A MITEL
PRODUCT
GUIDE

MiVoice Connect

Maintenance Guide

Release 20.0

May 2024

Mitel
Powering connections

Notices

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

Trademarks

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

Contents

What's New in this Document 1

This section describes changes in this document due to new and changed functionality in MiVoice Connect Release 20.0. The changes are summarized in the following table.

Table 1: Document Version 1.0

Feature	Update	Location	Publish Date
Certificate Authentication on Switches	Added a command to configure switches for certificate authentication.	Manually Configuring Switches to Use Fixed IP Addresses	December 2023
Points to note for CentOS to Rocky Linux migration	Added a section with points to consider while migrating devices from CentOS to Rocky Linux.	Points to Consider for CentOS to Rocky Linux Migration	December 2023

Preface 2

This chapter contains the following sections:

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

The *MiVoice Connect Maintenance Guide* describes how to troubleshoot and solve problems that can arise in a highly complex system.

2.1 Conventions Used

- Courier font

  For code examples and information that you type.
- UPPERCASE WORDS

  For keywords related to the Mitel system.
- WARNING (alert)

  For preventing data loss or equipment damage (if instructions are not followed).
- Italic text

  For variable parameters that can change depending on usage.

  For document names and path names.

  For command names.
- < > (brackets)

  For items supplied by user and variables in event codes.

2.2 For More Information

- *MiVoice Connect Planning and Installation Guide*

  Comprehensive guide to planning and implementing full-featured, enterprise-class VoIP system.
- *MiVoice Connect System Administration Guide*

  Detailed reference guide for administering the MiVoice Connect system.

MiVoice Connect Architecture 3

This chapter contains the following sections:

This chapter describes the MiVoice Connect architecture, and its components.

Overview

MiVoice Connect system is a single platform and user interface that provides business communications.The MiVoice Connect system provides a single-image system across all locations with complete feature transparency and integration of all PBXs, voicemail systems, automated attendants, and Automatic Call Distribution (ACD) systems. The MiVoice Connect system simplifies the way the organizations deploy, manage, scale, and secure their phone systems and provides a common user experience regardless of the deployment model. The MiVoice Connect system provides a platform that makes each switch and site an independent call processor which continues to operate seamlessly in the event of Wide Area Network (WAN) failure.

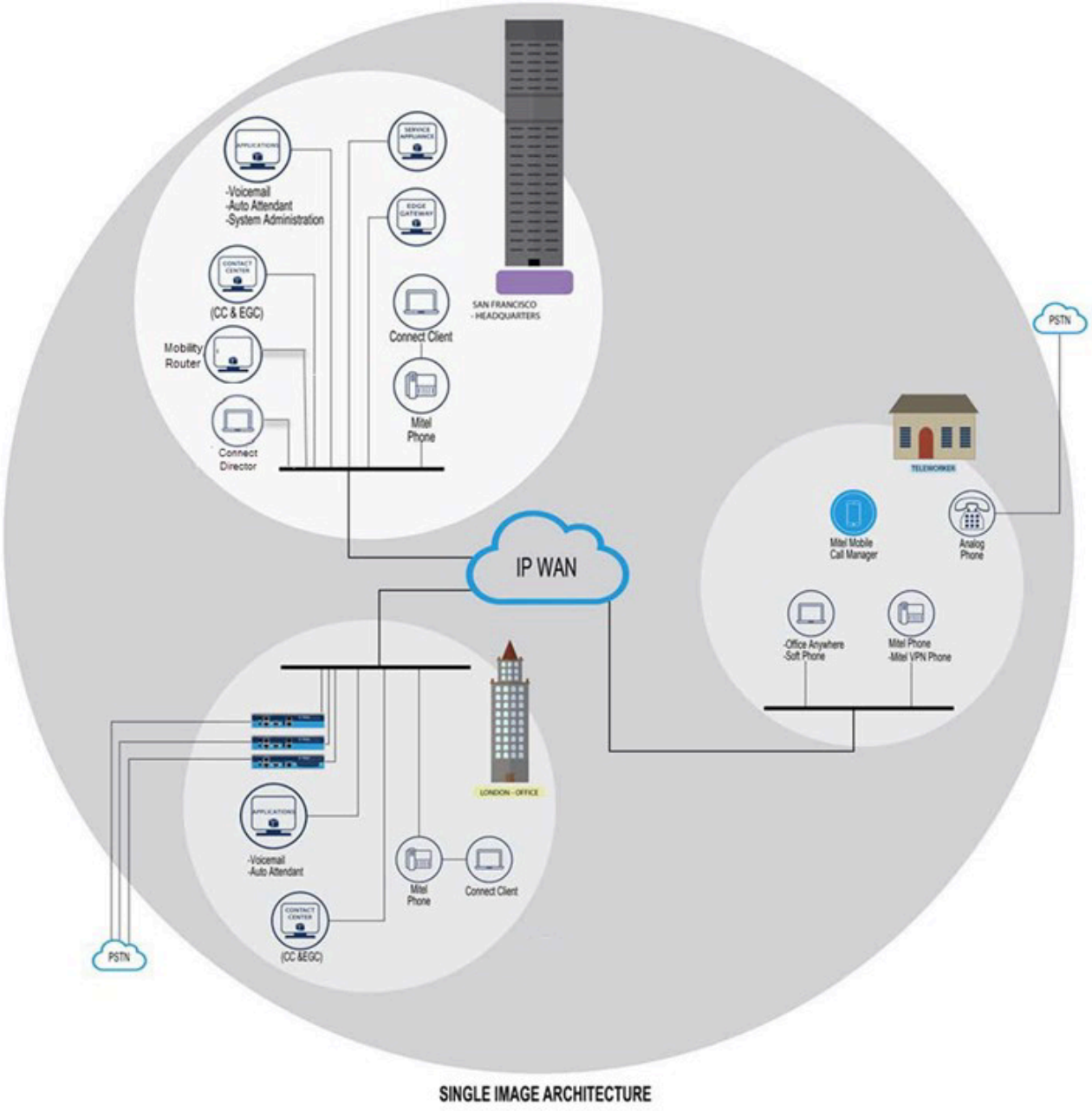
3.1 System Management

The MiVoice Connect system provides a browser-based network management application called Connect Director that provides a single management interface for all voice services and applications across all locations. The MiVoice Connect system provides automated software distribution for all components on the system. When you add a new voice switch to the system, it is automatically upgraded to the current software release by the server. Existing voice switches download the current software when you reboot the switches. The Headquarters server does not upgrade Distributed Voice Servers (DVS); these must be upgraded independently.

The management software also provides a complete suite of maintenance tools. The Diagnostics & Monitoring system, which is available through Connect Director, provides detailed status information about the components in your Mitel system. It also provides a system dashboard, a topology map, alerts, call quality information, and remote packet capture functionality.

When you add a new user to the system, that user automatically receives a dialing plan, voicemail, an extension, a mail box, an auto-attendant profile, and an email reminder to download the desktop software. You can also add the user to a workgroup, if required.

Figure 1: MiVoice Connect Single-Image Architecture



SINGLE IMAGE ARCHITECTURE

3.2 Benefits

The MiVoice Connect system is a highly distributed, flexible, easy to deploy, easy to use and manage, and reliable voice communication system.

- **Reliability:** All the components operate together as a single system. As a result, in the event of a WAN outage each site can function independently, and in the event of a hardware failure phones will register to a spare voice switch anywhere in the network so that not a single call is dropped.
- **Flexibility:** This approach allows Mitel to offer flexibility in implementation strategies and control. You can choose to deploy any combination of purpose-built, solid state physical appliances, or

virtual appliances installed on industry-standard x86 servers. This ensures that the Mitel Unified Communications (UC) systems scale easily and is suited for companies having multiple sites.

- **Ease:** Mitel presents a single interface to system administrators and end users alike. The Connect Director and Connect client UI software reduce training, configuration and maintenance hours and increase end-user adoption rates.
- **Voice Application Features:** Applications including voicemail, unified messaging, auto-attendant, basic ACD and Call Detail Reporting (CDR) are distributed through the enterprise as integral components of the Mitel UC platform core software. The Mitel UC platform provides enhanced communication solution applications such as Collaboration for Web, Connect Contact Center, Connect Mobility, and advanced applications from Professional Services and third-party technology partners.
- **Solution and Advanced Application Integration:** The UC platform is an end-to-end, all-in-one communication solution. Connect Contact Center, Collaboration for Web, Connect Mobility integrate into the Mitel UC platform's single-image architecture and automatically extend the functionality of Connect Director and Connect client management and user interfaces. UC platform is based on open standards to easily deploy the additional software solutions and business process applications. Mitel advanced applications integrates with Microsoft Outlook, Salesforce.com, Customer Relationship Management (CRM) applications, Interactive Voice Response (IVR) contact center tools, voicemail-to-text converters, emergency notification solutions.
- **Call Detail Reporting (CDR):** Integrated CDR tracks all call activity for users, trunks, and workgroups. Historical logs provide a management tool for monitoring employee workflow, inbound and outbound activity, and trunk utilization. The integrated call accounting system manages communication costs by using account codes to associate customer or project accounts to all calls and by enabling password access to advanced calling permissions.
- **Call Control:** The UC platform architecture distributes core voice communications capabilities across all core system components. A single system serves multiple locations and provides stand-alone survivability at every site in the event of a network or hardware failure. Each switch works with all other voice switches to create a single, transparent, and easily managed UC solution. Every voice switch hosts the call control application including IP-PBX and supports IP Phones, SIP phones and devices, and analog phones and devices. Voice Switches also provide network interfaces to bridge the communications beyond the enterprise by supporting SIP, analog, and ISDN trunking.
- **Voicemail and Unified Messaging:** Unified Messaging features can be deployed either centralized in a data center or distributed across the network on industry-standard servers or voice switches. Mitel provides a voicemail solution that uses advanced call routing rules. When combined with the Connect client and Connect Mobility, users can integrate their voicemail inside Microsoft Outlook inbox, and can direct the calls based on the calendar.
- **Auto-attendant and Automated Call Distribution (ACD):** Mitel's embedded auto-attendant provides automated call answering and routing. Outgoing prompts can be customized and linked to the time of day and/or day of the week. Mitel distributed workgroups feature provides basic ACD functionality for call centers. Simple call routing, overflows, announcements, historical reports and real-time alerts are integrated into the core platform software. Distributed workgroup ensures that the agents in remote sites or branches are available independent of any network outages.
- Additional reliability is provided by the following capabilities:

  - An embedded, real-time operating system and call control architecture, enables all switches to communicate with each other and distribute call processing across the network.
  - N+1 redundancy ensures that if a voice switch fails or is isolated by a network fault, the phones supported by that switch automatically fail over to another voice switch–either at that site or a shared

resource at a data center as long as the phone has the ability to reach the spare switch on the data network.

- **PSTN Fail over:** If the WAN is down or over-utilized for voice traffic, or if bandwidth limits extension-to-extension calls between sites, calls can automatically route over the PSTN to provide seamless communication.
- **Ethernet Port Fail over:** If the upstream network device fails, voice switches automatically fail over to the redundant link to provide continuous operation.
- **Power Fail over:** Voice switch provides power fail transfer. If a complete power outage exceeds reserve power duration, one analog trunk on the voice switch automatically connects to one analog telephone to provide emergency dial tone.

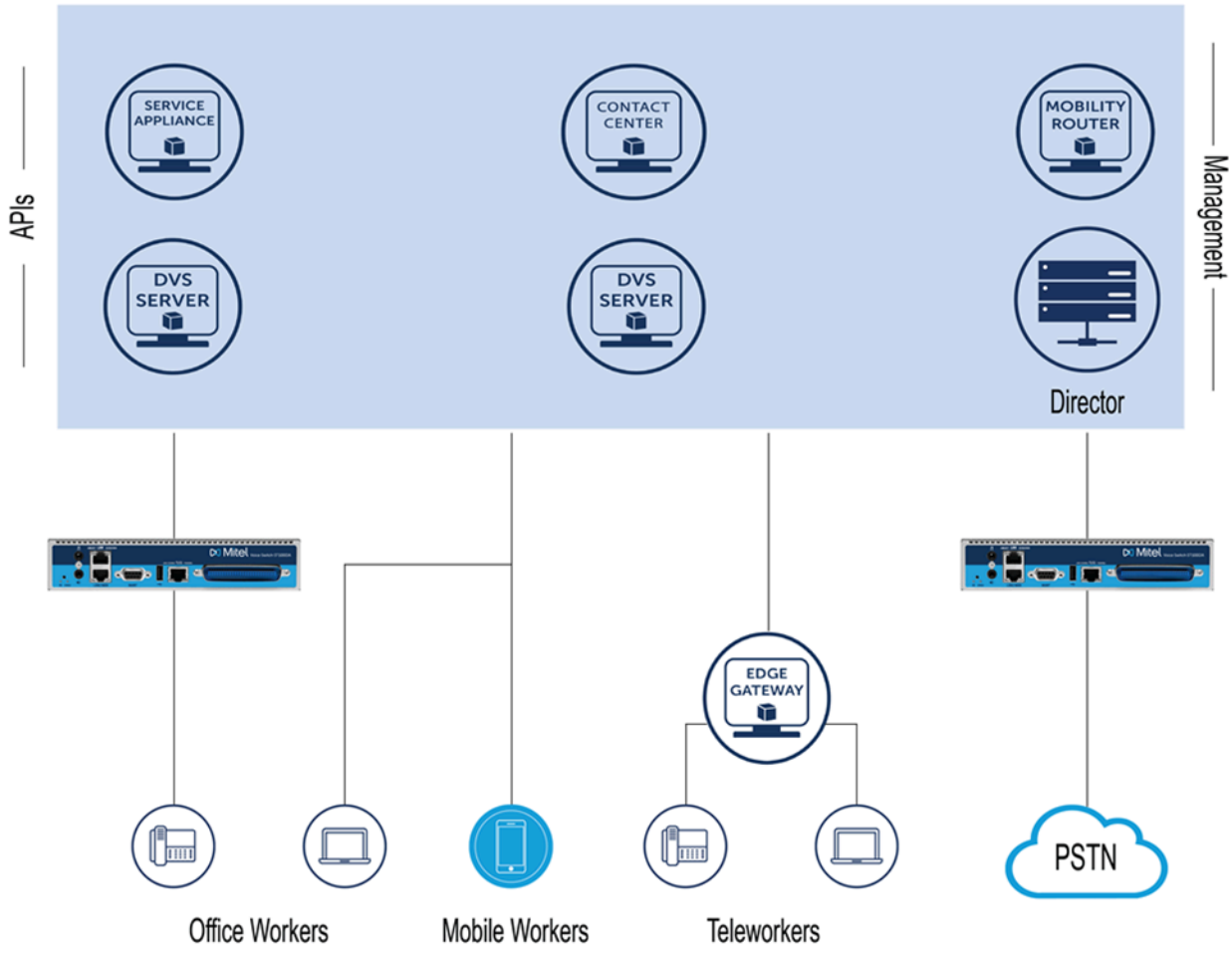
3.3 MiVoice Connect Architecture

MiVoice Connect system consists of:

- **Voice Switches:** provides voice switching and core PBX functionality.
- **Secure Access Layer:** protects phones, trunks, and the MiVoice Connect application against all security risks.
- **Application Layer:** consists of the higher-level applications, such as Voice mail, Connect Contact Center, Connect Mobility, Collaboration for Web.
- **Solution:** provides open APIs for both Mitel and third party users.

- **Management Framework:** tailors management interfaces depending on deployment model system, so you can direct your IT resources towards the other strategic business initiatives.

Figure 2: MiVoice Connect Architecture



The MiVoice Connect system includes:

- Connect Director
- Mitel Servers
- Voice Switches
- Service Appliances
- IP Endpoints
- Virtualized PBX and UC Components
- Connect Client Applications
- Connect Mobility
- Connect Contact Center
- Connect Edge Gateway
- Connect Deployment

3.3.1 Connect Director

Connect Director is a web-based application for managing the MiVoice Connect system from anywhere on an IP network. Using Connect Director, you can configure, manage, and maintain all aspects of the MiVoice Connect system. Connect Director includes maintenance pages to view status and issue maintenance commands for system components, including remote servers. Connect Director is hosted by primary HQ server and cannot be accessed if the HQ server is unavailable.

Connect Director provides simultaneous access to Connect Director by multiple users. The database is locked during save transactions in Connect Director to ensure the data integrity. If another user tries to save changes while the database is locked, Connect Director advises the user that the changes were not saved; the user needs to save the changes again.

Through administrative permissions, the MiVoice Connect system allows various levels of access to Connect Director. By default, the initial system administrator has access to everything on the system. You can assign other users one of several built-in roles, or you can define roles for more limited purposes such as allowing site administrators, directory list managers, and read-only users to perform specific tasks.

3.3.2 Mitel Servers

Each MiVoice Connect system includes a main server called the Headquarters server. Systems may optionally include distributed applications servers, called Distributed Voice Servers (DVSs). Each server provides a local instance of Telephony Management Service (TMS) that supports applications such as voicemail, workgroups and Connect client. Each instance of TMS manages its local soft switch and can be configured to manage voice switches as well. The DVSs rely on the HQ server for configuration changes, but otherwise DVSs can operate independently of the HQ server.

3.3.2.1 Headquarters Server (HQ)

The Headquarters server is the main Connect server and hosts the voice applications platform and the management web site (Connect Director), as well as the integrated voice applications. The Headquarters server is located at the largest site that contains the majority of users. The Headquarters server hosts a soft switch that provides extensions for the auto-attendant, workgroups, and virtual users.

3.3.2.2 Distributed Voice Servers (DVS)

DVS provides increased system reliability by distributing key services and applications at remote sites. Each DVS includes an instance of TMS that connects to and manages the local soft switch. DVSs can be configured to support distributed voice applications such as voice mail, workgroups, account codes, auto attendant and a distributed database. DVSs have Telephony Application Programming Interface (TAPI) access to the local soft switch. If a distributed database is optionally enabled on the DVS, the distributed TMS maintains a copy of the configuration database that allows it to provide call control and voice mail service during the outage. Each DVS manages its own soft switch, as well as voice switches assigned to it.

3.3.3 Voice Switches

Voice switches provide physical connectivity for the PSTN and analog phones, and logical connectivity for IP endpoints on a reliable, highly scalable platform for the call control software. The voice switches and service appliances receive the configuration information via TMS.

All physical Voice Switches have flash memory that allows permanent storage of the call control software and configuration information. The Voice Switches have no moving parts (that is, no hard drive) other than a highly reliable fan. The switches include the necessary DSP technology to enable features like echo cancellation, voice compression, and silence suppression.

The switch acts as a media gateway for the PSTN and analog phones by encoding the analog voice and transmitting it to the other endpoint over the IP network using RTP. The switch also uses Network Call Control (NCC) to send events to TMS about digit collection, caller ID, call establishment. TMS makes this information available to the server applications. These applications are not necessary for many calls (such as those between two phones or a trunk and a phone, which can be established with only the switches controlling the phones and trunks), but they can enhance the user experience. For example, Connect client can provide information about the call to the user's desktop.

3.3.4 Service Appliances

The Service Appliance is a sealed appliance, optimized for resiliency and security, capable of running Mitel services. The Service Appliance can host Audio Conferencing, Web Conferencing and Instant Messaging services.

Service appliances are deployed in the same manner as other voice switches and managed similarly to the voicemail-enabled switches. Director windows configure conference settings and provide status for the Service Appliance. Network settings are configured using a serial cable or the Service Appliance's switch command line interface (`stcli`). The management of the services running on the Service Appliance switch is done via the Service Manager command line interface (`svccli`). The `stcli` and *svccli* commands are accessible through a serial cable or remotely through SSH.

3.3.5 IP Endpoints

The Mitel system manages calls and applications for three types of IP endpoints: IP phones, Soft phones, and conference bridges. IP endpoints are identified by IP address and can exist anywhere on the network. All IP endpoints are supported by voice switches, which must have sufficient capacity for all the IP endpoints in the system. IP endpoints are configured in the system with Connect Director.

3.3.6 Virtualized PBX and UC Components

The PBX and UC software is built upon a distributed architecture. Multiple instances of each server type such as Phone Switch, Trunk Switch, DVS, and Conference Bridge are deployed in each cluster and the workload is distributed. Because of the distributed architecture, a failure to a server instance generally impacts a localized subset of the user population.

The server types run on a Linux platform and Windows platform that contains a service manager. The service manager automatically terminate and restarts processes that exhibit the following failures:

- A CPU consumption threshold that has been exceeded.
- A memory consumption threshold that has been exceeded.

Similar to Windows services, the service manager attempts to restart a process up to a predefined limit. The service manager is monitored by a separate watcher process which automatically restarts the service manager if it stopped running.

3.3.7 Connect Client Applications

Client applications, such as Connect client, interact with TMS using the Client Application Server (CAS) for call and data handling. Connect client provides desktop call control as well as voicemail, directory, and call logging features. Users of supported versions of Microsoft Outlook can integrate their voicemail, contacts, and calendar with the Mitel system.

3.3.8 Connect Mobility

The Connect Mobility is designed to create network transition points between Wi-Fi and Cellular where calls are expected to handover. The Connect Mobility Router (CMR), a platform for mobile convergence, provides seamless location-based voice handover as users roam between Wi-Fi and cellular networks, uses various metrics, such as voice quality, signal strength, packet loss, jitter, Signal to Noise Ratio (SNR), and battery life to make decisions on how calls are routed. When users are within the building, calls generally stay on Wi-Fi. As users walk outside, the Connect for iOS or Android and the Mobility Router jointly make a routing decision to provide seamless, zero-impact handover of an existing call. While within the building, the solution preserves the native Access Point-to-Access Point (AP-to-AP) roaming behavior of the Wireless Local Area Network (WLAN).

The CMR service is deployed using its own application-level HA solution. Users are statically assigned to a specific CMR instance. The Connect for iOS or Android connects to its CMR instance directly via RAST. If the CMR application HA capability is not deployed, there is no fail over if the CMR server is not responsive.

For each user, the CMR creates a SIP connection to the user's home Phone Switch, i.e. it does not connect via the Phone SBC. Recovery from a failure of the home Phone Switch is automatic. A user is dynamically re-assigned to another Phone Switch and the CMR is automatically redirected to the new home Phone Switch.

3.3.9 Connect Contact Center

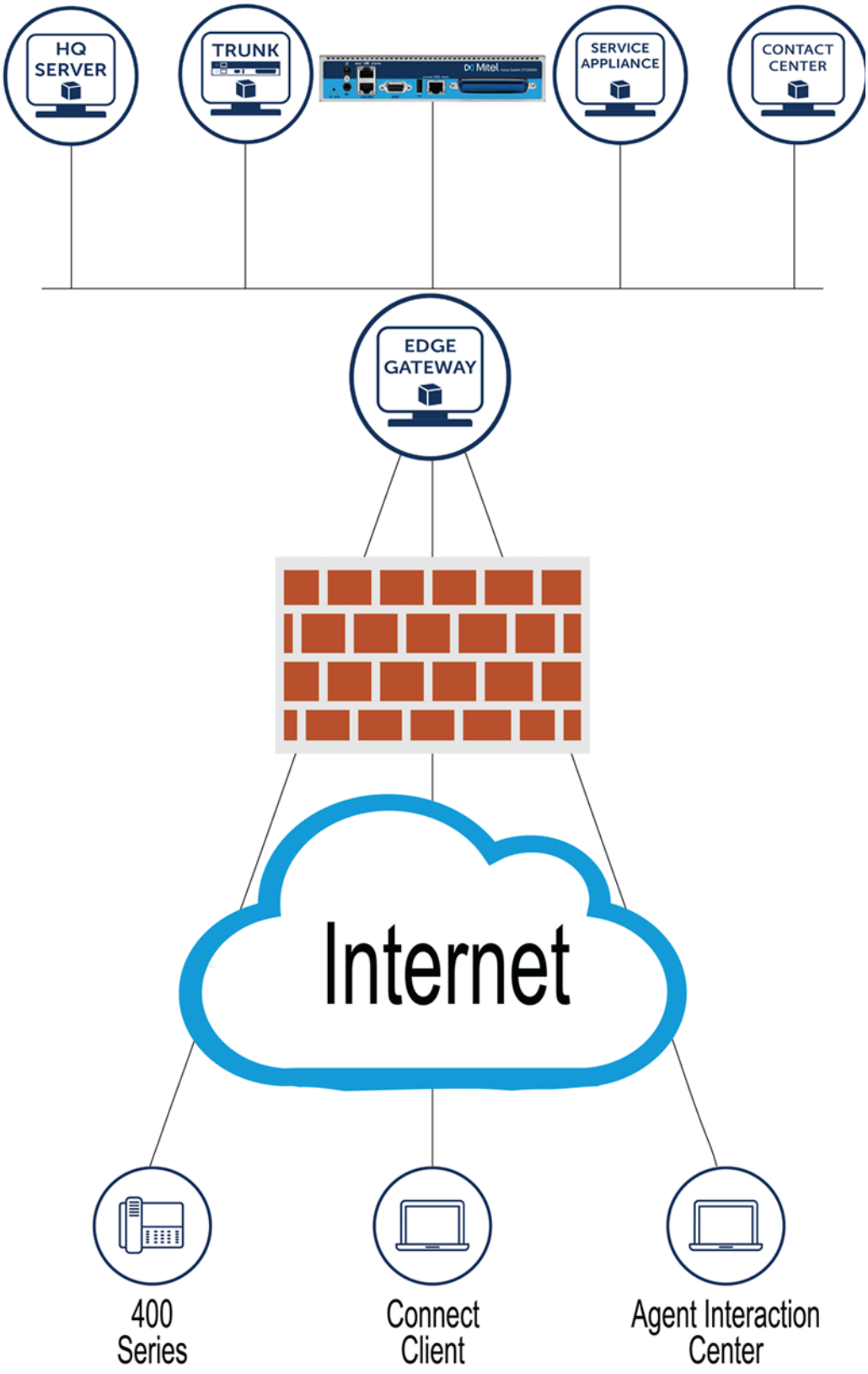
The Connect Contact Center software can be used by remote agents to connect to the Mitel network through the Connect Edge Gateway for advanced multimedia call center solutions. The Connect Contact Center services are deployed on Windows DVS. Windows DVS have the same underlying fault detection and recovery capabilities as the Linux DVS. Incoming calls to an IVR is sent to a backup destination if the Connect Contact Center service is unresponsive. This service has an application-level HA feature that allows a backup instance to be deployed on a separate server so that it can take over if the primary Connect Contact Center service becomes completely non-functional.

3.3.10 Connect Edge Gateway

The Connect Edge Gateway is a remote access solution offering to Mitel MiVoice Connect customers. The Connect Edge Gateway enables users to connect securely to their solution by using the following endpoints:

- IP 400 series phone (all models)
- Connect client
- Connect Contact Center
- Collaboration for Web

Figure 3: Connect Edge Gateway



Connect Edge Gateway uses RAST protocol (UDP-based) to control over an expanded codecs list.This appliance also provides end-to-end encryption for all traffic and does not require installation of a VPN client on any endpoint. Connect Edge Gateway also uses reverse proxy to manage the Connect client, and Collaboration for Web and uses TURN server to manage softphone audio from the client and Collaboration for Web.

To connect remotely to the Mitel network, all MiVoice Connect customers need an active Internet connection. The 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 Connect Edge Gateway through Connect Director.

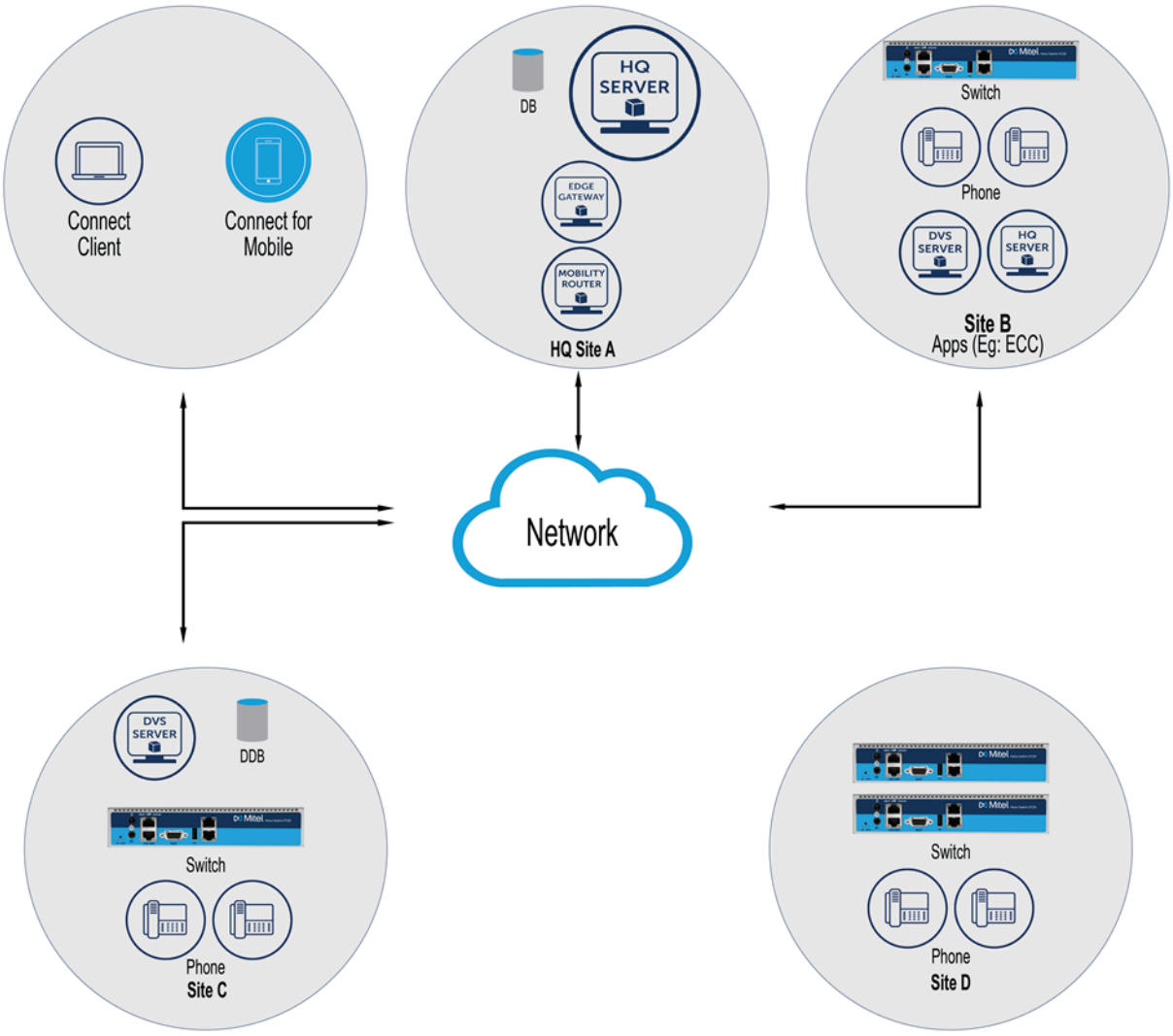
3.4 MiVoice Connect Deployment

3.4.1 Mitel MiVoice Connect

MiVoice Connect is an end-to-end UC solution that customer own, maintain and control their platform including IP-PBX telephony services, desk phones, and applications such as Connect client, Connect for Mobile, Collaboration for Web, and Connect Director.

A typical large multi-site deployment has the following components:

Figure 4: MiVoice Connect Deployment



- **HQ server:** Home of the primary database (DB), Connect Director, manage some switches.
- **Distributed Voice Server (DVS):** One or more distributed servers managing switches with an optional distributed database (DDB). DVS can either be on Windows Operating System (WinDVS) or Linux Operating System (Linux DVS).
- **Switch:** Tens to hundreds of switches to manage end points, provide call control/media capabilities.
- **Unified Communications in a Box (UCB):** Service appliance providing instant messaging and conferencing.
- **Phone:** Several thousand MGCP and/or SIP end points.
- **Connect client:** Several hundreds to thousand stand-alone or web-based client applications.
- **External applications:** A DVS dedicated to an external application such as Connect Contact Center, Syntellect or a Call recording server.
- **Connect Mobility:** Several hundred Connect Mobility clients.
- **Mobility Router:** One or more Mobility Routers.
- **WAN:** A wide area network for inter-site communications.
- **Edge Gateway:** An appliance for secure access of Mitel services by remote endpoints.

3.4.2 Connect HYBRID

Connect HYBRID enables companies to deploy MiCloud Connect and MiVoice Connect systems to different locations, and provides automated directory integration, extension-to-extension dialing, and Caller ID between the MiCloud Connect and MiVoice Connect systems. This feature requires a telephony-enabled MiCloud Connect account, and Mitel staff facilitate installation of the feature.

Mitel Server 4

This chapter contains the following sections:

This chapter provides an overview of Mitel servers.

4.1 Overview

The Connect voice over IP telephony solution is a suite of software modules, applications, and services running on a Mitel server. Every Connect system includes a main server called the Headquarters server. In a single-site system, the Headquarters server may be the only Mitel server. More complex systems may include Distributed Voice Servers (DVS) to add reliability for applications and switches on remote sites or to support distributed applications. The Headquarters server remains the main server and must be available to interact with the DVS servers for full system functionality.

4.1.1 Headquarters Server

The Headquarters server is the main Connect server and hosts the voice applications platform and the management web site (Connect Director), as well as the integrated voice applications. Typically, the Headquarters server is located at the largest site that contains the majority of users.

The Headquarters server hosts a SoftSwitch that provides extensions for the Auto-Attendant, Workgroups, and virtual users.

4.1.2 Distributed Voice Servers (DVS)

The Connect system also supports remote distributed voice servers (DVSs). DVSs provide increased system reliability by distributing key services and applications at remote sites. Each DVS includes an instance of TMS that connects to and manages the local softswitch. The softswitch provides extensions for use by the local Auto-Attendant, Workgroups, and virtual users.

Distributed voice servers can also be configured to support distributed voice applications such as voice mail, workgroups, account codes, auto attendant and a distributed database. DVSs have TAPI access to the local SoftSwitch. If a distributed database is optionally enabled on the DVS, the distributed TMS maintains a copy of the configuration database that allows it to provide call control and voice mail service during the outage. Each DVS manages its own softswitch, as well as voice switches assigned to it.

Remote DVSs are valuable for the following purposes:

- They reduce bandwidth usage because local users' calls to voice mail are answered by the local voice mail application and do not pass across the WAN.
- They increase system scale by extending the unified messaging and desktop call control services to additional users of the applications.
- They increase system scale and reliability by providing distributed switch management, call control services, and unified messaging.
- They increase system reliability by locating workgroups on other servers and providing a location for backup workgroups to reside if a workgroup's primary server becomes unavailable.
- They enable integration of value added applications such as ECC, Recording Servers, and more.

Call control is provided by Headquarters and distributed voice servers even if full network connectivity is unavailable. However, calls to unreachable endpoints cannot be made, and call detail recording requires Headquarters server communication.

The following sections provide more detail on the communications, services, and applications.

4.1.3 Configuration Communications

Connect system processes use Open Database Connectivity (ODBC) objects to share information from the configuration database among themselves and to write configuration information to the database. Static configuration parameters are written to the database by Connect Director, and system components access the database to read/write current state information. User configuration options are written to the database from the Connect client and the telephone interface (voice mail options). Connect Director is accessed via a web browser.

The service ST-ZIN, running on the Headquarters server, manages these COM communications for all services. There is a single writable instance of the database on the Headquarters server, even if distributed databases are created on distributed voice servers.

Each service on a distributed server caches a copy of the configuration database in internal data structures. When a distributed server loses connection to the Headquarters server, changes made to the Headquarters configuration database are no longer received by the distributed server. However, services continue to function with the most recent configuration data until connectivity is restored. When the connection is restored, the distributed server automatically receives and incorporates any changes made to the Headquarters database during the outage.

If a distributed server restarts without a connection to the Headquarters database, then services are started but are not functional. When the network connection is restored, the configuration is retrieved and again cached by each service and services become functional.

Connect client applications, such as the Connect client, use Client Application Server (CAS) for data handling. CAS communicates with clients via HTTP. Connect Director accesses the configuration database though IIS.

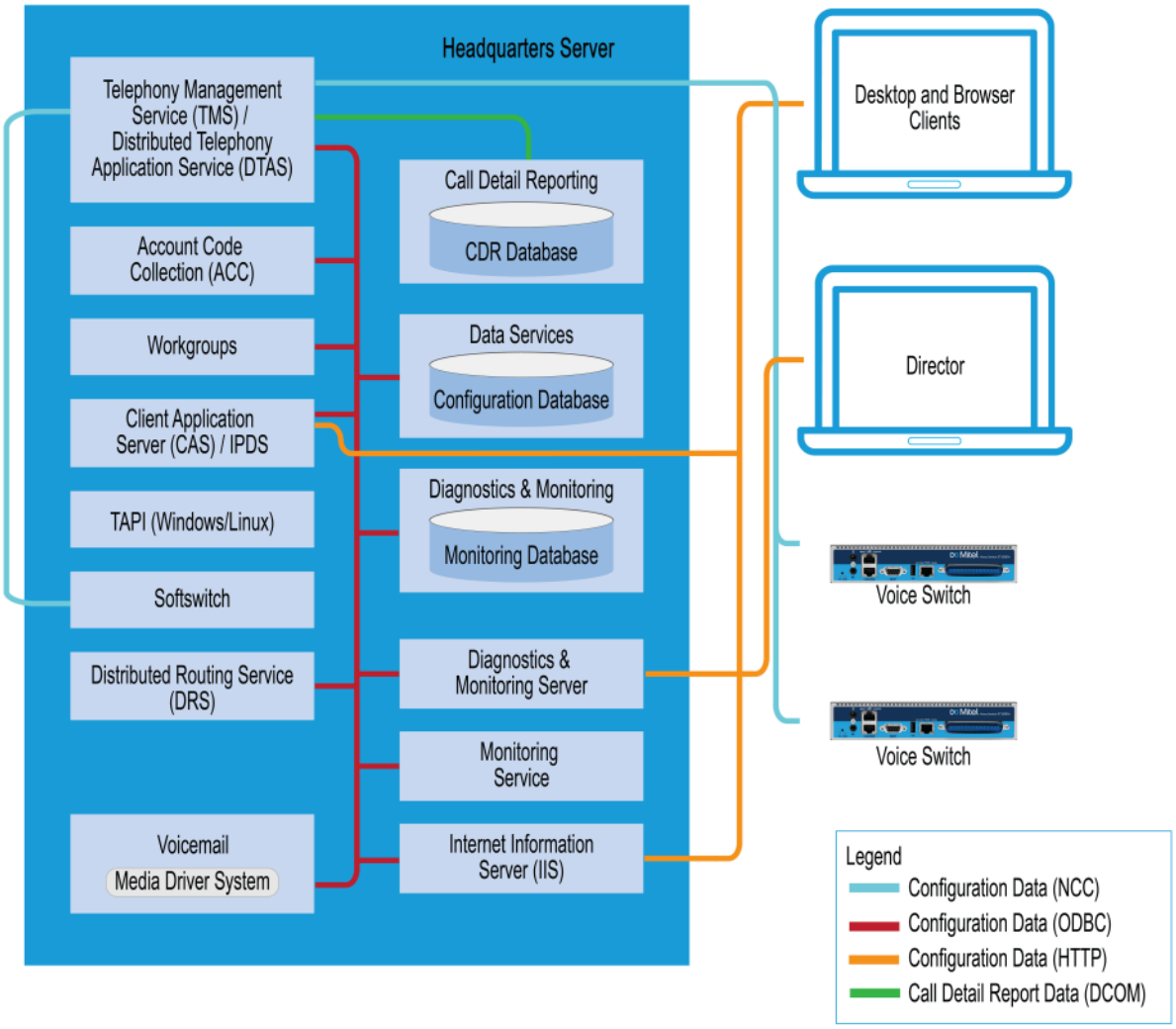
You can use the Component Service Manager to view COM objects installed by the software. Component Service Manager is located in the Administrative Tools folder available from the Windows Start menu.

Do not change any permission or security settings for Connect components.

Features accessible from the voice mail phone interface that require write access to the database, such as Extension Assignment and Call Handling Mode changes, are not supported during an outage unless a local distributed database instance is in use.

Server Database Communications shows how Mitel services use Open Database Connectivity (ODBC) to access the configuration database, and thus maintain the system status.

Figure 5: Server Database Communications



4.1.4 Services

The Connect system relies on a variety of services to perform processes within the system. This section describes some of the key services.

4.1.4.1 Internet Information Service (IIS)

The Mitel server uses IIS to implement Connect Director's browser-based interface. You can use the Internet Services Manager to view the configuration of the Connect Director Web site. Mitel installs the site configuration using the installation program. Changing the default configuration installed by Mitel might cause Connect Director or other system components to fail.

4.1.4.2 FTP Services

Both the Headquarters and DVS servers make an FTP service available for fallback use by Voice Switches. While this does not have to be active on a continuous basis, the FTP site needs to be active for the fallback capability to work. Mitel recommends that the FTP site always be available.

The Mitel server also uses the FTP service to transfer prompts between applications.

Legacy IP phones use the FTP server to download configuration information and the application program when they boot. (IP 400-Series phones uses HTTP for this purpose.) The IP phones download these files from the server that is controlling the switch managing the IP phone.

To view the FTP site properties, use the Internet Services Manager.

4.1.4.3 HFS Services

The HTTP File Server (HFS) services is used by MiVoice Connect service appliances and phones to upload log and backup files.

4.1.4.4 SMTP Services

The software uses SMTP to send email notifications (for example, when new client software is available for installation). The voice mail system uses SMTP to transport composed messages between the distributed servers. SMTP services are also required for the Event Notification feature to work.

The installer does not make any specific configurations to the SMTP service. The applications deposit outbound email on the server for forwarding elsewhere.

For proper operation of Mitel services, the hosting enterprise must have an email server configured to accept and forward SMTP mails. This is usually the exchange server or the primary email server of the company.

4.1.4.5 Client Application Server (CAS)

The Client Application Server (CAS) is a proprietary protocol that uses HTTP messages to communicate between client PCs and Mitel servers. The CAS protocol communicates configuration updates such as call handling mode settings and Outlook integration. Network devices, such as firewalls and proxies, must not automatically close these pending requests.

Note:

If the System Directory email address begins with digits, the CAS server response to a voicemail query returns stating incorrect email address.

4.1.4.6 IP Phone Services

IP phones in a Connect system rely on two services running on the Headquarters server and distributed servers:

- **Sysmgmt:** Runs on all servers.
- **IP Phone Display Service/CAS:** Runs on all servers.

The IP Phone Configuration Service (IPCS) manages the IP phone configuration process, including configuration file downloads and the database updates.

IP Phone Display Service/CAS controls any actions by the IP phone display not controlled by the device's firmware or switches.

4.1.5 Applications

This section provides information about applications that run on the Mitel server.

4.1.5.1 Event Watch

Event Watch monitors the NT Event Log and delivers email notifications of selected events. Event notifications are configured from the Events Filter page in Connect Director.

For more information about Events, see the *MiVoice Connect System Administration Guide*.

4.1.5.2 Call Detail Reporting (CDR)

TMS uses COM to write call data to the Call Detail Report database. The Connect system tracks all call activity and generates call detail records into a database as well as into a text file on the Mitel server. The call detail records are used to generate CDR reports.

For more information on Call Detail Reports, see the *MiVoice Connect System Administration Guide*.

4.1.6 Call Control Communications

The servers provides call control for server applications and for Distributed Routing Service (DRS).

4.1.6.1 Telephony Application Programming Interface (TAPI)

The Mitel server and its client applications use a Telephony Application Programming Interface (TAPI) to direct applications and provide the system with call control Server TAPI Communications

The TMS application service acts as the TAPI service provider and is responsible for managing the system's TAPI lines and routing information to other applications. When TMS starts up, it creates a TAPI line device for each endpoint in the system. Access to these TAPI lines is provided through Remote TAPI

Service Provider (RPCTSP.tsp). This is installed on each of the systems that run Connect clients (such as the Connect client), HQ, and distributed servers. Every application with access to these TAPI lines receives new calls, call state information, and line device information from TMS via RPCTSP.tsp.

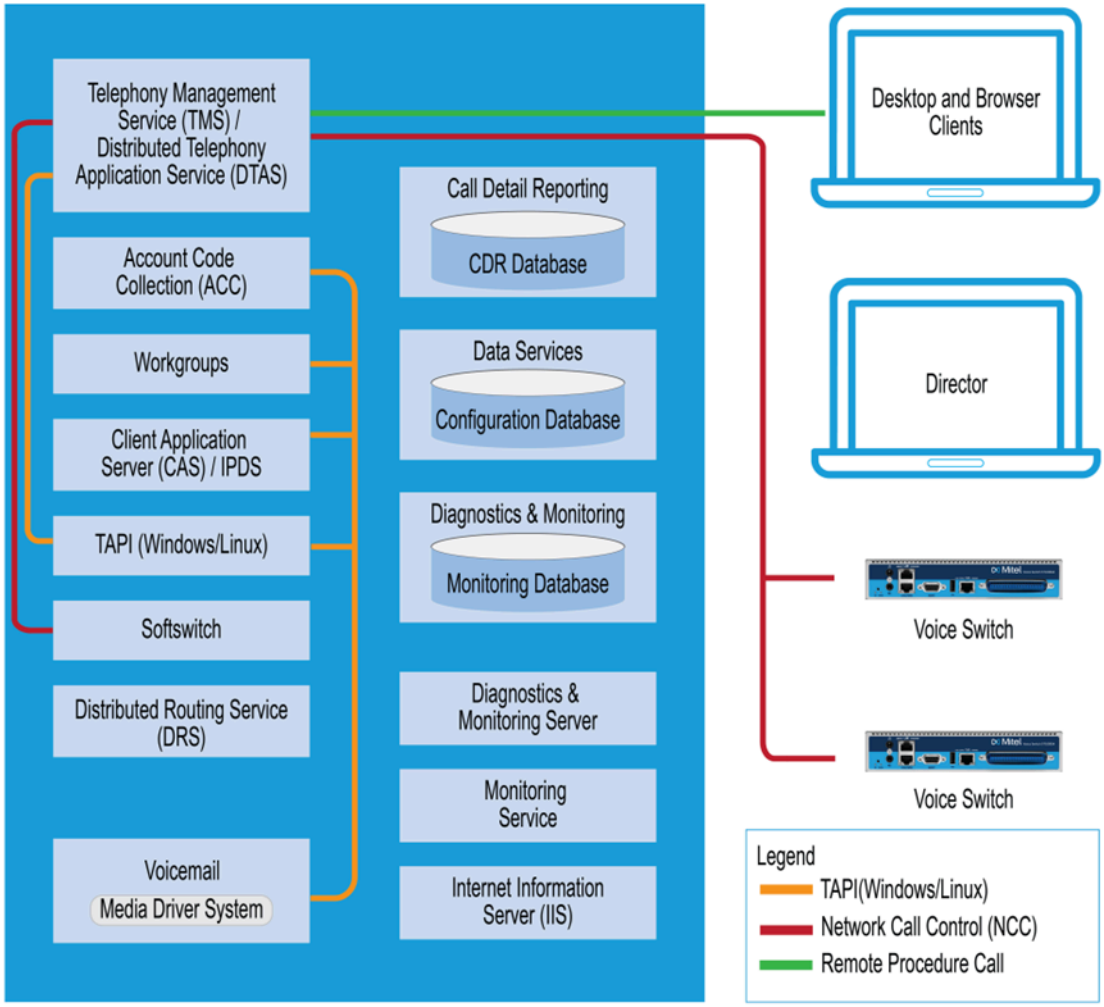
The Telephony Management Service (TMS) uses NCC to communicate with the Voice Switches, and a combination of RPC and Windows sockets (Winsock) to communicate with a Remote TAPI Service Provider.

To view the properties of the Remote TAPI Service Provider, open the Phone and Modem Options tab in the Windows Control Panel.

Note:

Never modify the TAPI properties of the Remote TAPI Service Provider. Modified TAPI properties can cause Mitel clients or applications to fail.

Figure 6: Server TAPI Communications



4.1.6.2 Distributed Routing Service (DRS)

DRS on each server provides routing information when switches cannot route the call in the local site and require intersite call routing information. An enhanced SIP protocol is used for communications between the switch and DRS. (See the Server Call Control and Media Communicationsfigure in the Media Communications on page 21 section)

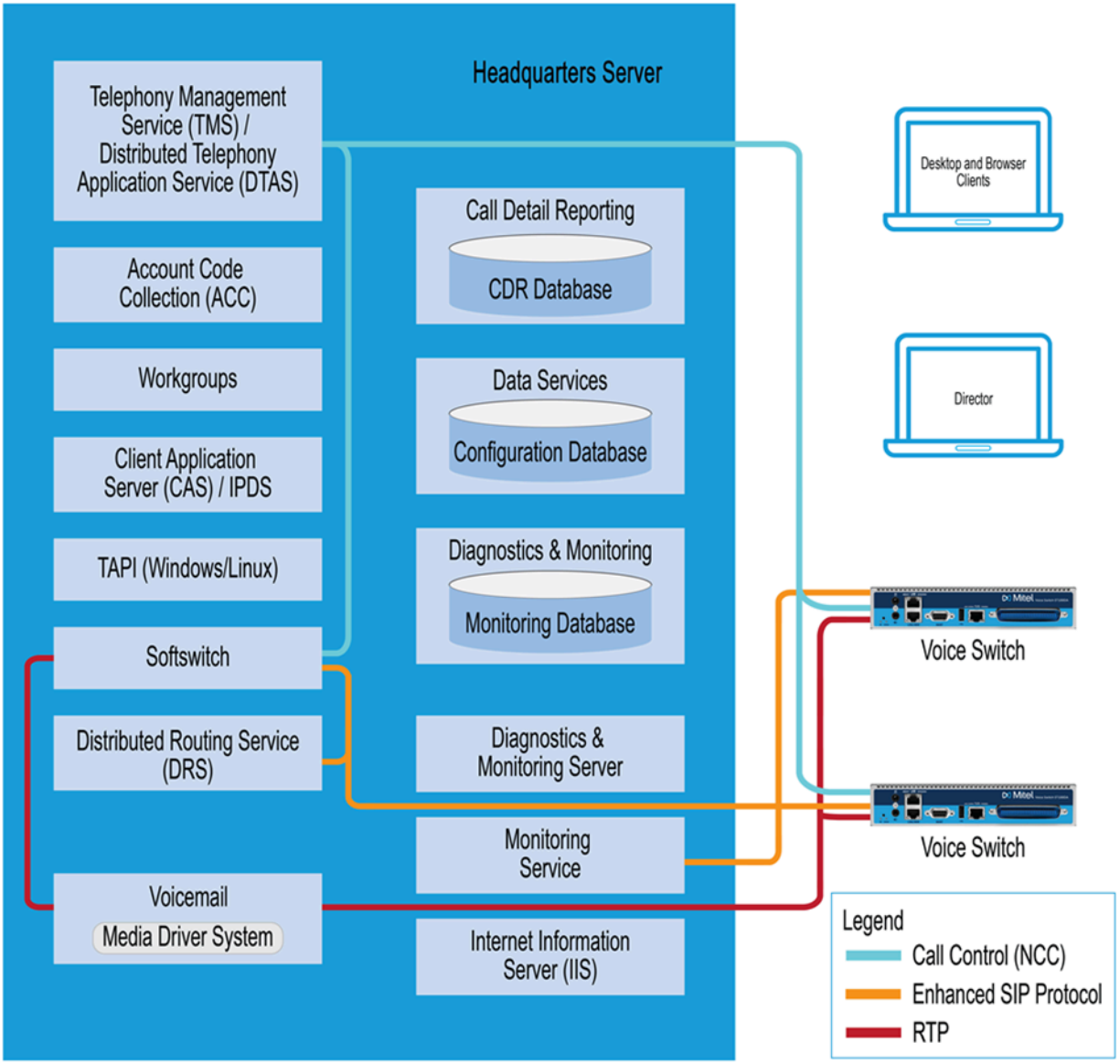
4.1.7 Media Communications

Media, from the perspective of the server, connects voice mail and the Auto-Attendant to switches and endpoints via the media driver. Media travels through the Connect system using Real-Time Protocol (RTP).

A voice mail message is normal RTP traffic, unless it is a recorded voice mail message moving from one server to another. Voice mail media streams conform to the G.711 codec. If a switch or IP phone is configured to use G.729 or ADPCM (for example, for an intersite call), a media server proxy is used to transcode between G.729/ADPCM and G.711. Since the media server proxy is a switch resource, there are a limited number of G.729 proxies. If there are insufficient G.729 proxies, then ADPCM is used instead.

Server Call Control and Media Communications shows the switch-to-switch call control and media communications flows.

Figure 7: Server Call Control and Media Communications



4.1.8 Integrated Server Applications

There are several integrated TAPI applications running on the server. These applications use TAPI to send and receive call control information, and can also manipulate calls. These applications also use ZIN Manager and ODBC to access and update the configuration database.

4.1.8.1 Voice Mail

Voice mail is a TAPI application that supports 254 simultaneous voice mail or Auto-Attendant connections. The voice mail system on the Windows HQ server and Windows Distributed Voice Server (DVS) uses SMTP to transport composed messages between the distributed servers. The Linux DVS uses Qmail. Media streams to voice mail use RTP packets to send media.

Voice messages are stored on the server's hard drive in the VMS MESSAGE subdirectory of the Shoreline Data directory. Voice mail messages are stored as `.wav` files. To help you calculate storage requirements, one hour of messages requires approximately 30 MB of disk space.

The voice mail application consists of the following services: Port Manager and Mail Server. The Port Manager uses TAPI to interact with TMS. The Connect system also supports linking to legacy voice mail systems using AMIS and SMDI protocols.

4.1.8.2 Distributed Voice Mail

If the Headquarters server loses network connectivity, the distributed voice mail application allows softswitches on Distributed Voice Servers to continue handling voicemail calls and access the auto-attendant.

During an outage, users can access voice mail only through their phone interface. Those using the Connect client are not able to access their voice mailboxes until connectivity is restored.

Voicemail messages to mailboxes hosted at other sites are stored and forwarded when connectivity to the destination voice mail service is restored.

4.1.8.3 Workgroups

Workgroups is an integrated Automated Call Distribution (ACD) application. Running on any HQ or DVS server, this TAPI application is responsible for routing and queueing calls directed to workgroups.

In the larger enterprise, there may be small- to medium-sized groups working together as a contact center. The Contact Center Solution is a server-based ACD and reporting package that includes the ability to queue and distribute calls, and provide agent and supervisor functions, as well as deliver reports on the call center activity.

4.1.8.4 Account Code Collection Service (ACC)

The Account Code Collection Service (ACC) is a TAPI application running on any HQ or DVS server. When it is enabled, it allows account codes to be required or optional for outbound calls. When a restricted PSTN call is attempted, and account code collection is enabled, the Voice Switch redirects the call to ACC.

Account Code Collection Service is responsible for:

- Prompting the user for the account code
- Collecting and validating the account code
- Attaching the account code to the call for reporting purposes
- Performing a blind transfer to the external number

If the managing server is down, or ACC is not available, the call is directed to the Backup Auto-Attendant.

TMS provides the following information to ACC:

- Dialed number
- User group

- Backup Auto-Attendant and correct menu number
- Account Code settings for each user group

CAS exposes a list of account code names and numbers within the Connect client to facilitate the account selection process for the user.

4.1.8.5 Softswitch

Softswitch is used to host virtual users who are not assigned a physical telephone port on any Voice Switch. The softswitch for each HQ or DVS server hosts all voice mail, Auto-Attendant, and Workgroup extensions as well as route points managed by that server.

When softswitch is down loss of connectivity to the softswitch makes the voice mail, Auto-Attendant, Workgroups, and route points supported by that softswitch unavailable.

The softswitch receives and transmits information using the same communication paths and protocols as the other switches in the system.

A softswitch is automatically created for every server added to the Connect system. By default, the name of the softswitch is the same as the name of the Mitel server hosting the switch, as specified on the Application Server page in Connect Director.

4.1.9 Server Maintenance

Server software upgrades take place any time new software is loaded. The Setup program detects the installed software and automatically converts any system files or databases.

Upgrading from one minor version to another automatically converts any system files or databases. Minor upgrades typically add incremental features to the software or correct product defects found in previous releases.

4.2 Diagnostic and Troubleshooting Information

The Connect system provides information about the operational status of the servers and services, as well as diagnostic and troubleshooting tools to resolve an event or error that might occur while the system is running or during installation.

The following tools are described in this section:

- Monitoring tools included in Connect Director
- Installer logging
- Event log
- system logs
- cfg utility

4.2.1 Monitoring Servers through Connect Director

You can monitor the components in your Connect system in the Diagnostics & Monitoring system that you can access through Connect Director. With the Diagnostics & Monitoring system, you can monitor server status and other aspects of the Connect system. For more information, see the *Monitoring and Diagnosing* chapter in the *MiVoice Connect System Administration Guide*.

You can also view system and application events in the Event Log, which you can access through Connect Director.

4.2.2 Installer Logging

Some logging information can be gathered by the installer technology native to the operating system. Mitel includes added proprietary code that provides more detail in the log files to assist you in troubleshooting software installation. This proprietary code adds information about calls to the installer and return values from all custom action functions invoked by the installer.

Log files are generated in the user profile temp directory and start with `msi` and end with `.log`. Sort the directory if there are many log files or if there is any doubt as to which log file to look at.

4.2.2.1 Configuring Installer Logging

Perform the following procedure on the server that is going to run the software before the software is installed on the system:

1. Click on the **Start** bar and select **Run**.
2. Type **regedit** to access the **Registry Editor** window.
3. Navigate to the following path:

   `[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]`
4. Right-click in the blank pane at the right of the window and select **New** > **String Value**.
5. Name the file **Logging**.
6. Right-click on the file and select **Modify**.
7. In the **Value data** field, type **voicewarmup!**
8. Click **OK**.

There are no obvious signs that installer logging is enabled. However, after you have enabled the feature (and performed a software installation), you can check the temp directory for log text files at the following location:

`C:\DocumentsandSettings\username\LocalSettings\Temp`

Note:

- After installer logging is enabled, you might see installation logs in the temp directory for other non-Mitel software installations.
- To view the log files, you might have to change the setting for the file view features in Windows Explorer so that hidden files, directories, and file extensions are visible.

4.2.3 Using the Event Log

The Connect system uses the Windows Event Log to report information and errors. Use the event logs in conjunction with the Diagnostics Monitoring system to determine the overall health of the system. The event log gathers information about event history. For example, the event log may provide information about an overnight SGT1 outage that was corrected but is no longer evident in the Diagnostics Monitoring system.

Each system task reports when it starts and stops. These messages can be helpful in determining whether the system started correctly. Events, such as switches losing connection to the server or rebooting, are also reported. For a list of all event codes, see Event Types on page 275.

4.2.4 Using the System Logs

The Connect system stores engineering-level log files that record transaction information about every event in the Connect system. The logs are used to help Mitel with debugging problems that may arise during system operation. In most cases, these logs require the assistance of Mitel Customer Support to understand.

Two utilities, one with a graphical user interface and the other with a command-line interface, can be used to automate the collection of server logs, Windows (OS) logs, and databases. Both applications have the same functional capabilities and offer two different ways for accomplishing the same tasks.

4.2.4.1 Using the Graphical User Interface

The GUI can be executed from MS Windows or from a command window.

1. Launch the graphical version of the Server Log Collection Utility by clicking on the following executable:

   ```
   <ShoreTel install directory>\slogWin.exe
   ```

   <ShoreTel install directory> is the location of the server files. The default installation location of server files is as follows:

   ```
   C:\Program Files\Shoreline Communications\Shoreware Server
   ```

   The Server Log Utility displays the Banner panel.
2. Press **Next** to proceed.

3. On the **Date Selection** panel, specify the dates to collect log files. The program collects files only for a contiguous date set. The default selection is today's date.
4. Press **Next** to proceed.
5. On the **Log Selection Method** panel, specify the log file selection method and the destination directory.

   - To select all log files for inclusion in the archive, select the **Default** radio button. Press **Next** to begin archiving all available log files.
   - To manually select the desired log files for inclusion in the archive, select the **Custom** radio button.Press **Next** to open the **Log Selection** panel. This panel prompts you to select the log files for inclusion in the archive.
   - To select the **Destination Directory**, press **Browse**.

   Note:

   The destination directory is listed above the **Browse** button

   The program opens a **Browse for Folder** panel for selecting the destination directory.
6. On the **Log Selection** panel, specify the log files that the program archives. System information might be gathered separately.

   Note:

   The utility does not display this panel if you select Default in the Log Selection Method panel.

   - The four options at the top of the panel select multiple log files. When you select one of these options, all log files included by that selection are selected and cannot be edited.
   - Select **ALL** to include all files in the archives.
   - All available log files are listed below the first four options at the top of the panel. You can select one file, all files, or any combination of files
7. Press Next to begin saving log files.

   The utility displays the **Archiving** panel while the program saves the selected files. The **Next** and **Back** buttons are disabled while the program is saving the files. The **Cancel** button remains available.
8. Press **Next** after the Save process is completed to display the **FTP Upload** panel. After archiving the files, the program presents an option to upload the archive file to a remote FTP server.

   After archiving the files, the program presents an option to upload the archive file to a remote FTP server.
9. Enter valid settings for all FTP parameters, then press **Upload**.
10. Press **Next** to proceed to the **Completion** panel.

    The Completion panel indicates that the log files and databases were successfully archived to the specified directory.
11. Press **Finish** to close the utility.

4.2.4.2 Using the Command-Line Application

The command-line version of the Server Log Collection Utility provides the identical functionality as the GUI from the windows command prompt.

The following program launches the Command Line version of the Server Log Collection Utility:

```
ShoreTel install directory>\ServerLog.exe
```

Note:

`ShoreTel install directory>` is the location of the server files.

The default installation location of server files is as follows:

```
C:\ProgramFiles\Shoreline Communications\Shoreware Server
```

Command Line Parameters and Description lists and describes available command-line parameters.

Table 2: Command Line Parameters and Description

Command	Description
`d destDir>`	Set Destination Directory. Note: This is a mandatory parameter.
`-d1 date1>`	Set Start Date. date1 – mmddyy.
`-d2 date2>`	Set End Date. date2 – mmddyy.
`If -d1 is not specified`	date1> and date2> are both set to the current date.
`If -d1 is specified,`	d2 becomes a mandatory parameter where date2> must be greater than or equal to date1> and less than (date1> + 7 days).
`-CDRDB`	Retrieve current CDR Database Log

Command	Description
-CONDB	Retrieve current Configuration Database Log
-CRASH	Retrieve Crash Dump Logs
-NTEL	Retrieve NT Event Logs
-TRIG	Retrieve Trigger Logs
-DB	Retrieve Database Logs
-DIR	Retrieve Director Logs
-DS	Retrieve DataServices Logs
-WGS	Retrieve Workgroup Server Logs
-VM	Retrieve Voice mail Logs
-IPDS	Retrieve IPDS Logs
-IPCS	Retrieve IPCS Logs
-DRS	Retrieve DRS Logs
-CSIS	Retrieve CSIS Logs
-ACC	Retrieve ACC Logs
-CDR	Retrieve CDR Logs
-TAPI	TAPI Logs

Command	Description
-DTAS	Retrieve DTAS Logs
-SS	Retrieve SoftSwitch Log
-TMS	Retrieve TMS Logs
-ALLCONDB	Retrieve All Configuration Database Logs
-ALLCDRDB	Retrieve All CDR Database Logs
-ALLWIN	Retrieve All Current Windows Logs (Mitel, NT Event, Crash Dump)
-ALLDBS	Retrieve All Database Logs (CDR, Config)
-ALLLOGS	Retrieve All Current Logs
-ALL	Retrieve All retrievable logs and databases
-f	Upload the archive to the specified FTP server
path> user> pass>	Specifies the FTP destination location when uploading the archive to an FTP server
-v	Display version number of command line program, then exit
-h	Display name and description of command line parameters, then exit

Examples

The following command line copies Voice Mail logs generated between 2 March 2023 and 6 March 2023 to `C:\LogsDir` directory:

```
ServerLog.exe -d1 030223 –d2 030623–VM –d “C:\LogsDir”
```

The following command line copies all voice mail logs generated today:

```
ServerLog.exe -VM –d “C:\LogsDir”
```

The following command line generates an error message because only one date is specified:

```
ServerLog.exe -d1 030223 –VM –d “c:\LogsDir”
```

4.2.5 Using the Trunk Test Tool

The Trunk Test tool is a TAPI application that monitors real-time activity on a trunk. You can find the tool in the program folder. The Trunk Test tool allows you to select a trunk to view by site, rather than viewing all trunks across your enterprise.

