TCPWave IP Address Management System®

Quick Start Guide

IPv4 Management

Version 11.32P4

TCPWave

TCPWave® Inc.
600 Alexander Road
Princeton, NJ 08540
USA
Phone: 888-831-8276
Email: customercare@tcpwave.com
Website: www.tcpwave.com

This manual is the proprietary and confidential property of TCPWave® Inc. All resulting rights and translation and duplication rights are reserved and subject to a separate agreement. Do not share without prior approval.

TCPWave® Inc. reserves the right to modify the described product in compliance with technical progress at any time and without prior notice unless otherwise provided in the agreement.

Contents

Document Change History **5**

Key Terms **5**

Scope and Purpose **6**

About TCPWave **6**

TCPWave DNS, DHCP, and IP Address Management **6**

Get Started **6**

Obtain Licenses 6

Log In to TCPWave IPAM 6

Update License Keys 6

Dashboard 7

Executive Dashboard 7

Capacity Planning Dashboard 7

Custom Dashboard 8

UI Modes 8

Lighter Mode 8

Darker Mode 9

Change Password 9

Set Up IPv4 Management **10**

Create Organization 10

Create Admin Role 11

Create Admin Group 11

Create Admin User 11

Add Location (Optional) 12

Create Contact (Optional) 12

Create Domain 13

Create IPv4 Network 13

Create Subnet Group (Optional) 14

Create IPv4 Subnet 14

Create IPv4 Object 15

Create DNS ACL 15

Create DNS Log Channels (Optional) 16

Create DNS Appliance Template 17

Create DNS Option Template 18

Create DNS Appliance 19

Create DNS Zone Template 20

Create DNS Zone 20

Create DNS Root Zone (Optional) 21

Create DHCP IPv4 Option Template 21

Create DHCP Policy Template 23

Create DHCP IPv4 Appliance 24

Create DHCP IPv4 Scope 26

Verify DNS and DHCP Setup 28
Verify DNS Setup 28
Verify DHCP Setup 28

Document Change History

Revision Date	Summary of Changes
August 2022	Added Capacity Planning Dashboard
February 2022	Added Custom Dashboard feature. UI supports two modes – lighter mode and darker mode.
April 2021	Added DNS TSIG Keys details
January 2021	Added DNS Views details
February 2021	Updated format slightly and clarified content
September 2020	Added License Details
January 24, 2020	Updated document to new format
August 07, 2019	Updated document to the new format
June 24, 2019	Updated few sections with screenshots
May 9, 2018	Updated all the sections with navigation and screenshots
October 2, 2017	Updated all the sections. Modified the navigation
May 2, 2017	Updated all the sections. Changed the navigation from DNS & DHCP to Network Management
November 22, 2016	Updated the following sections: Creating Object, Creating DNS Appliance, and Creating DHCP Appliance
October 6, 2016	Updated the following section: Creating DNS Appliance
August 24, 2016	Updated the Login information

Key Terms

Term	Description
ACL	Access Control List
BIND	Berkeley Internet Name Domain
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
FADM	Functional Administrator
GUI	Graphical User Interface
IPAM	Internet Protocol Address Management
SNMP	Simple Network Management Protocol

UADM	User Administrator

Scope and Purpose

This guide provides instructions to set up IPv4 Management, including creating a Domain Name System (DNS) Appliance and a Dynamic Host Configuration Protocol (DHCP) Appliance in the TCPWave Internet Protocol Address Management (IPAM) system. Emphasis is placed on critical operational tasks to configure TCPWave IPAM quickly and verify the basic setup of IPv4 Management.

About TCPWave

TCPWave is committed to securely developing the highest quality software solutions, products, and services for our customers. Our Infrastructure-as-a-Service (IaaS) design can manage and monitor large, complex environments, including cloud- and on-premise-based environments.

TCPWave has global customers in every primary market and serves them with a dedicated staff who work at the highest level of professionalism and help customers succeed in their ventures. Furthermore, TCPWave has strategic partnerships with leading appliance providers who maintain appliances in over 100 countries worldwide.

TCPWave DNS, DHCP, and IP Address Management

TCPWave's IP Address Management (IPAM) enables network administrators to efficiently and intelligently automate the allocation and de-allocation of IP address resources. The system dynamically manages available IP address space by complying with organizations' address and security policies. Also, the system provides an intuitive GUI through which users can manage Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services. TCPWave's IPAM has a rich feature set built using modern technology. It is a single, agile solution for IP, DNS, and DHCP Management for many organizations' constantly changing IT needs.

Get Started

To start using TCPWave IPAM, get needed licenses, log in to it, update license keys, and then change the password.

Obtain Licenses

TCPWave IPAM and Remote Appliances are licensed products. To request licenses, contact TCPWave Support (support@tcpwave.com) or visit the customer portal (https://www.tcpwave.com/portal).

Log In to TCPWave IPAM

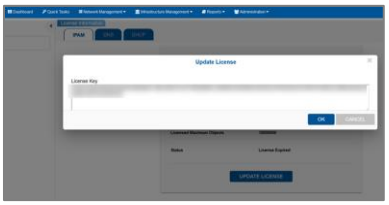
Log in to TCPWave IPAM by first navigating to the URL https://<your-fully-qualified-hostname>or<IP Address>:7443/tims (Example, https://10.1.1.10:7443/tims). Then log in to the IPAM GUI using the default credentials provided by TCPWave.

Update License Keys

To update the license keys in TCPWave IPAM, do the following:

1. Navigate to **Administration** >> **Configuration Management** >> **License Management**.
2. On each of the IPAM, DNS, and DHCP tabs, do the following:
    a. Click on **Update License**.

Result: The **Update License** dialog box is displayed.



b. Enter the license key.

c. Click **OK**.

Dashboard

TCPWave offers the following Dashboards:

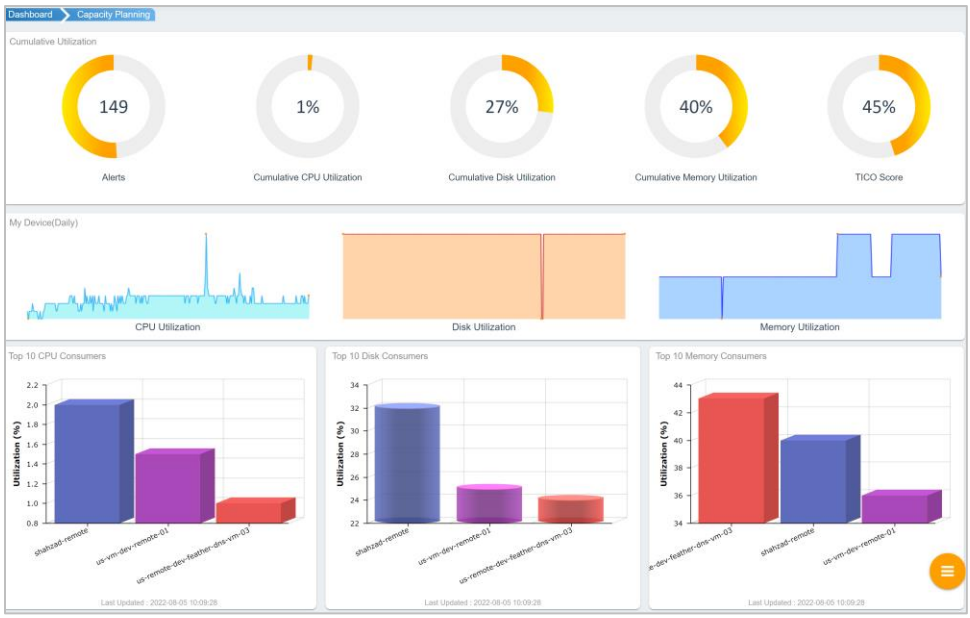
- Predefined Dashboard
    - Executive Dashboard
    - Capacity Planning Dashboard
- Custom Dashboard

Executive Dashboard

It presents an overview of network infrastructure metrics. It displays counters, statistics, alerts, graphical summary reports, and other information organized in nine widgets.

