MiVoice Connect

Conferencing and Instant Messaging Planning and Installation Guide

July 15, 2019

Mitel®

Notice

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

Trademarks

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

Contents

Chapter: 1 **Preface 1**

About This Book 1
Audience 1
Related Documentation 1
Technical Knowledge Base 1
Conventions 1

Chapter: 2 **Conferencing and Instant Messaging Overview 3**

About the SA100, SA400, and Virtual Service Appliance 3
Distributed Conferencing Capabilities 3
Single System Management 4
Integrated Services 4
Audio Conferences 4
Instant Messaging Service 5
Single Dial-in Number and Web Address 5
Service Appliance Failover 5
Complete Failure Scenario 5
Conferencing and Instant Messaging Resiliency 6
Service Appliance Logs and Records 6
Upgrading Service Appliance Data in System CDR Database . . . 7
Integration with Connect Client and Microsoft Office 7
Host and Participant Desktop Requirements 7
Internet Browsers 7
Microsoft Office Integration 8

Chapter: 3 **Planning and System Design 9**

Recommendations 9
Determining Your Conferencing Needs 9
Determining the Number of Service Appliances to Deploy 9
System Topology 11
Load Balancing 11
Redundancy 11

Licensing Requirements 11

Chapter: 4 Network Requirements and Preparation 13

Network Requirements for SA100, SA400 and VSA 13
Supported Codecs and Bandwidth 13
Network Bandwidth Requirements for Web Conference Sessions 14
IP Addressing 15
Time Services 15
Network Security 15
Internal Firewall 15
Security Considerations 16
Deployment Scenarios 16
Deploying a Service Appliance in the LAN 16
Deploying a Service Appliance In the DMZ 17
Requirements 18
Best Practice Tests 19

Chapter: 5 Site Requirements and Preparation 20

Recommendations 20
Specifications 20
SA100 Specifications 22
Front Panel 22
Back Panel 23
Power Cable 24
Ethernet Ports 24
Maintenance Cable 24
SA400 Specifications 24
SA400 Key Features 25
Front and Back Panels 25
Connection Specifications 26
Power Input Specifications 26
Virtual Service Appliance Specifications 26
Environmental Requirements 27

Chapter: 6 Installing Service Appliances 28

Preparing for Installation 28
Verifying the Contents of the Box 28
Location Guidelines 28
Installation 29
Mounting the Service Appliance 29
Connecting AC Power to the SA100 29
Connecting AC Power to the SA400 29
Setting the IP Address Manually 30
Using DHCP to Set the IP Address 32
Connecting the Service Appliance to the Network 33

Installing the Bezel 33
Configuring the Unit for Operation 33
Installing the Virtual Service Appliance 34

Chapter: 7 Configuring the Service Appliance 35

Upgrading the Service Appliance Firmware 35
Prerequisites 35
Configuration 35
Configuring the Service Appliance 35
Configuring the NTP Server 36
Integrating the Service Appliance with the Mitel System 36
Adding the Service Appliance to a Mitel Site 36
Verifying Date and Time Synchronization 38
Configuring a Service Appliance in the DMZ 38
Configuring a Backup Service Appliance Site for the HQ Server .39
Configuring a Remote Service Appliance and a Proxy Web Portal 39
Configuring Conferencing for a Service Appliance 40
Configuring HTTPS 40
Prerequisites 41
Configuring HTTPS 41
Configuring Firefox Browser 42
Configuring Mitel Licenses 43
Registering and Downloading Conference License Keys 43
Installing the Licenses 43
Enabling Conferencing for Service Appliance Users 44
Configuring a Conference Extension 44
Configuring the Conference Options Page 45
Integrating Conferencing with Microsoft Exchange 47
Enabling the Connector for Microsoft Exchange Integration . . 48

Chapter: 8 Going Live and Training 50

Complete Operational Testing of Service Appliances 50
Assign Users to Each Service Appliance 50
Verify Licensing 51
Distribute User Guides 51
Training 51

Chapter: 9 Backup and Restore 52

Service Appliance Backup 52
Service Appliance Restore 53

Preface

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

This Preface provides an overview of the *Conferencing and Instant Messaging Planning and Installation Guide*.

About This Book

This document provides planning, installation, and administration information for service appliances (including the SA100, SA400, and virtual service appliance), as well as the following services:

- Audio conferencing
- Web conferencing
- Instant messaging

Audience

This guide is for installers and administrators of the Mitel system. To use this guide effectively, you must be knowledgeable about data networking and telephony.

Related Documentation

Refer to the following documents for additional information about the Mitel system and Mitel products:

- *MiVoice Connect Planning and Installation Guide*
- *MiVoice Connect System Administration Guide*
- *MiVoice Connect Maintenance Guide*
- *MiVoice Connect Server Software Release Notes*
- *Telephone User Interface Guides*
- *Telephone Quick Install Guides*
- *MiVoice Connect Quick Reference Guides*

Technical Knowledge Base

For additional information, refer to the Technical Knowledge Base, which you can access from the Support website at https://oneview.mitel.com/s/support.