The tool is divided into two sections. The top section lists all the trunks in the system and their current status. The bottom section gives real-time monitoring information about the currently highlighted trunk. If this tool remains running on the server with an excessive number of lines selected, the server might have performance problems.

The interface for the Trunk Test Tool contains the following components:

- The **File** menu allows you to save log information to disk or print it.
- The **Edit** menu allows you to copy and paste data from the **Trunk Test** window.
- The **View** menu allows you to turn on and off the status and toolbars, and open the **Trunk Helper Settings** dialog box. The **Trunk Helper Settings** dialog box allows you to set the server you want to monitor, select an extension to dial out with, and set the number of lines of data to collect for each trunk.
- The **Operations** menu allows you to make or drop calls, view the properties of selected trunks, place trunks in service, and remove them from service. You can also access this menu by right clicking a selected trunk.
- The **Help** menu displays the version number of the Trunk Test tool.

4.2.6 Using the cfg Utility

The cfg utility is a command-line tool that provides detailed information about the voicemail application. It is available on all voicemail servers, including Windows DVS, Linux DVS, and voicemail-enabled switches. The `cfg.exe` file resides in the following path:

```
C:\Program Files\shoreline communications\Shoreware server
```

To start cfg:

1. Open a command line window pointing to the `\shoreline communications\Shoreware` server directory.

2. Type **cfg** and press **ENTER**.

   When you see the prompt **/*Local*//->**, cfg is ready.

   All commands are entered at the above prompt. Results are displayed in the command line window or in the voicemail logs.

> **Note**:
>
> Some `cfg utility` commands might damage the system if used incorrectly. Make sure you understand the commands before you use them.

cfg Commands lists and describes the commands available through the cfg utility. Variables are shown in italics.

Table 3: cfg Commands

Command	Parameters	Description	Comments
`call p`	p – v	Make a call from the voicemail application and play a prompt.	
`closem`		Close the open voicemail box.	
`dmask 0x`	0x – mask hex	Set voicemail debug mask in hex.	To see a list of available flags, enter without a parameter.
`exit`		Leave cfg.	
`laam t`	t – • 1 – DID • 2 – DNIS • 3 – Trunk	List Auto-Attendant menu mapping.	Displays mapping of trunks to Auto-Attendant menus.

Command	Parameters	Description	Comments
`lall f`	f – 1 for more details	List all mail boxes in the system.	Enter without “1” for a summary of system mail boxes and with "1" for more detail.
`lamp m f`	m = mail box f = (1 = on, 0 = off)	Turns the message waiting light on/off for a specified mail box.	
`list pb b`	b – (0 – last name, 1 – first name)	Dump dial by names directory to the voice mail log.	

`lmbox`
 	
`f`
	f = 1 for more details	List mail box information.	Enter without “1” for a summary of system mail box information, including messages IDs.

`lms`		List mail box schedule.	

`lmsg`
 	
`m`
	m
	
	– message ID
		List details about a specific message.	Message IDs can be found by using lnbox.

`loadc`		Load all voicemail configuration from the database.	
`loadm`		Load all mail box configuration from the database.	Requires that a mail box be open when you issue the command.
`lserv`		List information about all servers.	
`lsys`		List all voicemail system parameters.	

Command	Parameters	Description	Comments
`lsmtp`		List status of distributed voicemail.	
`ltapi`		List status of TAPI lines opened by voicemail.	
`msinfo`		Dump voice mail internal table to the voicemail log.	
`openm #`	# – mail box	Open specified mail box.	
`psinfo`		Dump port server information to the voicemail log.	
`purge`		Remove message in the deleted queue.	Requires that a mail box be open when you issue the command.

`sh`
 	
`str`
	str
	
	– string
		Search help for a string.	Searches only from the beginning.

`starth`		Remove old deleted messages.	
`symwi`		Run message waiting indication synchronization.	Sends current MWI status to all phones in the system.
`ver`		List cfg version.	
`?`		List help commands.	

4.3 Windows Postmortem Debugging

Note:
Mitel recommends using Windows Error Reporting on the Microsoft Windows operating system that is used for MiVoice Connect applications.

For Windows 2012 and later, refer to the following Microsoft article for information about enabling postmortem debugging:

https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/enabling-postmortem-debugging

To enable Dr. Watson:

1. Open the **Control Panel** and then double-click **System**.
2. Click on the **Advanced** tab.
3. Click **Error Reporting** (Error Reporting Window). Disable it, or if you choose to enable it, leave it enabled just for the Windows operating system. Leave the **Programs** check box clear.

   This must be done whenever a new machine is built or ghosted.
4. Install Dr. Watson from the command line by typing **drwtsn32 -i**.
5. Run `drwtsn32` to configure it. A window is opened (similar to the one shown in Configuring Dr. Watson).
6. Under **Crash Dump Type**, select the **Mini** radio button.
7. Select the **Visual notification** check box. This ensures that you are aware when a dump occurs.
8. Select the **Create Crash Dump File** check box.
9. Optionally, in case the dump file might be overwritten, it may be helpful to enable the following options by selecting the associated check boxes:
   - **Dump Symbol Table**
   - **Dump All Thread Contexts**
   - **Append to Existing Log File**
10. Click **OK** to store your changes.

To collect Dr. Watson dumps:

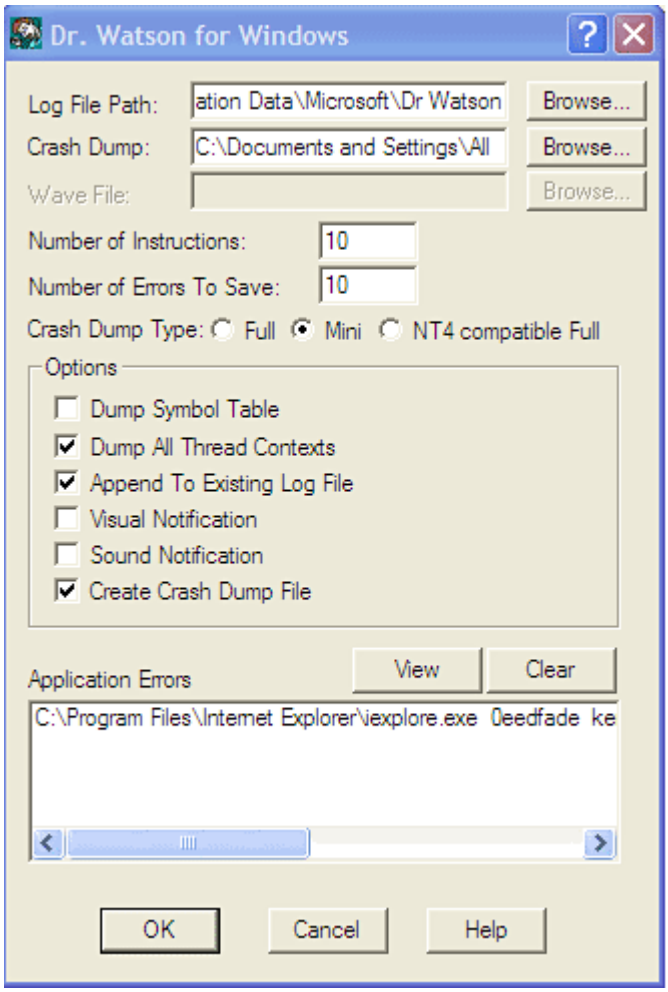
- Dumps for a logged in user appear under:

  `C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson`
- Dumps for services appear under:

  `%systemroot%\PCHEALTH\ERRORREP\UserDumps`

Figure 8: Error Reporting Window

Figure 9: Configuring Dr. Watson



4.4 Services

The Mitel server is made up of multiple processes working together to provide applications that include voicemail, Connect Director, and Workgroups. Each process runs as a Windows Service, which starts automatically when the server starts.

Service Descriptions lists and describes each service and its underlying process. All services run on the Headquarters Server. Services that also run on distributed voice servers are marked in the “Distributed Server” column.

Table 4: Service Descriptions

Service Name	Service ID	Process	Description	Distributed Server
ShoreTel Authenticator Service	ShoreTel-AuthenticatorService			
ShoreTel Bootstrapper Service	ShoreTel-BootstrapperService			
ShoreTel Connect Sync Service	ShoreTel-ConnectSync			
ShoreTel Key Notifier	ShoreTel_KeyNotifier		This service pushes the authentication keys into the web socket server (ST-WSS) so that it can complete authentication of its clients.	
Call Accounting	ShoreTel-CDR	TmsCDR.exe	Records call information (call accounting information, call queuing data, and media stream data) and writes it to the CDR database	

Service Name	Service ID	Process	Description	Distributed Server
ShoreWare CSIS Server	ShoreTel-CSISSVC	CSISSvc.exe	Provides legacy clients (ST12 or earlier) with an interface to the Mitel server	X
ShoreWare CSIS Virtual Machine Server	ShoreTel-CSISVMSVC		Provides notification for clients and voicemail	
ShoreWare Database Update Server	ShoreTel-DBUpdateSvc	DBUpdateSvc.exe	Accepts database updates from remote computers	
ShoreTel Connect Director	ShoreTel-Director		Provides diagnostics and monitoring capabilities for Connect system components	
ShoreTel Connect Director Proxy	ShoreTel-DirectorProxy		Provides a Web Server and a reverse proxy for the Director Service	
ShoreWare Distributed Routing Service	ShoreTel-DRS	DRS.exe	Allows the Connect system to scale beyond 100 switches When active, this service provides location information for routing intersite calls and additional routing information for trunk group selection.	X

Service Name	Service ID	Process	Description	Distributed Server
ShoreWare Event Service	ShoreTel-EventSvc	CEService.exe	Distributes events to Mitel applications and services	
ShoreTel-IMAA Service	ShoreTel-IMAA	IMAAService.exe	Collects archives from IM servers into a central location; runs on HQ server.	
ShoreWare Event Watch Server	ShoreTel-EventWatch	EventWatch.exe	Monitors the NT Event Log and delivers email notifications of selected events	X
ShoreTel Monitoring Service	ShoreTel MonitoringService		This service enables the monitoring processes necessary for the Diagnostics Monitoring system.	
ShoreWare Voice Mail Message Server	ShoreTel-MailServ	MailServ.exe	Provides user mailbox capabilities, AMIS features, and system auto-attendant menus. It also manages the voicemail message store.	X
ShoreTel-MYSQLCDR	ShoreTel-MYSQLCDR		This service is a database process related to the Call Detail Record database.	

Service Name	Service ID	Process	Description	Distributed Server
ShoreTel-MYSQLConfig	ShoreTel-MYSQLConfig	mysqld.exe	This service is a database process related to the configuration database for Connect Director.	
ShoreTel-MYSQLMonitor	ShoreTel-MYSQLMonitor		This service is a database process related to the monitoring database for the Diagnostics Monitoring system.	
ShoreWare Client Application Server	ShoreTel-IPDS	IPDS.exe	Manages voice mail clients and IP phone display not controlled by the device's firmware or switches. Responsible for managing changes made to the database by the clients. X	
ShoreWare Notification Server	ShoreTel-Notify	TriggerServer.exe	Notifies server applications of changes to the configuration	X
ShoreWare Voice Mail Port Manager	ShoreTel-PortMgr		Service component of the voice mail system	

Service Name	Service ID	Process	Description	Distributed Server
ShoreWare Port Mapper	ShoreTel-Portmap	PortMap.exe	Initiates RPC communication connections between the Telephony Management Server (TMS) and Voice Switches	X
ShoreWare Remote Logging Service	ShoreTel-RemoteLogSvc	LogService.exe	Accepts logging from remote computers	
ShoreTel Remote Packet Capture Service	ShoreTel-RPCAP		Runs remote packet capture operations for diagnostic purposes	
ShoreTel-SAMS	ShoreTel-SAMS		Provides services to Connect Director application	
ShoreWare Software Telephony Switch	ShoreTel-SoftSwitch	VTSMain.exe	The SoftSwitch hosts call endpoints for voice mail, Workgroup, route points, and other IVR extensions. Virtual users are hosted on the Headquarters SoftSwitch.	X
ShoreTel System Management Service	ShoreTel-SysMgrSvc	SysMgrSvc.exe	Provides IP phone registration and other functions	

Service Name	Service ID	Process	Description	Distributed Server
ShoreWare Telephony Management Service (TMS)	ShoreTel-TMS	Tms.exe	The telephony platform for Mitel applications, services, and third-party TAPI applications	X
ShoreWare Transport Server	ShoreTel-TransportSvc		Provides transport services for Mitel applications and services	
ShoreTel Voice Mail Synchronizer	ShoreTel-VmEmSync	VmEmSyncSvc.exe	Provides voicemail and email synchronization	
ShoreTel Web Framework Server	ShoreTel-WebFrameworkSvc	WebFrameWork.exe	Provides support for Connect client and interactions with Client Application Service	
ShoreWare Workgroup Server	ShoreTel-WGSvc		Manages workgroups and queues	
CMCA Service		CMCA	Conference bridge application	
File Transfer Service		FTService	Transfers files using SMTP (qmail) engine	
IM Service		IMService	XMPP-based Instant Messaging engine	
Media Service		STMedia/STTS	Media engine	

Service Name	Service ID	Process	Description	Distributed Server
QMail Service		QMailService	SMTP service on Linux servers	
Services Manager Service		SMgr	Services Manager for starting, stopping, and monitoring services	
SM Service		SMService	Backend service that enables service CLI access	

4.5 Connect Server File System

Server File System lists the directories where the Connect server installs its files.

The Windows System user and the IPBX user created by the Connect installer require full access to all the Mitel directories. All other users can be granted access on an as-needed basis.

Note:

The server installs files with default access permissions. System administrators might want to ensure a more secure environment.

To ensure the security of sensitive and/or personal information, confine access to the VMS and Database directories strictly to administrator, system, and IPBX users.

Table 5: Server File System

Directory	Description	Default Path
Mitel Server	Contains all server system files and dlls. This directory is located on the drive where program files are stored.	`drive>\Program Files\Shoreline Communications\Shoreware Server`
Connect Director	Contains all Connect Director Web site files. This directory is located on the drive where program files are stored.	`drive>\Program Files\Shoreline Communications\Shoreware director`
Presenter	Installed on systems with Conferencing Services. Contains the files, applications and dlls required to enable screen sharing capabilities for Web Conference Services. This directory is located on the drive where program files are stored.	`drive>\Program Files\Shoreline Communications\ShoreTel Presenter`
Shoreline Data	Contains all the dynamic information the server uses to run the system. This directory and all sub-directories may be saved as part of a backup and used for full system recovery.	`drive>\Shoreline Data`
Call Records 2	Contains all call record files and databases The MySQL database is ODBC compliant. Parameter settings required to access CDR records in the MySQL database include: • DRIVER – {MySQL ODBC 3.51 Driver} • SERVER – localhost (or the server where MySQL is installed) • DATABASE – Shorewarecdr • USER – st_cdrreport • password – passwordcdrreport	

Directory	Description	Default Path
Database	Contains the configuration database that stores all system configuration information	
dvs	Contains the files and configuration information used by the Linux Distributed Voice Server (DVS)	
Logs	Contains all debugging logs	`drive>\Shoreline Data \Logs`
Prompts	Contains copies of the auto attendant and workgroup menu prompts	`drive>\Shoreline Data \Prompts`
Scripts	Contains scripts for starting and stopping services that are used during system backup and restore.	• For HQ Server: `drive> \Program Files (x86)\Shoreline Communications \ShoreWare Server` • For Remote Server: `drive>\Program Files (x86)\Shoreline Communications \ShoreWare Remote Server`
SoftSwitch	Contains files needed to run the SoftSwitch	`drive>\Shoreline Data \SoftSwitch`
Templates	Contains configuration files needed for IP phones	`drive>\Shoreline Data \Templates`

Directory	Description	Default Path

VMS	Contains all the files and configuration information used by the voice mail system. The files in this directory and its sub-directories are very dynamic.
	
	Note:
	Never open these files. Opening any of the configuration files may cause the voice mail system to become corrupted in part or completely, and can cause loss of voice mail messages.
	
	• MESSAGE: Contains all voice mail messages as.wav files, along with an .enl pointer file for each message.
	• NetTempIn: Used by distributed voice mail servers
	• Servers
	• SHORETEL: Contains a subdirectory folder for each voice mailbox configured on the system. Each user, menu, and distribution list includes a mailbox. There are also system mail boxes for voice mail access and forwarding. Each of the sub-directories contain the names and greetings for that mailbox, as well as configuration and pointer files.
		`drive>\Shoreline Data \VMS`
		
		`drive>\Shoreline Data \VMS\MESSAGE`
		
		`local drive>\Shoreline Data\VMS\NetTempIn`
		
		`drive>\Shoreline Data \VMS\Servers`
		
		`drive>\Shoreline Data \VMS\SHORETEL`

Inetpub\ftproot	This is the default FTP directory installed by IIS.	`drive>\Inetpub\ftproot`

Directory	Description	Default Path
ts	Contains the boot files and system software for supported languages	
tsa	Contains the boot files and system software for all full-width voice switches	
tsb	Contains the boot files and system software for all Mitel ST-model switches	
tsk	Contains the boot files and system software for all half-width Voice Switch SG30, SG30BRI, SG50, SG90, SG90BRI, SGT1k, SGE1k, SG220T1, SG220E1, and SG220T1A switches	
tsk1	Contains the boot files and system software for all voice mailbox model switches SG50V, SG90V, SG90BRIV	
tsu	Contains the boot files and system software for the Service Appliance 100 (SA100) and Service Appliance 400 (SA400)	
tsv	Contains the system software for virtual phone and trunk switches	

4.6 Registry

The software uses the Windows registry to store various parameters used by the Connect system. These registry keys reside at the following paths:

- For 32-bit operating systems:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks`

- For 64-bit operating systems:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Shoreline Teleworks`

4.6.1 Maximum Transmission Unit (MTU) Size for Connections

The default Maximum Transmission Unit (MTU) setting for PPP (Point-to-Point Protocol) clients, VPN (Virtual Private Network) clients, PPP servers, or VPN servers running Routing and Remote Access on Connect systems is 1400. To change the MTU value, you must edit the registry. For further information, contact Mitel Technical Support.

4.6.2 Telephony Management Service (TMS)

A Connect server can be configured with a registry entry that TMS pushes to the server's managed switches. The registry entry typically configures and invokes some custom behavior in the switch. For example, when an administrator modifies the SwitchDebug value in the registry to configure the switch, TMS automatically reloads the value and pushes it to the managed switches. Other registry changes, such as CDRDataExpiration, are automatically reloaded by TMS so that TMS immediately starts using the new value.

When a registry change needs to be system-wide, the administrator must manually change the registry on every distributed server. On a large system, manual updates can be slow, repetitive, and error-prone.

To address this challenge, an administrator can configure a TMS registry entry on the HQ server, and then TMS automatically propagates the registry entry to all distributed servers. Each distributed server updates its local registry, which causes TMS to automatically reload its registry settings. Each distributed TMS then uses the new registry setting. If the registry setting is **SwitchDebug**, each distributed server pushes SwitchDebug to its managed switches.

It's possible to prevent updating a DVS, if needed. For example, this would be necessary when upgrading a system where a DVS has different settings from the HQ server. You can prevent the registry setting from being pushed to DVS by putting its name into the TMS registry setting **NoHQPushSettings**.

Both Windows DVS and Linux DVS are supported. Voice Mail Switch and SA100/SA400 Server Appliance do not get any registry pushes.

Changes on Servers (and Clients)

An administrator can add the string value `HKLM\Software\Shoreline Teleworks\Telephony Management Server\Settings\NoHQPushSettings`, but it is not installed. When the administrator changes a pushable TMS registry setting, TMS creates a backup as follows:

- CDRDataExpirationBackup
- DRDataCacheSizeBackup
- LogAssertsAsNTEventsBackup
- SwitchDebugBackup
- LogEvent108Backup

Voice Switches 5

This chapter contains the following sections:

This chapter describes maintenance considerations for Voice Switches.

Overview

Voice Switches provide physical connectivity for the PSTN and analog phones, and logical connectivity for IP endpoints on a reliable, highly scalable platform for the call control software. The call control software runs on the operating system of the switch, for example Linux or VxWorks®.

Refer to the *MiVoice Connect System Administration Guide* for information about Virtual Switches.

Voice Switches Operating Systems shows the available types of Voice Switches and the operating systems they use.

Table 6: Voice Switches Operating Systems

SG Voice Switches	ST Voice Switches	Voicemail Model Voice Switches	Softswitches	Virtual Switches
Operating system is VxWorks®	Operating system is Linux	Operating system is Linux	Operating system is Windows or Linux	Operating system is Linux
Switch-to-switch communication via CLI commands.	Switch-to-switch communication via CLI commands.	Switch-to-switch communication via CLI commands.	Switch-to-switch communication via CLI commands.	Switch-to-switch communication via CLI commands.

All physical Voice Switches have flash memory that allows permanent storage of the call control software and configuration information. The Voice Switches have no moving parts (that is, no hard drive) other than a highly reliable fan. The switches include the necessary DSP technology to enable toll-quality voice with features such as echo cancellation, voice compression, and silence suppression.

TMS propagates configuration data from the database to each switch upon reboot of either TMS or the switch. The data sent is a subset of configuration data specific to that switch. TMS also maintains this data by propagating changes to the database to those switches affected by the change. The TMS/Switch configuration interface uses the same Network Call Control protocol that is used for other TMS/Switch communication. The

NCC protocol is based on Sun RPC. You can obtain the configuration data that TMS sends to any specific switch with a CLI command. For more information, see Commands Available Through CLI on page 72.

Switches share their switch-specific configuration with other switches in the system using the UDP-based Location Service Protocol (LSP). Switches keep current with other switches by propagating their changes and receiving them from other switches. For information about viewing switch-to-switch communications, see Commands Available Through CLI on page 72.

Note:

For physical Voice Switches, switch-specific configuration is in FLASH but configuration for other switches is in RAM. After rebooting, the switch syncs with LSP to keep current with these configuration changes.

The Voice Switches communicate call control information on a peer-to-peer basis. When Distributed Routing Service (DRS) is enabled, switches exchange LSP messages only with other switches at the same site. DRS communicates directly with the database to keep the database configuration current. TMS tells each switch how to find DRS as part of the configuration process described earlier. When DRS is enabled, switches generally give DRS an opportunity to resolve numbers, so that its more complete view of the system can be leveraged to find the best contact. If the switch knows where an intra-site extension is, it does not involve DRS.

For analog phones, the switch detects whether the phone is on or off hook, collects digits from the phone, and (based on digits collected) determines when a call is established. If necessary, the switch communicates with other switches (in some cases this may not be necessary, such as when the call is to an endpoint directly on the switch) to establish a call between the appropriate endpoints.

The switch acts as a media gateway for the PSTN and analog phones by encoding the analog voice and transmitting it to the other endpoint over the IP network using RTP. The switch also uses NCC to send events to TMS about digit collection, caller ID, call establishment, and so forth. TMS makes this information available to the server applications. These applications are not necessary for many calls (such as those between two phones or a trunk and a phone, which can be established with only the switches controlling the phones and trunks), but they can enhance the user experience. For example, Connect client can provide information about the call to the user's desktop.

After the call is established, TMS monitors the call and logs call information on the Call Detail Report (CDR) database.

5.1 Voice Switches Software Upgrades

You can see the status of Voice Switches using the Diagnostics and Monitoring system which is available through Connect Director. To view the status of the switch, you navigate to the **Maintenance** > **Status and Maintenance** > **Appliances** page. You also can view the status of all switches by site in the **Maintenance** > **Status and Maintenance** > **Sites** page.

When a switch update is required, the value in the Service column of the list pane on the **Maintenance** > **Status and Maintenance** > **Appliances** page is one of the following:

- **Firmware Update Available** indicates that a patch is available and an upgrade is required to load the patch. When a switch is in this state, it is fully functional and in communication with TMS and the other switches in the system.
- **Firmware Mismatch** indicates that you must upgrade the switch before it can communicate with the TMS server. A switch with mismatched firmware can communicate with other switches of the same version and manage calls, but cannot support server and client applications.

You can use the **Maintenance** > **Status and Maintenance** > **Appliances** page to upgrade the switch software, or you upgrade switch software manually with the burnflash utility.

5.1.1 Virtual Switches Software Upgrade Options

Complete the following steps to choose the system to use as a source for software upgrades for virtual switches:

1. In Connect Director, click **Administration** > **Appliances/Servers** > **Options** > **Appliance Options**.
2. The default upgrade option is Connect Managing Server. Select one of the options to download the software for future upgrades:

   - **Connect Managing Server:** Using this server is ideal when the companies that prefer connect software to be distributed from the HQ and managing Windows DVS. When this option is selected, Virtual Voice Switches and Service Appliances (Collaboration) will download their software from their respective managing HQs or Windows DVS servers. However, Linux DVS and appliances managed by Linux DVS servers will download their software from the HQ servers.

     Software Upgrade Option using Connect Managing Server provides a list of components and the software;download location for Connect Managing Server.

Table 7: Software Upgrade Option using Connect Managing Server

Component	Software Download from Location
Headquarters	Headquarters Server Installer (exe)
Windows DVS	Remote Server Installer (exe)
Linux DVS (virtual)	Headquarters only
Voice Switch (physical)	Managing Server (Headquarters, Windows DVS or Linux DVS)
Voice Switch (virtual)	Managing Server (Headquarters or Windows DVS) Exception: if Managing Server is Linux DVS, then Headquarters

Component	Software Download from Location
Service Appliance - SA100 or SA400 (physical)	Managing Server (Headquarters or Windows DVS) Exception: if Managing Server is Linux DVS, then Headquarters
Service Appliance (Virtual)	Managing Server (Headquarters or Windows DVS) Exception: if Managing Server is Linux DVS, then Headquarters
IP Phone	Managing Server (Headquarters, Windows DVS or Linux DVS)
Connect Client	Managing Server (Headquarters, Windows DVS or Linux DVS)

3. Define admin and root passwords. Each must be between 4 and 26 characters.

   Refer to the *MiVoice Connect System Administration Guide* for information about Virtual Switches.

5.1.2 Staged Upgrades for ST Family and Virtual Switches

In Connect, you can download the Connect software on Connect appliances before performing an actual upgrade. This speeds up the upgrade process as you do not have to wait for the software to be distributed to all the appliances across the network during the maintenance window. Models supporting a staged upgrade include:

- ST24A/ST48A
- ST50A/ST100A
- ST100DA
- ST1D/ST2D
- ST200/ST500
- Voicemail Switches (SG50V and SG90V)

Note:
Voicemail switches such as SG90V and SG50V do not support survivable voicemail and auto-attendant features at a remote (non-headquarters) site.

- Virtual Switches (IP Phone and Trunk)

These switches include dual partitions, which allows the switch to perform a background download to store upgraded firmware on a secondary partition. The switch then installs the firmware on the main partition when the download has completed and the switch is rebooted or an upgrade is initiated.

Note:

These switches also can be upgraded using the regular upgrade process as described in Upgrade Switch Software Without Using Staged Upgrade on page 55.

Note:

You can schedule the download. Refer to the steps below.

Complete the following steps to perform a two-stage upgrade on a Voice Switch:

1. Install **Staging_Firmware** software on the HQ Server and Windows DVS. This step will create a directory under `\inetpub\ftproot\Switches\<build number>`, and in the `<build number>`, directory there will be a switch folder (dvs, tsb,tsu,tsv).

   Note:

   The process of installing software from “Connect Managing Server” on the HQ Server and Windows DVS will add files for the following devices:

   - Linux DVS
   - Connect Edge Gateway
   - Virtual Switches
   - Service Appliance (Collaboration)

2. When the software is installed on the server, open **Connect Director** and click **Maintenance** > **Status and Maintenance** > **Sites**.
3. To upgrade all Voice Switches on a particular site, select the appropriate site.
4. Select **Download Software** in **Command**, and then select **Download to Appliance(s)** in the **Command** sub list.

Note:

The **Download Software** and **Download to Appliance(s)** command combination applies only to ST Generation Switches, Voicemail Switches, Virtual Switches, and Linux DVS. Refer to Upgrade Switch Software in One Step without Using Staged Upgrade;for information about upgrading SG Generation Switches.

5. Click **Apply**.
6. In the dialog box that appears, specify the following information:
   - **Version** — Select the firmware version you installed on the server in step 1.
   - **Sites**— This read-only information lists the switches associated with the site.
   - **Stagger Rate**— Select the number of devices you want to install on simultaneously.
   - **Schedule**— Select immediate or specify a date and time you want to install on.
7. Click **OK** to accept the download or select **Cancel** to cancel it.

Note:

If necessary, you can cancel a pending firmware download before the download has started:

a. Navigate to **Maintenance** > **Status and Maintenance** > **Sites**.
b. Select the appropriate site.
c. Select **Download Software** in **Command**, and then select **Cancel Pending Download** in the **Command** sub list.
d. Click **Apply**.

8. After the firmware download is complete, you can upgrade the software on your ST Voice Switches as follows:

   a. To upgrade all Voice Switches on a particular site, select the appropriate site.
   b. Select **Update Software** in **Command**, and then select **Update Appliance(s)** or **Update Appliance When Idle** in the **Command** sub list.
   c. Click **Apply**.
   d. Review the location and firmware version information that is displayed, and then click **OK** to accept the update or select **Cancel** to cancel it.

You can view the progress of the download and update processes in the **Maintenance** > **Status and Maintenance** > **Sites** page or the **Maintenance** > **Status and Maintenance** > **Appliances** page.

ST Voice Switches will either reboot immediately if you selected **Update**, or they will reboot when the upgrade is completed during idle time if you selected **Update When Idle**.

5.1.3 Upgrade Switch Software Without Using Staged Upgrade

1. Launch Connect Director.
2. Complete one of the following steps:
   - To select an individual Voice Switch for upgrade, navigate to the **Maintenance** > **Status and Maintenance** > **Appliances** page and select the appropriate appliance(s).
   - To select a site for which to upgrade all associated Voice Switches, navigate to the **Maintenance** > **Status and Maintenance** > **Sites** page and select the appropriate site.
3. Select **Reboot and Reset** in **Command**, and then select **Reboot Appliance(s)** or **Reboot Appliance(s) When Idle** in the **Command** sub list.
4. Click **Apply**.
5. In the **Confirmation** dialog box, click **OK**.

5.1.4 Manually Upgrading the Switch's Software

You can use the burnflash utility to upgrade a switch manually.

From the server command line, enter the `burnflash` command in this format:

```
C:\ Program Files (x86)\ShorelineCommunications\ShorewareServer>burnflash -s
<switch IP Address>
```

5.2 Voice Switch Boot Options

When a Voice Switch boots, it requires an IP address to connect to the network and an application program. Voice Switches are set to use a DHCP server for an IP address and to retrieve the application from the switch's flash memory.

Mitel;recommends using static IP parameters configured via the serial port, as this is much more reliable. If DHCP is to be used, Mitel strongly recommends using DHCP reservations for each switch so that the DHCP lease is not lost.

If a DHCP server is not available, you can set the IP address manually from the switch's maintenance port.

The standard method for booting a Voice Switch is to boot from the switch's flash memory. When a Voice Switch is first powered on, it reads the boot parameters stored on the boot ROM, which instructs the switch to load software from flash memory. When the software starts, it loads its configuration, which is also stored in flash memory.

5.2.1 SG Generation Switch Boot Options

Booting from FTP is available only when the switch cannot boot from flash memory. When you boot a switch from FTP, the operating system and software load from the FTP site are identified in the boot parameters. The loaded configuration is a configuration received from the TMS server.

If the switch fails to load the application from flash and does not have the IP address of the Mitel server, you can set the IP address and boot parameters by connecting to the maintenance port and using the configuration menu. The configuration menu allows you to set the IP address of the switch and enter the IP address of the Mitel server (boot host).

5.2.2 ST Generation Switch Boot Options

ST generation switches boot only from flash. You can download the firmware image to flash through FTP or HTTP. The loaded configuration is a configuration received from the TMS server.

If the switch fails to load the application from flash memory and does not have the IP address of the Mitel server, you can set the IP address and boot parameters by connecting to the maintenance port and using the configuration menu. The configuration menu allows you to set the IP address of the switch and enter the IP address of the Mitel server (boot host).

5.2.3 IP Address from DHCP

The switch sends requests for an IP address to the DHCP server ten times at increasing intervals. When the switch receives a response from the DHCP server, the boot process begins. If the switch fails to get an IP address from the DHCP server, it uses the last assigned IP address. The switch continues sending IP address requests to the DHCP server.

If the DHCP server sends a conflicting IP address while the switch is using an address from a previous state, the entire system restarts. Use long lease times to prevent to prevent this. Mitel recommends either static IP parameters or DHCP reservations.

If the switch does not receive an IP address from the DHCP server and an address is not available from a previous state, the switch continues polling the DHCP server until it receives an address.

5.2.3.1 Setting SG Voice Switch IP Addresses with VxWorks®

If the switch or voicemail-enabled switch is not configured with an IP address and fails to boot from flash, it cannot download the application and configuration from the FTP server;or the HTTP location in the case of ST switches. In this case, you can manually set the IP address and boot parameters from VxWorks® or Linux, which are accessible from the maintenance port. Boot parameter changes do not take effect until the switch is rebooted.

Note:

This command line interface is not available through Telnet.

Connecting to the Maintenance Port of a Voice Switch

1. Connect a straight serial cable between a personal computer and the Voice Switch.

2. Use a terminal emulation program such as Tera Term Pro or PuTTY freeware to open a connection to the switch.
3. Apply these values to the terminal settings:

   - Speed: 19.2 Kbs (SG Voice Switches), 115.2 Kbs (ST Voice Switches)
   - Data bit: 8 bits
   - Stop bit: 1
   - Parity: No parity
   - Flow Control: None

5.2.3.2 The CLI Main Menu

The CLI main menu automatically appears at system startup. You can also invoke the menu at any time by entering a question mark **?**.

Commands in CLI Main Menu describes the commands available in the CLI main menu.

Table 8: Commands in CLI Main Menu

Command	Description	Notes
`0`	Exit	Exit from CLI of voicemail-enabled switch and go to the Linux shell.
`1`	Show version	Lists version numbers for firmware and boot ROM in addition to the base version and the CPU board version.

Command	Description	Notes
2	Show system configuration	Displays the switch's boot and IP configuration. **Note**: The **Image Server address** field in the **Show system configuration** screen should be blank or should show the IP address of the HQ server or the managing server. If you must modify this setting, choose item (3) at the main STCLI menu to change the system configuration, and then choose option **F** to set or change the optional image server address.
3	Change system configuration	Takes you to the system configuration menu where you can set a switch's boot and IP configuration.
4	Reboot	Reboots the switch
5	Shutdown	Shutdown the voicemail-enabled switch and be ready to power-off.
6	Archive Logs	Archive log files in `/cf/shorelinedata/Logs` directory and core files in /cf/core directory and save the archive file in `/inetpub/ftproot` directory in the server.

Command	Description	Notes
7	Archive Logs (HTTPS)	Archive log files in `/cf/shorelinedata/Logs` directory and core files in `/cf/coredirectory` and save the archive file in `/inetpub/ftproot/uploads/switch` directory in the server.
8	Restore Factory Defaults	Clears all the configuration
?	Help	Enter a **?** to print this menu.

To select an option in Voice Switch CLI, enter the number associated with the menu item and press **ENTER**.

5.2.3.3 Boot and IP Configuration Options

When you choose Change System Configuration from the CLI main menu, a menu of boot and IP configuration options appears.

Boot and IP Configuration Options describes the boot and IP configuration options.

Table 9: Boot and IP Configuration Options

Command	ST Voice Switches and Virtual Switches Description	Voicemail-Enabled Switch Description	SG Voice Switches
0	Return to previous menu	Return to previous menu	Return to previous menu
1	Change Voice Switch Service IP address	Change IP address	Change IP address
2	Change IP subnet mask	Change IP subnet mask	
3	Change the gateway IP address	Change the gateway IP address	

Command	ST Voice Switches and Virtual Switches Description	Voicemail-Enabled Switch Description	SG Voice Switches
4	Change server IP address: **Note**: This is the IP address the Mitel server with the FTP service for the switch.	Change server IP address: **Note**: This is the IP address the Mitel server with the FTP service for the switch.	Change server IP address.
5			Change boot method
6		Change boot method	Enable/disable DHCP
7	Enable/disable DHCP	Enable/disable DHCP	Change network speed and duplex mode
8	Change network speed and duplex mode	Change network speed and duplex mode	
D	Set/change domain name	Set/change domain name	
F	Set/change optional image server address		
P	Set/change primary DNS IP address	Set/change primary DNS IP address	Set/change primary DNS IP address
S	Set/change secondary DNS IP address	Set/change secondary DNS IP address	

Command	ST Voice Switches and Virtual Switches Description	Voicemail-Enabled Switch Description	SG Voice Switches
T		Set/change network time server IP address	
*	Display current configuration.	Display current configuration.	
?	Help	Help	Help

After you have set your IP address and boot options, enter **?** to return to the main menu. You must reboot the switch for the new setting to take effect.

5.2.4 Accessing Voice Switch CLI on the Headquarters SoftSwitch

To run Voice Switch `CLI` diagnostics on the SoftSwitch, you must create a Telnet session. Voice Switch `CLI` commands are listed in VxWorks® Command Line Interface on page 72.

Note:

All the information that is displayed in the session will also appear in the `SoftSwitch` log file.

1. Create the following `DWORD` entry in

   `HKEY_LOCAL_MACHINE\Software\Shoreline Teleworks\SoftSwitch`

   or, if you are using a 64-bit server, create the `DWORD` entry in

   `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Shoreline Teleworks\SoftSwitch: TelnetEnabled`
2. Set the value to **1**.
3. Open a **Command Prompt (DOS)** window and type **telnet localhost 2323**. To Telnet to the SoftSwitch, the Telnet port must be set to 2323. The standard Telnet port is 23.
4. Press **Enter**. No User ID or Password is required. This immediately logs you into the SoftSwitch.

5. Press **Enter** a second time to get the SoftSwitch prompt, which looks like the following:

   ```
   ????

   SHELL: ????

   SHELL:
   ```

6. Enter CLI commands as described in VxWorks® Command Line Interface on page 72.
7. End the SoftSwitch Telnet session by typing **x**.
8. Press **Enter**.
9. Remove the **Telnet Enabled** DWORD from the registry editor by right-clicking on it and select **Delete**.

To start a Telnet session to the SoftSwitch from a different computer, you must specify the IP address of the Mitel server and modify the Telnet port to 2323.

All switch commands are available in the SoftSwitch with the exception of the following:

- Any VxWorks-specific commands
- msps

5.2.5 Router Auto-Delete Properties for ICMP Redirects

When WAN links fail, ICMP redirect messages are received by the Voice Switches from routers on the network. These ICMP redirect messages notify hosts on the network, such as Voice Switches, that an alternate route is available, and the switch updates its routing table accordingly.

The default behavior for Voice Switches is to automatically delete any ICMP redirect messages three minutes after time of receipt.

You can shorten or lengthen this period of time in one-minute increments, or you can disable the automatic deletion of ICMP redirect messages altogether.

5.2.5.1 Modifying Time Period to Auto-Delete ICMP Redirect Messages

1. Create the following DWORD entry in

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ShorelineTeleworks\
   ```

   TelephonyManagementServer\Settings:

   ```
   SwitchDebug - “debug_options timeout_icmp_redirect n.”
   ```

2. Set the **value of n** to the desired time period. Note that this must be an integral value and the number represents minutes, not seconds. The value of **n** can be set to **zero (0)**to disable the auto deletion of ICMP redirect messages.

   When this key is defined in the main server, the switches automatically delete all of their routing table entries after the specified period of time. Note that sampling occurs once per minute, so routes do not disappear exactly 360 seconds later if **n** is set to **6**.

3. Reboot the Voice Switch for these changes to take effect.

5.2.6 Using a Telnet Session to Set IP Address and Boot Parameters

You have the option of setting IP address and boot parameters using the VxWorks® `bootChange` command. To access the `bootChange` command, you must establish a telnet session to the switch. For information on other commands available from VxWorks®, see VxWorks® Command Line Interface on page 72.

1. Start the Telnet process with an `ipbxctl` command entered in this format:

   ```
   C:\Program Files\ShorelineCommunications\ShoreWareServer>ipbxctl - telneton

   Switch IP Address>
   ```

2. After the Telnet process is running, open a Telnet session with the switch. You are prompted for a User ID and Password.
3. For User ID, enter **anonymous**.
4. For Password, enter **ShoreTel** (case sensitive). The CLI opens and displays the menu of choices.
5. At the **>** prompt, enter **bootChange**.

   The boot device parameter appears.
6. Modify parameters by typing values and pressing **ENTER** (do not backspace).

   When you press **ENTER**, the next boot parameter appears.

   Parameter Settings for Flash Boot and FTP/HTTPS Boot lists and describes the parameters required for flash and FTP or HTTPS booting of Voice Switches.
7. Close the Telnet connection with the following `ipbxctl` command:

   ```
   C:\ProgramFiles\ShorelineCommunications\ShoreWareServer>ipbxctl -telnetoff

   Switch IP Address>
   ```

Table 10: Parameter Settings for Flash Boot and FTP Boot

		Flash Boot	FTP Boot	
Parameter	**Description**	**SG24, SG90/50/ 220T1/220E1**	**SG24**	**SG30/50/90/220TI /220TIA/220E1**
boot device	A network interface or a flash location	flash = 0	fei	emac0

		Flash Boot	FTP Boot	
Parameter	**Description**	**SG24, SG90/50/ 220T1/220E1**	**SG24**	**SG30/50/90/220TI /220TIA/220E1**
processor number	Always 0	0	0	0
host name	Always bootHost	bootHost	bootHost	bootHost
file name: SG	Path to VxWorks.sys file for SG switches	/flash0/ vxworks	/tsa/ vxworks	/tsk/ vxworks
inet – ethernet	IP address>:Subnet Mask (hex)> [a]	10.10.0.59:ffff0000	10.10.0.59:ffff0000	10.10.0.102:ffff0000 i
inet – backplane	Not used			
host inet	IP address of the main Mitel server [a]	10.10.0.5	10.10.0.5	10.10.0.5
gateway inet	IP address of router [a]	10.10.0.254	10.10.0.254	10.10.0.254
user	FTP site – User name login (typically set to anonymous)	anonymous	anonymous	anonymous
ftp password (pw) (blank – use rsh)	FTP site – Password (typically set to st1)	st1	st1	tsk
flags	See Boot Flags	0x40	0x40	0x40
target name	Host name of switch that can be set to other values	ShorelineSwitch	ShorelineSwitch	Shoretelbuild

		Flash Boot	FTP Boot	
Parameter	**Description**	**SG24, SG90/50/ 220T1/220E1**	**SG24**	**SG30/50/90/220TI /220TIA/220E1**
startup script	Path to bootscrp.txt file for SG24, SG8	/flash0/bootflsh.txt	/tsa/ bootscrp.txt	/tsk/bootscrp.txt
other	Set to network interface	fei	fei	emac

Note:

[a]These IP addresses are examples. Use the IP address for your system.

5.2.7 Boot Flags

The boot flags allow you to alter how the switch boots up. The hexadecimal values of the flags and their actions are listed in Boot Flags. You can aggregate flags to perform multiple functions by summing the hex values for the commands.

For example, the following command aggregates the flags 0x40 + 0x2000 + 0x40000 and instructs the switch to use DHCP to get boot parameters, disable the shell, and set network speed and duplex mode to 100 Mb HD:

```
0x42040
```

Table 11: Boot Flags

Command	Description
`0x0`	Network speed and duplex mode auto-negotiate.
`0x20`	Disable login security.
`0x40`	Use DHCP to get boot parameters.

Command	Description
`0x2000`	Disable shell.
`0x10000`	Network speed and duplex mode 10 Mb full duplex (fixed).
`0x20000`	Network speed and duplex mode 10 Mb half duplex (fixed).
`0x30000`	Network speed and duplex mode 100 Mb full duplex (fixed).
`0x40000`	Network speed and duplex mode 100 Mb half duplex (fixed).

5.2.7.1 Setting IP and Boot Parameters from VxWorks® Boot Monitor

If you are unable to access the Voice Switch CLI, you can access the same configuration options available with the bootChange command from the switch's boot monitor.

Note:

Making incorrect settings in the boot monitor can cause the switch to malfunction.

1. Connect a serial cable between a personal computer and the Voice Switch.
2. Use a terminal emulation program such as HyperTerminal to open a connection to the switch.
3. Apply these values to the terminal settings:
   - Speed: 19.2 kbps
   - Data bit: 8 bits
   - Stop bit: 1
   - Parity: No parity
   - Flow Control: None
4. Type **c**at the prompt for SG24 switches, and press ENTER. You are guided through the options listed in Parameter Settings for Flash Boot and FTP Boot

Note:
For SG50/90/220T1/220T1A/220E1 and voicemail-enabled switches, change options using the `setenv` command, and save using the `saveenv` command. For example:

- To change IP address:

  ```
  setenv ipaddr 10.10.0.59
  ```
- To change subnet mask:

  ```
  setenv netmask 255.255.0.0
  ```
- To save all changes:

  ```
  saveenv
  ```

5.2.8 Voice Switch Configuration Reset

Each switch includes a hidden reset button on the front panel that restores the switch to factory default boot settings and requests a new configuration from TMS. To enable the reset, press the button for 5;seconds. This button reboots the Voice Switch.

This completely clears all boot parameters and clears the switch's configuration.

5.3 Voice Switch Utilities

Two utilities are available to help you diagnose and update Voice Switches.

- The **ipbxctl** utility allows you to perform diagnostics and Telnet to the switch.
- The **burnflash** utility updates the switch to the version of firmware compatible with the server software.

  Both utilities are available in the Server folder:

  ```
  C:\ProgramFiles\ShorelineCommunications\ShorewareServer
  ```
- The **UBOOT** utility allows you to boot the switch in the field.
- The **SSH** utility allows you to access the switch and then run CLI commands.

5.3.1 Ipbxctl Utility

ipbxctl Utility Commands lists and describes the commands available using the `ipbxctl` utility.

Table 12: `ipbxctl` Utility Commands

Command	Description
`-telneton Switch IP Address>`	Enables Telnet connection on the switch.
`-reboot Switch IP Address>`	Reboots the switch without using Connect Director.
`-flash Switch IP Address>`	Sets switch to boot from flash memory (allows you to boot without logging in).
`-ftp Switch IP Address>`	Sets switch to boot from FTP (allows you to do this without logging in).
`-diag Switch IP Address >`	Sends switch state information. By default, the system puts this information in the same folder where the ipbxctl utility is running.Sends switch state information. By default, the system puts this information in the same folder where the ipbxctl utility is running. **Note**: This command may be disruptive to normal switch function. Use this command only for diagnostic functions, not for reporting.
`-reset`	Clears all flash memory. Returns switch to factory defaults. **Note**: This command is not available from the CLI.
`-telnetoff Switch IP Address >`	Disables Telnet connection on the switch.

Command	Description
`-traceroute target IP Address >`	Network troubleshooting tool. For additional information about the parameters that can be used with this command, see Traceroute Parameters.

5.3.1.1 Password Access

After entering the `ipbxctl` command, the user is prompted to enter a password. After the user enters the correct password, the device permits access to executables that configure or diagnose the switch.

Performing a telnet session on a Voice Switch requires password access to ipbxctl before invoking the `telneton` command. After entering the correct password, a user can establish a telnet session during the next minute. At the expiration of this period, existing telnet sessions are not affected, but users cannot establish a new telnet session. Telnet access is permitted only from the IP address from where the CLI was entered and access granted through password authorization.

Telnet continues to require User ID and Password entry that is distinct from `ipbxctl` password access. However, unlike the `cli` command and password, Telnet transmits the User ID and Password in the clear.

Note:

The Voice Switch continues using the user ID of **anonymous** and a password of **ShoreTel** for initiating Telnet.

CLI passwords are configurable only through Director. The default password is **ShoreTel**.

Pressing the reset button on the switch resets the password to the default value of Mitel. The password that was active on the switch prior to the hardware reset is restored when the switch is connected to the network and receives an update from Mitel.

To set the Voice Switch passwords, select **Administration** > **System Parameters** > **Other System Parameters** in Connect Director.

5.3.2 Burnflash Utility

Burnflash Commands lists and describes the commands available using the `burnflash` utility.

Table 13: Burnflash Commands

Command	Description

`burnflash - s`
 	
`Switch IP address>`
	Updates all bootrom areas.

`burnflash - test - s Switch IP address>`	Checks to see if `burnflash` command can be used.

5.3.3 UBOOT Utility

UBOOT is the boot loader for ST family switches and voicemail-enabled switches. The UBOOT environment is accessed from a terminal emulator through the serial port when the switch is booted. Before starting the boot, UBOOT lists the processor characteristics and displays results of the Power On Self Test (POST). The switch then waits a specified period before starting the autoboot.

5.3.4 SSH Access for Utilities

You can access ST family voice switches via SSH, and then run CLI commands on the switch.

Complete the following steps to access ST switches through SSH:

1. Install PuTTYGEN on the HQ server.
2. Open **PuTTYGEN** and click **Load an existing private key file**.
3. Navigate to `Shoreline Data\keystore\ssh\`, and then complete the following steps:

    a. Select **All Files** to view the key record.
    b. Select the **hq_rsa** key.
    c. Click **Enter**.
    d. Click **OK** to dismiss the PuTTYGEN notice.

> **Note**:
>
> If you are not performing these steps on the HQ server, you must copy the hq_rsa file from the HQ server to the system you are logging in from.

4. When the key is loaded, click **Save private key**. In the popup, click **Yes** to save without a password.
5. Name the key and save it. For example, you could use ST1 as the name of the key.
6. Use Putty in SSH mode and enter the IP address of the switch.

7. In the left column, expand the SSH item, and select the **AUTH** item. Click the **Browse** button in **Private key** file for authentication.
8. In the list of private keys, right-click the key you created in step 5, and click **Open**. If a **Putty security alert** dialog box appears, click **Yes** to confirm.
9. Enter **admin** in username.

5.4 Diagnostics

This section describes the tools available for diagnosing problems with switches.

5.4.1 Power LED

Voice Switches have one power LED with standard on and off displays. When flashing, the LED indicates other information about the switch:

- 2 flashes
  - The switch failed its internal self-test.
  - The switch has a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to Mitel.
- 3 flashes
  - Booting via FTP.
  - Flash memory might be corrupted. Go to the Maintenance >;Status and Maintenance > Appliances page in the Connect Director to ensure that the system is running properly.
- 4 flashes
  - The IP address is unavailable.
  - DHCP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue the boot process. The switch will automatically reboot in five seconds and try again. Check the DHCP server and the network configuration to ensure that the Voice Switch is receiving a valid IP address.
- 5 flashes
  - The operating system is not available.
  - The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds.
- 6 flashes
  - The switch is using a previously stored IP address.
  - A DHCP transaction was attempted, but the DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the DHCP server and network configuration.

5.4.2 VxWorks® Command Line Interface

VxWorks® provides a variety of useful tools and debuggers. This command line interface offers access to both standard VxWorks® commands and Mitel commands. You can access the VxWorks® interface by opening a Telnet session to a switch without invoking CLI.

You may also enter the VxWorks® command line interface from a serial interface by entering the command gotoshell from the Shoreline> prompt. To return to CLI, enter the command cliStart.

Use caution when using the VxWorks® interface; running commands can degrade performance on the switch. Mitel does not support changing or setting IP or other parameters using the VxWorks® interface. Changes made using this interface may not be persistent and using it may cause unpredictable behavior in the system.

Note:

Mitel does not support changing or setting IP or other parameters using the VxWorks® interface. Changes made using this interface may not be persistent, and using it may cause unpredictable behavior in the system.

5.4.2.1 Commands Available Through CLI

CLI Commands describes the commands available through the CLI interface.

Table 14: CLI Commands

Command	Description	Available on Voicemail-Enabled Switches	Notes
adm_debug_level	Logs admission control and bandwidth manager signal flow onto serial port.		– 2 logs more diagnostics.
adm_diag_level	Logs admission control and bandwidth manager signal flow into IPBX log.		– 2 logs more diagnostics.
arpShow and arptabShow	Displays the ARP table.	X	

Command	Description	Available on Voicemail-Enabled Switches	Notes
autoReboot – 0	Turns the switch watchdog off to prevent rebooting after a catastrophic failure.		Use only as directed by Mitel Technical Support.
bigNvRamSetup	Erases switch's configuration in NvRam.		
bootChange	Changes the boot ROM parameters.		Use with caution.
cid_debug_level	Logs caller ID related information for extensions .		
cliStart	Opens the command line interpreter (from a Telnet session) from serial ports only.	X	Switch reboot required for returning switch to VxWorks® interface .
config_status	Outputs the configuration records for the switch.		
DEBUG_LEVEL	Sets the ShoreSIP debugging flags.		Recommend using level 0xe00.
diagdCommands	Outputs full switch diagnostic information.		
dial_num_dump	Displays information about switch's off-system extension configuration.		

Command	Description	Available on Voicemail-Enabled Switches	Notes
dn_plan_status	Displays information about the switch's dial plan.		
dnp_debug_level	Displays detail information (digit by digit) about dial plan access.		Recommend using level 1.
dtmf_debug	Displays RFC2833 for G729 related events. Settings are variable, so contact TAC at (800) 742-2348 for assistance.		
DumpSB	Displays maximum PMCSW outputs.		
dumpUsedBw	Displays information about actual bandwidth used on individual calls/ legs.		
etherMonBroadcast	Set command value to **1**to include broadcast network packets in packet capturing.	X	Default value **0** does not capture/broadcast network packets.
etherMonDump	Writes the ethernet trace information captured when using EtherMonStart. Writes to a .cap file in \inetpub \ftproot directory of the Mitel server controlling the switch. The .cap file name is ST-lst 3 bytes of MAC-time-date>.cap.	X	

Command	Description	Available on Voicemail-Enabled Switches	Notes
etherMonStart bytes>	Bytes is the number of bytes of information you want to capture (for example, 10000000). Recommended values are between 1000000 and 3000000. Captures ethernet packets for trace purposes.	X	Requires excessive switch memory. Use `memShow` to determine memory available for command.
etherMonStop	Stops capturing ethernet packets.		
eval_adm_var	Displays information about switch's own bandwidth usage.		
eval_bwm_var	Displays information about total and available bandwidth.		
ext_bca_status	Displays active BCA calls along with call stack usage information.		Run on switches hosting BCA extensions.
ext_cco_status	Displays information the switch's extension CCOs.		
ext_conf_status	Displays MakeMe conference port status.		
ext_debug_level1	Logs extension CCO configuration.		
ext_debug_level	Sets the extension debugging level.		Recommend using level 4.

Command	Description	Available on Voicemail-Enabled Switches	Notes
ext_pg_status	Displays active pickup group calls.		To be run on the switches hosting PG extensions.
ext_ecr_status	Displays all configured Personalized Call Handling rules on switch.		
ext_ecr_debug	Displays real-time behavior of Personalized Call Handling rule.		Shows triggering of rule during inbound call.
fax_debug_level	Displays fax-related events and processing such as tone detection, fax determination, and fax redirect. Valid settings are 0 and 1. Default value is 0.		
fax_verbose	Displays fax/silence detection, jitter buffer freezing. and echo canceller disabling related events. Valid settings are 0 and 1. Default value is 0.		
flsh_getVersion	Displays switches firmware and bootrom versions.		
flsh_printBootLine	Prints the boot parameters of the switch.		
flsh_setBootSourceFlash	Sets the switch to boot from flash memory.		Requires a restart for changes to take effect.

Command	Description	Available on Voicemail-Enabled Switches	Notes
flsh_setBootSourceFTP	Sets the switch to boot from FTP.		Requires a restart for changes to take effect.
g729_verbose	Displays more information for G729 calls.		Enable this for G729 calls with mscmd_verbose
hostShow	Displays the known hosts.	X	
hunt_load_debug	Logs basic huntgroup call flow.		Use when debugging heavy call load issues
icmpstatShow	Displays ICMP statistics.	X	
ipdt_debug_filter	To print out IPDT log for one extension (Ext A). > ipdt_debug_level – -1 > ipdt_debug_filter– 1 (tell IPDT that filter is enabled) > ipdt_restrictTraceExts "Ext A's #" (turn on Ext A log) > ipdt_remRestrictTraceExt "Ext A's #"(turn off Ext log) To print log for all extensions:> ipdt_debug_filter – 0		

Command	Description	Available on Voicemail-Enabled Switches	Notes
ipdt_debug_level	Recommend setting to **-1**to turn on all logging.		
ipdt_dumpCCOCK	Dumps BB call key state, since there is no extension associated with BB.		
ipdt_dumpExtCalls	Dumps call information in the extension (for example, callID, legID, call state and leg state, and so on.)		
ipdt_dumpExtDisplay	Dumps the current display view from IPDT.		
ipdt_dumpExtensions	Dumps information for all extensions controlled by the switch and the information for monitored extensions and MAE (BCA) extensions that are in the same switch and in the different switches .		
ipdt_dumpExtCK	Dumps information for call keys on the extension.		Useful for troubleshooting LED patterns and icon issues.
ipdt_resetExtDisplay	Redisplay on the extension. If the phone display and IPDT display (ipdt_dumpExtDisplay) are desynchronized, run ipdt_reset_ExtDisplay to synchronize them.		

Command	Description	Available on Voicemail-Enabled Switches	Notes
ipdt_restrictTraceExts	Set ipdt_debug_filter to 1. Then, use ipdt_restrictTraceExts to turn on logging on a particular extension.		
if Show	Displays the current configured network parameters.	X	
laa_debug_level	Logs backup auto attendant signal flow.		
lspConList	Displays switch connectivity to other switches.		
lsp_debug_level	Displays Location Service Protocol messages that are exchanged between switches.		Recommend using level 4.
lsp_ping	Tests the LSP UDP communication to the far end switch. Parameters include IP address and test iterations.		example: -> lsp_ping "192.168.1.1", 100 Sends 100 packets to the switch at 192.168.1.1 (nominally 1 second). If command lists only the IP address, 1000 packets (10 seconds) are sent.
lspTelList	Displays local and remote contacts.		

Command	Description	Available on Voicemail-Enabled Switches	Notes
lspTelList 1	Displays detailed information about local contacts.		
lspTelList 2	Displays detailed information about remote contacts.		
mae_debug_level	Logs BCA call flow information.		
mailbox_debug_level	Logs mail box destination for a particular call.		
memShow	Shows current memory usage of the switch.	X	
mgcp_msg_debug	Logs MGCP messages.		
mgcp_trans_debug	Logs MGCP transactions.		
mohc_debug_level	Prints diagnostic information for music on hold calls when set to 1.		Can be set to either 0 or 1. Default is 0.
mpm_debug_mask – 0x40	Sets mpm debug flag to output Caller ID information received on inbound calls.		
mpm_debug_mask – 0x10	Displays detailed DTMF information.		

Command	Description	Available on Voicemail-Enabled Switches	Notes
mpm_debug_mask – -1	Displays detailed mpm information. Full debug of inbound calls (CallerID, DTMF).		
mscmd_verbose	Prints diagnostic information for the media commands sent from Switch board layer when set to 1. Default is 0.		Main media command verbose variable.
msps	Displays media stream statistics for all active calls on the switch.		Use for all media-related issues.
msps 7	Displays media stream statistics for active calls.		
msps 8	Displays media stream statistics.		Use only as directed by Mitel Support.
msps 16	Displays media stream statistics.		Use only as directed by Mitel Technical Support.
mwi_debug_level	Logs message waiting indicator setting call flow.		
ping "IP Address>"	Include double quotes (“) around the IP address.	X	For voicemail-enabled switch: valid on ssh CLI, not CLI
pri_log = 4	Begins output of D-Channel information.		

Command	Description	Available on Voicemail-Enabled Switches	Notes
pri_trace = 4	Sets the PRI D-Channel trace debug level.		
pri_verbose	Traces a high level description of the PRI traffic sent and received by trunks on the switch.		Recommend setting pri_verbose=1
print_ether_stats	Prints Ethernet statistics from the network controller.		
rdn_diag_level	Used to determine why calls are routing to particular destinations, similar to what gets put in the DRSMain log when DRS is enabled.		Useful values are 0 (none) or 5 (trace resolve_dn).
reboot	Reboots the switch.		
Record2File2(port,time,file_name>;0)	Records inbound media on the specified port for the specified time (in seconds) and writers it to `/inetpub/ftproot`.		Writes to the TMS server controlling the switch. FTP write access must be enabled on the server.
rfc2833_for_g711_debug	Displays events related to RFC2833 for G711.		Default is 0. It is a bitmasked integer. Can be used as 1 and 2.
routeShow	Displays current routing table.	X	
routestatShow	Displays routing statistics.	X	

Command	Description	Available on Voicemail-Enabled Switches	Notes
sb_debug_level	Switch board debug variable that prints debug information for the commands sent from Call control.		Useful values range from 1-5.
set_mpm_debug (char *)	Used to print information regarding commands/ event interface between host CPU and DSPs. Uses string as the parameter. Valid parameters include “pots”, “pstn”, “dtmfd”, “dtmfg”, “cdis”, “class”, “cpm”		Example: To print POTS related information, enter set_mpm_debug(“pots’)
sip_debug_level –1	Logs ShoreSIP to SIP translation.		
sip_debug_level –4	Logs SIP messages also.		
sipuaCallList	Displays active SIP stack calls. sipuaCallList 2 dumps more call related information.		Run on switches hosting SIP trunks/ extensions.
sipuaList	Displays list of SIP trunk/ extension user agents.		Run on switches hosting SIP trunks/ extensions.
t2t_debug_level	Logs trunk interval information such as silence, trunk name, trunk state, and so on.		
tcpstatShow	Displays TCP statistics.	X	

Command	Description	Available on Voicemail-Enabled Switches	Notes
trans_debug	Logs ShoreSIP transactions.		
traceroute "IP Address>"	For troubleshooting network by mapping route packets use to traverse an IP network.	X	Remember to include double quotes (“) around the target IP address. (For details, see Running the Traceroute Command from the Voice Switch CLI.)
trunk_cco_status	Displays information about switch's trunk CCOs.		
trunk_debug_level	Sets the trunk debugging flag		Recommend using level 4.
uaCallList	Displays information about active calls and legs.		
ua_call_status	Shows a snapshot of the active call status of the switch.		
uaList	Displays list of ShoreSIP extension/trunk user agents.		
unset_mpm_debug(char*)	Disables set_mpm_debugcommand		
udpstatShow	Displays UDP statistics.	XS	

5.4.2.2 Creating an Ethernet Trace File Using a Voice Switch

You can capture the output of VxWorks®;commands from the Voice Switches in an Ethernet Trace file that is stored on the server that is managing that switch.

To create an Ethernet Trace file:

1. Open a Telnet session and type **memShow**.

   Run this command to verify that the switch has at least 1 MB of memory to perform the procedure.
2. From the **Start** menu, navigate to the **Control Panel** > **Administrative Tools** > **IIS Manager**.
3. Right-click the folder located in `C:\Inetpub\ftproot`, go to **Properties** and clear the **Read Only** option. This enables write permissions to the ftproot folder
4. At the command prompt, run the following VxWorks® commands:

   (See CLI Commands for more information about the specific commands.)

   ```
   etherMonStart 1000000
   ```

   Note:

   Do not exceed 6 zeroes.

   ```
   etherMonStatus

   etherMonBroadcast

   etherMonBroadcast=1 (enables capturing broadcast packets)

   etherMonBroadcast=0 (enables capturing broadcast packets - default)

   etherMonDump

   etherMonStop
   ```

   The data generated by running these commands is stored in the _.cap;file in the following directory:

   ```
   C:\Inetpub\ftproot
   ```
5. When you are finished capturing data, the file can be processed using an Ethernet packet analyzer, such as Ethereal or Wireshark.

5.4.2.3 Recording Audio from a Physical Voice Switch Port

You can capture audio output from a Voice Switch physical port (for example, trunk port) using VxWorks®;commands. Audio output is saved on the HQ or DVM server that controls the switch.

To capture audio output:

1. From the **Start** menu, navigate to the **Control Panel** > **Administrative Tools** and locate the IIS Manager.
2. Right-click the folder located in `C:\Inetpub\ftproot`, go to **Properties** and clear the **Read Only** option. This enables write permissions to the ftproot folder
3. At the command prompt, run the following VxWorks® commands.

   (See CLI Commands for more information about specific VxWorks® commands.)

   ```
   Record2File2 (1, 60, “test”)
   ```

   Audio data from running this command is stored in the `test_rx.pcm` and `test_tx.pcm` files in `C:\Inetpub\ftproot`.

When you are finished capturing data, a **PCM Raw Data** file is created with the following format profile: 8000 Hz, 16-bit, Mono.

5.4.2.4 Using the Traceroute Command from a Voice Switch

The `traceroute` command offers a useful troubleshooting tool that determines the route taken by packets as they traverse an IP network from a Voice Switch to a specified destination. The command sends IP packets across the network, and the successive batches of packets have increased time-to-live (TTL) values.

TTL is a packet variable that defines the number of hops (stations) that a packet can pass through before it expires. When a station receives an expired packet, it discards the packet and sends a time exceeded message to the originating station. The `traceroute` command uses these expiration messages to build the path map.

By determining the path to a known destination, network technicians can identify firewalls blocking access to a site and gather information about the structure of a network and the IP address ranges associated with a host.

The `traceroute` command can be executed from the switch’s command line or from the `ipbxctl.exe` utility.

Running the Traceroute Command from the Voice Switch CLI

1. Open a Telnet session and enter:

   ```
   tracepath "<IP address>"
   ```

   IP address is the address of the target destination and is a mandatory parameter. It must be in double-quotation marks.
2. Press **Enter**.

   Traceroute displays information about the number of hops, host IP addresses, and the amount of time required for each hop.

   Traceroute Parameters lists and describes the parameters that can be used with the `traceroute` command when executing the command from the Voice Switch command line.

Table 15: Traceroute Parameters

Parameter	Description
target IP address	This parameter specifies the target IP address of the traceroute. This parameter is mandatory. IP addresses must be used and surrounded by quotes. DNS names are not supported.
-C	Probe on call control (ShoreSIP) port, using a ShoreSIP Request message, to determine if the packets flow from the switch through the network. This parameter uses fixed ports and version compatibility among all switches receiving packets.
-e	This parameter specifies the use of a fixed destination port and an incrementing source port. By default, traceroute increments the destination port with each probe. This port number is then used as a sequence number for matching packet responses to the probes. Incrementing the destination port number may complicate troubleshooting when packets are being filtered or lost at certain ports.
-I	This parameter specifies the ICMP protocol. (UDP is the default protocol used for traceroute.)

Parameter	Description
-S	This parameter specifies that probes are sent with a SIP message on the SIP destination port. Set this parameter to determine if SIP is flowing from the switch through the network. This parameter uses fixed ports.
-m max_ttl>	max_ttl specifies the maximum time to live (TTL) value for traceroute packets. The default maximum TTL value is 30 bytes. Valid max_ttl values range from 1 to 255.
-f first_ttl>	first_ttl specifies the TTL value of initial traceroute packets. The default initial TTL value is 1. Valid settings of first_ttl range from 1 to 255 and must be less than max_ttl.
-l length>	length specifies the size of traceroute packet. The default packet size is 40 bytes, but valid user-entered length settings range from 100 to 1992.
-p port>	port specifies the port for the destination probe. Valid port setti ngs range from 1 to 65535.
-q nqueries>	nqueries specifies the number of queries execute with each TTL value. The default value is 3. All integers greater than 0 are acceptable nqueries values.
-t tos>	tos specifies Type of Server (tos) bit settings in the IP header of traceroute packets. The default value is 0. Valid settings range from 0 to 255.
-w waittime>	waittime specifies the period (seconds) a switch waits for a reply to a traceroute packet. The default value is 5 (seconds). Valid waittime settings range from 2 to 86400.

Parameter	Description
-z pause>	pause specifies the period (milliseconds) between successive probes sent by the command. The default value is 0 (milliseconds). Valid pause settings range from 0 to 3600000.
Entering `traceroute` without listing any parameters returns the list of available parameters.	

5.4.2.5 USB Logging on ST Voice Switches

The ST family of Voice Switches supports USB logging, which you can use when troubleshooting issues that require extra tracing on different features on the switch. Using the USB logging feature allows you to perform extended logging while storing the log files in off-switch memory. This ensures you do not encounter storage issues on the Voice Switch if the logging period is extensive and the log file is large. Using USB logging also prevents the log file from being deleted by log maintenance applications before the logging is complete or the data has been retrieved.

Note:

Because the USB logging procedure requires you to reboot the Voice Switch, Mitel recommends you perform USB logging during off-peak hours.

Complete the following steps to use USB logging:

1. Plug a USB device into the USB port on the ST Voice Switch.
2. Open Connect Director and navigate to **Maintenance** > **Status and Maintenance** > **Appliances**.
3. Select the ST Voice Switch you want to start USB Logging for.
4. Select **Start USB Logging** in **Command**, and click **Apply**.
5. Select **Reboot** in **Command**, and click **Apply**.
6. Select **Stop USB Logging** in **Command**, and click **Apply** when you are finished gathering logs.
7. Select **Reboot** in **Command**, and click **Apply**.

5.5 Connecting to a Voice Switch

Voice Switch Half-Width and Full-Width Voice Switches provide a serial communications port accessible through a straight-through 9-pin serial cable.

1. Connect a serial cable between a personal computer and the Voice Switch.
2. Use a terminal emulation program to open a connection to the switch.
3. Apply these values to the terminal settings:

   - Speed: 19.2 Kbs for SG Voice Switches and 115.2 Kbs for ST Voice Switches
   - Data bit: 8 bits
   - Stop bit: 1
   - Parity: No parity
   - Flow Control: None

For information on port pinouts, refer to the Voice Switches appendix in the *MiVoice Connect Planning and Installation Guide*.

5.6 Power over Ethernet Switches (PoE)

When considering the use of Power over Ethernet (PoE) data switches in your network, keep in mind that not all PoE data switches provide power to all data ports, and not all PoE data switches provide adequate power to support all devices.

- The power usage on an IP phone typically spikes during bootup, and during normal operation, the phone requires less power.
- Verify that power allocated to the PoE ports matches the switch wattage.
- Mitel recommends selecting a PoE data switch that includes four hardware queues for Quality of Service (QoS) to ensure that rules can be set up to ensure adequate bandwidth for VoIP and other critical traffic.

Refer to the *MiVoice Connect Planning and Installation Guide* for information about power usage of IP phones.

Voicemail-Enabled Switches 6

This chapter contains the following sections:

This chapter describes maintenance operations for voicemail-enabled switches.

6.1 Overview

Voicemail-enabled switches provide voicemail services and access to auto-attendant menus for extensions hosted by the switch. Voicemail-enabled switches provide local access to voicemail while being controlled by a distributed voice server (DVS) at a different location.

Note:

When callers try to leave voicemail messages or users attempt to call an auto attendant, a recording plays stating that there is no space available and a message cannot be left. In the voicemail log for calls, a message indicates the current percentage of disk space used.

Example:

```
09:12:20.017 ( 4600: 5096) [MS] VMSystem::getAvailableMessageStores ,
maxMessageStores = 1

09:12:20.017 ( 4600: 5096) [MS] Calling GetDiskFreeSpaceEx, Path= C:
\Shoreline Data\Vms\Message

09:12:20.017 ( 4600: 5096) [MS] GetDiskFreeSpaceEx method returned,
FreeSpace=2526 MB

09:12:20.017 ( 4600: 5096) [MS]
VMSystem::getAvailableMessageStores ,FreeSpace.QuadPart <
MIN_DISKSTORAGE_FOR_RECORD returning -1, FreeSpace =2526 MB,
currPercentUsed=96

09:12:20.017 ( 4796: 4992) [PM] VoiceApp::recordMessage, messageStoreIndex
= -1

09:12:20.017 ( 4796: 4992) [PM] PM: Play phrase 80 lang 1
```

Recordings are no longer created if 95% or more of disk space has been used.

Clearing space on the drive will correct this issue.

Voicemail-enabled switches store voicemail in Compact Flash (CF) cards. Auto-attendant menus, greetings, and prompts are stored in permanent flash memory. Voicemail backup and restore routines are available through Connect Director, allowing you to safely store voicemail on a regular basis. If a switch is disabled, information on the Compact Flash is retained and can be moved to another switch of the same model.

Voicemail-enabled switches are deployed in the same manner as other Switch 1-U Half Width switches,;and they are managed similarly to other switches and servers. You use Connect Director to configure switch, voicemail, and server settings. Device status is also monitored in Connect Director.

Three voice switches operate as voicemail-enabled switches, which are voice switches;and voicemail servers:

- Voice Switch 90V
- Voice Switch 90BRIV
- Voice Switch 50V

6.2 Utilities

This section describes the utilities available for voicemail-enabled switches.

6.2.1 Accessing Utilities for Voicemail-Enabled Switches

Utilities for voicemail-enabled switches are accessible through the maintenance port, an SSH client, or a Microsoft Windows program executed from a command prompt on the Headquarters server or a distributed voice server (DVS). The following sections describe utility access methods.

For security purposes, voicemail-enabled switches accept requests only from command-line interfaces (CLIs) running on the local host, the controlling DVS, or the Headquarters server.

6.2.1.1 Accessing Utilities from the Serial Port

Switch utilities and the UBOOT command interface are accessible through the maintenance port located on the faceplate. The state of the switch at the time of Maintenance port access determines the available utility.

- During normal switch operation, the maintenance port accesses a specified Linux shell. The default shell is the ST command-line interface (STCLI).
- During a switch boot, the maintenance port accesses UBOOT

To access voice switch utilities through the maintenance port:

1. Connect one end of a serial cable to a computer with a terminal emulator program installed.
2. Connect the plug end of the serial cable to the maintenance port on the front panel of the switch.
3. Launch the terminal emulation using the following settings for the serial port:
   - Speed: 19.2 kbps
   - Data bit: 8 bits
   - Stop bit: 1
   - Parity: No parity
   - Flow Control: None
4. Click **OK**. The ST command line interface appears.
5. Do one of the following:
   - If the interface shows that the switch has a Linux operating system:
     a. Type the user ID and password as required. The default values are “admin” and “root” respectively. (Root is available only through a serial connection.)
     b. At the command line, enter **STCLI**. The STCLI interface opens.
   - Do nothing if the interface shows that UBOOT is being used; a user ID and password are not required.

For more information about these utilities, see stcli or UBOOT.

6.2.1.2 Accessing Utilities from SSH

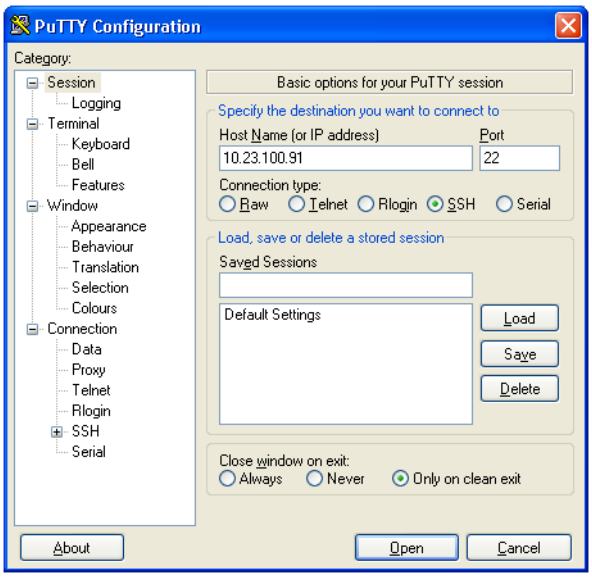
Mitel provides access to several utilities for voicemail-enabled switches through a Linux BASH command line, which you can access through an SSH client. Free SSH clients, such as PuTTY, are available through the Internet.

To access the Linux utilities, including all command line interfaces for voicemail-enabled switches, use the admin account. Logging into the admin account opens the STCLI interface.

1. Open an SSH client access panel.

   If you use PuTTY, the PuTTY Configuration page appears, as shown in the PuTTY Configuration Page figure.

Figure 10: PuTTY Configuration Page



2. On the **PuTTY Configuration** page, do the following:

   a. In the **Host Name (or IP address)** field, enter the IP address of the switch.
   b. In the **Port** field, enter **22**.
   c. Click **Open**. The command prompt window opens.

3. At the command prompt, enter **admin** and then press **Enter**. The **STCLI** command prompt opens.

6.2.1.3 Accessing Utilities from an MS Windows Server

Headquarters and distributed services contain executable files that access voicemail-enabled switches. On a typically installed server, the executable files for the utilities are located in the following directory:

`C:\Program Files\Shoreline Communications\ShoreTel Server`.

Commands that you can perform from a server through Microsoft Windows include:

- `svccli` (See svccli.)
- `burnflash` (See Burnflash.)
- `ipbxctl` (See ipbxctl.)

To run these utilities through MS Windows:

1. Open a command prompt by clicking **Start** > **Program** > **Accessories** > **Command Prompt**.
2. Enter the name of the utility on the command line, using the IP address of the voicemail-enabled switch as the switch parameter, then press **Enter**.

6.2.2 Switch Utilities

A set of command-line interface (CLI) commands supports operations such as backing up and restoring voicemail, stopping or starting services and groups, and formatting CF cards.

6.2.2.1 UBOOT

UBOOT is the boot loader for voicemail-enabled switches. The UBOOT environment is accessed from a terminal emulator through the serial port when the switch is booted. Before starting the boot, UBOOT lists the processor characteristics and displays results of the Power On Self Test (POST). The switch then waits a specified period before starting the autoboot. You can modify the duration of this period through an `svccli` command; the default period is three seconds.

To stop the autoboot during this delay, press any key.

The command `printenv` displays all booting shell variable settings. The following is a typical response to executing printenv:

```
bootdelay=3

serial#=50VJ0724081DFA

ethaddr=00:10:49:08:1d:fa

ipaddr=10.1.4.0

netmask=255.255.0.0

gatewayip=10.1.0.1

serverip=10.1.1.255

user=anonymous

pass=tsk

bootfile=/tskl/uImage
```

```
autoload=FTP

bootcmd=dhcp;bootm

flags=0x40
```

These settings are edited through the `setenv` command. The `setenv` command has the format `setenv` variable> value>.The `saveenv` command saves environment variable settings to the non-volatile memory on the switch. Execute `saveenv` after the variables are set to the required values. Boot flags control switch operations after startup.

For a description of UBOOT commands and flag values, see UBOOT Commands and Flags.

6.2.2.2 stcli

The ST Shell, `stcli`, displays and modifies system configuration parameters. You can implement static or dynamic IP addressing for the switch from `stcli`. You can also reboot the switch from `stcli`.

The main `stcli` menu appears below the Mitel logo. The switch model number is displayed in the command introduction line directly above the menu. `stcli` commands are described in stcli Commands.

To open `stcli`:

- Access the Maintenance port, as described in Accessing Utilities from the Serial Port. If the window displays the Linux prompt, enter `stcli` on the command line.
- Access through SSH and log in as the administrator, as described in Accessing Utilities from SSH

Exiting `stcli` returns the user to the login prompt.

6.2.2.3 CLI

The command-line interface (CLI) accesses diagnostic tools, manipulates debug setting levels, and displays system information. CLI can be run from any remote SSH session or from Windows prompts originating from the local host, the controlling Distributed server, or the main server.

To access CLI, do one of the following:

- Open a Linux BASH shell through the root account (see Accessing Utilities from SSH) and enter CLI.
- Open `stcli` and enter `gotoshell` at the command prompt.

To display a list of executable commands, enter **commands**on the command line. For a description of the CLI commands, see CLI Commands.

To perform actions on CLI variables, do one of the following:

- To view all of CLI variables and their current values, enter **variables**
- To view a variable current value, enter the variable name.
- To change a variable's current value, enter the variable name and new value.

To specify the destination of switch trace information, type one of the following commands:

- `trace_redirect 0` (Sends trace information to the Maintenance port)
- `trace_redirect 1` (Sends trace information to the current device)

Note:

Trace information is sent to the STTS log on the voicemail-enabled switch.

Only trace streams that are sent to the maintenance port can be redirected to an SSH terminal session; this prevents trace stealing from other SSH terminal sessions. All traces can be reverted to the maintenance port, making them accessible to SSH terminals.

To exit the CLI, do the following:

- Type **quit** or enter the letter **q** at the CLI prompt.
- Type **Ctrl-c** if the CLI was opened from the Linux BASH shell.

6.2.2.4 ipbxctl

`ipbxctl` commands perform switch control and diagnostic tasks, including switch rebooting, clearing flash memory, and running traceroute. For information about `ipbxctl` commands, see ipbxctl Utility Commands.

The `ipbxctl` commands are run as a windows program from the Main Server or the controlling Distributed Server, as described in Accessing Utilities from an MS Windows Server.

6.2.2.5 RegEdit

`RegEdit`, a utility that modifies registry-type data structures on the switch, is accessible through the Root account.

Voicemail-enabled switches have a registry similar to Windows Servers. The registry is a Mitel construct, not part of Linux. To edit the Registry, log in as root and run the `RegEdit` command line tool from the bash shell. `RegEdit` may be used to set logging levels on applications and set other parameters that change their behavior.

For more information about `regedit` commands, see regedit Commands.

6.2.3 Server Utilities

This section describes utilities available for servers: `svccli` and `cfg`.

6.2.3.1 svccli

The `svccli` commands control low-level switch parameter settings and application commands, including Compact Flash storage, switch password, and service control operations. You can run `svccli` from any remote SSH session or from Windows prompts originating from the local host, the controlling distributed voice server, or the Headquarters server.

To access `svccli`, perform one of the following:

- Open a Linux BASH shell through the root account (Accessing Utilities from SSH) and enter `svccli`
- Run `svccli` from the Main Server or a Distributed Server (Accessing Utilities from an MS Windows Server).

To display the `svccli` commands, enter **help** or **?**. For more information about `svccli` commands, see SVCCLI Commands.

To exit `svccli`, type **Ctrl-c** or enter the letter **q**.

6.2.3.2 cfg Utility

The `cfg` utility is a command-line tool that provides detailed information about the voicemail application. The `cfg.exe` file resides in the following directory:

```
\shoreline communications\ShoreTel server
```

To start `cfg`:

1. Open a DOS window pointing to the `\shoreline communications\ShoreTel server` directory.
2. Enter `cfg` and press **Enter**. The system displays the `/*Local*//->` prompt when `cfg` is ready.

   All commands are entered at the above prompt. Results are displayed in the DOS window or in the voicemail logs.

> **Note**:
>
> You can also initiate the `cfg` command from the voicemail-enabled switch directly by typing `cfg` at the command prompt.

Note:

Some `cfg` utility commands may damage the system if used incorrectly. Ensure you understand the commands before you use them.

For a list of the commands available through the `cfg` utility, see cfg Utility Commands.

6.3 Booting and Restarting Voicemail-Enabled Switches

Rebooting and restarting voicemail-enabled switches have different scopes:

- Rebooting a voicemail-enabled switch also reboots the Linux kernel. A reboot takes much longer than a restart.
- Restarting a voicemail-enabled switch only restarts the switch application layer without restarting the operating system and its services.

For voice switches running on VxWorks, rebooting and restarting are identical.

Under certain conditions, initiating a restart reboots the switch. One example is when a switch upgrade is available.

Voicemail-enabled switches boot, or load data and programs, from contents of their internal memory. Network parameters, including IP addresses, are required to complete the boot process. Switches obtain these parameters either from a DHCP server or through manual entry. New switches always attempt to access a DHCP server.

Within installations where a DHCP server is not available, switches must be manually configured, including the designation of the IP address and other configuration parameters. For switches not yet placed on a network, this configuration must be performed through the maintenance port. For switches that are on the network, switches can be configured through `stcli`.

When using DHCP, Mitel recommends using DHCP reservations for each switch to ensure that DHCP leases are not lost.

A voicemail-enabled switch can be brought up through a regular boot or by a software upgrade boot. FTP booting are also available for troubleshooting. Switches booted through FTP have limited functionality because internal memory contents are not loaded.

6.3.1 Manually Configuring Switches to Use Fixed IP Addresses

Voicemail-enabled switches normally use DHCP to dynamically set the device IP address and specify the addresses of the servers to which it communicates. Switches are set into fixed address mode through CLI instructions.

Beginning with Release 20.0, the Linux-based devices running on CentOS 7.x must be migrated manually to run on Rocky Linux 9.2. By default, Rocky Linux uses SHA256 for certificate authentication on switches. The 400-Series IP phones use SHA1 certificates. Hence, you must configure the switch to use SHA1 for certificate authentication on 400-Series IP phones.

Run the following command to configure the switch to use SHA1 for certificate authentication.

```
update-crypto-policies --set DEFAULT:SHA1
```

Voicemail-enabled switches require the following information:

- The IP address and subnet mask of the voicemail-enabled switch
- The IP address of the server that supervises the switch
- The gateway IP address of the supervising server if it resides on a different subnet from the voicemail-enabled switch
- The IP address of the Network Time Protocol (NTP) server. Voicemail-enabled switches require valid timestamps to operate; many services, including voicemail, cannot start without NTP access.

The following procedure places the voicemail-enabled switch into fixed-address mode:

1. Access the STCLI command line interface, as described in stcli.
2. Type **3** on the command line to select **Change System Configuration**. The CLI window displays the **Change System Configuration** options.
3. Type **6** on the command line to select **Enable/Disable DHCP**. The CLI window displays the **DHCP** options.
4. Type **0** on the command line to select **Manual Configuration**.
5. Change the network parameters as required to support the fixed address from the Change System Configuration entry line.
   - **DHCP** — To use a fixed address, this parameter must be disabled.
   - **IP address** — This is the voicemail switch's IP address. Set this parameter to an unused IP address.
   - **IP subnet mask** — Set this parameter to your network's subnet mask.
   - **Server IP address** — Set this to the IP address of the server that the voicemail switch gets firmware and configuration files from.
   - **Controlling Server IP address** — Typically, you set this to the same IP address for the same server you specified in Server IP Address. When you configure the voicemail switch in Connect Director, this field is set automatically.
   - **Gateway IP address** — This is the Gateway of the IP address selected.
   - **Time server IP address** — This is the IP address of your time server or of an NIST Internet Time Service (ITS). When you configure the voicemail switch in Connect Director, this field is set automatically.
6. After completing changes to the configuration, type **Exit** to close the CLI.
7. Reboot the switch.

6.3.2 Reboot Methods

A voicemail-enabled switch can be rebooted via a flash boot, a default button, FTP, or by using the `burnflash` command, each of which is described in this section.

6.3.2.1 Flash Boot

The standard method for booting a voicemail-enabled switch is to boot from the switch's flash memory. When a switch is first powered on, it reads the boot parameters stored on the non-volatile memory, which instructs the switch to load software from flash memory. When the software starts, it loads its configuration, which is also stored in flash memory.

6.3.2.2 Default Button

The **Default** Button is the small **paperclip** button on the left side of the switch. Pressing this button replaces the two configuration files with their default variants. The Compact Flash is not affected.

Pressing this button and holding for 10 seconds, in addition to replacing the configuration files, removes all files from the Compact Flash.

6.3.2.3 FTP Boot

Booting from FTP is available when you cannot boot the switch from internal memory. When booting a switch from FTP, the operating system and software are loaded from the FTP site identified in the boot parameters. The loaded files define a default configuration.

Voicemail services on the switch are disabled after booting from FTP and are restarted only by booting from Flash. After an FTP boot, the switch can perform telephony functions available via other voice switches.

Note:

Voicemail-enabled switches started with an FTP boot can operate only as a voice switch that controls phones, trunks, and call routing.

FTP boot is typically used for troubleshooting and also supports maintenance tasks and the backup and restore facilities. FTP boot supports certain maintenance functions, such as an emergency boot, if the flash becomes damaged.

6.3.2.4 Burnflash

Burnflash forces a reboot and installs new software.

The `burnflash` command burns a Mitel image to the CF card. It unconditionally replaces the resident image while rebooting the system, but it does not destroy any voicemail. The purpose of burning the image to the CF is to enable the switch to boot from solid state memory instead of performing an FTP boot from the server.

Note:

If a user created a static configuration for IP addresses and other system parameters through the `STCLI` (option 3), those parameters must be reconfigured after `burnflash` runs.

6.4 Switch Diagnostics and Repair

This section describes tools for diagnosing and repairing switch problems.

6.4.1 Remote Packet Capture

Remote packet capture is diagnostics tool in Connect Director that allows you to capture PRI/BRI ISDN packets. This tool is available at **Diagnostics** > **Remote Packet Capture**. Refer to the *MiVoice Connect System Administration Guide* for details about the parameters available to set for remote packet capture and for details about starting and stopping this tool.

6.4.2 Switch Trunk Debug Tools

Trunk_debug_level is a switch setting that identifies trunk events from the switch's perspective. Because Mitel applications manipulate dialed digit strings for both incoming and outgoing calls, the trunk debugger is typically used to validate the traffic between the Central office and the switch. The recommended trunk debug level is 4.

1. Access the CLI shell, as described in CLI.
2. Enter the following command: `trunk_debug_level=4`
3. When finished, turn off debug by typing: `trunk_debug_level=0`

Note:

Use D channel monitoring to view activity on the D;channel of a PRI span.

To monitor the D channel, complete the following steps using an SSH interface that is capable of capturing the output of the commands:

1. At the prompt, enter the following:

   ```
   -> pri_trace=4

   -> pri_log=4
   ```

   All D channel data is dumped to the screen.
2. When you are finished capturing data, turn the monitor off by entering the following:

   ```
   -> pri_trace=0

   -> pri_log=0
   ```

6.4.3 Creating a tcpdump File

> **Note**:
>
> Do not create `tcpdump` files without consulting Mitel Technical Support.

A `tcpdump` is a packet sniffer that operates from a;command line. Mitel can use tcpdump output to debug voicemail-enabled switch issues.

To create a `tcpdump` file:

1. Access the CLI shell, as described in CLI.
2. Execute the following: `tcpdump -C 10 -W 3 -w /var/log/tcpdump.pcap`

   This step captures ethernet traffic to the switch into ram.
3. After a brief period, press **Ctrl-C**.

   This step terminates the capture and saves the result to the following directory path: `cp /var/log/tcpdump.* /ftproot`
4. Submit the files to Mitel, as instructed by Mitel Technical Support.

6.4.4 Recording Audio from a Switch Port

You can capture audio output from a voice switch physical port,;such as a trunk port, using a CLI command. Audio output is saved on the HQ or DVM server that controls the switch.

To record audio from a switch port:

1. On the **Windows** server, click **Start** > **Control Panel** > **Administrative Tools** and locate the IIS Manager.

2. Right-click the **IIS Manager** and select **Properties**. Then select the **Write** checkbox and click **OK**.

   This enables the ability to write to the following directory: `C:\Inetpub\ftproot`
3. At the CLI prompt, run the following command: `Record2File2 (1, 60, “test”)`

   Audio data from running this command is stored in the `test_rx.pcm`file and file `test_tx.pcm` in `C:\Inetpub\ftproot`

When you are finished capturing data, a **PCM Raw Data** file is created with the following format profile: 8000 Hz, 16-bit, Mono and can be listened to using a standard application, such as “Adobe Audition.”

6.5 stcli Commands

The following describes the `stcli` commands. For a general description of `stcli`, see stcli.

- Option 0 – Exit

  This command logs out of `stcli` and returns control to the program from where `stcli` was entered.

  A user must exit `stcli` before starting `svccli`.
- Option 1 – Show Version

  This command displays the system software version running on the voicemail-enabled switch.
- Option 2 – Show System Configuration

  This command displays current values for system parameters that are viewable through `stcli`, a user enters a **2** at the `stcli` prompt.
- Option 3 – Change System Configuration

  This command provides access to editable parameters for modifying the system configuration. When option 3 is selected, the cursor displays **ShoreTel Config** to indicate that subsequent commands could alter the system configuration.

  The IP addressing mode is selected from this menu. To specify the addressing mode, select 6 from the **ShoreTel Config** menu. If static IP addressing is selected, all other Option 3 parameters must be configured. The static addressing configuration persists across upgrades.

  The configuration file is cleared if the `svccli burnflash` command is executed.

  If DHCP is enabled, the DHCP server must provide the IP address of the Network Time Protocol (NTP) server.

  Pressing 0 from the Config prompt returns the system to the main `stcli` menu. When exiting the `stcli` main menu, the user is prompted to confirm all configuration changes made in the Option 3 menu.
- Option 4 – Reboot

  Option 4 reboots the switch. The switch requests a confirmation of the command before rebooting.

- Option 5 – Shutdown

  Option 5 performs a graceful shutdown of the switch. This command is accessible only through the Maintenance port.

  Perform this command before removing power from the switch.
- Option 6 – Archive logs

  Option 6 archives all switch logs and uploads them to the Logs directory in the FTP root of the server managing the switch.
- Option ? – Help

  Entering a **?** lists the main menu items.
- Gotoshell – Entry to CLI shell

  Type `gotoshell`to enter the voicemail-enabled switch `cli` interface. For more information, see CLI.

6.6 SVCCLI Commands

For a general description of `SVCCLI`, see svccli.

- The `?` or `help` command displays a list of all commands and the syntax of each. The command takes no parameters (such as an individual command name.) An example of the command output follows:

  At the bottom of its display, `SVCCLI` states that a command can apply to all available arguments by inclusion of “all” or “*”. For example, the following SVCCLI entry restarts all services:

  ```
  >restartsvc *
  ```
- The `backupvm` command performs on-demand back up of voicemail, Auto-Attendant data, and the logs that are written to the CF card. On-demand backup begins immediately upon `backupvm` entry. During a backup, voicemail service continues, and an incoming voicemail message is backed up if it was already being recorded when the backup began. When the backup finishes, the `SVCCLI` displays a message indicating it is finished. Incontrast, during a restore operation, the voicemail server is stopped. Also, the restore operation can by started from the `SVCCLI` only.

  If automatic backup is disabled in Connect Director, `backupvm` still triggers the backup but only if backup is configured in the Connect Director.

  Whether for a scheduled or an on-demand backup, pre-configuration of the backup target is necessary. For a description of how to configure an FTP server to be the target of the backup, see the *MiVoice Connect System Administration Guide*.

  On-demand backup can serve a variety of purposes. These purposes are usually in response to anomalous situations. The main purpose of on-demand backup is to reduce the risk of losing voicemail if a damaged or faulty CF is suspected. For example, if the installation of a new CF card is immediately

required, on-demand backup is the first step. After the new card is formatted, the `restorevm` command can bring the backed-up voicemail to the new card.

Run `getsvcstatus all` to see the state of the CF file system. At the bottom of the screen for this command's output, the state of each file system is shown. The following line is from the file system lines of the `getsvcstatus all` output and shows that the CF file system is mounted.

```
/dev/kcfa1 984871 268663 666163 29% /cf
```

If the"/cf" is missing, then the CF file system is not mounted, and remedial action is necessary. In this case, not only does voicemail have nowhere to go, but the logs cannot be stored on CF, so the system provides some space in RAM for holding the most important logs.

After backup, the suspect CF card can be removed and tested in another system, and a new card can be installed after voicemail is backed up.

- `burnflash`- `Burn flash`: The `burnflash` command burns a Mitel image to the CF card. It unconditionally replaces the resident image and then reboots the system, but it does not destroy any voicemail. The purpose of burning the image to the CF is to enable the switch to boot from NAND flash memory rather than to do an FTP boot from the server. FTP boot supports certain maintenance functions, such as an emergency boot, if the flash becomes damaged. Do not use FTP boot to boot the switch. It does not support certain services. For example, an FTP boot does not mount the CF file system, so voicemail does not run after an FTP boot.

  If a user created a static configuration for IP addresses and other system parameters through the `STCLI` (option 3), those parameters must be reconfigured after `burnflash` runs.
- `chgrootpassword` - `Change root password`: The `chgrootpassword` command changes the root password for accessing the voice switch CLI. Arguments for this command are old and new passwords. This password was created in Connect Director on the **Administration** > **System Parameters** > **Other System Parameters**

  Syntax: `chgrootpassword password>`
- `chguserpassword` - `Change user password`: The `chguserpassword` command changes an administrator password for accessing the voice switch CLI. Arguments for this command are old and new passwords. This password was created in Connect Director on the **Administration**> **System Parameters** > **Other System Parameters** page.
- `disablegroup`- `Disable group`: The `disablegroup` command disables a group of services. Disabling means that one group or all groups of services are suspended but not completely turned off. To enable any disabled groups, use the `enablegroup` command.

  This command is primarily for trouble shooting. During normal operation, if a group of services fails, the system automatically tries to restart the stopped services. However, for troubleshooting purposes, it can be important for the group to remain inactive.

  Syntax: `disablesvc service name> *` or `all`

- `disablesvc` - `Disable service`: The `disablesvc` command disables one or all services. Disabling means that a service is suspended but not completely turned off. To enable disabled services, use the enablesvc command.

  This command is primarily for troubleshooting. During normal operation, if a service fails, the system automatically tries to restart any stopped services. However, for troubleshooting purposes, it can be important for the service(s) to remain inactive.

  This status of the service(s) is shown in the output of the `getsvcstatus` command.

  Syntax: `disablesvc service name> *` or `all`
- `dump` - `Dump`: The dump command sends a dump command to certain services. This command is used by engineering for debug only. Typically, the dump command dumps a service's internal state to a log file. The dump command does not work on all services.

  Syntax: `dump service name>`
- `enablegroup` - `Enable a group of services`: The `enablegroup` command enables one or more groups of services after they have been disabled by the `disablegroup` command. These two commands apply to troubleshooting.

  Syntax: `enablegroup group name> *` or `all`
- `enablesvc` - `Enable service`: The `enablesvc` command enables one or more services after they have been disabled by the `disablesvc` command. These two commands apply to troubleshooting.

  Syntax: `enablesvc service name> *` or `all`
- `erasecf` - `Erase CF`: The `erasecf` command completely erases all the contents of a CF card. Back up the CF before using this command. Examples of reasons to erase the CF are as follows:

  - To correct suspected memory corruption.
  - To erase a CF that is both formatted and mounted.

  Note:

  The `formatcf` command is not available for a CF card that is formatted and mounted.

  After CF erasure, the system automatically reboots. The reason for rebooting is so that, when the system detects that the CF is empty, the system recreates the file structure and replaces all other voicemails and other needed elements on the CF card.

  Syntax: `erasecf`
- `flushlogs` - `Flush logs`: The `flushlogs` command is a utility that copies certain system logs to the CF card. In normal operation, the system performs very little logging. Only severe problems are logged to files on the voicemail-enabled switch. The logging system is implemented in a memory circular buffer to record the logs (and perform certain tracing tasks.) Each log file includes its own circular buffer. These circular buffers can be forced to a log file by the `flushlogs` command.

  Syntax: `flushlogs`
- `formatcf` - `Format CF`: The `formatcf` command formats a new CF with the Linux file system format so that Linux recognizes it.

- `getsvcstatus - Get service status`: The `getsvcstatus` command displays details about all services on the switch. Regardless of the state of a service, this command displays it. (Therefore, it also shows whether a service exists.) The command can display a particular service or all services. A service name is case-sensitive, so it must be entered exactly. To see the spelling of a service name, use the all or (*) argument `getsvcstatus`.

  Syntax: `getsvcstatus service name> *` or `all`
- `killsvc -9 - Kill service`: The `killsvc -9` command immediately stops all Linux services on a voicemail-enabled switch.

  Syntax: `killsvc service name> *` or `all`
- `Q (or CTRL+C) - Quit svccli`: The q command or pressing the **Ctrl-c** keys terminates the `SVCCLI` and returns the user to the Linux CLI.

  Syntax: q or **Ctrl-c**
- `reboot [idle] - Reboot (if switch is idle)`: The `reboot` command causes the voicemail-enabled switch to reboot from NAND memory. With the optional idle argument, the reboot happens only if the switch is idle.

  Syntax: `reboot [idle]`

  Rebooting a voicemail-enabled switch and **restarting** a voicemail-enabled switch have different scopes. On other voice switches, rebooting and restarting are essentially the same. Rebooting a voicemail-enabled switch includes the Linux kernel and everything that a kernel reboot entails. In contrast, restarting a voicemail-enabled switch affects only the application layer.
- `restart [idle] - Restart services (if switch is idle)`: The `restart` command stops and then re-starts services. The **idle** option means that the operation waits until the process is idle. For instance, restarting the stts process when idle means waiting for stts not to be handling any calls, stopping stts, and then starting it again. Also, during the course of a restart or a reboot, the switch upgrades, if necessary.

  Syntax: `restart [idle]`
- `restorevm - Restore voice mail files`: The `restorevm` command causes the backed up voicemail, Auto-Attendant, and logs to be restored from the server to the CF card. Voicemail operation is unavailable during a restore. This process overwrites whatever is on the CF cards and puts the voicemail-enabled switch in the same state it was in at the time of the backup. The restore operation must be started from the `SVCCLI`. (Connect Director provides no option for starting a restore operation.) When the restoration is complete, the `SVCCLI` posts a message, and the switch is restarted.

> **Note**:
>
> The user must wait until the `restorevm` command completes the operation and the mail server comes up. This operation can be monitored from EventViewer of HQ server.

- `sendcmd - Send command`: The `sendcmd` command causes Linux to send a command to a particular service. This command is used by engineers for debug only.

  Syntax: `sendcmd service name>`
- `startgroup - Start group of services`: The `startgroup` command starts a stopped group. This command is the follow up to the `stopgroup` debug command.

  Syntax: `startgroup group name> *` or `all`

- `startsvc - Start service`: The `startsvc` command starts one or all services that have been stopped. This command might be able to restart one or more services that have stopped working. It can also be the follow up to the `stopsvc` debug command

  Syntax: `startsvc service name> * or all`
- `stopgroup - Stop group of services`: The `stopgroup` command stops one or all service groups. It stops the targeted group's process.

  Syntax: `stopgroup group name> * or all`
- `stopmgr - Stop services manager`: The `stopmgr` command completely stops the operation of the services manager.

  Syntax: `stopmgr`
- `stopsvc- Stop service`: The `stopsvc` command completely stops one or all services. It stops the targeted service's process.

  Syntax: `stopsvc service name> * or all`

6.7 CLI Commands

CLI Commands describes the CLI commands. For a general description of the CLI, see CLI.

Table 16: CLI Commands

Command	Description	Notes
adm_debug_level	Logs admission control and bandwidth manager signal flow onto serial port.	– 2 logs more diagnostics.
adm_diag_level	Logs admission control and bandwidth manager signal flow into IPBX log.	– 2 logs more diagnostics.
arpShow and arptabShow	Displays the address resolution protocol (ARP) table.	Not available on Voicemail-enabled Switch.
autoReboot – 0	Turns the switch watchdog off to prevent rebooting after a catastrophic failure.	Use this command only when direc ted by Mitel Technical Support.
bigNvRamSetup	Erases switch's configuration in NvRam. Use config_nv_format.	

Command	Description	Notes
bootChange	Changes the boot ROM parameters.	Use with caution. Not available on Voice Mail Switch.
cid_debug_level	Logs caller ID related information for extensions.	
cliStart	Opens the command line interpreter from a serial port.	Reboot the switch to return to the Linux interface. Not available on Vo icemail-enabled Switch.
config_status	Outputs the configuration records for the switch.	
DEBUG_LEVEL	Sets the ShoreSIP debugging flags.	Recommend using level 0xe00.
diagdCommands	Outputs full switch diagnostic information.	
dial_num_dump	Displays information about switch's off-system extension configuration.	
dn_plan_status	Displays information about the switch's dial plan.	
dnp_debug_level	Displays detail information (digit by digit) about dial plan access.	Recommend using level 1.
dtmf_debug	Displays RFC2833 for G729 related events.	Values can be 0 or 1 (default is 0).
DumpSB	Displays maximum PMCSW outputs.	
dumpUsedBw	Displays information about actual bandwidth used on individual calls/ legs.	

Command	Description	Notes
etherMonBroadcast	Writes the ethernet broadcast messages to a .cap file in \inetpub \ftproot directory of the server that are not intended for that switch.	Recommend using level 1. No `etherMonBroadcast` commands on Voicemail-enabled switches.
etherMonDump	Writes the ethernet trace information captured when using EtherMonStart. Writes to a .cap file in \inetpub \ftproot directory of the server controlling the switch. The .cap file name is ST-<First 3 bytes of MAC-time-date>.cap.	
etherMonStart <bytes>	Bytes is the number of bytes of information you want to capture (for example, 10000000). Captures ethernet packets for trace purposes	Command consumes switch mem ory. Run memShow to display avai lable memory. Do not specify more memory than is available.
etherMonStop	Stops capturing ethernet packets.	
eval_adm_var	Displays information about switch's own bandwidth usage.	
eval_bwm_var	Displays information about total and available bandwidth.	
ext_bca_status	Displays active BCA calls along with call stack usage information.	To be run on switches hosting BCA extensions.
ext_cco_status	Displays information the switch's extension CCOs.	
ext_conf_status	Displays MakeMe conference port status.	
ext_debug_level1	Logs extension CCO configuration.	
ext_debug_level	Sets the extension debugging level.	Recommend using level 4.

Command	Description	Notes
ext_pg_status	Displays active pickup group calls.	To be run on the switches hosting PG extensions.
ext_ecr_status	Displays all configured Personalized Call Handling rules on switch.	
ext_ecr_debug	Displays real-time behavior of Personalized Call Handling rule.	Shows triggering of rule during inb ound call.
fax_debug_level	Display fax-related events and processes, including tone detection, fax determination, and fax redirect.	Values can be 0 or 1 Default is 0
fax_verbose	Used to display fax/silence detection, jitter buffer freezing. and echo canceller disabling related events.	Values can be 0 or 1 Default is 0
flsh_getVersion	Displays switch's firmware and bootrom versions.	Not available on Voicemail-enabled Switch.
flsh_printBootLine	Prints the boot parameters of the switch.	Not available on Voicemail-enabled Switch.
flsh_setBootSourceFlash	Sets the switch to boot from flash memory.	Restart to enable changes. Not avai lable on Voicemail-enabled Switch.
flsh_setBootSourceFTP	Sets the switch to boot from FTP.	Restart to enable changes. Not avai lable on Voicemail-enabled Switch.
g729_verbose	Displays more information for G729 calls.	Enable this for G729 calls with msc md_verbose
hostShow	Displays the known hosts.	Not available on Voicemail-enabled Switch.
hunt_load_debug	Logs basic huntgroup call flow.	For debugging heavy call load is sues.
icmpstatShow	Displays ICMP statistics.	Not available on Voicemail-enabled Switch.

Command	Description	Notes

ipdt_debug_filter	Assume two extensions in the system: Ext. A and Ext. B.
	
	To print IPDT log for Ext. A:
	
	`ipdt_debug_level – -1`
	
	`ipdt_debug_filter – 1` (tell IPDT that filter is enabled)
	
	`ipdt_restrictTraceExts "Ext A's#"` (turn on log for Ext A)
	
	`ipdt_remRestrictTraceExt "Ext A's #"`(turn off log for Ext A).
	
	To print log for all extensions:
	
	`ipdt_debug_filter – 0`	

ipdt_debug_level	Recommend setting to – -1 to turn o n all logging.	
ipdt_dumpCCOCK	Dumps BB call key state, since there is no extension associated with BB.	Voicemail-enabled Switch does not s upport CCOCK.
ipdt_dumpExtCalls	Dumps call information in the exten sion (for example, callID, legID, call state and leg state, and so on.)	Not available on Voicemail-enabled Switch.
ipdt_dumpExtDisplay	Dumps the current display view from IPDT.	Not available on Voicemail-enabled Switch.
ipdt_dumpExtensions	Dumps information for all extension s controlled by the switch and the i nformation for monitored extensions and MAE (BCA) extensions that ar e in the same switch and in the diff erent switches.	Not available on Voicemail-enabled Switch.
ipdt_dumpExtCK	Dumps information for call keys on the extension. Useful for troublesho oting LED patterns and icon issues.	Not available on Voicemail-enabled Switch.
ipdt_resetExtDisplay	Redisplay on the extension. If the phone display and IPDT display (ipdt _dumpExtDisplay) are desynchroni zed, run ipdt_reset_ExtDisplay to sy nchronize them.	Not available on Voicemail-enabled Switch.
ipdt_restrictTraceExts	Set ipdt_debug_filter to 1. Then, use ipdt_restrictTraceExts to turn on log ging on a particular extension.	Not available on Voicemail-enabled Switch.

Command	Description	Notes
ifShow	Displays the current configured net work parameters.	Not available on Voicemail-enabled Switch.
laa_debug_level	Logs backup auto attendant signal f low.	
lspConList	Displays switch connectivity to other switches.	
lsp_debug_level	Displays Location Service Protocol messages that are exchanged betw een switches.	Recommend using level 4.
lsp_ping	Tests the LSP UDP communication to the far end switch for 100 iterations. Tests LSP UDP communication to the switch at 192.168.1.1, for 100 iterations (nominally 1 second). If only the IP address is supplied, 1000 iterations (nominally 10 seconds) is used.	Example: `-> lsp_ping "192.168.1.1",100`
lspTelList	Displays local and remote contacts.	
lspTelList 1	Displays detailed information about local contacts.	
lspTelList 2	Displays detailed information about remote contacts.	
mae_debug_level	Logs BCA call flow information.	
mailbox_debug_level	Logs mailbox destination for a part icular call.	
memShow	Shows current memory usage of the switch.	Not available on Voicemail-enabled Switch.
mgcp_msg_debug	Logs MGCP messages.	
mgcp_trans_debug	Logs MGCP transactions.	
mohc_debug_level	Prints diagnostic information for m usic on hold calls when set to 1.	Valid settings are 0 and 1. Default is 0.
mpm_debug_mask – 0x40	Sets mpm debug flag to output Calle r ID information received on inbound calls.	
mpm_debug_mask – 0x10	Displays detailed DTMF information.	
mpm_debug_mask – -1	Displays detailed mpm information. Full debug of inbound calls (CallerI D, DTMF).	
mscmd_verbose	Prints diagnostic information for the media commands sent from Switch board layer when set to 1.	Main media command verbose vari able. Default is 0.

Command	Description	Notes
msps	Displays media stream statistics for all active calls on the switch.	This is a helpful command for all m edia-related issues.
msps 7	Displays media stream statistics for active calls.	
msps 8	Displays media stream statistics.	Use only when directed by Mitel.
msps 16	Displays media stream statistics.	Use only when directed by Mitel.
mwi_debug_level	Logs message waiting indicator sett ing call flow.	
ping " <IP Address>"		Include double quotes (“) around the IP address.
pri_verbose	Traces a high-level description of the PRI traffic sent and received by trunks on the switch.	Recommended setting is pri_verb ose – 1
print_ether_stats	Prints the Ethernet statistics from the network controller.	Not available on Voicemail-enabled Switch.
rdn_diag_level	Used to determine why calls are rou ting to particular destinations, similar to what gets put in the DRSMain log when DRS is enabled.	Useful values are 0 (none) or 5 (tr ace resolve_dn).
reboot	Reboots the switch.	
`Record2File2(port,time, <file_name>;0)`	Records inbound media on the specified port for the specified time (in seconds) and writers it to `/inetpub/ftproot`.	Writes to the TMS server controlling the switch. FTP write access must be enabled on the server.
rfc2833_for_g711_debug	Displays events related to RFC2833 for G711.	Bitmask integer. Valid settings are 0, 1, and 2. Default is 0.
routeShow	Displays current routing table.	Not available on Voicemail-enabled Switch.
routestatShow	Displays routing statistics.	Not available on Voicemail-enabled Switch.
sb_debug_level	Switch board debug variable that prints debug information for the c ommands sent from Call control.	Values range from 1-5.
set_mpm_debug (char *)	Used to print information regarding commands/event interface between host CPU and DSPs.	Uses a string as a parameter (for example, “pots”, “pstn”, “dtmfd”, “dtmfg”, “cdis”, “class”, “cpm” are valid parameters). Example: To print POTS related information, use `set_mpm_debug (“pots”)`

Command	Description	Notes
sip_debug_level – 1	Logs ShoreSIP to SIP translation.	
sip_debug_level – 2	Logs SIP messages also.	
sipuaCallList	Displays active SIP stack calls. si puaCallList 2 dumps more call relate d information.	For switches hosting SIP trunks/ext ensions.
sipuaList	Displays list of SIP trunk/extension user agents.	For switches hosting SIP trunks/ext ensions.
t2t_debug_level	Logs trunk interval information like si lence, trunk name, trunk state, and so on..	
tcpstatShow	Displays TCP statistics.	Not available on Voicemail-enabled Switch.
trans_debug	Logs ShoreSIP transactions.	
trunk_cco_status	Displays information about switch's trunk CCOs.	
trunk_debug_level	Sets the trunk debugging flag	Recommend using level 4.
uaCallList	Displays information about active calls and legs.	
ua_call_status	Shows a snapshot of the active call status of the switch.	
uaList	Displays list of ShoreSIP extension/ trunk user agents.	
unset_mpm_debug(char*)	To disable set_mpm_debugcommand	
udpstatShow	Displays UDP statistics.	Not available on Voicemail-enabled Switch.

6.8 cfg Utility Commands

cfg Commands describes the commands available through the `cfg` utility. Variables are italicized. For a general description of the `cfg` utility, see cfg Utility on page 98.

Table 17: cfg Commands

Command	Parameters	Description	Comments
call p	p – phone number	Make a call from the vo icemail application and play a prompt.	;
closem	;	Close the open voicemail mailbox.	;
dmask 0x	0x – mask hex	Set voicemail debug mask (hex)	Enter without parameter to display flag list.
exit	;	Leave cfg.	;
laam t	t – (1 – DID, 2 – DNIS, 3 – Trunk)	List Auto-Attendant menu map.	Displays mapping of tru nks to Auto-Attendant me nus.
lall f	f– 1 for more details	List all mail boxes in the system.	Enter without “1” for a sum mary of system mail boxes and with “1” for more deta il.
lamp m f	m – mail box f – 1 - on; 2 - off	Turns the message waiting light on/off for a specified mail box.	;
list pb b	b – (0 - last name, 1 – first name)	Dump dial by names dire ctory to the voicemail log.	;
mbox l f	f= 1 for more details	List mail box information.	Enter without “1” for a sys tem mailbox summary, inc luding message IDs.
lms	;	List mail box schedule.	;
lmsg m	m – message ID	List details of a specific message.	Message IDs can be found by using lnbox.
loadc	;	Load all voicemail configur ation from the database.	;
loadm	;	Load all mailbox configurat ion from the database.	Requires that a mail box be open when you issue the command.
lserv	;	List information about all servers.	;
lsys	;	List voicemail system p arameters.	;
lsmtp	;	List status of distributed voicemail.	;
ltapi	;	List status of TAPI lines o pened by voicemail.	;

Command	Parameters	Description	Comments
msinfo	;	Dump voicemail internal table to the voicemail log.	;
openm #	#– mail box	Open specified mail box.	;
psinfo	;	Dump port server information to the voicemail log.	;
purge	;	Remove message in the deleted queue.	Requires that a mail box be open when you issue the command.
sh str	str – string	Search help for a string.	Searches only from the beginning.
starth	;	Remove old deleted messages.	;
symwi	;	Run MWI synchronization.	Sends MWI status to all phones in system.
ver	;	List cfg version.	;
?	;	List help commands.	;

6.9 UBOOT Commands and Flags

Parameter Settings for Flash Boot and FTP Boot describes the UBOOT environment variables.

Table 18: Parameter Settings for Flash Boot and FTP Boot

Parameter	Description	Flash Boot	FTP Boot
autoload	Specifies booting method for bringing up operating system	FLASH	FTP
bootcmd	Specifies boot actions that loads OS and software onto switch.		
bootfile	Path and filename of operating system file	tskl/uImage	tskl/uImage
flags	Variable passed to Linux that controls post startup operations.	0x40	0x40
gatewayip	IP address of gateway server	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
host	IP address of host running Connect Director	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
ipaddr	IP address of the switch	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
netmask	Subnet mask for subnet location of the switch	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
pass	Password for FTP account.	default setting is tsk	default setting is tsk

Parameter	Description	Flash Boot	FTP Boot
script	Path and filename of bo otscript file	tskl/bootflsh.txt	tskl/bootscrp.txt
serverip	IP address of host from which FTP transfer retr ieves the OS image.	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
user	User name of FTP accoun t.	default:anonymous	default: anonymous

The following actions are triggered by flag values:

- 0x0: Auto-negotiate network speed and duplex mode
- 0x20: Disable login security
- 0x40: Use DHCP to receive boot parameters
- 0x2000: Disable shell
- 0x10000: 10 MB full duplex (fixed)
- 0x20000:10 MB half duplex (fixed)
- 0x30000:100 MB full duplex (fixed)
- 0x40000:100 MB halfduplex (fixed)

Multiple functions are specified by adding the hex values of the individual functions. For example, the command 0x42040 instructs the switch to use DHCP to receive boot parameters (0x40), disable the Shell (0x2000) and set the speed and duplex mode to 10 Mb, half duplex (0x40000).

6.10 Burnflash Commands

The Burnflash Commands table describes the `burnflash` commands.

Table 19: Burnflash Commands

Command	Description
burnflash -s Switch IP Address>	Updates all bootrom areas.

6.11 ipbxctl Utility Commands

The ipbxctl Utility Commands table describes the `ipbxctl` commands.

Table 20: ipbxctl Utility Commands

Command	Description
-reboot <Switch IP Address >	Reboots the switch without using Connect Director.
-flash <Switch IP Address >	Sets switch to boot from flash memory> (allows you to b oot without logging in).

Command	Description
-ftp <Switch IP Address >	Sets switch to boot from FTP (allows you to do this wit hout logging in).
-diag <Switch IP Address >	Sends switch state information. By default, the system puts this information in the same folder where ipbxctl utility is running. **Note**: This may be disruptive to normal switch function. Use this command only for diagnostic functions, not for reporting.
-reset	Clears all flash memory. Returns switch to factory defa ults.

6.12 regedit Commands

The regedit Commands and Descriptions table describes the `regedit` commands.

Table 21: regedit Commands and Descriptions

Command	Description
`key keyname[\keyname]...`	Makes subkey keyname current key
`keyname[\keyname]...`	Makes subkey keyname current key
`.`	Displays current key, values recursively depending on display mode 'd'
`key .`	Displays current key, values recursively depending on display mode 'd'
`*`	Display current values
`key *`	Display current values

Command	Description
`..`	Go up one level
`key ..`	Go up one level
`addkey keyname`	Add subkey keyname to current key
`delkey keyname`	Delete subkey keyname from current key
`addstr valname strvalue`	Add valname strvalue to current key
`addnum valname numvalue`	Add valname numvalue to current key. numvalue is base10digit...
`addhex valname hexvalue`	Add valname hexvalue to current key. hexvalue is 0xhexdigit...
setstr valname strvalue	Set valname strvalue in current key
`setnum valname numvalue`	Set valname numvalue in current key. numvalue is base10digit...
`sethex valname hexvalue`	Set valname hexvalue in current key. hexvalue is 0xhexdigit...
`delval valname`	Delete value valname from current key
`d`	Toggle recursive display
`q`	Quit the program

Command	Description

`filename`
 	
`E.g RegEdit cmdfile`
 	
`Where cmdfile has the following contents`
 	
`VoiceMail`
 	
`Logging`
 	
`sethex Level 0xff`
	Read commands from a file

6.13 Server File System

This section describes where the server files for a voicemail-enabled switch are installed.

The server installs files with default access permissions. System administrators may want to ensure a more secure environment.

The Windows system user and the IPBX user created by the installer require full access to all the Mitel directories. All other users can be granted access on an as-needed basis.

To ensure the security of sensitive and/or personal information, confine access to the `vms` and `database` directories strictly to administrator, system, and IPBX users.

The server contains the following directories:

- The `shorelinedata` directory contains all the dynamic information the server uses to run the system. This directory and all sub-directories may be saved as part of a backup and used for full system recovery.

  `drive>\shorelinedata`
- The `prompts` directory contains copies of the auto attendant menu prompts.

  `drive>\shorelinedata\prompts`
- The `vms`directory contains all the files and configuration information used by the voicemail system. The files in this directory and its sub-directories are very dynamic. Never open these files. Opening any of the configuration files may cause the voicemail system to become corrupted in part or completely, and can cause loss of voicemail messages.

  `drive>\shorelinedata\vms`
- The `message`directory contains all voicemail messages as .wav files, along with an .enl pointer file for each message.

  `drive>\shorelinedata\mms\message`

Configuring and Maintaining 400-Series IP Phones

7

This chapter contains the following sections:

This chapter provides details about configuring and maintaining the 400-Series IP phones.

7.1 Overview

400-Series IP phones differ from other IP phones in that they use the Session Initiation Protocol (SIP). While this difference requires administrators to use slightly modified configuration and maintenance procedures, the 400-Series IP phones provide telephony features similar to other IP phone models. Users who are familiar with other phone models should have an easy transition to using the 400-Series IP phones.

This chapter provides details about configuring and maintaining the 400-Series IP phones.

All IP phones are supported by voice switches, which must have sufficient capacity for all the phones in the system. IP endpoints are configured in the system with Connect Director. For more information about configuring 400-Series IP phones, see the *MiVoice Connect Planning and Installation Guide* and the *MiVoice Connect System Administration Guide*.

7.1.1 IP Phone Failover

When IP phone failover is enabled on the IP Phone Options page in Connect Director, if an IP phone cannot communicate with its switch, the phone automatically connects to another switch at the same site that has available configured IP phone resources. For IP phone failover to be effective, the system must be planned with sufficient excess capacity to handle phones from at least one switch during a failover event. For example, if a switch with 20 IP phone ports fails, 20 IP phone ports need to be available elsewhere in the system.

7.1.2 Date and Time

400-Series IP phones depend on a Network Time Protocol (NTP) server to authenticate a secure connection and to provide the date and time to be displayed on for the phone's screen. The time displayed on the phone is the GMT value provided by the NTP server plus the offset from the time zone setting of the phone. Users can set the time zone through the phone's Options menu.

The IP address of the NTP server is delivered to the phone via DHCP or is manually configured in the phone. In the absence of an accessible NTP server, the phone can obtain the time from its controlling switch.

7.1.3 IP Phones and Voice Switches

Voice switches provide configuration and call manager functionality for 400-Series IP phones. Every site where IP phones are in use must have a voice switch configured to support the number of IP phones at the site. SIP Proxy ports are not required for the 400-Series IP phones.

Voice switches provide configuration for the 400-Series phones in a different manner than for other phone models. When a 400-Series IP phone downloads configuration files during the bootup process it receives a list of all available switches. The phone then randomly selects a switch from this list (starting with switches on the same subnet, if available) and attempts to register with the switch.

The contacted switch then redirects the phone to the appropriate call manager switch, which is the voice switch assigned to the phone to set up and tear down calls. The call manager switch handles the Session Initiation Protocol (SIP) information from the IP phones assigned to it and communicates call information to other switches in the system using SIP. After two IP endpoints are connected in a call, media streams are independent of the call manager switch.

After the phone registers with the call manager switch, any time the phone reboots it attempts to contact that same switch. If that switch does not respond, the phone attempts to contact another switch on the list until the phone successfully contacts a switch; the phone is then redirected to the appropriate call manager switch.

7.1.4 IP Phone Communications

Communications for 400-Series phones are routed through the following protocols:

- Secure Session Initiation Protocol (SIPS)
- Real-time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP)
- Client Application Server (CAS)

7.1.4.1 Secure Session Initiation Protocol (SIPS)

SIP is a standard protocol that is based on a client-server model and works at the application layer. Through SIP, networked users can initiate a call or receive a call. The protocol configures the parameters for the session and handles the call setup and tear-down.

Mitel uses the secure version of SIP, SIPS, for signaling between voice switches and 400-Series IP phones.

7.1.4.2 RTP and SRTP

Media flow for the 400-Series IP phones is either through Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP).

The use of SRTP, the encrypted version of RTP, depends on whether SRTP has been enabled through the Media Encryption option in the Call Control > Options page in Connect Director. If the Media Encryption option is set to **SRTP - 128 bit AES**, SRTP is used in the following scenarios:

- For calls between 400-Series IP phones configured as internal extensions, after the call is set up media flows directly between the IP phones using SRTP.
- For calls between a 400-Series IP phone and an external number over a trunk, after the call is set up media flows via the trunk using SRTP.
- For three-way mesh conference calls between 400-Series IP phones, after the call is set up media flows between the phones using SRTP.
- For up to eight 400-Series IP phones involved in a Make Me conference, media flows through SRTP when voice switches are used.
- or conference calls involving 400-Series IP phones that are initiated through a service appliance, media flows through SRTP.

When SRTP is used to encode the audio, the secure nature of the call is indicated with a lock icon in the call window.

If the Media Encryption option is not enabled, the connection negotiation between two 400-Series IP phones is through SRTP, but the resulting media stream between the two phones is through RTP.

Media flow for calls between 400-Series IP phones and other IP phones uses RTP. Make Me conference calls that involve at least one non-400-Series IP phone and a 400-Series IP phone also use RTP.

Note:
RTP is used when the endpoint is not a 6900-series IP phone or 400-series IP phone even if SRTP is enabled through the Media Encryption option in Connect Director.

7.1.4.3 Client Application Server (CAS) Service

On the 400-Series IP phones, the Client Application Server (CAS) supplies information such as call history, configuration details, directory, workgroup agent status, and visual voicemail. If CAS is inaccessible, these services are not available, but a phone can still make and receive calls.

7.2 Updating 400 Series IP Phone Firmware

While earlier phones automatically download available new firmware upon rebooting, updating firmware on the 400-Series IP phones is a process you manage through the Diagnostics and Monitoring system that you access through Connect Director.

For example, you can automatically maintain all 400-Series IP phones at the recommended firmware level, or you can override the automatic updates if you want to select a different firmware version or disable automatic update for certain phone models or for specific phones.

Control of phone firmware updates is accomplished through global-update and override settings that you specify on the Phone Firmware Update page of Connect Director. For details, see the *MiVoice Connect System Administration Guide*.

When you want to manage phone firmware on a more granular level, the Diagnostics and Monitoring interface provides a flexible approach for updating phone firmware because you can manage the firmware download and installation process in stages:

- If you want to download firmware to phones independently of installing it, use the Download command. You can choose to run this command at a time when you can spare the network bandwidth needed to accommodate the download. After firmware is loaded onto the phones, you can use the Update or Update When Idle commands at a later time to install the firmware that you have already downloaded without downloading it again.
- If you want to download firmware to phones and install it immediately, use the Update command. You can also use this command to install phone firmware that you have previously downloaded.
- If you want to download firmware to phones and install it when phones are idle, use the Update When Idle command. You can also use this command to install phone firmware that you have previously downloaded.

When a group of phones at a site is selected for firmware download and the server is remote, to minimize bandwidth utilization some of the phones at the site automatically download firmware from other phones at the site.

When phones are running at least the latest recommended firmware version, the value in the **Firmware Status** column is **Up to Date**. For more details about the possible values for Firmware Status, see the *MiVoice Connect System Administration Guide*.

If you are not using the automatic phone firmware update mechanism, you should upgrade phone firmware when the value in the **Firmware Status** column on the **Status** > **IP Phones** page is one of the following:

- **Firmware Version Mismatch** indicates that the phone's current firmware version is less than the minimum firmware version required for the phone.
- **Update Available** indicates that the phone is running an acceptable firmware version, but a more recent firmware version is available for download. In other words, the phone is running a firmware version above or equal to the minimum version, but less than the recommended version.

The **Advanced** option, which is available with the `Download`, `Update`, or `Update When Idle` commands, allows you to select a different firmware build for each model of phone. Furthermore, if there is more than one hardware version for each phone model, you can select a unique build to deploy to those phones as appropriate. The system prevents you from accidentally downloading a firmware version that is incompatible with a phone's hardware version. If there is no firmware version appropriate for a particular phone loaded on the server, you can select **Skip** from the **Version** dropdown list.

Because the Diagnostics and Monitoring system selects any available server from which to download the firmware update, you should ensure that all servers in the system, including servers that do not manage voice switches, have the latest firmware installed. If the Diagnostics and Monitoring system directs the phones to download from a server that does not have the specified firmware version, the download fails and the phones do not attempt to obtain the firmware from another server.

To download and install a firmware upgrade:

1. Launch Connect Director.
2. Click **Maintenance** > **Status and Maintenance** > **IP Phones**. The **IP Phones** page is displayed.
3. Select the check box for each phone for which you want to upgrade firmware.
4. In the **Command** drop-down menu, select **Update Firmware**.
5. Click **Apply**.
6. In the **Confirmation** dialog box, do one of the following:
   - To apply the recommended firmware version, click **OK**.
   - To select a particular firmware version:
     a. Click **Advanced**.
     b. For each type of phone selected, in the **Version** drop-down list, designate the firmware version.
     c. Click **OK**.

The **Firmware Status** column shows the progress as the firmware is downloaded and applied. The phones reboot.

7.3 Boot Process

The boot process varies depending on whether your network uses Dynamic Host Configuration Protocol (DHCP) or static configuration:

- DHCP— IP phones are pre-configured to work with your network's DHCP server. After the servers and voice switches are configured, the phones are automatically added to your Mitel system when they are connected to the network. Upon booting, IP phones use the configuration server address to acquire their configuration specifications. The configuration server address is set in the DHCP site-specific options (option tag 156). Alternatively, if DHCP is used without site-specific options, the server returned by DHCP option tag 66 (Boot Server Host Name field) is used for configuration. If DHCP is used without option tags 156 or 66, the phones are not automatically added to the system.
- Static configuration—If you are not using a DHCP server or it is not currently online, you can set a static IP address and other startup parameters directly on the IP phone. For details, see Specifying Configuration Parameters on a Phone.

Note:

If a phone is set to use DHCP but values are not provided for DHCP option **156** or **66**, when you plug a 400-Series IP phone into the network, by default the phone tries to connect to a MiCloud Connect system and displays a window prompting you to enter **MiCloud credentials**. If this happens, enter the phone setup process (**MUTE + 73887#**) and specify your configuration server. For details, see Entering SETUP from the Key Pad.

After the IP phone obtains the configuration server IP address or addresses, it downloads configuration files from the configuration server using HTTP (unless otherwise specified). If the configuration server cannot be reached because of some kind of error (such as a timeout) but the phone was configured with multiple configuration server IP addresses, then the phone tries to download the configuration files from the other servers. If no configuration server can be reached, or if a configuration file cannot be located, the phone uses the last successfully loaded configuration parameters. After a phone is finished reading configuration files, the current parameters are saved in flash memory.

7.4 Configuring 400-Series IP Phones

This section describes how you can specify custom configuration parameters for the phones.

When a 400-Series IP phone boots, it contacts the configured server and reads an initial configuration file from the server. You can override the default configuration parameters for a phone through DHCP site-specific options, through the phone interface, or through custom configuration files. As phone firmware is upgraded, some configuration information is overwritten, but parameters specified in custom configuration files are preserved across upgrades.

7.4.1 Parameter Precedence

While there are some exceptions, in general configuration parameters are processed by the phone in the following order. The last parameter source takes precedence:

- Defaults
- Values specified on the phone through the `MUTE 73887# SETUP#` command.
- LLDP-MED
- DHCP option tags 156 or 66 (if DHCP is enabled)
- Configuration files that reside on the server. The precedence order for these files is described in Processing Order for Configuration Files.
- Configuration settings from the voice switch

7.4.2 Specifying Configuration Parameters on a Phone

If you are not using a DHCP server to provide IP address and configuration parameters to the phones, you must manually configure the phones. You can enter the phone configuration menu at bootup or by entering a key sequence from the phone's keypad after the phone has finished booting up.

For descriptions of the parameters you can set on a phone, see Phone Information for 400-Series IP Phones.

If you are using DHCP, be aware that the order of precedence for certain parameters varies:

- Setting the Config server parameter on the phone (through the **Admin options** > **Services** menu) overrides the configServers parameter specified through DHCP.
- Setting the SNTP server parameter on the phone (through the **Admin options** > **Internet protocol** menu) does not override the SNTP value provided by a DHCP server because when the phone is rebooted the DHCP value overwrites the value entered on the phone. However, if you set this parameter on the phone, unplug the phone from the network that uses DHCP, and then plug it into a

network that does not supply the SNTP server value through DHCP, the parameter value entered on the phone is retained.

Table 22: Phone Information for 400-Series IP Phones

Admin Options Menu Item	Option Name	Description
Network policy	Use LLDP-MED	Network policy Use LLDP-MED If On, the phone captures link policy from a Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) broadcasting neighbor (presumably the upstream ethernet switch). If Off, you can manually set the policy values (such as using 802.1.Q tagging, VLAN ID, PCP, DSCP-audio). If On, these policy values are not editable. If present, the following MED data fields are used by the phone: • VLAN ID • PCP • DSCP If a new neighbor is found (that is, the phone has been moved to a new network), the network policy cache is updated with the new values. If no LLDP messages are found within the 5-second time-out period, the phone uses the cached network policy. If network policy caching is disabled, the default policy is used.
	LLDP neighbor	If Active, an LLDP-MED broadcasting neighbor has been found and the phone is actively using the received policy.
	Cache LLDP-MED	If On, then in the event of failure to receive an LLDP-MED messages, the previously received values are applied. If Off, the default values are used.
	Use 802.1Q	IEEE 802.1Q specifies the use of VLANs (Virtual LANs) on Ethernet. If enabled, you must also specify values for the following fields: • VLAN • ID PCP • DSCP audio If the value for the Use LLDP-MED option is On, this field is not editable.

Admin Options Menu Item	Option Name	Description
	VLAN ID	The Virtual LAN identifier The default value is 0, which means that VLAN tagging is disabled.
	PCP	The IEEE P802.1p Priority Code Point (PCP) value The default value is 5.
	DSCP audio	The Differentiated Services Code Point (DSCP) value to be used for audio packets. (For details on DSCP, see *RFC 2475*.) The default value is 46.
	DSCP SIP	The Differentiated Services Code Point (DSCP) value to be used for signaling (SIP) packets. (For details on DSCP, see *RFC 2475*.) The default value is 26.
Ethernet	Network port	Choose automatic configuration (Auto) or choose speed and duplex modes. The recommended value is Auto.
	PC port	Choose to disable the PC port, or choose automatic configuration (Auto) or speed and duplex modes. The recommended value is Auto.
	802.1Q	On or off, as dictated by the Use 802.1Q option in the Network policy menu
	VLAN ID	The Virtual LAN identifier The default is 0, which means that VLAN tagging is disabled.
	PCP	The IEEE P802.1p Priority Code Point (PCP) value The default value is 5.

Admin Options Menu Item	Option Name	Description
	Use 802.1X	Choose to enable or disable IEEE 802.1X link layer authentication. If enabled, enter the username and password. Note the following points about 802.1X usage: • If the phone has 802.1X turned on but the network does not have 802.1x authentication, the phone functions normally (and does not need a username and password). • If the network has 802.1X and the phone's user name and password credentials are missing or invalid, the phone prompts for a username and password on startup.
	Username	The user name to enable 802.1X link layer authentication
	Password	The password to enable 802.1X link layer authentication
	Authenticated	The current status of 802.1X authentication
Internet protocol	Use DHCP	If On, DHCP is used to collect the IP address layer information. If Off, you must manually enter the IP address layer information. If On, DHCP provides values for the following fields. If Off, specify static values for these fields: • IPv4 address • Subnet mask • Gateway • DNS • SNTP (Simple Network Time Protocol) server It is optional but recommended that DHCP option tag 156 be used to specify the designated configuration server for 400-Series IP phones. For more information about this DHCP option tag, see Specifying Config Parameters through DHCP Options on page 135
	DHCP lease	If Active, indicates a DHCP lease has been received by the phone.
	Cache DHCP	If On, the last received DHCP lease is cached and used if a DHCP lease is not received on the next renew. If Off and static values are not provided, the phone will fail to get an IP address if the DHCP server does not respond.

Admin Options Menu Item	Option Name	Description
	IPv4 address	The IP address of the phone. If Use DHCP is On, this field displays the value from the DHCP server.
	Subnet mask	If Use DHCP is Off, specify the static subnet mask for the phone. If Use DHCP is On, this field displays the value from the DHCP server.
	Gateway	If Use DHCP is Off, specify up to three static IP gateways. (If you do not want to specify a gateway, set the value of the Subnet mask field to 0.0.0.0 to confirm that no address needs a gateway.) If Use DHCP is On, this field displays the value from the DHCP server.
	DNS	The default list of static DNS servers. DHCP can override these servers. If Use DHCP is on, this field displays the current value.
	SNTP server	The IP address for the SNTP server, which is required for phone operation. The SNTP server should be synchronized with the time used by the Mitel Headquarters server. DHCP option tag 42 should be used to pass the time server IP address. If **Use DHCP** is **On**, this field displays the value from the DHCP server.
	DSCP audio	The Differentiated Services Code Point (DSCP) value to be used for audio packets. (For details on DSCP, see RFC 2475.) The default value is 46.
	DSCP SIP	The Differentiated Services Code Point (DSCP) value to be used for signaling (SIP) packets. (For details on DSCP, see RFC 2475.) The default value is 26.
VPN	Use VPN	If On, the phone can be used securely on a public Internet connection. If Off, the phone cannot be used off the network.
	VPN gateway	If connected, shows the connected VPN gateway and configures the list of VPN gateways to connect to
	VPN gateway port	The port used for the VPN connection
	Tunnel IP	When the tunnel is connected, the phone reports the current tunnel IP address obtained from the VPN gateway
	VPN protocol	Shows the active VPN protocol: rast-dtls

Admin Options Menu Item	Option Name	Description
	VPN debug mode	If **On**, VPN log information is included when you upload logs to the destination specified in the Diagnostic server field (in the **Diagnostics** menu). If you change the value of this field from **Off** to **On**, the phone reboots. If **Off**, VPN log information is not included in the logs.
Services	Config server	This is the IP address of the Headquarters server. It can be entered manually here or obtained from DHCP. If entered manually, this server overrides the server specified in DHCP option tags 156 or 66. If you specify a list of servers, the phone attempts to connect to subsequent servers in the list if a server fails.
	SIP	This is the IP address of the voice switch that the phone has successfully registered with or is attempting to register with.
	Directory	This is the IP address of the Client Application Server (CAS), which provides Directory and History services.
	MiCloud domain	For IP phones used with MiCloud Connect, this field specifies the domain for MiCloud connections. **Note**: This is not applicable for MiVoice Connect
Phone information	MAC address	The MAC address of the phone. This is a unique number forcthe device.
	Software version	The version of the phone software that the phone is running.
	Model number	The model number of the phone.
	HW version	The hardware version of the phone.
	Language	The language the phone is configured to use
	Country	The country for which the phone is configured
	Kernel version	The kernel version installed on the phone.
	Boot1 loader version	The boot1 loader version installed on the phone.
	Boot2 loader version	The boot2 loader version installed on the phone.
	Signature	Mitel internal use only
Diagnostics	System	For details on these menu options, see Viewing Diagnostic Information on a Phone
	Ping	
	Traceroute	

Admin Options Menu Item	Option Name	Description
	Capture	
	Clear configuration	
	Reset phone	
	Log upload	
	Diagnostic server	

7.4.2.1 Entering SETUP at Bootup

1. Connect the Ethernet cable to the data jack on the back of the IP phone.
2. As the phone is booting, when prompted press any key to enter setup.
3. At the **Admin Password** prompt, enter the default password **1234** or the password provided by your system administrator.

> **Note**:
>
> This password is configured through Connect Director on the Administration >;IP Phones > Options page. The parameter name is IP Phone Password. If the phone uses factory defaults, the phone has never been connected to a server, and you have not modified the IP Phone Password, use the default password, **1234**.

4. Do one of the following:
   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **OK** soft key. The **Admin Options** menu opens.
5. Use the navigation key pad and the selector button to open the submenus necessary to configure parameters as follows:
   - If you are not using a DHCP server to provide an IP address, enter the following information:
     - **Internet protocol** > **Use DHCP** (Toggle to Off.)
     - **Internet protocol** > **IPv4 address** (Enter the static IP address of the phone.)
     - **Internet protocol** > **Subnet mask** (Enter the static IP subnet mask of the phone.)
     - **Internet protocol** > **Gateway** (Enter the static IP gateway.)
     - **Internet protocol** > **SNTP server** (Enter the IP address of the time server.)
   - If you are not using DHCP to provide configuration parameters, in the Services > Config server field enter the IP address of the configuration server.
6. With the appropriate submenu highlighted, do one of the following:
   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Edit** soft key.

7. To return to the previous menu, do one of the following:
   - On the IP420, scroll down to the **Back** option and press the selector button on the navigation key pad until you return to the top-level menu.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key until you return to the top-level menu.
8. To apply the changes, do one of the following:
   - On the IP420, with **Exit** highlighted press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Apply** soft key.

Note:

On IP480, IP480g, and IP485g phones, to exit the menu and apply changes, press and hold the Back soft key for 2 seconds.

The phone reboots and applies settings.

7.4.2.2 Entering SETUP from the Key Pad

1. With the phone on hook, press the **MUTE** key followed by **73887# (SETUP#)**.
2. Go to step 3 in the Entering SETUP at Bootup on page 134, and proceed with the steps there.

7.4.3 Specifying Config Parameters through DHCP Options

By default, DHCP option tag 156 is used. The following parameters are specified in the site-specific options for option tag 156:

- configServers: Specify a comma-separated list of IP addresses or DNS names for the configuration server. If a server is not available, the phone cycles through the list of servers until it finds a working server.
- ftpServers: Specify a comma-separated list of IP addresses or DNS names for the configuration server. If a server is not available, the phone cycles through the list of servers until it finds a working server.

Note:

The ftpServers parameter is provided for compatibility with sites running MGCP phones. 400-Series IP phones use HTTP to download configuration files from servers specified in the ftpServers parameters. For new installations, the configServers parameters is recommended over the ftpServers parameter.

- vlan

While DHCP Option 156 can be used to enable VLAN tagging and set the VLAN ID, it is not recommended because VLAN hopping after the DHCP address is acquired forces the phone to re-start the network stack on the new VLAN a second time. LLDP-MED is the preferred method to enable VLAN tagging.

The complete Option 156 syntax including VLAN tagging is:

```
vlan=<number>,layer2tagging=<0|1>,configservers=<IP address>,ftpservers=<IP address>
```

Specify the parameters in any order, separating multiple parameters with a comma. Not all parameters are required. When providing multiple values for one parameter, use quotation marks around the comma-separated values. For example:

```
configServers="192.168.0.13, joe.test.com",vlan=2
```

If DHCP option tag 156 is not used, DHCP option tag 66 is used. The following parameters are specified in the site-specific options for option tag 66:

- tftpServers
- ftpServers

Note:

400-Series IP phones use HTTP to download their configuration files from the servers specified in DHCP option tag 156.

7.4.4 Specifying Config Parameters through Custom Config Files

The 400-Series IP Phone Model Configuration Files table lists the configuration file names for the 400-Series IP phones. These files are stored in the phone configuration directory created on the server when your Mitel system is installed. The default directory for these configuration files is as follows:

```
<Drive>:\inetpub\ftproot\phoneconfig
```

Table 23: 400-Series IP Phone Model Configuration Files

IP Phone Model	Custom Configuration File Name for All 400-Series IP Phones	Model-Specific Custom Configuration File Name for 400-Series IP Phones
IP420	custom.txt	custom_IP420.txt
IP480	custom.txt	custom_IP480.txt
IP480g	custom.txt	custom_IP480g.txt

IP Phone Model	Custom Configuration File Name for All 400-Series IP Phones	Model-Specific Custom Configuration File Name for 400-Series IP Phones
IP485g	custom.txt	custom_IP485g.txt

7.4.4.1 Processing Order for Configuration Files

Configuration files are processed in the following order:

- `country_ISO>.txt`, where ISO> is a two-character ISO country code (For example, the file for the United States is country_US.txt.)

  Do not edit these files. These files specify country-specific settings such as date/time formats.
- `generated.txt`

  Do not edit this file, because it is generated by the server and any changes would be overridden the next time the server generates the file. This file contains a list of voice switches for the phone and the default httpResources parameter setting, which specifies the default server path for wallpaper and ringtones. The server regenerates this file whenever the list of switches is updated.
- `custom.txt`

  This is the base custom configuration file for all 400-Series IP phones. Any configuration parameters that you add to this file are applied to all 400-Series IP phones in your system.
- `custom_phone_model>.txt` (where phone_model> is IP420, IP480, IP480g, or IP485g)

  This is the custom configuration file for a particular model of 400-Series IP phone. Any configuration parameters that you add to this file are applied to all phones of that model at your site.
- `custom_MAC address>.txt` (where MAC address> is the MAC address of a phone)

  This is the custom configuration file for a particular phone as identified by its MAC address (the 12-digit number on the white sticker on the back of the phone). Any configuration parameters that you add to this file will be applied to the phone identified by the MAC address.

Note:

- File names for MAC configuration files must be in lower case and not contain punctuation.
- The following is an example of a custom configuration file name for a particular phone identified by its MAC address: `custom_00104928630b.txt`

The phone-specific custom configuration file is the last file read. Any parameters in a custom configuration file override configuration parameters specified at a lower level of precedence, including the parameters entered on the phone, because they are processed first, before any configuration files are read. Any duplicate parameters specified in the configuration files are overridden according to their own precedence order.

Parameters are organized by group, and each parameter must begin on a new line within the proper group, as follows:

[group>]

parameter>=value>

parameter>=value>

[group>]

parameter>=value>

parameter>=value>

where

[group>] is the configuration parameter group as shown in Configuration Parameters.

<parameter> is the name of the configuration parameter as shown in Configuration Parameters.

value> is the name of the configuration parameter as shown in Configuration Parameters.

In specifying parameters, the following rules apply:

- IP addresses must be provided in dotted-decimal format.
- Parameters and values in configuration files are case sensitive.
- Cases are preserved in character strings unless otherwise indicated.
- Comments may be embedded in a configuration file by starting the comment line with a #.
- If a parameter value is formatted incorrectly or is outside the range of valid entries, the phone skips the value and moves to the next parameter. Errors are not logged in these cases.

7.4.4.2 Example of a Custom Configuration File

Assume that you want to configure the following custom settings on all of the 400-Series IP phones at your site:

- Specify a dedicated server other than the Headquarters server for ringtones and wallpaper (through the httpResources parameter)
- Specify a path where diagnostic log and capture files from the phones should be uploaded
- Use custom power settings as follows:
  - The phone screens return to partial brightness at 07:00 rather than the default of 06:00.
  - The phone screens enter sleep state (completely blank or dark) at 20:00 rather than the default of 19:00.
  - This schedule applies to the phone displays on weekdays and Saturdays, rather than the default of just weekdays.

To implement these custom configuration settings, you would add the following lines to `custom.txt`, which is the custom configuration file that applies to all models of 400-Series phones:

```
[system]

httpResources=http://10.53.53.53/fileserver

diagnosticServers=ftp://10.11.12.500/phonediagfiles


[power]

sleepInhibitStartTime=07:00

sleepInhibitStopTime=20:00

sleepInhibitDays=Mon,Tue,Wed,Thu,Fri,Sat
```

7.4.4.3 Receiving Configuration Settings from a Switch

After the configuration files are processed and the phones register with the system, they are automatically provided with the configuration information related to the system, their site, and the user assigned to the phone. This configuration information, which is specified in Connect Director and the Connect client,;overrides settings specified in configuration files. As changes are made in Connect Director or the Connect client,;these parameters are automatically kept up to date on the phones, whereas the configuration file values are provided only when the phone boots.

7.4.5 Configuration Parameters

Configuration Parameters lists the configuration parameters. The abbreviations listed in Source File Abbreviationsidentify the source of each parameter in the **Source** column in Configuration Parameters.

When adjusting values for any of the parameters in the [audiohaldm] group, keep in mind that analog gain and digital gain are cumulative values. To determine the total gain, add the analog gain and digital gain values. Be aware that increasing the gain level can cause echo in the network or distortion for users at either end. This distortion might be apparent only when one of the talkers is speaking loudly or close to the microphone.

Note:
This section contains detailed information that can be used to modify the behavior and functionality of your Mitel system. Make sure that you understand what you are doing before attempting to use this information to modify your system. Mitel is not responsible for any damage or expenses incurred through misuse of this information. If you have questions, contact Mitel Technical Support before attempting to modify your system.

Table 24: Source File Abbreviations

Source	Abbreviation in Table
DHCP Site Specific Option	DHCP
Configuration File	CFG
Manual Entry Using SETUP	Phone
Configuration Setting from the Voice Switch	SIP

Table 25: Configuration Parameters

Group	Parameter	Value Format and Default	Description	Source
[audio]	enableHacMode	on or off Default: off	Enable or disable hearing aid compatibility (HAC)	CFG
[audiohaldm]	gains.p2.handset MicAnalogGain	A numerical value between 12 (louder) and 0 (quieter). Values must be divisible by 3. Default: 6	The handset micr ophone analog gain l evel for the IP420	CFG
[audiohaldm]	gains.p8.handset MicAnalogGain	A numerical value between 12 (louder) and 0 (quieter). Values must be divisible by 3. Default: 6	The handset micr ophone analog gain level for the IP480 a nd IP480g	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p8cg.handsetMicAnalogGain	A numerical value between 12 (louder) and 0 (quieter). Values must be divisible by 3. Default: 6	The handset microphone analog gain level for the IP485g	CFG
[audiohaldm]	gains.p2.handsetMicDigitalGain	A numerical value between 9 (loud) and -3 (soft). Values must be divisible by 3. Default: 3	The handset microphone digital gain level for the IP420	CFG
[audiohaldm]	gains.p8.handsetMicDigitalGain	A numerical value between 9 (loud) and -3 (soft). Values must be divisible by 3. Default: 3	The handset microphone digital gain level for the IP480 and IP480g	CFG
[audiohaldm]	gains.p8cg.handsetMicDigitalGain	A numerical value between 9 (loud) and -3 (soft). Values must be divisible by 3. Default: 3	The handset microphone digital gain level for the IP485g	CFG
[audiohaldm]	gains.p2.handsetSpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The handset speaker analog gain level for the IP420	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p8.handsetSpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The handset speaker analog gain level for the IP480 and IP480g	CFG
[audiohaldm]	gains.p8cg.handsetSpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The handset speaker analog gain level for the IP485g	CFG
[audiohaldm]	gains.p2.handsetSpeakerDigitalGain	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The handset speaker digital gain level for the IP420	CFG
[audiohaldm]	gains.p8.handsetSpeakerDigitalGain	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The handset speaker digital gain level for the IP480 and IP480g	CFG
[audiohaldm]	gains.p8cg.handsetSpeakerDigitalGain	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The handset speaker digital gain level for the IP485g	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p2.headset MicAnalogGain	A numerical value between 18 (louder) and 6 (quieter). Values must be divisible by 3. Default: 12	The headset micr ophone analog gain l evel for the IP420	CFG
[audiohaldm]	gains.p8.headset MicAnalogGain	A numerical value between 18 (louder) and 6 (quieter). Values must be divisible by 3. Default: 12	The headset micr ophone analog gain level for the IP480 a nd IP480g	CFG
[audiohaldm]	gains.p8cg.heads etMicAnalogGain	A numerical value between 18 (louder) and 6 (quieter). Values must be divisible by 3. Default: 12	The headset micr ophone analog gain l evel for the IP485g	CFG
[audiohaldm]	gains.p2.headset MicDigitalGain	A numerical value between 9 (louder) and -3 (quieter). Values must be divisible by 3. Default: 3	The headset micr ophone digital gain level for the IP420	CFG
[audiohaldm]	gains.p8.headset MicDigitalGain	A numerical value between 9 (louder) and -3 (quieter). Values must be divisible by 3. Default: 3	The headset micr ophone digital gain level for the IP480 and IP480g	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p8cg.headsetMicDigitalGain	A numerical value between 9 (louder) and -3 (quieter). Values must be divisible by 3. Default: 3	The headset microphone digital gain level for the IP480g	CFG
[audiohaldm]	gains.p2.headseSpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The headset speaker analog gain level for the IP420	CFG
[audiohaldm]	gains.p8.headseSpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The headset speaker analog gain level for the IP480 and IP480g	CFG
[audiohaldm]	gains.p8cg.headse SpeakerAnalogGain	A numerical value between -6 (louder) and -18 (quieter). Values must be divisible by 3. Default: -12	The headset speaker analog gain level for the IP485g	CFG
[audiohaldm]	gains.p2.headsetSpeakerDigitalGain	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The headset speaker digital gain level for the IP420	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p8.headset SpeakerDigitalGa in	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The headset spea ker digital gain lev el for the IP480 and IP480g	CFG
[audiohaldm]	gains.p8cg.heads etSpeakerDigital Gain	A numerical value between 6 (louder) and -6 (quieter). Values must be divisible by 3. Default: 0	The headset spea ker digital gain level for the IP485g	CFG
[audiohaldm]	gains.p2.sideTon eGaindB	A numerical value between -9 (very loud) and -33 (quiet). Values must be divisible by 3. Default: -24	The handset/ headset sidetone level for the IP420 Sidetone refers to the level at which you hear your voice while speaking into a handset.	CFG
[audiohaldm]	gains.p8.sideTon eGaindB	A numerical value between -9 (very loud) and -33 (quiet). Values must be divisible by 3. Default: -24	The handset/ headset sidetone level for the IP480 and IP480g Sidetone refers to the level at which you hear your voice while speaking into a handset.	CFG

Group	Parameter	Value Format and Default	Description	Source
[audiohaldm]	gains.p8cg.sideToneGaindB	A numerical value between -9 (very loud) and -33 (quiet). Values must be divisible by 3. Default: -24	The handset/ headset sidetone level for the IP485g Sidetone refers to the level at which you hear your voice while speaking into a handset.	CFG
[headsetctl]	headsetCtl	On or Off Default: Off	This setting enables a user to use the electronic hook switch feature with a wireless headset that uses the Plantronics APD-80 adapter cable. If you want to enable this feature for a user of the IP420 or IP420g phone models, in Connect Director you must also set the **Users**> **Users** > **Telephony** > **Automatic off-hook** option to Wireless headset.	CFG Phone

Group	Parameter	Value Format and Default	Description	Source
[headsetctl]	headsetCtl (continued)		On the IP420 and IP420g models, this feature can be enabled only through a configuration file. On the IP480, IP480g, and IP485g models, administrators can enable the feature through a configuration file or end users can set the APD80 option through the phone interface (Options > Headset type> APD80), as described in the phone user guides.	
[net]	dot1XEnable	On or Off Default: On	Enable or disable 802.1x network	CFG Phone
[net]	dnsAddress	Comma-separated list of IP addresses	The default list of static DNS servers	DHCP CFG Phone
[net]	ntpServerAddress	Comma-separated list of IP addresses	The default list of Network Time Protocol servers	DHCP CFG Phone
[net]	policyCache	On or Off Default: On	Enable or disable caching of LLDP-MED network policy on the phone	CFG
[power]	idleBrightness	A number between 1 and 100, which indicates a percentage Default: 5	The intensity of the phone backlight when the phone is in the idle state	CFG

Group	Parameter	Value Format and Default	Description	Source
[power]	idleTimeout	A number that indicates minutes Default: 5	The number of minutes without phone activity (key presses or calls) that elapse before the phone transitions to the idle state, which dims the backlight. A value of 0 means that the phone never goes into the idle state.	CFG
[power]	sleepTimeout	A number that indicates minutes Default: 60	The number of minutes without phone activity (calls or key presses) that elapse before the phone transitions to the sleep state, which dims the backlight and lowers power usage depending on the settings for the sleepEthernetLowPower and sleepUsbSuspend parameters. A value of 0 means that the phone never goes into the sleep state. The value specified for the sleepTimeout parameter is in effect outside the hours specified by the sleepInhibitStartTime and sleepInhibitStopTime parameters.	CFG

Group	Parameter	Value Format and Default	Description	Source
[power]	sleepEthernetLowPower	On or Off Default: on	Whether or not the phone reduces Ethernet power when the phone is in a sleep state. If off, Ethernet power is not reduced.	CFG
[power]	sleepUsbSuspend	On or Off Default: on	Whether or not the phone supplies power to USB devices plugged into the USB port on the phone (on IP485g) when the phone is in a sleep state. If off, power to USB devices is not suspended when the phone is in a sleep state	CFG
[power]	sleepInhibitStartTime	A four-digit time on a 24-hour clock Default: 06:00	The time of day when the phone display goes from the sleep state to an idle state. This typically corresponds to the start of normal business hours at your site. During the hours when the sleep state is inhibited, the phone can go into an idle state, but it cannot go into a sleep state.	CFG

Group	Parameter	Value Format and Default	Description	Source
[power]	sleepInhibitStop Time	A four-digit time on a 24-hour clock Default: 19:00	The time of day when the phone transitions to the sleep state, in which the display turns blank or dark and other configured power-saving measures take effect. This typically corresponds to the end of normal business hours at your site	CFG
[power]	sleepInhibitDays	Comma-separated list of abbreviations for days of the week. Other valid values are “none” and “all”. Default: Mon, Tue, Wed, Thu, Fri	he days of the week when the sleepIn hibitStartTime andsl eepInhibitStopTime parameters are in eff ect	CFG
[syscontrol]	displayBrightnes sMax	A number between 1 and 100, which indicates a percentage Default: 100	The maximum inte nsity of the phone b acklight when the ph one is not in an idle or sleep state	CFG
[system]	diagnosticServers	A comma-separated list of IP addresses or full URL paths No default.	Specifies where log and capture file s generated by the phones are upload ed through FTP. The phone cycles thr ough the list of spe cified servers until it finds a server it can connect to.	CFG
[system]	enableSpeake rPhone	On or off Default: on	Specifies whether th e speakerphone is enabled. If off, only the handset or a hea dset can be used.	CFG

Group	Parameter	Value Format and Default	Description	Source
[system]	httpResources	An IP address or full URL path Default: `<Headquarters server/ fileserver` **Note**: To download wallpaper and ringtone using HTTPS set httpResources= https://(fqdn/ server ip)/ fileserver in custom.txt file.	The IP address or full URL path for a dedicated server that contains custom ringtone and wallpaper files. Typically, `/fileserver` points to the installation directory for the phone configuration files. By default, this is `<Drive>: \inetpub \ftproot\`	CFG
[system]	overrideConfigSe rvers	A comma-separated li st of IP addresses or fu ll URL paths	The configuration se rver with the highes t precedence. This c onfiguration server overrides the config uration server speci fied in DHCP option tag 156	CFG Phone
[system]	remoteSyslogger	A server address in the following format: `<IP_address or DNS_name>:port_ number;protocol`. The protocol is either tcp or udp. The protocol and port number are optional. If not specified, the default port is 514 and the default protocol is udp.	The address of the computer running the syslog server application.	CFG

Group	Parameter	Value Format and Default	Description	Source
[system]	longPressTimeForHistory	1500 (in milliseconds). **Note**: If no value is specified, the parameter is set to the value 1500 by default.	The configurable long press history button timer. A value (in milliseconds) within the admissible range can be configured. If the specified value is not within this range or if no value is specified, the parameter is set to its default value **Note**: The valid value range is from 1500 to 2500	CFG

Group	Parameter	Value Format and Default	Description	Source
[system]	enableUseOfHTTPS	true or false. Default is false.	If the value of enableUseOfHTTPS property is true, HTTPS will be used to download the config file; or else, HTTP will be used. **Note**: If the system has FQDN-based certificates, it is mandatory that 400-Series phone must be registered using server FQDN as the config server to download the config file using HTTPS.	CFG

Group	Parameter	Value Format and Default	Description	Source
[user]	apd80Selected	apd80Selected=true or false. Default is apd80Selected=false.	This setting configures the Headset Type on the 400-Series IP phone to be APD80. This is for users who have the Plantronics APD-80 adapter cable and need the **APD80** option enabled. In Connect Director, using the following path, you must set the Automatic off-hook preference option to Wireless headset: **Administration** > **Users** > **Users** > **Class of Service** > **Telephony tab** > **Automatic off-hook preference**	CFG SIP Phone

Group	Parameter	Value Format and Default	Description	Source
[user]	headsetType	One of the following values: Wired or Wireless Default: wired	The default headset type **Note**: SIP overrides the headset setting specified in a configuration file with the user's headset preference configured in Connect Director. Users can change the headset type on the IP480, IP480g, IP485g phones. For information about automatic off-hook and headset type settings, see the *MiVoice Connect System Administration Guide*.	CFG SIP Phone
[user]	timezone	The time zone, specified in plain text Default: Pacific Standard Time	The time zone for the time displayed on the phone. The time zone specified overrides the time zone value provided by the switch.	CFG Phone

7.5 Setting up an Alternate Configuration Server

If any of the default network configuration settings on the phone are not appropriate for your production network, to save time you might want to stage phones by using a custom configuration file on an alternate configuration server and network rather than manually changing the setting on each phone. To do this, you need to configure the phones using this method before connecting the phones to the Mitel system on the production network.

1. Set up a Web server that is appropriate for your operating system (such as IIS on a Windows server or Apache on a Linux server).

> **Note**:
>
> For details on setting up a Web server, consult the documentation for your operating system. When setting up a Web server for this purpose, it is generally appropriate to accept the default settings (such as using port 80 for an HTTP server) and permissions. For details about port usage, see Port Usage Tables on page 371.

2. On the Web server, create the following virtual directory where the custom configuration file will reside:

   `<httproot>/phoneconfig/`
3. Create the custom configuration file (for example, `custom.txt`) with the parameter setting appropriate for your purpose, and store it in the directory created in the previous step. (For details about creating custom configuration files, see Configuring 400-Series IP Phones on page 128.)
4. On the staging network, use DHCP option tag 156 or 66 to configure the ftpServers or configServers parameter to specify the Web server where the custom configuration file resides.

> **Note**:
>
> If you do not use DHCP to provide the configuration server value, you must enter the value manually on each phone.

5. Connect the phones to the staging network.

   Phones boot up and download the custom configuration file from the Web server. Because the phones have downloaded only configuration information and not switch information, the phones display a **No Service** message.
6. Connect the phones to the production network. (The configuration server value can be provided through DHCP option tag 156 or 66 or specified manually on each phone.)

   Phones boot up normally.

7.6 Migrating Phones Between Systems

The 400-Series phones were designed to be extremely secure and immune from compromise through the network. The first time a 400-Series phone is powered on and configured, it downloads the “UC Certificate Authority” certificate from the Headquarters Server and remembers it. After that, the phone connects only to services (SIPS, HTTPS) that provide certificates signed by that certificate authority or certificates signed by public certificate authorities.

If you need to move some or all 400-Series IP phones from one system to another and using MUTE CLEAR# on each phone would be burdensome, you can use the procedure described in this section.

While it is possible to move phones from one system to another, it is not possible to maintain the user binding for those phones. After moving the phones, an administrator can assign the phones to users through Connect Director, or users can assign themselves using the phone interface.

In the following procedure, the phones are being migrated from System A to System B.

Note:

Any 400-Series phones that are not operational during this process will not be able to reconnect to the system. For this reason, do not attempt this process during an upgrade or other down time.

1. Verify that System B has sufficient IP phone capacity for the phones that will be moved from System A.
2. Replace the UC Certificate Authority certificate/key on System A with the certificate/key from System B as follows:

   a. Ensure that System A is fully operational before attempting to replace the UC Certificate Authority.
   b. On System A, make a backup copy of the `<drive>:\Shoreline Data\keystore` directory.

   Note:

   You can accomplish this by doing a simple copy and paste using Windows Explorer.

   c. Copy the following private key and certificate files from System B and replace them in the same path on System A:

   ```
   <drive>:\Shoreline Data\keystore\private\hq_ca.key

   <drive>:\Shoreline Data\keystore\certs\hq_ca.crt
   ```

3. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**) stop and restart the WebFrameworkSvc service.

   This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.
4. Phones get their “Config Server” value through DHCP or by being entered directly on the phone, which is referred to as static configuration. Depending on your existing configuration for System A and System B, follow the instructions in the appropriate section below:

   - If the phones that you want to move are isolated to a subnet such that DHCP parameters pointing to the configuration server for System A can be modified, then follow the steps in If Both Systems Get Config Server Value from DHCP.
   - If the phones on System A are already using a static configuration or if you wish to move a subset of phones from System A to System B, but do not want to modify DHCP, then follow the steps in If Config Server Is from DHCP or Static for System A and Static for System B.

> **Note**:
>
> After a Phone has a static configuration, it is difficult to remove that configuration.

7.6.1 If Both Systems Get Config Server Value from DHCP

1. Modify your DHCP server to point to the IP address for System B by using the procedure in *MiVoice Connect Planning and Installation Guide* > *Network Requirements and Preparation* > *Configuring DHCP for IP Phones*.
2. Use the following procedure to reboot the phones you want to move:

   a. Launch Connect Director on System A, and in the navigation pane and click **Maintenance** > **Status and Maintenance** > **IP Phones**. The IP Phones page is displayed.
   b. Select the phones you want to move, and then select the **Reboot** command from the **Command** drop-down list and click **Apply**.
   c. In the **Confirmation** dialog, click **OK**.

   The selected phones reboot and get the new Config Server value for System B from DHCP and bind to System B.
3. Verify that the phones are in service on System B by checking the **Maintenance** > **Status and Maintenance** > **IP Phones** page in Connect Director.
4. On System A, delete the moved phones as follows:

   a. Launch Connect Director on System A, and in the navigation pane click **Administration** > **Telephones** > **Telephones**. The Telephones page is displayed.
   b. Select the phones you want to delete, and then click **Delete**.
   c. In the **Confirmation** dialog, click **OK**.The system deletes the selected phones.

5. Do one of the following:

   - If you plan to continue using System A and want it to have a certificate different from System B, restore System A's original certificate and private key:

     a. From the backup copy you made of System A's `<drive>:\Shoreline Data\keystore` directory, replace the private key and certificate files in the same path on Server A:

     ```
     <drive>:\Shoreline Data\keystore\private\hq_ca.key

     <drive>:\Shoreline Data\keystore\certs\hq_ca.crt
     ```

     b. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**), stop and restart the **WebFrameworkSvc** service.

     This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.

   - If you plan to leave the changed certificate on System A and you have a Mobility Router in your system, reboot the Mobility Router.

7.6.2 If Config Server Is from DHCP or Static for System A and B

1. On System A, edit the `<drive>:\inetpub\ftproot\phoneconfig\custom.txt file` to add the following lines, and then save and close the file:

   ```
   [system]

   overrideConfigServers=<IP address of System B Headquarters server>
   ```

> **Note**:
>
> When specifying the configuration server, be sure to use the IP address of your **System B** Headquarters server.

2. Use the following procedure to reboot the phones you want to move:

   a. Launch Connect Director on System A, and in the navigation pane click **Maintenance** > **Status and Maintenance** > **IP Phones**. The IP Phones page is displayed.
   b. Select the phones you want to move, and then select the **Reboot** command from the **Command** drop-down list and click **Apply**.
   c. In the **Confirmation** dialog, click **OK**.

   The selected phones download the new configuration setting. (However, the new configuration server is not applied until the phone is rebooted again.)

3. When the rebooted phones are back in service, reboot the phones again.

   The phones now honor their static configuration and bind to System B.
4. Verify that the phones are in service on System B by checking the **Maintenance** > **Status and Maintenance** > **P Phones**l page in Connect Director.
5. On System A, delete the moved phones as follows:

   a. Launch Connect Director on System A, and in the navigation pane click **Administration** > **Telephones** > **Telephones**. The Telephones page is displayed.
   b. Select the phones you want to delete, and then click **Delete**.
   c. In the **Confirmation** dialog, click **OK**. The system deletes the selected phones.
6. On System A, remove the lines added in Step 1 from your `custom.txt` file.
7. Do one of the following:

   - If you plan to continue using System A and want it to have a certificate different from System B, restore System A's original certificate and private key:

     a. From the backup copy you made of System A's `<drive>:\Shoreline Data\keystore` directory, replace the private key and certificate files in the same path on Server A:

     ```
     <drive>:\Shoreline Data\keystore\private\hq_ca.key

     <drive>:\Shoreline Data\keystore\certs\hq_ca.crt
     ```

     b. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**), stop and restart the **WebFrameworkSvc** service.

     This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.
   - If you plan to leave the changed certificate on System A and you have a Mobility Router in your system, reboot the Mobility Router.

7.7 Viewing IP Phone and BB424 Diagnostic Information

You can view diagnostic information about the 400-Series IP phones and BB424s in your system by using Connect Director.

You can view diagnostic information for a specific phone through that phone's user interface.

7.7.1 Viewing IP Phones and BB424s in the Mitel System

You can view information about the IP phones and BB424s in your Mitel system in the following ways:

- To check the status of IP phones and button boxes in your system, use one of the following methods:
  - To use the **Diagnostics and Monitoring system** in Connect Director to view the **IP Phones status** page, click **Maintenance** > **Status and Maintenance** > **IP Phones**.
  - To use Connect Director to view the **IP Phones page**, click **Administration** > **Telephones** > **Telephones**.

- To view the number of IP phones connected through a switch and the switch's phone configuration capacity, check the switch configuration information in Connect Director. Click **Administration** > **Appliances/Servers** > **Platform Equipment** and select the particular switch.

For details about viewing IP phone information, see the *MiVoice Connect System Administration Guide*.

7.7.2 Viewing Diagnostic Information on a Phone

By pressing a key combination on a phone's key pad, you can access various types of diagnostic information for a phone.

7.7.2.1 Viewing Real-Time System Status on a Phone

You can see the following real-time system status information for a phone:

- CPU load
- Memory usage
- Percentage of storage space used

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.
2. With the **System** submenu highlighted, do one of the following:
   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   Details for CPU load, memory usage, and storage space are displayed.
3. To return to the **Diagnostics** menu, do one of the following:
   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key or press the selector button on the navigation key pad.
4. To exit, do one of the following:
   - On the IP420, scroll to the bottom of the Diagnostics menu to select the **Exit** option and then press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Exit** soft key or press the selector button on the navigation key pad.

7.7.2.2 Using Ping to Check the Status of an IP Address

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.
2. Use the navigation key pad to scroll to the Ping submenu.

3. With the **Ping** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The Ping screen is displayed.

> **Note**:
>
> To proceed directly to the **Ping** screen, press the **MUTE** key followed by **7464#** (**PING#**).

4. Use the numbers or letters on the key pad to enter an IP address. On an IP480, IP480g, or IP485g, you also have the option of entering a DNS name.

> **Note**:

   - Press the * key to insert a period in an IP address or DNS name.
   - On the IP420, press the **speakerphone** button to backspace. To proceed with the value you have entered, press **#**.

5. Do one of the following:

   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **Start** soft key or press the selector button on the navigation key pad.

   The phone pings the IP address or DNS server five times, and then reports the ping statistics.

6. To return to the Diagnostics menu, do one of the following:

   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key or press the selector button on the navigation key pad.

7. To exit, do one of the following:

   - On the IP420, scroll to the bottom of the Diagnostics menu to select the **Exit** option and then press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Exit** soft key or press the selector button on the navigation key pad.

7.7.2.3 Using Traceroute to Determine the Network Route to a Host

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.

2. Use the navigation key pad to scroll to the Traceroute submenu.
3. With the **Traceroute** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The Traceroute screen is displayed.
4. Use the key pad to enter an IP address. On an IP480, IP480g, or IP485g, you can also enter a DNS name.

Note:

   - Press the * key to insert a period in an IP address or DNS name. In non-numeric mode (which is set through the left soft key), press the * key repeatedly to insert other symbols such as */ : @*.
   - On the IP420, press the **speakerphone** button to backspace. To proceed with the value you have entered, press **#**.
5. Do one of the following:

   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **Start** soft key or press the selector button on the navigation key pad.

   The phone displays the network route for the IP address or DNS server.
6. To return to the Diagnostics menu, do one of the following:

   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **Back** soft key or press the selector button on the navigation key pad.
7. To exit, do one of the following:

   - On the IP420, scroll to the bottom of the Diagnostics menu to select the **Exit** option and then press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Exit** soft key or press the selector button on the navigation key pad.

7.7.2.4 Capturing Packets for Phone Network Traffic

To diagnose problems on a phone, you might need to capture packets to see details about network traffic to and from the phone. You can capture packets by using the phone interface, which is described here, or you can initiate packet capture and view the results (using Wireshark or a similar network protocol analysis tool) through the Diagnostics Monitoring system. For details, see the *MiVoice Connect System Administration Guide*.

On the 400-Series IP phones signaling packets are encrypted, and packet capture tools available on the network cannot decrypt these packets. However, using the packet capture tool built into the phone, both the encrypted and decrypted versions of the packets are displayed.

The packet capture can run for up to two hours or until the resulting .pcap file reaches 70 MB.

If you specify a location through the diagnosticServers configuration parameter, packet capture (.pcap) files are uploaded to that location. (For details, see Configuration Parameters.) If your installation does not have a `diagnosticServers` path configured, by default the `.pcap` files from the capture operation are uploaded to the following directory on the Headquarters server:

`<Drive>:\inetpub\ftproot` (or the default FTP location on the server)

However, unless this directory allows anonymous write access (which is not recommended), uploading the capture file to this directory will fail.

Uploaded packet capture files are named as follows:

`<Phone MAC address>_YYYYMMDD_HHMMSS.pcap`

Where:

`YYYYMMDD` is the date (four-digit year, two-digit month, and two-digit day) when the `.pcap` file was created on the phone.

`HHMMSS` is the time (two-digit hour, two-digit minute, and two-digit second) when the `.pcap` file was created on the phone.

The results of a packet capture operation are also accessible through the phone interface until you start a new packet capture operation.

1. With the phone on hook, press the **MUTE** key followed by **73887#** (**SETUP#**). The **Password** prompt opens.
2. Enter the admin password, and press the **OK** soft key.
3. Use the navigation key pad to scroll to the **Diagnostics** submenu, and press the **Open** soft key.
4. Use the navigation key pad to scroll to the **Capture** submenu.
5. With the **Capture** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The Capture screen is displayed.
6. Do one of the following:

   - On the IP420, with **Start** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Start** soft key.

   The phone starts capturing packets. On the IP480, IP480g, and IP485g, you can see captured packet information on the phone display. You can drill down to get details about a packet by pressing the **Details** soft key.

Note:

While the packet capture operation is running, you can exit the Admin options menu and perform the problematic phone operation so that packets for that particular operation can be captured and used to diagnose the problem. After running the problematic scenario, return to the Capture page using steps 1-5 in this procedure and then proceed with step 7 to stop the packet capture operation.

7. To stop the capture process, do one of the following:
   - On the IP420, with **Stop** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Stop** soft key.
8. Optionally, on the IP480, IP480g, and IP485g, before or after you stop the capture process you can filter the results by protocol or IP address:
   - To filter by protocol, enter the protocol in the filter box. (For example, enter **SIP**.)
   - To filter by IP address, in the filter box enter `ip.addr==<IP_address>`.

Note:

- To enter a period in an IP address, press the * key.
- To enter the **=** symbol, while in either uppercase or lowercase alphanumeric entry mode, press the * key several times to move through various symbols until the **=** symbol is displayed.
- You can change the entry mode by pressing the soft key on the left.

9. Optionally, to see the contents of a packet on the IP480, IP480g, or IP485g, press the Details soft key.
10. To upload the captured packet information, do one of the following:
    - On the IP420, with **Upload** highlighted, press the selector button on the navigation key pad. After receiving a message about the upload process, press **#** to continue.
    - On the IP480, IP480g, and IP485g, press the **Upload** soft key. The phone returns a message to let you know whether the upload operation succeeded.
11. To return to the Diagnostics menu, do one of the following:
    - On the IP420, with **Back** highlighted press the selector button on the navigation key pad.
    - On the IP480, IP480g, and IP485g, press the **Back** soft key or press the selector button on the navigation key pad.
12. To exit, do one of the following:
    - On the IP420, scroll to the bottom of the Diagnostics menu to select the **Exit** option and then press the selector button on the navigation key pad.
    - On the IP480, IP480g, and IP485g, press the **Exit** soft key or press the selector button on the navigation key pad.

7.7.2.5 Clearing a Phone's Configuration

To return a phone to the factory settings, you can clear the phone's configuration through the Diagnostics menu. If you move phones from one Mitel system to another, you need to clear each phone's configuration.

You can also clear a phone's configuration by using **MUTE 25327#** (**CLEAR#**), which is described in Clearing a Phone's Configuration Settings on page 175.

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.
2. Use the navigation key pad to scroll to the Clear configuration submenu.
3. With the **Clear configuration** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The **Clear configuration** screen is displayed.
4. Do one of the following:

   - On the IP420, with **Clear & reboot** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Clear** soft key.

   The phone reboots.

7.7.2.6 Resetting a Phone

You can reset (reboot) a phone through the Diagnostics menu.

You can also reset a phone by using MUTE (**73738# RESET#**), which is described in .

You can also clear a phone's configuration by using **MUTE 73738#** (**RESET#**), which is described in Resetting an IP Phone.

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.
2. Use the navigation key pad to scroll to the **Reset phone** submenu.
3. With the **Reset phone** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The **Reset phone** screen is displayed.
4. Do one of the following:

   - On the IP420, with **Reset** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Reset** soft key.

   The phone reboots.

7.7.2.7 Uploading a Phone's Log

If a phone user experiences problems, you or the user might want to upload logs to debug the problem.

If you specify a location through the diagnosticServers configuration parameter, or through the Diagnostics server item on the phone's Diagnostics menu, log files are uploaded to that location. (see Configuration Parameters.) For information about how to specify a diagnostic server from a phone, see Configuring a Diagnostic Server from the Phone Interface on page 168.)

Note:

- For log upload from Connect Director using HTTPS, set the upload location for logs to `https://` `followed by HQ server IP address or FQDN` (for example, https://1.1.1.1) in Connect Director. If the system has FQDN-based certificates, it is mandatory that you provide the FQDN instead of the server IP address.
- For log upload from the phone using HTTPS, set `diagnosticservers=https://(FQDN/server IP address of HQ server)/hfs/api/v1/upload/phone` in the `custom.txt` file. For example, `https://1.1.1.1/hfs/api/v1/upload/phone`. If the system has FQDN-based certificates, it is mandatory that you provide the FQDN instead of the server IP address.
- The logs will be uploaded to `<drive>:\inetpub\ftproot\uploads\phone` if HTTPS is used for upload.

If your installation does not have a `diagnosticServers` path configured, by default the `.tgz` files from the capture operation are uploaded to the following directory on the Headquarters server:

If your installation does not have a diagnosticServers path configured,;by default the log files are uploaded to the following directory on the Headquarters server:

`<Drive>:\inetpub\ftproot` (or the default FTP location on the server)

However, unless this directory allows anonymous write access (which is not recommended), uploading the log files to this directory will fail.

Uploaded log files are named as follows:

`<Phone MAC address>_YYYYMMDD_HHMMSS.tgz`

Where:

`YYYYMMDD` is the date (four-digit year, two-digit month, and two-digit day) when the `.tgz` file was created on the phone.

`HHMMSS` is the time (two-digit hour, two-digit minute, and two-digit second) when the `.tgz` file was created on the phone.

1. With the phone on hook, press the **MUTE** key followed by **73887#** (**SETUP#**). The **Diagnostics** menu opens.
2. Use the navigation key pad to scroll to the **Log upload** submenu.
3. With the **Log upload** submenu highlighted, do one of the following:

   - On the IP420, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Open** soft key or press the selector button on the navigation key pad.

   The **Log upload** screen is displayed.
4. To start the log upload, do one of the following:

   - On the IP420, with **Start** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Start** soft key.
5. As the log upload is running, do one of the following:

   - To cancel the log upload after it has started:

     - On the IP420, with **Stop** highlighted, press the selector button on the navigation key pad.
     - On the IP480, IP480g, and IP485g, press the **Cancel** soft key and then the **OK** soft key.
   - To continue the log upload in the background:

     - On the IP420, with **Back** highlighted press the selector button on the navigation key pad or wait for the log upload to complete.
     - On the IP480, IP480g, and IP485g, press the **Back** soft key or wait for the log upload to complete.

     The phone displays a message indicating whether the log upload was successful.
6. When the log upload is finished, do one of the following:

   - On the IP420, press **#**.
   - On the IP480, IP480g, and IP485g, press the **OK** soft key.
7. To return to the Diagnostics menu, do one of the following:

   - On the IP420, with **Back** highlighted press the selector button on the navigation key pad .
   - On the IP480, IP480g, and IP485g, press the **Back** soft key or press the selector button on the navigation key pad.
8. To exit, do one of the following:

   - On the IP420, scroll to the bottom of the Diagnostics menu to select the **Exit** option and then press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Exit** soft key or press the selector button on the navigation key pad.

7.7.2.8 Configuring a Diagnostic Server from the Phone Interface

1. With the phone on hook, press the **MUTE** key followed by **3424#** (**DIAG#**). The **Diagnostics** menu opens.
2. Use the navigation key pad to scroll to the **Diagnostic server** submenu.

3. Press the **Edit** soft key. The **Diagnostic servers** screen is displayed.
4. Enter the IP address of a server where phone diagnostic server information will be uploaded, and then press the **Back** soft key. (For information about the path, see Uploading a Phone's Log on page 167.)

   The Diagnostics menu is displayed.
5. Do one of the following:

   - To configure another diagnostic server, repeat steps 3-4.
   - To exit, press the **Exit** soft key.

7.7.3 Viewing Diagnostic Information for a BB424 Button Box

You can view information about a BB424 device, such as its IP address, its position in a sequence of BB424 devices, and its MAC address.

1. Press and hold the first and fourth page indicator buttons on the BB424 for three seconds.

   The BB424 displays the Info menu with details about the BB424.
2. To advance to the next page of information, press the programmable button to the right of **Next**.

   The second page of the Info menu is displayed.
3. To return the BB424 to normal operation, press the programmable button to the right of **Next**.

   The BB424 exits the Info menu and returns to displaying labels for the programmed buttons.

7.7.4 Diagnostic and Failure Messages for 400-Series IP Phones

Diagnostic failure and error messages for the 400-Series IP phones are displayed on the phone, in remote and local syslog output, or both.

You can get more information about the status of a phone by using **MUTE 4636#** (**INFO#**) to enter the Admin options menu. Error conditions are indicated as follows:

- On the IP480, IP480g, or IP485g models, scroll to the submenu marked by an  icon, open that submenu, and with the error highlighted press the **Details** soft key. In addition, when an error message (such as "No service") is displayed on a phone, you can see details about the error by pressing the **Details** soft key.
- On the IP420,;scroll to the submenu marked by **!**, press the selector button on the navigation key pad, and scroll to the menu item marked by **!**. The **>** character indicates that details are available. Press the selector button to see details about the error condition. Press the selector button again to leave the error details page.

Note:

Though the Admin options menu displayed when you use **MUTE 4636#** (**INFO#**) is similar to the menu displayed when you use **MUTE 73887#** (**SETUP#**), the error indicators ( or **!** are not displayed when you access the Admin options menu through **73887# MUTE** (**SETUP#**).

In addition to messages displayed on the phone, syslog messages of CRITICAL, ALERT, and EMERGENCY priority levels are sent to a remote syslog server if configured. To configure a remote syslog server, you must specify a value for the remoteSyslogger configuration parameter. For more information about configuring the remoteSyslogger parameter, see Configuration Parameters.

The Error Messages table describes some of the important diagnostic and failure messages that may be displayed on 400-Series IP phones or in remote syslog output. (Other messages are self-explanatory.) The messages in the Error Messages table are listed in alphabetical order.

Table 26: Error Messages

Message on Phone or BB424 Display	Message in Remote Syslog and/or in Details View of Phone	Message Interpretation and Action
802.1X user, 802.1X password	802.1X authentication failed	802.1X authentication has failed. Reboot the phone. If that does not address the problem, check the VLAN configuration.
Button box HW Revision mismatch		There is a hardware version mismatch between the phone and the BB424 button box, which means that the button box and the phone are not compatible and will not work together.
Download failed		If you have a dedicated server configured for the httpResources configuration parameter, check the status of that server. Otherwise, check the status of the Headquarters server.
Download file missing		If you have a dedicated server configured for the httpResources configuration parameter, check the status of that server. Otherwise, check the status of the Headquarters server.
Download server busy		If you have a dedicated server configured for the httpResources configuration parameter, check the status of that server. Otherwise, check the status of the Headquarters server.
Error applying hotfixes		Confirm that the hotfix is applicable to the current phone release. If the hotifx is not applicable, remove it.

Message on Phone or BB424 Display	Message in Remote Syslog and/or in Details View of Phone	Message Interpretation and Action
Error downloading hotfixes		The hotfix could not be obtained from the server. Ensure that the hotfix specified in the phone configuration files on the server matches the hotfix files installed on the server.
Failed to connect to server		Check the status of the Headquarters server.
Invalid SNTP time zone		In Connect Director, on the Sites page check the value of the Time Zone parameter.
Log generation failed		Reboot the phone and try the log upload again.
Log upload failed		Reboot the phone and try the log upload again. If the diagnosticServers configuration parameter was used to specify a destination for log and capture uploads, check thestatus of that server. Otherwise, check the status of the Headquarters server.
Maximum allowed number of button boxes exceeded		The phone has detected that there are more than four BB424 button box devices connected through USB cables.
No compatible host discovered		This message is displayed on the BB424 button box in the following cases: • The button box was not able to connect to the phone. • There is a hardware version mismatch between the phone and the BB424.
No config server specified		If using DHCP, ensure that a configuration server is specified in the settings for DHCP option tag 156 and/or option tag 66. If not using DHCP, use MUTE 73887# (SETUP#) to specify a configuration server. For details, see Entering SETUP from the Key Pad
No download server configured		If you have a server configured for the httpResources configuration parameter, check the status of that server. Otherwise, check the status of the Headquarters server.
No download server could be reached		If you have a dedicated server configured for the httpResources configuration parameter, check the status of that server. Otherwise, check the status of the Headquarters server.
No Service	No SIP server found in config	The phone cannot connect with a SIP switch because no switch is configured. The phone did not obtain the IP address of a SIP switch from the configuration files. The most likely cause of this error is that the configuration server is down.

Message on Phone or BB424 Display	Message in Remote Syslog and/or in Details View of Phone	Message Interpretation and Action
	SIP authorization failed	You can obtain details about the error condition as follows: • On the IP480, IP480g, or IP485g models, press the Details soft key. • On the IP420, the > character indicates that details are available. Press the selector button on the navigation key pad, and scroll to the menu item marked by !. Press the selector button to see details about the error condition.
No Service	SIP bad request SIP connection keep-alive timeout SIP connection timeout SIP invalid username SIP permission denied SIP registration failed SIP registration stopped SIP server internal error SIP server timeout SIP service unavailable SIP switch failure, stale calls will be dropped	If you need more information to resolve the problem, you can perform the following actions in the following order until the problem is resolved: • Use the Ping or Traceroute tools in the phone's Diagnostic menu to check network connectivity to the voice switch and configuration server. • Check the status of the phone's call control switch. If the switch is down, the phone cannot register with the switch. The problem should resolve when the switch returns to normal operation. • Check the date and time on the phone's display while the phone is idle. If the date and time are not current, there might be a problem with certificate verification. Ensure that the SNTP server settings are valid, and then reboot the phone. • Press the Details soft key (on the IP480, IP480g, and IP485g) or the selector button on the navigation key pad (on the IP420) and select the Services menu. Select the SIP submenu, and monitor the IP address. If the SIP IP address changes every few seconds, the phone is actively trying tofind a voice switch with which to register, which could indicate a problem. Check the status of the Headquarters server and the switches.

Message on Phone or BB424 Display	Message in Remote Syslog and/or in Details View of Phone	Message Interpretation and Action
No Service	SIP switch failure, stale calls will be dropped	• If the switch is operating normally, these messages could indicate a problem with the phone's configuration. To address the issue, try rebooting the phone. If that does not address the problem, use MUTE 25327# (CLEAR#) to clear the phone's configuration. For details, see Clearing a Phone's Configuration on page 166
No Ethernet	No Ethernet link detected	If "No Ethernet" is displayed on the phone while the phone reboots, you can ignore the message because it is a normal part of the phone boot-up process. If "No Ethernet link detected" is displayed in the remote syslog output, then there might be an issue with the Ethernet connection. Check the network connection and/or reboot the phone.
No upload server configured		If the diagnosticServers configuration parameter was used to specify a destination for log and capture uploads, check the status of that server. Otherwise, check the status of the Headquarters server.
No upload server could be reached		If the diagnosticServers configuration parameter was used to specify a destination for log and capture uploads, check the status of that server. Otherwise, check the status of the Headquarters server.
No valid config server present		The phone has attempted to contact all configuration servers specified through DHCP option tags 156 or 66 or set manually through MUTE 73887# (SETUP#), but no configuration server is reachable. Check the status of the configuration server or servers.
	Phone application initialization: Remote syslog diagnostic message for <MAC Address>	This message is captured in the remote and local syslog when the phone reboots, regardless of the reason for the reboot.
	Phone crash for <MAC Address>	An error has occurred, causing the phone to automatically reboot.
	Phone deadlock detected for <MAC Address>	An error has occurred, causing the phone to automatically reboot.
	SIP server <IP Address> connection failure for <MAC Address>	The phone's connection to the switch was lost due to a switch or network issue. For example, the switch could be down because of a switch reboot or a switch error condition. Check the status of the switch and the network.

Message on Phone or BB424 Display	Message in Remote Syslog and/or in Details View of Phone	Message Interpretation and Action
Unassign user: Operation failed		There was an error during the user unassignment operation.
User assignment: Anyphone not allowed		The user assignment failed because the server sent an Anyphone not allowed response. Check the user's settings on the Headquarters server.
User assignment: CAS Connection failure	CAS failed to connect	The phone failed to establish a connection to CAS. As a result, no CAS-driven features (such as History and Directory) are available on the phone. Check the status of the Headquarters server. If you see this message in remote syslog output during initial bootup, wait several seconds for the error to clear and try again.
User assignment: CAS invalid login	CAS login failed	During an attempt to assign a phone to a user, the user extension and/or password provided were invalid.
User assignment: Permission required		The user assignment failed because the phone received a response from the Headquarters server indicating that the user does not have adequate permissions for the operation being attempted on the phone. Usually, this means that in Connect Director the user is not configured with the permissions necessary to execute a particular operation, such as using VPN and remotely authenticating with the server.

7.8 Displaying Settings for an IP Phone

1. With the phone on hook, press the **MUTE** key followed by **4636#** (**INFO#**). The Admin Options menu opens.
2. Use the navigation key pad and the selector button to scroll through and open the submenus as necessary to see the phone's settings.

   For descriptions of the parameters, see Phone Information for 400-Series IP Phones.

   To close the Admin options menu, do one of the following:

   - On the IP420, with **Exit** highlighted press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Exit** soft key.

7.9 Resetting an IP Phone

1. With the phone on hook, press the **MUTE** key followed by **73738#** (**RESET#**). The phone displays the Reset phone screen.
2. Do one of the following:

   - On the IP420, with **Reset** highlighted press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Reset** soft key.

   The phone reboots and applies settings.

7.10 Resetting a BB424

The following procedure resets all BB424 devices in a configuration. Performing the action on one BB424 device performs the reboot on all connected BB424 devices.

1. Press and hold the first and fourth page indicator buttons on the BB424 for three seconds.

   The BB424 displays the Info menu with details about the BB424.
2. To reset the BB424, press the programmable button to the left of **Reset**.

   The BB424 displays a confirmation message.
3. Press the programmable button to the left of **Reset**.

   The BB424 reboots.

7.11 Clearing a Phone's Configuration Settings

You can clear a phone's configuration settings and return it to factory settings by entering a key sequence on the phone's key pad. If you move phones from one Mitel system to another, you need to clear each phone's configuration.

1. With the phone on hook, press the **MUTE** key followed by **25327#** (**CLEAR#**). The phone displays the **Clear Configuration** screen.
2. Do one of the following:

   - On the IP420, with **Clear & reboot** highlighted, press the selector button on the navigation key pad.
   - On the IP480, IP480g, and IP485g, press the **Clear** soft key.

   The phone reboots and applies settings.

7.12 Clearing a BB424’s Configuration Settings

You can clear a BB424’s configuration settings and return it to factory settings by pressing a combination of buttons on the BB424.;This should be necessary very rarely and only if recommended by Mitel Technical Support.

The following procedure clears the configurations for all BB424 devices that are connected to a phone. Performing the action on one BB424 device affects all of the connected BB424 devices.

1. Press and hold the first and fourth page indicator buttons on the BB424 for three seconds.

   The BB424 displays the Info menu with details about the BB424.
2. To reset the BB424, press the programmable button to the left of **Clear**.

   The BB424 displays a confirmation message.
3. Press the programmable button to the left of **Clear**.

   The BB424 reboots.

Configuring and Maintaining 6900-Series IP Phones

8

This chapter contains the following sections:

Important:

Any reference to the 6900-Series exclusively indicates the support of the following specified models: 6910, 6915, 6920, 6930, 6970, 6920w, 6930w, and 6940w.

This chapter provides details about configuring and maintaining the 6900-Series IP phones.

8.1 Overview

6900-Series IP phones are similar to 400-Series IP phones. Both use Session Initiation Protocol (SIP). In general, both provide telephony features similar to those provided by the other IP phone models. However, the configuration and maintenance procedures for the 6900-Series phones are slightly different from those for the 400-Series IP phones. Users familiar with using the 400-Series IP phones should have an easy transition to using the 6900-Series IP phones.

Note:
6900-Series IP phones support the download of configuration files from MiVoice Connect using HTTPS with TLS 1.2.

8.1.1 IP Phone Failover

When IP phone failover is enabled on the **IP Phone Options** page in Connect Director, if an IP phone cannot communicate with its switch, the phone automatically connects to another switch at the same site that has available configured IP phone resources. For IP phone failover to be effective, the system must be

planned with sufficient excess capacity to handle phones from at least one switch during a failover event. For example, if a switch with 20 IP phone ports fails, 20 IP phone ports need to be available elsewhere in the system.

8.1.2 Date and Time

6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones depend on a Network Time Protocol (NTP) server to authenticate a secure connection and to provide the date and time to be displayed on for the phone's screen. The time displayed on the phone is the GMT value provided by the NTP server plus the offset from the time zone setting of the phone. Users can set the time zone through the phone's Options menu.

The IP address of the NTP server is delivered to the phone through DHCP or is manually configured in the phone. In the absence of an accessible NTP server, the phone can obtain the time from its controlling switch.

8.1.3 IP Phones and Voice Switches

Voice switches provide configuration and call manager functionality for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones. Every site where IP phones are in use must have a voice switch configured to support the number of IP phones at the site. SIP Proxy ports are not required for the 6900-Series IP phones.

Similar to 400-Series phones, the voice switches provide configuration for the 6900-Series (6910, 6920, 6930, and 6940) phones in a different manner than for other phone models. When a 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phone downloads configuration files during the bootup process it receives a list of all available switches. The phone then randomly selects a switch from this list (starting with switches on the same subnet, if available) and attempts to register with the switch.

The contacted switch then redirects the phone to the appropriate call manager switch, which is the voice switch assigned to the phone to set up and tear down calls. The call manager switch handles the Session Initiation Protocol (SIP) information from the IP phones assigned to it and communicates call information to other switches in the system using SIP. After two IP endpoints are connected in a call, media streams are independent of the call manager switch.

After the phone registers with the call manager switch, any time the phone reboots it attempts to contact that same switch. If that switch does not respond, the phone attempts to contact another switch on the list until the phone successfully contacts a switch; the phone is then redirected to the appropriate call manager switch.

8.1.4 IP Phone Communications

Communications for 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones are routed through the following protocols:

- Secure Session Initiation Protocol (SIPS)
- Real-time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP)
- Client Application Server (CAS)

8.1.4.1 Secure Session Initiation Protocol (SSIP)

Secure Session Initiation Protocol (SIP) is a standard protocol that is based on a client-server model and works at the application layer. Through SIP, networked users can initiate a call or receive a call. The protocol configures the parameters for the session and handles the call setup and tear-down.

Mitel uses the secure version of SIP, SIPS, for signaling between voice switches and 6900-Series (6910, 6920, 6930, and 6940) IP phones.

8.1.4.2 RTP and SRTP

Media flow for the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones is either through Real-time Transport Protocol (RTP) or through Secure Real-time Transport Protocol (SRTP).

The use of SRTP, the encrypted version of RTP, depends on whether SRTP has been enabled through the Media Encryption option in the **Call Control** > **Options** page in Connect Director. If the Media Encryption option is set to **SRTP - 128 bit AES**, SRTP is used in the following scenarios:

- For calls between 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones configured as internal extensions, after the call is set up, media flows directly between the IP phones using SRTP.
- For calls between a 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phone and an external number over a trunk, after the call is set up, media flows via the trunk using SRTP.
- For three-way mesh conference calls between 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones, after the call is set up, media flows between the phones using SRTP.
- In Make Me conference involving up to eight 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones, media flows through SRTP when voice switches are used.
- For Conference calls involving 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones that are initiated through a service appliance, media flows through SRTP.

When SRTP is used to encode the audio, the secure nature of the call is indicated with a lock icon in the call window.

If the **Media Encryption** option is not enabled, the connection negotiation between two 6900-Series IP phones is through SRTP, but the resulting media stream between the two phones is through RTP.

If the **Media Encryption** option is not enabled, the media flow for calls between 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones and other IP phones uses RTP. Make Me conference calls that involve at least one non-6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phone and a 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phone also use RTP.

Note:

RTP is used in these scenarios even if SRTP is enabled through the Media Encryption option in Connect Director.

8.1.4.3 Client Application Server (CAS) Service

On the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, the Client Application Server (CAS) supplies information such as call history, configuration details, directory, workgroup agent status, and visual voicemail. If CAS is inaccessible, these services are not available, but a phone can still make and receive calls.

8.2 Updating IP Phone Firmware

While earlier phones automatically download available new firmware upon rebooting, updating firmware on the 6900-Series IP phones is a process you manage through the Diagnostics and Monitoring system that you access through Connect Director. For example, you can automatically maintain all 6900-Series IP phones at the recommended firmware level, or you can override the automatic updates if you want to select a different firmware version or disable automatic update for certain phone models or for specific phones.

Control of phone firmware updates is accomplished through global-update and override settings that you specify on the Phone Firmware Update page of Connect Director. For details, see the *MiVoice Connect System Administration Guide*.

To manage phone firmware on a more granular level, the **Diagnostics & Monitoring** interface provides a flexible approach for updating phone firmware because you can manage the firmware download and installation process in stages:

- If you want to download firmware to phones independently of installing it, use the `Download` command. You can choose to run this command at a time when you can spare the network bandwidth needed to accommodate the download. After firmware is loaded on the phones, you can, later on, use the `Update` or `Update When Idle` commands to install the firmware that you have already downloaded without downloading it again.
- If you want to download firmware to phones and install it immediately, use the Update command. You can also use this command to install phone firmware that you have downloaded.

When a group of phones at a site are selected for firmware download and the server is remote, some of the phones at the site automatically download firmware from other phones at the site for minimizing bandwidth utilization.

When phones are running at least the latest recommended firmware version, the value in the **Firmware Status** column is **Up to Date**. For more details about the possible values for Firmware Status, see the *MiVoice Connect System Administration Guide*.

If you are not using the automatic phone firmware update mechanism, you should upgrade phone firmware when the value in the **Firmware Status** column on the **Status** > **IP Phones** page is one of the following:

- **Firmware Version Mismatch** indicates that the phone's current firmware version is earlier than the minimum firmware version required for the phone.
- **Update Available** indicates that the phone is running an acceptable firmware version, but a more recent firmware version is available for download. In other words, the phone is running a firmware version later than or at the minimum version required, but earlier than the recommended version.

The **Advanced** option, which is available with the `Download`, `Update`, or `Update When Idle` commands, allows you to select a different firmware build for each model of phone. Furthermore, if there is more than one hardware version for each phone model, you can select a unique build to deploy to each phone as appropriate. The system prevents you from accidentally downloading a firmware version that is incompatible with a phone's hardware version. If there is no firmware version appropriate for a particular phone loaded on the server, you can select **Skip** from the **Version** drop-down list.

Because the Diagnostics and Monitoring system selects any available server from which to download the firmware update, you should ensure that all servers in the system, including servers that do not manage voice switches, have the latest firmware installed. This is because the Diagnostics and Monitoring system directs the phones to download from a server that does not have the specified firmware version, the download fails and the phones do not attempt to obtain the firmware from another server.

To download and install a firmware upgrade:

1. Launch Connect Director.
2. Click **Maintenance** > **Status and Maintenance** > **IP Phones**. The **IP Phones** page opens.
3. Select the check box for each phone for which you want to upgrade firmware.
4. In the **Command** drop-down menu, select **Update Firmware**.
5. Click **Apply**.
6. In the **Confirmation** dialog box, do one of the following:
   - To apply the recommended firmware version, click **OK**.
   - To select a particular firmware version:
     a. Click **Advanced**.
     b. For each type of phone selected, in the **Version** drop-down list, designate the firmware version.
     c. Click **OK**.

The **Firmware Status** column shows the progress as the firmware is downloaded and applied. The phones reboot after firmware is updated.

8.3 Boot Process

The boot process varies depending on whether your network uses Dynamic Host Configuration Protocol (DHCP) or static configuration:

- DHCP— IP phones are pre-configured to work with your network's DHCP server. After the servers and voice switches are configured, the phones are automatically added to your Mitel system when they are connected to the network. Upon booting, IP phones use the configuration server address to acquire their configuration specifications. The configuration server address is set in the DHCP site-specific options (option tag 156).
- Static configuration—If you are not using a DHCP server or the server is not currently online, you can set a static IP address and other startup parameters directly on the IP phone. For details, see Specifying Configuration Parameters on a Phone on page 182.

After the IP phone obtains the configuration server IP address or addresses, it downloads configuration files from the configuration server using HTTP (unless otherwise specified). If the configuration server

cannot be reached because of some kind of error (such as a timeout) but the phone was configured with multiple configuration server IP addresses, then the phone tries to download the configuration files from the other servers. If no configuration server can be reached, or if a configuration file cannot be located, the phone uses the last successfully loaded configuration parameters. After the phone completes downloading the configuration files, the current parameters are saved in flash memory.

8.4 Configuring 6900-Series IP Phones

This section describes how you can specify custom configuration parameters for the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones.

When a 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phone boots, it contacts the configured server and reads an initial configuration file from the server. You can override the default configuration parameters for a phone through DHCP site-specific options, through the phone interface, or through custom configuration files. As phone firmware is upgraded, some configuration information is overwritten, but parameters specified in custom configuration files are preserved across upgrades.

8.4.1 Parameter Precedence

While there are some exceptions, in general configuration parameters are processed by the phone in the following order. The last parameter source takes precedence:

- Defaults
- LLDP
- DHCP option tag 156
- Configuration files that reside on the server. The precedence order for these files is described in Processing Order for Configuration Files on page 189.
- Configuration settings from the voice switch

8.4.2 Specifying Configuration Parameters on a Phone

If you are not using a DHCP server to provide IP address and configuration parameters to the phones, you must manually configure the phones. You can enter the phone configuration menu at bootup or enter a key sequence from the phone's keypad after the phone has finished booting up.

For descriptions of the parameters you can set on a phone, see the following table

If you are using DHCP, be aware that the order of precedence for certain parameters varies:

- Setting the Config server parameter on the phone (through the **Settings** > **Advanced** > **Voice Services** > **MiVoice Connect** > **Config Server N** (where N is value 1 through 6) menu) overrides the configServers parameter specified through DHCP.

Table 27: Phone Information for 6900-Series IP Phones

Advanced Options Menu Item	Option Name	Description
Time and Date	Settings	This field allows you to set the date and time format. The following fields are populated by default: • Time Format: 24-Hour • Daylight Savings: Automatic • Date Format: WWW DD MMM
	Time Zone	This field allows you to set the time-zone of your region. The timezone is Custom by default.
	Set Date and Time	This field allows you to set the date and time **Note**: The **Use Network Time** field is selected by default
Status	Firmware Info	This field displays firmware information.
	Network	Depending on the network that is connected, the following fields are populated by default: • **IP Address** • **MAC Address** • **LAN Port** • **PC Port** • **Cloud Domain** • **Language** • **Time Zone** • **Country**
	Error Messages	This field displays error messages related to the IP phone.

Advanced Options Menu Item	Option Name	Description
Bluetooth		This field allows you to switch the audio from your Bluetooth-paired mobile phone to your Mitel desktop IP phone. This function is available if your mobile phone is synchronized with your desk phone through the Mitel Mobilelink feature. It provides the list of Paired and Available devices. **Note**: Bluetooth functionality is not available for 6930L and 6930LT IP phones.
Wi-Fi		This field allows to enable provisioning of WLAN adapter through phone TUI for 6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w IP phones.
Connect Services	MiVoice Connect > Config. Server	Depending on the configuration server provided by end user, this field displays the configuration server FQDN/IP address (that is, HQ/LDVS/Windows DVS server). **Note**: This option available only in the **Advanced** menu.
	MiCloud Connect > Cloud Domain	This field displays the current cloud domain used for routing of MiCloud Connect authentication requests.
Diagnostics	Troubleshooting	For details on these menu options, see Viewing Diagnostic Information about a Phone.
	Ping	
	Traceroute	
	Capture	
	Log upload	
	Diagnostic server	
	Audio Diagnostics	
Display	Home Screen	This field has a default timer of 1800 seconds for screen lock.

Advanced Options Menu Item	Option Name	Description
	Brightness	This field enables you to adjust the brightness level. it has the following options: • Brightness Level • Brightness Timer **Note**: The values in these fields are populated by default.
	Push Notifications	This field has the following options: • Sound • Bluetooth • External
Network	IPv6 Settings	This option allows you to enable the IPv6 address. **Note**: Currently, this option is not supported on MiVoice Connect.
	Settings	The following fields are enabled by default: • Use DHCP • DHCP User Class • DHCP Download Option • IP Address • Subnet Mask • Gateway • Primary DNS • Secondary DNS • Hostname

Advanced Options Menu Item	Option Name	Description
	Ethernet Ports	The following options are available: • LAN Port: Auto (default) • PC Port: Auto (default) • Port Mirror: Auto (default) • Pass Thru Port: Enable (default)
	Use 802.1Q	IEEE 802.1Q specifies the use of VLANs (Virtual LANs) on Ethernet. If EAP Type is EAP-MD5 or EAP-TLS, you must also specify values for the following fields: • EAP-TLS Settings • Identity • MD5 Password
Network (Continued)	VLAN	This option is the Virtual LAN identifier. This field is disabled by default and the following fields are populated by default: • LAN Port VLAN • LAN Port VLAN ID • SIP Priority • RTP Priority • RTCP Priority • Other Priority • PC Port VLAN • PC Port VLAN ID • PC Port Priority
	DSCP	This option provides the Differentiated Services Code Point (DSCP) value to be used for audio packets. This option has the following fields: • TypeService SIP • TypeService RTP • TypeService RTCP

Advanced Options Menu Item	Option Name	Description
	LLDP	This field allows you to enable or disable LLDP using the following options: • Disabled • Enabled
Configuration Server	Download Protocol	If you select **FTP**, complete the following fields: • FTP Server • FTP Path • FTP Username • FTP Password If you select, **TFTP**, complete the following fields: • Primary Server • Pri TFTP Path If you select, **HTTP**, complete the following fields: • HTTP Server • HTTP Path **Note**: The HTTP Port is 80 by default. If you select, **HTTPS**, complete the following fields: • HTTPS Server • HTTPS Path **Note**: The HTTPS Port is 443 by default. The Client Method is TLS Preferred by default

Advanced Options Menu Item	Option Name	Description
Restart		This option allows you to restart the phone.
Reset		This option allows you to set Factory Default settings.

8.4.3 Specifying Config Parameters through DHCP Options

By default, DHCP option tag 156 is used. The following parameters are specified in the site-specific options for option tag 156:

- configServers: Specify a comma-separated list of IP addresses or FQDN for the configuration server. If a server is not available, the phone cycles through the list of servers until it finds a working server.

> **Note**:
> The factory MiNET firmware only supports reading the first IP/FQDN value from the list of configServers as provided in DHCP option 156. Once the phone upgrades to appropriate SIP firmware, it will support the list of IP/FQDN from DHCP 156.

- ftpServers: Specify a comma-separated list of IP addresses or FQDN for the configuration server. If a server is not available, the phone cycles through the list of servers until it finds a working server.

> **Note**:
>
> The ftpServers parameter is provided for compatibility with sites running MGCP phones. 6900-Series IP phones use HTTP to download configuration files from servers specified in the ftpServers parameters. For new installations, the configServers parameters is recommended over the ftpServers parameter.

- vlanid

While DHCP Option 156 can be used to enable VLAN tagging and set the VLAN ID, it is not recommended because VLAN hopping after the DHCP address is acquired forces the phone to re-start the network stack on the new VLAN a second time. LLDP-MED is the preferred method to enable VLAN tagging.

The complete Option 156 syntax including VLAN tagging is:

```
vlanid=<number>,layer2tagging=<0|1>,configservers=<HQ Server IP/
FQDN>,ftpservers=<HQ Server IP/FQDN>
```

Note:
FQDN is required if Subject Alternative Name (SAN) is root certified.

Specify the parameters in any order, separating multiple parameters with a comma. Not all parameters are required. When providing multiple values for one parameter, use quotation marks around the comma-separated values. For example:

```
configServers="192.168.0.13, joe.test.com",vlanid=2
```

Note:
6900-Series (6910, 6920, 6930, and 6940) IP phones use HTTP to download their configuration files from the servers specified in DHCP option tag 156.

8.4.4 Specifying Config Parameters through Custom Config Files

The following table lists the configuration file names for the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones. These files are stored in the phone configuration directory created on the server when your Mitel system is installed. The default directory for these configuration files is as follows:

```
<Drive>:\inetpub\ftproot\phoneconfig
```

Table 28: 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP Phone Model Configuration Files

IP Phone Model	Custom Configuration File Name for All 6900-Series IP Phones	Model-Specific Custom Configuration File Name for 6900-Series IP Phones
6910	startup.cfg	6910.cfg
6920	startup.cfg	6920.cfg
6930	startup.cfg	6930.cfg
6940 6920w	startup.cfg startup.cfg	6940.cfg 6920w.cfg
6930w	startup.cfg	6930w.cfg
940w	startup.cfg	6940w.cfg

8.4.4.1 Processing Order for Configuration Files

Configuration files are processed in the following order:

- `country_ISO>.txt`, where ISO> is a two-character ISO country code (For example, the file for the United States is country_US.txt.)

  Do not edit these files. These files specify country-specific settings such as date/time formats.
- `generated.txt`

  Do not edit this file, because it is generated by the server and any changes would be overridden the next time the server generates the file. This file contains a list of voice switches for the phone and the default httpResources parameter setting, which specifies the default server path for wallpaper and ringtones. The server regenerates this file whenever the list of switches is updated.
- `startup.cfg`

  This is the base custom configuration file for all 6900-Series IP phones. Any configuration parameters that you add to this file are applied to all 6900-Series IP phones in your system.
- `<model>.cfg` (where <model> is (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w)

  This is the custom configuration file for a particular model of 6900-Series IP phone. Any configuration parameters that you add to this file are applied to all phones of that model at your site.
- `<mac>.cfg` (where <mac> is the MAC address of a phone)

  This is the custom configuration file for a particular phone as identified by its MAC address (the 12-digit number on the white sticker on the back of the phone). Any configuration parameters that you add to this file will be applied to the phone identified by the MAC address.

Note:

File names for MAC configuration files must be in lower case and not contain punctuation. The following is an example of a custom configuration file name for a particular phone identified by its MAC address: `<mac>.cfg`.

The phone-specific custom configuration file is the last file read. Any parameters in a custom configuration file override configuration parameters specified at a lower level of precedence, including the parameters entered on the phone, because they are processed first, before any configuration files are read. Any duplicate parameters specified in the configuration files are overridden according to their own precedence order.

Parameters are organized by group, and each parameter must begin on a new line within the proper group, as follows:

[group>]

parameter>=value>

parameter>=value>

[group>]

parameter>=value>

parameter>=value>

where

[group>] is the configuration parameter group as shown in Configuration Parameters.

value> is the name of the configuration parameter as shown in Configuration Parameters.

In specifying parameters, the following rules apply:

- IP addresses must be provided in dotted-decimal format.
- Parameters and values in configuration files are case sensitive.
- Cases are preserved in character strings unless otherwise indicated.
- Comments may be embedded in a configuration file by starting the comment line with a # symbol.
- If a parameter value is formatted incorrectly or is outside the range of valid entries, the phone skips the value and moves to the next parameter. Errors are not logged in these cases.

8.4.4.2 Receiving Configuration Settings from a Switch

After the configuration files are processed and the phones register with the system, they are automatically provided with the configuration information related to the system, their site, and the user assigned to the phone. This configuration information, which is specified in Connect Director and the Connect client,;overrides settings specified in configuration files. As changes are made in Connect Director or the Connect client,;these parameters are automatically kept up to date on the phones, whereas the configuration file values are provided only when the phone boots.

8.5 Configuring the Time Zone on 6900-Series Phones

To configure the time zone on 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, do the following:

1. Go to **Settings** ⚙
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.

> **Note**:
>
> If phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

4. Select **Time and Date** > **Time Zone**.
5. Select the desired option from the list of options displayed on the **Time Zone** screen.
6. Click **Save**.

8.6 Migrating Phones Between Systems

The 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones are designed to be extremely secure and immune from compromise through the network. The first time a 6900-Series (6910, 6920, 6930, and 6940) phone is powered on and configured, it downloads the “UC Certificate Authority” certificate from the Headquarters Server and remembers it. After that, the phone connects only to services (SIPS, HTTPS) that provide certificates signed by that certificate authority or certificates signed by public certificate authorities.

While it is possible to move phones from one system to another, it is not possible to maintain the user binding for those phones. After moving the phones, an administrator can assign the phones to users through Connect Director, or users can assign themselves using the phone interface.

To move a 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, got to **Settings** > **Advanced Settings** > **Reset**.

In the following procedure, the phones are being migrated from System A to System B.

Note:

Any 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones that are not operational during this process will not be able to reconnect to the system. For this reason, do not attempt this process during an upgrade or other down time.

1. Verify that System B has sufficient IP phone capacity for the phones that will be moved from System A.
2. Replace the UC Certificate Authority certificate/key on System A with the certificate/key from System B as follows:

   a. Ensure that System A is fully operational before attempting to replace the UC Certificate Authority.
   b. On System A, make a backup copy of the `<drive>:\Shoreline Data\keystore` directory.

   Note:

   You can accomplish this by doing a simple copy and paste using Windows Explorer.

   c. Copy the following private key and certificate files from System B and replace them in the same path on System A:

   ```
   <drive>:\Shoreline Data\keystore\private\hq_ca.key

   <drive>:\Shoreline Data\keystore\certs\hq_ca.crt
   ```

3. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**) stop and restart the WebFrameworkSvc service.

   This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.
4. Phones get their “Config Server” value through DHCP or by being entered directly on the phone, which is referred to as static configuration. Depending on your existing configuration for System A and System B, follow the instructions in the appropriate section below:

   - If the phones that you want to move are isolated to a subnet such that DHCP parameters pointing to the configuration server for System A can be modified, then follow the steps in If Both Systems Get Config Server Value from DHCP on page 193.
   - If the phones on System A are already using a static configuration or if you wish to move a subset of phones from System A to System B, but do not want to modify DHCP, then follow the steps in If Config Server Is from DHCP or Static for System A and B on page 194.

> **Note**:
>
> After a phone acquires a static configuration, it is difficult to remove that configuration.

8.6.1 If Both Systems Get Config Server Value from DHCP

1. Modify your DHCP server to point to the IP address/FQDN for System B by using the procedure in *MiVoice Connect Planning and Installation Guide* > *Network Requirements and Preparation* > *Configuring DHCP for IP Phones*.
2. Use the following procedure to reboot the phones you want to move:

   a. Launch Connect Director on System A, and in the navigation pane, and click **Maintenance** > **Status and Maintenance** > **IP Phones**. The IP Phones page is displayed.
   b. Select the phones you want to move, and then select the `Reboot` command from the **Command** drop-down list and click **Apply**.
   c. In the **Confirmation** dialog, click **OK**.

   The selected phones reboot and get the new Config Server value for System B from DHCP and bind to System B.
3. Verify that the phones are in service on System B by checking the **Maintenance** > **Status and Maintenance** > **IP Phones** page in Connect Director.
4. On System A, delete the moved phones as follows:

   a. Launch Connect Director on System A, and in the navigation pane click **Administration** > **Telephones** > **Telephones**. The Telephones page is displayed.
   b. Select the phones you want to delete, and then click **Delete**.
   c. In the **Confirmation** dialog, click **OK**. The system deletes the selected phones.

5. Do one of the following:

   - If you plan to continue using System A and want it to have a certificate different from System B, restore System A's original certificate and private key:

     a. From the backup copy you made of System A's `<drive>:\Shoreline Data\keystore` directory, replace the private key and certificate files in the same path on Server A:

     `<drive>:\Shoreline Data\keystore\private\hq_ca.key`

     `<drive>:\Shoreline Data\keystore\certs\hq_ca.crt`

     b. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**), stop and restart the **WebFrameworkSvc** service.

     This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.

   - If you plan to leave the changed certificate on System A and you have a Mobility Router in your system, reboot the Mobility Router.

8.6.2 If Config Server Is from DHCP or Static for System A and B

1. On System A, manually set the config server value through phone Settings UI (**Settings** > **Advanced** > **Voice Services** > **Config Server N** parameters). They will not be able to use custom config file and reboot phones to pick up the value.

> **Note**:
>
> When specifying the configuration server, ensure to use the IP address/FQDN of your **System B** Headquarters server.

2. Verify that the phones are in service on System B by checking the **Maintenance** > **Status and Maintenance** > **P Phones**l page in Connect Director.
3. On System A, delete the moved phones as follows:

   a. Launch Connect Director on System A, and in the navigation pane click **Administration** > **Telephones** > **Telephones**. The Telephones page is displayed.
   b. Select the phones you want to delete, and then click **Delete**.
   c. In the **Confirmation** dialog, click **OK**. The system deletes the selected phones.
4. On System A, remove the lines added in Step 1 from your `custom.txt` file.

5. Do one of the following:

   - If you plan to continue using System A and want it to have a certificate different from System B, restore System A's original certificate and private key:

     a. From the backup copy you made of System A's `<drive>:\Shoreline Data\keystore` directory, replace the private key and certificate files in the same path on Server A:

     `<drive>:\Shoreline Data\keystore\private\hq_ca.key`

     `<drive>:\Shoreline Data\keystore\certs\hq_ca.crt`

     b. On System A, using either Windows Task Manager or Connect Director (**Maintenance** > **Status and Maintenance** > **Servers**), stop and restart the **WebFrameworkSvc** service.

     This service detects the certificate change and performs the necessary steps to regenerate and install the appropriate certificates throughout the system. This might take a few minutes.

   - If you plan to leave the changed certificate on System A and you have a Mobility Router in your system, reboot the Mobility Router.

8.7 Viewing Diagnostic Information about a Phone

To access various types of diagnostic information for a phone, do the following:

1. Go to **Settings** .
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.

> **Note**:
>
> If phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

4. Select **Enter**.
5. Select **Diagnostics**.

8.7.1 Viewing Troubleshooting Information about the Phone

1. Go to **Settings** .
2. Select **Advanced**.
3. Enter the password the **Enter Administrator Password** field.

Note:

If phone is in factory state, the password will be **22222** (generic SIP admin password). After the phone is registered to the MiVC system, the password will be set to the one that the admin has defined in the MiVC server setup. The default value is **1234**. However, it may be changed.

4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Troubleshooting**. The troubleshooting information is displayed.

Note:

The fields in the Troubleshooting information page is populated by default.

8.7.2 Using Ping to Check the Status of an IP Address

1. Go to **Settings**
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Ping**. The **Host Name or IP Address** field appears.
7. Enter the IP address in the **Host Name or IP Address** field. It displays the Ping status.

8.7.3 Using Traceroute to Determine the Network Route to a Host

1. Go to **Settings**
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Traceroute**. The **Traceroute Command** field appears.
7. Enter the traceroute command in the **Traceroute Command** field. It displays the Ping status.

8.7.4 Capturing Packets for Phone Network Traffic

To diagnose problems on a phone, you might need to capture packets to see details about network traffic to and from the phone. You can capture packets by using the phone interface, which is described in this section, or you can initiate packet capture and view the results (using Wireshark or a similar network protocol analysis tool) through the Diagnostics Monitoring system. For details, see the *MiVoice Connect System Administration Guide*.

On the 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones, signaling packets are encrypted, Packet capture tools available on the network cannot decrypt these packets. However, using the packet capture tool built into the phone, both the encrypted and decrypted versions of the packets are displayed.

The packet capture can run for up to two hours or until the resulting .pcap file reaches 70 MB.

If you specify a location through the **Diagnostic Server** field, the packet capture files (.pcap) are uploaded to that location. If your installation does not have a `diagnosticServers` path configured, by default the .pcap files from the capture operation are uploaded to the following directory on the Headquarters server:

`<Drive>:\inetpub\ftproot` (or the default FTP location on the server)

Note:

For 6900-Series IP phones, you must manually configure the diagnostic server using **Advanced** > **Diagnostics** > **Diagnostic Server** option.

However, unless this directory allows anonymous write access (which is not recommended), uploading the capture file to this directory will fail.

Uploaded packet capture files are named as follows:

`<Phone MAC address>_YYYYMMDD_HHMMSS.pcap`

Where:

`YYYYMMDD` is the date (four-digit year, two-digit month, and two-digit day) when the `.pcap` file was created on the phone.

`HHMMSS` is the time (two-digit hour, two-digit minute, and two-digit second) when the `.pcap` file was created on the phone.

The results of a packet capture operation are also accessible through the phone interface until you start a new packet capture operation.

1. Go to **Settings**.

2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Capture**. The **Timeout (1 - 1440 Minutes)** field appears.
7. Enter the timeout in the **Timeout (1 - 1440 Minutes)** field.
8. Select **Start** to capture the packets for phone network traffic.

8.7.5 Uploading a Phone's Log

If a phone user experiences problems, you as an administrator or the user might want to upload logs to debug the problem.

If you specify a location manually through the Diagnostics server item on the phone's Diagnostics menu, log files are uploaded to that location. For information about how to specify a diagnostic server from a phone, see Configuring a Diagnostic Server from the Phone Interface on page 199.)

Note:
Uploading Teleworker phone logs to HQ server through FTP or HTTPS does not work. To fix this issue, you must first upload the logs to the local FTP/TFTP server.

Uploaded log files are named as follows:

`<Phone MAC address>_YYYYMMDD_HHMMSS.tgz`

Where:

`YYYYMMDD` is the date (four-digit year, two-digit month, and two-digit day) when the `.tgz` file was created on the phone.

`HHMMSS` is the time (two-digit hour, two-digit minute, and two-digit second) when the `.tgz` file was created on the phone.

Note:

- For log upload from Connect Director using HTTPS, set the upload location for logs to `https://` followed by HQ server IP address or FQDN (for example, https://1.1.1.1) in Connect Director.
- For log upload from the phone using HTTPS, set the `cloud diagnostic server=https://(FQDN/server IP address of HQ server)/hfs/api/v1/upload/phone` in the `startup.cfg` file. For example, `https://1.1.1.1/hfs/api/v1/upload/phone` or `https://abc.xyz.com/hfs/api/v1/upload/phone`.
- The logs will be uploaded to `<drive>:\inetpub\ftproot\uploads\phone` if HTTPS is used for upload.
- The logs will be uploaded to `<drive>:\inetpub\ftproot` if FTP is used for upload.

Follow these steps to upload a phone's log:

1. Go to **Settings** .
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Log upload**.
7. Select **Upload**. The phone will collect all the logs.
8. Select **Upload** again and select **Close**.

8.7.6 Configuring a Diagnostic Server from the Phone Interface

1. Go to **Settings**
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Diagnostic Server**.
7. To use the FTP, enter the IP address of the desired FTP upload server in the following format **ftp://x.x.x.x** in the **Diagnostic Server** field to view the server information.

8.7.7 Viewing Audio Diagnostics Information

1. Go to **Settings** .
2. Select **Advanced**.

3. Enter the password in the **Enter Administrator Password** field.
4. Select **Enter**.
5. Select **Diagnostics**.
6. Select **Audio Diagnostics**.
7. Enter the timeout in the **Timeout (1 - 5 Minutes)** field to capture the RTP information.

8.8 Displaying Settings for an IP Phone

Follow these steps to display the settings for 6900-Series IP (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) phones:

1. Go to **Settings** ⚙.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.

> **Note**:
>
> If phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

4. Select **Enter**. The settings for the phone is displayed

8.9 Clearing a Phone's Configuration

To return a phone to the factory settings, you can clear the phone's configuration through the **Reset** menu. If you move phones from one Mitel system to another, you need to clear each phone's configuration.

1. Go to **Settings** ⚙.
2. Select **Advanced**.
3. Enter the password in the **Enter Administrator Password** field.

> **Note**:
>
> If phone is in factory-default settings, enter **22222** as the password. If the phone is registered with the MiVC system, use the default password **1234** or the password set by the administrator.

4. Select **Enter**.
5. Select **Reset** > **Factory Default** > **Select** to clear a phone's configuration.

Configuring 6970 as a Generic SIP Phone with MiVoice Connect

9

This chapter contains the following sections:

Overview

When set up as a Generic SIP device with MiVoice, the 6970 IP phone supports additional features as listed in the Supported Features on 6970 as Generic / Third-Party SIP Device on page 202 section. This chapter provides details of setting up a 6970 IP phone as a Generic SIP device with MiVoice Connect.It also provides information about converting a 6970 device from MiNet to Generic SIP and configuring and registering the device as a third-party or a Generic SIP device with MiVoice Connect.

Note:

- MiVoice Connect does not support TLS and TCP connections for third-party phones.
- For 6970 IP phones, you must not upgrade the firmware version to SIP 6.0 when MiVoice Connect is 19.2 SP1 or an earlier version.

9.1 Important Considerations

The following are important considerations for configuring and registering a 6970 device:

- Do not disable the web interface for 6970. This is because the web interface must provide logs and audio diagnostics that are useful for handling any issues that might occur during the setting up process.
- All options on the web interface with default values work fine for a third-party device. Therefore, it is recommended not to change any of the default options on the web interface.

9.2 Supported Features on 6970 as Generic / Third-Party SIP Device

As a generic or third-party SIP device, 6970 supports the following features:

- Registrations
- Basic Calls (Incoming and Outgoing)
- Hold/Retrieve
- Mute/UnMute
- Attended Transfer
- Blind Transfer
- Conference (third party only)
- Dial-In Conference
- Call Forward
- Dial by name (Local directory Only)
- Music on Hold
- Localization
- NTP
- Call History (through Programmable key)
- Speed Dial
- Inbound and Outbound trunk (PRI) calls
- Inbound and Outound trunk (SIP) calls
- Voice mail
- Intersite Calls
- Codec Negotiation
- Find Me
- Paging groups
- Feature Access Codes (Star Codes)
- DTMF (In-Band and Out-of-Ban)
- Transport protocol (UDP)
- Calls with CMR
- Meet Me Conference
- Phone Lock

9.3 Converting 6970 from MiNet to Generic SIP and Registering with MiVC

To configure a 6970 device with MiVoice Connect, you can convert the device from MiNet to Generic SIP by using DHCP Option 159 or by using the local TFTP server for the conversion and the registration process.

The following sections describe both these procedures.

Using DHCP Option 159

Note:

This method is recommended for users who have access to modify DHCP option.

To convert a 6970 device from MiNet to Generic SIP by using DHCP Option159 follow these steps:

1. Place the 6970 device SIP build files `6970.st`, `mac.cfg` and `startup.cfg` at the following location of your HQ server:

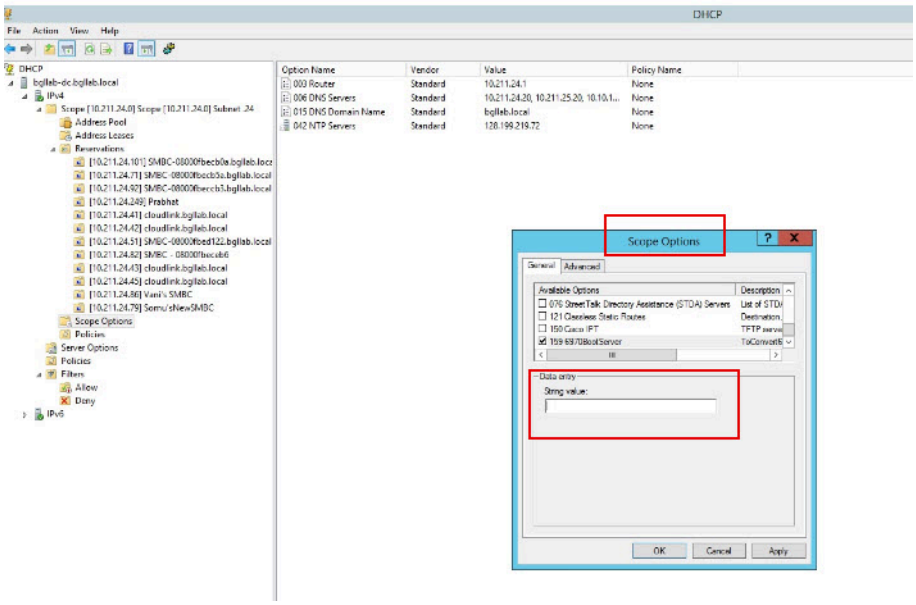
   `C:\inetpub\ftproot\6970files`
2. Log in to your local DHCP server.
3. Go to **Scope Options**, right-click, and select **Configure Options**.
4. In the **Scope Options** window that opens, go to **Option 159** and enable it.

Note:

You must predefine **Option 159** in the **DHCP Scope** options.

5. Go to **Data Entry** > **String Value** and enter **http://<<ip-address>>/fileserver/6970files**.

Figure 11: DHCP Scope Options



6. Click **Apply** > **OK**.
7. Connect the 6970 device to a LAN network.

Note:

After the device connects to the LAN, the following sequence of events occurs:

- The 6970 device fetches its IP address from the DHCP server and gathers information about the HTTP server from the DHCP offer.
- The device contacts the HTTP server and downloads the SIP build.
- The device is updated with the SIP build and boots-up with the Generic SIP build.

9.3.1 Using the Local TFTP Server

Note:

This procedure is recommended if you do not have the privileges to modify the DHCP option.

To convert the 6970 device from MiNet to Generic SIP by using the local TFTP server, follow these steps:

1. Run a TFTP server on your local test machine.
2. Place the 6970-specific Generic SIP build file `6970.st` on the TFTP server.
3. Connect the 6970 device to a PoE-enabled LAN network or switch port.

Note:

- The 6970 device takes two minutes to boots up.
- The device fetches its IP address from the DHCP server.
- While booting up, the device might display **Contacting Server 0.0.0.0** and might remain at 95% completion. This is because it is a new device and no servers are configured.

4. After the 6970 device boots up, select the **Dialpad** icon and select **Settings**.
5. Select **Advanced**.
6. Enter **73738** in the **Enter Administrator Password** field.
7. Press **Enter**.
8. Go to **Network** > **Static Settings**.
9. Enter the TFTP server address in the **TFTP Server** field.
10. Select **Save**.

Note:

- The device contacts the TFTP server and fetches the available SIP build files.
- The device is converted from MiNet to SIP and restarts with the Generic SIP build.

9.4 Configuring MiVoice Connect to Register 6970 Device

This section describes the procedure for configuring 6970 devices as SIP extensions on the MiVoice Connect platform.

9.4.1 Creating a User in Connect Director

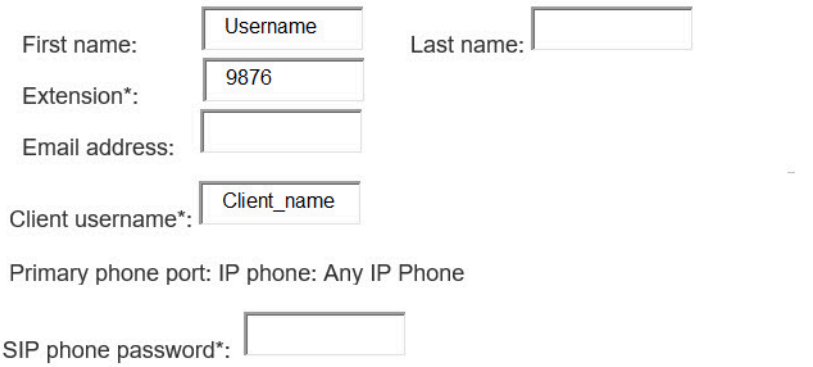
To configure the MiVoice Connect platform to register the 6970 device as SIP extensions, you must create a user in Connect Director. To create a user, complete the following fields in Connect Director:

- **First name**
- **Last name**
- **Extension***

- **Email address**
- **Client username***
- **SIP phone password**

Note:
* indicates mandatory fields for successfully registering 6970 phones on MiVoice Connect platform.

Figure 12: Creating a User in Connect Director

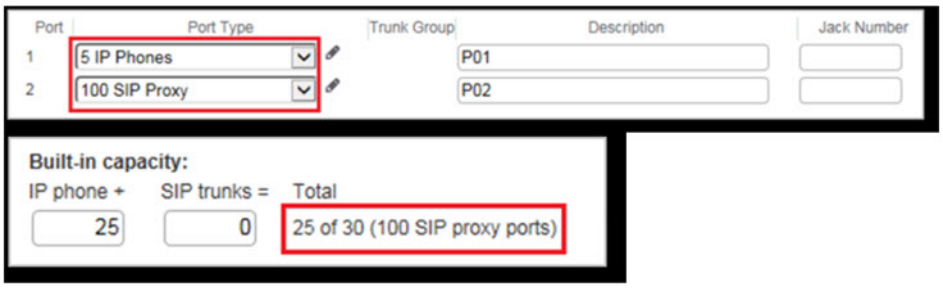


9.4.2 Allocating Ports for the SIP Extensions - SIP Proxy Settings

Following is a description of the switch configuration required on the Mitel system to work with the 6970 Phones. Depending on the switch type, Voice Switches and Virtual Phone Switches support variable numbers of SIP Proxies and IP Phones, which can be verified on the **Switch Edit** page of Mitel Connect Director.

Port Allocation Designated on Switches shows an example of the port allocation designated on switches for IP phones and SIP proxy resources.

Figure 13: Port Allocation Designated on Switches



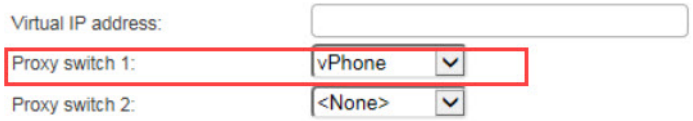
9.4.3 Configuring Site Settings

The Administrator can designate up to two Proxy switches per site for redundancy and reliability. The first switch is assigned as the primary proxy server, and the second switch acts as the backup proxy server, which takes over when the primary proxy server fails.

To configure the Site settings, follow these steps:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page appears.
3. In the list pane, select the name of the site in which SIP proxies will be assigned.
4. In the **General** tab > **Proxy switch 1** field, select the switch configured with SIP proxies for the site.
5. Click **Save**.

Figure 14: Proxy switch 1 Field



9.4.4 Configuring a SIP Profile

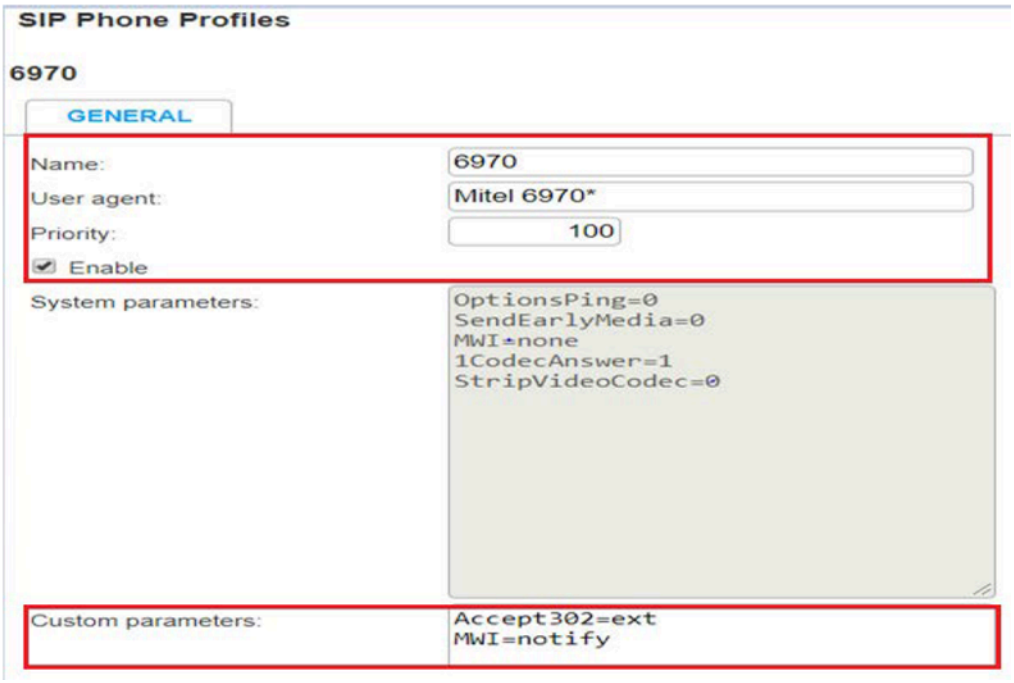
Following are the steps required to configure the SIP profiles for 6970 Phones. By default, 6970 phones use the “System” profile. To optimize the functionality, you must add a custom SIP profile. Follow these steps to configure SIP profiles:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **SIP Profiles**. The **SIP Profiles** page opens.
3. To create a new SIP profile, click **New**.
4. In the **General** tab, enter a name in the **Name** field.

> **Note**:
> It is recommended that you enter a name that describes the SIP endpoint.

5. In the **User agent** field, enter **Mitel 6970***.
6. To enable the SIP profile, select **Enable**.
7. In the **Custom parameters** field, enter **Accept302=ext**.
8. Click **Save**.

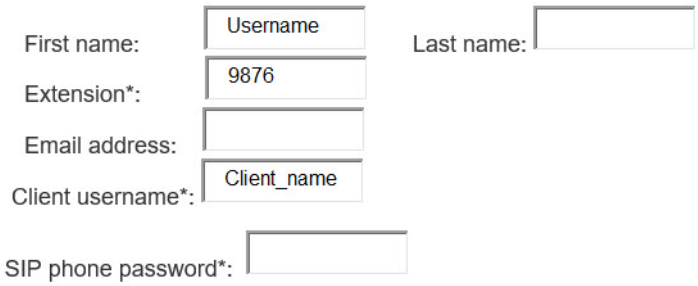
Figure 15: Configure a SIP Profile



9.5 Registering 6970 Device with MiVoice Connect as a Generic SIP Device

To register 6970 with Mivoice Connect, you must create a user in the Connect Director before registration. See the User Details in Connect Director figure for more details.

Figure 16: User Details in Connect Director



Note:

- * indicates mandatory parameters to successfully register the 6970 device with MiVoice Connect.
- You must specify the site proxy switch that performs the site's SIP server functions.

You can register the 6970 phone with MiVoice Connect by using one of the following methods:

- From 6970 Web UI
- From 6970 phone TUI
- Using DHCP option 159
- Using Local TFTP Server

The following sections describe the registration procedures using these methods.

9.5.1 Registering From 6970 Phone Web UI

After you convert 6970 from MiNet to SIP, follow these steps to register the 6970 device with MiVoice Connect as a Generic SIP device from 6970 Web UI:

1. Open the Web interface of the 6970 phone using the IP address of the phone.
2. In the Web interface, complete the following fields:
   - **Username:** admin
   - **Password:** 22222
3. In the 6970 Web interface window, go to **Advanced Setting** > **Global SIP** and complete the fields as indicated in Global SIP Parameter Description:

Table 29: Global SIP Parameter Description

Parameter	Description
Basic SIP Authentication Settings	
Screen Name	You can enter either a user name or an extension number as the value for this field.
Screen Name 2	You can enter either a user name or an extension number as the value for this field.
Phone Number*	Enter the user extension created on Connect Director.
Caller ID	You can enter either a user name or an extension number as the value for this field.
Authentication Name*	Enter the user's extension or client user name. **Note**: It is recommended that you enter the user's extension in this field.
Password*	Enter the SIP phone password provided in Connect Director.
Basic SIP Network Settings	

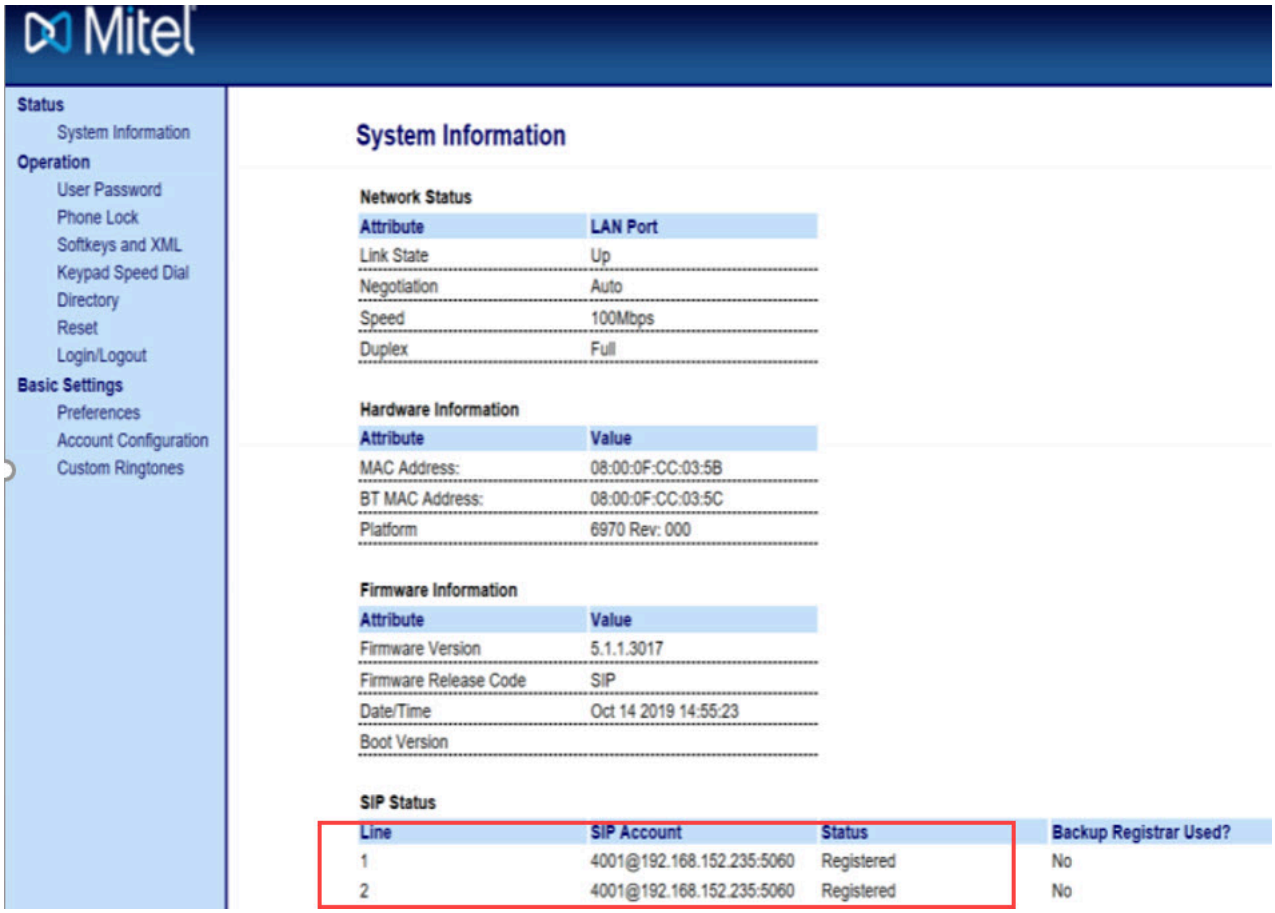
Parameter	Description
Proxy Server	Enter the IP address of a switch that has SIP proxy capacity. **Note**: You can provide the IP address of the switch that has SIP proxy capacity and that switch must be configured as the site proxy.
Registrar Server	Enter the switch IP address provided in the Proxy Server field.

4. Click **Save**.

Note:

- The device registers with MiVoice Connect server using the server IP address and user details.
- The device shows the assigned user name at the top left corner of the display after it enters the **Idle** state and enabling To and From calls for the device.
- The **Status** window on the 6970 Web UI shows that 6970 phone is successfully registered with MiVoice Connect. See Successful Registration of 6970 Device for details.

Figure 17: Successful Registration of 6970 Device



9.5.2 Registering From 6970 Phone TUI

After you convert Generic 6970 device from MiNet to SIP, follow these steps to register the 6970 device with MiVoice Connect as a Generic SIP device from the 6970 phone TUI:

1. On the 6970 device, go to **Settings** > **Advanced Settings**.
2. Enter **22222** in the **Enter Administrator Password** field.
3. On the device interface, press **SIP** > **Call Server** and enter the following details:
   - **Proxy Server:** 10.30.105.81
   - **Registrar Server:** 10.30.105.81

> **Note**:
>
> In these fields, you must enter the IP address of a switch that has SIP proxy capacity.

4. Click **Save**.

5. On the device interface, press **SIP** > **User** and enter the following details:
   - **SIP Auth Name:** 9876 (User extension or client Username created on MiVoice Connect)
   - **SIP Password:** 123456 (SIP Phone password on MiVoice Connect)
   - **SIP User Name:** Username
   - **SIP Display Name:** Display Name
   - **SIP Screen Name:** Screen Name
6. Click **Save**. The device restarts.

Note:

- The device registers with MiVoice Connect server using the server IP address and user details.
- The device shows the assigned user name at the top left corner of the display after it enters the **Idle** state and enabling To and From calls for the device.

9.5.3 Registering 6970 Using DHCP Option 159

To register a 6970 device as a Generic SIP from MiNet by using DHCP Option159, follow these steps:

1. Place the 6970 device SIP build files `6970.st`, `0800Fxxx.cfg` and `startup.cfg` at the following location of your HQ server:

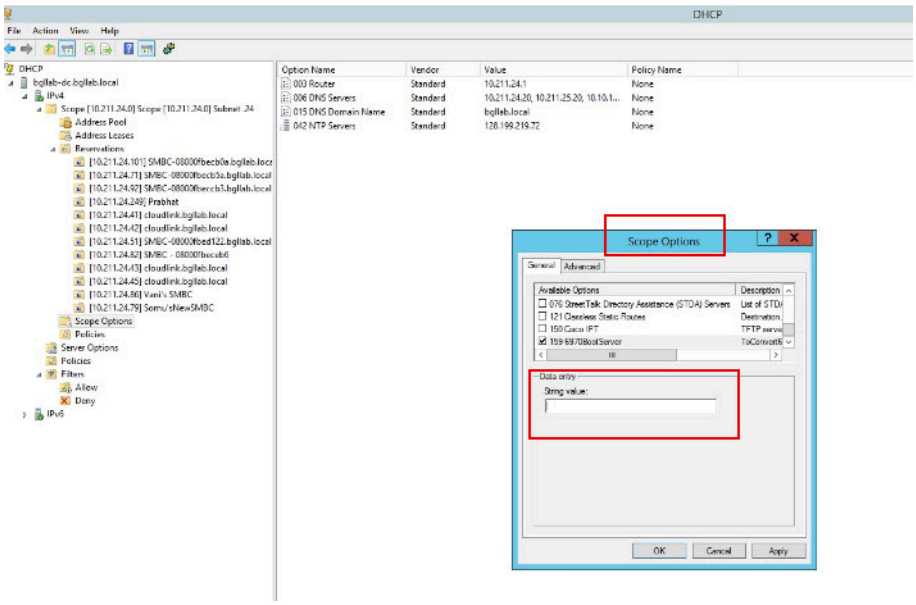
   `C:\inetpub\ftproot\6970files`
2. Log in to your local DHCP server.
3. Go to **Scope Options**, right-click, and select **Configure Options**.
4. In the **Scope Options** window that opens, go to **Option 159** and enable it.

Note:

You must predefine **Option 159** in the **DHCP Scope** options.

5. Configure the HTTP server IP address. Go to **Data Entry** > **String Value** and enter **http://<<ip-address>>/fileserver/6970files**.

Figure 18: DHCP Scope Options



6. Click **Apply** > **OK**.
7. Connect the 6970 device to a LAN network.

Note:

After the device connects to the LAN, the following sequence of events occurs:

- The 6970 device fetches its IP address from the DHCP server and gathers information about the HTTP server from the DHCP offer.
- The 6970 device contacts the HTTP server. Using the `0800Fxxx.cfg` and `startup.cfg` files, the 6970 device is registered with MiVoice Connect and enabling To and From calls for the device.

9.5.3.1 Example of 0800010fxxx.cfg File

Following is a sample `0800010fxxx.cfg` file:

Figure 19: 0800010fxxx.cfg file

```
sip auth name:9876            #User Extension created on MiVoice Connect
sip password: 123456           # sip phone password on MiVoice Connect
sip user name: Username
sip display name: Displayname
sip screen name: Screenname
```

9.5.3.2 Example of startup.cfg File

Following is a sample `startup.cfg` file:

Figure 20: startup.cfg File