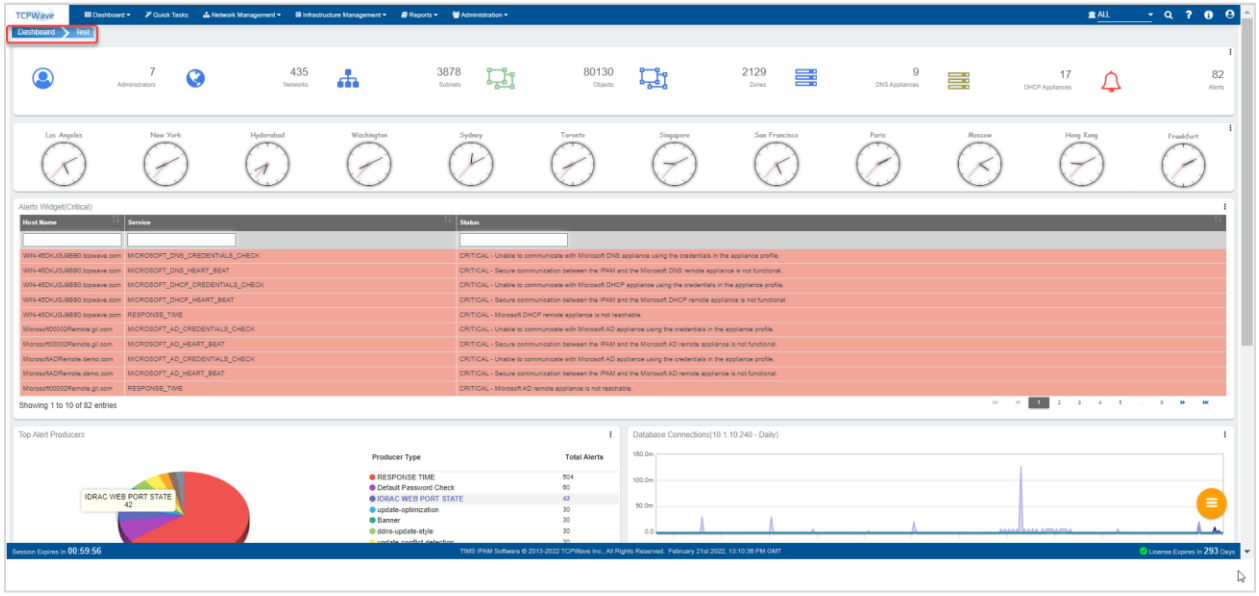
Capacity Planning Dashboard

It provides a comprehensive snapshot of DNS, DHCP, and IPAM parameters in various widgets. It helps the organizations make informed decisions that might impact business performance. For more details, refer to ***TCPWave Administrators Guide***



Custom Dashboard

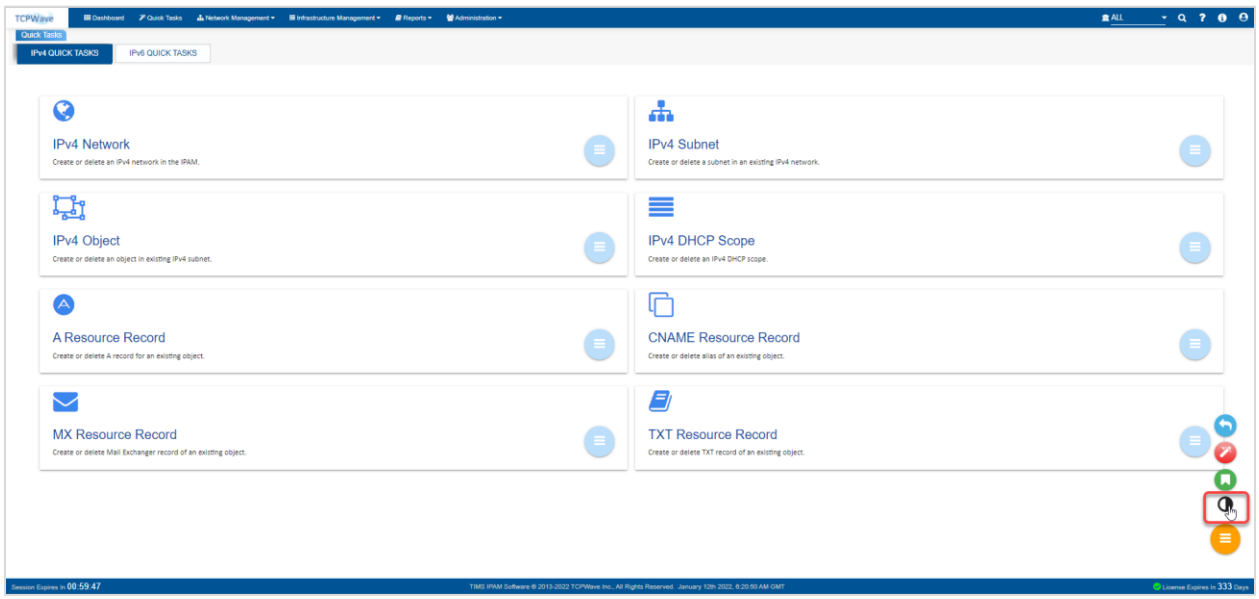
The TCPWave's Custom Dashboard enables you to analyze a set of comprehensive data from across the entire application in a single pane of glass on the home screen. After the patch deployment, users must click the Reset icon to load the latest dashboard changes. The Reset icon is present next to the Dashboard >> Executive



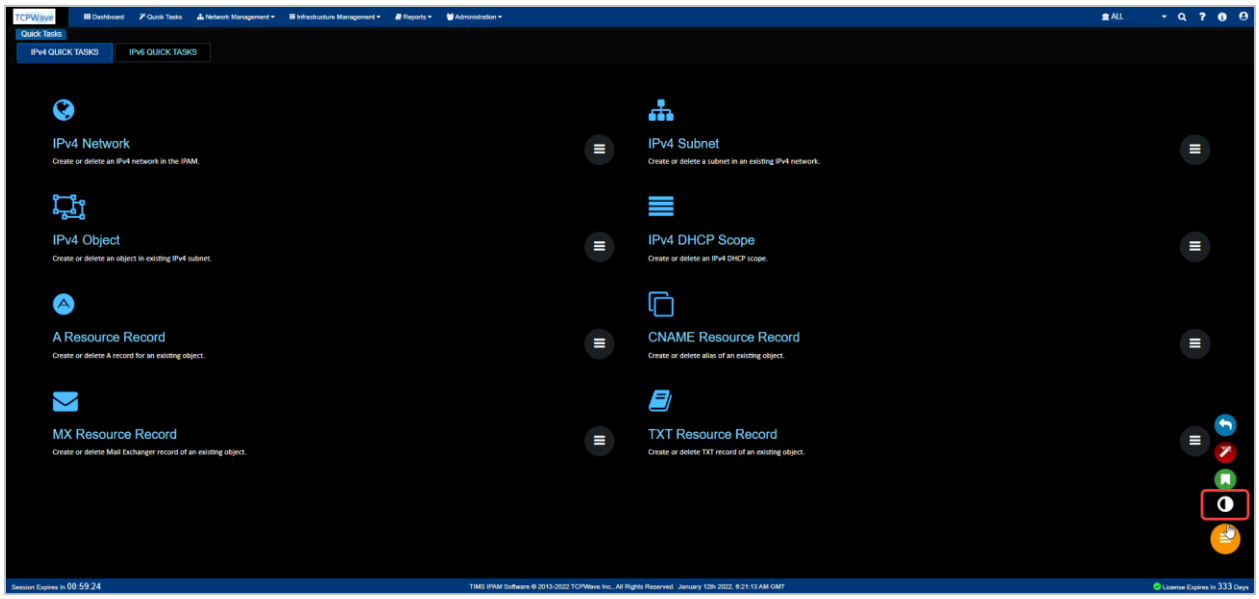
UI Modes

The UI supports two modes across the entire application – One is a lighter mode, and the other is the darker mode. The following figures illustrate the examples of both the modes of the Quick Tasks page.

Lighter Mode

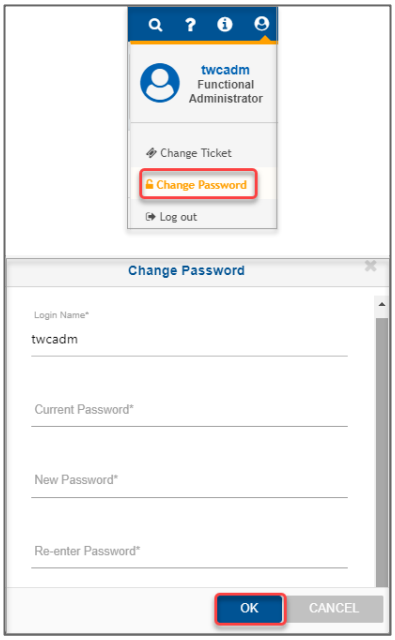


Darker Mode



Change Password

After logging in, immediately change the password of the Functional Administrator (FADM), which is named twcadm.



1. In the **Profile** section, click **Change Password**.

   Result: A validation message is displayed to check if you want to proceed.

2. Click **Yes.**

   Result: The **Change Password** screen is displayed.

3. Enter the **Current Password**.
4. Populate **New Password** and **Re-enter Password**.
5. Click **OK**.

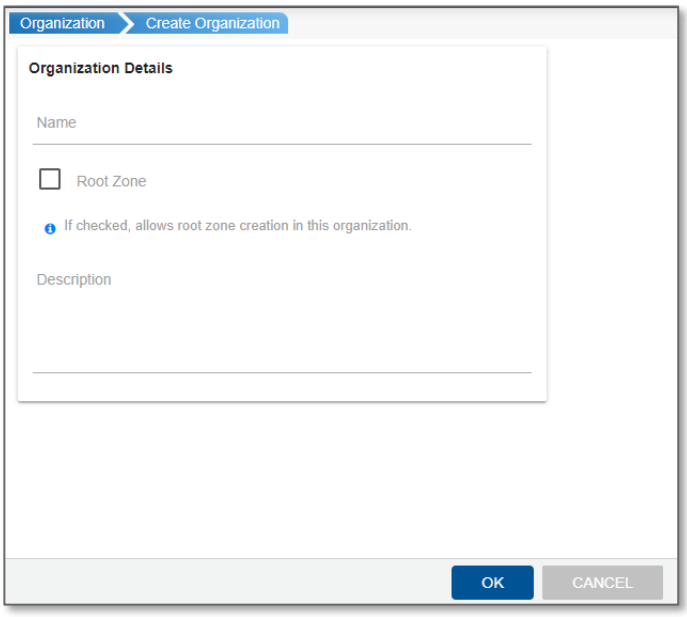
	You can create a User Admin (UADM) account and lock out the FADM (twcadm) account for improved security. See Create Admin User below for information on creating a UADM.

