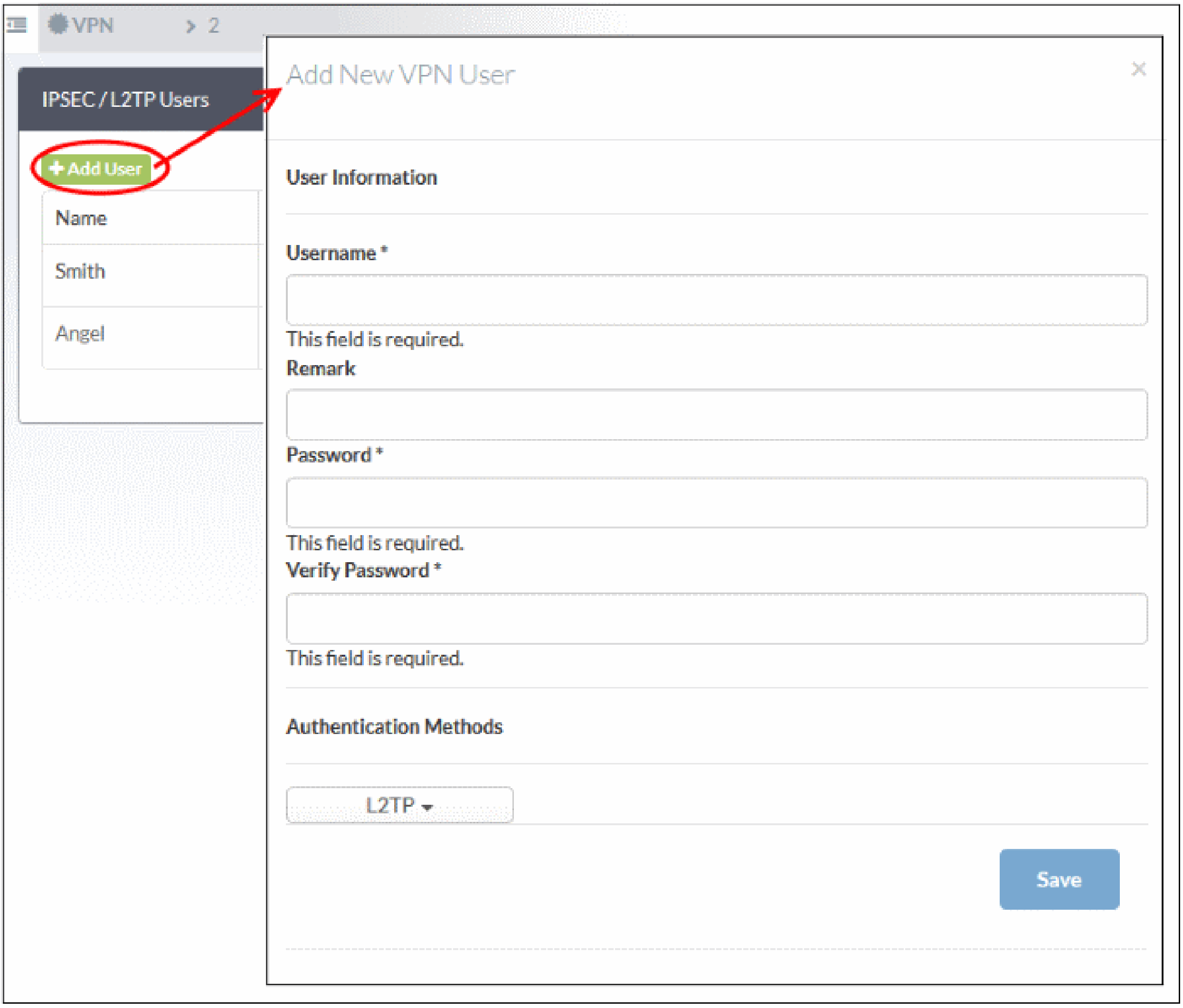
- **IPsec / L2TP Users Configuration**
- **IPsec Configuration**
- **L2TP Server Configuration**

9.1 Configure IPSec/L2TP Users

- Click 'VPN' > 'IPSec / L2TP Users' in the left-hand menu
- This area lets you add users for managed organizations that need to connect to the internal network via IPSec VPN tunnel
    - Note 1 - You need to configure **IPSec** and **L2TP** servers before the users you add can connect.
    - Note 2 - Existing users are not imported when you add a device to central manager. We recommend you remove them from the device before importing then configure them again in central manager.

Add a new user account

- Click 'VPN' > 'IPSec / L2TP Users' on the left
- Select a target device or organization from the gray bar above the table
- Click 'Add User':



- **Username / Password** - Specify the credentials that the user will use to log into the IPSec VPN.
- **Remark** – Add comments about the account that may be important for other admins to know.
- **Authentication Method** - The method by which this user will authenticate themselves to the VPN.

  Choose from:

    - IPsec (Xauth) – Used for net-to-net connections between sites.
    - IPsec (EAP) - Used for net-to-net connections between sites.

- L2TP – Useful for authenticating mobile devices to the firewall

Note – You have to choose at least one type of authentication.

Click 'Save' The user will be added to the list.

9.2 IPSec Configuration

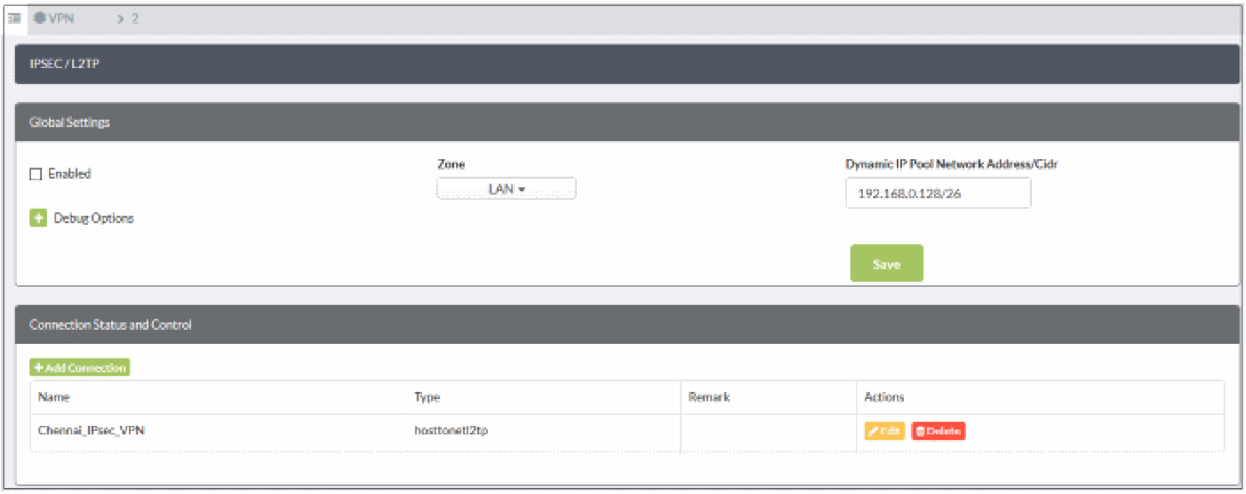
- Click 'VPN' on the left then 'IPSec'

The IPSec area lets you configure tunnels between different networks and sites for managed organizations.

- Dome Firewall supports two types of VPN protocols:
  - **'Net-to-Net' VPN connections** (aka 'Site-to-Site VPN') - Connect network to network via IPSec VPN.
  - **L2TP Host to Net VPN** – Connect external devices with L2TP clients to internal networks through an IPsec VPN.
- Note – Existing IPsec connections are not imported when you add a device. We recommend you remove them from the device before importing, then configure them again in central manager.
- Once configured, the IPSec connection type is available as a firewall object. This can be used in the source and destination address fields of a FW rule.

Configure IPSec settings and add tunnels

- Select a firewall device or organization from the gray bar above the table
- Click 'VPN' on the left then select 'IPSec'



□ Enabled

Zone: LAN

Dynamic IP Pool Network Address/Cidr: 192.168.0.128/26

Name	Type	Remark	Actions
Chennai_IPsec_VPN	hosttonetl2tp		Edit Delete

Use this interface to create, configure and monitor IPsec connections, and to configure authentication preferences. You can implement authentication between IPsec connected devices by pre-shared key.