```
sip proxy ip: 10.30.105.81                          # switch IP or FQDN
sip registrar ip: 10.30.105.81                      # switch IP or FQDN
log issue: 1
audio diagnostic: 1
```

9.5.4 Registering 6970 Using the Local TFTP Server

To register the 6970 as a Generic SIP from MiNet by using the local TFTP server, follow these steps:

1. Run a TFTP server on your local test machine.
2. Place the `0800Fxxx.cfg` and `startup.cfg` files in TFTP server running on your local test machine.
3. On the 6970 device, go to **Settings** > **Advanced Settings**.
4. Enter **22222** in the **Enter Administrator Password** field.
5. Select **Enter**.
6. Go to **Configuration Server**, select **Download Protocol** as TFTP (if not set already).
7. Enter the TFTP server address in the **TFTP Server** field.
8. Select **Save**. The device restarts and the following sequence of events occurs:
   - The device fetches the `0800Fxxx.cfg` and `startup.cfg` files from the TFTP server.
   - The device registers with MiVoice Connect server using the server IP address and user details fetched from the `0800Fxxx.cfg` and `startup.cfg` files.
   - The device shows the assigned user name at the top left corner of the display after it enters the **Idle** state, enabling To and From calls for the device.

Note:

- The `startup.cfg` file is mandatory because without this file, the device will not request a `0800Fxxx.cfg` file.
- Using this Configuration file, you can add the **Log Issue** and **Audio Diagnostics** soft key on to 6970 phone TUI. This action is not available when you register the 6970 phone through Web UI or Phone TUI.

Other IP Endpoints 10

This chapter contains the following sections:

This chapter provides information about phone IP endpoints other than the 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones, which are described in Configuring 400-Series IP Phones on page 128 and Configuring 6900-Series IP Phones on page 182.

Overview

The Mitel system manages calls and applications for three types of IP endpoints: IP phones, SoftPhones, and conference bridges. IP endpoints are identified by IP address and can exist anywhere on the network. All IP endpoints are supported by voice switches, which must have sufficient capacity for all the IP endpoints in the system. IP endpoints are configured in the system with Connect Director. For more information about IP endpoints, see the *MiVoice Connect Planning and Installation Guide* and the *MiVoice Connect System Administration Guide*

This chapter provides information about 100-, 200-, 500-, and 600-Series IP phones and the BB24 button box. For details about 400-Series and 6900-Series (6910, 6920, 6930, 6940, 6920w, 6930w, and 6940w) IP phones, see Configuring 400-Series IP Phones on page 128 and Configuring 6900-Series IP Phones on page 182.

10.1 IP Phones

IP phones allow you to deploy your telephony system as an end-to-end IP network without dedicated station wiring. Connecting anywhere on the network, IP phones work with the Connect client applications or can be used independently.

The IP phone controls basic display operations, such as volume level, date and time, and icons.

10.1.1 IP Phone Keep Alive

The Voice Switches that manage IP phones send a heartbeat to their associated IP phones once every minute. If the heartbeat is not acknowledged within approximately four seconds, the switch considers the IP phone to be offline or unavailable. The switch continues to broadcast the heartbeat every minute. Any currently offline IP phone that returns an acknowledgment is considered online and available.

10.1.2 IP Phone Failover

IP phones can be optionally configured to send a heartbeat to their Voice Switch every four minutes. If an IP phone cannot communicate with its switch, the phone automatically connects to another switch located at the same site with available configured IP phone resources.

For IP phone failover to be effective, the system must be planned with sufficient excess capacity to handle phones from at least one switch during a failover event. For example, if a switch with 20 IP phone ports fails, 20 IP phone ports need to be available elsewhere in the system.

10.1.3 Services

There are two services running on the HQ and DVS servers that interact with the system's IP phones:

- IP Phone Configuration Service (IPCS)
- Client Application Server (CAS)

10.1.3.1 IPCS

IPCS manages the IP phone configuration process, including configuration files and the database updates. Problems with IPCS connectivity can prevent IP phones from booting and prevent phone configuration data from being updated.

10.1.3.2 Client Application Server (CAS)

Client Application Server handles the remaining functions, such as event handling and feature button functions. It also controls any actions by the IP phone display not controlled by the device's firmware or switches. Problems with CAS or TMS connectivity can result in incorrect phone displays and errors in both the hard and soft key functions.

10.1.4 Embedded IP Phone Display Driver

The embedded IP phone display is provided by the server. Control of IP phone features (such as phone display, redial, and call transfers) are handled on the server. Features that require writing to the database (such as directory and speed dial) rely on the server.

10.1.5 Date and Time

IP phones depend on an SNTP server to maintain the correct time and date. Without an SNTP server, you can set the phone date and time via a GMT offset.

10.1.6 IP Phones and Voice Switches

IP phones in a Mitel system interact with two voice switches: the configuration switch and the call manager switch. The configuration switch helps the IP phone obtain its configuration from the server, which functions as an FTP/HTTPS server for IP phones. You must have at least one configuration switch and must be able to designate a second configuration switch for reliability.

The call manager switch is responsible for hold, transfer, conference, and park actions.

As part of the configuration information, each IP phone is assigned a Voice Switch that acts as the phone's call manager to help the IP phone set up and tear down calls.

10.1.6.1 Configuration Switches

In a DHCP environment, when an IP phone is enabled, it receives the IP address of the configuration switch from DHCP and the server. Each system includes at least one configuration switch for this purpose.

If you have configured the IP phones to start without a DHCP server, you must set the IP address of the configuration switch manually.

The switches, communicating with the HQ server, determine which switch manages calls for a particular IP phone. You have the option of assigning two switches to this function, in case one fails.

10.1.6.2 Call Manager Switch

The call manager module of the Voice Switches handles the Media Gateway Control Protocol (MGCP) information from the IP phones assigned to it. After a call is connected to an endpoint, media streams are independent of the call manager switch.

The Voice Switch communicates call information to other switches in the system using Mitel's enhanced SIP protocol. Every site where IP phones are in use must have a Voice Switch configured to support the number of IP phones at the site.

To configure IP phone support on a Voice Switch, you must reserve ports for IP phone support on the Voice Switch edit page in Connect Director.

10.1.7 IP Phone Communications

IP phone communications are routed through two protocols: MGCP and RTP (Real-time Protocol).

10.1.7.1 MGCP

IP phones (except 400-Series and 6900-Series (6910, 6920, 6930, and 6940) IP phones) communicate with voice switches via MGCP, a device control protocol. The relationship between the switch (call manager) and the phone (gateway) follows a primary-secondary model.

MGCP is used to:

- Deliver information to the IP phone display
- Set up and tear down media streams
- Report phone events such as key presses, on hook, and off hook

10.1.7.2 Real-time Protocol

Media travels through the Mitel system using Real-time Protocol (RTP). After call setup, media flows directly between IP phones through RTP. The Voice Switch is involved only when setting up or tearing down a call.

10.1.8 Boot Process

IP phones are pre configured to work in conjunction with your network's Dynamic Host Configuration Protocol (DHCP) server. After the servers are configured, when the phones deployed, they are automatically added to your Mitel system.

After the IP phone obtains the DHCP and FTP server IP addresses, it downloads the application and configuration files from the FTP server. The IP phone configuration file is modified by Connect Director during IP phone configuration.

If you are not using a DHCP server or if the server is not currently online, you can set a static IP address and other startup parameters directly at the IP phone. Static IP addresses for IP phones can also be assigned using the IP phone setup menus.

10.1.9 IP Phone Firmware Upgrades

The IP phone application software can be upgraded by replacing the application file on the FTP server. When 100-, 200-, 500-, and 600-Series IP phones and the BB24 button box boot up or reboot, they automatically download the available new firmware.

You can also initiate firmware updates by triggering a reboot through the Diagnostics & Monitoring system available through Connect Director.

Note:

Modifying the IP phone configuration files can cause unpredictable behaviour. If you have special needs, contact Mitel Technical Support for instructions.

10.2 Diagnostics

Viewing System IP Phones

IP phone connectivity is displayed in Connect Director in the IP Phone List on the Telephones page (**Administration** > **Telphones** > **Telephones**).

The number of IP phones connected through a switch and the number of IP phones that can be connected to a switch are displayed in Connect Director on the Platform Equipment page (**Administration** > **Appliances/Server** > **Platform Equipment**).

You can also use the Diagnostics & Monitoring system to view status of IP phones. For details, see the *MiVoice Connect System Administration Guide*.

10.2.1 On-Screen Error Messages

Any time a user action results in an error being returned by TAPI, the error is displayed on the IP phone display for six seconds (one North American ring cycle). The error message can be dismissed more quickly by pressing the **OK** soft key.

10.2.2 Diagnostic and Failure Messages

The Diagnostic and Failure Messages table lists and describes the diagnostic and failure messages that may be displayed on IP phones.

Table 30: Diagnostic and Failure Messages

Display Message	Interpretation
File System Failure	An internal, unspecified, problem detected while performing a file system operation.
Boot File Too Big	The boot file is too big and will not fit in RAM.
Boot Save Failed	Writing the boot image to flash memory failed.
Reconfiguring Network	The phone is switching VLANs. **Note**: This might be displayed after DHCP and/or after configuration file processing.
Duplicate IP Address	A duplicate IP address is typically caused by DHCP or a manual entry of the IP address onto multiple devices.
FTP Unreachable	The FTP server is unable to be pinged (for IP110 or IP115).
FTP Server Unreachable	The FTP server is unable to be pinged (for others).
Unresponsive task/Resetting	A task failed to respond to a keep alive request so the phone is restarted.
DSP Error/Repair Required	DSP testing failed on startup. Bad DSP.
NO MGC IP CONFIGURED	An IP address is not set for the MGC.
DSP Asserted/Resetting	The DSP crashed, and a reboot is started.

Display Message	Interpretation
DHCP lease/invalid!	The DHCP lease expired and the phone failed to acquire a new lease.
APP download failed!/filename	Application image download failed.
Invalid App Name	The application name does not follow the required format.
Format Failed	While trying to store a new image in flash, a failure occurred when era sing the flash device.
File System Error	An error was returned by the file system API.
Invalid Signature	The boot or application image file is the wrong type for this phone.
Invalid Image Version	The .bmp image was not of a known acceptable format.
Download CFG file failed/filename	Failed to download the main configuration file specified.
Couldn't Get INCL file/filename	Failed to read the specified Include file from the FTP server.
Using Cached CFG (for IP110 or IP115) Using Cached CFG Files! (for others)	If a complete config file and all includes cannot be downloaded, a cach ed config file is being used.
Enter Factory mode * – No # – Yes	In Response to Mute + RRAMOS.
Factory Test KPD Mode	You are in factory test mode ready to test the keypad (via Mute + R RAMOS).
Boot Application	If only a boot application is in flash and an application image cannot be downloaded, this information is displayed after the boot process is c ompleted.
No/Ethernet	Ethernet is not detected.
100 Mbps/Ethernet	100 Mbps Ethernet speed in use.
10 Mbps/Ethernet	10 Mbps Ethernet speed in use.
Request Service (for IP110 or IP115) Requesting Service (for others)	Being requesting service from MGC.
No Service	MGC service is unavailable.

10.2.3 Troubleshooting the IP Phone Display

This section presents some techniques for troubleshooting the IP Phone Display Server. When you suspect an IPDS (CAS) problem, verify that you can call into voicemail successfully. If you can call voicemail successfully, then you have an IPDS (CAS) issue. If voicemail does not answer or you hear a

message stating the voicemail system is unavailable, you have an issue with the communications to the server.

10.2.3.1 Phone Display Is Incorrect

If a phone display is incorrect, the following may occur:

- IPDS/CAS Sent a Bad Display Update

  This can be detected by searching through the IPDS log file for the display line in question. If it is found at the appropriate time and on the appropriate extension, IPDS/CAS is the cause of the problem. Provide the relevant IPDS log to your engineering resources.
- Switch Did Not Update the IP Phone Correctly

  It is possible for the switch to mishandle phone updates.

10.2.3.2 Enabling IPDT Debugging

By default, `IPDT` logging is turned off. However, you can enable `IPDT` logging to assist in troubleshooting efforts.

Enabling IPDT Debugging

To enable logging on the switch:

1. Telnet into the switch.
2. Enter the `ipdt_debug_level – -1` command.
3. Logging output appears on the screen.

Note:

- Mitel recommends that you enable IPDT logging only for short periods. This feature generates large amounts of data that consumes CPU cycles on the switch and slows it down.
- You can disable the logging feature by replacing -1 with a -0 in the command above.
- The -1 variable enables tracing for all IPDT-related components. You can selectively enable individual IPDT components by using the commands and variables listed in the IPDT Debugging Flags table:

Table 31: IPDT Debugging Flags

Debug flag	Decimal value	Hexadecimal value	Purpose
DEBUG_HOTDIAL	2	0x2	timeouts and logic associated with hot dial / fast transfer feature
DEBUG_NCC_RAW_EVENTS	256 256	0x100	raw device status, call control, and IPDS helper events from switch core
DEBUG_NCC_DEVICE_INVENTORY	512 512	0x200	ncc acquisitions and releases
DEBUG_NCC_FLOW1	4096 4096	0x1000	ncc event handling
DEBUG_NCC_FLOW2	8192 8192	0x2000	verbose ncc event handling
DEBUG_CONFIG_NOTIFICATIONS	65536 65536	0x10000	configuration data and changes
DEBUG_NCC_DISPLAY_BASIC	16777216	0x01000000	logic associated with determining which screen is shown
DEBUG_NCC_DISPLAY_DETAILED	33554432	0x02000000	the actual display commands sent to the phones

The functions listed in the IPDT Functions table can be executed from a terminal session. String arguments must be passed in quotes. Integer arguments may be passed in decimal form, or in hex form by prefixing with 0x.

Table 32: IPDT Functions

Function	Argument name	Argument Type	Purpose
`ipdt_dumpExtensions`	none	none	lists all phones and extensions configured on switch, along with CCOID, and phone type where appropriate.
`ipdt_dumpExtDisplay`	extension number	string	shows current value of all display elements: announcement area, soft keys, custom key labels, custom key icons/leds, message waiting indicator, location and format of date and time, location of borders.
`ipdt_dumpCCODisplay`	CCOID	integer	same as above, using CCOID as key. Use `ipdt_dumpExtensions` to find CCOIDs of non-extension devices such as anonymous phones.
`ipdt_dumpExtCalls`	extension number	string	lists all calls on the given extension. Works for “foreign extensions” too (that is, extensions whose call info is supplied by IPDS)
`ipdt_dumpCCOCalls`	CCOID	integer	same as above, using CCOID as key; native extensions only.
`ipdt_dumpExtCfg`	extension number	string	lists configuration and extension status for extension. For foreign extensions, lists those details supplied by IPDS.

Function	Argument name	Argument Type	Purpose
`ipdt_dumpCCOCfg`	CCOID	integer	same as above, using CCOID as key; native extensions only.
`ipdt_dumpActiveTime`	none	none	lists currently active timed objects in IPDT
`ipdt_resetExtDisplay`	extension number	string	redraws the entire display of the phone, by the given extension.
`ipdt_resetCCODisplay`	CCOID	integer	redraws the entire display of the phone, by the given CCOID.
`ipdt_adminMsgExt`	extension number	string	displays an administrative message in announcement area of given phone for `ipdt_admin_timeout` seconds. "" or “all” indicates all phones on switch.
`ipdt_adminMsgCCO`	CCOID	integer	displays an administrative message in announcement area of given phone for `ipdt_admin_timeout` seconds. 0 indicates all phones on switch

10.2.4 Manual Phone Configuration

Phones must be manually configured if you are not using a DHCP server to provide IP address and configuration parameters.

You can enter the phone configuration menu at bootup or enter a key sequence from the phone’s keypad.

10.2.4.1 Manually Configure the IP Phones at Bootup

1. Connect the Ethernet cable into the data jack on the back of the IP phone.

2. At the Password prompt, enter the default password **1234** or the password provided by your system administrator, followed by the **#** key.

> **Note**:
>
> You have four seconds to enter the password, after which the phone enters normal operation with its current settings.

The default Password can be changed in Connect Director. For more information, see the *MiVoice Connect System Administration Guide*.

3. Enter the values listed in Boot up Configuration Prompts when prompted. Press **#** to advance to the next settings or ***** to exit.

Table 33: Boot up Configuration Prompts

Prompt	Value
Clear all values?	Press **#**. (No.)
DHCP – ON	Press * and **#**.
IP –	Enter the IP address for the phone. Press **#**.
Subnet –	Enter the Subnet mask. Press **#**.
Gateway –	Enter the gateway IP address. Press **#**.
FTP –	Enter the IP address of your server. Press **#**.
MGC –	Press **#**. **Note**: The phone obtains the address from configuration files on the server.

Prompt	Value
SNTP –	Enter the IP address of your time server. Press **#**.
802.1Q Tagging – OFF	Press **#**. **Note**: Consult your network administrator before changing this value.
VLAN ID –	Press **#**.
Save all changes	Press **#**. (**Yes**.)

The phone downloads the latest bootROM and firmware from the server and in the process, reboots several times. When the phone displays the date and time, the boot and upgrade process is complete.

Manually Configuring a Phone from the Keypad

1. With the phone on hook, press the **MUTE** key followed by **73887#** (**SETUP#**).
2. At the Password prompt, enter the default password **1234** or the password provided by your system administrator, followed by the **#** key.

Note:

The default IP Phone Password can be changed in Connect Director. For more information, see the *MiVoice Connect System Administration Guide*.

3. Enter the values when prompted. Press **#** to advance to the next settings or ***** to exit.

The phone downloads the latest bootROM and firmware from the server and in the process, reboots several times. When the phone displays the date and time, the boot and upgrade process is complete.

10.2.5 Displaying IP Phone Settings

You can display the phone's current IP parameters setting by entering a key sequence from the phone's keypad.

1. With the phone on hook, press the **MUTE** key followed by **4636#** (**INFO#**). The phone displays the first two parameters.
2. Press * to advance the display or**#** to exit.

The phone resumes normal operation after the last parameter is displayed.

10.2.6 Resetting the IP Phone

1. With the phone on hook, press the **MUTE** key followed by **73738# (RESET#)**

The phone reboots.

10.3 Configuration for IP Phones

Boot Configuration Operation

Upon booting, IP phones use the FTP server address to acquire their configuration specifications. The FTP server address is determined from DHCP site-specific options (default option 156). If DHCP is disabled, the FTP server address can be manually entered on the phone, and the information is stored in the flash memory of the phone. Alternatively, if DHCP is used (but no site-specific option is returned), the FTP server returned by option 66 is used.

If the FTP server cannot be reached, or if a configuration file cannot be located, the phone uses the last successfully-loaded configuration parameters. After a phone is finished reading configuration files, the current parameters are saved into flash memory.

10.3.1 IP Phone Configuration

When an IP phone boots, it contacts the configured FTP server and reads an initial configuration file from FTP root. This file corresponds to its coded model name. Each of these initial configuration files, references a custom configuration file that can be manually edited by a system administrator. As phone software is upgraded, the contents of configuration files are overwritten at the time of update by `Kadotautil`, but custom configuration files are preserved across upgrades.

Configuration parameters are prioritized by the phone in the order that they are processed. Custom configuration files are the last file read. Any parameters in a custom configuration file override previous configuration parameters. This applies to local parameters also, as they are processed first, before any configuration files are read.

Parameters and values are case sensitive. A parameter and its value are separated by one or more spaces or tabs. Each parameter must begin on a new line of the text file.

The Phone Models table lists the phone configuration file names.

Table 34: Phone Models

IP Phone Name	Name on Top of Phone	Model Name on Barcode Label Underside of Phone	Base Configuration Name	Custom File Name
IP 110	110	S0	shore_s0.txt	s0custom.txt
IP 115	115	S01	shore_s01.txt	s01custom.txt
IP 212k	212k	S12	shore_s12.txt	s12custom.txt
IP 230	230	SEV	shore_sev.txt	sevcustom.txt
IP 230g	230g	SEG	shore_sevg.txt	sevgcustom.txt
IP 265	265	S36	shore_s36.txt	s36custom.txt
IP 530	530	S2	shore_s2.txt	s2custom.txt
IP 560	560	S6	shore_s6.txt	s6custom.txt
IP 560g	560g	S6G	shore_s6g.txt	s6gcustom.txt
IP 565g	565g	S6C	shore_s6c.txt	s6ccustom.txt
IP 655	655	SWE	shore_swe.txt	swecustom.txt
BB24	24	SBB	shore_sbb.txt	sbbcustom.txt

While booting, IP phones look in FTP root for the unique configuration file, `shore_<MACaddress>.txt` (the MAC address of the phone).

Note:

MAC configuration files must be named in lower case. While Windows is usually not case-sensitive, the `LIST` command within the Windows FTP server is case-sensitive.

If `shore_<MACaddress>.txt`is found, it is used to provide configuration files and configuration parameters for the phone. If `shore_<MACaddress>.txt`is not found, the phone uses the`<coded-model-name>.txt` file for configuration.

The format of a configuration file is:

Parameter1	Value
Parameter2	Value

where the parameter and value are separated by one or more spaces or tabs, and each parameter is on a new line of the text file (CR/LF is the nominal new line indicator).

Comments may be embedded in a configuration file by starting the line for- the comment with a **#** symbol.

The maximum permitted size of any configuration file is 5000 bytes.

Additional configuration files may be included in the file by using the Include parameter where its value is the name of the file (and optionally a path) to include. All Include parameters should be located in the original file downloaded from the FTP server. Includes must be located at the end of the main configuration file. The maximum number of included files is 5.

The most commonly customized configuration parameters are audio levels, described in Configuring Audio Levels. All other customizable phone configuration parameters are described in Other Customizable Parameters.

10.3.1.1 Configuring Audio Levels

Four sets of audio levels can be custom configured for each phone:

- handset
- headset
- ringer
- speaker

Default Audio Levels for IP Phones (except IP655, IP400-Series, and 6900-Series) lists the default audio levels for all IP phones except the IP655 and the IP400-Series phones. Default audio levels for the IP655 are provided in the table below. Information about audio parameters for the IP400-Series phones is provided in Configuring 400-Series IP Phones on page 128.

For more information about the parameters, see Parameter Definitions.

Table 35: Default Audio Levels for IP Phones (except IP655, IP400-Series, and 6900-Series)

Parameter	Handset Levels	Headset Levels	Bluetooth Headset Levels (for IP565g)	Ringer Levels	Speaker Levels
TxGain	5157	6144	6143	—	8192
RxGain1	183	183	182	130	258
RxGain2	258	258	258	258	410
RxGain3	365	365	364	410	649
RxGain4	516	516	515	649	1029
RxGain5	728	728	727	1029	1631
RxGain6	1029	1029	1028	1630	2584
RxGain7	1631	1631	1631	2584	4096
RxGain8	2303	2303	2303	4096	6492
RxGain9	3254	3254	3253	6491	10289
RxGain10	4596	4596	4595	10288	16305
SideTone	517	649	0	—	—
Handset DTMF Attenuation	13	13	13	—	17

Parameter	Handset Levels	Headset Levels	Bluetooth Headset Levels (for IP565g)	Ringer Levels	Speaker Levels
Call Progress Tone Attenuation	13	13	13	—	17

Note:

If the value of the RxGain1 parameter for the ringer level is set to **0**, the audio is turned off. (The phone does not ring.)

Default Audio Levels for IP655 Phones lists the default audio levels for IP655 phones:

Table 36: Default Audio Levels for IP655 Phones

Parameter	Handset Levels	Headset Levels	Ringer Levels	Speaker Levels
TxGain	0	3	—	-2
RxGain1	-27	-27	-30	-24
RxGain2	-24	-24	-24	-20
RxGain3	-21	-21	-20	-16
RxGain4	-18	-18	-16	-12
RxGain5	-15	-15	-12	-8
RxGain6	-12	-12	-8	-4
RxGain7	-8	-8	-4	0

Parameter	Handset Levels	Headset Levels	Ringer Levels	Speaker Levels
RxGain8	-5	-5	0	4
RxGain9	-2	-2	4	8
RxGain10	1	1	8	12
SideTone	-14	-10	—	—
Handset DTMF Attenuation	-19	-13	—	-17
Call Progress Tone Attenuatio	-25	-7	—	-11

10.3.1.2 Parameter Definitions

- The **TxGain** (transmit gain) parameter sets the level of the audio transmitted from the phone onto the network.
- The **RxGain** (receive gain) values correspond to each of the 10 volume setting levels shown when the volume on the phone is adjusted. Sometimes, the RxGains are not high enough and need to be customized for an individual system.
- **SideTone** is the audio picked up from the microphone and transmitted to the speaker (speakerphone, handset or headset speaker) that provides feedback to the user that the phone is working. SideTone gain is very subjective, and is sometimes lowered and sometimes raised.
- **DTMF** (dual-tone multi-frequency) **Attenuation** sets the receive DTMF level that the phone user hears.
- **Call Progress Tone Attenuation** sets the level for the various tones played after a call is placed and before audio is connected.
- The **Plantronics CS50** wireless headset provides its own side tone, plus “+” inserts 20 ms delay between the headset and the phone, which causes some people to say they hear echo when using the Plantronics headset; in this case, headset side tone may need to be reduced. When you speak, Plantronics reduces the gain on the speaker by -24dB; but when you stop speaking, the gain is turned up, and you can hear the last little bit echoed in your ear.

For example, inserting the following line in s2custom.txt or s6custom.txt and rebooting the phone increases the headset volume settings 11 dB at the highest setting, which may be required in noisy environments:

Headset levels: 6144,183,258,409,649,1028,1630,2899,6491,10288,14333,917,13,13

Inserting the following line reduces the headset side tone by 6 dB, which some CS50 users prefer:

Headset levels: 6144,183,258,365,516,728,1029,1631,2303,3254,4596,643,13,13

Minimum gain values are 0 and maximum are 32536. Setting values very high may saturate the speaker and create poor sound quality.

You can change gains on an individual phone by changing the configuration files and then rebooting the phone. Eventually, all phones on the system obtain these values when they reboot.

10.3.1.3 Displaying Gain Levels

The `prtaudCfgValues` command can be used from a telnet session to display the RxGain (receive gain) levels for a device.

10.3.1.4 Other Customizable Parameters

In addition to changing the audio parameters, the custom configuration text files allow you to customize other parameters, such as phone brightness or day of week abbreviations used in time displays.

Note:

The tables in this section contain detailed information that can be used to modify the behavior and functionality of your Mitel system. Make sure that you understand what you are doing before attempting to use this information to modify your system. Mitel is not responsible for any damage or expenses incurred through misuse of this information. If you have questions, contact Mitel Technical Support before attempting to modify your system.

The phones support the parameters described in Source File Abbreviations.

In specifying parameters, the following rules apply:

- IP addresses from the keypad must be provided in dotted-decimal format.
- Cases are preserved in character strings unless otherwise indicated.
- Parameter checking is performed on all parameters to look for illegal values, and illegal values are ignored.
- White space within a parameter is ignored.

The file names used for AppName, BootName, and FontPixmap, IconPixmap, WallpaperPixmap and in include parameters may also include a path to the file. Upper and lower case characters are ignored except when specified in the path or file name for these parameters to preserve operation with case-sensitive FTP servers.

For the purpose of comparing the file in flash and the value on the server, only the file name and date are used.

The abbreviations listed in Source File Abbreviations are used to identify the source of each parameter in the “Source” column in the table.

Table 37: Source File Abbreviations

Source	Abbreviation in Table
DHCP ACK	DHCP
DHCP Site Specific Option	SSON
Configuration File	CFG
Manual Entry Using SETUP	MAN
MGCP Message	MGCP

DHCP Site Specific Options

Parameters may be set from within a DHCP ACK message in the site specific option field (default is 156, but it may be modified with the SiteOption parameter). These parameters may be specified in the site-specific option field:

- FtpServers
- Country
- Language
- Layer2Tagging
- VlanId

Enclose each parameter in quotes, and separate multiple parameters with a comma. For example:

FtpServers – ”192.168.0.13, 192.168.0.23”, Country – 1, Language – 1, SetupPassword – ”12345abcde12345abcde12345abcde12”

Table 38: Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
AppName	Up to 32 alphanumeric characters	This is the name of the application image that is in the telephone. The application file name can be at most 24 characters long. The combination of filename and path can be up to 32 characters long. A new application name is specified in a configuration file and is checked against the NV value to decide if a new version needs to be downloaded. The NV value is updated after a successful download and flash programming sequence.	CFG	Value from factory in NV Storage
BackLight	Up to 4 ASCII characters	Number of minutes the backlight remains on at full brightness when the phone is idle. Format: Backlight NN, where NN is a number 0-60. 0 – n/a. 1-60 – number of minutes after which display is shut off	CFG	5

Parameter	Value Type	Value	Source	Default
BackLightDim	Up to 4 ASCII characters	**Note**: Only applicable to the S6C and S36. Number of additional minutes the backlight remains on at a DIM level after the BackLight interval passed since an idle state was entered. A value of 0 causes the backlight to remain at the dim level indefinitely.	CFG	120
BootName	Up to 32 alphanumeric characters	The name of the boot image is in the telephone. The boot file name can be 24 characters long. The combination of filename and path can be up to 32 characters long. A new boot name is specified in a configuration file and is checked against the NV value to decide if a new version needs to be downloaded. The NV value is updated after a successful download and flash programming sequence.	CFG	Value from factory in NV Storage
Country	Up to 3 ASCII Characters	This parameter specifies the Country that is used by the Include parameter to identify a particular file to include. May be between 1 and 255.	SSON, CFG, MAN	1
DHCP	1 ASCII Characters	DHCP enable/disable 0 – Disabled 1 – Enabled	MAN	1

Parameter	Value Type	Value	Source	Default
DscpAudio	Up to 2 ASCII characters	Differentiated services code point for audio packets. Allowed values of 0 to 63.	CDG	0
DscpSignaling	Up to 2 ASCII characters	Differentiated services code point for audio packets. Allowed values of 0 to 63.	CFG	0
DtmfLevels	Up to 3 ASCII Characters	This specifies the DTMF level in dB of in-band tones sent from the phone to the network. The allowed values are -1 to -20. These are attenuation levels in dB, so -1 is louder than -20.	CFG	-10
Ethernet1	Up to 10 ASCII Character	Status of the 1st Ethernet Interface. Ethernet2 Status, Speed/Duplex Where: Status is 0 or 1 (disabled or enabled) Speed/Duplex is one of the following: Auto 10/FD 10/HD 100/FD 100/HD 1000/HD 1000/FD	CFG, MAN	1,Auto

Parameter	Value Type	Value	Source	Default
Ethernet2	Up to 10 ASCII Character	Status of the 2nd Ethernet Interface. Ethernet2 Status, Speed/Duplex Where: Status is 0 or 1 (disabled or enabled) Speed/Duplex is one of the following: Auto 10/FD 10/HD 100/FD 100/HD 1000/HD 1000/FD	CFG, MAN	1,Auto
FontPixmap	Up to 32 ASCII Character	Name of the .bmp format file that contains the font pixmap. Format is windows .bmp 16 color except on the S6c where it is 256 colors.	CFG	"fontpixmap.bmp"
Font2Pixmap	Up to 32 ASCII Character	Name of the .bmp format file that contains the large font pixmap used by the U/dlt2 signal. Format is windows .bmp 16 color except on the S6c where it is 256 colors.	CFG	"font2pixmap.bmp"
FtpServers	Up to 255 ASCII Characters	A comma-separated list of up to 2 FTP servers. If a server is unavailable the phone goes through the list until a working server is found.	DHCP, MAN	0.0.0.0

Parameter	Value Type	Value	Source	Default
GatewayAddress	Dotted Decimal ASCII	Gateway address for the telephone.	DHCP, MAN	0.0.0.0
GreyLevels	Up to 3 ASCII Characters	Grey level setting for the middle grey levels on the IP530 and IP560 only. Low middle grey level may have the values: 0 – 1/4 1 – 1/3 2 – 1/2 High middle grey level may have the values: 0 – 1/2 1 – 2/3 2 – 3/4 Example: 1,2	CFG	1,1
IcmpArpTimeout	Up to 5 ASCII Characters	Number of seconds before routing table entries that are created by ICMP redirects are timed out of the routing table. If 0, then they never time out.	CFG	0
IconPixmap	Up to 32 ASCII characters	Name of the .bmp format file that contains the icon pixmap. Format is windows .bmp 16 color.	CFG	"iconpixmap.bmp"

Parameter	Value Type	Value	Source	Default
Include	Up to 64 ASCII Characters	The file name that is specified is read and its contents included into the master configuration file. Files may be specified completely, or may include the variables $Hardware, $Country or $Language. The value of the Hardware Version (programmed into flash at the factory e.g. K01M01P01L01), Country or Language Parameter is substituted for $Hardware, $Country or $Language when the file name is created. For example: Include Country_$Country.txt with the Country parameter set to 3 loads in the file Country_3.txt This permits parameters to be specified based on the Country and Language parameter values.	CFG	""
IPAddress	Dotted Decimal ASCII	IP address to be used by the telephone.	DHCP, MAN	0.0.0.0
KeepAlive	Up to 3 ASCII Characters	Number of seconds to wait for an audit endpoint command before initiating the IP phone failover. **Note**: If set to zero, recovery procedures are never started. The valid range is 0 to 999 seconds.	CFG	120

Parameter	Value Type	Value	Source	Default
Language	Up to 3 ASCII Characters	This parameter specifies the Language that is used by the Include parameter to identify a particular file to include. The valid range is 1 to 255.	SSON, CFG, MAN	1
Layer2Audio	1 ASCII character	Layer 2 audio priority values from 0 to 7.	CFG	5
Layer2Tagging	1 ASCII character	802.1Q tagging enable on Port 1 0 – Disable 1 – Enable	SSON, CFG, MAN	0
Layer2Signaling	1 ASCII character	Layer 2 signaling priority values from 0 to 7.	CFG	0
MaxJitter	Up to 4 ASCII characters	The maximum value that the jitter buffer may be allowed to grow. Valid values are 10 to 300 mS in 1 mS steps.	CFG	50
MgcAuthenticate	Up to 1 ASCII Character	If enabled, then only authenticated MGC messages are accepted by the phone. 0 – disable 1 – enable	CFG	0
MgcServers	Up to 64 ASCII Characters	Comma separated list of up to 2 MGC Servers. Must be in dotted decimal format. Example: 192.168.0.1, 192.168.0.2	SSON, CFG, MAN	0.0.0.0

Parameter	Value Type	Value	Source	Default
MonthsOfYear	Up to 64 ASCII Characters	Comma separated list of the months of the year abbreviations used by the phone to display the time. The first month is January.	CFG	Jan,Feb,Mar,Apr, May,Jun,Jul,Aug, Sep,Oct,Nov,Dec
NoSvc	Up to 64ASCII Characters	String displayed when phone service is lost. Characters in this string must be specified using UTF-8.	CFG	"No Service"
PersistantEvents	Up to 255 ASCII Characters	Comma separated list of persistent events. Example: L/hu,L/hd, U/kd,U/ku	CFG	""
ReqSvc	Up to 64 ASCII Characters	String that is displayed as the phone is waiting for service from the switch. Characters in this string must be specified using UTF-8.	CFG	"Requesting Service"
RingDefine	Up to 64 ASCII Characters	See the MiVoice Connect System Administration Guide for a definition of permissible values.	CFG	""
RingMap	Up to 64 ASCII Characters	See the MiVoice Connect System Administration Guide for a definition of permissible values.	CFG	""

Parameter	Value Type	Value	Source	Default
RtpBase	Up to 5 ASCII characters	This is the base port from which the phone transmits and receives media. The valid range is an even number from 3000 to 65408.65408 is the highest even 16-bit number that allows enough headroom for the 64 RTP and 64 RTCP ports that are reserved when you establish an RTP base value. Given an RTP base, the phone should use the next 64 consecutive even numbers for RTP ports. If within that range an existing (reserved) odd or even UDP port number is used, the phone should skip over an even/odd pair to the next even number. For example, if the user set rtpBase to 5550, then 5550, 5552, 5556, 5558, etc., is usedIn this example, 5554 is skipped because 5555 is a reserved port used by the phonectl server (actually, 5554 is also used and also provides a reason for skipping over 5554). If an odd number is specified, the phone should use the next lowest even number if it fits the above limitations.	CFG	3000

Parameter	Value Type	Value	Source	Default
SetupPassword	32 ASCII Characters	This is the MD5 hash of the password that must be entered after the mute button is pushed to enter a manual key command. **Note**: This password must be saved in flash after a value is received from the MGC so it can be enforced on subsequent reboots. It is not cleared by the CLEAR command nor the clear step in the SETUP command.	MGCP	1234
SiteOption	Up to 3 ASCII Characters	Site-specific option number used by DHCP between 128 and 254.	CFG	156
SntpServer	Dotted Decimal ASCII	SNTP server address in dotted decimal format.	DHCP, CFG, MAN	0.0.0.0

Parameter	Value Type	Value	Source	Default
SpeakerLevels	Up to 255 ASCII Characters	Set the audio levels of the speakerphone using a comma-separated list of values for the following settings: TxGain RxGain1 RxGain2 RxGain3 RxGain4 RxGain5 RxGain6 RxGain7 RxGain8 RxGain9 RxGain10 Speaker DTMF Attenuation Call Progress Tone Attenuation	CFG	Defaults vary by phone model. For details, see Default Audio Levels for IP Phones (except IP655, IP400-Series, and 6900-Series) and Default Audio Levels for IP655 Phones
SubNetMask	Dotted Decimal ASCII	Network Mask for the telephone. On boot, the phone checks for a non-zero NV value, and if one is present it is used.	DHCP, MAN	0.0.0.0

Parameter	Value Type	Value	Source	Default
SysLogInfo	Up to 32 ASCII Characters	IP Address, module, verbose level, facility code, and output device of the SysLog function. The port number may be optionally identified and appended to the IP address. **Note**: The default of 514 is used if no port is specified. The module is a 32-bit integer where each bit refers to the debug enable/disable status from a specific software module. Bit assignments are defined in Configuring Syslog Functionality for the IP Phones on page 252. The verbose level indicates the level of information that is printed. Levels are 0 to 7. Facility code is the syslog facility code. The output devices are 0 – serial port, 1 – syslog server. Example: 192.168.0.3:514, 279,33,1	CFG	0.0.0.0,0,0,0,0
ToneDefine	Up to 64 ASCII Characters	See the MiVoice Connect System Administration Guide for a definition of permissible values.	CFG	""

Parameter	Value Type	Value	Source	Default
ToneMap	Up to 64 ASCII Characters	See the MiVoice Connect System Administration Guide for a definition of permissible values.	CFG	""
TouchBeep	0 or 1	If enabled, the phone plays a beep when the touch screen is touched for user feedback.	CFG	0
Version	Up to 16 ASCII Characters	This parameter specifies the version identifier of the configuration file. It is then reported via the Mgc/gi signal request.	CFG	""
VlanId	Up to 9 ASCII Characters	VLAN ID to be used on tagged packets from the phone. Example: 1234	SSON, CFG, MAN	0
WallpaperPixmap	Up to 32 ASCII Characters	Name of the .bmp format file that contains the wallpaper pixmap. Format is windows .bmp 16 color.	CFG	"wallpaperpixmap.bmp"
WallPaper2Pixmap	Up to 32 ASCII Characters	Name of the .bmp format file that contains the user pixmap.	CFG	"wallpaper2pixmap.bmp"
WaveRinger1	Up to 64 ASCII Characters	Used to assign one wave file to any of the ring signals. The first value is the signal, and the second value is the location of the file on the FTP server. Example: L/rg 192.168.0.20/audio/dave.wav	CFG	""

Parameter	Value Type	Value	Source	Default
WaveRinger2	Up to 64 ASCII Characters	Used to assign one wave file to any of the ring signals. The first value is the signal, and the second value is the location of the file on the FTP server. Example: L/rg 192.168.0.20/audio/ dave.wav	CFG	""

10.3.2 Local Keypad Procedures

If DHCP is turned off and manual settings are being used, the set should display the text Password – ? and Speaker – # – OK * – . for at least 1 second. The string assigned to SetupPassword (by the MGC server or the default) must be provided to access the SETUP command. All other commands are accessible without a password.

While the Password? prompt is displayed during the boot sequence the user might enter the **muteINFO# (mute4636#)** sequence to enter the local INFO command. When the INFO command is exited, the phone again displays the Password prompt and continues boot operations.

The SetupPassword is sent by the MGC in hashed MD5 format. The telephone compares the MD5 hash of the password the user entered with this value to determine if the correct password is entered.

On the IP phones, “Line 1” and “Line 2” refer to the top and bottom lines of the display. On newer models that support the programmable buttons feature, adapt the display of these positions to suit the capabilities of the LCD in use. The IP110 and 115 models are slightly different from the other models in that they have one line for displaying information. Thus, the “Line 1” information is scrolled across the LCD display and is followed by the more detailed “Line 2” information. (See Local Command Interface for clarification.)

The IP212k model includes a narrow LCD display. Thus, the “Line 1” and “Line 2” information cannot fit on one line (as is possible with the other phones). Instead, the text must be wrapped around to appear on as many as 4 lines, for long strings.

If at any time during normal operation these sequences are entered, the operational display state is maintained while these commands are displayed, and the display is returned to the current state after the commands are finished (unless they require a restart). While the phone is in any of these local key procedures, it returns an error code “501” indicating it is not ready, in response to any MGCP command received. Because there is not a mute key on the IP110 phone, use the transfer key instead of the mute key in the following access sequences.

Table 39: Local Command Interface

Access Sequence	Mnemonic	Procedure Description
Mute 25327#	CLEAR	A shortcut for enabling DHCPdoes not do anything else and is not password protected (only SETUP is). This command is present in the event someone hijacks the phone using the SETUP command. CLEAR allows it to be brought under DHCP control without knowing the password.
Mute 4636#	INFO	Display the following information sequentially on the top and bottom lines of the display. All data is retrieved from the currently active configuration. Use ***to exit and **#**to go to the next item. The phone returns to normal operation after the last screen. • IP address static/dynamic • Subnet mask • Gateway • Link speed • FTP server • MGC server • SNTP server • Tagging on/off • Application file • Boot file • Config file date • App version • Boot version • Country • Language • Model number • MAC address • Serial number • Hardware version
Mute 7464#	PING	The phone prompts for an IP address and then pings that IP address 5 times and report the result after 10 seconds.
Mute 73738#	RESET	After displaying a warning, resets the phone. On the top line **Reset Phone?** and on the bottom line ***=No #=Yes**.

Access Sequence	Mnemonic	Procedure Description
Mute 73887#	SETUP	After the mute sequence is provided, if `SetupPassword` is not null, then prompt for the proper password ending in **#**. Do not display password digits as they are entered but use *****. If a match, then prompt to **Clear All Values?**. If no, then prompt for DHCP On/Off. If DHCP is on skip over the prompts for IP Address, Subnet Mask, and gateway. Then prompt for FTP Server, MGC Server, SNTP Server, Tagging On/Off, VLAN ID, Ethernet1, Ethernet 2, Country, and Language. Save to NV storage if values are modified. If **Clear all Values?** is answered with yes, in addition to returning settings to the **<Not Set>** state, any cached DHCP values including the IP address are cleared. If a value was never configured using SETUP, it is displayed **<Not Set>** when its prompt is displayed. Otherwise, the value stored in flash is displayed. The only exception is the DHCP value, which defaults and clears to the **ON** state. Setup value may be returned to the <Not Set> state by: • Answering yes to the “Clear All Values?” query • Executing the factory CLEAR command (executable only from the serial port) • All values are <Not Set> when the phone is new. Perform this error checking on IP address entries during setup: • Only 0-9, * and # are accepted. • Leading zeroes are ignored • Values outside 0-255 are ignored. If 2 digits are input, a third digit that makes the value >255 is ignored. So, upon entering 654, the 4 is ignored. • Multiple “.” inputs are ignored. • If no entry is provided before “.” is entered, a 0 is automatically inserted.

10.3.2.1 Parameter Precedence

The IP phones use the following order of precedence sources for all parameters:

1. Config file
2. DHCP (if active)
3. `Setup` Command
4. Defaults

In other words, configuration parameters have precedence over DHCP over Setup over Defaults.

Not all parameter sources may be supported for every parameter. Phone Configuration Parameters indicates which sources are allowed for each parameter.

To fully manually configure a phone simply turn off DHCP, then use the Setup command but be sure not to specify an FTP server that might download a configuration file and overwrite your manual settings.

10.4 PhoneCTL Command Line Tool

PhoneCTL is a command-line tool used to configure and diagnose IP phones. PhoneCTL commands can be run from the Windows command prompt.

Syntax for PhoneCTL commands can be obtained by typing `ping` at the prompt and pressing **Enter**.

10.4.1 Commands

The supported commands are the following:

- `authentic8`
- `telnetOn`
- `telnetOff`

Note:

All commands are case-insensitive.

After the `phonectl` command, the user is prompted to enter a password.

After the user enters the correct password, the device permits access to executables that configure or diagnose the respective device.

CLI passwords are configurable only through Connect Director. The default password is **ShoreTel**.

10.5 Configuring Syslog Functionality for the IP Phones

Several commands are used to set up syslog functionality. These must be run before any logging messages can be received.

10.5.1 SetLogLevel

The `setLogLevel` command (see setLogLevel Command) sets the logging severity level.

A log level remains in effect until a new `setLogLevel` command is issued.

Table 40: setLogLevel Command

Syntax	Example	Parameters
`Prompt:\phonectl -setLogLevel [moduleID] [level] [destIP]`	`Prompt:\phonectl -setLogLevel 3 7 192.168.0.170`	moduleIDis the ID number of the specific IP phone software modules the logging level is being set for. It is a 32-bit integer. Values must be 0-655335. Each bit in the integer enables or disables a specific module. Any module bit that is not set is not logged. Hexadecimal values for phone software modules include: 0x1 Call Processing (MGCC) 0x2 Config File Processing (MCFGP) 0x4 User Storage (MUSTG) 0x8 Network Configuration (MNETC) 0x10 User Interface (MELUI) 0x20 Display Driver (MDIS) 0x40 Provisioning (MPROV) 0x80 Task Maintenance (MAINT) The number used in the parameter is the decimal equivalent of the sum of the hex values for all modules that are to be logged. For example, to turn on only the user interface module, enter 16 in the [moduleID] parameter (which is the decimal value of 0x10). To turn on call processing and config file process, enter 3 in the [moduleID] parameter (which is 0x1 + 0x2 in decimal). This is the value shown in the example command shown above. To turn on all modules, enter 255 (which is 0x1 + -x2 + 0x4 + 0x8 + 0x10 + 0x20 + 0x40 = 0x80).

10.5.2 SetServerIP

The `setServerIP` command (see setServerIP Command) sets the server's IP address and points to the location where messages are to be logged.

Table 41: setServerIP Command

Syntax	Example	Parameters
`Prompt:\phonectl -setServerIP [newServerIP] [destIP]`	`Prompt:\phonectl -setServerIP 192.168.0.3 192.168.0.170`	newServerIP is the address of the computer running the syslog server application. destIP is the IP address of the destination IP phone to which the command is sent.

10.5.3 SetOutputDev

The `setOutputDev` command (see setOutputDev Commands) sets the output device to which the syslog messages are sent. The device may be either a serial port or the syslog server.

Table 42: setOutputDev Commands

Syntax	Example	Parameters
`Prompt:\phonectl -setOutputDev [devID] [destIP]`	`Prompt:\phonectl -setOutputDev 0 192.168.0.170`	devID is set to zero if the device is a serial port or one for the syslog server. destIP is the IP address of the destination IP phone to which the command is sent.

10.6 Retrieving Information about the IP Phone

Dump2pc

The `dump2pc` command (see dump2pc Command) is used to retrieve the syslog messages from the IP phone's buffer. The results are printed to the command line.

Table 43: dump2pc Command

Syntax	Example	Parameters
`Prompt:\phonectl -dump2pc [destIP]`	`Prompt:\phonectl -dump2pc 192.168.0.170`	destIP is the IP address of the destination IP phone to which the command is sent.

10.6.1 ShowLogLevel

The `showLogLevel` command (see showLogLevel Command) prints the log level of each module for which logging is active. Information is printed to the command line.

Table 44: showLogLevel Command

Syntax	Example	Parameters
`Prompt:\phonectl -showLogLevel [moduleNum] [destIP]`	`Prompt:\phonectl -showLogLevel 4 192.168.0.170`	destIP is the IP address of the destination IP phone the command is sent to. You retrieve the log level settings for this phone.

10.6.2 ShowConnInfo

The `showConnInfo` command (see showConnInfo Command) shows information about connections created by MGCP_create messages.

Table 45: showConnInfo Command

Syntax	Example	Parameters
`Prompt:\phonectl -showConnInfo [destIP]`	`Prompt:\phonectl -showConnInfo 192.168.0.170`	destIP is the IP address of the destination IP phone to which the command is sent.

10.6.3 ShowStats

The `showStats` command (see showStats Command) shows information about connections created by MGCP_create messages.

Table 46: showStats Command

Syntax	Example	Parameter
`Prompt:\phonectl -showStats [cxid] [destIP]`	`Prompt:\phonectl -showStats 5 192.168.0.170`	cxid is the ID number of a specific connection. The value can be discovered by reading the value returned by the showConnInfo command. destIP is the IP address of the destination IP phone to which the command is sent.

10.6.4 ShowTime

The `showTime` command (see showTime Command) prints the time of day on the command line for the destination IP phone.

Table 47: showTime Command

Syntax	Example	Parameters
`Prompt:\phonectl -showTime [destIP]`	`Prompt:\phonectl -showTime 192.168.0.170`	destIP is the IP address of the destination IP phone to which the command is sent.

10.6.5 Version

The `version` command (see Version Command) prints the version of the PhoneCTL software.

Table 48: Version Command

Syntax	Example
`Prompt:\phonectl -version`	`Prompt:\phonectl -version`

10.7 Softphone

The Softphone can be launched through Connect client. Softphone does not support NAT or firewall transversal. Problems with the Headquarters server or network connectivity can prevent the softphone from being loaded.

From a configuration and management standpoint, the softphone appears to be an IP phone with some limitations. User have access to the DTMF keys (0-9, #, *), on hook, off hook, and flash.

The softphone user interface does not have a display, so it does not interact with IPDS. Just like an IP phone, the softphone uses MGCP for call setup and teardown, and RTP for media.

IP phones are uniquely identified by their MAC address. In most cases the softphone is identified by the NIC of the user PC. If a softphone is installed on a PC without a NIC, the softphone generates a fake MAC address that is still unique.

The softphone page contains an ActiveX control that implements the VoIP media support. Because it requires an ActiveX control, the softphone only works on PCs with Internet Explorer and Microsoft Windows. The ActiveX object attempts to reach the switch call manager configured in Connect Director. If the switch call manager is successfully contacted, the softphone buttons are enabled.

When the switch call manager is contacted, Connect Director detects that a new IP phone is being registered. Depending on licensing and IP phone port availability, a new port is automatically created in the configuration database. The softphone then appears in the Individual IP Phones list in Connect Director.

In some situations, Connect client waits for several seconds for a corresponding IP phone port to appear in the configuration database. If this times out, a warning message is displayed in the softphone status bar.

When Connect client is closed, the operation is reversed to return the user to his or her home port.

10.8 Dial Tone Behavior

The following section discusses the dial tone behavior for various call operations.

10.8.1 Transfer

When a user is on a call and hits the transfer button, the phone remains off-hook and plays a dial tone. When the user completes the blind or consultative transfer while on the speakerphone or headset, the phone automatically goes on-hook. Only if a user is on the handset does the phone stay off-hook and play a dial tone. A user using hands-free mode with speaker or headset goes on-hook without a dial tone.

10.8.2 Park

When a user is on a call and hits the park button, the phone remains off-hook and plays a dial tone. When a user parks a call while on the speakerphone or headset, the phone automatically goes on-hook. The phone plays dial tone only if the user is on the handset. When using hands-free mode with the speaker or headset, the phone goes on-hook without a dial tone.

10.8.3 Hold (Multi-line IP Phones)

When a user on a multi-line IP phone places a call on hold while on the speakerphone or headset, the phone goes on-hook. If the user is on the handset, the phone plays a dial tone. A user using hands-free mode with speaker or headset goes on-hook without a dial tone.

- To retrieve the call, go off-hook by lifting the handset, pushing the speaker button, pushing the headset button, or pushing the call appearance
- To answer a second incoming call, press the second call appearance.
- To retrieve a second held call, press the second call appearance.

10.8.4 Hold (Single-line IP Phones: IP110/IP115)

When a user on a single-line IP phone places a call on hold while on the speakerphone or handset, the phone remains off-hook and plays a dial tone. A user using hands-free mode with speaker or headset goes on-hook without a dial tone.To retrieve a call, the user can go off-hook by lifting the handset and pushing the speaker button.

10.8.5 New Voice Mail Indicators

Your voice mailbox contains unplayed messages if:

- There is an interrupted dial tone for two seconds after a new line is opened.
- The phone's Message Waiting Indicator (MWI) light flashes.

10.9 Connect Client

Connect Client Logs

The Connect client creates a log file each time the user logs in. The logs are used to help the Mitel Technical Support with debugging problems that may arise during the client operation. Users can send the log files to the Mitel Technical Support while opening a troubleshooting ticket.

To send the client logs:

1. Press **Ctrl+F12**.
2. In the **Log Level** tab, select the following:
   - Type of logs to be captured in the log report (Information or Debug)
   - Specify the number of log files. The default value is **20** and you can set the maximum number up to 1000 files.

Note:

Upon reaching the maximum limit, the newly generated log file replaces the oldest file in the logs folder.

- Specify the size limit for each log file. The default value is **20** megabytes and you can set the maximum size up to 1000 megabytes

3. In the Logs tab, do one of the following:

- Click **Send Client Logs** to send the logs through email to the Mitel Technical Support.
- Click **Open Log Folder** to open the log folder on your system. You can select the required log file and send through email to the Mitel Technical Support.
- The log files are stored in the *Connect-<date>.<time>.log* format.

Service Appliances 11

This chapter contains the following sections:

This chapter contains information about Service Appliances.

Overview

The Service Appliance is a sealed appliance, optimized for resiliency and security, capable of running Mitel services. The Service Appliance can host Audio Conferencing, Web Conferencing and Instant Messaging services.

Service appliances are deployed in the same manner as other voice switches and managed similarly to the voicemail-enabled switches. Director windows configure conference settings and provide status for the Service Appliance. Network setting are configured using a serial cable or the Service Appliance's switch command line interface (`stcli`). The management of the services running on the Service Appliance switch is done via the Service Manager command line interface (`svccli`). The `stcli` and `svccli` are accessible via a serial cable or remotely via SSH.

This chapter describes the processes and procedures necessary to back up and restore your Service Appliance, locate key log files, produce logs, and various switch commands and utilities useful for monitoring and troubleshooting the Service Appliance.

11.1 Using the Service Appliance

Service Appliance Maintenance

A few key tasks are required to maintain the Service Appliance (see Service Appliance Maintenance Tasks).

Table 49: Service Appliance Maintenance Tasks

Task	Description
Backup	Performs regular automatic backups of your Service Appliance to protect conference data, generated recordings, and uploaded user content

Task	Description
Restore	Restore your Service Appliance based on a saved backup of both the Service Appliance and the HQ database. Coordinates the restore of the Service Appliance with the restore of the HQ database.
Disk Management	Watches disk utilization to avoid running out of disk space.

11.1.1 Service Appliance Backup

The Service Appliance uses the same backup and restore methods as the voicemail-enabled switches. Backup scheduling and configuration is performed in Connect Director. The manual backup and restore commands are executed on the Service Appliance using the Service Manager command line interface (`svccli`).

Back up your system to protect the conference data, generated recordings, and user files uploaded to the Service Appliance. This feature is NOT meant as a method of archiving or as a method for retrieving accidentally deleted files.

Note:

Install the Service Appliance on the same network as the FTP backup server to avoid bandwidth issues. The Service Appliance can generate more than 1GB of data per day and have more than 100GB stored internally.

There are two methods for backing up the Service Appliance:

- Automatic scheduled backup
- Manual backup.

11.1.1.1 Automatic Backup

Automatic backups are performed after the system administrator configures the backup parameters in Connect Director.

FTP Server Parameter lists and describes the parameters.

Table 50: FTP Server Parameter

Field	Description
Enable Daily Backup	Turn on/off automatic backupsr
IP Address	The IP address of the FTP Server.
FTP Port	The FTP port used to access the FTP server. **Note**: The FTP port must be set to 21. The Service Appliance can only perform backup and restore against a FTP server running on port 21.
Directory	The directory on the FTP server where the backup files are stored. **Note**: If you are backing up multiple Service Appliances, use a separate directory for each Service Appliance.
User ID	The User ID for accessing the FTP server.
Password	The Password for accessing the FTPserver.

11.1.2 Manual Backup

To perform a manual backup, you must have configured the FTP parameters in Connect Director per the automatic backup set.

1. Access the Service Appliance using either the serial Port or via SSH.
2. Start the Service Manager command line interface (`svccli`).
3. Run the `backupweb` command.

Accessing the Service Appliance Using the DB9 Serial Port

1. Connect a serial cable from a desktop/laptop PC to the DB9 serial connector on the rear of the Service Appliance.

> **Note**:
>
> Establishing the serial console connection requires a DB9 socket to DB9 socket cable connector, instead of a DB9 plug connector to DB9 socket connector cable with the voice switches. A Null-Modem connection (crossover cable) is required, instead of the straight-through cable (extension cable) used on voice switches.

2. Open a terminal emulation program such as Hyper-terminal or Putty and set it for a serial connection using the following parameters:
   - Serial Port: COM X (where 'X' is the port number used on your PC)
   - Speed: 19200 baud
   - Data Bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow control: None
3. After establishing a serial connection, login to the Service Appliance environment using **Admin** as the User ID and **ShoreTel** as the Password.

11.1.2.1 Accessing the Service Appliance Using a SSH Connection

Open an SSH client and connect to your Service Appliance using SSH.

> **Note**:
>
> Telnet to the Service Appliance is not supported.

You can create a SSH connection on the command line by issuing the following command:

```
SSH -l admin <ip address or domain name of the Service Appliance>
```

11.1.2.2 Manually Backing Up the Service Appliance

1. At the `Linux` prompt ($ for admin access; # for root access), run the `svccli` command to start the services cli.
2. Start the backup using the `backupweb` command.
3. When the `backupweb` command returns you to the `svccli` prompt ('>'), exit the `svccli`.
4. Verify that the backup is complete by checking the `/cf/shorelinedata/Logs/FtpSync-<date>.<time>` log file where:
   - <date> is the current date
   - <time> is the time when the log file was created

11.1.3 Restoring the Service Appliance Backup

You may restore a previous backup of the Service Appliance by executing the `restoreweb` command using the svccli. See Automatic Backup for more information about the location of the backup files.

11.1.3.1 Restoring Best Practices

Restore the Service Appliance with a restoration of the HQ database from the same day.

Note:

Since the file pointers are stored in the database in HQ application server, users MUST back up/ restore BOTH the HQ database and Service Appliance(s) altogether to ensure consistency between HQ database and Service Appliance file system.

Note:

Restoring a Service Appliance backup without restoring HQ database taken from the same time as the Service Appliance backup may cause the following issues:

- Ghost files - These are the files that exist during the time when the Service Appliance backup was made, but have since been removed.
- Wrong metadata files - Service Appliance restore overwrites existing files on the Service Appliance even if the existing files might be more up to date than the ones in backup.

To ensure the file system on the Service Appliance is consistent with HQ database:

- Enable daily backup for Service Appliance in Director

- Schedule a windows task to back up the HQ database at the same time as the daily backup
- Restore HQ database from a backup that was created at the same time as the Service Appliance backup that is going to be restored
- Restore Service Appliance from a backup created at the same time as the HQ database backup

11.1.4 Manual Restore

A manual restore is the only method for restoring the Service Appliance. The system administrator accesses the Service Appliance (through the serial port or via SSH) and executes the `restoreweb` command from the Service Manager command line interface (svccli).

11.1.4.1 Manually Restoring the Service Appliance

1. At the `Linux` prompt ($ for admin access; # for root access), run the `svccli` command to start the services cli.
2. Start the backup using the `restoreweb` command.

   The restore is complete when the `restoreweb` command returns you to the `svccli` prompt ('>').
3. Verify that the backup is complete by checking the `/cf/shorelinedata/Logs/FtpSync-<date>.<time>.Log File` where:

   - <date> is the current date
   - <time> is the time when the log file was created

11.1.5 Disk Management

The system administrator must monitor the disk space usage on the Service Appliance to ensure that users can continue uploading presentation data for web meetings. The system administrator can monitor disk usage via the system administrator's Conferencing User Interface.

Note:

The system administrator cannot delete media uploaded to the Service Appliance without deleting the user. Users must delete their own uploaded media files. If the system administrator deletes the user, all of the media files and recordings uploaded by the user are deleted.

11.1.5.1 Disk Usage from the Command Line

Disk Usage from the Command Line lists and describes disk usage from the command line.

Table 51: Disk Usage From The Command Line

Name	Description
df -h	`Linux` free disk command. This command displays statistics about the amount of free disk space on all mounted files systems (that is, disks) on the Service Appliance
du -bc --excludes – '.*'*|grep -i total	`Linux` disc usage command. This command returns the total apparent size (in bytes) for all the files and sub-directories of the current directory
getstatus all	`svccli` command that shows high CPU usage processes, memory usage and disk usage

11.2 Log Files and Processes

The Service Appliance provides log files for various processes running on the appliance. Most logs are located in the `/cf/shorelinedata/Logs directory`.

11.2.1 Service Appliance Logging Process

Collaboration Manager/Collaboration Attendant (CMCA)

The CMCA provides session control for new and existing conferences. Monitoring conference extensions via TMS and manages participant and Reservation-less or Scheduled conference calls arriving at the Conference Extension. It uses the media module for playing prompts, playing files, playing tones, recording media sessions.

11.2.1.1 STTS (SoftSwitch)

The STTS process hosts local Conference Extensions (CEs). To create conference calls between users and CMCA, join and end conference calls, and provide call signaling during the conference session.

11.2.1.2 Media Module

The media module provides media resources (prompts and user audio mixing) for audio conference sessions. The CMCA uses the media module to setup media resources during conference calls.

11.2.1.3 Telephony Management Server (TMS)

The TMS provides call control for conference sessions. It also manages Participant Lists and provides the Call Detailed Record (CDR) interface for the CMCA.

11.2.1.4 Web Bridge

The Web Bridge provides Internet conference viewing screen and data sharing, and provides a server side interfaces for user conference and Service Appliance web conference administration.

11.2.1.5 Other Services

The list of services running on the Service Appliance can be viewed using the `svccli` interface.

11.2.2 Service Appliance Processes and Protocols

Service Appliance Protocols shows the processes and protocols are used by the Service Appliance:

Table 52: Service Appliance Protocols

Name	Description
TAPI TAPI	Telephony API - provides call control information between CMCA and TMS. STCTSP is the client side of the TAPI connection. STSTSP is the server side of the TAPI connection.
Media Control	Messages between CMCA and Media to provide media resources to conference participants
Call Control	Messages between Media and STTS to provide media resources to conference participants
CDS	Call Data Service - provides CDR records to the HQ database
NCC	Network Call Control provides call setup/teardown between TMS and network switches
SIP	Session Initiation Protocol - setup and teardown phone calls between switches. It is also used for 3rd party SIP phones

Name	Description
MCGP	Media Gateway Control Protocol - setup and teardown phone calls between IP phones and voice switches

11.3 Log Files

Service Appliance Log Files lists and describes the key log files in the Service Appliance:

Table 53: Service Appliance Log Files

Name	Description
WC2Access and WC2Error logs	Access and error log files for web bridge
apache_access and apache_error logs	Apache access and error logs when accessing the web bridge
STMEDIA log	New media log file for audio mixing. Media are the audio prompts played to audio bridge users.
STTS log	SoftSwitch Logs
CMCA log	Access and error log files for the Service Appliance CMCA process
STCTSP and STSTSP logs	TAPI client and server logs for communication between CMCA and TMS
TmsCDS, TmsMain, and TmsNCC logs	Telephony Management Server logs

11.4 Service Appliance Utilities

- UBOOT on page 270
- Stcli on page 270

- Cli on page 271
- Regedit on page 271

11.4.1 Accessing Utilities from SSH

Mitel provides access to several voicemail utilities through a Linux BASH command line. Voicemail-enabled switches define two accounts: Admin and Root.

- **Admin:** The Admin account provides access to selected Mitel and Linux utilities, including all voicemail-enabled switch command line interfaces.

> **Note**:
>
> Mitel recommends that user log into the Admin account when accessing Linux utilities.

  Unlike the voicemail-enabled switches, logging into the Admin account does not open the `stcli` interface. Logging into the Root account immediately opens a Linux BASH `shell`. The administrator must run the `stcli` command to use the `stcli`.
- **Root:** The root account provides access to all Mitel and Linux utilities. Restrict access to this account to help prevent potential switch problems.

  Logging into the Root account immediately opens a Linux BASH `shell`.

  Access to the Linux BASH command line through an SSH client.

11.4.1.1 Appliance Utilities

The Service Appliance uses the same switch architecture as the voicemail-enabled switches. The switch utilities are nearly identical to the voicemail-enabled switches. As such, only general descriptions are provided in the following sections.

See Overview on page 91 for detailed descriptions and processes. Relevant differences between the voicemail-enabled switches and the Service Appliance are described in the following sections.

11.4.1.2 UBOOT

UBOOT is the boot loader for the Service Appliance. The UBOOT;environment is accessed from a terminal emulator through the serial port when the switch is booted.

See UBOOT Commands and Flags;for a detailed description of the UBOOT boot loader.

11.4.1.3 Stcli

Shell (`stcli`) displays and modifies system configuration parameters. You can implement static or dynamic IP addressing for the switch from `stcli`. You can also reboot the switch from `stcli`.

See stcli Commands for a description of the `stcli` commands.

Option 7 is unique to the Service Appliance; it restores the Service Appliance back to factory defaults. See Restore Factory Default for details.

The administrator can execute this command only by using the root account for the SSH session.

11.4.1.4 Cli

The `cli` interface accesses diagnostic tools, manipulates debug setting levels, and displays system information. `cli` can be run from any remote SSH session or from Windows prompts originating from the local host, the controlling Distributed server, or the Main server.

11.4.1.5 Regedit

`Regedit`, a utility that modifies registry-type data structures in the switch, is accessible through the root account. voicemail-enabled switches have a registry similar to Windows Servers. To edit the Registry, log in as root and run the `RegEdit` command line tool from the bash shell. `RegEdit` might be used to set logging levels on applications and set other parameters that change their behavior.

Note:

The Registry is a construct, not part of Linux.

11.5 Diagnostics and Repair

The Service Appliance uses the same switch architecture as the voicemail-enabled switches. See Booting and Restarting Voicemail-Enabled Switches for a detailed description of the booting and restarting process. The Service Appliance does not use compact flash. As such, compact flash commands and boot methods do not apply to the Service Appliance. Also, the Service Appliance does not capture audio output from a switch port.

11.5.1 Restore Factory Default

If the Service Appliance becomes non-operational due to corruption of the OS or application, it may be possible to restore the appliance to an operational state.

Procedural steps to follow depend upon whether a backup exists for the appliance to be restored, whether HTTPS is being used and whether the Service Appliance is in a single appliance installation or one of multiple Service Appliances in a distributed system.

Depending on configuration, various recovery steps may be required:

- Turn off/on HTTPS and uploading of SSL certificates. See the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* for details.
- Configuring a Service Appliance with original IP address settings. See the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* for details.
- Installing a Service Appliance in Director. See the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* for details.
- Restoring a backup to an Service Appliance. See Restoring the Service Appliance Backup.
- Perform Restore to Factory Default. See Restoring Service Appliance to Factory Default.

11.5.1.1 Restoring Service Appliance to Factory Default

1. Using the serial port, login to the Service Appliance as **root**.
2. Enter **stcli** to open STCLI menu.
3. Select **7 -- Restore factory default**.
4. The Service Appliance reboots and start up login prompt.

Note:

Following the restoration to factory default condition, the Service Appliance requires configuration with IP addressing before any backups can be restored into the appliance. See the *MiVoice Connect Conferencing and Instant Messaging Planning and Installation Guide* for detailed instructions.

Points to Consider for CentOS to Rocky Linux Migration

12

The following points must be noted with regards to device migration from CentOS to Rocky Linux:

- Beginning with MiVoice Connect Release 20.0, the following Linux-based devices running on CentOS 7.x must be migrated manually to run on Rocky Linux 9.2.
  - LDVS
  - Virtual Switch
  - Virtual UCB
  - Edge Gateway
- The CentOS-based devices are not automatically migrated to Rocky Linux-based devices; instead, you must create new Rocky Linux-based devices.
- For information about backing up for CentOS to Rocky Linux migration, see the **Backing Up for CentOS to Rocky Linux Migration** section in the MiVoice Connect System Administration Guide.
- Run the following command to configure the switch to use SHA1 for certificate authentication.

