A MITEL
PRODUCT
GUIDE

MiVoice Connect

Administration Guide for Edge Gateway

Release 19.3 SP3

May 2023

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Preface 1

ShoreTel is now part of Mitel. Together, we look forward to helping you power connections that are brilliantly simple.

This preface provides information about the objectives, organization, and conventions used in the *Administration Guide* .

Introduction to the Connect Edge Gateway

2

This chapter introduces the Connect Edge Gateway and describes the various protocols used in configuring the appliance.

Overview

The Connect Edge Gateway is a remote access solution to Mitel MiVoice Connect customers. The Connect Edge Gateway makes it possible for users to connect remotely to the MiVoice Connect system by using a Mitel endpoint such as the 400-series IP phone or the Connect client.

To connect remotely to the MiVoice Connect system, all MiVoice Connect customers need an active Internet connection. The Connect Edge Gateway is deployed on the premises of the customer, and supports remote connectivity without the need for a third-party VPN client. You can access and configure the Connect Edge Gateway through Connect Director.

Note:

Connect supports only one Edge Gateway per system.

Note:
Remote 6900 series IP phone requires the use of the Ingate Siparator.

This section discusses the various protocols that the Connect Edge Gateway uses to securely connect remote users to the MiVoice Connect system.

Note:

The Connect Edge Gateway deployment requires all Mitel appliances, such as HQ, DVS, ECC, Conferencing, and so on to have internal FQDNs.

2.1 Connect Edge Gateway Components

The Connect Edge Gateway enables remote users to use any of the components described in this section.

2.1.1 IP Phone

Mitel provides a variety of 400-series IP phones that are used by remote users to connect to the MiVoice Connect system through the Connect Edge Gateway. By using a compatible IP Phone, remote users can access contacts internal to their organization, and use the 3-5 digit dialing function to make calls as if they are inside their corporate network. Users must enable the VPN, and provide RAST FQDN as VPN gateway address on the phone to connect remotely. The minimum firmware version required for 400-series IP phones is 802.841.5100.0.

Legacy phones using the Media Gateway Control Protocol (MGCP) such as the 200, 500 or 600-series are not compatible with the Connect Edge Gateway.

2.1.2 Connect Client

The Connect client provides advanced call management and quality desktop video in an easy-to-use interface for users connecting to the MiVoice Connect system through the Connect Edge Gateway.The Connect client is integrated closely with Microsoft Outlook and offers instant messaging to users who want to stay connected all the time.

2.1.3 Connect Contact Center

The Connect Contact Center software is used by remote agents to connect to the MiVoice Connect system through the Connect Edge Gateway for advanced multimedia call center solutions. The Connect Contact Center can be accessed through a web interface using the URL: https://call_center_ext_fqdn/ecc for advanced call handling. Users must specify Contact Center FQDN configured on the Edge Gateway for accessing Connect Contact Center.

2.1.4 Connect Conference

If you are an existing conferencing service user and you want to use the conferencing service remotely, an Edge Gateway is not required. However, if you place the conferencing service behind a reverse proxy for secured access, you must add an Edge Gateway on the Internet facing side.

To access conferencing through Edge Gateway, you must configure and enable a unique Collaboration FQDN on the Edge Gateway. Also, each Service Appliance requires a unique FQDN.

The Collaboration FQDN must resolve to the internal IP Address of a single Service Appliance or you must configure DNS such that it resolves to the internal IP Address of one of the existing Service Appliances.

2.2 Connect Edge Gateway Technologies

This section includes information about the technologies available through the Edge Gateway, the client that uses these technologies, and the client end user experience using the client through the Edge Gateway. Use port 443 for RAST, Reverse Proxy, and TURN services.

2.2.1 Remote Access Secure Tunneling (RAST) Protocol

Remote Access Secure Tunneling protocol deploys an encrypted tunnel that uses UDP to transport voice packets to maximize voice quality in situations with significant packet loss, and uses TCP as fallback transport mechanism, if UDP fails. RAST uses TCP for signaling.

RAST offers two types of sessions:

- **IP-based session:** The remote user is assigned a unique IP address. The user owns the IP address and all IP traffic to and from the user is encapsulated as RAST payload packets. This session is used in the Connect Edge Gateway.
- **Flow-based session:** The remote user establishes a session and opens one or more TCP/UDP flows. Each flow has a unique destination IP address, destination port number, protocol, source IP address and source port number. The user specifies these unique identifiers in the flow start request message and the Connect Edge Gateway assigns the source IP and port number to the flow. Each connection that the user initiates is unique because of the unique identifiers assigned to that particular flow. Flow-based session is used in the Connect Edge Gateway by default.

2.2.1.1 Client Endpoint

RAST is the technology used to connect external 400-series IP phones to the MiVoice Connect system without using a third-party VPN.

2.2.1.2 Client End User Experience

Users using a 400-series IP phone outside the PBX network have a seamless experience that does not differ from their experience using the 400-series IP phone from inside the PBX network. On the 400-series IP phone, users must enable the VPN, and provide the RAST FQDN as VPN gateway address to connect remotely.

2.2.2 Reverse Proxy

Reverse proxy is an intermediate proxy server that provides server resources to a requesting client outside the internal network. The clients interact with the proxy server as if it were the original server and have thus no knowledge of the actual server providing the resources. Reverse proxies are configured in the proximity of one or more web servers. Any public Internet traffic destined for the web servers is directed to the reverse proxies.

The Connect Edge Gateway uses a reverse proxy to service remote clients needing access to the Mitel Authenticator, Bootstrapper, CAS service, proxy service for voicemail audio streaming or downloading, collaboration Unified Communications in a Box (UCB) conferencing, WebSocket Server (WSS) for softphone, and Contact Center agents on the premises. A reverse proxy can help data encryption, load balancing, caching static content, data compression, and data security.

2.2.2.1 Client Endpoint

Reverse proxy is the technology used by Connect Contact Center agents to access the Interaction Center web page from a location outside the contact center. It is also used by the Connect client and conferencing through Edge Gateway.

2.2.2.2 Client End User Experience

When a Connect Contact Center agent accesses the Interaction Center from outside the contact center or Connect client accesses the Edge Gateway, either the FQDN configured by the administrator or an IP address to a DNS configured for external use must be specified. In both cases, the administrator configures and provides the information to the agent.

2.2.3 Network Address Translation (NAT)

Network Address Translation (NAT) is typically deployed for a private stub network that communicates with the public Internet by dynamically mapping a set of private addresses to a set of globally valid network addresses. The addresses in the private network are local to the network and are not valid outside the network. Hence, other private networks can reuse the same private addresses.

NAT is used on the Connect Edge Gateway to map a set of private IP addresses on the same network to a public IP address that can be used over the Internet. This helps limit and conserve the amount of IP addresses in use and also protects the private network from the public Internet. By deploying NAT, the Connect Edge Gateway can allow clients in a private network access

the external network, and enable access to selective remote clients from the public Internet. The Connect Edge Gateway generates and stores an NAT forwarding table containing the list of private and public IP addresses to be used as reference for translation. Hence, all users communicating through the NAT firewall are assigned a local IP address and an external IP address by the Connect Edge Gateway.

When users communicate using the Connect Edge Gateway that deploys NAT, they have no mechanism of finding out their public IP address or the public IP address of the destination. NAT uses Session Traversal Utilities for NAT (STUN) to assign a unique port for the private IP address of the Edge Gateway. Hence, NAT can be traversed to establish end-to-end peer connections by using Session Traversal Utilities for NAT (STUN), Traversal Using Relay around NAT (TURN), and Interactivity Connectivity Establishment (ICE) Protocol, as explained in the following sections.

2.2.3.1 Session Traversal Utilities for NAT (STUN)

Session Traversal Utilities for NAT (STUN) is a client-server protocol used by remote clients to establish a peer-to-peer connection through the NAT firewall. STUN is not an NAT traversal solution by itself, but used with traversal solutions, such as ICE. A typical STUN setup consists of a STUN client connecting from a private network to another private network and/or Internet through one or more NAT firewalls. The STUN server is located on the Internet.

STUN helps a remote client determine the IP address and the port number (the combination of which is termed as transport address) allocated to itself by NAT. STUN can also be used to check connectivity between two remote clients and as a keep-alive protocol to maintain NAT bindings.

STUN runs over TCP in addition to UDP and supports two types of transactions:

- **Request-response transaction:** A client sends a request to the server and the server returns a response. A transaction ID is generated, which allows a client to associate the response with the respective request.
- **Indication transaction:** A client or a server sends an indication that generates no response. A transaction ID is generated, which serves as a debugging aid.

The STUN server performs the translation of private IP addresses to a public IP address. The users contact the STUN server to retrieve their translated public IP address that they send to the remote user directly.

2.2.3.2 Traversal Using Relay Around NAT (TURN)

Clients behind an NAT firewall can exchange packets with clients behind a different NATfirewall by using hole punching techniques to discover a direct communication path. When a direct path cannot be found, it becomes necessary to use an intermediate server that acts as a relay for packets. The relay serverthat is based on Traversal Using Relay around NAT (TURN), is located on the public Internet and relays packets between the two remote clients.

A typical TURN setup consists of a TURN client in a private network to connect to the public Internet through one or more NAT firewalls. The TURN protocol enables the TURN client to request a server (TURN server) to act as a relay.The TURN server is located on the public Internet and assigns relay addresses to remote clients. Through the TURN server, the TURN client communicates with one or more clients on the public Internet that may or may nor be behind NAT firewalls.

The TURN client controls how the packets are relayed, by obtaining the IP address and port number of the TURN server to form the relayed transport address. When a remote client sends a packet to the relayed transport address, the TURN server relays the packet to the TURN client. The TURN client communicates the relayed transport address of the TURN server to remote clients, which in turn communicate the server-reflexive transport address to the TURN client. The exchange of transport addresses can take place through email messages, or by using a special-purpose rendezvous protocol.

When TURN is used with ICE protocol, the relayed transport addresses and the server-reflexive transport addresses are included in the ICE candidate information to be sent using the rendezvous protocol.

Client Endpoint

TURN technology is used by the Connect client to connect to the PBX network when a user is outside the network.

Client End User Experience

The Connect client end user, using the client outside the PBX network must specify either the FQDN configured by the administrator or an IP address to a DNS configured for external use. In both cases, the administrator configures and provides the information to the user.

2.2.3.3 Interactivity Connectivity Establishment (ICE) Protocol

To establish multimedia sessions, a two-phase exchange of Session Description Protocol (SDP) messages is used by SIP. SIP carries the transport addresses of media source in messages that creates problems while passing through NAT firewall. To reduce media latency, decrease packet loss, and reduce operational costs of deploying the application, Interactivity Connectivity Establishment (ICE) protocol is used in conjunction with STUN or TURN.

The ICE protocol allows communicating clients to discover paths in network for exchanging information. The ICE protocol is also responsible for the handshake between two clients attempting to communicate. ICE retrieves the local IP address, the public IP address, and the relay IP address and treats them as ICE candidates that have to be validated before establishing an end-to-end peer relationship between two users.

The ICE protocol grants higher priority to sending packets through the STUN server than relaying packets through the TURN server.

2.2.4 Demilitarized Zone (DMZ)

The Demilitarized Zone (DMZ) is the region between the external firewall and the internal firewall, where the Connect Edge Gateway is deployed. External networks can only access devices in the DMZ, thereby securing internal private networks on the other side of the internal firewall.

The following rules apply to a DMZ:

- Both the external and internal network can access the DMZ.
- Hosts in the DMZ can only access the external network, but not the internal network.

Deploying the Connect Edge Gateway 3

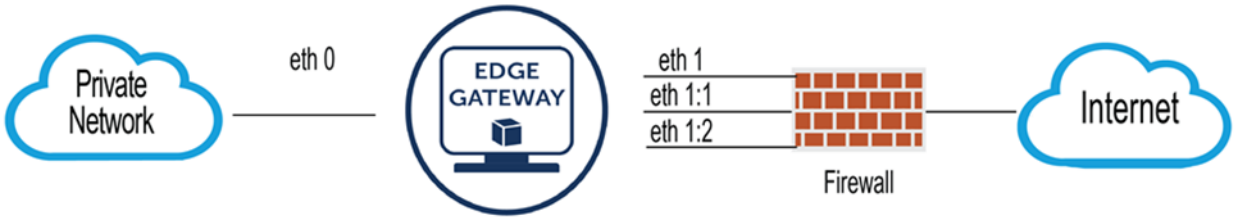
This chapter describes the different models for deploying the Connect Edge Gateway.

3.1 Network Topology

In a typical MiVoice Connect deployment, the Connect Edge Gateway is placed in the Corporate DMZ and is the device where all outside tunnels and sessions terminate. For security reasons, it is the only device in the DMZ that external devices can access.

3.1.1 Edge Gateway Interface

Figure 1: Edge Gateway Interface



The Connect Edge Gateway has two physical interfaces: eth0 and eth1.

- The eth0 interface connects to Enterprise network, and has one IP address.

  Table 1: For eth0, the ports are as follows:

NTP	123
EGWDS	5440, 5452, and 5453
HTTPS	443
SSH	22
TURN/STUN media ports	10,000 - 14,999

- The eth1 interface connects to the Internet, and has three IP addresses over UDP/TCP on port 443
  - One main IP address—Only used for RAST
  - Two aliases—TURN uses eth1:0 and Reverse Proxy uses eth1

Note:

- Ensure that the eth0 and eth1 IP addresses are not in the same subnet.
- If you intend to assign internal IP addresses (DMZ network) to the eth1 interfaces and use NAT to map publicly accessible IP addresses on a firewall to the eth1 IP addresses, you must add firewall rules to map the public IP addresses to the eth1 IP addresses.

3.1.2 Corporate DMZ

Corporate DMZ refers to the area between the external and internal firewalls of the corporate network. External devices have direct access only to the devices in the DMZ, therefore keeping the internal network unexposed.