The interface contains two areas:

- Global Settings
- Connection Status and Control

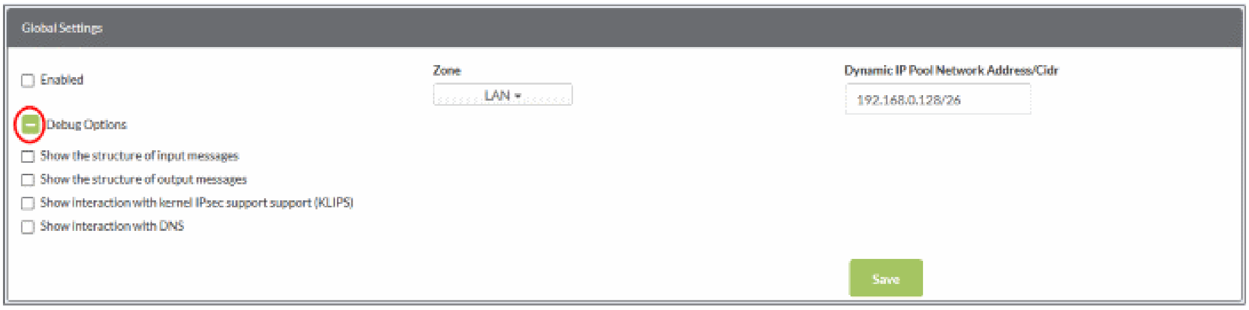
Global Settings

The 'Global Settings' area allows you to:

- Enable or disable the IPsec VPN service
- Configure which internal network zones can be accessed over IPsec

- Specify the dynamic IP address pool that should be used when assigning addresses to external clients.

The 'Debug Options' area allows you to choose how much information is included in IPsec events in debugging logs.


Global Settings

☐ Enabled

Zone: LAN ▾

Dynamic IP Pool Network Address/Cidr: 192.168.0.128/26

⊟ Debug Options

☐ Show the structure of input messages

☐ Show the structure of output messages

☐ Show interaction with kernel IPsec support support (KLIPS)

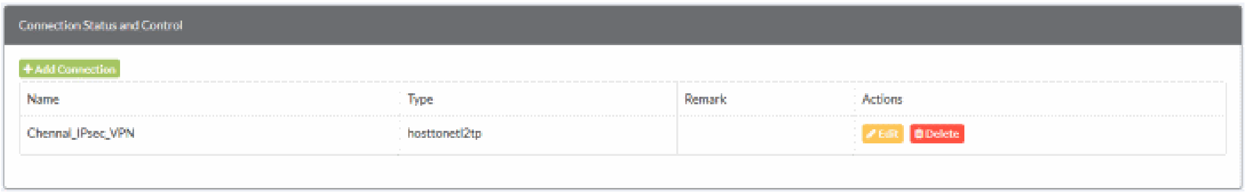
☐ Show interaction with DNS

- **Enabled** – Activate or deactivate the IPsec VPN service
- **Zone** - Choose the internal network to which external clients/networks will connect over the VPN.
- **Dynamic IP pool network address/cidr** – The range of addresses from which IPs are drawn and dynamically assigned to external clients.
- **Debug options –** The level of detail that should be logged about an IPsec event such as a connection failure. The log file is stored at /var/log/messages on the virtual appliance. Click the '+' button to view further options.

- Click 'Save' for your settings to take effect

Connection Status and Control

- Select a firewall device or organization from the gray bar above the table
- Click 'VPN' on the left then select 'IPSec'
- The 'Connection Status and Control' area of the page lets you view, edit and add IPsec tunnels.

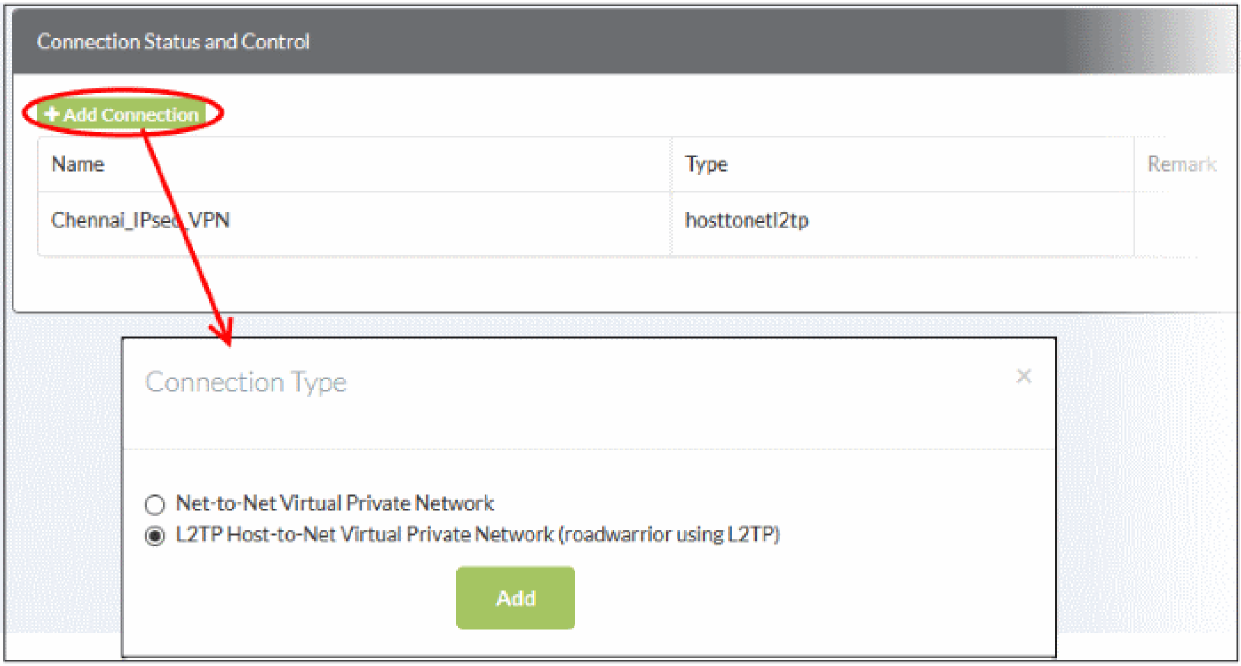

Connection Status and Control

Name	Type	Remark	Actions
Chennai_IPsec_VPN	hosttonetl2tp		Edit Delete

- Name - Label to identify the connection.
- Type - The type of tunnel - site-to-site or host-to-net.
- Remark - A short description of the tunnel.
- Actions – Edit or delete a VPN connection. Editing a connection is similar to adding a new connection explained **below**.

Add a New Tunnel Configuration

- Select a firewall device or organization from the gray bar above the table
- Click 'VPN' on the left then select 'IPSec'
- Click 'Add Connection' in the 'Connection Status and Control' area



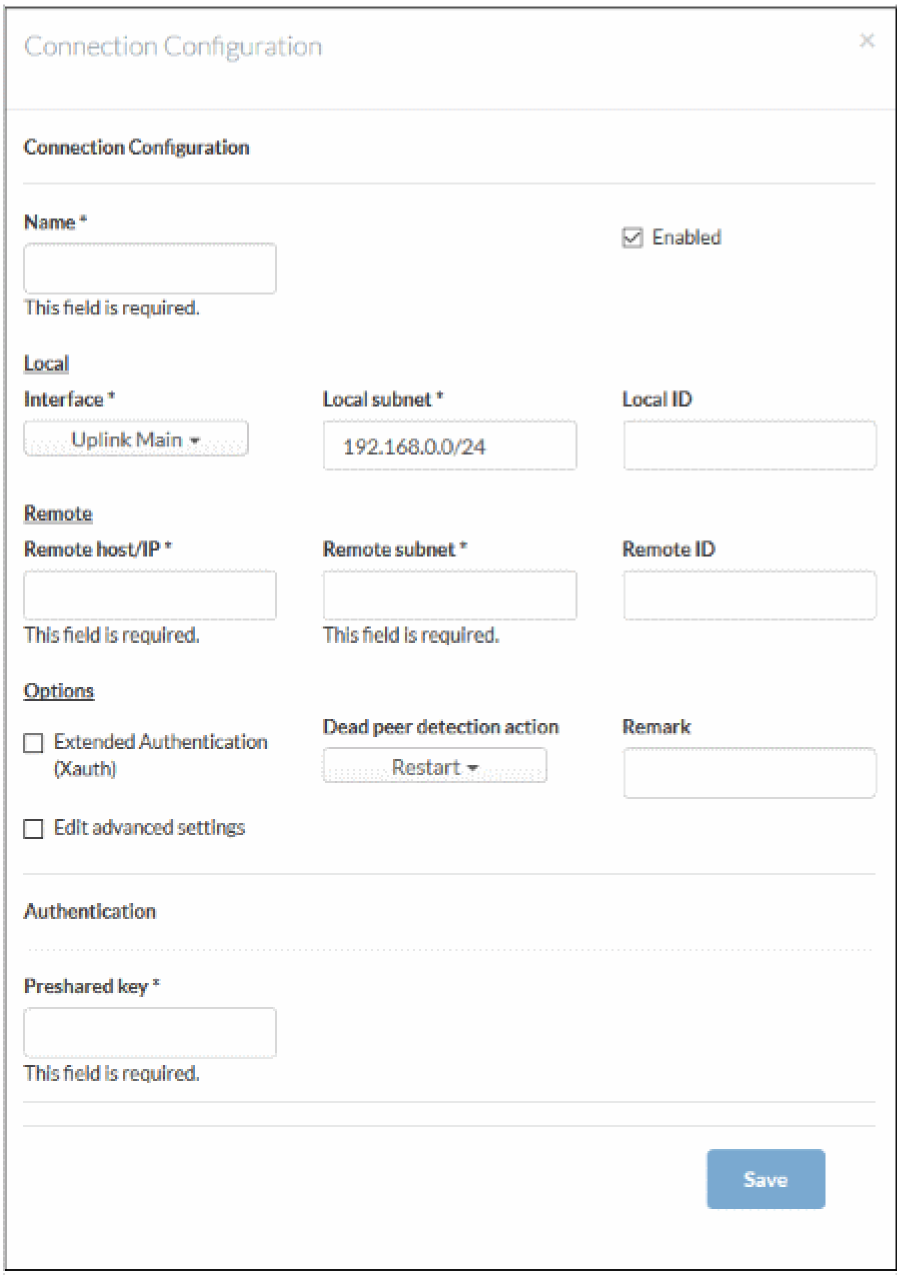
Name	Type	Remark
Chennai_IPsec_VPN	hosttonetl2tp	

