Administration Guide for ShoreTel Connect Edge Gateway

February 4, 2015

Version Information

Administration Guide for ShoreTel Connect Edge Gateway
Date: February 4, 2015

Company Information

ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085 USA
+1.408.331.3300
+1.408.331.3333 (fax)
www.shoretel.com

Preface

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

About this Guide

The Administration Guide includes the following chapters:

Table 1: Administration Guide Contents

Chapter	Description
Preface	Provides an overview of this document and describes notations and conventions.
Introduction to the ShoreTel Connect Edge Gateway	Provides an overview of the ShoreTel Connect Edge Gateway and the related technologies.
Deploying the ShoreTel Connect Edge Gateway	Describes the network topology for deploying the ShoreTel Connect Edge Gateway.
Installing the ShoreTel Connect Edge Gateway	Describes the procedures for installing the virtual image of the ShoreTel Connect Edge Gateway.
Configuring the ShoreTel Connect Edge Gateway	Describes the procedures for configuring the ShoreTel Connect Edge Gateway by using ShoreTel Connect Director.
Configuring ShoreTel Connect Edge Gateway Phones	Describes the procedures for configuring the phones to be used with the ShoreTel Connect Edge Gateway.
Managing Security on the ShoreTel Connect Edge Gateway	Describes the procedures for managing security on the ShoreTel Connect Edge Gateway by generating and using certificates.
Maintaining the ShoreTel Connect Edge Gateway	Describes the procedures for maintaining the ShoreTel Connect Edge Gateway by using the Gateway UI.

Table 1: Administration Guide Contents

Chapter	Description
Monitoring the ShoreTel Connect Edge Gateway	Describes the procedures for monitoring the ShoreTel Connect Edge Gateway by using ShoreTel Connect Director.
Troubleshooting the ShoreTel Connect Edge Gateway	Describes the procedures for troubleshooting the ShoreTel Connect Edge Gateway by using the Gateway UI.

CHAPTER

1

Introduction to the ShoreTel Connect Edge Gateway

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

Overview

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

To connect remotely to the ShoreTel network all ShoreTel ONSITE customers need an active Internet connection. The ShoreTel Connect Edge Gateway is deployed on the premises of the customer, and hence there is no requirement for a third-party VPN client. You can access and configure the ShoreTel Connect Edge Gateway through ShoreTel Connect Director.

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

ShoreTel Connect Edge Gateway Components

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

ShoreTel IP Phone

ShoreTel provides a variety of IP phones that can be used by remote users to connect to the ShoreTel network through the ShoreTel Connect Edge Gateway. By using a compatible ShoreTel IP Phone, remote users can access contacts internal to their organization, and use the 3-5 digit dialing functionality to make calls as if they were inside their corporate network. User 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 phone is 802.841.5100.0.

Users cannot connect to the ShoreTel network using Media Gateway Control Protocol (MGCP) phones or 200, 500, and 600-series IP phones through the ShoreTel Connect Edge Gateway.

ShoreTel Connect client

The ShoreTel Connect client provides advanced call management and quality desktop video in an easy-to-use interface for users connecting to the ShoreTel network through the ShoreTel Connect Edge Gateway. The Connect client can be accessed from a public Internet hotspot.The Connect client is integrated closely with Microsoft Outlook and offers instant messaging to users who want to stay connected all the time.

ShoreTel Connect Contact Center

The ShoreTel Connect Contact Center software can be used by remote agents to connect to the ShoreTel network through the ShoreTel 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. User must specify Contact Center FQDN configured on the Edge Gateway for accessing Connect Contact Center.

ShoreTel Connect Conference

For existing conferencing service users, it works the same way. You do not require an Edge Gateway to use conferencing service remotely. 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 the Edge Gateway, Collaboration FQDN must to be configured and enabled on it.

ShoreTel 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.

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. IP-based session is used in ShoreTel 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 ShoreTel 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 ShoreTel Connect Mobility Router.

Client Endpoint

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

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 RAST FQDN as VPN gateway address to connect remotely.

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

Client Endpoint

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

Client End-User Experience

When a ShoreTel Connect Contact Center agent accesses the ShoreTel Interaction Center from outside the contact center or ShoreTel 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.

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 ShoreTel 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 ShoreTel 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 ShoreTel Connect Edge Gateway generates and stores a 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 ShoreTel Connect Edge Gateway.

When users communicate using the ShoreTel 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.

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 a 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 a 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.

Traversal Using Relay around NAT (TURN)

Clients behind a NAT firewall can exchange packets with clients behind a different NAT firewall 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 server that 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 ShoreTel Connect client to connect to the PBX network when a user is outside the network.

Client End-User Experience

The ShoreTel 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.

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 a 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.

ICE protocol allows communicating clients to discover paths in network for exchanging information. 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.

Demilitarized Zone (DMZ)

The Demilitarized Zone (DMZ) is the region between the external firewall and the internal firewall, where the ShoreTel 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.

CHAPTER

2

Deploying the ShoreTel Connect Edge Gateway

This chapter describes the different models for deploying the ShoreTel Connect Edge Gateway:

Network Topology

In ShoreTel deployment, the ShoreTel 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.