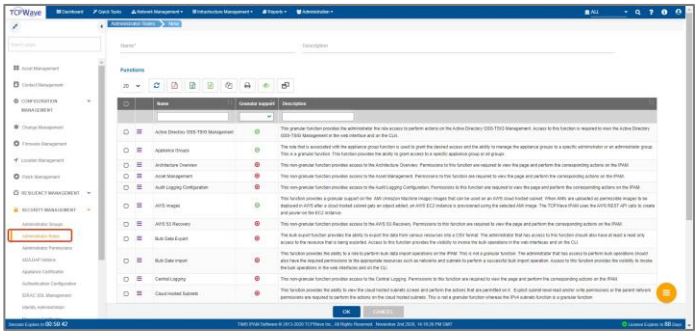
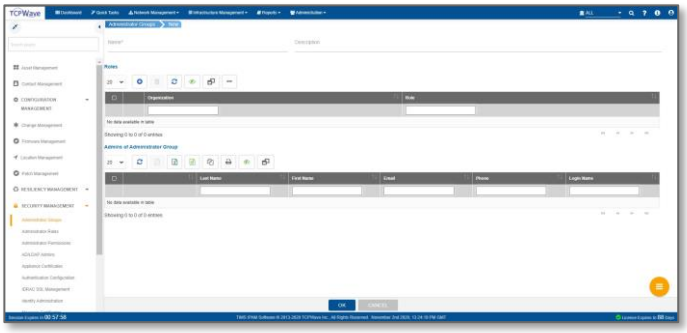
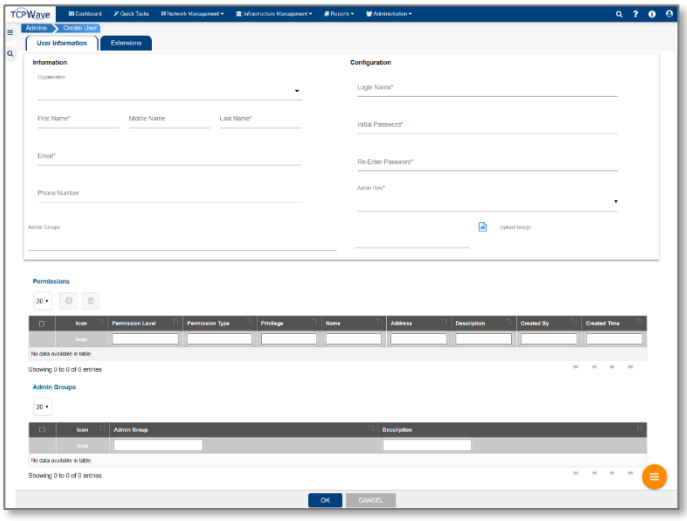
Set Up IPv4 Management

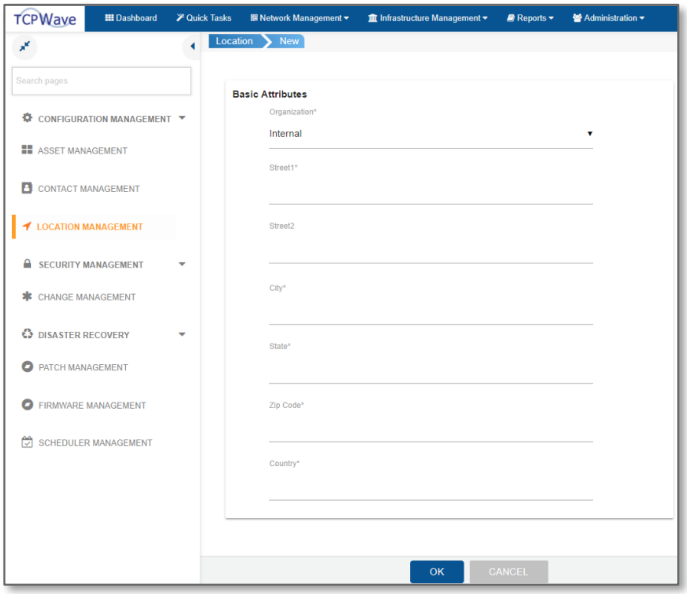
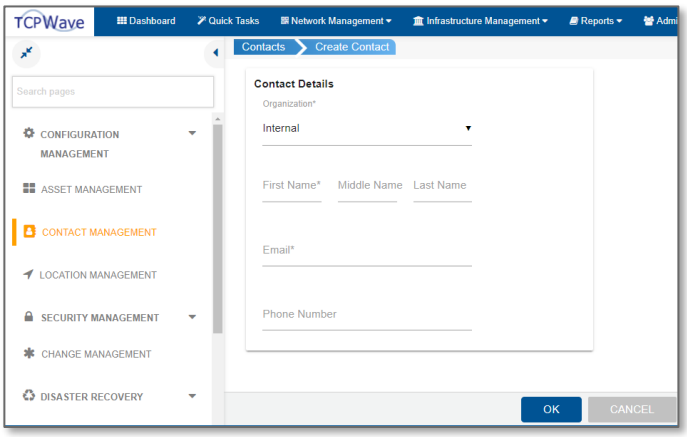
To set up IPv4 Management, including creating a DNS Appliance and DHCP Appliance, complete one or more steps in each of the following areas in the stated sequence:

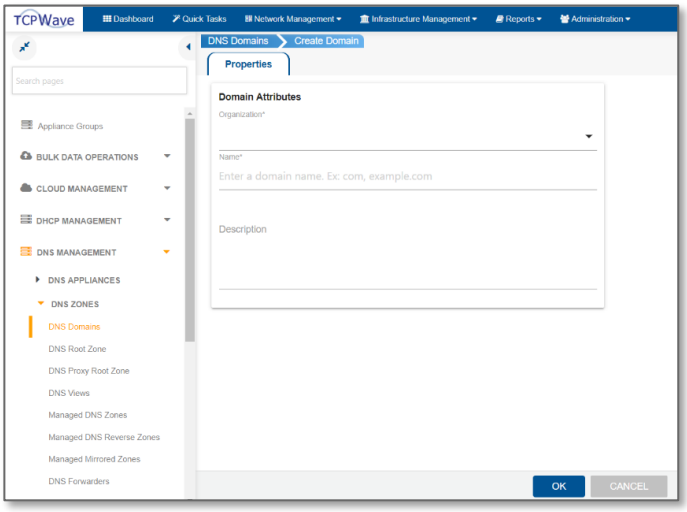
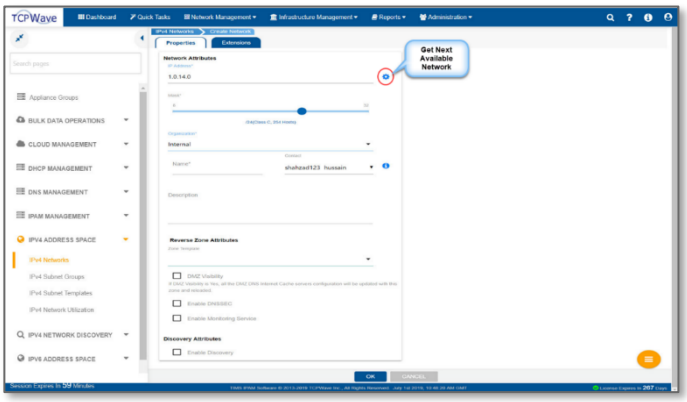
1. Organization
2. Administrator
3. Domain
4. Network
5. Subnet
6. Object
7. DNS Appliance
8. DHCP Appliance

The details of the steps in these areas are provided in the table below. Note that some steps are optional and can be skipped or done later.

<table>
<tr><th>Step</th><th>Procedure</th><th>Screenshot</th></tr>
<tr><td rowspan="2">1</td><td><h3>Create Organization</h3>To create an Organization, navigate to Administration >> Configuration Management.
a. Click ⊕.
b. Enter the organization Name and, optionally, a Description.
c. Click OK.</td><td> 
</td></tr>
<tr><td colspan="2">• There is a default Organization called Internal. However, it is recommended that you create your own Organization.
• If Root Zone is enabled, you can create a root zone in an Organization.</td></tr>
</table>

Step	Procedure	Screenshot
2	**Create Admin Role** To create an Administrator Role, navigate to **Administration** >> **Security Management** and select **Administrator Roles**. a. Click ⊕. b. Enter an admin role **Name** and, optionally, a **Description**. c. Click **OK**.	
3	**Create Admin Group** To create an Administrator Group, navigate to **Administration** >> **Security Management** and select **Administrator Groups**. a. Click ⊕. b. Enter an admin group **Name** and, optionally, a **Description**. c. Click **OK**.	
4	**Create Admin User** To create an Administrative User, navigate to Administration >> Security Management >> Identity Administration. a. Click ⊕. **Result**: The **Create User** page is displayed. b. Enter **First Name**, **Last Name**, **Email ID**, **Login Name**, **Initial Password**, and **Re-Enter Password**. c. Select one or more administrator groups and click ⏩. **Result**: The selected administrator group(s) are changed to be associated administrator group(s). d. (Optional) Click ⏪. **Result**: The system disassociates the selected administrator group(s) and changes them to be available administrator groups.	