Connection Type

○ Net-to-Net Virtual Private Network

● L2TP Host-to-Net Virtual Private Network (roadwarrior using L2TP)

- Choose the connection type and click 'Add'
  - You next have to configure the connection.
  - The interface is the same for both types of connection, except that 'Net to Net' connections have an additional parameter - 'Remote subnet'.



Connection Configuration

Connection Configuration

Name *

☑ Enabled

This field is required.

Local

Interface * Uplink Main

Local subnet * 192.168.0.0/24

Local ID

Remote

Remote host/IP *

This field is required.

Remote subnet *

This field is required.

Remote ID

Options

☐ Extended Authentication (Xauth)

Dead peer detection action Restart

Remark

☐ Edit advanced settings

Authentication

Preshared key *

This field is required.

Connection Configuration

- **Name** - Create a label to identify the tunnel
- **Enabled** - The tunnel will be activated after you click 'Save'. Do not select this if you just want to configure the connection and enable it later.

Local

- **Interface –** The uplink interface on the DFW virtual appliance through which the external client should connect to the local network.
- **Local Subnet** - This field is auto-populated with the local sub-net of the LAN. If you want to specify a different subnet, enter the address in CIDR format.
- **Local ID** - Enter an identification string for the local network.

Remote

- **Remote host/IP** - IP address or hostname of the external host or network
- **Remote subnet** - The option is available only if you are creating 'Net to Net' connection type. Specify the sub-net of the external network that can connect through the tunnel

- **Remote ID** - Enter an identification string for the local network.

Options

- **Extended Authentication (Xauth)** - Select if you want to enable additional, certificate based authentication for the remote client. You must install the client certificate on to the external client if you select this option.
- **Dead peer detection action** - Choose the action the firewall should take if the peer disconnects. The options available are:
    - Clear - Disconnect
    - Hold - Wait for the peer to reconnect
    - Restart - Reboot the peer
- **Remark** - Enter a short description of the connection
- **Edit advanced settings** - Advanced parameters can be edited only after saving the tunnel configuration. See **edit advanced parameters of IPsec tunnel configuration** for more details.

Authentication

- Use a pre-shared key - Select this option if you wish to apply PSK type authentication for the remote client. Enter the password to be used for authentication by the remote client.

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

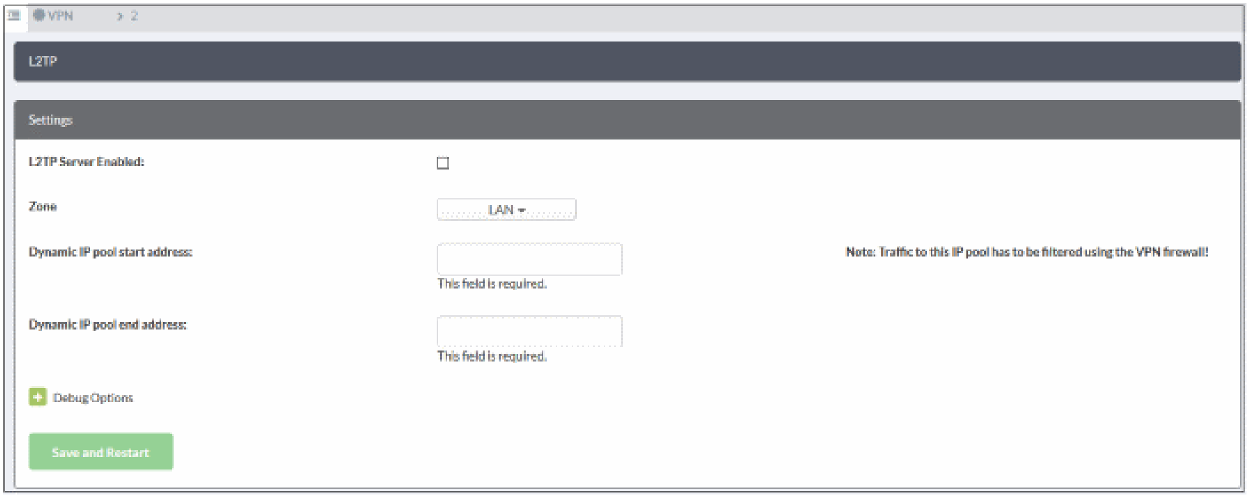
The connection will be added to the **Connection status and control** area.

9.3 Configure L2TP Server

- Click 'VPN' > 'L2TP' in the left-hand menu to open the L2TP server interface
- Dome Firewall allows remote clients using Layer 2 Tunneling Protocol (L2TP) to connect to an IPsec VPN tunnel.
- You need to enable L2TP server on the appliance in order to allow L2TP clients.
- Note - Existing L2TP server configurations are not imported when you add a device. We recommend you remove them from the device before importing, then configure them again in central manager.

To configure L2TP server

- Select a firewall device or organization from the gray bar above the table
- Click 'VPN' on the left then select 'L2TP'



VPN > 2

L2TP

Settings

L2TP Server Enabled: □

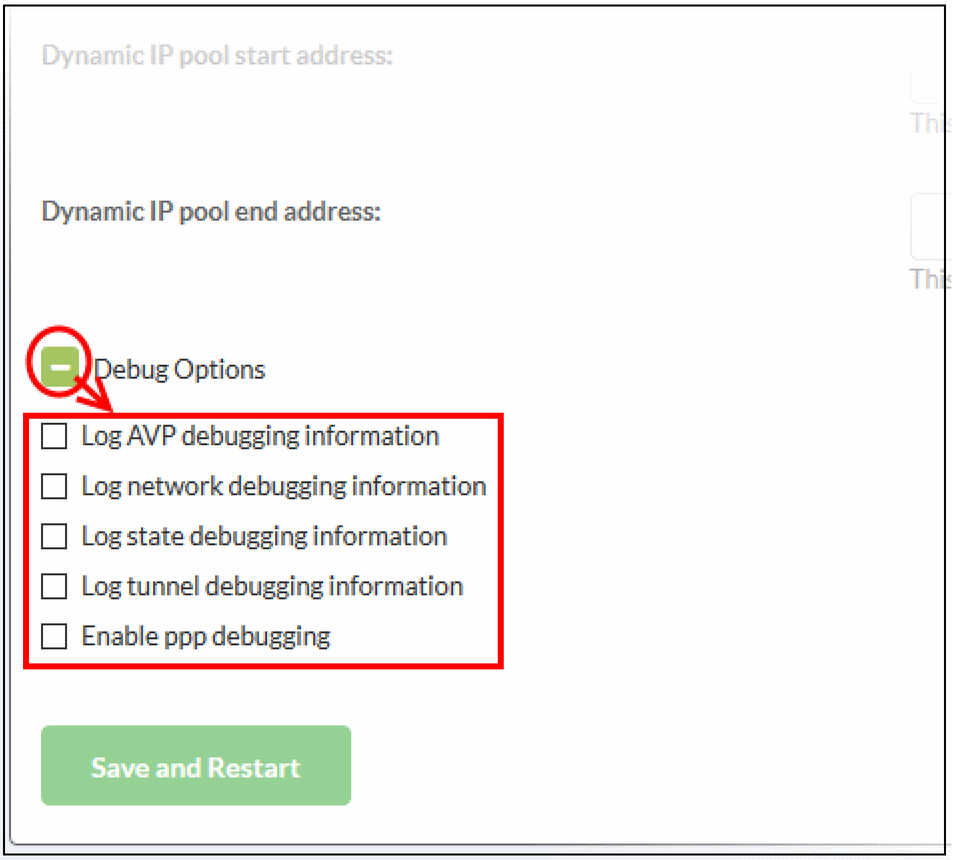
Zone: LAN ▾

Dynamic IP pool start address: This field is required.