Edge Gateway Interface

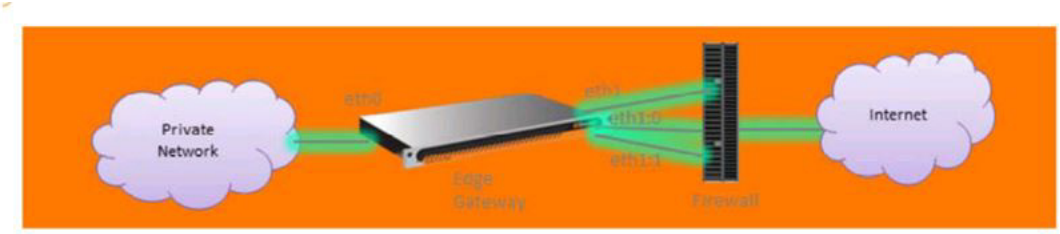

Figure 1: Edge Gateway Interface

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

- eth0 interface connects to Enterprise network, and has one IP address.
- 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 eth1:1

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 ShoreTel Connect Edge Gateway has private interfaces (eth0, eth1) for management and applications data and three different public or DMZ IP addresses have to be on the same subnet (IP1, IP2, and IP3 as shown in Figure 2).

Note

ShoreTel recommends disabling the firewall for the internal interface, eth0. If you do not want to disable the firewall, enable the required media relay ports on the TURN server.

Network Architecture

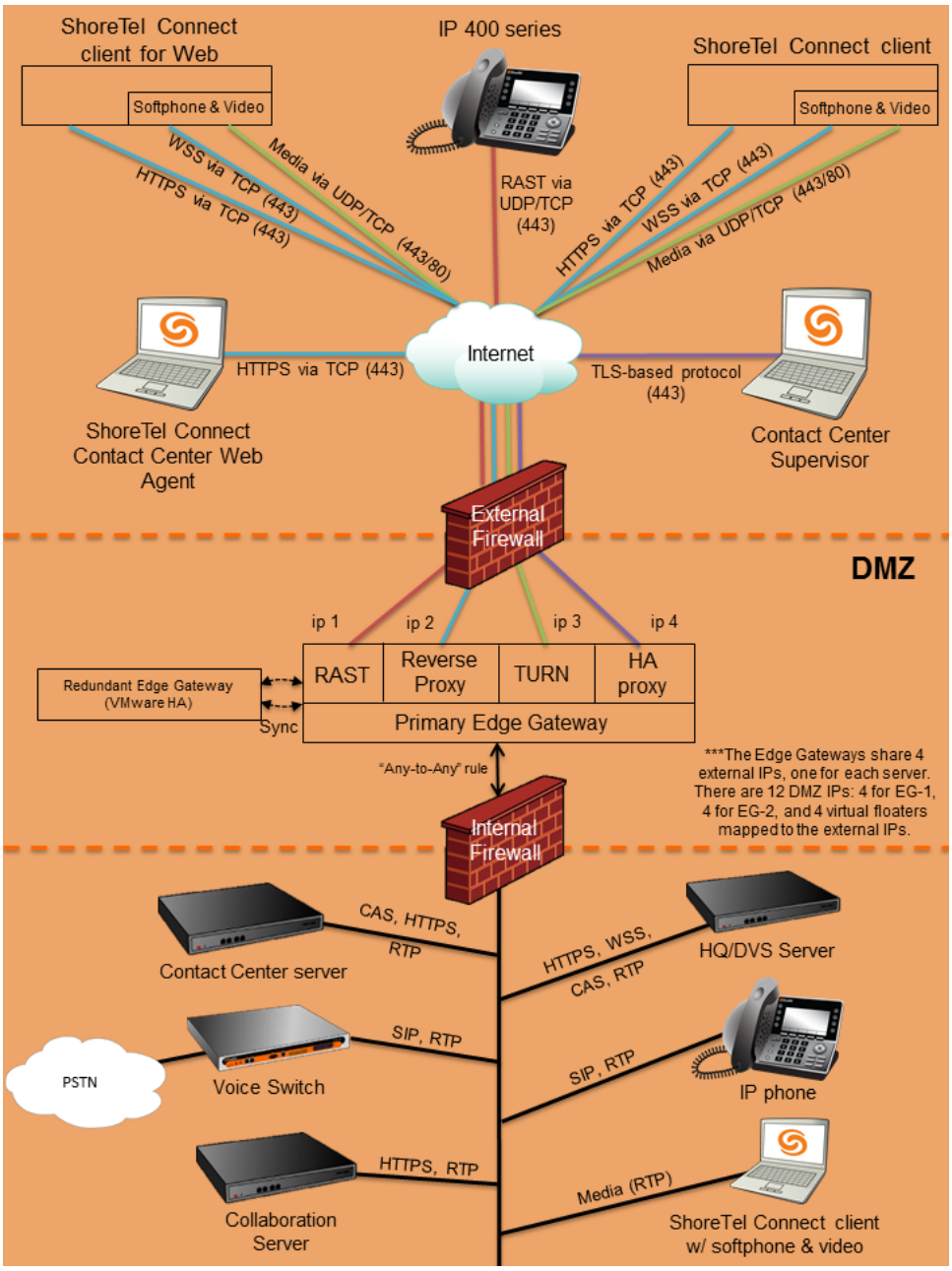

Figure 2: ShoreTel Connect Edge Gateway Network Architecture

Types of Deployments

The ShoreTel Connect Edge Gateway can be deployed as a virtual appliance. ShoreTel Connect supports the Edge Gateway as a virtual appliance, also known as the Virtual Edge Gateway. The support for the Physical Edge Gateway will be added in a later release.