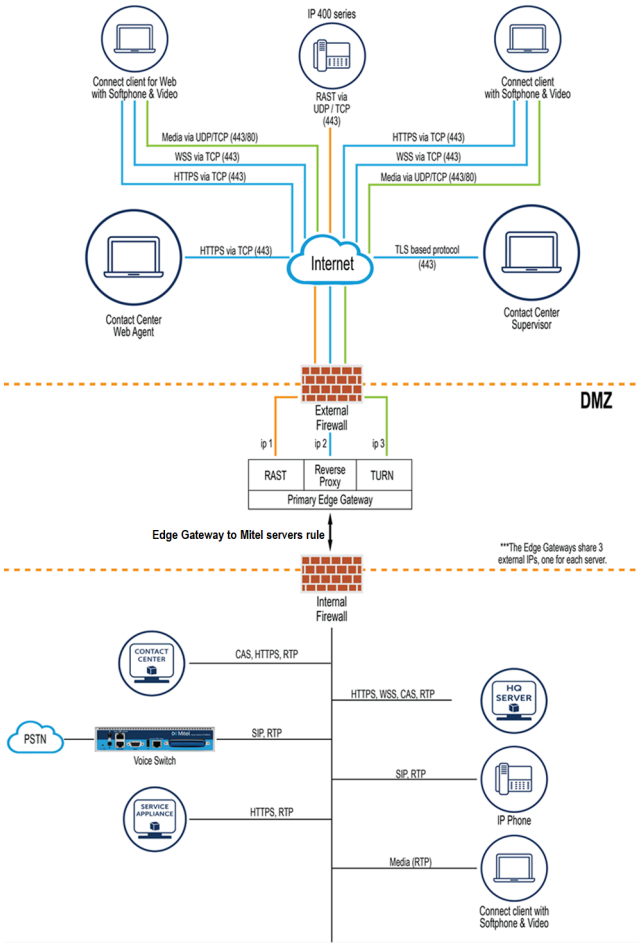
The Connect Edge Gateway has private interface (eth0) for management and public or DMZ facing interface (eth1) for application data. Three different public or DMZ IP addresses must be on the same subnet (IP1, IP2, and IP3 as shown in Network Architecture) and configured on the eth1 interface.

Note:

- For eth0, enable the required media relay ports on the TURN server.
- Connect Edge Gateway needs three public IP addresses for RAST, TURN, and Reverse Proxy all are on port 443. These three IP addresses are either configured directly on the Connect Edge Gateway on eth1 interface using Connect Director or using NAT outside of the Connect Edge Gateway for corresponding three DMZ addresses configured on Connect Edge Gateway.

3.1.3 Network Architecture

Figure 2: Network Architecture



3.2 Types of Deployments

The Connect Edge Gateway can only be deployed as a virtual appliance. It is sometimes also referred to as the vEdgeGW.

3.2.1 Connect Edge Gateway as a Virtual Appliance

MiVoice Connect users can deploy the Connect Edge Gateway as a virtual appliance, where Mitel provides the virtual image that the users can install on their hardware. The vEdgeGW is allotted resources depending on the scale of deployment.

3.2.1.1 System Capacity

To increase the number of users that are supported on an Edge Gateway, you can allocate more virtual CPUs and RAM and buy more licenses (this might require loading the VM on another physical server).

To ensure adequate real-time system performance, follow these criteria for virtual servers:

- Use a dedicated NIC that can be shared with all MiVoice Connect virtual appliances, including Edge Gateway.
- The virtual machine CPU and memory must be reserved or dedicated to the guest computer so that real-time communications are not delayed while being allocated to the host resources.
- A dedicated NIC can be shared with all MiVoice Connect virtual appliances. Total bandwidth use must be considered. If the real-time audio is impacted, then the appliances using real-time audio (for example, LDVS, UCB, and so on.) must be moved to their own dedicated NICs.
- Never use a 100-Mbit Ethernet for any MiVoice Connect virtual server.

The following lists the various system capacity values for the Connect Edge Gateway.

Table 2: System Capacity for the Connect Edge Gateway - Part 1

Size	Cores	RAM per VM	Disk Space	Networks	Processor
Small	2	2 GB	100 GB	100 Base-T or Gigabit Ethernet	Intel Xeon CPU E5-2680v3@ 2.5GHz
Medium	4	4 GB	100 GB	Gigabit Ethernet	Intel Xeon CPU E5-2630 v4 2.2 GHz
Large	8	8 GB	100 GB	Gigabit Ethernet	Intel Xeon CPU E5-2630v5@ 2.2GHz

Table 3: System Capacity for the Connect Edge Gateway - Part 2

Size	400-Series IP Phones Using RAST: Registered	400-Series IP Phones Using RAST: Active Calls	Clients: Registered	Clients: Concurrent Voice Calls
Small	100	50	50	50
Medium	500	100	400	100
Large	2,000	200	2,000*	200

Table 4: System Capacity for the Connect Edge Gateway - Part 3

Size	AIC Registered with KPI Dashboard**	AIC Registered with KPI Dashboard + Client Registered	Contact Center: Concurrent Voice Calls
Small	200	50	50
Medium	200	200	100
Large	200	200	100

All other processors must be benchmarked to ensure equivalent or better performance. CPUbenchmarking is available at: http://www.cpubenchmark.net/.

Note:
The Clients Registered can either be Connect Client or Chrome Plugin or a combination of both Connect Client and Chrome Plugin.

Note:
* A maximum of 2000 connections is applicable for existing softphone user registrations and 500 concurrent connections for first-time softphone user logins. Only the first-time user request goes to the HQ server. After the login is successful, a corresponding server will be assigned and later all the subsequent login requests goes to the assigned server.

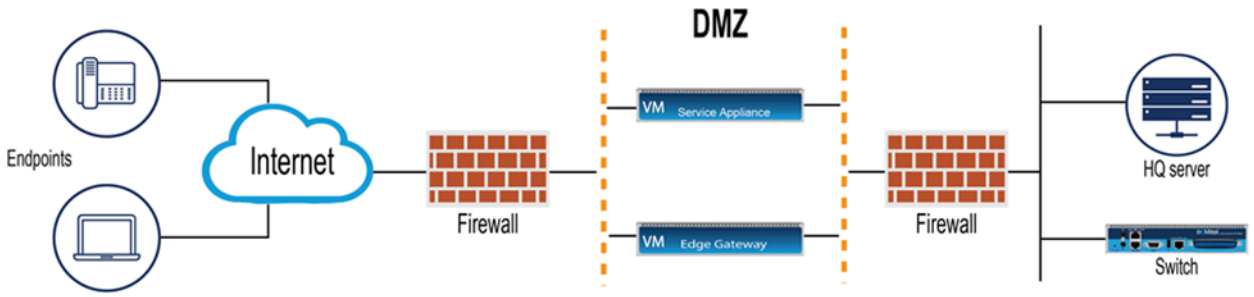
Note:
**AIC refers to the Agent Interaction Center web page. See Client Endpoint on page 5 for more details. The KPI Boards feature allows you to configure the Interaction Center to include key performance information (KPI) about specific interactions. For more information, see the *Using KPI Boards* section in the MiVoice Connect Contact Center Administration Guide.

3.2.1.2 Service Appliance Deployment for Edge Gateway

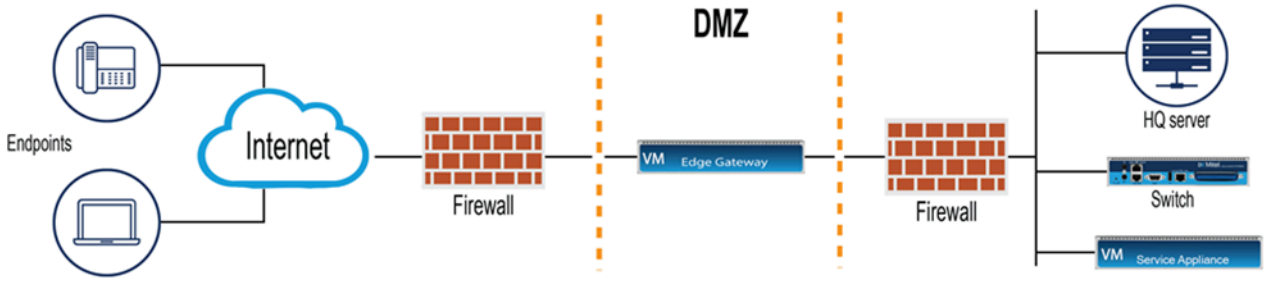
The Edge Gateway can be deployed with MiVoice Connect collaboration service appliances in two separate scenarios (as shown in the Service Appliance Deployment for EG, Figure 3). It is placed in parallel with the service appliance in the corporate DMZ or the Edge Gateway can be placed in the DMZ and have the service appliance in the internal corporate network.

Figure 3: Service Appliance Deployment for EG

Scenario 1: Existing Customers



Scenario 2: New Customers



Installing the Connect Edge Gateway 4

- Installing the Virtual Connect Edge Gateway Software

This chapter describes installation procedures for the Connect Edge Gateway.

4.1 Installing the Virtual Connect Edge Gateway Software

Follow the steps to create a new virtual machine for Connect Edge Gateway Software by using ISO installer or OVA installer:

- Installing Virtual Edge Gateway using ISO Installer (for Connect builds 21.87.9724.0 and later)
- Installing Virtual Edge Gateway using OVA Installer
- Certificate Configuration

4.1.1 Installing Virtual Edge Gateway Using ISO Installer

Note:

This procedure requires the vSphere Web Client, and connection to an ESXi server. The ISO installer is supported for Connect builds 21.87.9724.0 and later.

4.1.1.1 Creating New Virtual Machine in VMware or Hyper-V

VMware

Before creating a new virtual machine in VMware, it is recommended to upload the ISO installer to the VMware datastore. The ISO installer is uploaded only once for a given build, and it can be reused for creating multiple new virtual machines.

To upload ISO Installer file to the vSphere Web Client ESXi 6.0 or later, do the following:

1. Open the vSphere Desktop Client and log in to VMware ESXi server with valid credentials.

2. Navigate to **Home** and click **Inventory**.
3. Click **Datastores and Datastore Clusters**
4. On the **Datastores and Datastore Clusters** tab, select the datastore to which you want to upload the ISO installer file.
5. Right-click the datastore and select **Browse Datastore**.

   The **Datastore Browser** window appears.
6. (Optional) Select the root folder and click **Create a new folder** icon from the menu bar, type the required name, and click **OK**.
7. Select the folder that you created or select an existing folder, and click **Upload a File** icon from the menu bar, and select **Upload File**.
8. Click **Browse** and select the virtual Edge Gateway iso file located at: `C:\inetpub\ftproot\egw\edge_gateway_installation.iso`.
9. Click **Open**.

   Time required to upload the ISO installer file varies, depending on the file size and the network upload speed.
10. In the confirmation dialog box, click **Yes**.

    Refresh the datastore file browser to verify the uploaded ISO installer file is in the list.

To create a new virtual machine in VMware:

1. Log in to VMware ESXi server.
2. On the vSphere Web Client, click **Create / Register VM**.

   The new **Virtual Machine wizard** appears.
3. On the **Select creation type** tab, select **Create a new virtual machine** and click **Next**.
4. On the **Select a name and guest OS** tab, do the following

   - Type the required name of a new virtual machine in the **Name** field. The virtual machine name must be unique within each ESXi instance, and can contain up to 80 characters.
   - Compatibility: ESXi 6.0 or later virtual machine.
   - Guest OS family: Linux.
   - Guest OS version: CentOS 4/5/6/7 (64-bit).
5. Click **Next**.
6. On the **Select storage** tab, select the appropriate datastore location, and click **Next**.

7. On the **Customize settings** tab, click **Virtual Hardware** and do the following

   - CPU: 2
   - Memory: 2048 MB
   - Hard disk 1: 100 GB

   > **Note**:
   >
   > Disk Provisioning should be Thin Provisioned.

   - SCSI Controller 0: VMware Paravirtual
   - SATA Controller 0:
   - USB controller 1: USB 2.0
   - From the **Network Adapter 1** drop-down menu, select **VM Network**. By default, **Connect** is enabled.

     This network is added to the internal network.
   - Click **Add network adapter** to add a new Network Adapter, and select **VMnic2** network from the drop-down menu. By default, **Connect** is enabled.

     This network is added to the external or DMZ network.
   - From the **CD/DVD Drive 1** drop-down menu, select **Datastore ISO file**.
   - In the **Datastore browser** window, select the appropriate datastore on the first pane, and **edge_gateway_installation.iso** file on the second pane. Click **Select**. By default, **Connect** is enabled.
   - Video Card: Specify custom settings.
8. Click **Next**.
9. On the **Ready to complete** tab, review the virtual machine details, and clcik **Finish**.

   The virtual machine appears in the vSphere Web Client window.
10. Right-click the virtual machine, and select **Power on**.

Hyper-V

To create a new virtual machine in Hyper-V:

1. On the **Hyper-V Manager**, right-click **HYP-V** and click **New**.
2. In the pop-up menu, select **Virtual Machine**.

   New Virtual Machine Wizard appears.

3. On the **Specify Name and Location** tab, type the required virtual machine name, and click **Next**.
4. On the **Specify Generation** tab, select **Generation 1** and click **Next**.
5. On the **Assign Memory** tab, type the memory size to allocate the virtual machine:
   - Startup memory: 2048 MB (2 GB)
6. Click **Next**.
7. In the **Configure Networking** tab that opens, do the following:
   - CPU: 2
   - Select **Broadcom NetXtreme Gigabit Ethernet #3 - Virtual Switch** from the **Connection** drop-down menu.
   - Click **Next**
8. On the **Connect Virtual Hard Disk** tab, type the virtual hard disk size:
   - Size: 100 GB
9. Click **Next**.
10. On the **Installation Options** tab, select **Install an operating system from a bootable CD/DVD-ROM.** Select **Image file (.iso)**
11. Browse to the virtual Edge Gateway iso file located at: `C:\inetpub\ftproot\egw\edge_gateway_installation.iso`. Click **Next**.

    Time required to upload the ISO installer file varies, depending on the file size and the network upload speed.
12. In **Completing the New Virtual Machine Wizard**, verify the details you have entered and click **Finish**.
13. From the **Virtual Machines** list, right-click the newly created virtual machine, and do the following:
    - Click **Start** to start the virtual machine.
    - Click **Connect** to connect to the console.

4.1.1.2 Configuring and Installing the Virtual EG

1. After the virtual machine is turned on, select the virtual machine, and click **Console** and **Open browser console** from the drop-down menu to see the CLI console. The virtual machine starts with the boot menu, and prompts for HQ server IP address.
2. Type the HQ server IP address. For example, 10.23.174.136.

Note:

Based on the network speed, the installation approximately takes five to ten minutes.

3. After the installation is complete, type **reboot** and press **Enter**.

   The Virtual Edge Gateway restarts, and the login screen appears.
4. Log in as **admin** and do the following:

Note:

Mitel recommends you to create, a new user with the administrator privilege and a complex password. After you assign the System Administrator role to a user, the default user “admin” is disabled. For additional information about granting administrative permissions to users, refer to the *Administrative Permissions* in the *MiVoice Connect System Administration Guide*.

   a. For **To accept the Mitel End User License Agreement**, type **YES**.
   b. For **Initial configuration wizards**, type **YES**.
   c. Type the required Hostname. (for example, egw01)
   d. For **Use DHCP on eth0 interface?**, type **No**.
   e. Type the Primary IPv4 address, and masklen [0.0.0.0/0]: (for example, 10.23.174.100)
   f. Type the Default Gateway. (for example, 10.23.174.1)
   g. Type the Primary DNS server address.
   h. Type the Domain Name.
   i. For **Admin password, (Enter to leave unchanged)?**, press **Enter**.
   j. Verify the details you have entered, and press **Enter** to save the changes.
5. After the configurations are saved successfully, type the following command:

```
enable

_crusto

reboot
```

Note:
Admin users have root privileges and *_crusto* provides CLI access to the Admin user.