Step	Procedure	Screenshot
	e. Select the default **Admin Role**. **Note**: The system selects a default **Organization** based on the selected role. f. Click **OK**.	
5	**Add Location (Optional)** To add a Location, navigate to **Administration >> Location Management**. a. Click ⊕. b. Choose an **Organization** from the drop-down menu. c. Enter **Street 1**, **City**, **State**, **Zip Code**, and **Country**. d. Click **OK**.	
6	**Create Contact (Optional)** To create a Contact, navigate to **Administration >> Contact Management**. a. Click ⊕. **Result**: The **Create Contact** page is displayed. b. Choose an **Organization** from the drop-down menu. c. Enter **First Name**, **Last Name**, and **Email**. d. Click **OK**.	

<table>
<tr><th>Step</th><th>Procedure</th><th>Screenshot</th></tr>
<tr><td>7</td><td><h2>Create Domain</h2>To create a DNS Domain, navigate to Network Management >> DNS Management >> DNS Zones >> DNS Domains.
a. Click .
Result: The Create Domain page is displayed.
b. Choose an Organization from the drop-down menu.
c. Enter the Name of the domain, and then click OK.</td><td> 
</td></tr>
<tr><td></td><td colspan="2">
• To create a subnet in TCPWave IPAM, a Domain is needed.
• Domain and Zone are different entities. A Zone is created later in a step below.</td></tr>
<tr><td>8</td><td><h2>Create IPv4 Network</h2>To create an IPv4 Network, navigate to Network Management >> IPv4 Address Space >> IPv4 Networks.
a. Click .
b. In the Properties tab, enter the IP Address.
c. Select the desired network prefix length by using the Mask slider.
d. Choose an Organization from the drop-down menu.
e. Enter the Name of the network.
f. (Optional) Choose a Reverse Zone Template from the drop-down menu if at least one has already been created.
g. Select DMZ Visibility, DNSSEC, and Monitoring Service, as needed.
h. If discover functionality is needed, then under Discovery Attributes, select Enable Discovery.
i. Click OK.</td><td> 
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Procedure</th><th>Screenshot</th></tr>
<tr><td>9</td><td>

Create Subnet Group (Optional)

To add an IPv4 Subnet Group, navigate to Network Management >> IPv4 Address Space >> IPv4 Subnet Groups.

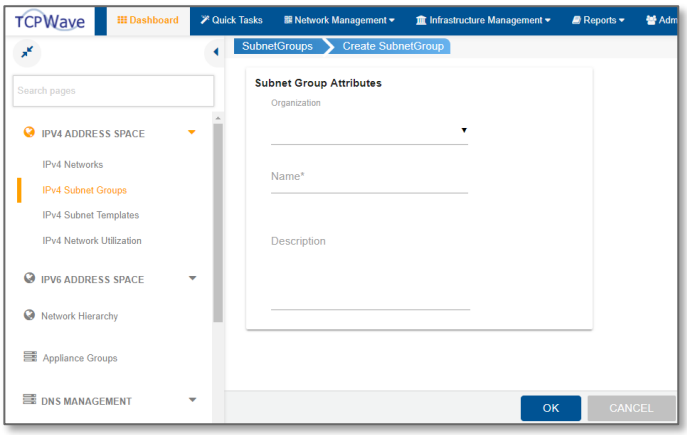
a. Click .

Result: The **Create Subnet Group** page is displayed.

b. Choose an **Organization** from the drop-down menu.

c. Enter the **Name** of the subnet group and, optionally, a **Description**.

d. Click **OK**.

</td><td> 
</td></tr>
<tr><td></td><td colspan="2">

Subnet Groups are used to assign privileges to administrators. Privileges assigned at a higher level in the network hierarchy are inherited by lower-level network elements. For example, a Read privilege in a Network or Subnet Group applies to the underlying Subnets and Objects.</td></tr>
<tr><td>10</td><td>

Create IPv4 Subnet

To create an IPv4 Subnet, navigate to Network Management >> IPv4 Address Space >> IPv4 Networks.

a. Select the network in which you want to create the subnet.

b. Click .

Result: The **Create Subnet** page is displayed.

c. To **Create multiple subnets**, select **Yes**.

d. Select the desired mask length by using the **Mask** slider.

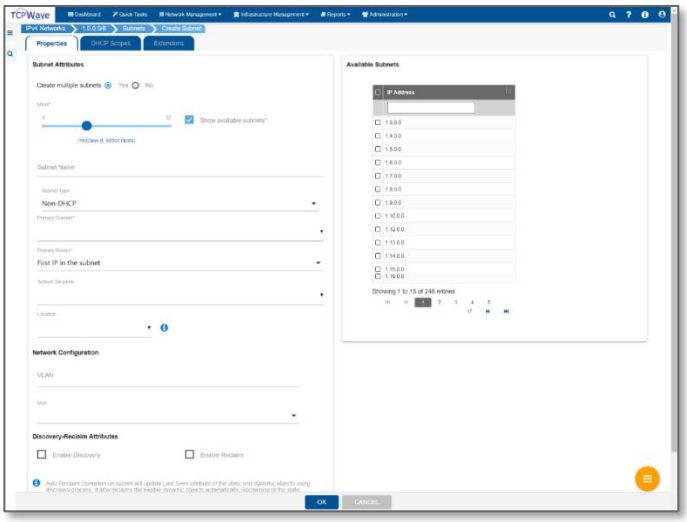
e. Select **Show available subnets** to view the available subnets for the selected mask.

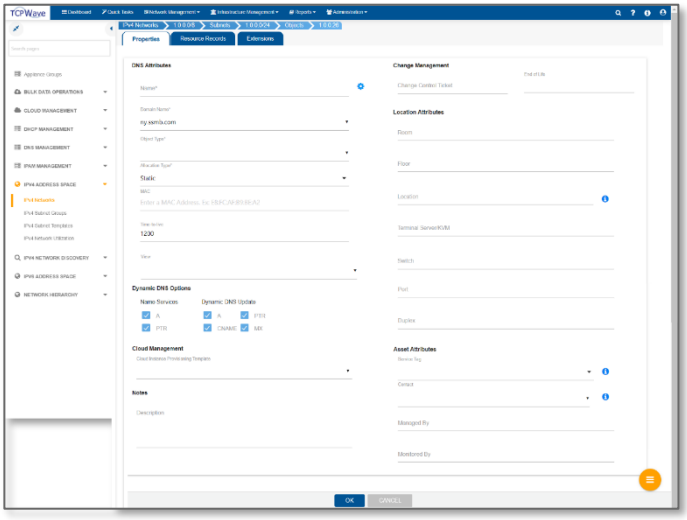
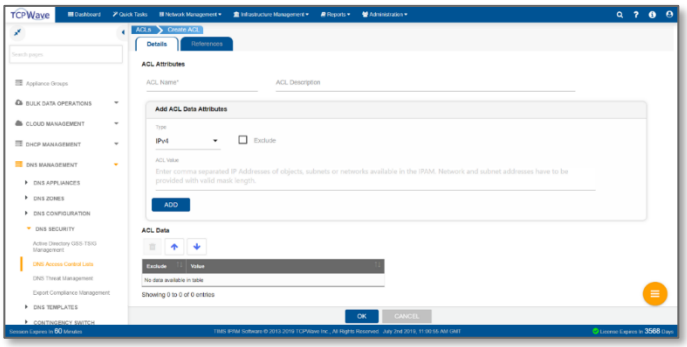
f. Choose the desired subnets from the **Available Subnets** list.

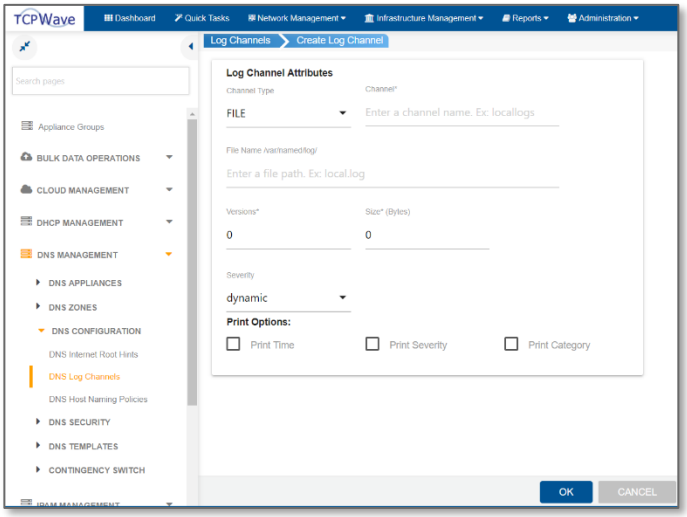
g. Enter a **Subnet Name**.