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

Dynamic IP pool end address: This field is required.

- **L2TP Server Enabled** – Activate the L2TP service
- **Zone** - Choose the internal zone which external clients/networks will access over the IPsec VPN
- **Dynamic IP pool start address/end address** -The IP range from which addresses are assigned to external clients connecting over L2TP
- **Debug options** - Configure the level of detail logged for L2TP events in the event of connection failures. The log file is stored at /var/log/messages on the appliance. Click the '+' button to view further options.



Dynamic IP pool start address:

Dynamic IP pool end address:

□ Log AVP debugging information
□ Log network debugging information
□ Log state debugging information
□ Log tunnel debugging information
□ Enable ppp debugging

- Click 'Save and restart'. The VPN server will be restarted for your configuration to take effect.

In order to allow several L2TP users to connect through the IPsec tunnel, the end users have to be created for the service. See '**Configure IPSec / L2TP Users**' for more details.

10 Manage Advanced Threat Protection Profile

- Click 'Advanced Threat Protection' on the left to open this interface.
- Advanced Threat Protection (ATP) safeguards networks against malware, hack attempts, data breaches and other attacks.
- ATP scans internet downloads and email attachments with a combination of antivirus scans, behavior analysis and blacklist checks.
- This interface lets you configure ATP profiles for organizations and devices.
- You can then select these profiles when creating firewall rules for organizations and devices.

ATP uses the following techniques to analyze files:

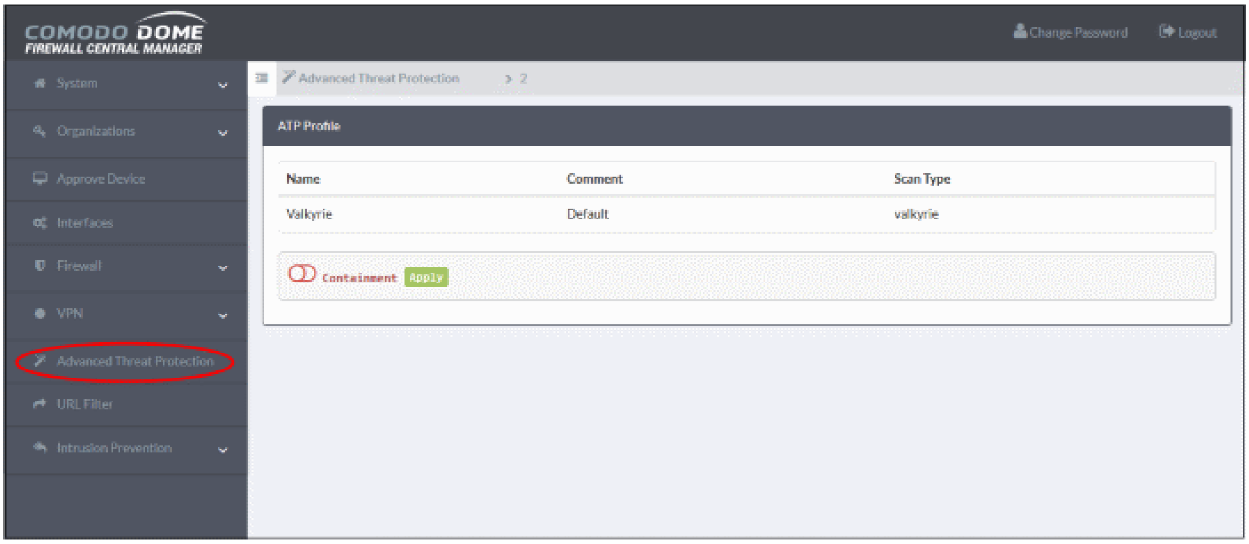
- **Comodo Antivirus -** Continuously updated antivirus scanner which provides dependable protection against known malicious files.
- **Comodo Valkyrie -** A cloud based behavior analysis service which improves detection of zero-day threats by rigorously testing the run-time actions of unknown files.

The antivirus and Valkyrie tests provide a trust verdict for each file. There are three possible verdicts:

- **Safe** – Trusted files. These are allowed to run on the endpoint.
- **Threats** – Malicious files. These are automatically blocked and a warning shown on the endpoint.
- **Unknown -** Files that could not be identified as safe or threatening are classified as 'Unknown'. Users are not allowed to download these files directly. Instead, they are are wrapped in Comodo's containment technology and forwarded to the endpoint. When executed, the file runs in a secure virtual environment and is not allowed to access other processes or user data.

The ATP Profile

- Click 'Advanced Threat Protection' on the left to open the interface.



ATP Profile

Name	Comment	Scan Type
Valkyrie	Default	valkyrie

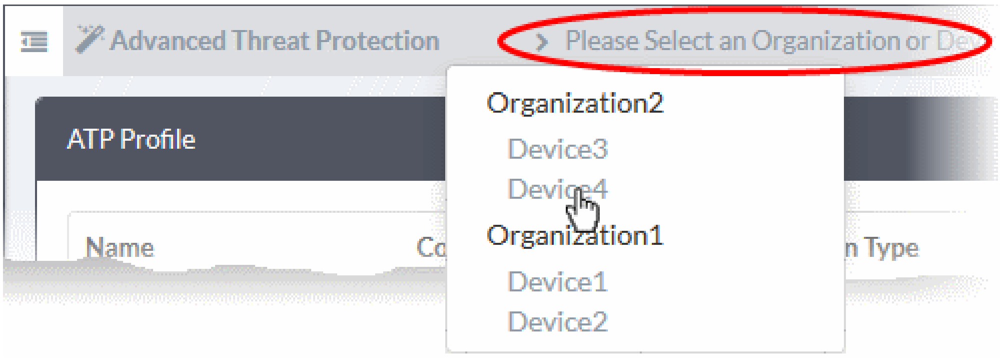
Containment Apply

The ATP profile defines types of scan applied to files downloaded by end-users. You can also choose whether or not to apply containment to unknown files.

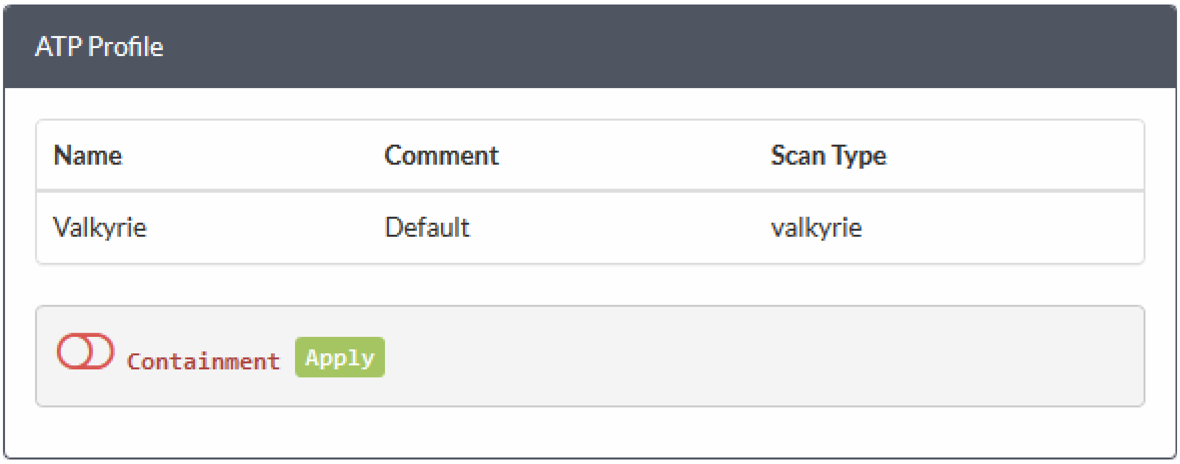
By default, a profile with Valkyrie analysis is available. You can configure whether or not auto-containment is also enabled on the profile.