6. You must restart the virtual Edge Gateway system to complete the virtual Edge Gateway deployment.

4.1.2 Installing Virtual Edge Gateway Using OVA Installer

Note:

This procedure requires the vSphere Web Client ESXi 6.0 or later, and connection to an ESXi server.

Note:

First time Connect Edge Gateway installation is completed using a combination of the following steps, including using the flash drive in your packaging and steps performed using Connect Director. Refer to Configuring the Connect Edge Gateway on page 24 for configuration information after completing these steps.

1. From vSphere client log on to vCenter server.
2. Click **File** > **Deploy OVF Template**.
3. Browse to the virtual Edge Gateway **ova** file located at: `C:\inetpub\ftproot\egw\edge_gateway_installation.ova`. Click **Next**.
4. Review the OVF template details and click **Next**.
5. Type a name for the deployed template and click **Next**.
6. Select the host, cluster, or resource pool that you want to deploy the virtual Edge Gateway. Click **Next**.
7. Select the destination storage for virtual Edge Gateway files.

   Ensure that you have at least 100 GB of free disk space.
8. Click **Next**.

9. Map the networks used in the OVF template to networks in customer's inventory. Map the VM network to internal network and VMnic2 network to external network. Click **Next**.
10. Review the settings. Uncheck **Power on** after deployment and click **Finish** to deploy the virtual machine.
11. To power on the Edge Gateway, right-click the VM and select **Power** > **Power on**.
12. Go to the newly deployed Edge Gateway console. After power on, it boots from bootflop image and tries to get the DHCP IP. Else, it prompts for static IP address.
13. Enter the HQ server IP address.

    After installation, it reboots and displays the login prompt.
14. Log in as **admin** (no password required).
15. When prompted to accept the Mitel End User license Agreement, type **Yes**.
16. The Initial Configuration Wizard is displayed. Type **Yes**

    a. Enter the **Hostname**
    b. Type **No** for **Use DHCP on eth0 interface?**
    c. Enter the **Primary IPv4 address and masklen [0.0.0.0/0]**.

       For example, 10.23.174.100/24
    d. Enter the **Default gateway [0.0.0.0]**.
    e. Enter the **Primary DNS server** address.
    f. Enter the **Domain Name**.
    g. Enter a new **Admin password (Enter to leave unchanged)?**

> **Note**:
>
> Mitel recommends you to create a new user with the administrator privilege. After you assign the System Administrator role to a user, the default user “admin” is disabled. For additional information about granting administrative permissions to users, refer to the *Administrative Permissions* in the *MiVoice Connect System Administration Guide*.

    h. Select **Enter the step number** to edit the above parameters or press **Enter** to save changes and exit.
    i. **Reboot** the Edge Gateway.

Note:

When you change the admin password from Edge Gateway, it overrides the configuration of Connect Director till the Edge Gateway restarts. Therefore, do not change the password from Edge Gateway. Instead, you can change the admin password for all Mitel appliances from Connect Director by navigating to **Administration** > **System** > **Additional Parameters**.

If you want to change the Hostname, eth0 address, default gateway, DNS, and domain name, and passwords for admin and monitor accounts, execute the following commands:

```
[admin@egw-test ~]# cli

egw-test > en

egw-test # config t

egw-test (config) # config jump-start
```

The Edge Gateway displays Step 1 to Step 8, and you can edit them as required. Reboot Edge Gateway.

Configuring the Connect Edge Gateway

5

This chapter describes how to configure the Connect Edge Gateway.

Note:
Adobe Flash Player is no longer supported on Web browsers.

Server Configuration Considerations

Open port 443 on all the public facing IP addresses for both UDP and TCP traffic on the Edge Gateway. If public IP addresses are configured on NAT firewall, then open the port 443 for all the public facing IP addresses. Refer to Connect Edge Gateway Technologies on page 4 for more information about the Edge Gateway technologies.

5.1 Adding an Edge Gateway to Connect

Use Connect Director to perform the following procedures:

Note:

The following instructions assume an IP PBX running Connect has already been installed. See Installing the Virtual Connect Edge Gateway Software on page 15for EGW installation information before proceeding.

1. Launch Connect Director.

2. Click **Appliances/Servers** > **Platform Equipment**. This page provides access to the Platform Equipment list. The list is displayed in alphabetical order.
3. In the upper-right corner of the Platform Equipment page, select **New**. The **General** page displays. Select **Virtual Edge Gateway** from the Hardware type drop-down list.

5.2 Configuring the Connect Edge Gateway

Follow these steps to configure the Connect Edge Gateway using Connect Director:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click **New**. From the **Site** drop-down list, select the site where you want to install Edge Gateway. Select **Virtual Edge Gateway** from the Hardware Type drop-down list.
4. Enter the Connect Edge Gateway parameters as required and click **Save**.

You must enter the **Name**, **IP address**, and **MAC address** of Connect Edge Gateway. You can configure RAST service, TURN service, and Reverse Proxy service as required. If you want to configure all these services, then you must have three public IP addresses or DMZ IP addresses.

5.2.1 Connect EG General Parameters

The following table includes a list of general parameters required for configuring a new Connect Edge Gateway:

Table 5: General Parameters

Parameter	Description
Name	Name of a new or existing server.
Description	Description of the servertype, for example, EdgeGW. (Optional)
IP Address	Private IPaddress of the Connect Edge Gateway's eth0 interface. Select Find Edge Gateway to select from a list of available Edge Gateways.
Find Edge Gateway	Displays all the Connect Edge Gateways found in the subnet. You can select the IP address and MAC address so that the IP address and MAC address fields are aut omatically filled.
MAC Address	Media Access Control (MAC) address of the server.
Fully Qualified Domain Name	Internal FQDN of the Edge Gateway.

The following table includes a list of Gateway IP Address parameters required for configuring a new Connect Edge Gateway. Select the checkboxes to enable the appropriate service and enter the IP address.

The Connect Edge Gateway has two physical interfaces—eth0 and eth1. eth0 interface is used in a private network and has one IP address. eth1 interface has three IP addresses—one main IP address—eth1, and two aliases—eth1:0 and eth1:1. RAST uses eth1. TURN uses eth1:0 and Reverse Proxy uses eth1:1.

Table 6: Gateway IP Address Parameters

Parameter	Description
RAST IP Address	External IP address of RAST Service. Public IP address is mapped to eth1's private addr ess (in the DMZ) by the NAT firewall.
TURN IP Address	External IP address of TURN Service. It cannot be empty when TURN is enabled and can be empty when TURN is disabled. For more information, see Traversal Using Relay around NAT (TURN).
Reverse Proxy IP Ad dress	External IP address of Reverse Proxy Service. It cannot be empty when Reverse Proxy is enabled and can be empty when Reverse Proxy is disabled. For more information see, R everse Proxy.
Subnet Mask	Enter the subnet mask for eth1 interface. It cannot be empty when any of these services are enabled. RAST, Reverse Proxy, and TURN IP addresses share this subnet mask.
Gateway	IP address of the gateway for eth1 interface.It cannot be empty. RAST, Reverse Proxy, and TURN IP addresses share this gateway.

5.2.2 RAST Configuration

1. In the **RAST** tab, modify or add parameters as needed. Save the Edge Gateway configuration, and then click the **RAST** tab.

5.2.2.1 General Parameters

The following table includes a list of basic parameters that are accessed when editing an existing Connect Edge Gateway:

Table 7: RAST Parameters

Parameter	Description
IP Address (read-only)	IP address of the RAST service.
Network Time Protocol Server	Enter the IP address of the NTP server.
Max Tunnels	Enter the maximum number of tunnels. The range is from 0 to 10000.
Add Configuration Servers	Enter the IP address of the Connect Director (HQ server) or fully qualified domain name. Add or remove the configuration servers as necessary.

5.2.2.2 IP Pool Parameters

You must configure the IP pool (range of IP addresses) for Connect Edge Gateway to assign an internal IP address for each remote IP phone to communicate with other Mitel servers or switches in the enterprise network. Number of IP addresses must be configured depending on the number

of remote IP phones that you require. If you do not have single range of IP addresses, you can configure multiple range of IPaddresses as multiple pools. This IP pool must be reserved and cannot be used by the DHCP.

The table below includes a list of IP Pool parameters that are accessed when editing an existing Connect Edge Gateway. Multiple IP Pools can be added. Refer to Client IP Pool Parameters for more configuration information using the Connect Edge Gateway Administration Portal.

1. **Add** or **Remove** IP Pool from the list as necessary.
2. Click **Save**.
3. Click **Reset** if you want to reset or clear the IP Pool parameters.

Table 8: IP Pool Parameters

Parameter	Description
Name	Name of the IP Pool.
Low IP Address	Starting IP address for the RAST session.
High IP Address	Ending IP address for the RAST session.

5.2.3 Reverse Proxy Configuration

Internal DNS server is the IP address of the DNS server that is reachable from the Edge Gateway internal interface eth0. The internal DNS server resolves internal FQDN for the Edge Gateway to connect to those upstream appliance servers, such as HQ, DVS/ECC, and UCB. In particular, the UCB is required to work with the Edge Gateway with internal FQDN only. The other appliances work with the Edge Gateway without internal FQDN configured, but it is recommended to have the internal FQDN.

The FQDNs listed in the Reverse Proxy tab of the Edge Gateway appliance are the external FQDNs of the corresponding services. The FQDNs must be resolved to the same external IP address of the reverse proxy of Edge Gateway, or public IP of reverse proxy on the firewall, by public DNS servers which clients can access from the Internet.

Note:

You must set up the public DNS so that all the three FQDNs (reverse proxy, conference bridge and ECC) resolve to the same public IP address of the reverse proxy on the Edge Gateway.

For example, if you do not point the conference bridge FQDN to the public IP of the reverse proxy, you will not be able to set up meetings.

The external clients cannot use the public IP of reverse proxy to access the services. To access the services, enter FQDN in the server address field of Connect client or in the address line of web client browser. These FQDNs must be included in the reverse proxy server certificate as Subject Name or Alternative Subject Name to access through HTTPS.

Wildcard certificates are also supported for all external FQDNs on the Edge Gateway, including the RAST service. This means that the RAST and Reverse proxy server certificate can be the same, for example, “*.acme.com”.

Note:

A wildcard certificate only supports the same level of FQDNs. For example, a certificate with a subject of “*.acme.com” can verify “vpn.acme.com” and “connect.acme.com”, but not “conference.uc.acme.com”.

1. In the **Reverse Proxy** tab, modify or add parameters as needed.
2. Click **Save**.

5.2.3.1 Reverse Proxy Parameters

The following table includes a list of reverse proxy parameters that is accessed when editing an existing Connect Edge Gateway. Check the box to select the appropriate reverse proxy FQDN, then enter the address.

Table 9: Reverse Proxy Parameters

Parameter	Description
IP Address (read-only)	IP address of the Reverse Proxy service.
Internal DNS	Enter the IP address of the internal DNS server. This is the IP address of the DNS server deployed in the enterprise local area network.
Max Connections	Enter the maximum number of concurrent HTTP connections.
Connect Client FQDN	Enter the external fully qualified domain name for Connect client. This is the public F QDN advertised to users, for example, start.acme.com.
Collaboration FQDN	Enter a unique external fully qualified domain name for Collaboration. This is a public FQDN, which allows you to use the conferencing service from an external network.

Parameter	Description
	It is functional only when the Global conferencing URL is set in the Other System Parameters page.
Contact Center FQDN	Enter the external fully qualified domain name for Contact Center. This is a public FQDN, which must be accessible by systems outside the HQ network. **Note**: If Contact Center cannot read the FQDN configured in the HQ server even though FQDN is specified correctly, contact Mitel Support Center.

5.2.4 TURN Configuration

1. In the **TURN** tab, modify or add parameters as needed.
2. Click **Save**.

5.2.4.1 TURN Parameters

The following table includes a list of TURN server parameters that is accessed when editing an existing Connect Edge Gateway. Enter the appropriate values and click **Apply**.

Table 10: TURN Parameters

Parameter	Description
IP Address (read-only)	IP address of the TURN server.
Server FQDN	Enter the external fully qualified domain name or public IP address.
Port	Enter the port number as 443.
Min Media Relay Port	Minimum media relay port number. The port range is from 1024 to 65535. Media Relay port is configured for Internal IP.

Parameter	Description
	Note: Media Relay port is configured for internal IP address.
Max Media Relay Port	Maximum media relay port number. The port range is from 1024 to 65535. **Note**: Media Relay port is configured for internal IP address.

5.3 Certificate Configuration

The Connect Edge Gateway solution uses the following certificates to secure communications between the Connect Edge Gateway and devices running Connect:

- **Edge Gateway Certificate:** Certificate used to access the administration portal of the Connect Edge Gateway.
- **RAST Certificate:** Certificate used to authenticate the secured connection between Remote IP phones and Connect Edge Gateway.
- **Reverse Proxy Certificate:** Certificate used to securely access the Mitel services through Reverse Proxy.
- **TURN Certificate:** Certificate used to securely use the TURN service from the Connect Edge Gateway.

You can generate certificates on the Connect Edge Gateway, import self-signed certificates, or individual/wildcard certificates from other certificate authorities.

5.3.1 Locally Generated Certificates

You can create a locally generated certificate on the Connect Edge Gateway. This is a convenient option for enterprises that have not already purchased a certificate. The certificate is signed by the certificate authority on the Connect Edge Gateway.

5.3.2 Certificate Signing Request

Administrators can generate a Certificate Signing Request (CSR) for all Connect Edge Gateway Certificates. The Connect Edge Gateway stores only one set of CSRs and corresponding private keys per type of certificate, and automatically syncs them to the standby node, if applicable.

5.3.3 Generating a Certificate

Use the Connect Edge Gateway administration portal to perform the following procedures:

There are four certificates that establish secure sessions with the Connect Edge Gateway. In addition, these certificates establish authenticated secure remote connections mutually when the clients are outside of the enterprise.