  ```
  update-crypto-policies --set DEFAULT:SHA1
  ```

Appendix A - Event Codes 13

This chapter contains the following sections:

This appendix includes information about Event codes.

13.1 Overview

This appendix provides a comprehensive list of event codes. Organized by error type and sorted by event ID numbers, the tables in this appendix are a helpful resource for troubleshooting events reported by the Mitel system.

Connect Director provides the following methods for viewing events:

- Clicking **Maintenance** > **HQ Event Log** > **System** or **Application** allows you to see all events the system or application generates. For more information, see the *Maintenance* section in the *MiVoice Connect System Administration Guide*.
- Clicking **Maintenance** > **Diagnostics and Monitoring** > **Alerts** allows you to view the events associated with a particular alert. For more information, see the *Monitoring and Diagnosing* section in the *MiVoice Connect System Administration Guide*.

13.2 Event Types

The tables in this appendix lists the event types according to the following categories associated with components in the Mitel system:

- Switch
- TMS
- Voice Mail Port Manager
- Media Driver
- Event Watch
- System Management Interface
- Port mapper
- Trigger Server
- Distributed Routing Service (DRS)
- Kadota Utility
- Call Accounting
- Workgroup Server
- CSIS
- IP Phone Configuration Service (IPCS)
- ABC
- Edge Gateway
- Offline Migration
- IP Phone Display Server (IPDS) (also known as CAS)

13.3 Using the Event Code Tables

The event tables in this appendix provide a structured view of events you may encounter in messages and log files. Each event table entry includes a unique event ID number, a severity level, the event message text, possible causes, and suggested courses of action (if any).

In some cases, event codes result from other error conditions that cause related problems. For this reason, always review event codes in the context in which they appear. For example, if event code 171 (internal operating temperature of switch is exceeding acceptable range) appears with code 166 (internal fan failure), you should replace the fan—not the entire switch—to solve the problem.

Each event is assigned one of three levels of severity. Severity Level Descriptions lists and describes the severity levels used in the tables:

Table 54: Severity Level Descriptions

Severity Level	Explanation
Information	Reports status Indicates normal operation, or a transition between normal operating states. Typically, no action is required.
Error	Reports an exception to normal operations Depending on the event and its context with other events, it requires no action, monitoring, troubleshooting, or referral.
Warning	Alerts you to a failure or an impending failure (for example, when a service or hardware component is disabled) In most cases, a warning requires immediate response and resolution.

13.4 Switches

Event Codes: Switches lists and describes event codes for switches.

Table 55: Event Codes: Switches

ID	Severity Level	Message	Cause	Action
100	Error	Switch < Voice Switch Host Name>: Event message lost, queue overflow.	The Voice Switch is receiving too many events from the NT Server. Possibly caused by an application problem on the server.	Check the server for events that might indicate an application problem. Troubleshoot the problem and reboot the server, if you cannot identify a cause.

ID	Severity Level	Message	Cause	Action
101	Warning	Switch < Voice Switch Host Name>: The <area> in flash memory is corrupt and is being reset.	Flash memory area is corrupt.	If problem persists, return for repair.
102	Error	Switch < Voice Switch Host Name>: Unable to reset <area> in flash memory, erase failure.	Application is unable to erase area of Flash memory.	If problem persists, return for repair.
103	Error	Switch < Voice Switch Host Name>: Unable to update <area> in flash memory, write failure.	Application is unable to write area of flash memory.	If problem persists, return for repair.
105	Error	Switch < Voice Switch Host Name>: Task exception occurred. System needs to be restarted.	A software exception occurred.	Contact Mitel Technical Support and be prepared to provide the log files for further analysis.
106	Error	Switch < Voice Switch Host Name>: Task exception occurred. System automatically restarting.	A task exception occurred. The Voice Switch experienced an internal error and is rebooting.	Contact Mitel Technical Support and be prepared to provide the `ipbx` and`tmsncc` log files for further analysis.
107	Information	Switch < Voice Switch Host Name>: Restart request received —system is being shutdown and restarted.	;Voice Switch restarted via the Maintenance > Appliances > Servers page in Connect Director.	No action.

ID	Severity Level	Message	Cause	Action
108	Error	Switch < Voice Switch Host Name>: Internal error:	No longer reported in NT event log.	This event code reports internal software debug statements for use by developers.
109	Error	Switch < Voice Switch Host Name>: Unable to seize trunk on port <port number>. Taking trunk temporarily out of service.	The switch cannot seize a trunk.	Verify that the trunk line is connected to the Voice Switch. Check wiring between Voice Switch and the telephone company De-marc. Connect a phone or telephone test set to the line, then go off-hook and listen for a dial tone. If no dial tone is present, report the problem to your service provider.
110	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> taken out of service by the administrator.	The system administrator took the port out of service.	No action.
111	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> is back in service.	The trunk line is again functional and is back in service.	No action.
112	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> put back in service by the administrator.	Trunk is back in service.	No action.

ID	Severity Level	Message	Cause	Action
113	Warning	Switch < Voice Switch Host Name>: Extension on port <port number> taken out of service by the administrator.	Specified extension port removed from service.	Put the port back in service when the system administrator indicates that it is appropriate.
114	Information	Switch < Voice Switch Host Name>: Extension on port <port number> put back in service by the administrator.	Specified extension port is back in service.	No action.
115	Information	Switch < Voice Switch Host Name>: System restarted. Product: Firmware Version: < Voice Switch firmware version number> BootROM Version: < Voice Switch bootrom version number> Telephone Board: < Voice Switch telephone board revision number> CPU Board: < Voice Switch CPU revision number>	The switch was reset and subsequently restarted. (The event also provides current version information for the switch.)	No action.

ID	Severity Level	Message	Cause	Action
116	Error	< Voice Switch Host Name> Lost connection to switch < Voice Switch Host Name>.	The switch is unable to communicate with the other Voice Switch specified in the event. The switches are not able to place calls to each other.	The specified switch may be off or disconnected from the network. Check the switch in question to confirm that it is powered on and connected to the network. If the switch is connected to the network, verify with Director that it is properly configured. For event 205 and 206, update the configuration and power cycle the switch. After restart, confirm network visibility and the switch's configuration.
117	Information	Switch < Voice Switch Host Name >: Established connection to switch < Voice Switch Host Name>.	The switches established a connection and are communicating with each other.	No action.
119	Warning	Switch < Voice Switch Host Name >: Excessive number of packets lost from < Voice Switch Host Name>.	The switch is losing an excessive number of packets.	Verify that your network configuration meets the requirements.

ID	Severity Level	Message	Cause	Action
127	Error	Switch < Voice Switch Host Name>: Failed to forward call on <CHM Type> from <extension number> to <extension number>.	The call cannot be forwarded to the specified extension.	Confirm that the specified extension's call handling mode configuration is valid. This error can appear when the destination extension is connected to a Voice Switch that is either offline or unavailable to the network.
130	Error	Switch < Voice Switch Host Name>: Failed to redirect incoming fax from <extension number> to <extension number>.	An incoming fax transmission call was not redirected to the fax extension.	Confirm that the extension is properly configured for fax redirection. Confirm that the fax extension is operating properly.
131	E Error	Switch < Voice Switch Host Name>: Extension <extension number> failed to acquire port <port number>.	The Voice Switch was unable to configure the specified extension on the desired port.	Reboot the switch. If this error persists, contact Mitel Technical Support.
132	Information	Switch < Voice Switch Host Name>: Call restriction violation, call placed from <extension number> to <dialed number>.	The specified extension dialed a restricted number.	Inform user about dial-out restrictions.

ID	Severity Level	Message	Cause	Action
138	Error	Switch < Voice Switch Host Name>: Memory corruption detected - bad block <parameter pinpointing failing block> in partition <parameter pinpointing failing partition>.	Memory block corruption detected.	Reboot the switch. If the event persists, replace the switch.
140	Error	Switch < Voice Switch Host Name>: Cannot re-initialize NvRam - Cannot Continue.	The flash memory in the Voice Switch is bad.	Replace the switch.
141	Warning	Media module is taking too long to respond.	Media response timed out.	Restart the switch in case of non-linux switches or restart stts in case of virtual switch/ VMB or restart stmedia and stts in case of UCB.
143	Warning	Switch < Voice Switch Host Name>: Echo train grade F port <port number>.	The specified port did not receive proper echo cancellation properties. The trunk or phone connected to the port may exhibit poor sound quality or echo.	Use Connect Director to reset the port. If the error was reported on a phone port, lift the phone's receiver to view the event log. (You may need to cover the mouthpiece to prevent ambient noise pickup.) If the error persists on a phone port, you may need to replace the phone.

ID	Severity Level	Message	Cause	Action
144	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> connected for more than two hours.	The specified trunk connected to the port for two or more hours.	Confirm that an active call is in progress. If no call is present, reset the port from Connect Director.
145	Warning	Switch < Voice Switch Host Name>: Echo coeffs stuck possibly needs to be retrained port <port number>.	The echo suppression software was unable to adapt to a call in progress.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.
146	Information	Switch < Voice Switch Host Name>: Echo train grade A port <port number>.	The echo suppression software is properly configured.	No action.
147	Information	Switch < Voice Switch Host Name>: Echo train grade C port <port number>.	The echo suppression software is properly configured.	No action.
148	Warning	Switch < Voice Switch Host Name>: Low Erl possible hardware problem port <port number>.	The echo suppression software detected a low echo-return loss on the specified port. This error can occur when modem or fax calls connect to a port. Event is infrequent and random.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.

ID	Severity Level	Message	Cause	Action
149	Warning	Switch < Voice Switch Host Name>: Low Erle port <port number>.	The echo suppression software detected a low echo-return loss on the specified port.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.
151	Information	Switch < Voice Switch Host Name>: Reboot due to configuration synchronization.	Reboot due to configuration change.	No action.
152	Warning	Switch < Voice Switch Host Name>: DSP< DSP number> - 80% utilization.	The DSP on this switch is nearing capacity.	No action for an isolated occurrence.
153	Error	Switch < Voice Switch Host Name>: DSP <DSP number> - 100% utilization.	The DSP on this switch reached maximum capacity. In most instances, this event does not affect operations.	No action for an isolated occurrence. If the error persists, reboot the switch.

ID	Severity Level	Message	Cause	Action
157	Error	Switch < Voice Switch Host Name>: Received DHCP NAK for IP address <IP Address>.	The DHCP server responded negatively to a DHCP lease renewal request. The IP address previously assigned to the switch is no longer available for that device. The DHCP server assigns the switch a new IP address.	In Connect Director, display the Switches page and open the switch's record. Change the switch's IP address to the address assigned to it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the server.)
158	Warning	Switch < Voice Switch Host Name>: DHCP lease expired for IP address <IP Address>.	The DHCP lease for the switch expired and the switch is currently obtaining a new IP address. While the switch is obtaining another IP address, it is unable to communicate with the server.	In Connect Director, display the Switches page and open the switch's record. Change the switch's IP Address to the address assigned it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the server.)
159	Error	Switch < Voice Switch Host Name>: DHCP IP address mismatch: <IP Address> Existing address: <IP Address> Offered address: <IP Address> Fatal Error... Rebooting < Voice Switch Host Name>.	The IP address currently stored in the switch's flash memory is not the same as the address that DHCP is trying to assign to it. The switch automatically reboots and obtains a new address.	In Connect Director, display the Switches page and open the switch's record. Change the switch's IP address to the address assigned to it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the server.)

ID	Severity Level	Message	Cause	Action
160	Error	Switch < Voice Switch Host Name>: HAPI command failed. System automatically restarting.	The Voice Switch experienced a fatal internal software error.	Contact Mitel Technical Support for updated information about fatal errors.
161	Error	Switch < Voice Switch Host Name>: Connection to Telephony Management Service terminated - too many unacknowledged events.	The Voice Switch stopped communicating with the TMS Server. This error can result from a CPU overload on the server.	Check the server for applications that are placing inordinate demands on the processor. Correct any application errors causing CPU overload.
162	Error	Switch < Voice Switch Host Name>: Another device using the same IP address detected.	A device with the same IP address as the switch appeared on the network.	Remove the offending device from the network, or ask the network administrator to assign the switch an alternate IP address.
163	Information	Switch < Voice Switch Host Name>: Ethernet link established: using <Ethernet speed> <Duplex mode>.	The switch is connected to the Ethernet network.	No action.
164	Error	Switch < Voice Switch Host Name>: Ethernet link lost.	The switch is no longer connected to the Ethernet network.	Confirm that network cables and ports are connected properly and are in working order.
165	Warning	Switch < Voice Switch Host Name>: Receive pair polarity reversed.	The twisted pairing wiring for an ethernet cable is reversed.	Although the switch continues to function, replace the suspect cable.

ID	Severity Level	Message	Cause	Action
166	Error	Switch < Voice Switch Host Name>: Fan failed.	The fan in the Voice Switch failed.	Replace the Voice Switch.
167	Warning	Switch < Voice Switch Host Name>: Fan running slow.	The fan in the Voice Switch is running slow. If the condition persists, the switch may overheat.	If this event is accompanied by Event 168, no action is required. If the error persists, replace the switch.
168	Information	Switch < Voice Switch Host Name>: Fan running normally.	The fan in the switch is running normally.	No action.
169	Information	Switch < Voice Switch Host Name>: Operating temperature: normal.	The internal operating temperature of the switch is within normal operating parameters.	No action.
170	Warning	Switch < Voice Switch Host Name>: Operating temperature: above normal.	The internal operating temperature of the switch is above the acceptable range.	Check if the event is accompanied by Event 166. If so, replace the switch. If the fan is working properly, check the environment in which the switch is operating to confirm that it is capable of supporting a temperature range within the switch's operating parameters.

ID	Severity Level	Message	Cause	Action
171	Error	Switch < Voice Switch Host Name>: Operating temperature: too hot.	The internal operating temperature of the switch exceeded the acceptable operating range. The switch may soon fail.	Check if the event is accompanied by Event 166. If so, replace the switch. If the fan is working properly, check the physical location of the switch for environmental causes.
172	Error	Switch < Voice Switch Host Name>: NvRam failure.	The Voice Switch was unable to write to the flash memory.	Reboot the switch. If the error persists, contact Mitel Technical Support.
173	Error	Switch < Voice Switch Host Name>: VTALK failure.	The 48-Volt DC power supply failed.	Replace the switch.
174	Error	Switch < Voice Switch Host Name>: -70 Volt failure.	The 70-Volt DC power supply failed.	Replace the switch.
175	Information	Switch < Voice Switch Host Name>: Voltage OK.	The power supply that reported a failure is once again operating correctly.	No action.

ID	Severity Level	Message	Cause	Action
176	Error	Switch < Voice Switch Host Name>: Firmware Upgrade Failed: < Voice Switch Host Name> <specific diagnostic message>.	The firmware upgrade for the switch failed.	Check the switch event logs for subsequent appearances of Events 177 and 178. The presence of these events means that the switch automatically recovered and you can ignore the alert of upgrade failure. If Events 177 and 178 are not also present, perform a manual upgrade of the firmware by rebooting the switch. If a reboot does not complete the upgrade, enter the `burnflash` command at the command prompt. This may indicate an installation problem.
177	Information	Switch < Voice Switch Host Name>: Firmware Upgrade Started.	A firmware upgrade started.	No action.
178	Information	Switch < Voice Switch Host Name>: Firmware Upgrade Finished	The firmware upgrade was successful.	No action.
179	Error	1.5V too high: value – d.dV 1.5V too low: value – d.dV	Board failure	Return for repair.
180	Error	1.6V too high: value – d.dV 1.6V too low: value – d.dV	Board failure	Return for repair.

ID	Severity Level	Message	Cause	Action
181	Error	2.0V too high: value – d.dV 2.0V too low: value – d.dV	Board failure	Return for repair.
182	Error	2.5V too high: value – d.dV 2.5V too low: value – d.dV	Board failure	Return for repair.
183	Error	3.3V too high: value – d.dV 3.3V too low: value – d.dV	Board failure	Return for repair.
184	Error	12V too high: value – d.dV 12V too low: value – d.dV	Board failure	Return for repair.
185	Error	25V too high: value – d.dV 25V too low: value – d.dV	Board failure	Return for repair.
186	Error	48V too high: value – d.dV 48V too low: value – d.dV	Board failure	Return for repair.
187	Error	75V too high: value – d.dV 75V too low: value – d.dV	Board failure	Return for repair.

ID	Severity Level	Message	Cause	Action
188	Warning	Operating temperature: below normal	Temperature in room too cool.	Fix the environment.
189	Error	Operating temperature: too cold	Temperature in room too cold.	Fix the environment.
278	Information	Unknown request id or request may have been timedout.	This event is displayed when the switch does not return a status for a TAPI application call or the request-id returned by the switch is not found in TMS. This might occur if the TAPI application releases the call before it could get established, which causes the entries to be deleted in TMS or if the switch is not able to make a call or it took more time to respond to the TMS query.	No action.
284	Warning	Message Processing Duration Exceeded	This event is generated by TMS if it does not receive a response within the processing duration after a request is sent to the switch.	No action.

ID	Severity Level	Message	Cause	Action
1300	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> connected for <number of minutes> minutes.	The trunk on the specified port was continuously active for the number of minutes specified. This message is generated after every two hours of continuous trunk activity.	Check the trunk and verify that an active call is in progress. If no call is present, reset the port from Connect Director.
1301	Error	Switch < Voice Switch Host Name>: Second TMS connection attempt from <IP Address of second TMS server>.	Another Server attempted to take control of the switch.	Only one server can control a switch; multiple servers cannot manage a switch simultaneously. Decide which server you want to manage the switch, then delete the switch from the other server.
1303	Error	Switch < Voice Switch Host Name>: Configured IP <IP Address> does not match actual IP <IP Address>.	The IP address configured for the switch in Director is not the IP address the switch is using.	From Director, change the switch's IP address to match the address the switch uses.
1305	Information	Switch < Voice Switch Host Name>: Free memory reduction trend. Min <minimum memory used>. Avg <Average memory used>.	Reports the switch's memory usage.	No action.

ID	Severity Level	Message	Cause	Action
1306	Warning	Switch < Voice Switch Host Name>: Call was unable to be completed due to insufficient network bandwidth between sites.	An attempted call exceeded the limit on the number of media streams allowed for multiple sites. May indicate the number of media streams configured for multiple-site calls cannot handle the inter-site call traffic.	From Connect Director, open the Site Parameters page and check the number of media streams specified for the “Other Number of Media Streams for Multi_Site” parameter. Use the *Site-Link Configuration Guide* to determine the number of media streams the connection's bandwidth can support. If the bandwidth can support more media streams, raise the value specified for the site. Increasing the number of media streams may reduce sound quality for multiple-site calls.
1307	Information	Switch < Voice Switch Host Name>: Trunk on port <port number> forced out of service.	Not reported in NT event log.	;
1308	Warning	Switch < Voice Switch Host Name>: SGT1 is in %2 loopback mode.	The SGT1 switch is in a local or payload loopback.	Your service provider is performing diagnostic tests.
1309	Information	Switch < Voice Switch Host Name>: SGT1 is out of %2 loopback mode.	Loopback on this switch removed.	No action.

ID	Severity Level	Message	Cause	Action
1310	Error	Switch < Voice Switch Host Name>: SGT1 framing error <specific error>.	The SGT1 switch is experiencing framing errors.	Check the cabling. Contact your service provider.
1311	Information	Switch < Voice Switch Host Name >: SGT1 framing ok.	Framing restored.	No action.
1312	Error	Switch < Voice Switch Host Name>: SGT1 signal error <specific error>.	SGT1 switch lost the SGT1 carrier signal.	Check the cabling. Contact your service provider.
1313	Information	Switch < Voice Switch Host Name>: SGT1 signal ok.	SGT1 carrier signal restored.	No action.
1314	Error (Severity level varies depending on error)	Switch < Voice Switch Host Name>: Config Store: <specific error>.	Notable event while reading non-volatile switch configuration.	No action. The configuration received from the server supplies any missing data.
1316	Information	Switch < Voice Switch Host Name>: Trunk to trunk transfer from port <port number> stopped after <time interval> of connection.	The system disconnected trunks on the reported ports as a result of option settings in Director.	No action.

ID	Severity Level	Message	Cause	Action
1317	Information	Switch < Voice Switch Host Name>: Software Telephony Switch < Voice Switch> Starting.	SoftSwitch started.	No action.
1319	Warning	Switch < Voice Switch Host Name>: Emergency Services Call on port <port> from user <user> at <ext or ani>.	User called emergency number.	No action -- someone already called for help.
1320	Error	Switch < Voice Switch Host Name>: SoftSwitch Cannot Start: Logger Failed.	The SoftSwitch failed to start because it was unable to contact the NT event log.	This message appears only after SoftSwitch successfully contacts the NT Event Log Manager—meaning that the error condition is cleared (possibly by the clearing of a full NT event log).
1324	Information	Switch < Voice Switch Host Name>: Reboot due to configuration change.	Certain configuration changes, for example, changing signalling protocols for a SGT1, requires a switch reboot.	No action.
1325	Warning	Switch < Voice Switch Host Name>: Received request to reset the configuration and restart the system.	Can only be caused by executing a `ipbxctl` command. The command is only for use by Mitel Technical Support personnel.	This message confirms that SoftSwitch stopped on command from the NT Service Manager. No action is needed.

ID	Severity Level	Message	Cause	Action
1326	Information	Switch < Voice Switch Host Name>: SoftSwitch Stopping %2.	SoftSwitch service stopped.	If the SoftSwitch service does not restart within two minutes, perform a manual restart and contact Mitel Technical Support.
1330	Error	Switch < Voice Switch Host Name>: Soft Switch Stopping <reason>.	SoftSwitch service stopped.	If the SoftSwitch service does not restart within two minutes, perform a manual restart and contact Mitel Technical Support.
1331	Error	Switch < Voice Switch Host Name>: Assertion failure <failure>	A software assertion failed.	If the problem persists, contact Mitel Technical Support and be prepared to provide the log files for further analysis.
1332	Information	Switch < Voice Switch Host Name>: Trunk <trunk> received digits <digits> (no match), redirected to <destination>.	Incoming call on trunk failed to route.	Check trunk configuration.
1333	Information	Switch < Voice Switch Host Name>: Trunk <trunk> received digits <digits> (too many), used <number>, redirected to <destination>.	Incoming call on trunk failed to route.	Check trunk configuration
1334	Information	Switch < Voice Switch Host Name>: Trunks unavailable to route <extension> to <dialed number>.	Outgoing call failed due to no available trunks.	Verify that trunks are in-use.

ID	Severity Level	Message	Cause	Action
1338	Information	Switch < Voice Switch Host Name>: Using PSTN failover to reach extension <extension> from extension <extension>, reason <reason>.	PSTN failover feature invoked.	Verify network connectivity between sites.
1339	Error	Switch < Voice Switch Host Name>: <message>.	Request to record a call failed.	If the problem persists, contact Mitel Technical Support and be prepared to provide the log files for further analysis.
1340	Warning	Switch < Voice Switch Host Name>: <message>.	Attempt to conference using switch conference resources failed.	Check switch configuration.
1341	Warning	Switch < Voice Switch Host Name>: Call was unable to be completed due to insufficient network bandwidth at site <site name>.	Bandwidth limits have been exceeded.	Check site configuration.
1342	Error	Switch < Voice Switch Host Name>: SGT1/ E1 PRI D channel down.	PRI D channel down.	If the problem persists, contact PRI service provider.
1343	Information	Switch < Voice Switch Host Name>: SGT1/E1 PRI D channel up.	PRI D channel up.	No action.

ID	Severity Level	Message	Cause	Action
1344	Information	Switch < Voice Switch Host Name>: SIP Dynamic Trunk Event: <description>.	Information about SIP trunk registrations.	No action.
1355	Information	Switch < Voice Switch Host Name>: Monitoring Agent was started. or Switch < Voice Switch Host Name>: Monitoring Agent was stopped.	The Monitoring Agent was started or stopped.	No action.
1356	Warning	Switch < Voice Switch Host Name>: Monitoring Agent Warning: <message>	A recoverable error occurred for the Monitoring Agent.	Be aware that metrics collected for a specific call might be inaccurate.
1357	Error	Switch < Voice Switch Host Name>: Monitoring Agent Warning: <message>	The Monitoring Agent experienced a fatal error and is no longer running.;As a result, call metrics are not collected for calls to that switch.	Restart the switch. If the problem persists, contact Mitel Technical Support.

13.5 Telephony Management Service (TMS)

Event codes: TMS lists and describes event codes for TMS.

Table 56: Event codes: TMS

ID	Severity Levels	Message	Cause	Action
200	Error	TMS Assertion Failure: <parameters>.	TMS encountered a non-fatal error.	Restart the TMS service. Contact Mitel Technical Support and submit a support incident.
201	Information	TMS service started. Version: <version number>.	TMS service started.	No action.
202	Information	TMS service stopped.	TMS service stopped.	No action. If the stoppage was unintentional, check the event logs for a cause.
203	Information	Updated switch < Voice Switch Host Name> switch firmware to revision <version number>.	Switch upgraded to the version of firmware identified in the event.	No action.
204	Error	Failed to update switch < Voice Switch Host Name> switch firmware to revision <version number>.	An upgrade to the switch's firmware failed. This switch does not operate properly until the firmware upgrade is complete.	Review the event log and correct any errors related to the upgrade failure. Reset the switch from Connect Director. If the event persists, contact Mitel Technical Support.

ID	Severity Levels	Message	Cause	Action
205	Warning	Switch Ethernet Address to IP Address mapping change. Old Mapping: <MAC Address> <IP Address> New Mapping: <MAC Address> <IP Address> Detected telephony switch that changed its IP address or is using an IP address previously in use by a different switch.	TMS detected a configured switch with a changed IP address changed. The event reports previously assigned and current MAC and IP addresses for the switch.	Ensure that the Switch <MAC Address> is set up with a correct IP address. If the DHCP lease for the switch expires and the switch receives a new IP address. If this happens frequently, contact Mitel Technical Support.
206	Error	Switch Ethernet-Address IP-Address conflict. Expect: <MAC Address> <IP Address> Found: <MAC Address> <IP Address> Detected telephony switch with IP address or Ethernet address in conflict with the configuration database.	TMS detected a switch with a MAC address and/or an IP address that conflicts with the address(es) configured for the device in Connect Director. The conflicting address or addresses result from a misconfigured DHCP server or an incorrect switch record.	If address information was entered incorrectly for the switch, use Connect Director to edit the record to include the correct address(es). (The switch reboots automatically when you save the record.) If the DHCP server assigned an incorrect IP address to the switch, correct the DHCP record and reboot the switch force reassignment of a new IP address.

ID	Severity Levels	Message	Cause	Action
211	Warning	Switch < Voice Switch Host Name> booted via FTP. Possible switch firmware corruption. If a failure occurs during firmware upgrade, a switch must boot via FTP instead of from its firmware.	The switch is no longer able to boot from flash memory and is now booting via FTP. The cause of the error is a failed firmware upgrade, bad firmware, or a reset caused by pressing the reset button.	Reburn flash memory. On the server, open a command prompt window and change the directory to the server directory (typical path is `Program Files\Shoreline Teleworks\ShoreTel Server`) Enter the `burnflash` command in this format: `burnflash -s <IP address>` (Use the IP address of the switch you are upgrading.) When the `burnflash` process is complete, check the event logs to confirm that the switch is no longer booting from FTP. If the event persists, replace the switch.
212	Warning	Switch < Voice Switch Host Name> software version mismatch: TMS Version: <TMS version> Switch Version:< Voice Switch version> The switch firmware is upgraded the next time the switch boots.	TMS detects a switch with outdated firmware.	New switches ship with base firmware that is “down” from the current version. An automatic upgrade is confirmed when the device is put into service. (This event also appears during field upgrades.) From Connect Director, open the **Maintenance** > **Status and Maintenance** > **Appliances** page and reboot the switch.

ID	Severity Levels	Message	Cause	Action
213	Error	Unexpected Ethernet address for switch < Voice Switch Host Name> Expect:<MAC Address> Found:<MAC Address>. The switch is reporting an Ethernet address different from the one specified in the configuration database.	The MAC address in the switch's configuration record is incorrect.	From Connect Director, open the switch configuration record and correct the MAC address.
214	Warning	Switch "< Voice Switch Host Name>" firmware file version mismatch: TMS Version: <TMS Version> File Version: <File version> Cannot upgrade switch firmware. The firmware file used to upgrade the switch firmware does not have the correct version.	The firmware file `filessys.dll` does not match the TMS file version. The switch’s firmware cannot be upgraded.	Re-install the server software. If the event persists, contact Mitel Technical Support.

ID	Severity Levels	Message	Cause	Action
221	Error	Failed to load firmware image file <FileSys.dll>. Telephony Management Service was unable to load the switch firmware image file.	A switch firmware upgrade may not be possible.	This error appears when the `\Shoreline Communications \ShoreTel Server` does not have the `FileSys.dll` file, and TMS cannot find or access this file. If this error appears frequently, contact Mitel Technical Support.
223	Warning	Detected an unexpected configuration change. This may indicate that TMS was not notified of a change. Configuration inconsistency corrected.	TMS corrected a configuration mismatch that it detected on a switch.	No action. If this error appears frequently, contact Mitel Technical Support.
227	Information	TMS service starting. Version: <TMS version>	TMS service started.	No action.
230	Warning	TMS was unable to find an TCP/IP network interface. This computer may not have a network adapter or may not be connected to a network. Operation continues in stand-alone mode until the next TMS restart.	TMS failed to detect a network interface on the server.	Reboot the server. Troubleshoot the server's network configuration and make necessary repairs or modifications.

ID	Severity Levels	Message	Cause	Action
231	Error	The configuration for switch "< Voice Switch Host Name>" no longer matches the system configuration database. This condition may exist on additional switches, and may result in unexpected behavior. To resolve the problem, restart any switch having a configuration mismatch (as shown on the Maintenance > Status and Maintenance > Appliances page in Connect Director).	The configuration on the switch does not match the one stored on TMS. The mismatch can cause irregular behavior on devices connected to this switch. The error appears when there are network problems between the server and the switch, or is generated as a result of corrupted flash memory.	To synchronize the configuration data, reboot the switch. After the switch restarts, check the event log for messages that indicate network problems between the switch and the server to correct any network errors. If the event persists, check for events that indicate corrupted flash memory and follow the instructions for correcting the problem.
233	Warning	TMS disconnected from switch "< Voice Switch Host Name>" (< Voice Switch IP Address>). This may be as a result of a network outage, administrative action, or unexpected switch behavior.	TMS is reporting that it cannot communicate with the switch.	The disconnect is typically caused by a network-related problem such as outage or degraded performance. Correct the network problem. (The event also appears when the switch is taken offline for maintenance.)

ID	Severity Levels	Message	Cause	Action
234	Information	TMS connected to switch "< Voice Switch Host Name>" (< Voice Switch IP Address>).	TMS detected a switch and opened communications with the device.	No action.
235	Information	<Connection type user or App Server> TAPI connection for login <user ID> from <IP address or name of system initiating the connection> initiated.	New TAPI connection accepted from a user at a specific IP address.	No action.
237	Information	TAPI connection for login <user ID> from <IP address or name of system that is connected> closed.	The TAPI connection to the specified user was closed.	No action.
238	Warning	TAPI connection with login <user ID> from <IP address> denied access to extension <Extension DN>.	A user's remote TSP configurati on tried to get ownership ac cess to an exten sion the user do es not own.	Contact the user and help him or her correct the client configuration.

ID	Severity Levels	Message	Cause	Action
239	Error	Attempting to connect to switch at IP address <IP address> with incorrect product type: Expected product type: <Product Type ID> Actual product type: <Product Type ID>. Configuration database includes incorrect product type for the switch at this IP address.	The switch at an IP address does not correspond to the switch type identified in the configuration database.	Edit the switch configuration information to reflect the correct data. Correct the IP address, or delete the switch, and create a new switch configured with the correct switch type.
241	Error	The Call Accounting Service returned the following error (<Error code>, Source = < component that returned error>): <Message description>.	TMS received an error code from the call accounting service in response to logged data.	Contact Mitel Technical Support and be prepared to provide server logs from the day of the occurrence. Note: This error is sometimes the result of a “false positive” and may not indicate serious problems.
243	Warning	TAPI request thread timed out after <number of seconds> seconds for context <context handle ID> performing request type <request type ID>.	TMS is not responding to internal messages in a timely fashion.	This event can precede a significant failure in TMS. Contact Mitel Technical Support and be prepared to provide server logs from the day of the occurrence.

ID	Severity Levels	Message	Cause	Action
244	Warning	<Connection type user or App Server> TAPI connection attempt for login <user ID> from <IP address> failed. Invalid <LoginID>.	A TAPI connection request was denied due to an invalid login or password.	Contact the user and assist him or her with login information.
246	Information	Telephony Management Service logged an informational debug message. The debug message contents are:<Message>	A logic assertion within TMS failed.	No action, unless the event is accompanied by system failures. If system failures are occurring, contact Mitel Technical Support.
247	Information	The log file <log file name> current size is <log file size> bytes. It exceeded its maximum size limit of <max log size> bytes. Further logging is suspended.	The log file cannot write new events because it reached its maximum size.	This event typically results from a configuration that creates an event loop. Review all configured call handling modes for loops. Example: UserA forwards calls to userB, who in turn is forwarding all calls to userA. If no logic fault is found, contact Mitel Technical Support.

ID	Severity Levels	Message	Cause	Action
248	Information	Failed to write to the log file <log file name> (Error Code – <error code>). Further logging is suspended until midnight or service restart. The log files collect diagnostics and are not required for correct system behavior.	TMS failed to write to a log files. (The embedded error code identifies the cause of the write failure.)	No action. ; Log files are not essential for telephony operations. ; If the problem persists, contact Mitel Technical Support.
249	Information	Failed to write to the log file <log file name> because another process locked a portion of the file .	A write to the log file failed because the file was locked by another process.	This event can occur during normal backups of system log files. Local administrators can choose to suspend logging activity during scheduled backups.

ID	Severity Levels	Message	Cause	Action
251	Information	<Connection type user or App Server> TAPI connection did not give NEWCALL event (CallID – <Call ID>, Login: <user ID>, From: <IP address>). This may indicate a TAPI connectivity outage between the server and Telephony Management Service on the machine specified.	When TMS notified a remote TSP of a new call, the remote TSP failed to accept or acknowledge that notification.	No action. If the event is accompanied by unusual client behavior, report the error to Mitel Technical Support.
252	Information	A time change of %1 was detected in the system clock.	The system clock was changed.	No action. Changing the system clock can result in inaccurate call timers for applications and skew call detail reporting records. A system clock adjustment affects only calls in progress at the time of the change.

ID	Severity Levels	Message	Cause	Action
253	Error	Detected rogue IP Phone Call Agent that established a control connection with an IP Phone. IP Phone Details: IP Address:<IP address> MAC Address:<MAC Address> Call Agent Details:<Call Agent Details> Config'd Agent:<Configured Agent> Rogue Agent:<Rogue Agent>.	This error can occur when a Call Agent switch is replaced and the previous switch is still on-line, or if an IP phone is moved from one IP Phone System to another. This error can cause the IP phone to exhibit unexpected behavior.	Reconfigure the IP phone from the rogue Call Agent or take the rogue agent off-line. Typically this event occurs when two call agents attempt to control the same IP phone.
255	Warning	The configuration database does not list this server as a configured server. The TMS (Telephony Management Services) on this system remains in standby and is not fully available while this condition is present. Check the Connect Director configuration of servers for correctness.	This server is not configured in Connect Director as one of the servers; or IP addresses on this server do not match any of the configured IP addresses for servers in Connect Director.	The administrator must configure this server correctly in Connect Director and ensure that a correct IP address is given.

ID	Severity Levels	Message	Cause	Action
256	Warning	This server is configured with `Loopback` IP address. This may prevent other servers from reaching this server. Configure with proper IP address for this server.	Servers cannot be configured with `loopback` IP addresses.	The administrator must configure this server correctly in Connect Director and ensure that the correct IP address is given.
257	Error	Telephony Management Service (TMS) was unable to connect to or access the configuration database on the computer. Ensure that network connectivity exists between this computer and the configuration database, and that the database services are operational on the main server. TMS on this system remains in standby and is not fully available while this condition is present. Check the Connect Director configuration of servers for correctness. (Error code – <Error code>).	This server is unable to connect to the database on the Headquarters server.	The administrator must ensure there is network connectivity between this server and headquarters server. If the network connection is present and this condition persists, contact Mitel Technical Support.

ID	Severity Levels	Message	Cause	Action
258	Error	The main server is configured in the configuration database with `loopback` IP address 127.0.0.1. Ensure that proper IP address is configured for the main server. The TMS (Telephony Management Service) remains in standby and is not fully available while this condition is present. Check the Connect Director configuration of servers for correctness.	The main Headquarters server is configured with a `loopback` IP address.	The administrator must provide the correct IP address of the Headquarters server.
259	Information	The Telephony Management Service is reinitializing because new configuration changes have occurred. <Version of Server>	When an administrator changes the IP address of a remote server, the Telephony Management Service on that remote server is reinitialized with the new IP address. This event indicates the start of the initialization process.	No action needed.

ID	Severity Levels	Message	Cause	Action
260	Information	The Telephony Management Se rvice is reinitializ ed with the new configuration ch anges. <Version of Server>	When the administrator changes the IP address of a remote server, The Telephony Management Service on that remote server is reinitialized with the new IP address. This event indicates end of the reinitialization process.	No action needed.
261	Warning	This Server is deleted from the configuration database. The server was deleted permanently or configuration changes were made to this server that caused it to be deleted and added again. TMS (Telephony Management Service) on this server is reinitialized and remains in standby until the server is added again.	The Telephony Management Service is reinitialized if configuration changes caused this server to be deleted and added again, or the service remains in standby if this server is deleted.	If administrator made the configuration changes that caused server to be deleted and added again, check the Maintenance > Status and Maintenance > Servers page in Connect Director to see if all the services are running correctly. If not, contact Mitel Technical Support.

ID	Severity Levels	Message	Cause	Action
262	Error	Configured IP address for this server changed in the configuration database. TMS (Telephony Management Service) needs to bind to new IP address and needs to be reinitialized with the new IP address.	The IP address configured for this server changed in configuration database and Telephony Management service is reinitialized with the new IP address.	Check whether all the services are reinitialized correctly after the IP address is changed. Check the Maintenance > Status and Maintenance > Servers page in Connect Director to see if all the services are running correctly. If not, contact Mitel Technical Support.
275	Information	The Telephony Management Server received an invalid configuration type: <number>.	An internal TMS configuration error occurred.	No action, unless the event is accompanied by system failures. If system failures are occurring, contact Mitel Support.

13.6 Voice Mail Port Manager

Event Codes: Voice Mail Port Manager lists and describes event codes for voice mail:

Table 57: Event Codes: Voice Mail Port Manager

ID	Severity Level	Message	Cause	Action
401	Information	Voice Mail Port Manager starting.Version: <version number>.	Voice Mail Port Manager service started.	No action.

ID	Severity Level	Message	Cause	Action
402	Information	Voice Mail Port Manager stopping.	Voice Mail Port Manager service stopped. This error usually results from an intentional service stoppage, stoppage by a dependent service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for related errors and correct them. If necessary, restart the service.
410	Information	Recording stopped. The disk got full during recording.	A message was not completely recorded. ; The hard drive on which `\shoreline data\vms` resides is full.	Free up space on the drive.
411	Information	Recording stopped. The caller went silent during recording.	The person leaving a voice message was silent for more than 30 seconds, triggering automatic termination of the recording. The message is still sent so no action is required.	No action. The recipient is still able to retrieve the partial message.
412	Information	Recording stopped. No response from the switch.	The recording of a message halted when the connection to the switch dropped.	Check the event log and correct any errors related to the dropped connection.

ID	Severity Level	Message	Cause	Action
414	Error	The outbound AMIS phone number %1 for System ID %2 was a wrong number. No more attempts are made to this system/number until it is corrected. Verify that the number is correct.	;	Verify that the phone number is correct.
415	Error	The outbound AMIS phone number for System ID %1 was not found. Verify that the System ID includes a phone number associated with it.	;	Verify that the System ID includes a phone number associated with it.
416	Error	An internal error occurred. The system was unable to delete an AMIS message from the outbound message queue. System ID%1 mail box ID %2 Message ID %3	;	;
417	Error	The undeliverable AMIS message from %2 was not able to be delivered to %3 for AMIS System ID %1. The message is being deleted.	;	;

ID	Severity Level	Message	Cause	Action
418	Error	An error occurred during the delivery of an AMIS message from %2 to %3 for AMIS System ID %1, which prevents retrying delivery at a later time. The message is missing.	;	;
419	Error	An error occurred during the delivery of an AMIS message from %2 to %3 (AMIS System ID:mail box), and the system tried %1 times to deliver this message. The message is returned to the sender and deleted from the outbound queue.	;	;
420	Error	An internal error occurred communicating between the Port Manager and another server. The error code was %1.	;	;
421	Error	Number of delivery attempts (%2) to AMIS System ID %1 exceeded. Verify that the number is correct.	;	;

ID	Severity Level	Message	Cause	Action
1001	Information	Voice Mail Message Server starting. ;Version: <version number>	Voice Mail Message Server service started.	No action.
1002	Information	Voice Mail Message Server stopping.	Voice Mail message service stopped. This error usually results from an intentional service stoppage, stoppage by a dependant service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for related errors and correct them. If necessary, restart the service.
1003	Information	Voice Mail disk usage reached maximum capacity.	A message was not completely recorded. ; The hard drive on which `\shoreline data\vms` resides is full.	Take necessary action to free up space on the hard disk.
1004	Information	No available message stores in Voice Mail.	The voice mail system cannot locate message storage directory `\shoreline data\vms` on the server.	Verify that the hard drive or drive partition where \shoreline data\vms resides is operating properly. Correct any disk problems and restart the server. If event persists, call Mitel Technical Support.

ID	Severity Level	Message	Cause	Action
1005	Information	Voice Mail disk usage is greater than 90 percent.	The hard drive on which the message storage directory \shoreline data\vms resides is nearly full. When no disk space remains, Voice Mail is unable to store new messages. This error appears once each day when the system disk is more than 90% full.	Free up disk space on the hard drive where \shoreline data\vms resides.
1006	Information	Error writing mail box file to disk.	The Voice Mail system failed to a mailbox.dat file on the disk where the message storage directory \shoreline data\vms resides.	The write failure can result from corrupted data or a Windows NT error. Verify that the hard drive or drive partition where \shoreline data\vms resides is operating properly. Correct any disk problems and restart the server.
1007	Information	Error, disk got full when writing mail box <mail box number>.	The hard drive on which the message storage directory \shoreline data\vms resides is full. The mail box a user attempted to create was not added.	Free up disk space on the hard drive where \shoreline data\vms resides. ;

ID	Severity Level	Message	Cause	Action
1009	Information	Failed to get <registry string> from registry	Unable to open required entry in the registry.	This may indicate an installation problem. Contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.
1011	Information	Voice Mail Message Server was unable to open message <file name> Error < specific error>.	The Voice Mail server was unable to retrieve a message because it was unable to read the disk.	Verify that the hard drive or drive partition where `\shoreline data\vms` resides is operating properly. Correct any disk problems and restart the server. If the error persists, contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.
1014	Information	Failed to attach message <file name> to mail box <mail box ID> Error < specific error>.	Error resulted from a failure with a specific mail box.	This event results from a full mail box included in a distribution list (or any other general failure related to a mail box). Verify that the mail box is full. If not, contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.
1015	Error	All Voice Mail Message Server threads in use.	The mail server cannot access resources.	This event corresponds to a logged NT event indicating serious problems that can prevent clients from retrieving voice mail. Contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.

ID	Severity Level	Message	Cause	Action
1016	Error	The system failed to send voice message <file name>.	The Voice Mail server failed to add a message to a user mail box.	The probable cause is corrupted mail box data. Verify that the mail box is functioning properly. If not, contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.
1018	Error	The SMTP server used by voice mail is not sending messages.	The SMTP server is not forwarding stored messages on to recipients.	Verify that the SMTP server is down or that its address is set up incorrectly
1019	Error	Voice message sent to voice mail server <file name> returned.	Message sent to a remote server returned.	Contact Mitel Technical Support and be prepared to provide the voice mail log files for further analysis.
1020	Error	Failed to find entry in database for voice mail server.	A Voice Mail server looks up its own address in the database. The event indicates that the server was unable to locate a database record that matched its server name and/or IP address.	The probable cause is incorrect server information or incorrect IP address in the database. Edit the database record to include the correct data.
1101	Information	Voice Mail Application starting. Version: <version number>.	Voice Mail Application service started.	No action.

ID	Severity Level	Message	Cause	Action
1102	Information	Voice Mail Application stopping.	Voice Mail Application service stopped. This error usually results from an intentional service stoppage, stoppage by a dependant service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for event watch errors and correct them. If necessary, restart the service.
1109	Information	Unable to create message <message number> Error <error number>.	The system was unable to write to the mailbox.dat file on the disk where the message directory `\shoreline data\vms` resides.	A write failure is usually the result of corrupted data or a Windows NT error. Verify that the hard drive or drive partition where `\shoreline data\vms` resides is operating properly. Correct any disk problems and restart the server.
1110	Information	Voice Mail disk usage reached maximum capacity.	The hard disk drive or disk partition where the message directory `\shoreline data\vms` resides is full. Voice mail is unable to accept any new messages until disk space is made available.	Free up disk space on the drive where `\shoreline data\vms` resides.

ID	Severity Level	Message	Cause	Action
1111	Information	Removed <file name> millisecond message. Messages from callers must be at least <configured limit> milliseconds to send.	The message was too short to retain. Error is no longer logged.	;
1112	Information	Message notification was unable to open phrase libraries.<file name> Error <error number>.	The voice mail system was unable to locate system prompts. The hard disk drive or disk partition where the message directory `\shoreline data\vms` resides is unavailable, was intentionally removed from the system, or is corrupted.	Verify that the hard drive or drive partition where `\shoreline data\vms` resides is operating properly. Correct any disk problems and restart the server.

ID	Severity Level	Message	Cause	Action
1113	Information	There have been too many invalid logon attempts for mail box <mail box number>.	An attempt to log in to this mail box failed. While this event can indicate an unauthorized user, it most often results from a forgotten (or mistyped) password. The number of attempts is customizable and based on the **Max login attempts before disconnect** setting under **Administration** > **Features** > **Voice Mail** > **Options** in Connect Director.	No action.
1114	Information	Listen unheard was unable to open message <message number>.	The server was unable to locate the indicated message number. The hard disk drive or disk partition where the message directory `\shoreline data\vms` resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where `\shoreline data\vms` resides is operating properly. Correct any disk problems and restart the server.

ID	Severity Level	Message	Cause	Action
1115	Information	Listen saved was unable to open message <message number>.	The server was unable to locate the indicated message number. The hard disk drive or disk partition where the message directory `\shoreline data\vms` resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where `\shoreline data \vms`resides is operating properly. Correct any disk problems and restart the server.
1116	Information	Listen deleted was unable to open message <message number>.	The server was unable to locate the indicated message number. The hard disk drive or disk partition where the message directory `\shoreline data\vms` resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where `\shoreline data\vms` resides is operating properly. Correct any disk problems and restart the server.
1119	Error	Voice Mail Application determined that the Voice Mail Message Server is down.	Sending of voice messages failed.	Restart mail server.

ID	Severity Level	Message	Cause	Action
1121	Error	The SMTP message delivery was not a success. More details on the error can be found in the QMAIL logs available at: `/shoretel/qmail/logs/qmail.lo`	Details can only be found by checking the qmail logs in the specified folder.	The corrective action depends on the error found in qmail logs For example, 1. User wasn't able to establish an SMTP connection because there is a problem with the SMT/ Network configuration. 2. 550 5.7.1 Unable to relay for User@10.57.1.218 because there is a problem with the user configuration and current network statistics of the user.

13.7 Media Driver

Event Codes: Media Driver lists and describes event codes for the Media Driver.

Table 58: Event Codes: Media Driver

ID	Severity Level	Message	Cause	Action
2100	Information	Media Driver started.Version: <Version Number>.	Media Driver started.	No action.
2101	Information	Media Driver stopped.	Media Driver stopped.	No action.
2102	Error	Media Driver failed to start. <Message>.	The Media Driver failed to start.	Contact Mitel Technical Support and be prepared to provide the NT system, and NT application log files for further analysis.

ID	Severity Level	Message	Cause	Action
2103	Error	Failed to allocate non-paged pool memory. <Message>	The Media driver was unable to allocate non-paged pool memory. This failure can result in an inability to deliver media to IVR applications, and/or force a system restart with a crash dump.	Perform a system restart. Contact Mitel Technical Support and be prepared to provide the NT system application log files for further analysis.
2104	Information	Poor audio timer resolution. <Message>	The Media driver's internal timer detected an inaccuracy that was corrected.	No action. The event can indicate the occurrence of a voice-quality event that caused the driver to reset its internal timer.
2105	Error	Unable to map application buffer into kernal memory space. <Message>	The Media driver was unable to translate a user buffer to system memory. This failure can result in an inability to deliver media to IVR applications, and/or force a system restart with a crash dump.	If this error is appearing frequently, perform a system restart, In addition, contact Mitel Technical Support and be prepared to provide the NT system, and NT application log files for further analysis.
2106	Information	Recording of call was terminated due to silence. <Message>	The Media driver detected silence when recording a message. This may be due to incorrect behavior from one of the switches.	If this error is appearing frequently, perform a system restart, In addition, contact Mitel Technical Support and be prepared to provide the NT system, and NT application log files for further analysis.

ID	Severity Level	Message	Cause	Action
2107	Error	Media Driver is unable to bind all media channels within the configured UDP port range. Either the UDP port range given is not sufficient, or some of the UDP ports are being used by other components in this system. <Configured UDP Range from registry for the Driver>	The UDP ports to be used by the Media Driver can be configured using the registry by giving the range of UDP ports. Driver is unable to bind to the UDP ports given in the range.	The administrator must ensure that the UDP port range configured in the registry includes at least 255 empty UDP ports, and reboot the server. Or this configuration option may be completely eliminated by removing the registry setting. This option enables the driver to choose any empty UDP port.
2108	Error	Media Driver is configured with invalid UDP port range. <Configured UDP Range from registry for the Driver>	The UDP ports to be used by the Media Driver can be configured using the registry by giving the range of UDP ports. The driver is configured with an invalid UDP port range.	The administrator must ensure that the UDP port range configured in the registry is between 1024 and 65535. After providing the correct UDP port range, the system must be rebooted.
2109	Warning	Media Driver encountered an assertion statement that failed. In some cases an assertion failure may precede a more significant problem. The assertion statement details follow. <Message description>	A logic assertion in Media Driver failed.	If this error is appearing frequently, perform a system restart. In addition, contact Mitel Technical Support and be prepared to provide the NT system, and NT application log files for further analysis.

13.8 Event Watch

Event Codes: Event Watch lists and describes event codes for event watch.

Table 59: Event Codes: Event Watch

ID	Severity Level	Message	Cause	Action
1200	Information	Event Watch service successfully started.	;	No action.
1201	Information	Event Watch service successfully stopped.	;	No action.

13.9 System Management Interface

Event codes: System Management Interface lists and describes event codes for the system management interface.

Table 60: Event codes: System Management Interface

ID	Severity Level	Message	Cause	Action
5102	Information	User <user name> successfully logged in.	Specified user logged into Connect Director. A user history is maintained for auditing purposes.	No action.
5103	Information	User <user name> failed to log in.	The specified user unsuccessfully attempted to log into Connect Director. A user history is maintained for auditing purposes.	No action. (Monitor if the event persists.) While this event might indicate an unauthorized user is trying to access Connect Director, it most often results from a forgotten (or mistyped) password.

13.10 Port Mapper

Event Codes: Port Mapper lists and describes event codes for port mapper.

Table 61: Event Codes: Port Mapper

ID	Severity Level	Message	Cause	Action
700	Information	ShoreTel-PortMap> service starting. Version: <version number>	Port Mapper service started.	No action.
701	Information	<ShoreTel-PortMap> service stopping.	Port Mapper service stopped.	No action.
702	Error	Can't bind <protocol type> socket; port <port number> in use.	The preferred port for the RPC Portmapper (111) is already in use. Another network application or service is probably running on that system. While the port remains unavailable, no communication is possible between TMS and the switches.	Mitel Technical Support, and be prepared to provide server log files.

13.11 Trigger Server

Event Code: Trigger Server lists and describes event codes for trigger server.

Table 62: Event Code: Trigger Server

ID	Severity Level	Message	Cause	Action
800	Information	<Service name> service starting. Version: <Software version number>.	Trigger Server started.	No action.
801	Information	<Service name> service stopping.	Trigger Server stopped.	No action.
805	Error	The notification server lost connectivity with a notification client. This may indicate a network outage or unexpected client behavior. Client: <name of affected service> Status: <error code>.	Usually indicates that one of the services crashed without properly closing its connection.	No action, when related to a service failure. In other instances, check for network outages.
806	Error	The notification server lost connectivity with the primary notification server. This may indicate a network outage or unexpected behavior from the primary notification server.	The connection between a Distributed Voice Mail Server and the HQ Server failed	If the problem persists, collect log files from affected servers and contact Mitel Technical Support. No action, when related to a network outage or other administrative action.

13.12 Distributed Routing Service (DRS)

Event Codes: Distributed Routing Service (DRS) lists and describes event codes for DRS.

Table 63: Event Codes: Distributed Routing Service (DRS)

ID	Severity level	Message	Cause	Action
3100	Information	The Distributed Routing Service (Version %1) started successfully.	The specified version of DRS started.	No action.
3101	Information	The Distributed Routing Service stopped.	DRS stopped.	No action.
3108	Information	The Distributed Routing Service failed to connect to this switch: %n%1	DRS re-established communications with the specified switch.	No action.
3109	Information	The Distributed Routing Service reconnected to this switch: %n%1	Network connectivity may be lost to the specified switch, or the switch may be down.	Fix network connectivity issues, and confirm that the switch is up.

13.13 Kadota Utility

Event Codes: Kadota Utility lists and describes event codes for Kadota utility.

Table 64: Event Codes: Kadota Utility

ID	Severity level	Message	Cause	Action
1400	Information	<ShoreTel-KadotaUtil> service starting. Version: <version number>	Specified version of Kadota Utility started.	No action.

ID	Severity level	Message	Cause	Action
1401	Information	<ShoreTel-KadotaUtil> service stopping.	Kadota Utility stopped.	No action.

13.14 Call Accounting

Event Codes: Call Accounting lists and describes event codes for call accounting.

Table 65: Event Codes: Call Accounting

ID	Severity level	Message	Cause	Action
2000	Warning	TmsCdr records an attempt to archive an entry from table <table name> of <database name> to that of <archive name> with a duplicate <duplicate ID> primary key. It might be caused by a manual manipulation between CDR.mdb and its backup version.	During archiving, the call accounting service encountered a duplicate key value in a table. ; A duplicate value usually means the item was already archived. Results from renaming or moving the CDR database file without also renaming or moving the CDR archive database files.	Remove or replace the CDR archive database files.
2008	Information	CDR service <starting or stopping>	Used to record service start/stop events.	No action.

13.15 Workgroup Server

Event Codes: Workgroup Server lists and describes event codes for workgroup server.

Table 66: Event Codes: Workgroup Server

ID	Severity level	Message	Cause	Action
1600	Information	WorkgroupServer Started.	Workgroup server started.	No action.
1604	Information	WorkgroupServer Stopping.	The workgroup server is stopping.	No action if server was stopped intentionally. Otherwise, review the WG*.log and SC*.log to identify reason for stoppage.

13.16 CSIS

Event Codes: CSIS lists and describes event codes for CSIS.

Table 67: Event Codes: CSIS

ID	Severity Level	Message	Cause	Action
1898	Information	CSIS Web Services starting.	;	No action.
1899	Error	CSIS Web Services failed to start (<error code>).	CSIS Web services failed to start. ; (The embedded error code is a Microsoft error code.)	Contact Mitel Technical Support and be prepared to provide the CSIS log for review.
2400	Information	CSIS Web Services stopping.	CSIS Web services are stopping. (Occurs when web services are stopped.)	No action.

ID	Severity Level	Message	Cause	Action
2401	Error	CSIS Web Services contained an error (<error code>).	CSIS Web services experienced a non-fatal error. (The embedded error code is a CSIS or Microsoft error code.)	Contact Mitel Technical Support and be prepared to provide the CSIS log for review. ;
2402	Information	User <username> at Workstation <workstation name> authenticated.	The specified user is authenticated for CSIS server access.	No action.
2403	Information	User <username> at Workstation <workstation name> authentication revoked <reason>.	The specified user is no longer authorized for CSIS server access. ; Causes include client logout, or an inactive connection as the result of a client going offline without logging out.	No action.
2405	Information	CSIS Web Services execution enabled.	CSIS Service started. Client access to CSIS Services is enabled.	No action.

ID	Severity Level	Message	Cause	Action
2406	Warning	CSIS Web Services execution disabled.	CSIS Service stopped. Client access to CSIS Services is disabled. (Web services continue to run.)	No action. The event is assigned a severity level of “warning”, because a service (CSIS) is disabled and no longer accept logins or requests. But the result is “non-destructive”; the service can be enabled at any time.

13.17 IP Phone Configuration Service (IPCS)

Event Codes: IP Phone Configuration Service (IPCS) lists and describes event codes for IPCS.

Table 68: Event Codes: IP Phone Configuration Service (IPCS)

ID	Severity Level	Message	Cause	Action
2700	Information	IPCS Server started.	IPCS Server started.	No action.
2701	Error	Handler not installed.	The service was not installed properly.	Re-install the service.
2702	Information	The IPCS Server Stopped.	IPCS Server stopped.	No action.
2703	Warning	Spare fail-over to site Headquarters in zero second(s).	Switch outage.	For information about outages, review Director.
2704	Warning	Spare HQ220 from site Headquarters fail-over to site Headquarters.	Switch outage.	For information on outages, review Director.

ID	Severity Level	Message	Cause	Action
2705	Warning	Spare HQ220 fail-back from site Headquarters to home Headquarters.	Switch outage, fail-back.	For information on outages, review Director.
2706	Information	IP-Phone was unable to be configured. No IP Phone switches are configured on Site: <site name>.	No switches are configured to support IP phones at the destination site.	To support more IP phones, configure a new switch, or add additional IP ports to existing switches.
2707	Information	IP Address for IP-Phone Device: <MAC address of phone> is set to NULL in the configuration database.	The IP address for a “downed” IP phone is set to NULL. This usually indicates that a new IP phone appeared on the system using the same IP address as the phone that is “down”.	No action.
2708	Error	IP-Phone could not be configured. No switches are available on Site: <variable> _Headquarters. The existing switch(es) have reached maximum capacity or may temporarily be down.	;	Check switch status and address any issues.

ID	Severity Level	Message	Cause	Action
2709	Error	IP-Phone could not be configured. No IP Phone switches are configured on Site: <variable> _Headquarters.	;	;
2710	Error	The IP Address for IP-Phone Device: <MAC address of phone> has been set to NULL in the configuration database because another IP Phone has contacted the system with the IP address that had been assigned to the device. The IP Phone with the IP Address now set to NULL is currently not communicating with the server. If communication is reestablished the configuration database will be updated with the device's current IP Address.	;	;
2711	Error	The IP-Phone Device: <MAC address of phone> could not be configured since another IP Phone device is using the same IP Address.	The IP address assigned to an IP phone is already in use by another IP phone. The new phone cannot be configured.	Troubleshoot the DHCP server to determine why it is assigning the same IP address to two different phones.

ID	Severity Level	Message	Cause	Action
2712	Error	The IP-Phone Device: <MAC address of phone> could not be configured since the IP Phone is using an IP Address that is not allowed.	;	;
2713	Information	The IP-Phone Device: <MAC address of phone> has been updated to be managed by Switch: <variable>.	;	No action.
2714	Warning	Too many pending IP phone registration requests. Restart SysMgrSvc to clean up the queue.	;	Restart the SysMgrSvc service.
2715	Warning	LDVS failover from Failed <variable> to Spare <variable> initiated.	;	No action.
2716	Warning	LDVS failover from Failed <variable> to Spare <variable> completed.	;	No action.
2717	Warning	LDVS failover from Failed <variable> to Spare <variable> failed.	;	;

13.18 ABC

Event Codes: ABC lists and describes event codes for ABC.

Table 69: Event Codes: ABC

ID	Severity Level	Message	Cause	Action
5100	Information	Authenticator <version number> has started successfully.	The specified version of Authenticator started.	No action.
5101	Information	;Authenticator has been stopped.	;Authenticator stopped.	No action.
5103	Warning	An authentication attempt by user <user ID>, using Mitel credentials, failed with status code <status code>.	A user attempted to authenticate using an invalid user ID, password or expired password.	Contact and assist the user with login information.
5104	Information	The user <user ID> authenticated successfully using network credentials.	User ID and password authentication is successful.	No action.
5105	Warning	An authentication attempt by user <user ID>, using network credentials, failed with status code <status code>.	A user attempted to authenticate using an invalid user ID, password, or expired password.	Contact and assist the user with login information.
5106	Information	An entity authenticated successfully using a client certificate issued to <phone MAC address>.	Phone authentication is successful.	No action.

ID	Severity Level	Message	Cause	Action
5107	Warning	An authentication attempt by an entity using a client certificate issued to <phone MAC address> failed with status code <status code>.	Unsuccessful authentication by a phone, or an intrusion attempt.	If a phone fails to register with the system or cannot be assigned to a user after power-cycling the phone, contact Mitel Technical Support.
5108	Information	A ticket issued to <user ID> was successfully renewed.	An application is successful in getting a new ticket when the old one expires.	No action.
5109	Warning	An attempt to renew a ticket issued to <user ID> failed with status code <status code>.	A user attempted to renew a ticket using an invalid user ID, password, or an expired password.	Contact and assist the user with login information.
5110	Warning	An attempt to renew an unrecognized ticket failed with status code <status code>.	A user attempted to renew a ticket using an invalid user ID, password, or an expired password.	Contact and assist the user with login information.
5111	Warning	A malformed authentication request <HTTP request> was received.	This may be due to an intrusion attempt.	If the client application continues to fail, contact Mitel Technical Support. Otherwise, block the source IP address of the HTTP request.

ID	Severity Level	Message	Cause	Action
5112	Warning	A request <HTTP request> was received through HTTP and is allowed only through HTTPS.	The client application does not use HTTPS when the system is configured for secure client access.	If the client application continues to fail, contact Mitel Technical Support.
5113	Information	An entity authenticated successfully as the trusted server application with ID <trusted server ID>.	An application, such as Conferencing, received an authentication ticket.	No action.
5114	Warning	An authentication attempt by an entity claiming to be a trusted server application <trusted server ID> failed with status code <status code>.	An application, such as Conferencing, failed to receive an authentication ticket.	Contact Mitel Technical Support.