To configure an ATP profile for an organization or device

- Click 'Advanced Threat Protection' on the left.
- Select a target organization/device by clicking the link in the gray bar.
  - Organization – applies the profile to all devices in the organization
  - Device – applies the profile to an individual device



This opens the ATP profile for the target org/device:


ATP Profile

Name	Comment	Scan Type
Valkyrie	Default	valkyrie

- Use the switch beside 'Containment' to enable or disable the auto-containment of unknown files at the endpoints.
- Click 'Apply'

The profile can be applied for web protection settings when configuring firewall policies. See the explanation of **Web Protection** in the section **Configure Firewall Policy Rules** for more details.

11 Manage URL and Content Filtering Profiles

- Click 'URL Filter' in the left-hand menu to open the filter configuration screen.
- The web filter allows you to control which websites your end-users can access.
- You need to create a URL/content filter profile to implement this feature. The profile can then be added to a firewall rule.

There are two elements of a URL profile:

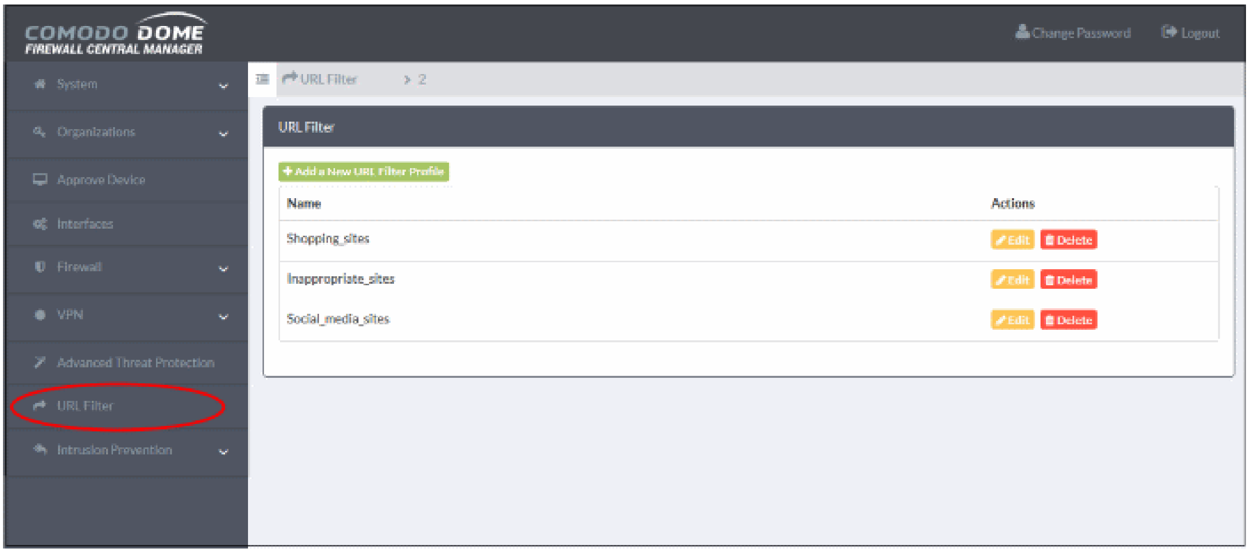
- A website category filter.
- A whitelist / blacklist of specific websites.

Once created, URL profiles can be activated in the 'Web Protection' section of a firewall rule. See **Web Protection Settings** for help with this.

- Profiles created for an organization are available to all devices in that organization.
- Profiles created for an individual device are only be available for that device.

Open the URL filter interface

- Click 'URL Filter' on the left



Name	Actions
Shopping_sites	Edit Delete
Inappropriate_sites	Edit Delete
Social_media_sites	Edit Delete

URL Filter - Column Descriptions		
Column		**Description**
Name		Profile label.
Actions	Edit	Opens the profile editor so you can modify the profile. The editor interface is similar to the interface for adding a profile. See **Create a URL Filter Profile** for more details.
	Delete	Removes the profile.

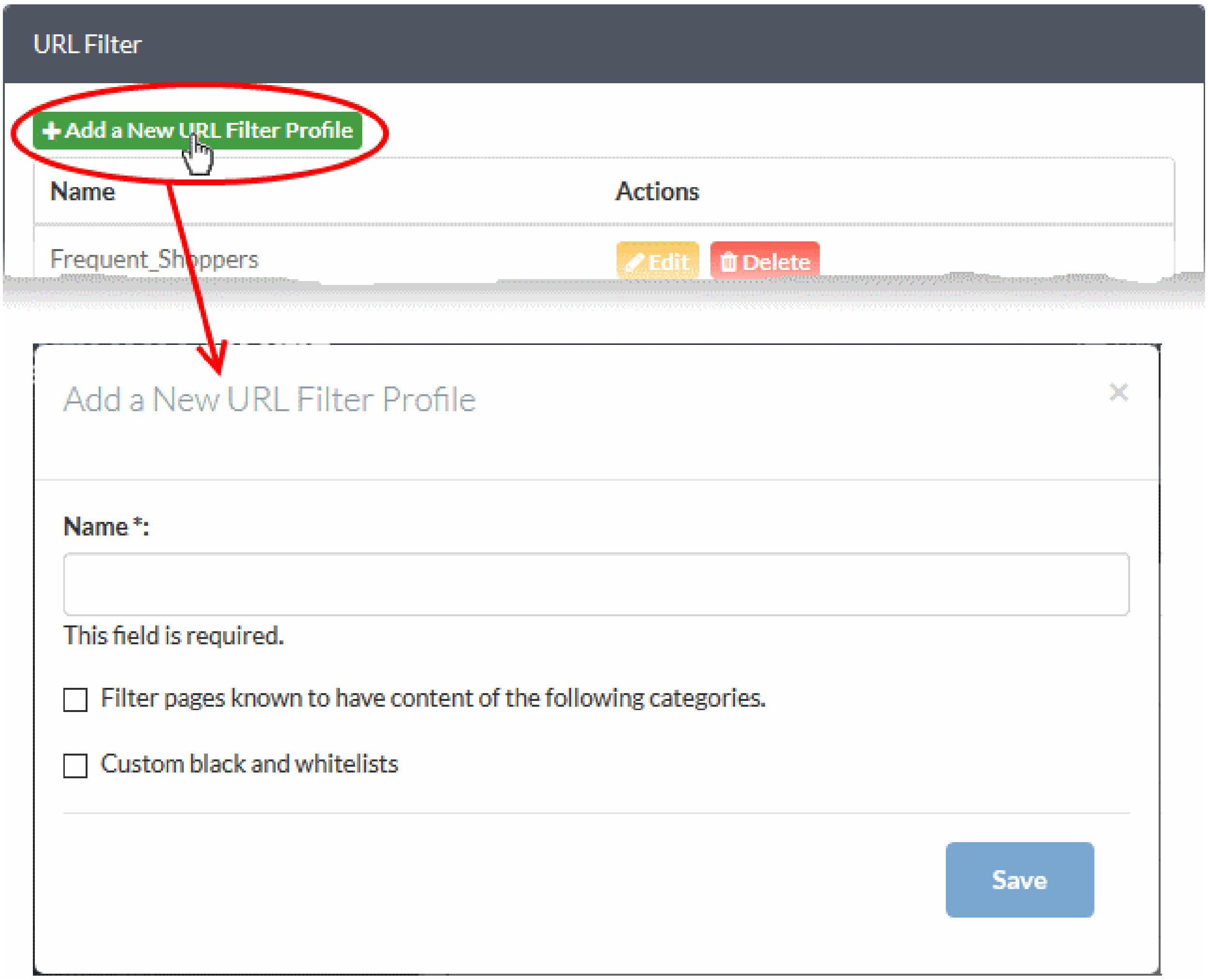
Create a URL Filter Profile

URL filter profiles are constructed from the following two items:

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

To create a URL filtering profile

- Click 'URL Filter' on the left
- Select an organization/device from the drop-down in the title bar
- Click the 'Add a New URL Filter Profile' button at the top-left of the interface.