The Connect Edge Gateway presents different certificates when a client initiates a connection from local or remote interfaces.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **System**> **Certificate**.
5. Select **Edge Gateway**, **RAST**, **Reverse Proxy**, or **TURN** as needed.
6. Click **Generate**. The Generate Certificate page appears.
7. In the **Country Name** field, type the two-letter country code for the country where the Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.
8. In the **State** or **Province** field, type the state or province where the Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.
9. In the **Locality** field, type the locality where the Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located. Typically, this is the name of a city.
10. In the **Organization** field, type the name of the organization. Typically, this is the name of the company.
11. In the **Organization Unit** field, type the name of the organization unit (for example, enter the name of a department within the organization).
12. In the **Common Name** field, type the domain name for the Connect Edge Gateway, RAST, Reverse Proxy, or TURN.
13. In the **Key Length (bits)** field, select the required key length from the drop-down list.
14. In the **Subject Alternative Names** field, select the alternative names for the Connect Edge Gateway, RAST, Reverse Proxy, or TURN.
15. In the Other **Alternative Names** field, select **Alternative IP Address** or **DNS** from the drop-down list. Enter the IP Address or domain name and click **Add**.

16. Click **Generate** to generate a certificate signed by the certificate authority installed on the Connect Edge Gateway or click **Generate CSR** to generate a certificate signing request (CSR) to be sent to a third-party certificate signing authority.

> **Note**:
>
> - When generating a CSR, the Connect Edge Gateway outputs both a certificate request as well as an RSA private key. Save the RSA private key in a secure location for future use. This information is necessary when importing the signed certificate.
> - The private key of the CSR is stored in the Connect Edge Gateway.

17. If generating a CSR in the previous step, submit the CSR to a trusted certificate signing authority and save the RSA private key.
18. A confirmation message to restart the Edge Gateway appears. Do either of the following:
    - Click **OK** to restart the service and activate the newly generated certificate.
    - Click **Cancel** if you do not want to restart. The newly generated certificate will be activated on next restart.

> **Note**:
>
> The generated certificate displays in a separate window. The Last Generated Date field updates the current date and time. Verify that the certificate was created correctly by checking the status line at the top of the certificate.

19. Click the **Close** tab to close the certificate window.

The following table includes a list of Generate Certificate parameters:

Table 11: Generate Certificate Parameters

Parameter	Description
Country Name	Indicates the two-letter country code for the country where the Connect Edge Gatewa y, RAST, Reverse Proxy, or TURN is located.
State or Province	Indicates the state or province where the Connect Edge Gateway, RAST, Reverse P roxy, or TURN is located.

Parameter	Description
Locality	Indicates the locality where the Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located. Typically, this is the name of a city.
Organization	Indicates the name of the organization. Typically, this is the name of the company.
Organization Unit	Indicates the name of the organization unit (for example, enter the name of a depar tment within the organization).
Common Name	Indicates the domain name for the Connect Edge Gateway, RAST, Reverse Proxy, or TURN.
Key Length (bits)	Indicates the key length for generating self signed certificate. The Connect Edge G ateway supports key length of 1024, 2048, 3072 and 4096. The longer the number, the stronger the security of the key.
Subject Alternative Names	Indicates the alternative names for the Connect Edge Gateway, RAST, Reverse Pro xy, or TURN.
Other Alternative Names	Indicates the IP Address or domain name for the Connect Edge Gateway, RAST, Rev erse Proxy, or TURN.

5.3.4 Importing a Certificate

You can import a purchased or self-signed certificate to the Connect Edge Gateway, RAST, Reverse Proxy, or TURN. For example, if you purchased a certificate from VeriSign, that certificate can be imported and used by the Connect Edge Gateway.

Note:

- The remote access certificate is used for the secure connection initiated from the external networks such as homes and hotspots. Mitel recommends use of FQDN rather than IP address for imported remote access certificates.
- An imported certificate must be in unencrypted Privacy Enhanced Mail (PEM) format and contain the X.509 certificate and the RSA key. Ensure that the certificate contains Beginning and End lines within the certificate file.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name of the Edge Gateway** from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **System** > **Certificate**.
5. Select **Edge Gateway**, **RAST**, **Reverse Proxy**, or **TURN** as needed.
6. Click **Import**. The Import Certificate page appears.
7. Paste the Certificate, Private Key, and Intermediate Certificate and root certificates received from the trusted certificate signing authority into the text box on the **Import**

Certificate page. Ensure to include both “BEGIN” and “END” statements for all information in the following order:

- Certificate
- RSA private key
- Any certificate chain/bundle that may have been included from the certificate authority

8. Click **Import**. A message appears.

   If the certificate is valid, a restart prompt displays. If the certificate is not valid, an error prompt displays. In the case of an error, generate a valid certificate or obtain a new certificate to paste in the field.
9. Restart the Connect Edge Gateway, activate the newly generated certificate, click **OK**. If you do not want to restart the Connect Edge Gateway, click **Cancel**. The newly generated certificate is stored on the Connect Edge Gateway until the next restart.
10. Refresh the browser to regain access, then log in.

Note:

Optionally, click **Verify** to view if the certificate is valid.

The system verifies whether the certificate is issued by genuine CA. If the certificate is signed by genuine CA, then verify succeeds. For self-signed certificates, as both, the issuer and presenter are same, verify succeeds.

5.4 Configuring the Connect Edge Gateway Network

This section describes how to configure network settings such as hostname and DNS, Ethernet interfaces, routing, and static hosts on the Connect Edge Gateway Administration Portal:

5.4.1 Secondary and Tertiary DNS

The Edge Gateway allows users to access the applications and/or the PBX on the corporate network regardless of whether they access it from the corporate network or from a location outside the corporate network. To facilitate the users’ seamless experience, you must specify secondary and tertiary DNS addresses to handle access requests from outside the corporate network.

5.4.2 Configuring Hostname and DNS

To access the administration portal, do the following:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Hostname/DNS**. The **Hostname/DNS** page appears.

   This page contains basic networking information about the Connect Edge Gateway. Most of this information is entered during the Initial Configuration Wizard and does not require changes.
5. Enter the appropriate values and click **Apply**.

The following table includes a list of reverse proxy parameters that is accessed when editing an existing Connect Edge Gateway.

Table 12: Hostname and DNS Parameters

Parameter	Description
Hostname	Verify that the Connect Edge Gateway hostname is the value specified in the Hos tname field during the Initial Configuration Wizard. You typically do not need to ch ange the hostname. The hostname can be up to 64 alphanumeric characters long and can contain hyphens (-). However, it cannot contain spaces or underscores (_).
Domain Name	Verify the domain name. This value defaults to the domain name provided during the Initial Configuration Wizard and does not require changes.
Primary DNS IP Address	Verify the primary DNS IP address. This value defaults to the IP address provided during the Initial Configuration Wizard.
Secondary DNS IP Address	Enter an IP address for a second DNS server.
Tertiary DNS IP Address	Enter an IP address for a third DNS server.

5.4.3 Configuring Ethernet Interfaces

Some information in the fields under the Interface menu reflects the responses provided during the Initial Configuration Wizard setup. Some fields are set to system defaults that generally do not require changes.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.

4. Select **Configuration** > **System** > **Networking** > **Interface**. The Interface page appears. By default, the **eth1** tab is selected.
5. Verify that the internet side connection is **Enabled**.

The following table includes a list of Ethernet interface parameters. Enter the appropriate value or verify the current setting and click **Apply**.

Table 13: Ethernet Interface Parameters

Parameter	Description
IP Address	• Use DHCP — If you entered **N** in response to the **Use DHCP on eth0 interface** prompt in the **Initial Configuration Wizard**, you can change **eth0** to **DHCP** by selecting this field and then selecting **Apply**. • Static — This field defaults to the IP address entered in the **Primary IP Address** field entered in the **Initial Configuration Wizard** and should not be changed.
Gateway	This value defaults to the IP address provided during the Initial Configuration Wizard and d oes not require changes.
Speed	The default and recommended value is **Auto**. To change the speed, select one of the following in the Speed list: • 10 Mbps • 100 Mbps • 1000 Mbps • Auto — Speed is auto-detected
Duplex	Select the duplex value. The default value is **Auto**. To change the duplex setting, select one of the following in the Duplex list: • Full — Full-duplex • Half — Half-duplex • Auto — Auto-detect duplex setting
MTU	Verify the Maximum Transmission Unit (MTU) value.
MAC Address	Verify the MAC address.
Status	Verify the Connect Edge Gateway online status.

5.4.4 Viewing RAST Settings

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **RAST** to view the Connect Edge Gateway RAST parameters. By default, the **General** tab is selected.
5. Ensure that the **Enable** check box is selected.
6. To save your changes, click **Apply**.

5.4.4.1 General Parameters

The following table includes a list of RAST General parameters:

Table 14: RAST General Parameters

Parameter	Description
Remote Access IP Interface	In the Remote Access IP Interface (read-only) list, select the Ethernet int erface used for remote access. By default, the eth1 interface is selected.
Tunnel Interface MTU	The range is from 576 to 9000. The default value is 1360.
Remote Client IP Lease Duration	The range is from 30 to 65535 minutes.The default value is 1440 minutes.

5.4.4.2 Protocol Parameters

The following tables includes a list of RAST Protocol parameters:

Table 15: RAST Protocol Parameters (Datagram / TLS UDP)

Parameter	Description
Datagram / TLS UDP	1. In the **Cipher** list, select one of the following: • NULL-MD5 — Uses no encryption (null cipher) and Message-Digest Algorithm 5 (MD5) for authentication. (This is the weakest cipher.) • AES128-SHA — Uses Advanced Encryption Standard (AES) with 128-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication. • AES256 - SHA—Uses Advanced Encryption Standard (AES) with 256-bit key as the encryption method and

Parameter	Description
	Secure Hash Algorithm (SHA) for authentication. (This is the strongest cipher.) **Note**: Although choosing the strongest cipher increases security, using the strongest cipher uses more resources on the mobile devices and Connect Edge Gateway. 2. Port — The port number can be between 80 and 49151. The default port number is 443. 3. MTU — The MTU can be a value from 576 to 1440.The default MTU value is 1376. 4. Keep Alive — The Keep Alive time can be value between 2 and 3600 seconds. The default value is 55 seconds. 5. Session Timeout— The amount of time that the client can be inactive before the session is disconnected. The timeout can be a value between 60 and 65535 seconds. The default timeout is 600 seconds. 6. Renegotiation Time — The amount of time that elapses before the encryption key is refreshed.The renegotiation time can be a value between 0 and 65535 minutes. Setting the time to 0 disables the refreshing of the encryption key. The default value is 0.

Table 16: RAST Protocol Parameters (TLS / TCP)

Parameter	Description
TLS / TCP	1. In the **Cipher** list, select one of the following: • NULL-MD5 — Uses no encryption (null cipher) and Message-Digest Algorithm 5 (MD5) as authentication. • RC4-MD5 — Uses a common algorithm created by RSA Security as the encryption method and Message-Digest Algorithm 5 (MD5) as authentication. • AES128-SHA — Uses Advanced Encryption Standard (AES) with 128-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication. • AES256-SHA — Uses Advanced Encryption Standard (AES) with 256-bit key as the encryption method and Secure Hash Algorithm (SHA) for authentication. (This is the strongest cipher.) **Note**: RC4-MD5 cipher suite is not supported by Connect Edge Gateway. 2. Port — The port number can be between 80 and 49151. The default port number is 443. 3. MTU — The MTU can be a value from 576 to 1500. The default MTU value is 1376. 4. Keep Alive — The Keep Alive time can be a value between 1 and 3600 seconds. The default value is 480 seconds. 5. Session Timeout — The amount of time that the client can be inactive before the session is disconnected. The timeout can be a value between 60 and 65535 seconds. The default timeout is 600 seconds. 6. Renegotiation Time — The amount of time that elapses before the encryption key is refreshed. The renegotiation time can be a value between 0 and 65535 minutes. Setting the time to 0 disables the refreshing of the encryption key. The default value is 0.

5.4.4.3 Client IP Pool Parameters

The following table includes a list of RAST Client IP Pool parameters (read-only). Refer to IP Pool Parameters for more configuration information using Connect Director.

Table 17: RAST Client IP Pool Parameters

Parameter	Description
Name	Name of the IP Pool.
Start IP Address	Starting IP Address for the RAST session.
End IP Address	Ending IP Address for the RAST session.

5.4.5 Viewing Routing Settings

View the default gateway or additional static routes.

5.4.5.1 Viewing Static Routes

The default gateway is automatically setup as a static route.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Routing**. The **Routing** page appears.

5.4.6 Managing Static Routes

The default gateway is automatically setup as a static route. You can optionally create additional static routes to send packets to specific IP addresses or a specific network.

5.4.6.1 Adding Static Routes

To add a Static Route:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Routing**.
5. Click **Add**. The **Add Route** page appears.

6. In the **IP Address** field, type the IP address for the static route.
7. In the list of subnet mask values, select the value of the subnet mask for the IP address.
8. In the **Gateway** field, type the IP address of the gateway for the route.
9. In the **Interface** list, select the Ethernet interface for the route.
10. To save your changes, click **Apply**.

5.4.6.2 Modifying Static Routes

To modify a Static Route:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Routing**. The **Routing** page appears.
5. Select the static route that you want to modify, and click **Modify**.
6. Make any necessary changes, and click **Apply**.

5.4.6.3 Deleting Static Routes

To delete a Static Route from the Routing list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Routing**. The **Routing** page appears.
5. Select the static route that you want to delete.
6. To select multiple contiguous items, hold the **Shift** key while selecting the items. To select multiple non-contiguous items, hold the **Ctrl** key while selecting the items.
7. Click **Delete**.
8. A confirmation message appears to delete the selected Routes, click **OK**.

The following table includes a list of Route parameters:

Table 18: Route Parameters

Parameter	Description
IP Address	IP address of the status route.

Parameter	Description
Gateway	IP address of the gateway for the route.
Interface	Ethernet interface for the route. Select one of the following: • eth0 • eth1

5.4.7 Viewing Static Hosts

View the static hosts defined for the most frequently used hosts, such as HQ server and switch. The IP address for the Connect Edge Gateway, which you provided as the primary IP address in the Initial Configuration Wizard, is automatically added as a static host.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Static Hosts**. The **Static Hosts** page appears.

5.4.8 Managing Static Hosts

Static Hosts can be added and deleted but cannot be modified.

5.4.8.1 Adding Static Hosts

To add a Static Hosts:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Static Hosts**. The **Static Hosts** page appears.
5. Click **Add**. The **Add Static Host** page appears.
6. In the **IP Address** field, type the IP address of the static host.
7. In the **Hostname** field, type a name for the static host.

> **Note**:
>
> The name can be up to 64 alphanumeric characters long and can contain hyphens (-) and underscores (_).