ShoreTel Connect Edge Gateway as a Virtual Appliance

ShoreTel Network users can deploy the ShoreTel Connect Edge Gateway as a virtual appliance, where ShoreTel provides the virtual image that the users can install on their own hardware. The virtual Edge Gateway is allotted resources depending on the scale of deployment. Virtual appliance can be accessed through reverse proxy.

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 may require loading the VM on another physical server).

Table 2 lists the various system capacity values for the ShoreTel Connect Edge Gateway.

Table 2: System Capacity for the ShoreTel Connect Edge Gateway

Virtual Appliance	Small Configuration	Medium Configuration	Large Configuration
Processor	2 CPUs	4 CPUs	8 CPUs
Memory	2 GB	4 GB	8 GB
Hard Disk	100 GB	100 GB	100 GB
RAST sessions	100	500	2000
Active RAST calls	50	100	200
Connect clients	50	400	800
Concurrent audio and video calls on the Connect client	50	100	200

Service Appliance Deployment for Edge Gateway

The Edge Gateway can be deployed with ShoreTel Connect ONSITE collaboration service appliances in two separate scenarios (as shown in 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.

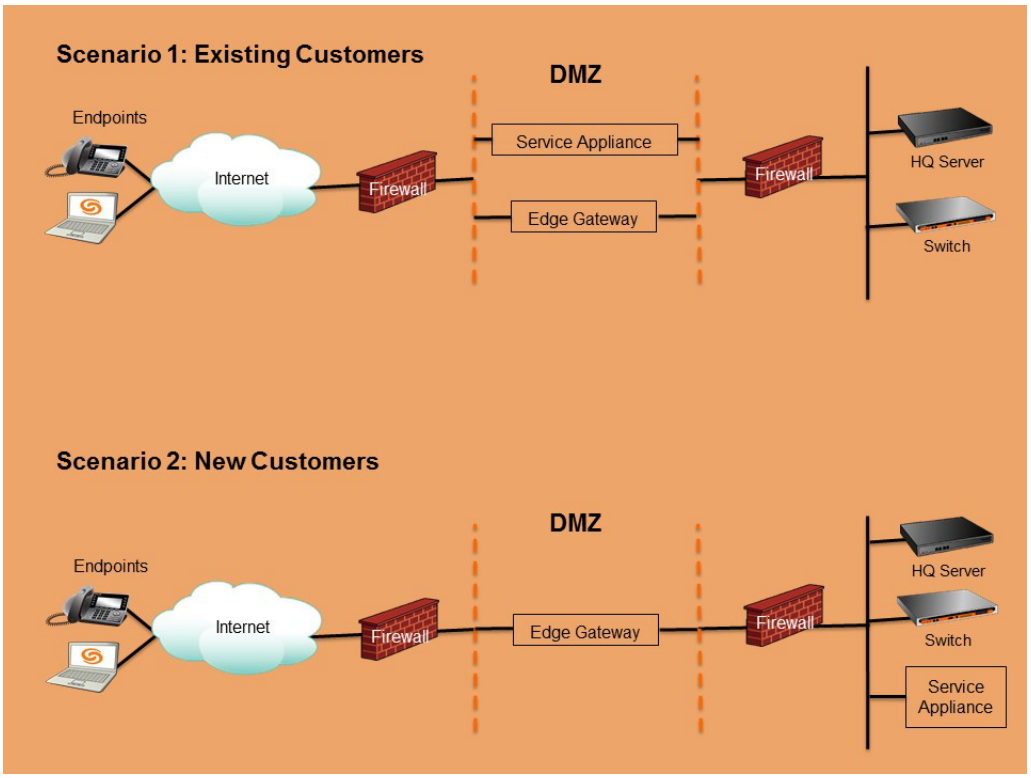

Figure 3: Service Appliance Deployment for Edge Gateway

CHAPTER

3

Installing the ShoreTel Connect Edge Gateway

This chapter describes installation procedures for the ShoreTel Connect Edge Gateway. The topics discussed in this chapter include:

Installing the ShoreTel Connect Edge Gateway Software

Installing Virtual Edge Gateway using OVA File

Note

This procedure requires the vSphere Client and connection to an ESXi server, version 5.1 and 5.5.

Note

First time ShoreTel 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 ShoreTel Connect Director. Refer to Chapter 4, Configuring ShoreTel Connect Edge Gateway Using ShoreTel Connect Director on page 29 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\BareMetalInstall.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 on which 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 choose **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 ShoreTel End User license Agreement, type **Yes**.

16. 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. Type a new **Admin password (Enter to leave unchanged)?**

    h. Type a new **Monitor password (Enter to leave unchanged)?**

    i. **Enter the step number** to edit the above parameters. Or, press **Enter** to save changes and exit.

    j. **Reboot** the Edge Gateway.