URL Filter

+Add a New URL Filter Profile

Name	Actions
Frequent_Shoppers	Edit Delete

Add a New URL Filter Profile

Name *:

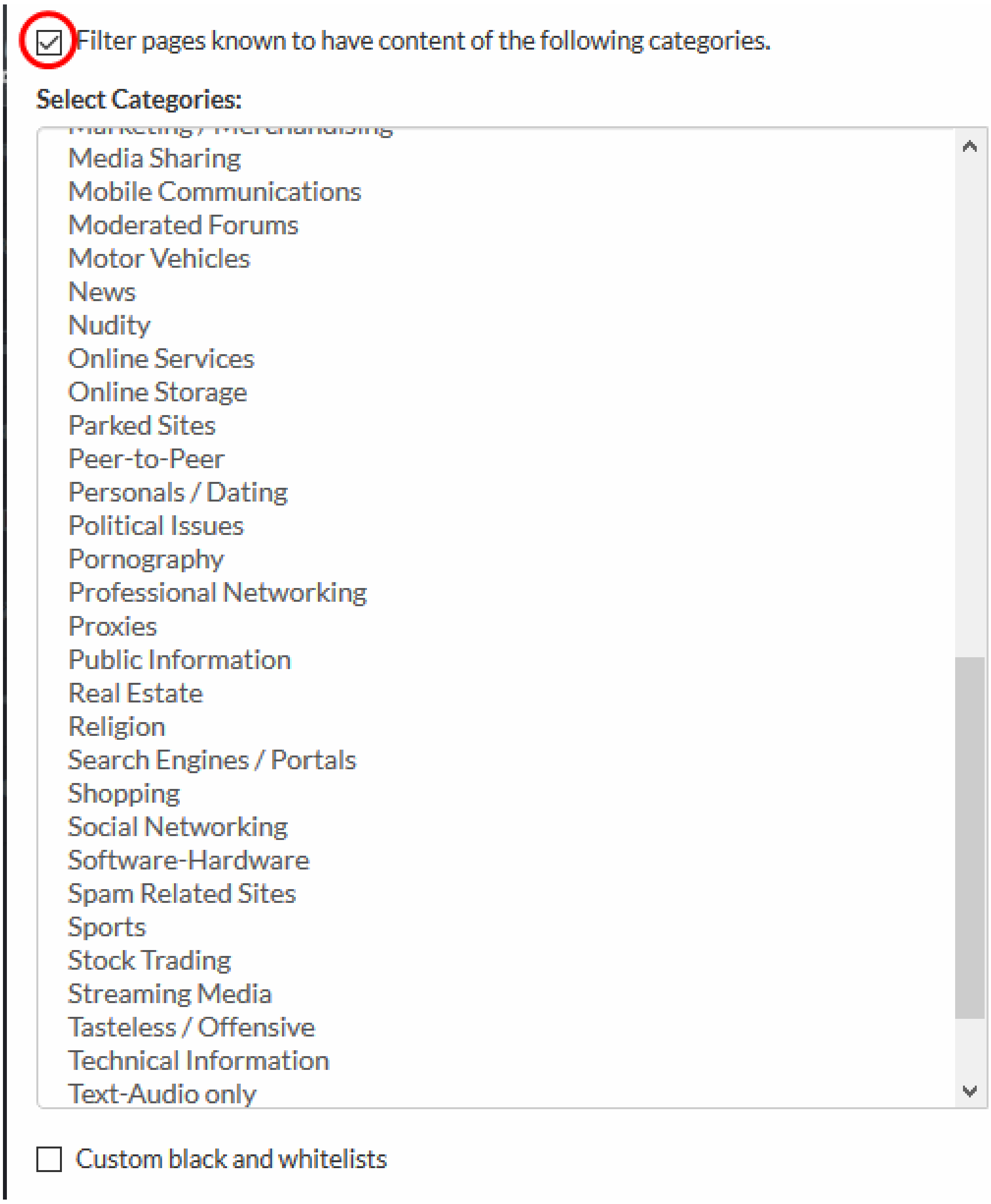
This field is required.

□ Filter pages known to have content of the following categories.

□ Custom black and whitelists

Complete the following details in the form:

- **Name -** Friendly label to identify the purpose of the profile.
- **'Filter pages known to have...' -** Choose website categories that you want to block:



☑ Filter pages known to have content of the following categories.

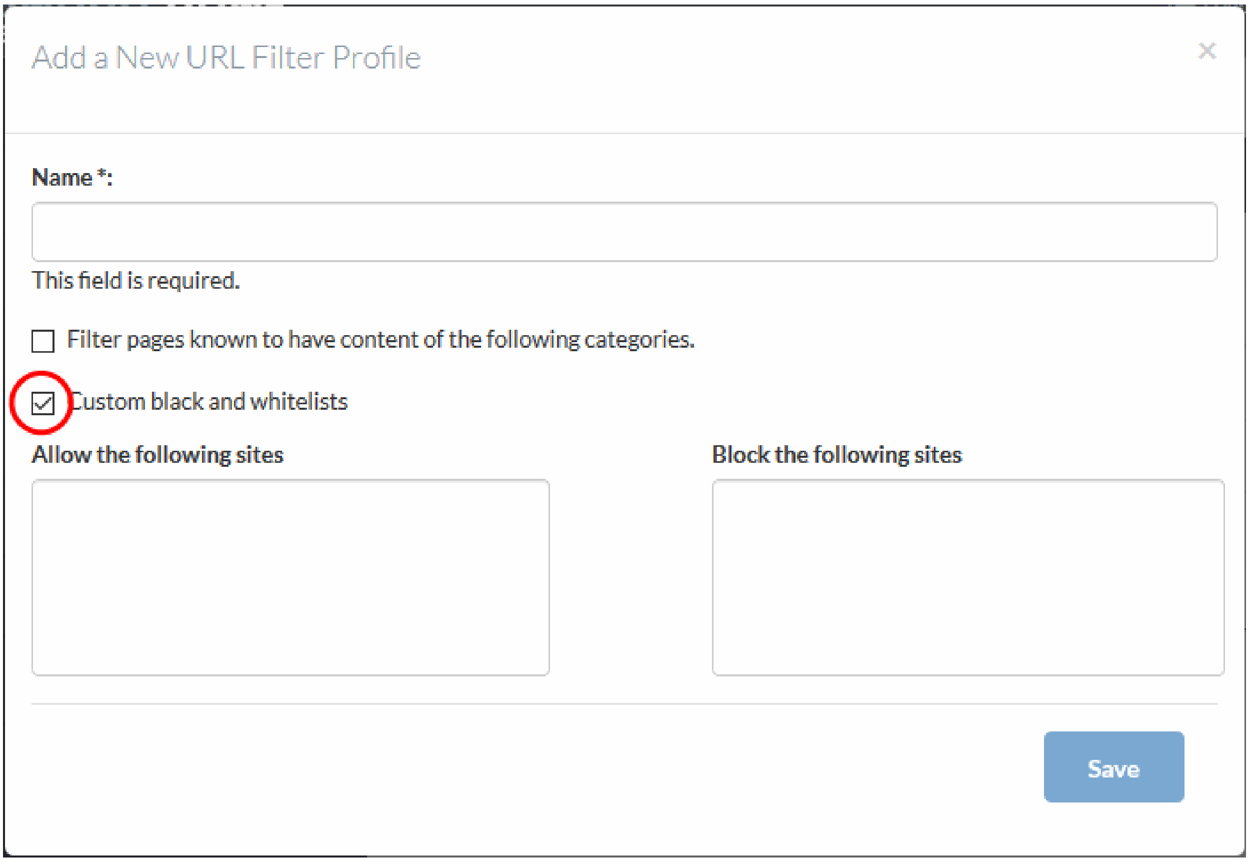
Select Categories:

Marketing / Merchandising
Media Sharing
Mobile Communications
Moderated Forums
Motor Vehicles
News
Nudity
Online Services
Online Storage
Parked Sites
Peer-to-Peer
Personals / Dating
Political Issues
Pornography
Professional Networking
Proxies
Public Information
Real Estate
Religion
Search Engines / Portals
Shopping
Social Networking
Software-Hardware
Spam Related Sites
Sports
Stock Trading
Streaming Media
Tasteless / Offensive
Technical Information
Text-Audio only

□ Custom black and whitelists

Tip: Press and hold the 'Ctrl' key to select multiple items.

- 'Custom black and whitelists' - Specify URLs you want to allow or block. Black and whitelists are usually created to provide exceptions to the categories you have allowed/blocked.



Add a New URL Filter Profile

Name *:

This field is required.

□ Filter pages known to have content of the following categories.

☑ Custom black and whitelists

Allow the following sites

Block the following sites

- **'Allow the following sites'** – Whitelisted websites. Users are allowed to access the sites you type here.
- **'Block the following sites'** – Blacklisted websites. Users are not allowed to access sites you type here.

Note:

- Type URLs in the format **www.example.com** (without http:// or https://)
- Wildcard characters are allowed. For example, *.example.com will block all sub-domains of example.com

- Click 'Save'.