8. To save your changes, click **Apply**.

5.4.8.2 Deleting Static Hosts

To delete a Static Host from the Static Hosts list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **Static Hosts**. The **Static Hosts** page appears.
5. Select the static host that you want to delete.
6. To select multiple contiguous items, hold the **Shift** key while selecting the items. To select multiple non-contiguous items, hold the **Ctrl** key while selecting the items.
7. Click **Delete**.
8. A confirmation message appears to delete the selected static host, click **OK**.

The following table includes a list of static host parameters:

Table 19: Static Host Parameters

Parameter	Description
IP Address	IP address of the static host.
Hostname	Displays the name of the static host. The name can up to 64 alphanumeric characters long and can contain hyphens (-) and underscores (_).

5.4.9 Configuring SSH

Select SSH (Secure Shell) to enable the SSH service on a selected interface. SSH is enabled by default.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.

3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Networking** > **SSH**. The **SSH** page appears.
5. Select an **Interface**.

   The following table includes the SSH parameters:

Table 20: SSH Parameters

Parameter	Description
Interface	By default, the IP address associated with the primary interface is selected. This interface is used by the Connect Edge Gateway for communicating with the SSH server. SSH can be configured on any interface, but it is recommended to use eth0 for system security purpose. Valid interfaces are Any, eth0 and eth1. **Note**: SSH must not be enabled on eth1 (the Internet connection).

6. Click **Apply** to save your changes.

5.5 Configuring Logging and Monitoring Options

Use the logging options to record events on the Connect Edge Gateway. Logging option levels can be configured to report based on the level of information needed.

This section contains the following options:

- Configuring Email (Optional)
- Configuring Logging Settings
- Configuring SNMP

5.5.1 Configuring Email (Optional)

Use the Email page to specify an SMTP server, mail domain name, and individual email addresses that should receive notification of specific events on the Connect Edge Gateway.

5.5.1.1 Setting General Email Options

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Email**. The **Email** page appears and by default the **General**tab is selected.

   The following table includes the Email parameters:

   Table 21: Email Parameters

Parameter	Description
SMTP Server	The IP address or hostname of the SMTP server to which email notifications shou ld be sent.
Mail Domain Name	The domain name associated with the SMTP server.

5. Click **Apply** to save your changes.

5.5.1.2 Setting Auto Notification

To set automatic notification of events:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Email** > **Auto Notifications** tab.

5. Check the appropriate event boxes for which automatic notifications will be sent:
   - **Cluster Status Change Event:** A node has unexpectedly joined or left the cluster, or the number of nodes is unexpected.
   - **Link Status Change Event:** The interface link state changed.
   - **Process Crash Event:** A process in the system was detected as hung.
   - **Process Unexpected Exit Event:** A process in the system unexpectedly exited.
   - **High CPU Utilization Event:** CPU utilization has risen too high.
   - **High Disk I/O Utilization Event:** Disk I/O per second has risen too high.
   - **Low Free Disk Event:** File system free space has fallen too low.
   - **High Interface Utilization Event:** Network utilization has risen too high.
   - **Low Free Memory Event:** Memory usage has risen too high.
   - **High Memory Paging Event:** Paging activity has risen too high
   - **Unexpected Shutdown Event:** The system shut down unexpectedly.
   - **Login/Logout:** The system sends email notification to administrator with user name and IP address of the user who has logged in or out.
   - **Client Log upload Event:** Email notification with user's uploaded log and subject information.
   - **Scheduled Config Backup Event:** If a configured backup is scheduled, an email notification is send whenever this backup is performed.
6. Click **Apply** to save changes.

5.5.1.3 Managing Notification Recipients

Adding Notification Recipients

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Email** > **Notify Recipients** tab.
5. Click **Add**. The **Add Recipient** page appears.
6. In the **Email Address** field, type the email address of the person to receive notification. Select the appropriate check boxes to receive details or failure information. The following is a sample output for failure information:

Table 22: Failure Sample

Failure Type	Description
process-crash	A process in the system has crashed.

Failure Type	Description
unexpected-shutdown	The Connect Edge Gateway has unexpectedly shut down.

7. Click **Apply** to save your changes.

Modifying Notification Recipients

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Email** > **Notify Recipients** tab.
5. Select the recipient email address that you want to modify, and click **Modify**.
6. Make any necessary changes, and click **Apply**.

Deleting Notification Recipients

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Email** > **Notify Recipients** tab.
5. Select the recipient email address that you want to delete.
6. To select multiple contiguous items, hold the **Shift** key while selecting the items. To select multiple non-contiguous items, hold the **Ctrl** key while selecting the items.
7. Click **Delete**.
8. A confirmation message appears to delete the selected recipient email address, click **OK**.

The following table includes the Notify Recipients Parameters:

Table 23: Notify Recipients Parameters

Parameter	Description
Email Address	Indicates the email address of the person to receive notification.

5.5.2 Configuring Logging Settings

Use the **Logging** page to configure the settings to monitor events.

5.5.2.1 Configuring Module Settings

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Logging**. By default, the **Modules** tab is selected.
5. Specify the minimum level of events to be logged for each module. Select the level by choosing from the available list for each of the following modules:
   - Infrastructure
   - Configuration
   - RAST
   - Edge Gateway
6. Click **Apply** to save your changes.

See the following table for a list of event levels and their definitions.

Table 24: Filtering Levels for Logging Connect Edge Gateway Events

Severity Level	Description
debug	Provides low-level debugging messages. Generally, this logs only developer-targeted messages that contain more detailed information about the internal state of the system. Debug messages can be used for debugging problems where the INFO-level logs do not provide enough information. **Note**: Changing the logging level to debug can adversely affect Connect Edge Gateway performance.
info	Lists events that are expected to happen. These events are used to trace data flow and process activity.
notice	Indicates notification of a normal, expected event.
warning	Warning of a potential or mild error. Indicates that an unusual condition has been detected that might be cause for concern. Action should be taken to further diagnose (if necessary) and correct the problem.

Severity Level	Description
err	Indicates a minor error that might require operator intervention if it recurs. Investigatio n and corrective action should be taken to prevent a more serious (for example, serv ice-affecting) fault.
crit	Indicates that a service-affecting condition has developed and an urgent corrective act ion is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be re stored.
alert	Indicates a severe error condition that requires operator intervention. Critical parts of t he system are operational. However, either a less critical part of the system is nonfunc tional or the overall system is operating at a degraded capacity.
emerg	Indicates a service-affecting error condition that requires immediate attention. A critical part of the system is either not functioning correctly or failed.
fatal	Internal server error from which the server cannot recover and will terminate.
debug0	This is the first level of debugging and should be used for brief indications of actions or events. Usually those actions and events are either visible to customers oreasily explained. **Note**: Changing the logging level to debug0 can adversely affect Connect Edge Gateway performance.
debug1	A more detailed level of debugging. This can be used to provide more detailed information about events and actions that are usually not obvious to the customer. Details require a knowledgeable person to analyze them. **Note**: Changing the logging level to debug1 can adversely affect Connect Edge Gateway performance.
debug2	Reserved. Can be used for more debugging levels or to connect to third-party modules that have multiple debugging levels.

Severity Level	Description
	Note: Changing the logging level to debug2 can adversely affect Connect Edge Gateway performance.
debug3	Reserved. Can be used to view the summary logs of every packet received. **Note**: Changing the logging level to debug3 can adversely affect Connect Edge Gateway performance.
debug4	Reserved. Can be used to viewthe detailed logs of every packet. **Note**: Changing the logging level to debug4 can adversely affect Connect Edge Gateway performance.

The following table includes a list of Logging parameters:

Table 25: Logging Parameters

Parameter	Description
Infrastructure	Indicates the complete message log of the system.
Configuration	Indicates the Connect Edge Gateway configuration daemon logs.
RAST	Indicates the RAST configuration daemon logs.
Edge Gateway	Indicates the Edge Gateway configuration daemon logs.

5.5.2.2 Configuring Local Log Settings

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **Logging** > **Local Log** tab.
5. In the **Format** list, select the format for the local log files:
   - standard — Standard log format (text file)
   - welf — WebTrends Enhanced Log Format (WELF)
6. In the **Rotation** list, specify the frequency at which the log is rotated.
   - Every
     - Day: starting at 12:00:00 a.m.
     - Week: from Sunday 12:00:00 a.m. to Sat 11:59:59 p.m.
     - Month: from the 1st of each Month at 12:00:00 a.m. to the last day of the specific calendar month at 11:59:59 p.m.
     - When log reaches: The value can be between 1048576 and 1048711424 bytes.
   - When log reaches (thousandths of a percent of /var size): The value can be between 1 and 100000.
7. In the **Max log file to keep** field, type the maximum number of log files that are stored on the Connect Edge Gateway. The value can be between 1 and 4,294,967,295.
8. Click **Apply** to save your changes.

The following table includes a list of Local Log parameters:

Table 26: Local Log Parameters

Parameter	Description
Format	Indicates the format for the local log files. The following is the Format list: • standard: Standard log format (text file) • welf: WebTrends Enhanced Log Format (WELF)
Rotation	Indicates the frequency at which the log is rotated. The following is the Rotation list:

Parameter	Description
	1. Every • Day: starting at 12:00:00 a.m. • Week: from Sunday 12:00:00 a.m. to Sat 11:59:59 p.m. • Month: from the 1st of each Month at 12:00:00 a.m. to the last day of the specific calendar month at 11:59:59 p.m. 2. When log reaches: The value can be between 1048576 and 1048711424 bytes. 3. When log reaches (thousandths of a percent of /var size): The value can be between 1 and 100000.
Max log file to keep	Indicates the maximum number of log files that are stored on the Connect Edge G ateway. The value can be between 1 and 4,294,967,295.

5.5.2.3 Managing Syslog Servers

You can define syslog servers to archive the Connect Edge Gateway logs in a centralized location for auditing and reporting purposes.

Adding Syslog Servers

1. Click **Configuration** > **System** > **Logging/Monitoring** > **Logging** > **Syslog Servers** tab.
2. Click **Add**.
3. In the **Remote Address** field, type the IP address of the syslog server.
4. In the Minimum Severity field, select the minimum level of severity at which events are sent. See Filtering Levels for Logging Connect Edge Gateway Events for a list of severity levels and their definitions.
5. Click **Apply** to save your changes.

Modifying Syslog Servers

1. Click **Configuration** > **System** > **Logging/Monitoring** > **Logging** > **Syslog Servers** tab.
2. Select the Syslog Server that you want to modify, and click **Modify**.
3. Make any necessary changes, and click **Apply**.

Deleting Syslog Servers

1. Click **Configuration** > **System** > **Logging/Monitoring** > **Logging** > **Syslog Servers** tab.

2. Select the Syslog Server that you want to delete.
3. Select the Syslog Server that you want to delete.To select multiple contiguous items, hold the **Shift** key while selecting the items. To select multiple non-contiguous items, hold the **Ctrl** key while selecting the items.
4. Click **Delete**.
5. A confirmation message appears to delete the selected Syslog Server, click **OK**.

The table below includes a list of Add Logging Server parameters:

Table 27: Add Logging Server Parameters

Parameter	Description
Remote Address	Indicates the IP address of the syslog server.
Minimum Severity	Indicates the minimum level of severity at which events are sent. See Filtering Levels for Logging Connect Edge Gateway Events for a list of severity levels and their definiti ons.

5.5.3 Configuring SNMP

Use the SNMP page to enable SNMP on a selected interface and specify a community. SNMP is disabled by default. SNMP must only be enabled on the LAN interface, Eth0. Set the Community to value other than public for security reasons.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Logging/Monitoring** > **SNMP**.
5. Click **Enable**.
6. Select an **Interface**. By default, the IP address associated with the primary interface is selected.

   This interface is used by the Connect Edge Gateway for communicating with the SNMP server.
7. Specify a **Community**. Use community string other than public for security purpose.
8. Click **Apply**.

Table 28: SNMP Parameters

Parameter	Description
Interface	By default, the IP address associated with the primary interface is selected. This inte rface is used by the Connect Edge Gateway for communicating with the SNMP server.
Community	Indicates the community string defined for SNMP server. Use community string other than public for security purpose.

5.6 Setting the System Date and Time

You can manually set the system date and time for the Connect Edge Gateway, or configure it to use a Network Time Protocol (NTP) server to automatically set the system date and time. The system date and time are used to time stamp log messages, certificate time generation, licensing, and call detail records (CDRs).

5.6.1 Manually Setting the System Date and Time

NTP Servers must be disabled for manual settings to take effect. Refer to Enabling NTP for configuration information.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Date and Time** > **Manual**.

   The following table includes a list of manual time and date parameters:

   Table 29: Manual Time and Date Parameters

Parameter	Description
Time Zone	The time zone in which the Connect Edge Gateway is located.
Date	The current date in the format YYYY/MM /DD, where YYYY indicates the year, MM i ndicates the month, and DD indicates the day.
Time	The current time in the format HH:MM:SS, where HH indicates the hour, MM indica tes the minutes, and SS indicates the seconds. Specify the time using 24-hour clock format.

5. Click **Apply** and continue to the NTP Configuration page to disable NTP servers. Refer to Enabling NTP for information.

Note:

Optionally, click **Refresh** to get current server time and time zone.

5.6.2 Enabling NTP

If you configure the Connect Edge Gateway to get the system date and time from an NTP server, The Edge Gateway polls the specified NTP server at regular intervals and updates the system date and time so that they are synchronized with the server. By default, NTP is enabled. A default NTP server has already been defined. You can add other NTP servers.

Note:

If NTP is enabled, the Connect Edge Gateway reads the time from the NTP server, not the time set manually. The manual date and time settings are ignored.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Date and Time** > **NTP**.
5. Ensure that NTP is enabled. Select **Enable NTP** check box if this function has been previously disabled.
6. Click **Apply**.

5.6.2.1 Adding NTP Servers

If you do not want to use the default NTP server that is defined, you can add NTP servers. If you add multiple NTP servers, the Connect Edge Gateway contacts the first NTP server listed alphabetically. If that server is unavailable, the Connect Edge Gateway uses the alphabetical list of NTP servers to contact subsequent servers until a connection is made.

To add an NTP server:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Date and Time** > **NTP**. The **NTP** page appears.
5. To add a new NTP server, click **Add**. The **Add NTP Server** page appears.
6. Make any necessary changes, and click **Apply**. In the **Server** field, type the fully qualified domain name or IP address of the NTP server. The name or IP address can

be up to 64 alphanumeric characters. No special characters except periods (.) are allowed.

7. In the Version list, choose the version of NTP to be used:
   - Version 4 (default value)
   - Version 3
8. Select **Enabled** to activate the NTP server. If you want to use this server as an NTP server, ensure you select this check box in addition to enabling NTP, as described in Enabling NTP.
9. Click **Apply**.