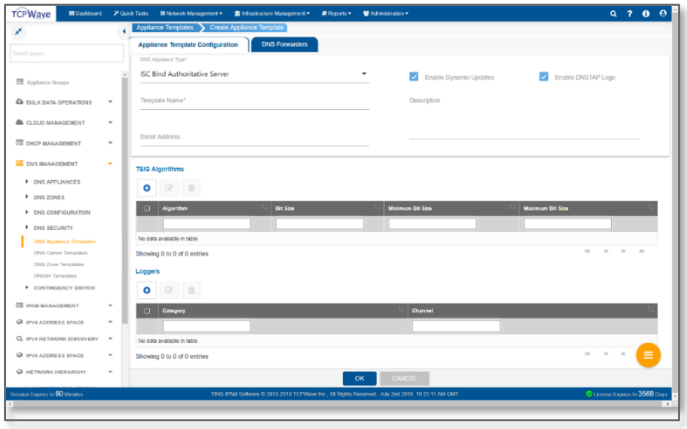
h. Choose **Primary Domain** and **Primary Router** values from the respective drop-down menus.

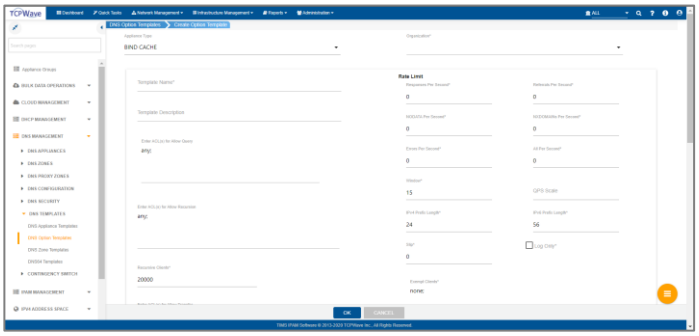
i. Click **OK.**

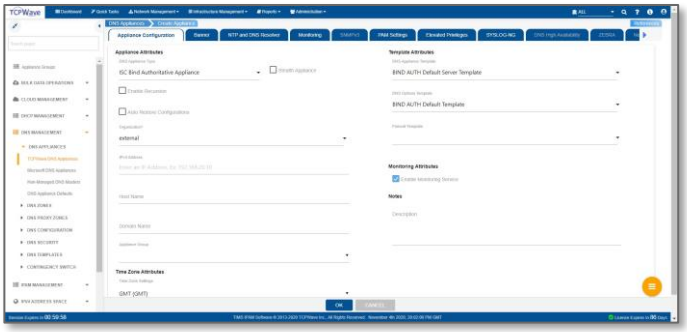
</td><td> 
</td></tr>
</table>

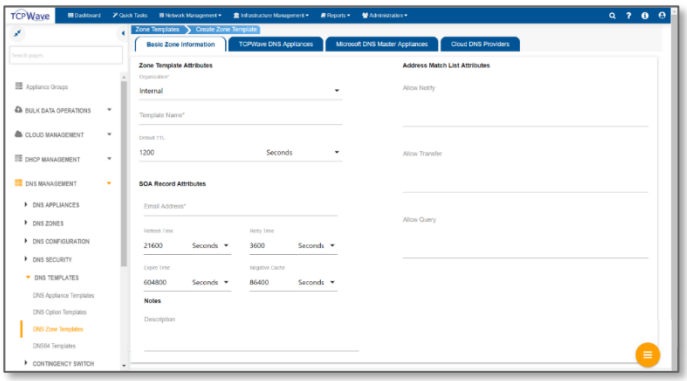
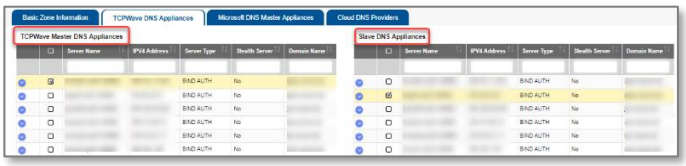
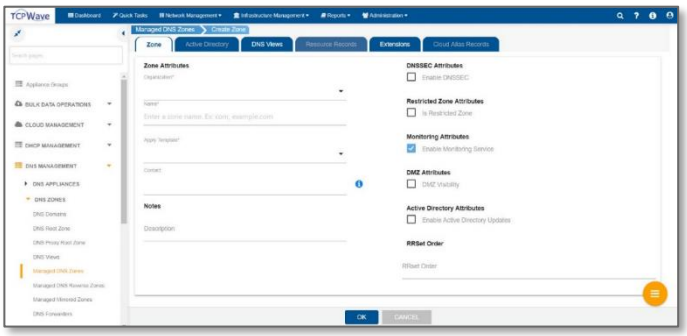
<table>
<tr><th>Step</th><th>Procedure</th><th>Screenshot</th></tr>
<tr><td></td><td colspan="2">Subnet Name, Subnet Group, Subnet Type (non-DHCP by default), Subnet Template, Location, VLAN, VRF, Enable Discovery, Enable Reclaim, and Description are all optional.</td></tr>
<tr><td>11</td><td><h3>Create IPv4 Object</h3>To create an IPv4 Object, navigate to Network Management >> IPv4 Address Space >> Select IPv4 Network.
a. Select a Network and Subnet in which to create the new object.
b. Select an IP Address and then click .
c. Choose an Object Type.
d. Enter the Name of the object or click to generate the Name automatically based on the selected Object Type.
e. Choose Domain Name and Allocation Type values from the respective drop-down menus.
f. Click OK.</td><td>  </td></tr>
<tr><td>12</td><td><h3>Create DNS ACL</h3>To create a DNS Access Control List, navigate to Network Management >> DNS Management >> DNS Security >> DNS Access Control Lists.
a. Click .
b. Enter an ACL Name.
c. In the Add ACL Data Attributes section, select the Type, either IPv4 or ACL, from the drop-down menu.
d. To exclude the selected IPv4 address or ACL, select Exclude.
e. Click OK.</td><td>  </td></tr>
<tr><td></td><td colspan="2">• To change the sequence in which ACL data is applied, use the Move Up and Move Down arrows.
• DNS ACLs apply to DNS Zone Templates and DNS Option Templates and allow query, transfer, notify, and/or recursion based on client IP addresses. Also, these templates support associating IP addresses with</td></tr>
</table>

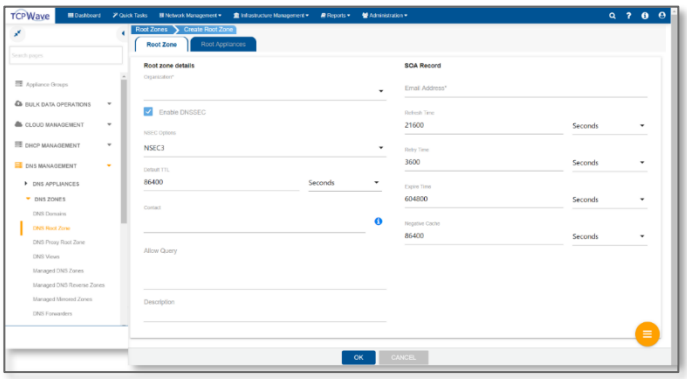
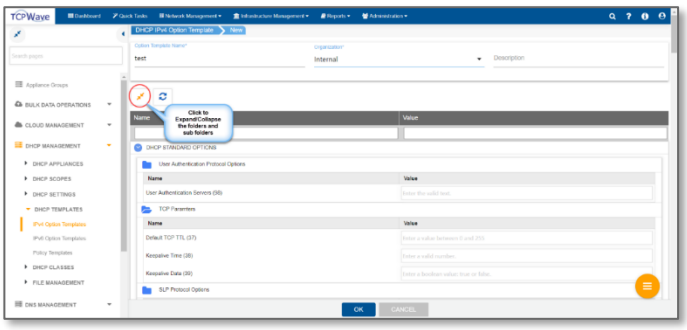
Step	Procedure	Screenshot
	the blackhole option. DNS Zone Templates and DNS Option Templates apply to DNS Managed Zones and DNS Appliances.	
13	**Create DNS Log Channels (Optional)** To create DNS log channels, navigate to Network Management >> DNS Management >> DNS Configuration >> DNS Log Channels. a. Click . b. Choose a **Channel Type** from the drop-down menu. c. Enter a name for the **Channel**. **Note**: This name can later be associated with one or more BIND categories, such as lame-servers or RPZ, in the Loggers section of a DNS Appliance Template. d. If the **Channel Type** was left at the default of **File**, then do the following: i. Enter the **File Name** for the log. ii. Enter the number of log file **Versions** to keep before the files are rotated. iii. Enter the **Size** of each log file in MB before it is rotated. e. If the **Channel Type** is **SYSLOG**, choose the **SYSLOG Facility** from the drop-down menu. f. Choose the desired **Severity**, such as **Info**, from the drop-down menu. This controls the level of detail in the log, and it will contain the chosen level and higher. g. Select **Print Time**, **Print Severity,** and **Print Category** as needed for the information desired in the log. h. Click **OK**.	
	TCPWave IPAM provides default DNS log channels for all appliance types, but user-created log channels can be used instead to have different file names or sizes. These log channels can be associated with BIND Categories in the Loggers section of a DNS Appliance Template**.**	