Note

Do not change the admin password. It overrides with ShoreTel Connect Director configuration after the restart.

If you want to change the Hostname, eth0 address, default gateway, DNS, and domain name, 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.

Certificate Configuration

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

- Edge Gateway Certificate—Certificate used to access the administration portal of the ShoreTel Connect Edge Gateway.
- RAST Certificates—Certificate used to authenticate the secured connection between Remote IP phones and ShoreTel Connect Edge Gateway.
- Reverse Proxy Certificate—Certificate used to securely access the ShoreTel services via Reverse Proxy.
- TURN Certificate—Certificate used to securely use the TURN service from the ShoreTel Connect Edge Gateway.

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

Generating a Certificate

Use the ShoreTel Connect Edge Gateway administration portal to perform the following procedures.

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

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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 opens.
7. In the **Country Name** field, type the two-letter country code for the country where the ShoreTel Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.
8. In the **State or Province** field, type the state or province where the ShoreTel Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.

9. In the **Locality** field, type the locality where the ShoreTel 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 ShoreTel 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 Name**s field, select the alternative names for the ShoreTel 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**. It displays a confirmation message to restart the Edge Gateway.
17. To generate the certificate, click **OK**.

Note

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

18. Click **Close** to close the certificate window.
19. A restart prompt displays. Do one of the following:
    - Click **OK** to restart the service and activate the newly generated certificate.
    - If you do not want to restart, click **Cancel**. The newly generated certificate will be activated on next restart.

Importing a Certificate

You can import a purchased or self-signed certificate the ShoreTel 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 ShoreTel Connect Edge Gateway.

Note

The remote access certificate is used for the secure connection initiated from the external networks such as homes and hotspots. ShoreTel recommends use of FQDN rather than IP address for imported remote access certificates.

Note

An imported certificate must be in unencrypted Privacy Enhanced Mail (PEM) format and contain the X.509 certificate and the RSA key. Make sure the certificate contains Beginning and End lines within the certificate file.

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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 opens.
7. Paste the certificate, private text, and intermediate certificate authority into the text box on the **Import Certificate** page.
8. Paste the ShoreTel Connect Edge Gateway certificate on the **Import Certificate** page issued by the trusted certificate authority, RSA private key, and the intermediate and root certificates you may have received from the certificate signing authority. Be sure 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
9. Click **Import**. Displays a warning message.

   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.
10. Restart the ShoreTel Connect Edge Gateway, activate the newly generated certificate, click **OK**. If you do not want to restart the ShoreTel Connect Edge Gateway, click **Cancel**. The newly generated certificate is stored on the ShoreTel Connect Edge Gateway until the next restart.
11. Refresh the browser to regain access, then log in.

CHAPTER

4

Configuring the ShoreTel Connect Edge Gateway

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

Server Configuration Considerations

Open port 443 on all the public facing IP addresses for both UDP and TCP traffic on the Edge Gateway. Refer to ShoreTel Connect Edge Gateway Technologies on page 11 for more information about the Edge Gateway technologies.

Adding an Edge Gateway to ShoreTel Connect

Use ShoreTel Connect Director to perform the following procedures.

Note

The following instructions assume a ShoreTel IP PBX running ShoreTel Connect has already been installed. Refer to Chapter 3, Installing the ShoreTel Connect Edge Gateway for EGW installation information before proceeding.

1. Launch ShoreTel 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.

Configuring ShoreTel Connect Edge Gateway Using ShoreTel Connect Director

The following section describes configuring the ShoreTel Connect Edge Gateway.

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

You must enter the Name, IP address, and MAC address of ShoreTel 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.

ShoreTel Connect Edge Gateway General Parameters

Table 3 includes a list of general parameters required for configuring a new ShoreTel Connect Edge Gateway.

Table 3: General Parameters

Parameter	Description
Name	Name of a new or existing server.
Description	Description of the server type, for example “EdgeGW”. (Optional)
IP Address	Private IP address of the ShoreTel Connect Edge Gateway’s eth0 interface. Select **Find Edge Gateway** to choose from a list of available Edge Gateways.
Find Edge Gateway	Displays all the ShoreTel 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 automatically filled.
MAC Address	MAC address of the server.
Fully qualified domain name	Internal FQDN of the Edge Gateway.

Table 4 includes a list of Gateway IP Address parameters required for configuring a new ShoreTel Connect Edge Gateway. Check the box to enable the appropriate service, then enter the IP address.

The ShoreTel 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 4: Gateway IP Address Parameters

Parameter	Description
RAST IP Address	External IP address of RAST Service. Public IP address is mapped to eth1's private address (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) on page 13.
Reverse Proxy IP Address	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, Reverse Proxy on page 12.

Table 4: Gateway IP Address Parameters(Continued)

Parameter	Description
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.

RAST Configuration

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

General Parameters

Table 5 includes a list of basic parameters that are accessed when editing an existing ShoreTel Connect Edge Gateway.

Table 5: 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 ShoreTel Connect Director (HQ server) or fully qualified domain name. Add or remove the configuration servers as necessary.