5.6.2.2 Modifying NTP Servers

To modify an NTP server:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Date and Time** > **NTP**. The **NTP** page appears.
5. Select the NTP server that you want to modify, click **Modify**.
6. Make any necessary changes, and click **Apply**.

5.6.2.3 Deleting NTP Servers

To delete an NTP server:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Configuration** > **System** > **Date and Time** > **NTP**. The **NTP** page appears.
5. Select the NTP server that you want to delete.
6. To select multiple contiguous items, hold the **Shift** key while selecting the items. To select multiple non-contiguous items, hold the **Ctrl** key while selecting the items.
7. Click **Delete**.
8. A confirmation message appears to delete the selected recipient email address, click **OK**.

The following table includes a list of NTP parameters:

Table 30: NTP Parameters

Parameter	Description
Server	Indicates the fully qualified domain name or IP address of the NTP server. The name or IP address can be up to 64 alphanumeric characters. No special characters except per iods (.) are allowed.
Version	Indicates the version of NTP to be used. 4 is the default.

5.7 Connect Edge Gateway Licensing

The Connect Edge Gateway has two associated licenses in Connect Director— vEdgeGW License and Remote Phone License. One vEdgeGW license is required for each virtual appliance to enable and use the virtual appliance. The remote phone license enables remote phones, remote softphone, or Conferencing for the Web. One remote phone license is included in each MiVoice Connect standard license bundle. Additional licenses can be purchased separately for each softphone to use Conferencing for the Web.

Reverse proxies on the Edge Gateway are accessible without a remote phone license. You can use Contact Center MiVoice Connect Client and Connect Client without remote phone licenses.

Remote phone license is required for the following scenarios:

- For using IP400 series phone.
- For using softphone in the Connect Client remotely.
- To join a conference using the softphone built into the Conferencing for the Web.

Connect Director tracks and enforces the number of remote phone licenses installed in the system. When users enable for remote phone authentication, it automatically uses a license. All other remaining licenses in the system are available to guests using Conferencing for the Web. For example, if 100 remote phone licenses are available in the Connect Director and 75 users are enabled for remote phone authentication, other 25 users can access Conferencing for the Web using the softphone. Any additional guests joining the conference have to dial-in through the standard dial-in process.

Configuring Connect Edge Gateway Phones

6

This chapter describes how to configure the Connect Edge Gateway phones.The topics discussed include:

Allowed, Pending, and Blocked Lists

This section includes information about how the Edge Gateway handles 400-series IP phones connecting remotely.

- Allowed — When you provision the phone for the first time, the phone gets added to the allowed list when the remote phone authentication is enabled and the correct extension and voice mail PIN are entered.
- Pending — When you provision the phone for the first time, the phone gets added to the pending list when the remote phone authentication is not enabled or you have entered the incorrect extension, or you have entered the incorrect voice mail PIN more than three times.
- Blocked — When you provision the phone for the first time, the phone gets added to the blocked list when the remote phone authentication is not enabled or you have entered the incorrect extension and voice mail PIN more than three times. The phone gets moved from pending list to blocked list.

  When a phone is in the blocked list, an administrator must delete the phone from the blocked list to enable the phone to access the Edge Gateway.

6.1 General

The General page displays the Config Server address and NTP Server address. The Connect Edge Gateway sends this information in RAST Session Start Response message.

A maximum of 6 Config servers can be configured. The phone connects and downloads the configuration details from the Config server. The NTP server address is taken from the NTP Sites configuration page. The phone syncs its time from the NTP server.

Note:

IP 400-Series phones must be using firmware version 802.84x.xxxx.0 or later to work with the Edge Gateway.

To view the configuration details:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **General**.

6.2 Configuring the Allowed List

If a phone is provisioned by an authenticated user (who has entered a valid extension and voice mail PIN, and has remote phone authentication privileges), then the phone gets added to the allowed list automatically. The next time the phone tries to connect, it gets connected without any authentication. The allowed list contains the MAC Address, Phone Name, and User ID of the allowed phones.

6.2.1 Adding Phones to the Allowed List

To add a phone to the allowed list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Click **Add**. The **Add an Allowed Phone** page displays.
6. Enter the **MAC Address**, **Phone Name**, and **User ID** of the phone that you want to add to the allowed list.

   The User ID is the extension number of the provisioning user. The extension number entered on the phone is displayed in the Allowed list.
7. Click **Apply**.

The following table includes a list of allowed list parameters:

Table 31: Allowed List Parameters

Parameter	Description
MAC Address	Indicates the MAC Address of the phone that you want to add to the allowed list.
Phone Name	Indicates the Phone Name of the phone that you want to add to the allowed list.
User ID	Indicates the User ID of the phone that you want to add to the allowed list. The User I D is the extension number of the provisioning user.

6.2.2 Moving Phones to the Blocked List

To move a phone from the allowed list to the blocked list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to move to the blocked list.
6. Click **Move to Blocked List**.
7. Click **Apply**.

Note:

Phones that are moved to the blocked list cannot connect again as long as their MAC addresses are in the blocked list.

6.2.3 Modifying the Allowed List

To edit the MAC Address, Phone Name, and User ID of the phone in the allowed list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to modify. Click **Modify**.
6. Edit the **MAC Address**, **Phone Name**, and **User ID** of the phone.
7. Click **Apply**.

6.2.4 Deleting Phones from the Allowed List

To delete a phone from the allowed list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to delete from the allowed list.
6. Click **Delete**.

6.3 Managing the Pending List

Pending list contains the list of phones that failed to connect, but has not exceeded the maximum login attempts. Each request shows the MAC address, Phone Name, and User ID. The pending list has temporary entries of phones waiting for administrator's action. These are the phones that tried to connect through the Connect Edge Gateway, but the provisioning user did not have a valid extension and a voice mail PIN, and/or did not have a remote phone authentication privilege.

Administrator can move the phone to the allowed list, blocked list, or delete it from the pending list.

6.3.1 Moving Phones to the Allowed List

To move a phone from the pending list to the allowed list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Pending List**.
5. Select the phone that you want to move to the allowed list.
6. Click **Move to Allowed List**.
7. Click **Apply**.

6.3.2 Moving Phones to the Blocked List

To move a phone from the allowed list to the blocked list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to move to the blocked list.
6. Click **Move to Blocked List**.
7. Click **Apply**.

Note:

Phones that are moved to the blocked list cannot connect again as long as their MAC addresses are in the blocked list.

6.3.3 Modifying the Pending List

To edit the MAC Address, Phone Name, and User ID of the phone in the pending list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to modify. Click **Modify**.
6. Edit the **MAC Address**, **Phone Name**, and **User ID** of the phone.
7. Click **Apply**.

6.3.4 Deleting Phones from the Pending List

To delete a phone from the pending list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Pending List**.
5. Select the phone that you want to delete from the pending list.

6. Click **Delete**.

6.4 Managing the Blocked List

The blocked list contains the list of phones that are blocked by the administrator, or got added to this list after maximum failed authentication attempts. The phones that are in the blocked list cannot connect again as long as their MAC addresses are in the blocked list. The blocked list contains the MAC Address, Phone Name, and User ID of the blocked phones.

6.4.1 Moving Phones to the Allowed List

To move a phone from the blocked list to the allowed list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Blocked List**.
5. Select the phone that you want to move to the allowed list.
6. Click **Move to Allowed List**.
7. Click **Apply**.

6.4.2 Modifying the Blocked List

To edit the MAC Address, Phone Name, and User ID of the phone in the blocked list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Allowed List**.
5. Select the phone that you want to modify. Click **Modify**.
6. Edit the **MAC Address**, **Phone Name**, and **User ID** of the phone.
7. Click **Apply**.

6.4.3 Deleting Phones from the Blocked List

To delete a phone from the blocked list:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Configuration** > **Phones** > **Blocked List**.
5. Select the phone that you want to delete from the blocked list.
6. Click **Delete**.

6.5 Configuring Remote Phones for Edge Gateway

Voice codecs convert an analog voice signal to digital form. The choice of codec can affect sound quality, bandwidth, and the computational resources.

Connect comes with an expanded list of audio codecs.The Connect Edge Gateway configuration allows additional control over remote phone codecs.

By default, MiVoice Connect selects “Low Bandwidth Codecs” as the codecs list for remote phones to use. This list includes iLBC, G729, BV32, and so on.

However, if higher bandwidth is available, and you want to choose codecs that improve voice quality, you can change the remote phone codecs list.

1. Launch Connect Director.
2. Click **Administration** > **Features** > **Call Control** > **Codec Lists**.

   Select the required Codec Lists from the available options. It is recommended to select Low Bandwidth Codecs, Medium Bandwidth Codecs, or High Bandwidth Codecs.
3. Click **Administration** > **Features** > **Call Control** > **Options**.

   In the Voice encoding and quality of service area, from the Remote IP phone codec list dropdown list, select the codecs list that you chose in Step 2.
4. Click **Administration** > **Appliances/Servers** > **Edge Gateway** > **RAST** > **IP Pool**.

Define IP pools for RAST phones as necessary.

The MiVoice Connect system automatically assigns new remote IP phones to the same site where the Edge Gateway is located. The assigned remote phone automatically gets the codec list configured for the remote phones. You need not create a separate IP Phone Address Map for the remote phones.

6.6 Configuring VPN Access on 400-Series Phones

To configure Virtual Private Network (VPN) access on IP 400-Series phone that is connected through the Connect Edge Gateway, do one of the following:

- If the phone prompts to enter the MiCloud credentials, do the following:

  1. On the phone's keypad, press the **MUTE** button and dial the numbers corresponding to **SETUP#** (73887#).
  2. Enter the Administrator password. The default Administrator password is 1234.
  3. Scroll to **VPN** and press the **Open** soft key.
  4. With the **Use VPN field** highlighted, press the **Toggle** soft key to change the setting to **On**.
  5. In the **VPN gateway** field, enter the IP address or Fully Qualified Domain Name (FQDN) of the Edge Gateway appliance.
  6. Press the **Back** soft key.
  7. Scroll to **Services** and press the **Open** soft key.
  8. Scroll to **Config Server** and press the **Edit** soft key.
  9. In the **Config Server 1** field, enter the IP address of the Headquarters server.
  10. Press and hold the **Back** soft key.

- If you want to clear the phone configuration and restart the setup procedure before the phone prompts to enter the MiCloud credentials, do the following:

  1. On the phone's keypad, press the **MUTE** button and dial the numbers corresponding to **CLEAR#** (25327#).
  2. Press the **Clear**soft key. The phone resets and begins the normal startup sequence.

     During the startup sequence, the phone pauses and displays **Press any key to enter setup**.
  3. Press any key to enter the setup mode.
  4. Enter the Administrator password. The default Administrator password is 1234.
  5. Scroll to **VPN** and press the **Open** soft key.
  6. With the **Use VPN** field highlighted, press the **Toggle** soft key to change the setting to **On**.
  7. In the **VPN gateway** field, enter the IP address or Fully Qualified Domain Name (FQDN) of the Edge Gateway appliance.
  8. Press the **Back** soft key.

6.6.1 Configuring the Time Zone on 400-Series Phones

To configure the time zone on IP 400-Series phone that is connected through the Connect Edge Gateway, do the following:

1. On the phone's keypad, press the **Options** soft key.
2. Enter the voicemail password.
3. Scroll to **Time Zone** and press the **Edit** soft key to select the correct time zone.
4. Press the **OK** soft key.
5. Press the **Exit** soft key.

Maintaining the Connect Edge Gateway

7

Use Connect Director or the Connect Edge Gateway administration portal to reboot, restart, shut down, and restore the factory-default settings of the Connect Edge Gateway. It is recommended to use Connect Director first, and then use the Connect Edge Gateway administration portal for advanced options.

7.1 Backing up the Connect Edge Gateway

The Connect Edge Gateway configuration can be backed up to an FTP, SCP (for secure EGW backup), or TFTP server by using the On Demand method or by scheduling a backup.

Note:

To restore a configuration, refer to Restoring the Connect Edge Gateway Configuration.

7.1.1 On Demand Backup

To perform on demand back up of the Connect Edge Gateway (EGW) configuration:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.

4. Select **Maintenance** > **On Demand Backup**. The **On Demand Backup** page appears.
5. Enter the **Hostname** or **IP Address** of the location to send the configuration file.
6. Select the **Protocol** to send the file: TFTP, FTP or SCP (for secure EGW backup).
7. Enter the **Port** number.
8. Enter the **User ID**. The entry must match the User ID for the selected server (TFTP/ FTP/SCP [for secure EGW backup]).
9. Enter the **Password** for the User.
10. In the **Path** field, type the path to the directory and the filename to which you want to save the configuration file, for example, `/home/user/backup/test.bakthe Port number`.

Note:

The FTP or TFTP server must be running for the backup to succeed.

Note:

/var/tmp should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

11. Click **Backup**. The Connect Edge Gateway displays a status prompt indicating the backup is in progress. If the backup is successful, the **Backup Succeeded** message displays. If the backup fails, the **Backup failed. See server log** message displays.

The following table includes a list of on demand parameters for the Connect Edge Gateway:

Table 32: On Demand Backup Parameters

Parameter	Description
Hostname or IP Address	Location to send the configuration file.
Protocol	Protocol to send the file: TFTP, FTP or SCP.
Port	Port number.
User ID	Entry must match the User ID for the selected server (FTP/SCP/TFTP)
Password	Password for the user.

Parameter	Description
Path	Path to the directory and the filename to which you want to save the configuration file, for example, /home/user/backup/test.bak

7.1.2 Scheduled Backup

To schedule a back up of the Connect Edge Gateway configuration:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **Scheduled Backup**. The **Schedules** tab displays any previous scheduled backup yet to be performed. The **History** tabs display previously performed backups.
5. To add a new scheduled backup, click **Add** on the **Schedules** tab.
6. On the **Add Schedule** page, enter a **Name** for the backup. This name displays on the Connect Edge Gateway's **Schedules** and **History** pages.
7. Enter a **Description**.
8. Select the frequency at which the backup occurs as follows:

    a. **Daily:** Select the Hour in 24 hour increments.
    b. **Weekly:** Select the Day of the week and the Hour in 24 hour increments.
    c. **Monthly:** Select the Date and the Hour in 24 hour increments.
9. Enter the **Hostname** or **IP Address** of the location to send the configuration file.
10. Select the Protocol to send the file: **FTP**, **SCP** or **TFTP**. Depending upon the type of protocol, for example, FTP or SCP, enter the relevant information such as Port number, User ID and Password.
11. Enter the **Port number**.
12. Enter the **User ID**. The entry must match the User ID for the selected server (TFTP/FTP/SCP).
13. Enter the **Password** for the User.
14. In the **Path** field, type the path to the directory to which you want to save the configuration file, for example, `/home/user/backup//test.bak`.