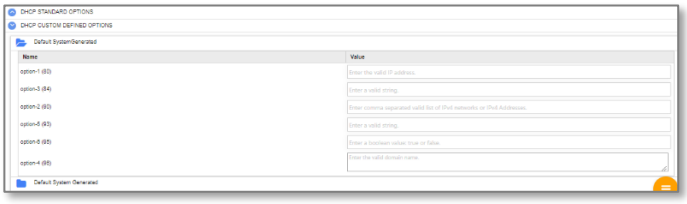
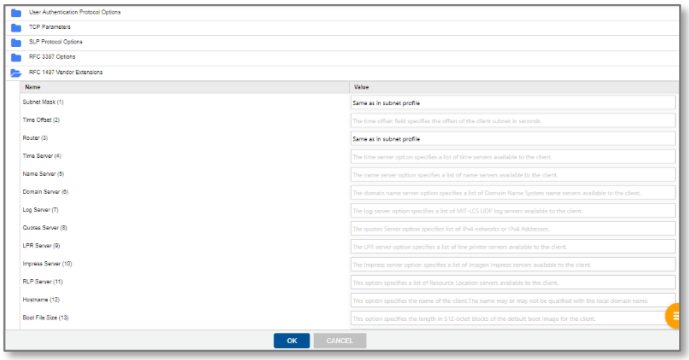
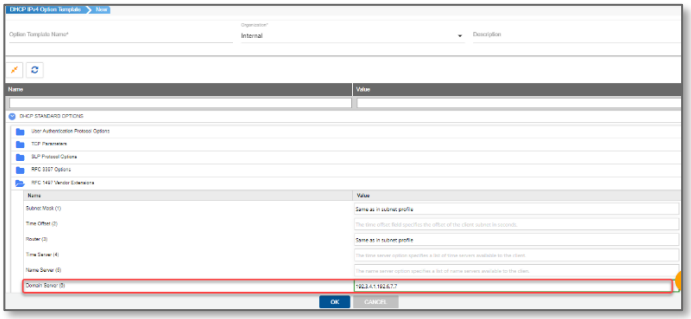
Step	Procedure	Screenshot
14	**Create DNS Appliance Template** To create a DNS Appliance Template, navigate to Network Management >> DNS Management >> DNS Templates >> DNS Appliance Templates. a. Click ⊕. b. Choose a **DNS Appliance Type** from the drop-down menu. c. Enter a **Template Name**. d. If automatic updates of IPAM, DNS, and DHCP Appliances are desired**,** select **Enable Dynamic Updates**. e. If logging of DNS queries and responses is desired, select **Enable DNSTAP Logs**. f. If the **DNS Appliance Type** is **ISC BIND Authoritative** or **DNS Proxy**, then the **TSIG Algorithms** section is displayed. In this case, click ⊕, and choose an **Algorithm** from the drop-down menu, enter the **Bit Size,** and then click **OK**. **Note**: Transaction Signatures (TSIG) are a mechanism used to secure DNS messages and provide secure appliance-to-appliance communication. g. If the **DNS Appliance Type** is **ISC BIND Authoritative**, **ISC BIND Cache**, or **DNS Proxy**, then the **Loggers** section is displayed. Loggers are used to log messages to different log channels. If this section is shown, click ⊕ and do the following: i. Choose a **Category** from the drop-down menu. The choices are based on the logging categories in BIND DNS. ii. Choose a **Channel** from the drop-down menu. The choices are the default log channels in TCPWave plus any that were	

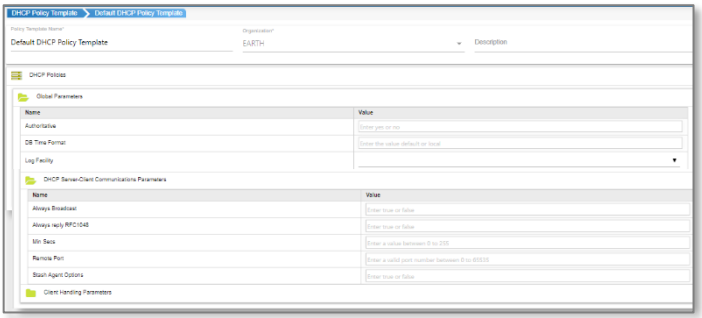
Step	Procedure	Screenshot
	created in the step Create DNS Log Channels (Optional). h. (Optional) Under certain conditions, configure information in the **DNS Forwarders** tab. This tab is enabled for both Internal Cache appliances and BIND Authoritative and Cache appliances. Appliances with an internal cache can resolve zones that are in TCPWave IPAM. If a user wants to resolve to external zones using an appliance with an internal cache, then the user should add the external zones in the **DNS Forwarders** tab. Note that it is not possible to create DNS forwarders when DNS Views are enabled in IPAM. i. Click **OK**.	
	TCPWave IPAM provides default DNS Appliance Templates for all appliance types, but user-created DNS Appliance Templates can be used instead of default ones to customize template values. DNS Appliance Templates are applied to DNS Appliances at the server level.	
15	**Create DNS Option Template** To create a DNS Option Template, navigate to Network Management >> DNS Management >> DNS Templates >> DNS Option Templates. a. Click ⊕. b. Choose an **Organization** from the drop-down menu. c. Enter a **Template Name.** d. Enter additional information, such as in the **Rate Limit** section, as needed e. Click **OK**.	
	DNS Option Templates are applied to DNS Appliances in order to set values in the options blocks of DNS configuration files.	

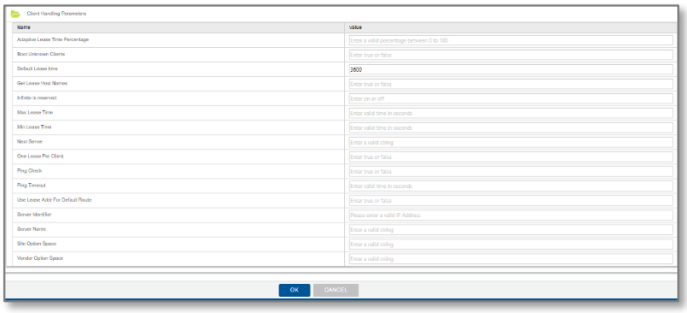
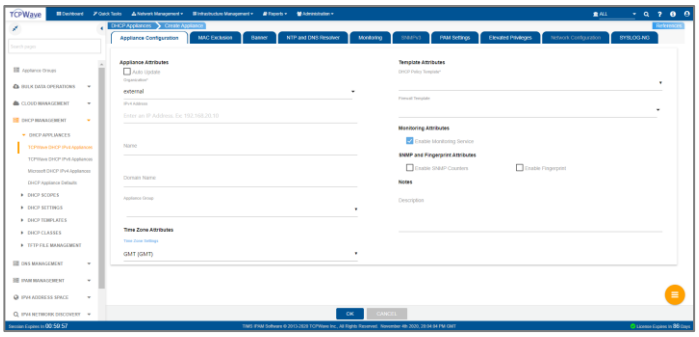
Step	Procedure	Screenshot
16	**Create DNS Appliance** To create a DNS Appliance, navigate to **Network Management >> DNS Management >> DNS Appliances**. a. Click ⊕. **Result**: A page is displayed on which BIND Authoritative, BIND Cache, NSD, Unbound, and DNS Proxy appliances can be created. b. Enter an **IPv4 Address** of an existing object that has an Object Type of TCPWave Remote. **Result**: A lookup is done, and values for **Host Name** and **Domain Name** are retrieved. c. Choose values for the **DNS Appliance Template** and **DNS Option Template** from the respective drop-down menus. d. Click the **NTP and DNS Resolver** tab, and then enter the IP address of an NTP server. **Note**: A TCPWave appliance requires a time server for synchronization. If there is not an NTP server, such as a Domain Controller, in your network, you can do a search on the internet to find a public NTP server to use. e. Also on the **NTP and DNS Resolver** tab, in **Name Appliance** enter the IP address of another DNS server that can be used for DNS resolution during server startup. This can be a DNS server on your network or a public DNS server, such as 8.8.8.8. Up to four other DNS servers can be entered in case one or more are unavailable. f. Click the **Monitoring** tab, and then enter values for **Trap Sink-1**, **Trap Sink-2**, **Community String**, and **Processes to be Monitored**. The trap sink values are IP addresses that are destinations for sending SNMP traps. Also, select at least one	

Step	Procedure	Screenshot
	processes to be monitored. g. Click **OK**.	
17	**Create DNS Zone Template** To create a DNS Zone Template, navigate to Network Management >> DNS Management >> DNS Templates >> DNS Zone Templates. a. Click ⊕. b. Choose an **Organization** from the drop-down menu. c. Enter a **Template Name.** d. In the **SOA Record Attributes** section, enter the **Email Address** of the administrator responsible for the zone. e. Click the **TCPWave DNS Appliances** tab, and then select master and slave DNS appliances. f. Click **OK**.	 
	Microsoft DNS Master Appliances tab: When a Microsoft DNS master appliance is selected in the Zone Template page, all the zones associated with the template are updated in the Microsoft DNS appliances. **Cloud DNS Providers** tab: This tab displays the list of cloud DNS providers that are associated with the zone template.	
18	**Create DNS Zone** To create a DNS Zone, navigate to Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones. a. Click ⊕. b. Choose an **Organization** from the drop-down menu. c. Choose a zone template from the **Apply Template** drop-down menu. d. Enter a valid **Zone Name**, for instance example.com. e. (Optional) Enter a **Contact**, a **Description**, or both. f. (Optional) Select the options **Enable DNSSEC**,	