IP Pool Parameters

You must configure the IP pool (range of IP addresses) for ShoreTel Connect Edge Gateway to assign an internal IP address for each remote IP phone to communicate with other ShoreTel 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 IP addresses as multiple pools. This IP pool must be reserved and cannot be used by the DHCP.

Table 6 includes a list of IP Pool parameters that are accessed when editing an existing ShoreTel Connect Edge Gateway. Multiple IP Pools can be added. Refer to Client IP Pool Parameters on page 38 for more configuration information using the ShoreTel Connect Edge Gateway Administration Portal.

1. **Add** or **Remove** IP Pool from the list as necessary.
2. Click **Save**.

Click **Reset**, if you want to reset or clear the IP Pool parameters.

Table 6: 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.

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 works 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. 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.

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

Reverse Proxy Parameters

Table 7 includes a list of reverse proxy parameters that are accessed when editing an existing ShoreTel Connect Edge Gateway. Check the box to select the appropriate reverse proxy FQDN, then enter the address.

Table 7: 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 connections.
Connect Client FQDN	Enter the external fully qualified domain name for Connect client. This is the public FQDN advertised to users, example, start.acme.com.
Collaboration FQDN	Enter the external fully qualified domain name for Collaboration. Public FQDN for outside user to use conference. This is ready 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.

TURN Configuration

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

TURN Parameters

Table 8 includes a list of TURN server parameters that are accessed when editing an existing ShoreTel Connect Edge Gateway. Enter the appropriate values and select **Save**.

Table 8: 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. **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.

Configuring the ShoreTel Connect Edge Gateway Network

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

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 user's seamless experience, you must specify secondary and tertiary DNS addresses to handle access requests from outside the corporate network.

Configuring Hostname and DNS

To access the administration portal:

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

4. Click **Configuration > System > Networking > Hostname/DNS**. The **Hostname/DNS** page displays.

   This page contains basic networking information about the ShoreTel Connect Edge Gateway. Most of this information is entered during the Initial Configuration Wizard and should not require changing.

Table 9 includes a list of reverse proxy parameters that are accessed when editing an existing ShoreTel Connect Edge Gateway. Enter the appropriate values and select **Save**.

Table 9: Hostname and DNS Parameters

Parameter	Description
Hostname	Verify that the ShoreTel Connect Edge Gateway hostname is the value specified in the Hostname field during the Initial Configuration Wizard. You typically do not need to change 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 changing.
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.

Configuring Ethernet Interfaces

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Configuration > System > Networking > Interface**. The Interface page displays. The **eth**1 tab is active.
5. Verify that the interface is **Enabled**.

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

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 should not require changing.
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**.
MTU	Verify the MTU value.
MAC Address	Verify the MAC address.
Status	Verify the ShoreTel Connect Edge Gateway online status.

Viewing RAST Settings

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

General Parameters

Table 10 includes a list of RAST General parameters..

Table 10: RAST General Parameters

Parameter	Description
Remote Access IP Interface (read-only)	Remote Access IP Interface.
Remote Access FQDN (read-only)	Remote Access FQDN.
Tunnel Interface MTU	The range is from 576 to 9000.
Remote Client IP Lease Duration	The range is from 30 to 65535 minutes.

Protocol Parameters

Table 10 includes a list of RAST Protocol parameters.

Table 11: RAST Protocol Parameters

Parameter	Description
Datagram / TLS UDP	■ Cipher ■ Port ■ MTU ■ Keepalive ■ Session Timeout ■ Renegotiation Time
TLS / TCP	■ Cipher **Note:** RC4-MD5 cipher suite is not supported by ShoreTel Connect Edge Gateway. ■ Port ■ MTU ■ Keepalive ■ Session Timeout ■ Renegotiation Time

Client IP Pool Parameters

Table 12 includes a list of RAST Client IP Pool parameters (read-only). Refer to IP Pool Parameters on page 31 for more configuration information using ShoreTel Connect Director.

Table 12: 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.

Viewing Routing Settings

View the default gateway or additional static routes.

Viewing Static Routes

The default gateway is automatically set up as a static route.

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

Table 13 includes a list of Route parameters.

Table 13: Route Parameters.

Parameter	Description
IP Address	IP address of the status route.
Gateway	IP address of the gateway for the route.
Interface	Ethernet interface for the route.

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

Table 14 includes a list of static host parameters.

Table 14: 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 (_).

Configuring SSH

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Click **Configuration > System > Networking > SSH**.
5. Verify **Enable** is checked.

Table 15 includes the SSH parameter.

Table 15: SSH Parameters

Parameter	Description
Interface	By default, the IP address associated with the primary interface is chosen. This interface is used by the ShoreTel 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.

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

Configuring Logging and Monitoring Options

Use the logging options to record events on the ShoreTel 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)

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 ShoreTel Connect Edge Gateway.

Setting General Email Options

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

Table 16 includes the Email parameters.