Note:

The FTP or TFTP server must be running for the backup to succeed.

Note:

/var/tmp should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

15. Enter the **Filename Prefix**. This is the name of the file as it displays at the backup location. This name is prefixed to the default file name which includes the Connect Edge Gateway name, the date of the backup, and the time of the backup in the form “[filename prefix]-[hostname]- [YYYYMMDD]-[HHMMSS].bak”. For example, if “test” is the Filename Prefix, the results display “test-egw-20110826-103000.bak”.
16. To save your changes, click **Apply**. The **Scheduled Backup** page appears.

Note:

Optionally, click **Verify** to verify the scheduled backup configuration is correct.

17. To execute the Scheduled Backup, click **Execute**.

The following table includes a list of scheduled backup parameters for the Connect Edge Gateway:

Table 33: Scheduled Backup Parameters

Parameter	Description
Name	Name displays on the Connect Edge Gateway’s Schedules and History pages.
Description	Description of the backup.
Frequency	• **Daily:** Select the **Hour** in 24 hour increments. • **Weekly:** Select the **Day** of the week and the Hour in 24 hour increments.

Parameter	Description
	• **Monthly:** Select the **Date** and the Hour in 24 hour increments.
Hostname or IP Addr ess	The location to send the configuration file to.
Protocol	Protocol to send the file.
Port	Port number.
User ID	Entry must match the User ID for the selected server (FTP/SCP/TFTP).
Password	Password for the user.
Path	Path to the directory and the filename to which you want to save the configuration file, for example, /home/user/backup/test.bak
Filename Prefix	Name of the file as it displays at the backup location. This name is prefixed to the defaul t file name which includes the Connect Edge Gateway name, the date of the backup, and the time of the backup in the form [filename prefix]-[hostname]-[YYYYMMDD]-[HHMMSS].bak. For example, if test is the Filename Prefix, the results display test-egw-2011082 6-103000.bak

7.2 Restoring the Connect Edge Gateway Configuration

If you need to roll back to a previous Connect Edge Gateway configuration file, you can restore the previous configuration. You can restore a configuration file only if it has been saved and uploaded to a TFTP, FTP, or SCP server.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **Restore**. The **Restore** page appears.
5. Enter the **Hostname** or **IP Address** or name of the server where the configuration file is stored.
6. Select the **Protocol** to send the file. Depending upon the type of protocol, for example, FTP or SCP, enter the relevant information such as ` **Port**, **User ID**, and **Password**.
7. In the **Path** field, type the path to the directory to which you want to save the configuration file, for example, `/home/user/backup//test.bak`.

Note:

The FTP or TFTP server must be running for the backup to succeed.

Note:

/var/tmp should not be used in the local host machine for backups. This is a temporary folder and the file is susceptible to being deleted. Use an external host to complete the backup.

8. Select **Include Network Information**, and/or **Include Certificates** as appropriate.
9. Click **Restore**. A confirmation message appears to restore the previous configuration, click **OK**. Status about the restore process appears.

   If the restore is successful, the **Configuration is restored. You need to restart your browser.** message displays. If the restore fails, the **Restore failed. See server log.** message displays.
10. Exit and restart the browser.
11. Log in to the Connect Edge Gateway admin portal by entering the Admin login and password.

The following table includes a list of restore parameters for the Connect Edge Gateway.

Table 34: Restore Parameters

Parameter	Description
Hostname or IP Address	IP address or name of the server where the configuration file is stored.
Protocol	Protocol to send the file. Depending upon the type of protocol, for example,FTP or SCP, enter the relevant information such as Port, User ID, and Password.
User ID	Entry must match the User ID for the selected server (FTP/SCP/TFTP).
Password	Password for the user.
Path	Path to the directory and the filename to which you want to save the configuration file , for example, /home/user/backup/test.bak
Filename Prefix	Name of the file as it displays at the backup location. This name is prefixed to the de fault file name which includes the Connect Edge Gateway name, the date of the ba ckup and time of the backup in the form [filename prefix]-[hostname]-[YYYYMMDD]-[HHMMSS].bak. For example, if test is the Filename Prefix, the results display test-egw-20110826-103000.bak

7.3 Restoring Factory-Default Settings

If necessary, you can restore the Connect Edge Gateway to its default settings. If you restore to default settings, all settings but the following is reset to default values:

- Connect Edge Gateway IP address
- Default gateway

- Domain name

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **System** > **Factory Defaults**.
5. Click **Revert**.
6. Click **OK** to confirm setting the Connect Edge Gateway to the factory-default configuration. You are logged out.
7. Exit and restart the Web browser. Log in as administrator to the Connect Edge Gateway admin portal by entering the Admin login and password.

7.4 Restarting Connect Edge Gateway Services

You can restart the services on the Connect Edge Gateway if there are issues with calls on devices, yet nothing appears to be wrong with the Connect Edge Gateway configuration or the devices.

If you restart the Connect Edge Gateway, active calls might be dropped.

To restart the Connect Edge Gateway using Connect Director:

1. Launch Connect Director.
2. Select **Maintenance** > **Status** > **Appliances**.
3. Select **Connect Edge Gateway** from the **Appliances** list.
4. Select **Restart** from the **Command** drop-down list.
5. Click **Apply** to confirm the restart.
6. At the confirmation prompt, click **OK**.

To restart the Connect Edge Gateway:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Maintenance** > **Restart/Reboot/Shutdown**.
5. Click **Restart Services**.
6. At the confirmation prompt, click **OK**.
7. Access a Web browser and log in to re-authenticate to the Connect Edge Gateway.

7.5 Rebooting the Connect Edge Gateway

You can reboot the Connect Edge Gateway to restart the entire system. An example of when you might need to reboot is if you have problems connecting to the network interfaces.

If you reboot the Connect Edge Gateway, active calls might be dropped.

To reboot the Connect Edge Gateway using Connect Director:

1. Launch Connect Director.
2. Select **Maintenance** > **Status** > **Appliances**.
3. Select **Connect Edge Gateway** from the **Appliances** list.
4. Select **Reboot** from the **Command** drop-down list.
5. Click **Apply** to confirm the restart.
6. At the confirmation prompt, click **OK**.

   The Connect Edge Gateway immediately reboots, and you are immediately logged out.

To reboot the Connect Edge Gateway:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Maintenance** > **Restart/Reboot/Shutdown**.
5. Click **Reboot Services**.
6. At the confirmation prompt, click **OK**.
7. Access a Web browser and log in to re-authenticate to the Connect Edge Gateway.

7.6 Shutting Down the Connect Edge Gateway

You can shut down and power off the Connect Edge Gateway. All active connections are disconnected and initiation of new connections are not possible during and after the Connect Edge Gateway is shut down.

Note:

To restore services after you shut down the Connect Edge Gateway, you must manually power on from logging into VMware vSPhere Client.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Maintenance** > **Restart/Reboot/Shutdown**.
5. Select **Connect Edge Gateway** from the list of devices.
6. Click **Shutdown**.
7. Click **OK** to confirm the shutdown. You are immediately logged out, and the Connect Edge Gateway shuts down.

To restore services after you shut down the Connect Edge Gateway,you must manually power on the vEdgeGW from VMware vSphere Client.

7.7 Starting and Stopping Connect Edge Gateway Services

Note:

Do not restart any Connect Edge Gateway service unless directed to do so by Technical Support.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Maintenance** > **Start/Stop Services**. On the **Start/Stop Services** page, the services and status (running or stopped) are listed. Next to the service status are **Start** and **Stop** buttons, which you can use to start and stop a service, respectively.

5. Find the service that you want to change, and do one of the following:
   - Click **Start** to start the service. At the confirmation prompt, click **OK**.
   - Click **Stop** to stop the service. At the confirmation prompt, click **OK**.
6. Repeat step 5 for each service that you need to start or stop.
7. Click **Refresh**. The Start/Stop Services is refreshed.

7.8 Managing Connect Edge Gateway Images

Note:

You can install an image from Connect Edge Gateway administration portal or Connect Director. However, it is recommended to install using Connect Director.

The Connect Edge Gateway contains two hard-drive partitions with factory-default system image installed on each partition.

The Connect Edge Gateway Images page provides information about Connect Edge Gateway images that have already been installed and options to upload a new Connect Edge Gateway image from an URL or a local file.

7.8.1 Reviewing Installed Images

To review installed Connect Edge Gateway images, select **Maintenance** > **Images** > **Edge Gateway**. The page lists the following:

- Edge Gateway images installed.
- Partition on which each image is installed (partitions 1 and 2).
- Which image is currently active (selected check box in Active column).
- Which image will be used at the next reboot of the Edge Gateway (selected check box in the Next Boot column).

7.8.2 Uploading and Installing Connect Edge Gateway Images

You can install Connect Edge Gateway images from a local file system or using HTTP, SCP, or FTP.

Note:
You can start using the administration portal only after the installation of Connect Edge Gateway images.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Maintenance** > **Images** > **Edge Gateway**.
5. Do one of the following:
   - **Select From URL** — Type the hostname, select the protocol, and enter the path of the server on which the Connect Edge Gateway image is installed. If using FTP or SCP, a User ID is required. If using FTP, the FTP server must be running for the upload to succeed.
   - **Select From local file** — Select to install the Connect Edge Gateway image from a local file system or click Browse to navigate the file system. Navigate to and select the Connect Edge Gateway image (*.img), and click **Open**.
6. Click **Install**. The image is uploaded to the Connect Edge Gateway.

7.8.3 Changing Connect Edge Gateway Image

After installing an image, you can specify that it can be used at the next reboot:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Click **Maintenance** > **Images** > **Edge Gateway**. In the list of installed images, select the image to be used at the next Connect Edge Gateway reboot.
5. Click **Set Next Boot**. The next time the Connect Edge Gateway is rebooted, the image selected becomes the active image.
6. Click **Reboot**. At the confirmation prompt, click **OK**. You are logged out, and the Connect Edge Gateway is restarted.
7. Log in after the Connect Edge Gateway restarts. The system software image for the Connect Edge Gateway is updated.

7.9 Migrating EG from VMware to Microsoft Hyper-V

This section describes how to migrate your existing Edge Gateway virtual machine from VMware infrastructure to Microsoft Hyper-V environment.

7.9.1 Backing up Edge Gateway on VMware Infrastructure

Procedure to back up Edge Gateway:

1. Log in to Edge Gateway with the administrator access.
2. Click **Maintenance** > **System** > **On Demand Backup**.
3. On the **On Demand Backup** page, do the following:

    a. Enter **Hostname** or the **IP Address** of the location to which you want to send the configured file.
    b. Select **scp** as the protocol and **22** as the port number.
    c. Enter the **User ID** and the **Password** that match the Hostname credentials.
    d. In the **path** field, enter the path to the directory and the file name you want to save the configuration file, as shown in the following example:

    You can enter `/home/admin/backup/sample.bak`.

    e. Click **Backup**. The status of the Edge Gateway backup is displayed. A notification appears when the backup is complete.
4. Log in to the Edge Gateway host that you have created.

For the successful completion of the backup procedure, ensure that the backup files are created in the specified location.

7.9.2 Restoring Edge Gateway on Hyper-V

1. Create a new virtual machine in the Microsoft Hyper-V infrastructure for Edge Gateway similar to that of VMware infrastructure. Make sure the ISO file, and the network configuration are the same as in the backup procedure.
2. Log in to Edge Gateway by using the admin credentials.
3. Click **Maintenance** > **System** > **Restore**.

4. On the **Restore** page, do the following:

   a. Enter **Hostname** or the **IP Address** of the location to which you want to send the configured file.
   b. Select **scp** as the protocol and type 22 as the port number.
   c. Enter the **User ID** and **Password** that match the Hostname credentials.
   d. In the **path** field, enter the path to the directory and the file name from which you want to retrieve the file as shown in the following example:

      You can enter **/home/admin/backup/sample.bak**.
   e. Enable the following:

      - Include License
      - Include Network Information
      - Include Certificates
   f. Click **Restore**. The status of the Edge Gateway restore is displayed. A notification appears when the backup is complete.

   > **Note**:
   >
   > When you click **Restore**, and the page stops responding, restart the appliance and open Edge Gateway on a new browser tab.

5. Click **Exit** and restart the browser.
6. Log in to Edge Gateway by using the admin credentials.

For the successful completion of the restore procedure, ensure that the backup files are restored in the specified location.

Monitoring the Connect Edge Gateway 8

You can monitor the status and usage of the Connect Edge Gateway by using reports. Historical data and real-time reports are available.

8.1 Monitoring the Connect Edge Gateway

Monitoring the Status Using Connect Director

Follow these steps to monitor the status of the Connect Edge Gateway using Connect Director:

1. Launch Connect Director.
2. Select **Maintenance** > **Status and Maintenance** > **Appliances**. The **Appliances** page opens.
3. Select **Connect Edge Gateway** from the Appliances list.

Status Parameters lists the status parameters

Table 35: Status Parameters

Status Parameter	Details Description
Last Boot Time	The last time the Connect Edge Gateway was booted.
Connect Time	The most recent time that the connection was reestab lished with the Connect Edge Gateway.
Platform Version	The version number of the platform for the Connect E dge Gateway.
CPU Usage	The current CPU utilization (by percentage) for the Conn ect Edge Gateway.
Memory Usage	The current memory utilization (by percentage) for the C onnect Edge Gateway.
Number of CPU Cores	The number of CPU cores configured for the Connect E dge Gateway.
CPU Speed	The CPU speed of the Connect Edge Gateway

8.1.1 Monitoring the Performance

You can monitor the Connect Edge Gateway performance based on a daily or hourly usage.The **Performance** tab includes the following chart:

- **Platform Resources** — The Platform Resources chart shows the CPU and memory usage trend for the selected Connect Edge Gateway for the selected time period.

8.2 Monitoring the Status Using Connect Edge Gateway

When you first log in to the Connect Edge Gateway as an administrator, the Dashboard is shown. Use the Dashboard to quickly get an overview of activity.

To access the Dashboard from another area of the Connect Edge Gateway.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Monitor** > **Dashboard**. The **System Status** page appears.

   The Dashboard includes the following information:

   - System Status — The System Status shows the hostname and model number of the Connect Edge Gateway. Also, provides information about the CPU and memory utilization, percent of free memory, and system uptime. This page is updated every two minutes.

8.3 Monitoring Phones

Active Phones

You review the status of the active phones on the Connect Edge Gateway.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Monitor** > **Phones** > **Active Phones**. The **Active Phones** page appears.