5200	Information	Bootstrapper <version number> has started successfully.	The specified version of Bootstrapper started.	No action.
5201	Information	Bootstrapper has been stopped.	Bootstrapper stopped.	No action.

13.19 Edge Gateway

Event Codes: Edge Gateway lists and describes event codes for Edge Gateway.

Table 70: Event Codes: Edge Gateway

ID	Severity Level	Message	Cause	Action
5600	Information	EdgeGW <EGW host name>: <service name> is running.	<service name> is started and running.	No Action.
5601	Information	EdgeGW <EGW host name>: <service name> is stopped.	<service name> is stopped.	No Action.
5602	Information	EdgeGW <EGW host name>: Restart command is received.	Admin applied restart command through Connect Director.	EGW service will restart.
5603	Information	EdgeGW <EGW host name>: Reboot command is received.	Admin applied reboot command through Connect Director.	1. EGW check version again HQ/Linux DVS. If version mismatch, it will download new image and install automatically. 2. Reboot EGW machine.
5604	Information	EdgeGW <EGW host name>: Upgrade command is received.	Admin applied upgrade command through Director.	EGW download image for HQ/Linux DVS, install the image and reboot. Note: It does not check version in this command. It's supposed to be used for diagnostic purpose.
5605	Information	EdgeGW <EGW host name>: Download image from <FTP server IP address>.	EGW starts to download image when it receives the reboot or the upgrade command under version mismatch.	Download image from HQ/Linux DVS server.

ID	Severity Level	Message	Cause	Action
5606	Information	EdgeGW <EGW host name>: Install new image.	EGW starts the new image installation after download.	Start to installs new image.
5607	Information	EdgeGW <EGW host name>: Upgrade completed.	EGW completed upgrading to new image.	Complete installing new image.
5608	Error	EdgeGW <EGW host name>: Upgrade abort. Please check more details in egwds.log.	EGW failed to upgrade to new image.	Write error message to log file and quit current upgrading task.
5609	Warning	EdgeGW <EGW host name>: Second TMS connection attempt from <IP address>.	EGW is already connected with HQ/Linux DVS server, but another HQ/Linux DVS server tries to connect with it.	Reject the new connect request.
5610	Error	EdgeGW <EGW host name>: Internal diag: <internal diagnostic messages >.	Non-fatal internal error happened.	This is a diagnostic message to be used by TS and engineers.

ID	Severity Level	Message	Cause	Action
5611	Error	EdgeGW <EGW host name>: <service name> IP address <IP address> is invalid.	Admin input incorrect RAST IP address, TURN IP address, Reverse Proxy IP address, or Gateway in Connect Director->Administration->Appliances/ Servers->Platform Equipment->General page of EGW configuration.	Reject the incorrect IP address and send event to administrator.
5612	Error	EdgeGW <EGW host name>: Network mask length <number> is invalid.	Admin input incorrect Subnet mask in Connect Director->Administration->Appliances/ Servers->Platform Equipment->General page of EGW configuration.	Reject the incorrect subnet mask and send event to administrator.
5613	Warning	EdgeGW <EGW host name>: Connect client FQDN is invalid. Disable RP service for it.	Admin input incorrect Connect client FQDN in Connect Director->Administration->Appliances/ Servers->Platform Equipment->REVERSE PROXY page of EGW configuration.	Reject the incorrect FQDN and send event to administrator.

ID	Severity Level	Message	Cause	Action
5614	Warning	EdgeGW <EGW host name>: Collaboration FQDN is invalid. Disable RP service for it.	Admin input incorrect Collaboration FQDN in Director->Administration->Appliances/ Servers->Platform Equipment->REVERSE PROXY page of EGW configuration.	Reject the incorrect FQDN and send event to administrator.
5615	Warning	EdgeGW <EGW host name>: ECC FQDN is invalid. Disable RP service for it.	Admin input incorrect Contact Center FQDN in Director->Administration->Appliances/ Servers->Platform Equipment->REVERSE PROXY page of EGW configuration.	Reject the incorrect FQDN and send event to administrator.

13.20 Offline Migration

Event Codes: Offline Migration lists and describes event codes for Offline Migration.

Table 71: Event Codes: Offline Migration

ID	Severity Level	Message	Cause	Action
5400	Information	Message CDR Migration has started.	The CDR Offline data migration service has started.	No Action.

ID	Severity Level	Message	Cause	Action
5401	Information	CDR Migration has stopped.	The CDR Offline data migration service has stopped.	No Action.
5402	Error	CDR Migration halted due to error. <Error Message>.	An error has occurred while migrating CDR data.	Contact Mitel technical support with the error message and log files.
5403	Information	CDR Migration has completed.	The CDR Offline data migration completed.	No Action.
5404	Information	DM Migration has started.	The DM Offline data migration service has started.	No Action.
5405	Information	DM Migration has stopped.	The DM Offline data migration service has stopped.	No Action.
5406	Error	DM Migration halted due to error. <Error Message>.	An error has occurred while migrating DM data.	Contact Mitel technical support with the error message and log files.
5407	Information	DM Migration has completed.	The DM Offline data migration completed.	No Action.

13.21 IP Phone Display Server (IPDS)

IP Phone Display Server (IPDS) lists and describes event codes for IPDS.

Table 72: IP Phone Display Server (IPDS)

ID	Severity Level	Message	Cause	Action
2800	Information	The IP Phone Display Service (Version x.x.xxxx.x) started successfully.	IPDS service started.	No action.
2801	Information	The IP Phone Display Service stopped.	;IPDS service stopped.	No action.
2802	Error	The IP Phone Display Service (Version x.x.xxxx.x) encountered a fatal error during startup; the service is terminated.	The IPDS service crashed upon startup. (This is a fatal condition.)	Contact Mitel Technical Support and be prepared to provide server logs.
2803	Warning	An unexpected service control message <Message ID as hexadecimal integer> was encountered.	The Win32 Service Control Manager reports an unexpected message. The IPDS installation was probably modified manually by the user.	Contact Mitel Technical Support and be prepared to provide server logs.

ID	Severity Level	Message	Cause	Action
2804	Warning	An unexpected exception was encountered and handled. Exception description <Description here>.	An exception occurred and was handled by the logging of the error. Typically, one or more of the phones are displaying anomalies; a display update may not have been sent or a phone display is out of sync.	Contact Mitel Technical Support and be prepared to provide server logs. If users are experiencing problems, perform an administrative restart on the phones.
2805	Error	An unhandled exception was encountered. ;Exception description: <Description here>.	An exception occurred, but was not handled.	Immediately notify all IP phone users and restart IPDS to restore normal service. (Use the Send Diagnostic Message to dispatch a message to all phone displays.) Contact Mitel Technical Support and be prepared to provide server logs.
2806	Warning	The following warning condition was encountered in the IP Phone Display Service: <Warning description>.	A general error message that can indicate minor user problems. Usually the result of a non-fatal TAPI error.	Contact Mitel Technical Support and be prepared to provide server logs.
2807	Error	The following error condition was encountered in the IP Phone Display Service: <Error Description>.	A general error message that can accompany extensive user problems. Usually the result of a fatal TAPI error.	Contact Mitel Technical Support and be prepared to provide server logs. Perform other diagnostics at your discretion.

ID	Severity Level	Message	Cause	Action
2808	Information	The phone display was reinitialized because of an administrative request: Extension: <Extension number>.	An administrator reset the display on the phone at the specified extension.	No action.
2809	Information	The phone display was reinitialized because of an administrative request: Port ID: <Port ID>.	An administrator reset the display on the phone configured for the specified port.	No action.
2810	Information	All phone displays were reinitialized because of an administrative request.	An administrator reset the display on all IP phones.	No action.
2811	Information	The phone display was reinitialized because of an administrative request: IP Address <IP address>.	An administrator reset the display on the phone having the specified IP address.	No action.

ID	Severity Level	Message	Cause	Action
2812	Warning	The IP Phone Display service encountered an apparent crash in the Microsoft Telephony Service. IPDS attempts to recover from this problem. If users report anomalous behavior, stop and restart the Microsoft Telephony Service and all services that depend on it.	Fault in Microsoft Telephony Service; there is potential to recover automatically.	Watch for anomalous behavior. Restart the following if problems persist: • TMS • IPDS • Workgroup • All Voice Mail Services
2813	Error	The IP Phone Display service was unable to recover from an apparent crash in the Microsoft Telephony Service. Stop and restart the Microsoft Telephony Service and all services that depend on it.	Fault in Microsoft Telephony Service; there is no potential to recover automatically.	Restart the following if problems persist: • TMS • IPDS • Workgroup • All Voice Mail Services
2814	Warning	The following config option was set to a value that is only intended for engineering use: <option name>.	An administrator set a debug flag in the registry that was only intended for use by engineers.	Unset the option listed in the event message.

ID	Severity Level	Message	Cause	Action
2815	Warning	The IP Phone display service is unable to connect to the database. It retries in 30 seconds. <error code that was encountered>	IPDS was unable to access the database upon startup. It tries again in 30 seconds. No action needs to be taken at this time.	Also see 2816 and 2817.
2816	Error	The IP Phone display service is unable to connect to the database. It continues to retry once every minute.<error code that was encountered>	This only happens 30 seconds after a 2815 error, in the event that the retry for 2815 failed. At this point, the most common cause is that the most recent installation or upgrade on the server where the even t is generated did not properly register the database access libraries.	If recovery is not possible (see error 2817), contact Mitel Technical Support.
2817	Information	The IP Phone display service's connection to the database recovered from the previous error.	A database retry after 2815/1816 errors was successful and the situation was recovered from.	No action.

ID	Severity Level	Message	Cause	Action
2818	Error	The database is missing a table or stored procedure needed to run the following stored procedure: (name if query). This causes degraded functionality in IPDS. Ensure that the HQ server and all Remote servers are running the same version of software.	Database file corrupted, or a query removed or otherwise inaccessible at this time.	Call Mitel Technical Support.

13.22 CMCA

Event Codes: CMCA lists and describes event codes for CMCA.

Table 73: Event Codes: CMCA

ID	Severity Level	Message	Cause	Action
4400	Warning	Conferencing audio license near max capacity.	Occurs when 80% or more of the audio licenses are in use.	Go to licenses tab in Director and add extra licenses that are required and configure.
4401	Warning	Conferencing audio license max capacity.	Occurs when audio license have already reached the maximum capacity.	Go to licenses tab in Director and add extra licenses that are required and configure.

ID	Severity Level	Message	Cause	Action
4402	Informational	Conferencing CMCA started.	Occurs when CMCA service is started or restarted on UCB.	No action.
4403	Informational	Conferencing CMCA has stopped.	Occurs when CMCA service is stopped on UCB.	No action.
4404	Warning	Conferencing CMCA approaching full disk capacity. Certain operations like recording and library upload failed.	Occurs when the CMCA was unable to finish the recording or able to upload the library because the disk capacity is full.	To free up the disk space on UCB by deleting some recordings or free up logs from `/cf/shorelinedata/logs`.
4405	Warning	Conferencing web license near max capacity.	Occurs when 80% or more of the web licenses are in use.	Go to licenses tab in Director and add extra web conferencing licenses that are required and configure.
4406	Warning	Conferencing web license reached max capacity.	Occurs if web license have already reached the maximum capacity.	Go to licenses tab in Director and add extra licenses that are required and configure.
4407	Warning	Conferencing HTTPS disabled.	HTTPS is disabled for the UCB in Director.	Go to appliances in Director and check if HTTPS is enabled for the respective UCB, if not enable it.

ID	Severity Level	Message	Cause	Action
4408	Error	Conferencing exchange connector failed because the Exchange UserID and/or Password set in Director is incorrect.	Occurs if the credentials entered for exchange connector in the Director are wrong.	Go to system parameters in Director and make sure the credentials entered is correct and connection is successful.
4410	Informational	Conferencing Exchange Connector started successfully.	Occurs when exchange connector is started.	No action.
4411	Informational	Conferencing exchange connector stopped.	Occurs when exchange connector is stopped.	No action.
4414	Error	Conferencing audio port usage reached maximum capacity.	Occurs when audio port usage on the UCB is maximum.	Verify the usage of the ports by performing the following tasks in Director: • Navigate to **Maintenance** > **Status and Maintenance** > **Audio/Web Conferencing** and check the peak and current usage of the audio and web ports. • Navigate to **Maintenance** > **Status and Maintenance** > **Appliances** and check the ports that are free and the ports that are in use. If all the ports are in use for web or audio, the system might not have enough conferencing resources for the current load levels. Therefore, you may need to add additional conferencing devices to the system. When there are no ongoing meetings and if the **Maintenance** page still shows the devices are in use, contact Mitel Technical Support for assistance before you restart the device.

ID	Severity Level	Message	Cause	Action
4415	Error	Conferencing web port usage reached maximum capacity.	Occurs when web port usage on the UCB is maximum.	Verify the usage of the ports by performing the following tasks in Director: • Navigate to **Maintenance** > **Status and Maintenance** > **Audio/Web Conferencing** and check the peak and current usage of the audio and web ports. • Navigate to **Maintenance** > **Status and Maintenance** > **Appliances** and check the ports that are free and the ports that are in use. If all the ports are in use for web or audio, the system might not have enough conferencing resources for the current load levels. Therefore, you may need to add additional conferencing devices to the system. When there are no ongoing meetings and if the **Maintenance** page still shows the devices are in use, contact Mitel Technical Support for assistance before you restart the device.

Appendix B - Alerts 14

This chapter contains the following sections:

This chapter includes information about Connect alerts.

14.1 Overview of Alerts

This appendix provides a comprehensive list of alerts organized by category. These alerts are a valuable resource for understanding events reported by the Mitel system.

Alerts identify system issues by correlating events that occur in the Mitel system. The data for these correlations comes from the Windows event log, the Monitoring Database and an internal database that keeps track of status information on sites and switches.

Alerts are available for the following aspects of the Mitel system:

- Bandwidth
- Connections
- Servers
- Switches
- Trunk Groups
- Voice Quality

The tables in this appendix provide a structured view of alerts displayed in the Diagnostics and Monitoring web application. Each alert includes a severity level, ID number, description text, possible causes, suggested courses of action (if any), and whether the alert clears automatically or must be cleared manually.

For information about monitoring alerts using the Diagnostics & Monitoring system in Connect Director, see the *MiVoice Connect System Administration Guide*.

Each alert is assigned a level of severity. Severity Levels of Alerts describes the three severity levels.

Table 74: Severity Levels of Alerts

Severity Level	Explanation
Information	Indicates normal operation, or a transition between normal operating states Typically, no action is required.
Warning	Reports an exception to normal operations that might need to be monitored
Critical	Reports a failure or an impending failure (for example, when a service or hardware component is disabled) that requires immediate response and resolution

14.2 Bandwidth Alerts

Bandwidth Alerts describes the alerts related to bandwidth. Messages are listed alphabetically within each severity level.

Table 75: Bandwidth Alerts

Severity Level	Description	Cause	Action and Clearing Status
Critical	Bandwidth utilization critical threshold has been exceeded.	A site has reported a bandwidth utilization percentage above the accepted threshold. High bandwidth utilization could result from excessive network activity because of high call volume or some other cause. High bandwidth utilization could also mean that there is simply not enough network bandwidth for the site.	Monitor the (outbound) call volume and trunk utilization within the site to determine if there could be a correlation between the number of calls and the bandwidth usage. This alert clears automatically when the bandwidth utilization percentage for the site sustains a level below the critical threshold for 3 minutes. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.

Severity Level	Description	Cause	Action and Clearing Status
Warning	Bandwidth utilization warning threshold has been exceeded.	A site has reported a bandwidth utilization percentage above the accepted threshold. High bandwidth utilization could result from excessive network activity because of high call volume or some other cause. High bandwidth utilization could also mean that there is simply not enough network bandwidth for the site.	Monitor the (outbound) call volume and trunk utilization within the site to determine if there could be a correlation between the number of calls and the bandwidth usage. This alert clears automatically when the bandwidth utilization percentage for the site sustains a level below the threshold for 3 minutes. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.
Warning	Switch is experiencing low bandwidth.	The switch has reported that it does not have sufficient bandwidth to initiate an intersite call.	Increase the amount of intersite bandwidth or decrease the amount of call traffic between the two sites that are experiencing the issue. This alert clears automatically when the bandwidth utilization percentage for the target site increases or decreases. A decrease in the percentage of bandwidth utilization represents a decrease in call traffic or an increase in configured intersite bandwidth. An increase in the percentage of bandwidth utilization indicates that an intersite call was successfully established since the alert was generated.

14.3 Connection Alerts

Connection Alerts lists and describes the alerts related to connections. Messages are listed alphabetically within each severity level.

Table 76: Connection Alerts

Severity Level	Description	Cause	Action and Clearing Status
Critical	Switch has lost connection to the network.	The switch's managing server cannot communicate with the switch.	Ensure that the switch is running and is connected to the network. If you manually restarted the switch, you can ignore this alert, as it was generated while the switch was restarting. This alert clears automatically after the switch is running and connected to the network. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.
Information	IP phones are having DHCP issues with IP addresses.	The phone is having issues related to its IP address.	Review the events associated with the alert, and take corrective action as appropriate. After correcting the switch configuration, you must clear this alert manually. Otherwise, the system deletes the alert according to the parameters set for purging and reclaiming space used for alerts in the shoreware monitoring database. (The default is three days.) Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.

14.4 Server Alerts

Server Alertsdescribes the alert related to servers.

Table 77: Server Alerts

Severity Level	Description	Cause	Action and Clearing Status
Warning	TMS has detected invalid Director configurations.	The server is having issues with its current IP address, which could be due to a configuration issue.	Review the associated events and determine appropriate configuration changes. After resolving the configuration issue, you must clear the alert manually. Otherwise, the system deletes the alert according to the parameters set for purging and reclaiming space used for alerts in the shoreware monitoring database. (The default is three days.) Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.

14.5 Switch Alerts

Switch Alerts describes the alerts related to switches. Messages are listed alphabetically within each severity level.

Table 78: Switch Alerts

Severity Level	Description	Cause	Action and Clearing Status
Warning	Invalid switch configurations detected.	The switch has been configured with a characteristic that does not match what the switch is reporting.	Review the events associated to the alert, and modify the configuration of the switch as appropriate. After correcting the configuration issue, you must clear this alert manually. Otherwise, the system deletes the alert according to the parameters set for purging and reclaiming space used for alerts in the shoreware monitoring database. (The default is three days.)

Severity Level	Description	Cause	Action and Clearing Status
Warning	Possible switch firmware corruption.	The switch has failed in an attempt to upgrade its firmware and has resorted to an alternate booting method.	Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. After resolving the switch issue so that the switch boots normally, you must clear this alert manually.
Warning	Switch core is operating at an unsafe temperature.	The switch is operating at a temperature level that is over the switch's threshold.	Ensure that the switch is running in a temperature-friendly environment. This alert clears automatically if the switch's temperature returns to normal. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.
Warning	Switch is experiencing issues with its trunks.	A trunk on the switch is experiencing unexpected behaviors.	Review the events associated with the alert. If the identified trunk is causing issues in the system, restart the switch. This alert clears automatically when the trunk re-establishes expected behavior and is back in service, or when the switch is restarted. However, if this alert was generated because you intentionally forced all ports on a switch to the "Unavailable" state, you can manually clear this alert. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists.
Warning	Switch is experiencing issues with the fan.	The fan on the switch is having trouble running and may be too old.	The fan or switch may need to be replaced. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears automatically if the fan begins running at normal speed.

Severity Level	Description	Cause	Action and Clearing Status
Warning	Switch is experiencing issues with the power supply.	The switch is experiencing unexpected power failures.	Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears automatically if the voltage level of the switch returns to normal.
Warning	Switch is experiencing memory issues.	The memory on the switch may be corrupt, or an invalid memory access may have occurred.	Restart the switch. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears automatically after the switch is restarted.
Warning	Switch is having firmware upgrade issues.	The switch has failed in an attempt to upgrade its firmware. This could be a result of a disconnection between the switch and its managing server.	Ensure that the managing server is connected to the network and that the managing server can communicate with the switch. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears automatically when the firmware upgrade is successful.
Warning	Switches have reached maximum capacity of IP phones.	No ports allocated for IP phones are available on any of the available switches.	Reserve a port on a switch for an IP phone, or if no ports can be reserved add a switch to the system. Refer to the *MiVoice Connect System Administration Guide* or contact Mitel Technical Support for assistance. After making the necessary configuration changes (reserving a port for the phone or assigning the phone to a switch that has adequate port capacity for additional phones), you must clear this alert manually. Otherwise, the system deletes the alert according to the parameters set for purging and reclaiming space used for alerts in the shoreware monitoring database. (The default is three days.)

Severity Level	Description	Cause	Action and Clearing Status
Warning	The switch is not running a sufficient firmware version.	The switch is running a firmware version that is not compatible with the version of the PBX. This is typically encountered during an upgrade, because after the Headquarters server is upgraded switches require an updated firmware version.	Restart the switch to initiate a firmware upgrade. This alert clears automatically when the firmware upgrade has completed.
Warning	TMS has detected invalid switch configurations.	The switch is having issues that are related to its IP address.	Review the events associated with the alert, and take corrective action as appropriate. If necessary, contact Mitel Technical Support for assistance. If the switch is restarted, the alert clears automatically. Otherwise, after taking corrective action, you must clear the alert manually.

14.6 Trunk Group Alerts

Trunk Group Alerts describes the alerts related to trunk groups. Messages are listed alphabetically within each severity level.

Table 79: Trunk Group Alerts

Severity Level	Description	Cause	Action and Clearing Status
Critical	Trunk occupancy critical threshold has been exceeded.	A trunk on a switch is being used for a high volume of calls. This situation could occur for either of the following reasons: • An insufficient number of ports are allocated for use as trunks. • Outbound call volume is high.	Allocating more ports on the switch for trunk usage will more evenly distribute the trunk utilization load. Refer to the *MiVoice Connect System Administration Guide* for more information, or contact Mitel Technical Support for assistance. This alert clears automatically when the trunk utilization percentage on the switch has sustained a level below the critical threshold for 3 minutes.
Warning	Switch is experiencing issues with its trunks.	A trunk on the switch is experiencing unexpected behaviors.	Review the events associated to the alert. If the identified trunk is causing issues in the system, restart the switch. Contact Mitel Technical Support for further assistance. This alert clears automatically when the trunk reestablishes expected behavior and is back in service, or when the switch is restarted.
Warning	Trunk occupancy warning threshold has been exceeded.	A trunk on a switch is being used for a high volume of calls. This situation could occur for either of the following reasons: • An insufficient number of ports are allocated for use as trunks. • Outbound call volume is high.	Allocating more ports on the switch for trunk usage will more evenly distribute the trunk utilization load. Refer to the *MiVoice Connect System Administration Guide* for more information, or contact Mitel Technical Support for assistance. This alert clears automatically when the trunk utilization percentage on the switch has sustained a level below the warning threshold for 3 minutes.

14.7 Voice Quality Alerts

Voice Quality Alerts describes the alerts related to voice quality. Messages are listed alphabetically within each severity level.

Table 80: Voice Quality Alerts

Severity Level	Description	Cause	Action and Clearing Status
Critical	Call quality critical threshold has been exceeded.	A stream within a call occurring over a switch has been identified as having poor voice quality (“bad call”).	Monitor the calls on the switch and any alerts from the same switch that could be related. If the issue consistently occurs or a possible issue is identified, collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. Assuming that no “bad” calls occur over the switch, this alert clears automatically 3 minutes after a “good” call occurs. (A “good” call is one in which all streams of the call are identified as having good voice quality.)
Warning	Call Quality warning threshold has been exceeded.	A stream within a call occurring over a switch has been identified as having poor voice quality (“bad call”).	Monitor the calls on the switch and identify any alerts from the same switch that could be related. If the issue occurs consistently or a possible issue is identified, collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. Assuming that no “bad” calls occur over the switch, this alert clears automatically 3 minutes after a “good” call occurs. (A “good” call is one in which all streams of the call are identified as having good voice quality.)
Warning	Switch DSP is reaching its limit.	The switch has reported that its digital signal process is experiencing issues.	Restart the switch. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears when the switch is restarted.

Severity Level	Description	Cause	Action and Clearing Status
Warning	Switch is experiencing issues with echo cancellation.	The switch has reported that its echo-suppression software is experiencing issues.	Restart the switch. Collect all necessary logs and screen shots before contacting the Mitel Technical Support for further assistance if the problem persists. This alert clears automatically when the switch reports that its echo-suppression software has been corrected or when the switch is restarted.

Appendix C - DCOM Permissions 15

This chapter contains the following sections:

This chapter contains an overview of DCOM permissions.

15.1 Overview

Mitel systems have one HQ server and multiple remote servers. Applications running on remote servers access data service components residing on the HQ server through Distributed Component Object Model (DCOM). DCOM permissions are configured by the Installer when the servers are installed and by the SP1Repair command line utility.

The following service logon accounts are available in Windows:

- Local System account: This account includes full system access, including the directory service on domain controllers. Services logged onto the Local System account on domain controllers can access the entire domain. Some services log onto the Local System account by default. Do not change default service settings.
- Local Service account: This account is similar to authenticated user accounts. Services logged onto the Local Service account have the same access rights as members of the Users group and access network resources as null sessions with no credentials.
- Network Service account: This account is similar to authenticated user accounts. Services logged onto this account have the same access rights as members of the Users group and access network resources through the credentials of the computer account.

15.2 Editing DCOM Permissions

You can modify DCOM permissions on the HQ system by using the procedures in the following sections.

15.2.1 My Computer Properties

1. Open the **My Computer Properties** panel by selecting **MMC** > **Component Services** > **Computers** > **My Computer** > **Properties**.
2. Open the **Default Properties** panel, and select **Enable DCOM**.

3. Open the **COM Security** panel:

   a. Click **Edit Default** in the **Access Permissions** section and select the following permissions:

   - **SELF:** Local Access – allow; Remote Access – allow
   - **SYSTEM:** Local Access – allow; Remote Access – no selection.

   Return to the **My Computer Properties** window by clicking **OK**.

   b. Click **Edit Default** in the **Launch and Activation Permissions** section and select the following permissions:

   - **Administrators:** Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
   - **INTERACTIVE:** Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
   - **SYSTEM:** Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow

15.2.2 TriggerServer Properties

1. Open the **TriggerServer Properties** window by selecting **MMC** > **Component Services** > **Computers** > **My Computer** > **DCOM Config** > **Trigger Server** > **Properties**.
2. Open the **General** panel, and set **Authentication** level to **Default**.
3. Open the **Location** panel, and select **Run application on this computer**.
4. Open the **Security panel**

   a. Click **Edit** in the **Launch and Activation Permissions** section and select the following permissions:

   - **Administrators:** Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
   - **ANONYMOUS LOGON:** Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow
   - **SYSTEM:** Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow

   Return to the **TriggerServer Properties: Security** panel by clicking **OK**.

   b. Click **Edit** in the **Configuration Permissions** section and select the following permissions:

   - **Administrators:** Full Control – allow; Read – allow
   - **SYSTEM GROUP:** Full Control – allow; Read – allow
   - **CREATOR OWNER:** Full Control – no selection; Read – no selection
   - **other Users:** Full Control – no selection; Read – allow

5. Open the **Identity** panel and select **The system account (services only)**.

15.2.3 ZinManager Properties

1. Open the **ZinManager Properties** window by selecting **MMC** > **Component Services** > **computers** > **My Computer** > **DCOM Config** > **ZinManager** > **Properties**.
2. Open the **General** panel, and set **Authentication** level to **Default**.
3. Open the **Location** panel, and select **Run application on this computer**.
4. Open the **Security** panel and complete the following steps:

   a. Click **Edit** in the **Launch and Activation Permissions** section and select the following permissions:

   - **Administrators:** Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow
   - **SYSTEM:** Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow

   Return to the **ZinManager Properties** window by clicking **OK**.

   b. Click **Edit** in the **Configuration Permissions** section. Select the following permissions:

   - **Administrators:** Full Control – allow; Read – allow
   - **CREATOR OWNER:** Full Control – no selection; Read – no selection
   - **SYSTEM:** Full Control – allow; Read – allow

   Return to the **ZinManager Properties** window by clicking **OK**.
5. Open the **Identity** panel, and select **The system account (services only)**.

Appendix D - Port Usage 16

This chapter contains the following sections:

- Port Usage Tables

This appendix contains port usage information.

16.1 Port Usage Tables

Devices Included in Parts 1, 2, and 3.

Table 81: Devices Included in Parts 1, 2, and 3

Originating Device	Destination Device
SG-Generation Switch	Destination Devices Shown in Part 1 (Port Usage — Part 1) • SG Switch • V- Switch and ST Switch • Service Appliance (Conferencing and IM) • IP Phone • MGCP Phone Destination Devices Shown in Part 2 (Port Usage — Part 2) • ECC Supervisor Client • Connect Mobility Client (CMC) • Connect Mobility Router (CMR) • D&M Server (Standalone) • Edge Gateway Destination Devices Shown in Part 3 (Port Usage — Part 3) • Connect Client Softphone • Connect Client for Web Softphone • Linux DVS • Windows DVS • Headquarters Server • Other
V-Switch & ST-Generation Switch	
Service Appliance (Conferencing and IM)	
IP Phone	
MGCP Phone	
Connect Client and Softphone	
Connect Client for Web and Softphone	
ECC Supervisor Client	
Linux DVS	

Originating Device	Destination Device
Windows DVS	
Headquarters Server	
Connect Mobility Client (CMC)	
Connect Mobility Router (CMR)	
D&M Server (Standalone)	
Edge Gateway	
Other (such as SIP endpoints)	

16.1.1 Port Usage Part 1

Port Usage — Part 1 contains the first part of the port usage information for the Connect system.

Table 82: Port Usage — Part 1

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Switch	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 2427 MGCP **Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255NA

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
V-Switch	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255 Transport: TCP 5432 – Xprt SMTP TCP 25 – SMTP	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 2427 MGCP **Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
V-Switch		**Transport:** TCP 5432 – Xprt **SMTP** TCP 25 – SMTP			
Service Appliance (Conferencing and IM)	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445– Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443– Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Call Control** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control **Media Stream** UDP 10000-20000 RTP (configurable)	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** ICMP 33434+255

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Service Appliance (Conferencing and IM)			**CMCA (Web Share)**: TCP/UDP 5450 Ping Sync TCP 80 HTTP Web share TCP 443 HTTPS Web share **Transport** TCP 5432 – Xprt **SMTP** TCP 25 – SMTP		
IP Phone	**Call Control** TCP 5061 SIPS **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Call Control** TCP 5061 SIPS **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Peer SW Update** TCP 80 HTTP **Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 10000-10550 RTP (configurable) **IP Path Trace** ICMP Traceroute

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
MGCP Phone	**Call Control** UDP 2727 MGCP **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Call Control** UDP 2727 MGCP **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 10000-10550 RTP (configurable) **IP Path Trace** ICMP Traceroute
Connect Client and Softphone	**Media Stream** UDP 10000-20000 RTP (configurable)	**Media Stream** UDP 10000-20000 RTP (configurable)	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP 33434+500	**Media Stream** UDP 10000-10550 SRTP	**Media Stream** UDP 10000-10550 RTP

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Linux DVS	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: UDP 5458 SUNRPC Broadcast	**Call Control** TMS RPC: UDP 5458 SUNRPC Broadcast	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Linux DVS	**Call Control** UDP 2427 MGCP – Media proxy UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC NCC commands UDP 5453 – Broadcasts	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC/ NCC commands UDP 5453 - Broadcasts **Transport** TCP 5432 – CDS	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC/ NCC commands UDP 5453 – Broadcasts **Transport** TCP 5432 – CDS		

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Linux DVS	**Configuration Control (for VxWorks switches Only)** TCP 1024-65535 – Firmware download (Burn flash) **WSS call control (MGCP)** TCP 2727 – WSS to switch **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**WSS call control (MGCP)** TCP 2727 – WSS to switch **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**IP Path Trace** UDP 33434+255 **CAS-XMPP** TCP 5222 – XMPP/TLS		

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Windows DVS	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: UDP 5458 SUNRPC Broadcast	**Call Control** TMS RPC: UDP 5458 SUNRPC Broadcast	**Media Stream** UDP 10000-10128 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Windows DVS	**Call Control** UDP 2427 MGCP – Media proxy UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC NCC commands UDP 5453 – Broadcasts	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC/ NCC Commands UDP 5453 – Broadcasts **Transport** TCP 5432 – CDS	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC/ NCC Commands UDP 5453 – Broadcasts **Transport** TCP 5432 – CDS		

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Windows DVS	**Configuration Control (for VxWorks switches only)** TCP 1024-65535 – Firmware download (Burnflash) **WSS call control (MGCP)** TCP 2727 – WSS to switch **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**WSS call control (MGCP)** TCP 2727 – WSS to switch **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Transport** TCP 5432 – CDS **IP Path Trace** UDP 33434+255		

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Headquarters Server	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: UDP 5458 SUNRPC Broadcast	**Call Control** TMS RPC UDP 5458 SUNRPC Broadcast	**Media Stream** UDP 10000-10128 RTP (configurable) **SoftSwitch** **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Headquarters Server	**Call Control** UDP 2427 MGCP – Media proxy UDP 5440 - Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC NCC commands UDP 5453 – Broadcasts	**Soft Switch** UDP 2427 MGCP – Media proxy UDP 5440 - Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC NCC commands UDP 5453 – Broadcasts	**Soft Switch** UDP 2427 MGCP – Media proxy UDP 5440 - Location Service UDP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control TCP 5452 RPC NCC commands UDP 5453 – Broadcasts		

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Headquarters Server	**Configuration Control** TCP 1024-65535 – Firmware download. (Burnflash) **WSS call control (MGCP)** TCP 2727 – WSS to switch **Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Transport** TCP 5432 - CDS **Media Stream** UDP 10000-20000 RTP (configurable) **WSS call control (MGCP)** TCP 2727 – WSS to switch **IP Path Trace** UDP 33434+255	**Transport** TCP 5432 – CDS **IP Path Trace** UDP 33434+255		
Connect Mobility Client (CMC)	NA	NA	**Media Stream** UDP 10000-20000 RTP (configurable)	**Media Stream** UDP 10000-10128 RTP (configurable)	**Media Stream** UDP 10000-10128 RTP (configurable)

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Connect Mobility Router (CMR)	TCP 5061 - SIPS TCP/UDP 5060 – SIP **Media Stream** UDP 10000-20000 RTP (configurable)	TCP 5061 - SIPS TCP/UDP 5060 – SIP **Media Stream** UDP 10000-20000 RTP (configurable)	**Media Stream** UDP 10000-20000 RTP (configurable) **Instant Messaging** TCP 5222 – XMPP/TLS	**Media Stream** UDP 10000-10128 RTP (configurable)	**Media Stream** UDP 10000-10550 RTP (configurable)
DM Server (Standalone)	TCP 22 - SSH (RpCap Maintenance)	TCP 22 - SSH (RpCap Maintenance)	NA	TCP 22 - SSH (RpCap Maintenance)	NA
Edge Gateway	**TURN**: **Media Stream** UDP 10000-20000 RTP (configurable)	**TURN**: **Media Stream** UDP 10000-20000 RTP (configurable)	**TURN**: **Media Stream** UDP 10000-20000 RTP (configurable)	**TURN**: **Media Stream** UDP 10000-10128 RTP (configurable)	TBD
Other (such as SIP endpoints)	**SSH** TCP 22	**SSH** TCP 22	**SSH** TCP 22	**SH** TCP 22 **PAPI** TCP 8086	**Telnet** TCP 23

Originating Device	Destination Device				
	SG Switch	V-Switch ST Switch	Service Appliance (Conferencing and IM)	IP Phone MGCP Phone	
Button Box	NA	NA	NA	Port: 9000 **Note**: The 400-Series IP phones listen on this port for events from the BB-424 button box.	NA
Automation Server Port	NA	NA	NA	Port: 9005 **Note**: The 400-Series IP phones listen on this port for events from an automated testing server.	NA

16.1.2 Port Usage Part 2

Port Usage — Part 2 contains the second part of the port usage information for the Connect system.

Table 83: Port Usage — Part 2

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
Switch	NA	**Media Stream** UDP 42000-42100 RTP **P Path Trace** UDP 33434+255	**SIP Lines and Trunk** UDP/TCP 5060- SIP TCP 5061 - SIPS UDP - 50000 - 60000 – SIP Lines **Media Stream** UDP 15000-32000 **IP Path Trace** UDP 33434+255	UDP 5060 - SIP	**TURN** **Media Stream** UDP 10000-15000 SRTP (configurable) **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
V-Switch	NA	**Media Stream** UDP 42000-42100 RTP **IP Path Trace** UDP 33434+255	NA	NA	**TURN** **Media Stream** UDP 10000-15000 SRTP (configurable) **IP Path Trace** UDP 33434+255
Service Appliance (Conferencing and IM)	NA	**Media Stream** UDP 42000-42100 RTP **IP Path Trace** UDP 33434+255	**Media Stream** UDP 15000-32000 (RTP) **IP Path Trace** UDP 33434+255	UDP 5060 - SIP	**TURN** **Media Stream** UDP 10000-15000 RTP (configurable) **IP Path Trace** UDP 33434+255
IP Phone	NA	**Media Stream** UDP 42000-42100 RTP **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 15000-32000 (SRTP) **IP Path Trace** ICMP Traceroute	NA	**RAST (for OFF-NET phones)** TCP/UDP 443 – RAST (on external interface)

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
MGCP Phone	NA	**Media Stream** UDP 42000-42100 RTP **IP Path Trace** ICMP Traceroute	**Media Stream** UDP 15000-32000 (SRTP) **IP Path Trace** ICMP Traceroute	NA	**TURN** **Media Stream** UDP 10000-15000 RTP (configurable) **IP Path Trace** ICMP Traceroute
Connect Client and Softphone	NA	**Media Stream** UDP 42000-42100 RTP (configurable)	**Media Stream** UDP 15000-32000 (SRTP)	NA	**TURN** **Signaling** TCP/UDP 443 – STUN and Media **Media Stream** UDP 10000-15000 RTP (configurable) **Reverse Proxy** TCP 443 – HTTPS (Auth, Bootstrapper, CAS, Conferencing)

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
Connect Client for Web and Softphone	NA	NA	NA	NA	**TURN** **Signaling** TCP/UDP 443 – STUN & Media **Media Stream** UDP 10000-15000 RTP (configurable) **Reverse Proxy** TCP 443 - HTTPS (Auth, Bootstrapper, CAS, Conferencing)
ECC Supervisor Client	NA	NA	NA	NA	**HAProxy (not available yet)** **ECC Supervisor** TCP 31451-31452

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
CMC	NA	Video CMCP (Server) – TCP 5464 CMCP (Client) – TCP 5465 Media Stream UDP 42000-42100 RTP (configurable)	Call Control TCP 5061 - SIPS TCP/UDP 5060 – SIP Management TCP: 80 - http TCP: 443, 4433 – https RAST TCP/UDP 443 – RAST (on external interface) Media Stream UDP 15000-32000 RTP (configurable)	NA	NA

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
Linux DVS	NA	**Media Stream** UDP 42000-42100 RTP (configurable) IP Path Trace UDP 33434+255	**Media Stream** UDP 15000-32000 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**TURN:** **Media Stream** UDP 10000-15000 RTP (configurable) **WSS Media Control** UDP 2223 – NG Allocator **IP Path Trace** UDP 33434+255
Windows DVS	NA	**Media Stream** UDP 42000-42100 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 15000-32000 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**TURN**: **Media Stream** UDP 10000-15000 RTP (configurable) **WSS Media Control** UDP 2223 – NG Allocator **IP Path Trace** UDP 33434+255

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
Headquarters Server	NA	**Media Stream** UDP 42000-42100 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 15000-32000 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**TURN**: **Media Stream** UDP 10000-15000 RTP (configurable) **WSS Media Control** UDP 2223 - NG Allocator **IP Path Trace** UDP 33434+255
CMR	NA	**Call Control** TCP 5061 - SIPS TCP/UDP 5060 – SIP **Media Stream** UDP 42000-42100 RTP (configurable)	NA	NA	**TURN**: **Media stream** UDP 10000-20000 RTP (configurable)

Originating Device	Destination Device				
	ECC Supervisor Client	CMC	CMR	D&M Server (Standalone)	Edge Gateway
D&M Server (Standalone)	NA	NA	NA	**D&M Offline Upgrade - TRANSIENT** TCP 4312 - Old MySQL D&M	NA
Edge Gateway	NA	NA	**Media stream** UDP 10000-32000 RTP (configurable)	NA	**TURN**: **Media Stream** UDP 10000-20000 RTP (configurable)
Other (such as SIP) endpoints	NA	NA	**SSH** TCP 22	NA	NA

16.1.3 Port Usage Part 3

Port Usage — Part 3 contains the third part of the port usage information for the Connect system.

Table 84: Port Usage — Part 3

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Switch	**Media Stream** UDP10000-10550 RTP IP Path Trace UDP 33434+255	NA	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast TCP/UDP 5500-5600	**Configura-tion Control** UDP 162 SNMP TRAP **Call Control** UDP 5060 SIP **Media Stream** UDP 1024-65535 RTP – for SIP **IP Path Trace** ICMP 33434+255

Originating Device	**Destination Device**					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
Switch			**SoftSwitch** UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	**SoftSwitch** UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	**SoftSwitch** UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	
Switch			**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
V-Switch	**Media Stream** UDP10000-10550 RTP **IP Path Trace** UDP 33434+255	NA	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast	**Port Mapper** TCP 111 RPC Port Mapper UDP 111 RPC Port Mapper **Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast TCP/UDP 5500-5600	**Configuration Control** UDP 67 DHCP Server Maintenance UDP 162 SNMP TRAP **Call Control** UDP 5060 SIP Media Stream UDP 1024-65535 RTP – for SIP

Originating Device	**Destination Device**					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
V-Switch			**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5442 – DRS UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**IP Path Trace** ICMP 33434+255 SMTP TCP 25 – SMTP (third party for Virtual Machine notification)

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
V-Switch			**Database** TCP 4306 - MYSQLCC TCP 4308 – MYSQL config **Transport** TCP 5432 – Xprt **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	**Database** TCP 4306 - MYSQLCC TCP 4308 – MYSQL config **Transport** TCP 5432 – Xprt **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	**Database** TCP 4306 - MYSQLCC TCP 4308 – MYSQL config **Transport** TCP 5432 – Xprt **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files	
V-Switch			**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255 SMTP TCP 25 - SMTP	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255 SMTP TCP 25 - SMTP	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** UDP 33434+255 SMTP TCP 25 - SMTP	

Originating Device	Destination Device					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
Service Appliance (Conferencing and IM)	**Media Stream** UDP10000-10550 RTP **IP Path Trace** UDP 33434+255	Browser determined d ynamic port (WebRTC)	**Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast **SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5442 – DRS UDP 5443 – Bandwidth Manager	**Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast **SoftSwitch** UDP 5440 – Location Service UDP 5441 – Call Control UDP 5442 – DRS UDP 5443 – Bandwidth Manager	**Call Control** TMS RPC: TCP 5457 NCC Event port UDP 5458 SUNRPC Broadcast TCP/UDP 5500-5600 **SoftSwitch** UDP 5440 – Location Service UDP 5442 – DRS UDP 5442 – DRS	**Configuration Control** UDP 162 SNMP TRAP **Call Control** UDP 5060 SIP **Media Stream** UDP 1024-65535 RTP – for SIP

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Service Appliance (Conferencing and IM)			**SoftSwitch** UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Database** TCP 4306 MYSQLCC TCP 4308 – MYSQL config **Transport** TCP 5432 – CDS	**SoftSwitch** UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Database** TCP 4306 MYSQLCC TCP 4308 – MYSQL config **Transport** TCP 5432 – CDS	**SoftSwitch** UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive **Database** TCP 4306 MYSQLCC TCP 4308 – MYSQL config	**IP Path Trace** ICMP 33434+255 SMTP TCP 25 – SMTP (third party for email notification)

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Service Appliance (Conferencing and IM)			**ABC** TCP 80, 443 – ABC (for Exo-IM) **CAS** TCP 5447/5448– CAS (for Exo-IM) **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files **IP Path Trace**UDP 33434+255	**ABC** TCP 80, 443 – ABC (for Exo-IM) **CAS** TCP 5447/5448– CAS (for Exo-IM) **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files **IP Path Trace**UDP 33434+255	**Transport** TCP 5432 – CDS **Conferencing License** TCP 80 – HTTP **Voice Prompts** TCP 21 – FTP of phr files **ABC** TCP 80, 443 – ABC (for Exo-IM)	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Service Appliance (Conferencing and IM)					**CAS** TCP 5447/5448– CAS (for Exo-IM) **Configuration Control** TCP 21 FTP CTL – Boot files TCP 20 FTP DATA – Boot files **IP Path Trace**UDP 33434+255	

Originating Device	Destination Device					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
IP Phone	**Media Stream** UDP10000-10550 RTP **IP Path Trace** ICMP Traceroute	NA	**Media** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute File Download/ Linux DVS Update TCP 80 HTTP TCP 443 HTTPS **ABC** TCP 80, 443 HTTPS	**Media** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute File Download/ WinDVS Update TCP 80, 443 HTTPS **ABC** TCP 80, 443 HTTPS	**Media** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute File Download/ WinHQ Update TCP 80, 443 HTTPS **ABC** TCP 80, 443 HTTPS	**Syslog Server** UDP 514 NTP Server UDP 123 – This is the default port. Can be configurable. UDP 61373 – RpCap end of capture
IP Phone			CAS TCP 5447/5448 HTTPS	CAS TCP 5447/5448 HTTPS	CAS TCP 5447/5448 HTTPS	

Originating Device	Destination Device					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
MGCP Phone	**Media Stream** UDP10000-10550 RTP **IP Path Trace** ICMP Traceroute	NA	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute **FTP** TCP 21 – FTP	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute **FTP** TCP 21 – FTP	**Media Stream** UDP 10000-20000 RTP (configurable) **IP Path Trace** ICMP Traceroute **FTP** TCP 21 – FTP	NA

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Connect Client Softphone	**Media Stream** (if both clients are on same network) – Both audio & video UDP 10000-10550 RTP (configurable)	NA	**Configuration Control** TCP 5449, 5469 – TBD: webproxy, Mgmt API– TCP 80 HTTP – Online help **WSS call (MGCP)** TCP 4431 - WSS nginx TCP 7777 - WSS internal only TCP 9090, 8181 - Mgmt TCP 2427 - Switch to WSS	**Configuration Control** TCP 5449, 5469 – TBD: webproxy, Mgmt API– TCP 80 HTTP – Online help **WSS call (MGCP)** TCP 4431 - WSS nginx TCP 7777 - WSS internal only TCP 9090, 8181 - Mgmt TCP 2427 - Switch to WSS	**Configuration Control** TCP 5449, 5469 – TBD: webproxy, Mgmt API– TCP 80 HTTP – Online help **WSS call (MGCP)** TCP 4431 - WSS nginx TCP 7777 - WSS internal only TCP 9090, 8181 - Mgmt TCP 2427 - Switch to WSS	NA

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Connect Client Softphone			**Media Stream** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 HTTPS **CAS** TCP 5447/5448 HTTPS **Image Download** TCP 80, 443	**Media Stream** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 HTTPS **CAS** TCP 5447/5448 HTTPS **Image Download** TCP 80, 443	**Media Stream** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 HTTPS **CAS** TCP 5447/5448 HTTPS **Image Download** TCP 80, 443	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Linux DVS Media	**Stream UDP** 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**Voice Mail Notification** TCP 25 SMTP

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Linux DVS Media			**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport **Transport** TCP 5432 – Xprt	**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport **Transport** TCP 5432 – Xprt	**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport **Transport** TCP 5432 – Xprt	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Windows DVS	**Stream UDP** 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 – Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**Voice Mail Notification** TCP 25 SMTP

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Windows DVS			**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport **Transport** TCP 5432 – Xprt	**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport **Transport** TCP 5432 – Xprt	**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/DTAS interserver communication **Distributed Voice Mail** TCP 25 SMTP - Voice Mail transport	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
Windows DVS					**Database** TCP 4308 – config DB (RO via ODBC for DDB) (R11.x) **CAS Session Manager (R11.x)** TCP 5449 – TMS to Data API to fulfill CSR **Transport** TCP 5432 – Xprt	

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
HQ Server	**Stream UDP** 10000-10550 RTP (configurable) **IP Path Trace** UDP 33434+255	NA	**SoftSwitch** UDP 5440 - Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**SoftSwitch** UDP 5440 - Location Service TCP 5441 – Call Control UDP 5443 – Bandwidth Manager UDP 5445 – Admission Control UDP 5446 – DRS keepalive	**CDR Offline Upgrade - TRANSIENT** TCP 4311 – Old MySQL CDR DB **D&M Offline Upgrade TRANSIENT** TCP 4312 – Old MySQL D&M DB	**Voice Mail Notification** TCP 25 SMTP CDR TCP 3306 - CDR archive on remote server

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
HQ Server			**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/ DTAS interserver communication **WSS-SoftPhone (Int Prod)** TCP 4431 – WSS nginx (Keypush from HQ Key Notifier)	**TMS** UDP dynamic [1024-65535] – broadcast. TMSTMS disaster recovery TCP 5430 – TMS/ DTAS interserver communication **WSS-SoftPhone (Int Prod)** TCP 4431 – WSS nginx (Keypush from HQ Key Notifier)		
HQ Server			**Distributed Voice Mail** TCP 25 SMTP – Voice Mail transport **Transport** TCP 5432 – Xprt	**Distributed Voice Mail** TCP 25 SMTP – Voice Mail transport **Transport** TCP 5432 – Xprt		

Originating Device	Destination Device					
	Connect Client and Softphone	Connect Client for Web and Softphone	Linux DVS	Windows DVS	HQ Server	Other
ECC Supervisor Client	NA	NA	NA	**ECC Supervisor** TCP 31451 - 31452	NA	NA
CMC	**Media Stream** UDP 10000-10550 RTP (configurable)	NA	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 **CAS** TCP 5447/5448	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 **CAS** TCP 5447/5448	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 80, 443 **CAS** TCP 5447/5448	NA

Originating Device	Destination Device					
	Connect Client and Softphone	**Connect Client for Web and Softphone**	**Linux DVS**	**Windows DVS**	**HQ Server**	**Other**
CMR	**Media Stream** UDP 10000-10550 RTP (configurable)	NA	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 443 HTTPS **CAS** TCP 5447/5448 HTTP(S)	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 443 HTTPS **CAS** TCP 5447/5448 HTTP(S)	**Media** UDP 10000-20000 RTP (configurable) **ABC** TCP 443 HTTPS **CAS** TCP 5447/5448 HTTP(S) **Data API** TCP 5449/4430 HTTP(S)	NA
Edge Gateway	**TURN:** **Media Stream** UDP 10000-10550 RTP (configurable)	**TURN:** Browser determined dynamic port (WebRTC)	**TURN:** **Media Stream** UDP 10000-10550 RTP (configurable)	**TURN:** **Media Stream** UDP 10000-10550 RTP (configurable)	**TURN:** **Media Stream** UDP 10000-10550 RTP (configurable)	NA
Other	NA	NA	**SSH** TCP 22	NA	**D2, D&M** TCP 5478	NA

16.1.4 Port Usage - Ingate

The following is the port usage information for Ingate.

Table 85: Port usage for Ingate

Originating Device	Destination Device				
	6900-Series Phones (for Ingate)	Linux DVS	Windows DVS	HQ Server	Switch
IP Phone	**Media Stream** UDP 58024 – 60999 (Media RTP) **Call Control** UDP and TCP port 5060 (SIP Signaling) TCP port 5061 open (TLS for SIP signaling) TCP 443 (HTTPS requests to Ingate HTTPS services) TCP 444 (Secure HTTP connect tunnel) TCP 80	NA	NA	NA	NA
IP Phone	**IP Path Trace** ICMP Traceroute	NA	NA	NA	NA

Originating Device	Destination Device				
	6900-Series Phones (for Ingate)	**Linux DVS**	**Windows DVS**	**HQ Server**	**Switch**
Ingate	NA	**Call Control** TCP 443 TCP 444 TCP 80 **IP Path Trace** ICMP Traceroute	**Call Control** TCP 443 TCP 444 TCP 80 **IP Path Trace**	**Call Control** TCP 443 TCP 444 TCP 80 **IP Path Trace**	**Call Control** UDP and TCP port 5060 (SIP Signaling) TCP 5061SIPS **MediaStream** UDP10000-20000RTP(config
Ingate	NA				**IP Path Trace** ICMP Traceroute

Appendix E - Connect System Logs 17

This chapter contains the following sections:

This appendix contains information about Connect System Logs.

17.1 System Logs

Table 86: System Logs

Log file name	Module	Location	Description	Debug Setting
bootlog	Switch	VMB	Switch bootup log. Captures initialization, upgrade, and other functions.	No debug setting. The log is always on.
caswebsrv	CAS	HQ/DVS	Internal CAS web server - used for troubleshooting Development systems. Can be used to troubleshoot performance.	Contact Support for debugs per specific issue.
CheckDatabase	DB	HQ	Runs at installer (beginning of installation). Check DB compatibility during upgrade.	No setting available. Runs at installer time.
ConnectSync	ConnectSync	HQ	MiVoice Connect service used to push data to the MiCloud for HYBRID deployments.	`HKEY_LOCAL_MACHINE\SOFTWARE \Shoreline Teleworks\ConnectSync \Logging` Level = 0x1 PriMaskLF = 0xFFF The default log level is 1, and logging levels are a mask with 0x2 and 0x4, the higher levels of internal logging. 0x8 is the HTTP logging where, the service logs are all HTTP requests in full text format.
CSISSvr	CSIS	HQ/DVS	CSIS server log	Contact Support for debugs per specific issue.
csisvm	CSIS	HQ/DVS	Interface to access Voicemail. Interactions from applications such as CAS, VMEMSync, CSISVMService to Voicemail are captured.	Contact Support for debugs per specific issue.
CSISVMEvt	CSIS	HQ/DVS	Voicemail events sent through CSIS.	Contact Support for debugs per specific issue.

Log file name	Module	Location	Description	Debug Setting
Database	DB	HQ/DVS	Runs during installation (this is the actual upgrade log).	No setting available. Runs at installer time.
dbhs	Voicemail	HQ/DVS/VMB	Voicemail status reporting to Director (Mailbox status and other runtime status).	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\logsvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
dbq	DB	HQ/DVS/VMB/ UCB	DBQuery log. ODBC queries to database from applications such as CAS, Voicemail, and TMS.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\DataServices\DBQuery\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
dbu	DB	HQ/DVS/VMB/ UCB	DB Update log. Updates;queries to database from applications such as CAS, Voicemail, and TMS.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\DataServices\DBUpdate\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
dbusvc	DB	HQ/DVS (wherever we have DB or DDB)	DB Update service. DB Update requests go through this service.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\DataServices\DBUpdateSvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
director2_dm	D&M	HQ	D&M	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\SvrAppMsgSvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
director2_uc	Director2, D&M	HQ	D2 and D&M	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\SvrAppMsgSvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.

Log file name	Module	Location	Description	Debug Setting
Director2	Data API, SessionMgr	HQ/DVS	Data API and SessionMgr	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\SvrAppMsgSvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
DistributedDB	DB	HQ/DVS	Backup of HQ DB (nightly backup). On DVS it is mostly blank.	No setting available. Runs at installer time.
DRS	DRS	HQ/DVS	Main DRS operations, LSP ping and DN resolution covered in this log.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Distributed Routing Service\Logging` Level = 0x1 PriMaskLF = 0xFFF 0x0100 and smaller control DRS.log 0x0200 and larger control DRSTrans.log 0x0010 logs DRS-ping keep-alives.
DRSTran	DRS	HQ/DVS	ShoreSIP and switch related logging are covered here.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Distributed Routing Service\Logging` Level = 0x1 PriMaskLF = 0xFFF 0x0100 and smaller control DRS.log 0x0200 and larger control DRSTrans.log 0x0010 logs DRS-ping keep-alives.
DSTrace	DRS	HQ/DVS	COM Trace for update queries (DDB update on DVS). Most reads go through DBQuery and get captured in dbq log.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\DataServices` DebugLevel=0x1 Set DebugLevel=0x5 for query level details.
EventWatch	Event Notification	HQ	The log for the service that performs email notification for NT events.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\DataServices` DebugLevel=0x1 Set DebugLevel=0x5 for details.

Log file name	Module	Location	Description	Debug Setting
evt	Trigger	HQ/DVS	Service that dispatches the triggers from the database to the applications.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\EventSystem\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
IIS	IIS	HQ/DVS	Microsoft IIS web server	Contact Support for debugs per specific issue.
Install_Shoreware_Server	Installer	HQ/DVS	Installer log file	`HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer` Set key Logging with type REG_SZ and Value "voicewarmup!" • Gives information about the step the installer is at, and the values of the properties. In case of a rollback, it gives information about when the rollback happens • Gives more information about the files and the sequence of actions. • Gives detailed information about the functions installer performs on the machine.
IPBX	Switch	HQ/DVS	Switch level logs/events sent to the server.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\STSTSPI\Logging` Level = 0x1 PriMaskLF = 0xFFF
ipds	CAS	HQ/DVS	CAS main log	Contact Support for debugs per specific issue.
kmessages	Kernel	VMB/UCB	Linux kernel messages	No debug setting available. The log is always on.
LogLibTrace	LogLib	HQ/DVS/VMB/UCB	Trace for logger	No setting available.The log is always on.
LogLibTraceX	LogLib	HQ/DVS	Trace for logger for logging from TapiSrv.	No setting available. The log is always on.
LogSvc	LogLib	HQ/DVS	LogSvc helps VMB switches do remote logging (this is unused). In addition, both VMB and UCB switches also log their NT events through this service on the Windows NT event log.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\logsvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on developer's request.

Log file name	Module	Location	Description	Debug Setting
MakeCDR	System Mgmt	HQ	Run by installer for new install/upgrade.	No setting available. Runs at installer time.
messages	Kernel	VMB/UCB	Linux kernel messages + user level system log messages.	No debug setting available. The log is always on.
mon_log	Switch	VMB	System resource usage by individual modules/process.	No debug setting available. The log is always on.
mon_nand_log	Switch	VMB	System Nand usage	No debug setting available. The log is always on.
MonitoringAgentVM	D&M	HQ	Log from Monitoring agent that lives on switch to report call quality.	To turn on this log, enable switch level setting.
MonitoringService	D&M	HQ/D&M standalone server	D&M log	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Monitoring Service\Logging` Level=0x1 PriMaskLF=0xFFF Turn on level if developer recommends.
QMailService	Qmail	VMB/UCB	Qmail service that launches Qmail engine.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\QMailService\Logging` Level=0x1 PriMaskLF=0xFFF Turn on level if Support recommends.
qmail-cleanup	Qmail	VMB/UCB	Qmail cleanup log (logs internal cleanup).	No setting available. The log is always on.
RegLibTrace	RegLib	HQ/DVS/VMB/UCB	Trace for registry library	No setting available. The log is always on.
RegLibTraceX	RegLib	HQ/DVS	Trace for registry library from TapiSrv	No setting available. The log is always on.
RpCap	D&M	HQ	Logic to invoke the Wireshark trace for P-phone and switch. Actual Wireshark trace is on the switch/p-phone.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\RpCap\Logging` Level=0x1 PriMaskLF=0xFFF Turn on level if Support recommends.

Log file name	Module	Location	Description	Debug Setting
SAMS	System Mgmt	HQ	zeroMQ (D2, D&M use it, it is a Ruby to C++ bridge. For example, AnyPhone).	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\SvrAppMsgSvc\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
SC	Workgroup	HQ/DVS	WG puts a call on queue (technically park the call on its own number, try to unpark.WG extension from another extension will show list of calls in WG queue) if agent is not available. ;All these activities related to queuing WG call get logged in SC logs.	No debug setting. The log is always on.
SDMS	System Mgmt	HQ	ZinManager runs periodically for phone home audit.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Data Services` Set DebugLevel=0x5.
smgr	ServicesMgr	VMB/UCB	Linux services manager that administers all processes.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\ServicesMgr\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
SMTP	SMTP	HQ/DVS	Microsoft SMTP log	Use Microsoft IIS manager to turn on this log.
SoftSw	Soft Switch	HQ/DVS	Soft switch log on Windows server.	`HKEY_LOCAL_MACHINE\Software\Shoreline Teleworks\SoftSwitch` Create a key called TelnetEnabled and set it to 1. telnet <softswitch-ip> 2323 To get the SHELL access, turn on the appropriate switch trace.
STCTSP	ShoreTapi	VMB/UCB	Legacy ShoreTapi interface for Voicemail (VMB) and Conferencing (UCB).	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\STCTSP\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.

Log file name	Module	Location	Description	Debug Setting
STCTSPI	ShoreTapi	HQ/DVS	ShoreTapi interface for CAS, Workgroup.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\STCTSPI\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.
STMedia	Switch media	UCB	Switch media log file.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\STMedia\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
stpi	ShoreTapi	HQ/DVS	ShoreTapi client side log for CAS, WG.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\ShoreTapi\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.
STSTSP	TAPI	HQ/DVS/VMB/UCB	TAPI Path entry point into TMS.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\STSTSPI\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.
STTS	Switch	VMB/UCB	Switch log file	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\STTS\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.
SysMgmt	System Mgmt	HQ/DVS	SysMgmtSvc (former IPCS/Heap status activity)	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\SysMgmt\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0xFF for debugging.

Log file name	Module	Location	Description	Debug Setting
TAPI	Microsoft TAPI	HQ/DVS	Microsoft portion of the TapiSrv..	`HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tapisrv` Set FileDirectory to a directory (For example, C:\Tmp) where you want the TAPI logs - default location is C:\Windows\Tracing Set EnableFileTracing = 1 Set FileTracingMask = 0xffffffff
Tapi32	API side Microsoft TAPI	HQ/DVS	Application (For example, Voicemail) TAPI API side.	`HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\tapi32` Set FileDirectory to a directory (For example, C:\Tmp) where you want the TAPI logs - default location is C:\Windows\Tracing Set EnableFileTracing = 1 Set FileTracingMask = 0xffffffff
TapiSrv	TAPI	HQ/DVS	RemoteTSP - Legacy TAPI interface for Voicemail, ECC ProSvcs/Third Party applications.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\TapiSrv\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TAPI signaling debugging.
TapiWav	Windows media driver	HQ/DVS	Windows media driver	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\TDIMedia` "LogTapiWaveToFile"=dword:00000001 "TapiWaveDebugLevel"=dword:00000007 "Playdebuglevel"=dword:00000007 "SipWaveDebugLevel"=dword:00000007 "IoctlDebugLevel"=dword:00000007 "RecordDebugLevel"=dword:00000007 Lower the debugs once debugging is complete.
TmsCDR	System Mgmt	HQ	Call accounting service	No setting available. Runs at installer time.
TMSCDRArchive	System Mgmt	HQ	Backup to archive server (nightly)	No setting available. Runs at installer time.

Log file name	Module	Location	Description	Debug Setting
TmsCDS	TMS	HQ/DVS	TMS call data service - plumbing layer. Used for low level call tuple and CDR data debugging.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\CDS\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
TmsDTAS	DTAS	HQ/DVS	TMS distributed telephony log - plumbing layer. Used for TAPI debugging.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\TmsDTAS\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level=0x1F on Support's request for debugging TAPI level problems.
TmsHeapStatus_AppODBC	TMS	HQ/DVS	TMS updates to heap status DB to report runtime status to Director, D&M.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\TmsHeapStatus_ODBC\Logging` Level = 0x1 PriMaskLF = 0xFFF Turn on level only on Support's request.
TmsMain	TMS	HQ/DVS	TMS main log. All the TMS processing is divided into small steps and the steps are executed here.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\Main\Logging` Level = 0xF PriMaskLF = 0xFFF Set Level =0x3F for TMS level debugging.
TmsMgmt	TMS	HQ/DVS	TMS Management log. Captures TMS reporting runtime status on switches, devices, trunks, and others.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\TmsMgmt\Logging` Level = 0xF PriMaskLF = 0xFFF Set Level =0x3F for TMS level debugging.
TmsNcc	TMS	HQ/DVS	TMS to switch communication including call debugging using GUID.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\NCC\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TMS switch debugging.

Log file name	Module	Location	Description	Debug Setting
TMSPerf	TMS	HQ/DVS/VMB/ UCB	TMS sub-task level performance debugging. Useful to debug low level delays in TMS.	`HKEY_LOCAL_MACHINE\SOFTWARE \Shoreline Teleworks\Telephony Management Server\TmsTCC\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TMS switch debugging.
TMSTCC	TMS	HQ/DVS/VMB/ UCB	TMS TAPI call control log. Useful for tracing end to end call flows. This log is not generated by default. Set elevated log level for it to be generated.	`HKEY_LOCAL_MACHINE\SOFTWARE \Shoreline Teleworks\Telephony Management Server\TmsPerf\Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0x1F for TMS switch debugging.
Uninstall_Shoreware_Server	Installer	HQ/DVS	Installer log file	`HKLM\SOFTWARE\Policies\Microsoft \Windows\Installer` Set key Logging ;with type REG_SZ and Value “voicewarmup!” • Gives information about the step the installer is at, and the values of the properties. In case of a rollback, it gives information about when the rollback happens. • Gives more information about the files and the sequence of actions • Gives detailed information about the functions installer performs on the machine.
Vmail	Voicemail	HQ/DVS/VMB	Voicemail log. Useful for Voicemail call debugging (recording, playback, find me, AA menus, account code, and other features).	`HKEY_LOCAL_MACHINE\SOFTWARE \Shoreline Teleworks\Voicemail \Logging` Level = 0x1 PriMaskLF = 0xFFF Increase debug level as recommended by Support.
VMCAS	CAS	HQ/DVS	Reusable VMCAS library applications such as CAS, VMEmSync are used to talk to Voicemail.	Contact Support for debugs per specific issue.
VMEMSync	VMEmSync	HQ/DVS	Voicemail to external mail server (For example, Gmail) sync.	`HKEY_LOCAL_MACHINE\SOFTWARE \Shoreline Teleworks\VmEmSync \Logging` Level = 0x1 PriMaskLF = 0xFFF Set Level =0xFF for debugging.

Log file name	Module	Location	Description	Debug Setting
VMStats	Voicemail	HQ/DVS	The Voicemail mailbox starts debugging.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Voicemail\Logging` Level = 0xF PriMaskLF = 0xFFF Setting Vmail log level to 0xF generates VMStats log file.
WavAPI	Windows media driver	HQ/DVS	Windows media driver	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\TDIMedia` "LogWaveAPIToFile"=dword:00000001 "WaveAPIDebugLevel"=dword:00000007 "Playdebuglevel"=dword:00000007 "SipWaveDebugLevel"=dword:00000007 "IoctlDebugLevel"=dword:00000007 "RecordDebugLevel"=dword:00000007 Lower the debugs once debugging is complete.
WG	Workgroup	HQ/DVS	Workgroup log	`HKEY_LOCAL_MACHINE\SOFTWARE\WGSvc\Logging` Level = 0x1F PriMaskLF = 0xFFF
xprt	Transport	HQ/DVS/VMB/ UCB	Transport log. Useful to debug box to box communication issues.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Transport\Logging` Level = 0x1 PriMaskLF = 0xFFF and Set Level =0xF for debugging, 0xFF for pipe level debugging. This can be intrusive.
Zin	System Mgmt	HQ	COM+ (all legacy business logic) for example, AnyPhone;logic in Visual;Basic, Voicemail backup time update in C++.	`HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks` Key: ZinDebugLevel=0x3 for debug traces.