Table 16: Email Parameters

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

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

Setting Auto Notification

To set automatic notification of events:

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

Adding Notification Recipients

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

4. Click **Configuration > System > Logging/Monitoring > Email > Notify Recipients** tab.
5. Click **Add**. The **Add Recipient** page displays.
6. In the **Email Address** field, type the email address of the person to receive notification. Check the appropriate boxes to receive details, information, or failure information. The following is a sample output for failure information:

Table 17: Failure Sample

Failure Type	Description
`process-crash`	A process in the system has crashed.
`unexpected-shutdown`	The ShoreTel Connect Edge Gateway has unexpectedly shut down.

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

Configuring Logging Settings

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

Configuring Module Settings

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

   See Table 18 for a list of event levels and their definitions.

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

Table 18: Filtering Levels for Logging ShoreTel 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 ShoreTel 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.
err	Indicates a minor error that might require operator intervention if it recurs. Investigation and corrective action should be taken in order to prevent a more serious (for example, service-affecting) fault.
crit	Indicates that a service-affecting condition has developed and an urgent corrective action 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 restored.
alert	Indicates a severe error condition that requires operator intervention. Critical parts of the system are operational. However, either a less critical part of the system is nonfunctional 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 has failed.
fatal	Internal server error from which the server cannot recover and will terminate.

Table 18: Filtering Levels for Logging ShoreTel Connect Edge Gateway Events

Severity Level	Description
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 customer or can be easily explained. **Note:** Changing the logging level to debug0 can adversely affect ShoreTel 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 ShoreTel 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. **Note:** Changing the logging level to debug2 can adversely affect ShoreTel 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 ShoreTel Connect Edge Gateway performance.
debug4	Reserved. Can be used to view the detailed logs of every packet. **Note:** Changing the logging level to debug4 can adversely affect ShoreTel Connect Edge Gateway performance.

Configuring Local Log Settings

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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 through1048711424 bytes.
   - When log reaches (thousandths of a percent of /var size): The value can be between 1 through 100000.
7. In the **Max log file to keep** field, type the maximum number of log files that are stored on the ShoreTel Connect Edge Gateway. The value can be between 1 through 4,294,967,295.
8. To save your changes, click **Apply**.

Adding Syslog Servers

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

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 Table 18 for a list of severity levels and their definitions.
5. To save your changes, click **Apply**.

Configuring SNMP

Use the SNMP page to enable SNMP on a selected interface and specify a community. SNMP is disabled by default. SNMP can be configured on any interface, but it is recommended to use eth0 for security purpose. Set the Community to value other than public for security reasons.

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

3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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 chosen. This interface is used by the ShoreTel 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**.

Setting the System Date and Time

You can manually set the system date and time for the ShoreTel 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).

Manually Setting the System Date and Time

NTP Servers must be disabled for manual settings to take effect. Refer to Enabling NTP on page 47 for configuration information.

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

Table 19 includes a list of manual time and date parameters.

Table 19: Manual Time and Date Parameters

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

5. Select **Apply** and continue to the NTP Configuration page to disable NTP servers. Refer to Enabling NTP on page 47 for information.

Enabling NTP

If you configure the ShoreTel 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 ShoreTel 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 ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Click **Configuration > System > Date and Time > NTP**.
5. By default, NTP is enabled. Select **Enable NTP** if this function has been previously disabled.
6. Click **Apply**.

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 ShoreTel Connect Edge Gateway contacts the first NTP server listed alphabetically. If that server is unavailable, the ShoreTel Connect Edge Gateway uses the alphabetical list of NTP servers to contact subsequent servers until a connection is made.

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

Table 20 includes a list of NTP parameters.

Table 20: NTP Parameters

Parameter	Description
Server	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.
Version	Select the version of NTP to be used. 4 is the default.

6. Select **Enabled** to activate the NTP server. If you want to use this server as an NTP server, make sure you select this check box in addition to enabling NTP, as described in Enabling NTP on page 47.
7. Click **Apply**.

ShoreTel Connect Edge Gateway Licensing

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

Reverse proxies on the Edge Gateway are accessible without a ShoreTel remote phone license. You can use ShoreTel Connect Contact Center ONSITE Client and ShoreTel 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 ShoreTel Conferencing for the Web.

ShoreTel Connect Director tracks and enforces the number of remote phone licenses installed in the system. When users enable for remote phone authentication 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 ShoreTel 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.

CHAPTER

5

Configuring ShoreTel Connect Edge Gateway Phones

This chapter describes how to configure the ShoreTel 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.

General

The General page displays the Config Server address and NTP Server address. The ShoreTel 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

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

To view the configuration details:

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

Allowed

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.

To add a phone to the allowed list:

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

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

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

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

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

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

3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Configuration > Phones > Allowed List**.
5. Choose 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**.

To delete a phone from the allowed list:

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

Pending

Pending list contains the list of phone 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 ShoreTel 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.

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

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

7. Click **Apply**.

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

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

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

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

To delete a phone from the pending list:

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

Blocked

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 Names, and User ID of the blocked phones.

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

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

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

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

To delete a phone from the blocked list:

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

5. Choose the phone that you want to delete from the blocked list.
6. Click **Delete**.

Configuring Remote Phone 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.

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

By default, ShoreTel system 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 ShoreTel 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** drop-down list, select the codecs list that you chose in Step 2a.
4. Click **Administration > Appliances/Servers > Edge Gateway > RAST > IP Pool**.