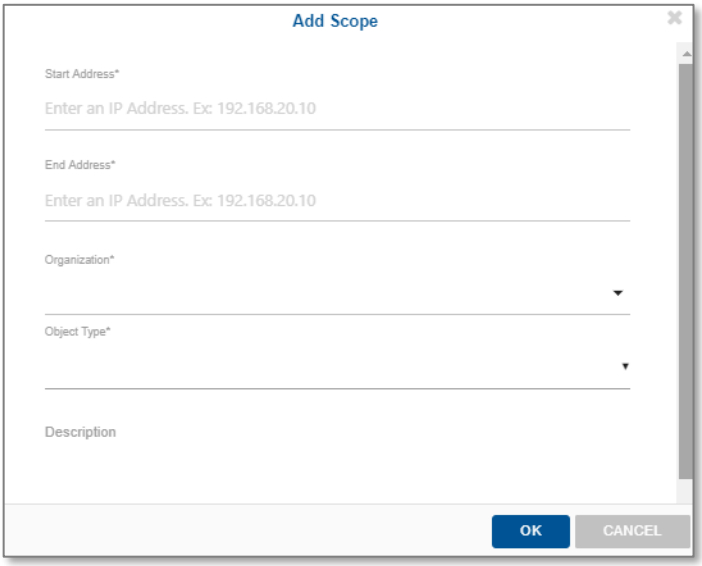
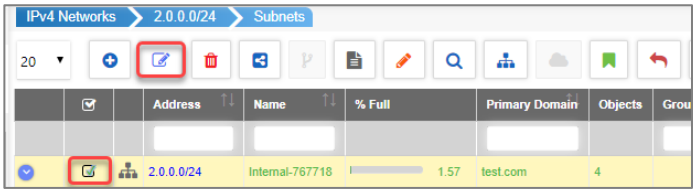
Step	Procedure	Screenshot
	Restrict Zone, **Monitoring Service**, **DMZ Visibility**, and **Enable Active Directory Updates** as needed. g. (Optional) Click the **Resource Records** tab, and then add any resource records that are needed at the zone level. Supported record types are A, AAAA, CNAME, MX, SRV, TXT, NAPTR, and NS. h. Click **OK.**	
19	**Create DNS Root Zone (Optional)** To create a DNS Root Zone, navigate to Network Management >> DNS Management >> DNS Zones >> DNS Root Zone. a. Click ⊕. b. Choose an **Organization** from the drop-down menu. c. (Optional) Select **Enable DNSSEC**, and then choose an **NSEC Option** from the drop-down menu. d. Enter a **Default TTL** value, and choose an associated time unit from the drop-down menu. e. For **Allow Query**, enter an IP address or ACL. f. (Optional) Enter a **Contact,** a **Description**, or both. g. Click the **Root Appliances** tab, and then select a **Root Server.** h. Click **OK.**	
20	**Create DHCP IPv4 Option Template** To create a DHCP IPv4 Option Template, navigate to **Network Management** >> **DHCP Management** >> **DHCP Templates** >> **IPv4 Option Templates**. Note that this step is required to create a DHCP IPv4 Scope. a. Click ⊕. b. Enter an **Option Template Name**. c. Choose an **Organization** from the drop-down menu.	

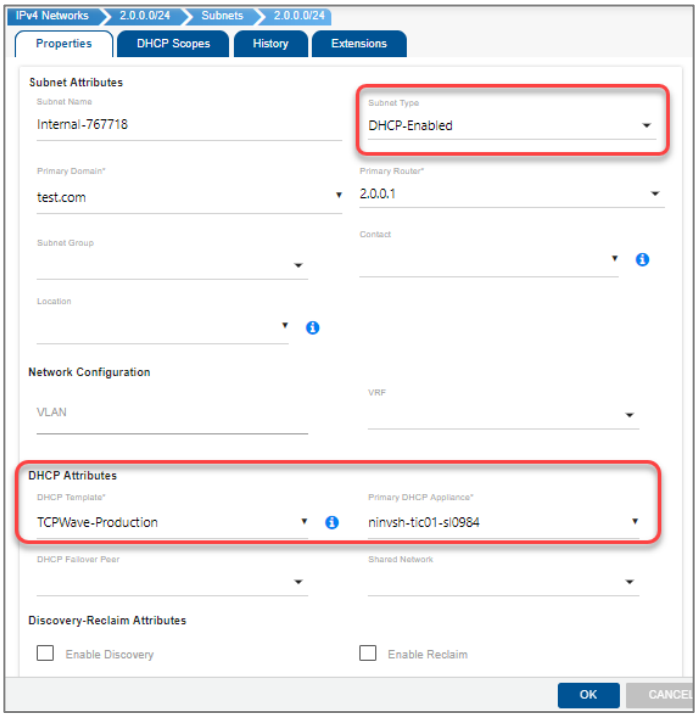
Step	Procedure	Screenshot
	d. Click the expand icon in the upper left part of the screen to see the available DHCP options, which are defined in Internet RFCs. The options are grouped based on the RFC in which they were introduced. Also, at the bottom of the page are custom-defined DHCP options. Many of the options that are blank, such as **Name Server (5)**, are seldom used in modern networks. Others are used for only special kinds of DHCP clients. Some option values in the group **RFC 1497 Vendor Extensions** cannot be changed. **Subnet Mask (1)** and **Router (3)** are populated with **Same as in Subnet Profile**, and these cannot be changed or removed. **Domain Name (15)** is set to **Same as the primary domain in subnet profile** and also cannot be changed or removed. e. Enter values for **Option 1**, **3**, **6**, and **15**, since these are required for almost all DHCP clients. f. Enter a value for the **Domain Server (6)** option. It is not defined by default, but at least one DNS IP address is needed in order for this template to be useful for Windows, Apple, Android, and most other DHCP clients. This option specifies the DNS appliance(s) that DHCP clients use for DNS queries. One or more IP addresses (not names) are required for this server option. If you do not remember the IP address of a DNS appliance, you can open another IPAM window and do a Global Search using a DNS appliance name. For multiple IP addresses, separate them with commas. For example, "192.168.1.27,196.168.0.5". An IP address does not necessarily have to be a TCPWave-managed IP address. For example, you	  

Step	Procedure	Screenshot
	can enter “8.8.8.8,” which is for one of Google’s public DNS servers. g. Populate other options as needed. Some of the more commonly used options are highlighted in green. Some options use a specific type of value, such as a numeric, boolean, IP address, or text string. There is a drop-down list for **Domain Search (119)**. Some options are used just for special DHCP clients (such as PXE clients, clients running old Windows versions, and certain phone models) that need to receive these options from DHCP appliances. DHCP option values are null by default and are only used if values are assigned to them. h. Click **OK**.	
	DHCP IPv4 Option Templates are applied to DHCP IPv4 Scopes to configure the DHCP options that DHCP servers send to clients.	
21	**Create DHCP Policy Template** To create a DHCP Policy Template, navigate to **Network Management** >> **DHCP Management** >> **DHCP Templates** >> **Policy Templates**. Note that this step is required to create a DHCP IPv4 Appliance. a. Click ⊕. b. Enter a **Policy Template Name**. c. Choose an **Organization** from the drop-down menu. d. (Optional) Enter a **Description**. e. Click **DHCP Policies** to expand the folders named **Global Parameters**, **DHCP Client-Server Communications Parameters**, and **Client Handling Parameters**. f. In the **Global Parameters** folder, enter values for **Authoritative** (yes or no), **DB Time Format**, and **Log Facility** as needed.	

<table>
<tr><th>Step</th><th>Procedure</th><th>Screenshot</th></tr>
<tr><td></td><td>g. In the DHCP Client-Server Communications Parameters folder, populate values as needed.
h. In the Client Handling Parameters folder, populate values as needed. Note that Default Lease Time is prepopulated with a default value.
i. Click OK.</td><td>  </td></tr>
<tr><td></td><td colspan="2">DHCP Policy Templates are applied to DHCP Appliances to set server-level policies.</td></tr>
<tr><td>22</td><td><h2>Create DHCP IPv4 Appliance</h2>To create a DHCP IPv4 Appliance, navigate to Network Management >> DHCP Management >> DHCP Appliances >> DHCP IPv4 Appliances. The following configuration options are available for DHCP Appliances:
Primary DHCP Appliance
Primary DHCP Appliance with no failover
Primary DHCP Appliance with a failover
Complete the steps below on the following tabs:
Appliance Configuration tab:
a. Click .
b. Choose an Organization from the drop-down menu.
c. Enter the IPv4 Address of an existing object that has an Object Type of TCPWave Remote.
Result: The Name of the DHCP Appliance and its Domain Name are automatically populated.
d. Select a DHCP Policy Template from the drop-down menu.
e. Select a time zone from the Time Zone Settings drop-down menu.
f. Click OK.
MAC Exclusion tab (Optional):</td><td>  </td></tr>
</table>

Step	Procedure	Screenshot
	a. Enter MAC addresses of clients that should not receive DHCP information from the Appliance. **Banner** tab (Optional): a. Enter a message to display after a user logs in to the DHCP Appliance. **NTP and DNS Resolver** tab: a. Enter one or more IP addresses in **NTP Appliances**. b. In the **Name Appliances** section, enter an IP address in **NS Appliance-1**. **Monitoring** tab (Optional): a. In the **SNMP Configuration** section, enter values for **Trap Sink-1**, **Trap Sink-2**, and **Community String**. The trap sink values are IP addresses that are destinations for sending SNMP traps. b. In the **Process Monitored by SNMP** section, select processes as needed. c. In the **TCPWave Watchdog Configuration** section, click to automatically populate default values. Other tabs (Optional): a. Enter values in other tabs, such as **PAM Settings**, **Network Configuration,** and **SYSLOG-NG**, as needed.	