5. The active phones can be searched based on multiple criteria. In the **Active Phones** drop-down window, select the means to find the Active Phones. The options are **User ID**, **MAC Address**, **Session ID**, **LAN local IP**, **Protocol**, or **Established**.
6. Select the criteria to find the active phones. The options are **equal to** or **contains**.
7. Type the appropriate string in the **search** field and click **Find**. All rows containing the configured criteria display in the table.
8. The current page number displays at the bottom-right. Select a new page number to begin with and the number of rows to follow using the Go to page field and the Retrieve pulldown on the bottom-right. The valid values are 50, 100 and 500. For example, enter Go to row 101 and select Retrieve 50 to begin sorting the rows on number 101 and end on number 151.
9. Select **Prev** or **Next** to view the pages before or after the current page.
10. Click **Refresh** to return to the original table.
11. To delete the active phones, select the phone, and click **Delete**.
12. Click the **Ping** to check the reachability of a host and network connectivity.

The following table lists the interface information.

Table 36: Active Phones Parameters

Parameters	Description
MAC Address	Indicates the MAC address of the Active Phones.
Phone Model	Indicates the Phone Model type.
Last Assigned	Indicates the Last Assigned.
Session ID	Indicates the Session identification number.
LAN IP	IP address of the mobile device (assigned from the clie nt IP pool).
Tunnel	Indicates the Tunnel.
Remote Public	Indicates the Remote Public.
Protocol	Indicates the security protocol used for the remote ses sion.
Established	Indicates the Date and time when the remote session was established.
Rx Packets	Indicates the number of packets received by the mobile device.
Tx Packets	Indicates the number of packets transmitted by the mobi le device.
Rx Bytes	Indicates the number of bytes received by the mobile de vice.
Tx Bytes	Indicates the number of bytes transmitted by the mobile device.

8.4 Monitoring the System

Interfaces shows type of usage report available for the Connect Edge Gateway.

8.4.1 Interfaces

You review the status of the eth0, eth1, and loopback (lo) interfaces on the Connect Edge Gateway.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Monitor** > **System** > **Interfaces**.

The following table lists the interface information:

Table 37: Interface Information

Column Title	Description
Name	Interface name.
IP Address	Interface IP address.
MAC Address	Interface MAC address (Ethernet interfaces only).
Speed	Interface speed (Ethernet interfaces only).
Admin Up	Indicates whether the interface can be administered.
Link Up	Indicates whether the network link is up.

Troubleshooting the Connect Edge Gateway

9

Connect Edge Gateway logs are available to assist in troubleshooting.

9.1 Running Network Troubleshooting Commands

Run the following network troubleshooting commands:

- ping (See Running ping)
- traceroute (See Running traceroute)
- nslookup (See Running nslookup)
- netstat (See Running netstat)

9.1.1 Running ping

Run the `ping` command to check the reachability of a host and network connectivity. The ping command sends Internet Control Message Protocol (ICMP) echo request messages to the host and listens for ICMP echo response messages from the host.

To run the `ping` command:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Commands**.
5. In the **Command** drop-down list, select **ping**.
6. In the **Interface** drop-down list, select **eth0** or **eth1**.
7. In the **Host** field, type the IP address or name of the device that you are trying to ping.

8. Click **Apply**. The ping output displays.

   The following is an example of ping output:

```
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

64 bytes from 192.168.1.10: icmp_seq=1 ttl=63 time=0.319 ms

64 bytes from 192.168.1.10: icmp_seq=3 ttl=63 time=0.311 ms

64 bytes from 192.168.1.10: icmp_seq=4 ttl=63 time=0.208 ms

64 bytes from 192.168.1.10: icmp_seq=5 ttl=63 time=0.355 ms

--- 192.168.1.10 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4001ms

rtt min/avg/max/mdev = 0.165/0.271/0.355/0.074 ms
```

   The output lists five ping attempts to 192.168.1.10 and a summary of the attempts.

9.1.2 Running traceroute

Run the `traceroute` command to check the route packets that take to a specified host. To run the `traceroute` command:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Commands**.
5. In the **Command** drop-down list, select **traceroute**.
6. In the **Interface** drop-down list, select **eth0** or **eth1**.
7. In the **Host** field, type the IP address or name of the device that you are trying to trace the route.

8. Click **Apply**. The traceroute output displays.

   The following is an example of traceroute output:

```
traceroute to www.example.com (192.168.5.39), 30 hops max, 40 byte
packets

1 192.168.5.39 (192.168.5.39) 0.479 ms 0.864 ms 1.051 ms

2 server10.example.com (192.168.2.21) 1.989 ms 2.186 ms 2.250 ms
```

   The first row of the output lists the target destination, maximum number of hops, and packet size. Each numbered row provides information about one hop. The rows are listed in the order in which the hops occur, starting with the hop closest to the Connect Edge Gateway. Each row for a hop lists the time in milliseconds (ms) for each packet to reach the destination and return to the host.

9.1.3 Running nslookup

Run the `nslookup` command to get Domain Name System (DNS) information for a specified host. To run the `nslookup` command:

9.1.4 Running netstat

Run the `netstat` command to get information about incoming and outgoing network connections, routing tables, and network interface statistics.

The following options are supported with the `netstat` command:

-a	-g	-N	-t
-C	-i	-o	-u
-e	-l	-r	-v
-F (default)	-n	-s	-w

The following options are not supported with the netstat command:

- -c
- -M
- -p

To run the `netstat` command:

1. Select **Troubleshooting** > **Commands**.
2. In the **Command** list, select **netstat**.

3. (Optional) In the **Flags** field, type the options to use with the `netstat` command.
4. Click **Apply**. The netstat output displays.

9.1.5 Running Sniffer

Run the Sniffer to monitor the command exchange between the Connect Edge Gateway and the associated IP-PBX.

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Commands**.
5. Select **Start Sniffer**, or use the keyboard shortcut **CTRL+ALT+S**.
6. Use the associated controls below the Sniffer screen to Search for a specific string, copy to the clipboard, clear the screen, or close the Sniffer. The string is not case-sensitive. A list of up to 50 messages displays. Select/highlight the message to display the details below.

9.2 Managing Connect Edge Gateway Logs

To view the Connect Edge Gateway logs:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Edge Gateway Logs** > **View**. By default, the **Current** tab is selected. The log displays in a separate browser window with the most recent data displayed first.
5. Scroll through the log to review the activity for the Connect Edge Gateway. You view Current Log, Archived Log, Reverse Proxy Log, and TURN Log. Switch the display from the Current Log to the Archived Logs by selecting one of the Archived Logs from the list at the side of the page.

   The Connect Edge Gateway keeps a log that provides detailed information that you can use when troubleshooting. The Current Connect Edge Gateway log is named **messages**, and it is stored uncompressed on the Connect Edge Gateway. **Archived** logs are stored as files that are compressed by the GNU zip (gzip) utility. The gzip utility is available on most UNIX-based

systems. Third-party compression utilities, such as WinZip, also support this compression format. Reverse Proxy and TURN logs can be downloaded.

How many and how often Connect Edge Gateway logs are archived are determined by the local log configuration settings, as described in Configuring Logging and Monitoring Options. Archived logs are named messages.n.gz, where n is a number starting with one and incremented for each archived log (for example, messages.5.gz).

Archivable log modules are:

Table 38: Access Point Information

Log Name	Description
All	Complete message log of the system.
Configuration	Connect Edge Gateway configuration daemon logs.
RAST	RAST configuration daemon logs.
Edge Gateway	Edge Gateway configuration daemon logs.

6. To save/view current logs, select the **Current** tab.
7. Use the Log Name field to select the Connect Edge Gateway log you want to save or view. There are 3 ways to view the log:

   - Click **View** to see the contents of the entire file.
   - Click **View Continuous** to see the data in the file as it is written.
   - Click **Save to Local Disk** to select a location to download the Connect Edge Gateway log, then click Save. When the log is saved, a “Transfer complete” message displays on the **Connect Edge Gateway Logs** page.

     The Connect Edge Gateway log is saved in your computer. By default, if you save the current Connect Edge Gateway log, it is saved as a text file named **edge_gateway_log.txt**. If you save an archived server log, it is saved as a file compressed with gzip (for example, messages.5.gz).
8. To view/save older logs, select the **Archive** tab. Refer to Configuring Logging and Monitoring Options for information on configuring the details of the log files. The files shown in the Archive tab are dependent upon these settings.

   a. Select a file and click **Save**.
   b. Select a location to download the Connect Edge Gateway log, then click **Save**. When the log is saved, a “Transfer complete” message displays on the Edge Gateway Logs page.

      The Connect Edge Gateway log is saved in your computer. By default, if you save the current Connect Edge Gateway log, it is saved as a text file named edge_gateway_log.txt.

If you save an archived server log, it is saved as a file compressed with gzip (for example, messages.5.gz).

Use a utility, such as gunzip or a third-party compression utility, WinZip that supports the .gz format, to decompress the archived Connect Edge Gateway log. After you decompress the file, you have an ASCII file, which you can open in a text editor.

9.3 Managing Technical Support Snapshots

If you must contact Technical Support, you may be asked to provide a support snapshot, which is a a compressed file containing information about the Connect Edge Gateway.

9.3.1 Generating Support Snapshots

When you generate a support snapshot, a set of files containing diagnostic information is compressed (.tgz) and added to the Connect Edge Gateway.

To generate a support snapshot:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Support Snapshots**.
5. Click **Generate**. A support snapshot is generated and displayed on the **Support Snapshots** page.

   The snapshot name is in the following format:

   ```
   sysdump-server_name-timestamp.tgz
   ```

   where timestamp is the year, month, day, and time (for example, sysdump-server1-20150402-094428.tgz).

9.3.2 Reviewing Support Snapshots

After generating a support snapshot, you can review a summary of the snapshot. To review a support snapshot:

1. Select **Troubleshooting** > **Support Snapshots**.
2. Select the support snapshot to review.
3. Click **View**. The support snapshot summary is opened in a new Web browser window.

4. Close the browser window when you are finished reviewing the support snapshot.

9.3.3 Saving System Snapshots

After generating a support snapshot, you can save it to your computer's hard drive. To save a support snapshot:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Support Snapshots**.
5. Select the support snapshot to save.
6. Click **Save**. Select a location to download the Connect Edge Gateway log, then click **Save**.
7. Navigate to the location to save the support snapshot, and if necessary, change the name of the snapshot.

   By default, the name of the snapshot is in the following format:

   ```
   sysdump-server_name-timestamp.tgz
   ```

   where timestamp is the year, month, day, and time (for example, sysdump-server1-20150402-094428.tgz).
8. To save the snapshot, click **Save**.

As the snapshot is saved, you see the progress of the save process on the **Support Snapshots** page. When the save process is complete, a "Transfer complete" message displays on the Support Snapshots page. The snapshot is saved as a .tgz file.

Support snapshots are compressed by the GNU zip (gzip) utility. The gzip utility is available on most UNIX-based systems. Third-party compression utilities, such as WinZip, also support this compressionformat. For more information about gzip, see http://www.gnu.org/software/gzip/.

9.3.4 Deleting System Snapshots

After generating a support snapshot, you delete it from the Connect Edge Gateway. To delete a support snapshot:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.

4. Select **Troubleshooting** > **Support Snapshots**. The Support Snapshots page displays.
5. Select the support snapshot to delete.
6. You can select multiple snapshots to delete. To select contiguous snapshots, press the **Shift** key while selecting the snapshots. To select non-contiguous snapshots, press the **Ctrl** key while selecting the snapshots.
7. Click **Delete**.
8. When prompted to confirm whether you want to delete the snapshot, click **OK**. The snapshot is deleted from the Connect Edge Gateway.

9.4 Capturing Packets

You capture (dump) packet details on a specific interface by using the Packet Capture function.

To capture packets:

1. Launch Connect Director.
2. Click **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the Connect Edge Gateway administration portal.
4. Select **Troubleshooting** > **Packet Capture**.
5. Select the Interface to capture the packets. Valid interfaces are **Any**, **Eth0**, **Eth1** and **lo** (loopback).
6. Select the Protocol to capture. The options are **ARP**, **ICMP**, **TCP** and **UDP**.
7. Enter number of packets to be captured. The range is 1-100000.
8. Enter the range of ports to be included in the capture in the **Start** and **End** fields.
9. Use the **Capture Output** area to view the capture. To send the details of the dump to a screen for immediate viewing, click **Browser** then click **Start Capture**. The following is an example of ARP capture details:.

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture
 size
65535 bytes
13:15:13.770168 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc
13:15:13.779377 arp
who-has 192.168.3.20 (Broadcast) tell 192.168.3.20 13:15:28.785852
 arp
reply
192.168.3.20 is-at 00:30:48:63:02:cc 13:15:28.793387 arp who-has
192.168.3.20
(Broadcast) tell 192.168.3.20 13:15:43.803708 arp reply
 192.168.3.20
is-at
```

```
00:30:48:63:02:cc 13:15:43.812843 arp who-has 192.168.3.20
 (Broadcast)
tell
192.168.3.20 13:15:58.821968 arp reply 192.168.3.20 is-at
00:30:48:63:02:cc
13:15:58.830004 arp who-has 192.168.3.20 (Broadcast) tell
 192.168.3.20
13:16:13.837083 arp reply 192.168.3.20 is-at 00:30:48:63:02:cc
13:16:13.844120 arp
who-has 192.168.3.20 (Broadcast) tell 192.168.3.20 13:16:17.598572
 arp
who-has
192.168.3.1 tell 192.168.3.136 13:16:28.852448 arp reply
 192.168.3.20
is-at
00:30:48:63:02:cc 13:16:28.861481 arp who-has 192.168.3.20
 (Broadcast)
tell
192.168.3.20 13:16:43.868711 arp reply 192.168.3.20 is-at
00:30:48:63:02:cc
13:16:43.875797 arp who-has 192.168.3.20 (Broadcast) tell
 192.168.3.20
13:16:51.004425 arp who-has 192.168.3.138 tell
```

10. To save a summary of the dump, click **File** then click **Save**. Select a location to download then click **Save**.

The following table includes a list of Packet Capture parameters for the Connect Edge Gateway.

Table 39: Packet Capture Parameters

Parameter	Description
Interface	Indicates the Interface to capture the packets. Valid interfaces are Any, Eth0, Eth1 and lo (loopback).
Protocol	Indicates the Protocol to capture. The options are ARP, ICMP, TCP and UDP.
Packet Count	Indicates the number of packets to be captured. The range is 1-100000.
Port Ranges	Indicates the range of ports to be included in the capture in the Start and End Port.
Capture Output	Indicates the area to view the capture.