   Define IP pools for RAST phones as necessary.

The ShoreTel 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.

CHAPTER

6

Maintaining the ShoreTel Connect Edge Gateway

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

This chapter contains the following sections:

Backup the ShoreTel Connect Edge Gateway

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

Note

To restore a configuration, refer to Restoring the ShoreTel Connect Edge Gateway Configuration on page 60.

On Demand Backup

To perform on demand back up of the ShoreTel Connect Edge Gateway configuration:

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

Table 21 includes a list of on demand parameters for the ShoreTel Connect Edge Gateway.

Table 21: On Demand Backup Parameters

Parameter	Description
Hostname or IP Address	Location to send the configuration file.
Protocol	Protocol by which 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

Note

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

WARNING!

/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.

5. Select **Backup**.

The ShoreTel 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.

Scheduled Backup

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Maintenance > System > Scheduled Backup**. The **Schedules** tab displays any previous scheduled backup yet to be performed. The **History** tabs displays previously performed backups.
5. To add a new scheduled backup, select **Add** on the **Schedules** tab.

Table 22 includes a list of scheduled backup parameters for the ShoreTel Connect Edge Gateway.

Table 22: Scheduled Backup Parameters

Parameter	Description
Name	Name displays on the ShoreTel 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. ■ **Monthly**: Select the **Date** and the **Hour** in 24 hour increments.
Hostname or IP Address	The location to send the configuration file to
Protocol	Protocol by which to send the file
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 prepends the default file name which includes the ShoreTel 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"

Note

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

WARNING!

/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.

Restoring the ShoreTel Connect Edge Gateway Configuration

If you need to roll back to a previous ShoreTel 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 ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.

3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.

4. Select **Maintenance > System > Restore**.

Table 23 includes a list of restore parameters for the ShoreTel Connect Edge Gateway.

Table 23: Restore Parameters

Parameter	Description
Hostname or IP Address	IP address or name of the server where the configuration file is stored.
Protocol	Protocol by which to send the file. Depending upon the type of protocol, for example FTP or SCP, enter the relevant information such as **Port number**, **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 prepends the default file name which includes the ShoreTel Connect Edge Gateway name, the date of the backup 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”

Note

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

WARNING!

/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.

5. Check **Include License**, **Include Network Information**, and/or **Include Certificates** as appropriate.

6. Select **Restore**. 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.

7. Exit and restart the browser.

8. Log in to the ShoreTel Connect Edge Gateway admin portal by entering the Admin login and password.

Restoring Factory-Default Settings

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

- ShoreTel Connect Edge Gateway IP address
- Default gateway
- Domain name

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

Restarting ShoreTel Connect Edge Gateway Services

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

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

To restart the ShoreTel Connect Edge Gateway:

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

Rebooting the ShoreTel Connect Edge Gateway

You can reboot the ShoreTel 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 ShoreTel Connect Edge Gateway, active calls might be dropped.

To reboot the ShoreTel Connect Edge Gateway:

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

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

Upgrading the ShoreTel Connect Edge Gateway

To upgrade the ShoreTel Connect Edge Gateway:

1. Upgrade the HQ/DVS server to a new version. Launch ShoreTel Connect Director.

   For information on how to upgrade the HQ/DVS server, see *ShoreTel Connect Planning and Installation Guide*.
2. Select **Maintenance > Status> Appliances**.
3. Select the **Edge Gateway** for which the service column shows Firmware Mismatch.
4. Choose **Reboot** from the **Command** drop-down list.
5. Click **Apply**.
6. At the confirmation prompt, click **OK**.

Shutting Down the ShoreTel Connect Edge Gateway

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

WARNING!

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

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

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

Starting and Stopping ShoreTel Connect Edge Gateway Services

WARNING!

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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.
   - Click **Stop** to stop the service.
6. Repeat step 5 for each service that you need to start or stop.

Managing ShoreTel Connect Edge Gateway Images

Note

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

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

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

Reviewing Installed Images

To review installed ShoreTel Connect Edge Gateway images, select **Maintenance > Images > Edge Gateway Images**. 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).

Uploading and Installing ShoreTel Connect Edge Gateway Images

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

Note

If you are uploading the ShoreTel Connect Edge Gateway image from a local file system, you must use the Microsoft Internet Explorer Web browser.

WARNING!

When you upload and install an ShoreTel Connect Edge Gateway image, you cannot use the administration portal until the upload and installation are finished.

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **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 ShoreTel 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 ShoreTel Connect Edge Gateway image from a local file system or click Browse to navigate the file system. Navigate to and select the ShoreTel Connect Edge Gateway image (*.img), and click Open.
6. Click **Install**. The image is uploaded to the ShoreTel Connect Edge Gateway.

Changing ShoreTel Connect Edge Gateway Image Used at the Next Reboot

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

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

CHAPTER

7

Monitoring the ShoreTel Connect Edge Gateway

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

This chapter contains the following sections:

Monitoring the ShoreTel Connect Edge Gateway Using Director

Monitoring the Status

1. Launch ShoreTel Connect Director.
2. Select **Maintenance** > **Status** > **Appliances** > **Status**.
3. Select **ShoreTel Connect Edge Gateway** from the Appliances list.