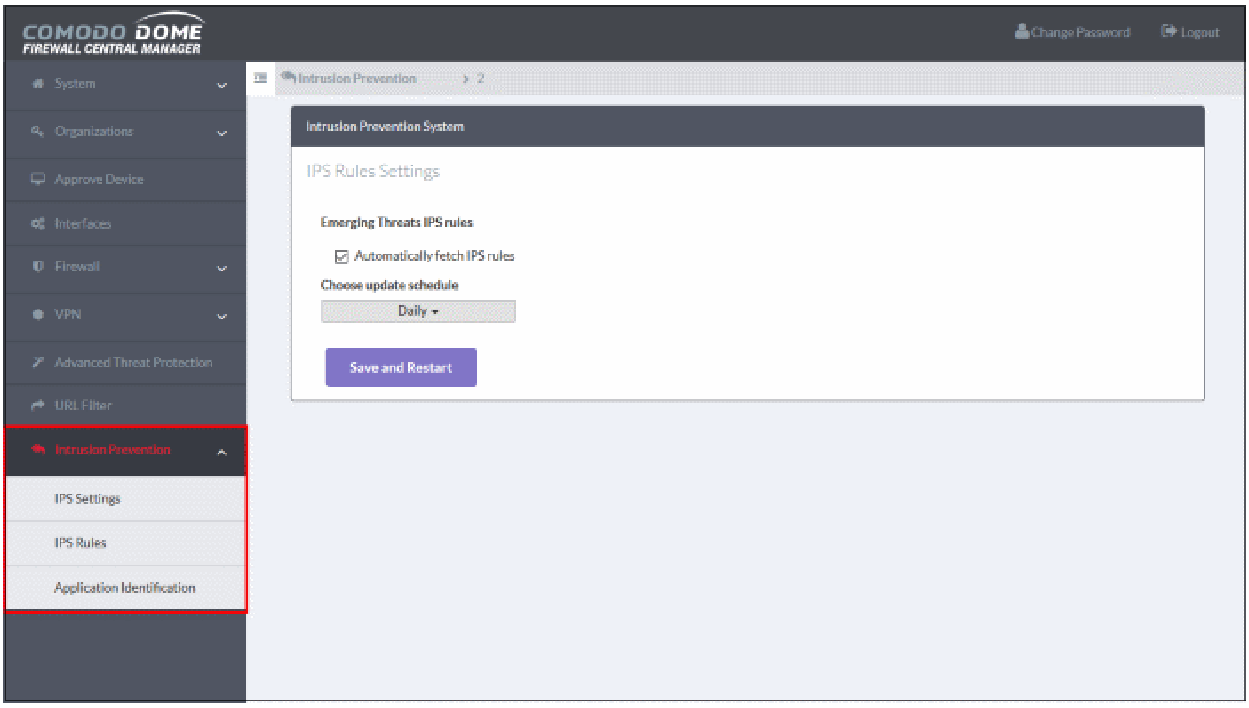
The profile is now available in the 'URL Filter' drop-down when creating/editing a firewall rule.

- Repeat the process to add more filter profiles.

12 Intrusion Prevention

- Click 'Intrusion Prevention' in the left-hand menu
- 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 rules to identify applications generating traffic on your network.
- All rule sets are constantly updated to confront emerging network intrusion techniques.

The intrusion prevention menu lets you configure Snort rule updates and enable IPS/application rule sets for organizations and devices.



IPS Rules Settings

Emerging Threats IPS rules

☑ Automatically fetch IPS rules

Choose update schedule: Daily

See the following sections for more details:

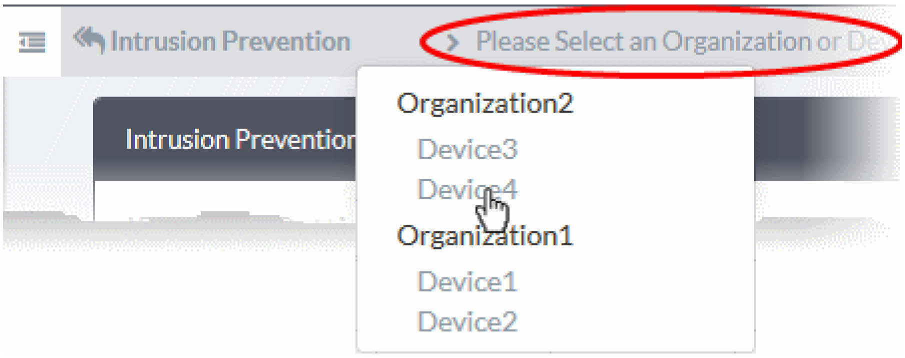
- **Configure the Intrusion Prevention System**
- **Manage IPS Rulesets**
- **Manage Application Identification Rulesets**

12.1 Configure the Intrusion Prevention System

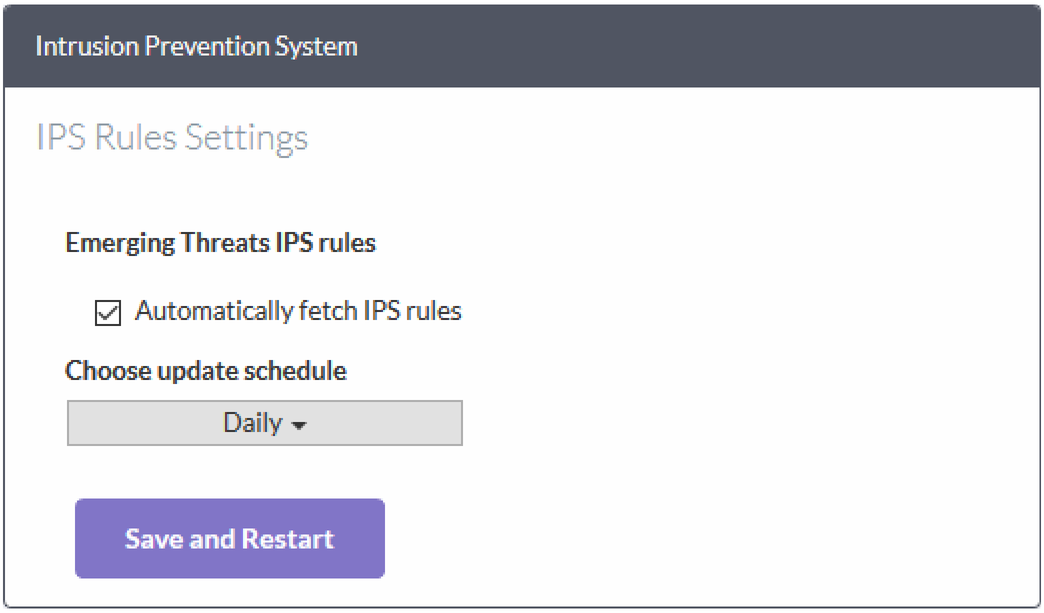
- Click 'Intrusion Prevention' > 'IPS Settings' in the left-hand menu
- The 'IPS Settings' interface lets you configure ruleset updates for Snort. Updates can be scheduled to run automatically at specific intervals.
- These settings will be applied to devices when you choose the 'default' intrusion prevention profile in the 'Content Flow Check' section of a firewall rule.
  - See **Content Flow Check Settings** if you want more advice on this.

To configure the IPS ruleset update schedule for default profile

- Click 'Intrusion Prevention' > 'IPS Settings'
- Select the organization/device from the drop-down in the title bar
  - A default profile applied to an organization will apply to all devices in the organization.
  - A default profile applied to an individual device will apply only to the device in question.



The 'IPS Rules Settings' interface for the selected organization/device will appear.



Intrusion Prevention System

IPS Rules Settings

Emerging Threats IPS rules

☑ Automatically fetch IPS rules

Choose update schedule

Daily

- **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.