<table>
<tr><th>Step</th><th colspan="2">Procedure</th><th>Screenshot</th></tr>
<tr><td rowspan="2">23</td><td colspan="2"><h3>Create DHCP IPv4 Scope</h3>To create a DHCP IPv4 Scope, navigate to Network Management >> DHCP Management >> DHCP Scopes >> DHCP IPv4 Scopes. A scope can be created only for a DHCP-enabled subnet. Note that scopes can also be created on the Subnets page by selecting a continuous range of objects.
a. Click .
Result: The Add Scope page is displayed.
b. Enter the Start Address and End Address of the scope.
c. Choose an Organization and an Object Type from the respective drop-down menus.
d. (Optional) Enter a Description.
e. Click OK.</td><td> 
</td></tr>
<tr><td></td><td>Convert Non-DHCP Subnet to DHCP Subnet
As stated above in this step, a scope can be created only for a DHCP-enabled subnet. To convert a non-DHCP-enabled subnet to a DHCP-enabled subnet, do the following:
a. On the Subnets page, select the non-DHCP-enabled subnet and click .
b. Choose the Subnet Type of DHCP-Enabled.
c. In the DHCP Attributes section, choose a DHCP Template and a Primary DHCP Appliance from the respective drop-down menus.
d. Click OK.</td><td> 
</td></tr>
</table>

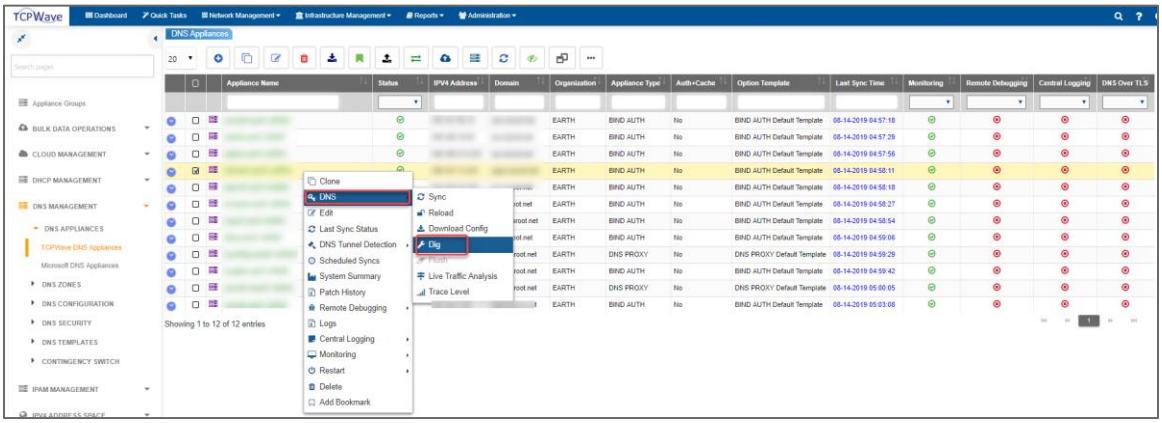
Step	Procedure		Screenshot
			

Verify DNS and DHCP Setup

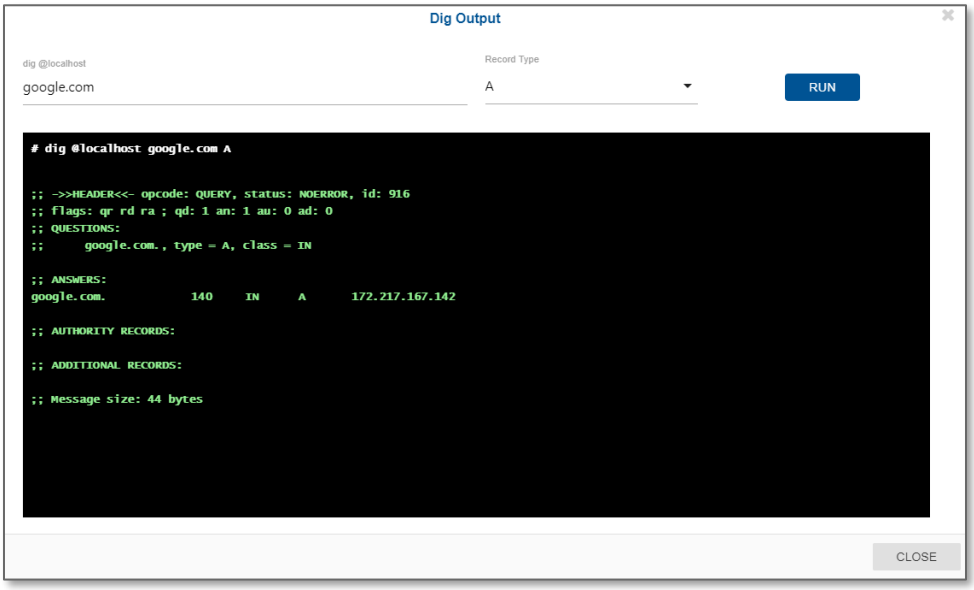
Verify DNS Setup

To verify that the DNS service functions correctly, do the following:

1. Navigate to **Network Management** >> **DNS Management** >> **DNS Appliances**.
2. Right-click on an appliance, select **DNS**, and then select **Dig**.



3. In the **Dig Output** screen, enter the hostname and domain of an IPv4 object that was created in the step above on Create IPv4 Object, for example, server1.company.com.
4. Choose a DNS **Record Type**.
5. Click **Run**.



6. Verify that the Dig output matches the object's information in TCPWave IPAM.

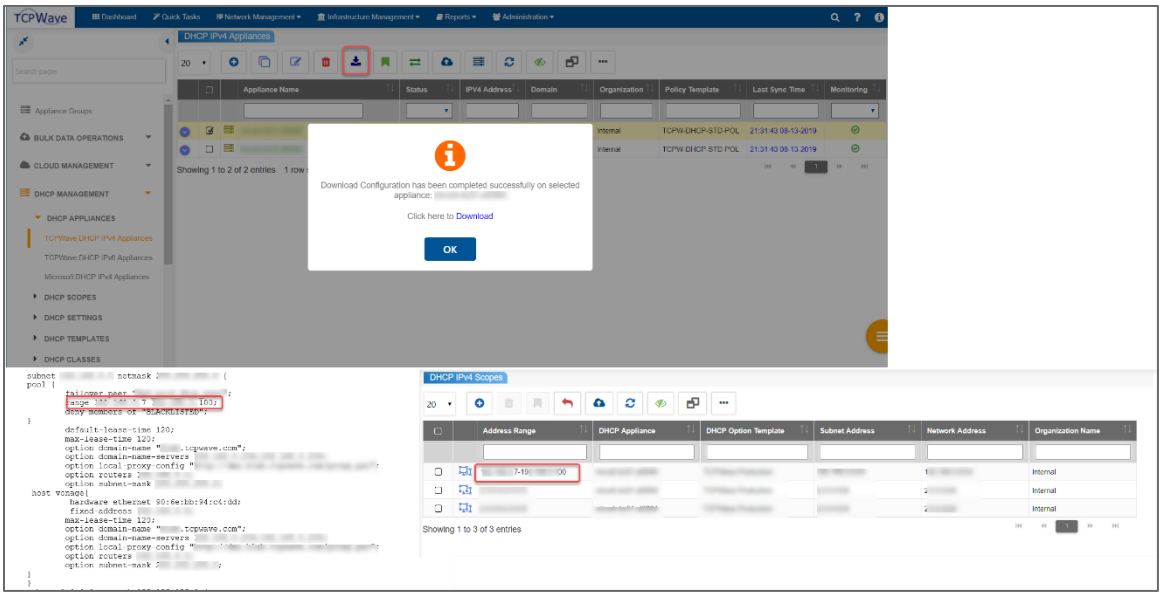
Verify DHCP Setup

To verify that the DHCP configuration is correct, do the following:

1. Navigate to **Network Management** >> **DHCP Management** >> **DHCP IPv4 Appliances**.

2. Select an appliance, and then click the **Download Configuration** icon, as shown highlighted in the upper part of the screenshot below.
3. In the dialog box, click **Download**.

   Result: A dump file is downloaded with the scopes created from the DHCP Scopes page.
4. Rename the file using a ".zip" extension, and then unzip it to view the configuration files in it.
5. Verify that the configuration information in the file matches the DHCP information in TCPWave IPAM.



	For complete information on using TCPWave IPAM, see the TCPWave IP Address Management System Administrator Reference Guide.