Table 24 lists the status parameters.

Table 24: Status Parameters

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

Monitoring the Performance

You can monitor the ShoreTel 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 ShoreTel Connect Edge Gateway for the selected time period.

Monitoring the ShoreTel Connect Edge Gateway

When you first log in to the ShoreTel 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 ShoreTel Connect Edge Gateway,

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

The Dashboard includes the following information:

- System Status
- Phones
- System

Monitoring Phones

Active Phones

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

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

Monitoring the System

The following types of usage reports are available for the ShoreTel Connect Edge Gateway system:

- Interfaces on page 72

Interfaces

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

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

Table 25 lists the interface information.

Table 25: 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)

Table 25: Interface Information

Column Title	Description
Admin Up	Indicates whether the interface can be administered
Link Up	Indicates whether the network link is up

CHAPTER

8

Troubleshooting the ShoreTel Connect Edge Gateway

ShoreTel Connect Edge Gateway logs are available to assist in troubleshooting. This chapter contains the following sections:

Running Network Troubleshooting Commands

Run the following network troubleshooting commands:

- ping (See Running ping on page 75)
- traceroute (See Running traceroute on page 76)
- nslookup (See Running nslookup on page 76)
- netstat (See Running netstat on page 77)

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 ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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, choose **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=2 ttl=63 time=0.165 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.

Running traceroute

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel 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, choose **eth0** or **eth1**.
7. In the **Host** field, type the IP address or name of the device for which you want 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 ShoreTel 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.

Running nslookup

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Troubleshooting > Commands**.
5. In the Command list, select **nslookup**.
6. In the **Host** field, type the IP address or name of the device for which you are trying to look up.
7. Click **Apply**. The nslookup output displays.

The following is an example of nslookup output:

```
Server:     server1.example.com
Address:    192.168.8.4

Name:       server2.example.com
Address:    192.168.2.240
```

The first two lines list the name and IP address of the device providing the information for the nslookup request. The last two lines provide the name and IP address of the device being looked up.

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 that you want to use with the netstat command.
4. Click **Apply**. The netstat output displays.

Running Sniffer

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

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

Managing ShoreTel Connect Edge Gateway Logs

To view the ShoreTel Connect Edge Gateway logs:

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Troubleshooting > Edge Gateway Logs > View**. 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 ShoreTel Connect Edge Gateway. You can 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.
6. Click the **Prev** and **Next** buttons to view additional pages of data.

   The ShoreTel Connect Edge Gateway keeps a log that provides detailed information that you can use when troubleshooting. The Current ShoreTel Connect Edge Gateway log is named “messages”, and it is stored uncompressed on the ShoreTel 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 ShoreTel Connect Edge Gateway logs are archived are determined by the local log configuration settings, as described in Configuring Logging and Monitoring Options on page 40. 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 26: Unknown Access Point Information

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

Table 26: Unknown Access Point Information

Log Name	Description
RAST	RAST configuration daemon logs.
Edge Gateway	Edge Gateway configuration daemon logs.

7. To save/view current logs, select the **Current** tab.
8. Use the **Log Name** field to select the ShoreTel 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 ShoreTel Connect Edge Gateway log, then click Save. When the log is saved, a “Transfer complete” message displays on the ShoreTel Connect Edge Gateway Logs page.

     The ShoreTel Connect Edge Gateway log is saved to your computer. By default, if you save the current ShoreTel 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).
9. To view/save older logs, select the **Archive** tab. Refer to Configuring Logging and Monitoring Options on page 40 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 ShoreTel Connect Edge Gateway log, then click **Save**. When the log is saved, a “Transfer complete” message displays on the Edge Gateway Logs page.

      The ShoreTel Connect Edge Gateway log is saved to your computer. By default, if you save the current ShoreTel 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, such as WinZip, that supports the .gz format, to decompress the archived ShoreTel Connect Edge Gateway log. After you decompress the file, you have an ASCII file, which you can open in a text editor.

Managing Technical Support Snapshots

If you need to contact Technical Support, you might be asked to provide a support snapshot, which is a a compressed file that contains files that provide information about the ShoreTel Connect Edge Gateway.

Generating Support Snapshots

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

To generate a support snapshot:

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

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 that you want 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.

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 ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Troubleshooting > Support Snapshots**.
5. Select the support snapshot that you want to save.

6. Click **Save**. Select a location to download the ShoreTel Connect Edge Gateway log, then click **Save**.
7. Navigate to the location to which you want 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 can 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 compression format. For more information about gzip, see http://www.gnu.org/software/gzip/.

Deleting System Snapshots

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

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Troubleshooting > Support Snapshots**. The **Support Snapshots** page displays.
5. Select the support snapshot that you want 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 ShoreTel Connect Edge Gateway.

Capturing Packets

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

To capture packets:

1. Launch ShoreTel Connect Director.
2. Click **Administration > Appliances/Servers > Platform Equipment**.
3. Click the **Name** of the Edge Gateway from the list pane to launch the ShoreTel Connect Edge Gateway administration portal.
4. Select **Troubleshooting > Packet Capture**.
5. Select the Interface on which 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 **to 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 **to File** then click **Save**. Select a location to download then click **Save**.