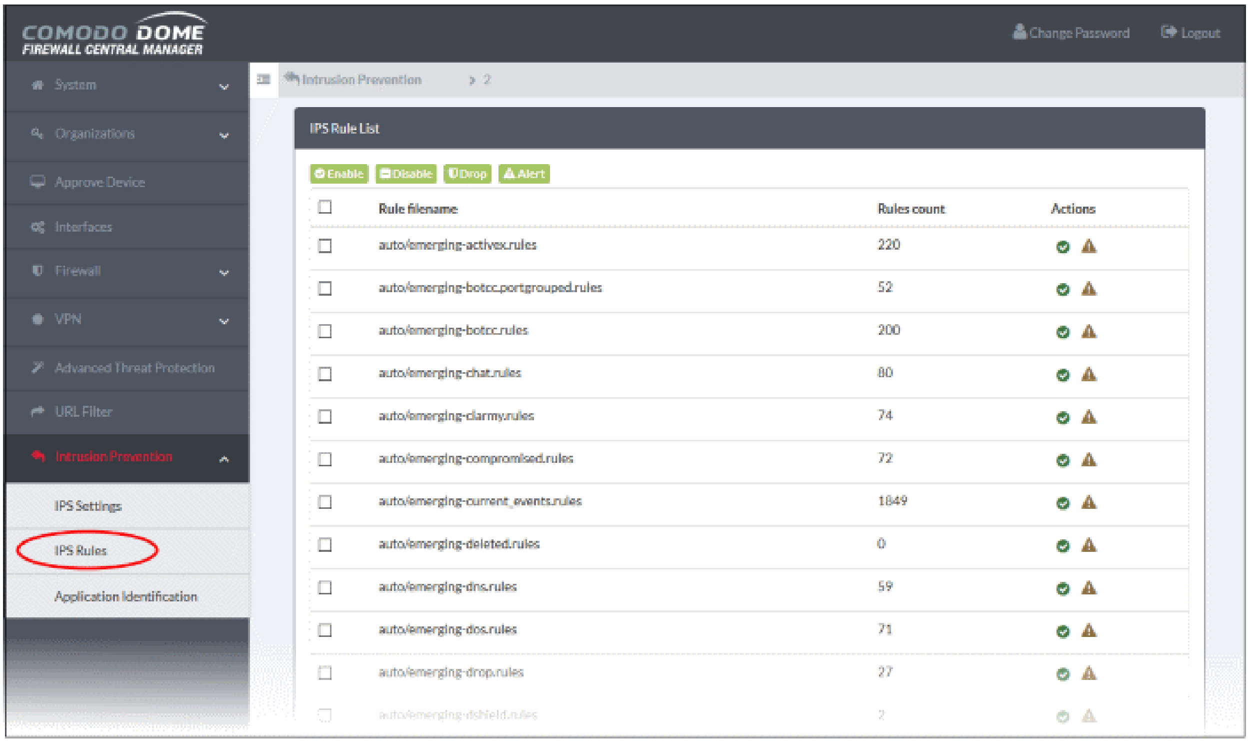
12.2 Manage IPS Rulesets

- Click 'Intrusion Prevention' > 'IPS Rules' in the left-hand menu
- The 'IPS Rules' interface displays a list of currently loaded IPS rulesets for the selected organization or device.
- You can enable/disable rulesets and configure them to allow/block packets as required.
- These settings will be applied to devices when you choose the 'default' IPS profile in the 'Content Flow Check' section of a firewall rule.

- See **Content Flow Check Settings** if you want more advice on this.

To configure IPS Rulesets

- Click 'Intrusion Prevention' > 'IPS Rules'
- Select the organization/device from the drop-down in the title bar
  - A default profile applied to an organization will apply to all devices in the organization.
  - A default profile applied to an individual device will apply only to the device in question.



☐	Rule filename	Rules count	Actions
☐	auto/emerging-activex.rules	220	✓ ⚠
☐	auto/emerging-botcc.portgrouped.rules	52	✓ ⚠
☐	auto/emerging-botcc.rules	200	✓ ⚠
☐	auto/emerging-chat.rules	80	✓ ⚠
☐	auto/emerging-ciarmy.rules	74	✓ ⚠
☐	auto/emerging-compromised.rules	72	✓ ⚠
☐	auto/emerging-current_events.rules	1849	✓ ⚠
☐	auto/emerging-deleted.rules	0	✓ ⚠
☐	auto/emerging-dns.rules	59	✓ ⚠
☐	auto/emerging-dos.rules	71	✓ ⚠
☐	auto/emerging-drop.rules	27	✓ ⚠
☐	auto/emerging-dshield.rules	2	✓ ⚠

IPS Rule List - Column Descriptions	
Column	**Description**
Rule filename	The label of the ruleset
Rules count	The number of constituent rules in the rule set
Actions	✓ / ⊖ - Indicates whether the ruleset is enabled or disabled. • Click on the icon to switch states. • See **Enable/Disable rulesets** for more details. ⚠ / 🛡 - Rule action. Can be 'Alert' or 'Drop'. • Click the icon to switch between 'Alert' and 'Drop' actions. • See **Change application policy of rulesets** for more details.

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 - 🛡

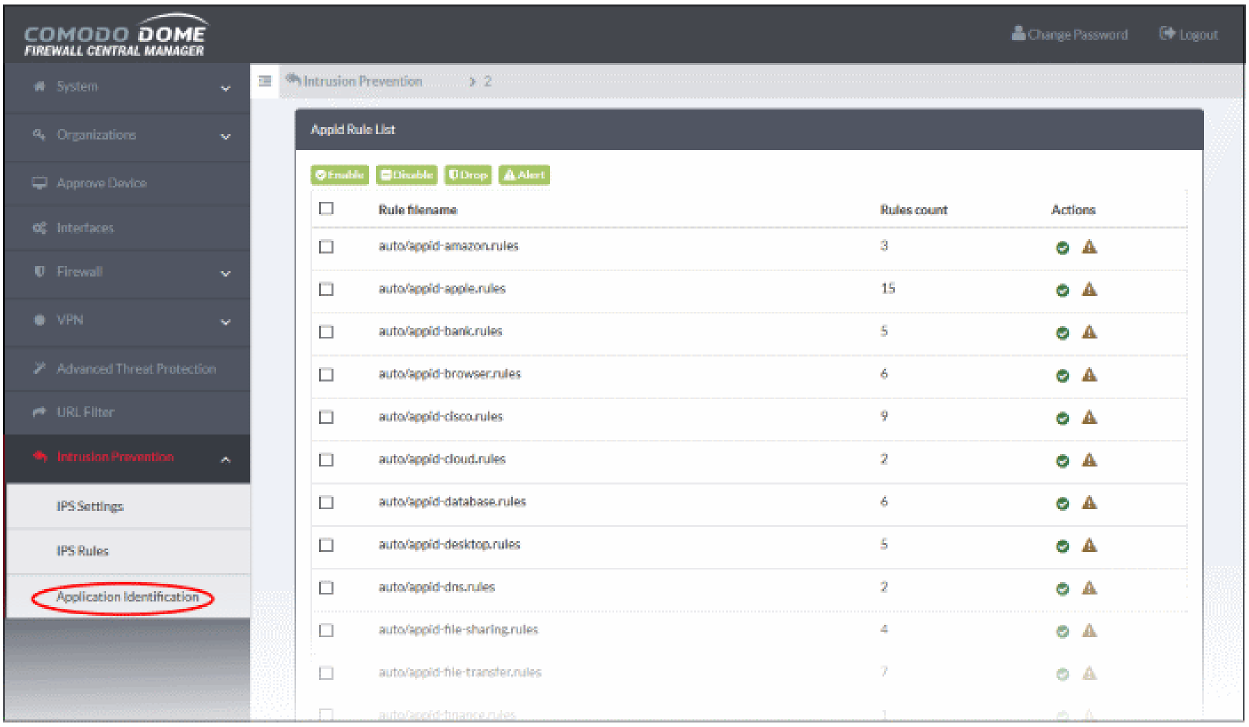
Any changes will be saved to the default profile and immediately applied to devices on which the profile is active.

12.3 Manage Application Identification Rulesets

- Click 'Intrusion Prevention' > 'Application Identification' in the left-hand menu.
- Application identification rules intercept traffic from specific apps and allow or block that traffic according to your preference.
- The interface shows rules that are currently in the default profile for the selected organization or device.

To configure Application Identification Rulesets

- Click 'Intrusion Prevention' >'Application Identification'
- Select the organization/device from the drop-down in the title bar
    - Organization - Configure rulesets that can be applied to all devices in the organization.
    - Device - Configure rulesets that can be applied to a specific device.



□	Rule filename	Rules count	Actions
□	auto/appid-amazon.rules	3	✓ ⚠
□	auto/appid-apple.rules	15	✓ ⚠
□	auto/appid-bank.rules	5	✓ ⚠
□	auto/appid-browser.rules	6	✓ ⚠
□	auto/appid-cisco.rules	9	✓ ⚠
□	auto/appid-cloud.rules	2	✓ ⚠
□	auto/appid-database.rules	6	✓ ⚠
□	auto/appid-desktop.rules	5	✓ ⚠
□	auto/appid-dns.rules	2	✓ ⚠
□	auto/appid-file-sharing.rules	4	✓ ⚠
□	auto/appid-file-transfer.rules	7	✓ ⚠
□	auto/appid-finance.rules	1	✓ ⚠

AppId Rule List - Column Descriptions	
Column	**Description**
Rule filename	The file that contains the constituent rules of the ruleset
Rules count	Indicates the number of constituent rules in the rule set
Actions	Displays control buttons for the ruleset. ✓ / ⛔ - Indicates whether the ruleset is currently enabled or disabled. • Click on the icon to toggle the enabled/disabled status • See **Enable/Disable rulesets** for more details. ⚠ / 🛡 - Indicates the application policy of the ruleset. • Click on the icon to toggle the application policy between 'Alert' and 'Drop' policies. • See **Change application policy of rulesets** for more details.

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.

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**