Conventions

The following typographical conventions are used in this document:

Table 1.1:Typographical conventions

Convention	Meaning
Bold	Names of interface objects, such as buttons and menus.
Courier Font	Code examples.
Courier Italic	Variables in code examples.
Blue	Cross references with hyperlinks. Click the blue text to go to the indicated section. All chapters have a list of section links on the first page.

Conferencing and Instant Messaging Overview

This document is designed for planners and system administrators looking to deploy Service Appliances in their Mitel system to perform conferencing and instant message services.

The Service Appliance installs on your network and augments the Mitel system with conferencing and instant messaging services. These services give Mitel system users the ability to create and participate in scheduled and impromptu media-rich conferences and to send and receive instant messages. Service Appliances support audio and web conferences and allow Microsoft® Outlook® to schedule conferences.

This chapter presents an overview of the Service Appliance, including a description of the integrated applications and capacities to guide you in planning your installation.

About the SA100, SA400, and Virtual Service Appliance

The Service Appliance is a 1U, dedicated, plug-and-play appliance designed to integrate seamlessly into the Mitel system and to install where you need it on your network to provide cost-effective conferencing and instant messaging (IM) services for Mitel system users.

The 1U footprint means the unit is suitable for 19-inch equipment racks. It is shipped with a versatile rack-mounting kit that easily accommodates different rack styles and a locking front bezel.

The Service Appliance is a node that installs on a Mitel server site and performs processing functions for conference calls and IM sessions. In conference calls, the Service Appliance serves as a hub that receives audio and data streams from the participants, bundles the streams, and broadcasts the bundles to the other conference participants. The Service Appliance also maintains conference web pages and manages IM sessions for users.

Telephony Management Service (TMS) and other software installed on the Service Appliance ensure the integration of the unit into the Mitel system. This allows the system to use a universal conference number while directing conference requests to the appropriate appliance in environments where two or more Service Appliances are installed. The software also allows the system to collect and store call data from the Service Appliance where it can be retrieved and viewed as Call Detail Records (CDR) in MiVoice Connect Director.

The Virtual Service Appliance provides users with flexibility and scalability while providing all features supported in the Service Appliances. The Virtual Service Appliance is a VMWare virtual appliance in OVA format that can be configured with CPU, memory, hard disk and other required network specifications and modified by user/system administrators when required.

The conferencing and instant messaging services the Service Appliance provide seamlessly integrate with user desktop applications such as Connect Client and Microsoft Outlook.

Distributed Conferencing Capabilities

The Conferencing and Instant Messaging services are scalable. For the number of simultaneous audio and web conference ports that Service Appliances can support, refer to the *Specifications*.

Service Appliances may be assigned to physical or logical Mitel sites. One Service Appliance must be assigned to the Mitel Headquarters site or the service appliance conference backup site, which may be located anywhere on the network. For more information about creating Mitel server sites, see the *MiVoice Connect System Administration Guide*.

When multiple Service Appliances are deployed, the Mitel system automatically assigns a conference request to the appropriate appliance based on the conference information. Multiple deployment also allows automatic failover to be implemented whereby the server can reroute conference requests to other appliances, should a Service Appliance experience a connectivity or hardware problem.

Single System Management

After the Service Appliance is installed on the network, you must register and configure the Service Appliance with MiVoice Connect Director.

For more information about using MiVoice Connect Director to configure Service Appliances, see *Chapter 6, Configuring the Service Appliance on page 51*. For information about using MiVoice Connect Director, refer to the *MiVoice Connect System Administration Guide*.

NOTE: The Mitel system provides automated software distribution for all components on the system, including Service Appliances. When you add a new Service Appliance to the system, it is automatically upgraded to the current software release by the server. When you upgrade the Mitel system, Service Appliances will automatically upgrade as required when the device restarts.

Integrated Services

Conferencing allows the Mitel system to provide conferencing to Mitel users. The Mitel system supports the following types of conferencing:

- Audio conferences
- Web-only conferences
- Web and audio conferences
- Instant messaging

This section provides a brief description about the types of conferences that Service Appliances support.

Audio Conferences

An audio conference is a virtual meeting of people in different locations using communication tools to hear and talk with each other. For the number of simultaneous audio conference ports that Service Appliances can support, refer to the *Specifications*.

Ports are not reserved but allocated on a first-come-first-serve basis. When all of the audio ports on an Service Appliance are in use, calls that initiate new conferences are routed to an available Service Appliance. New calls to an existing conference are routed to an auto attendant and informed that there are no available ports. When all of the ports available to the system are in use, all callers that access the conference receive a message that the call cannot be completed.

Similarly, when the number of conference participants exceeds the number of audio conference licenses you have, the extra participants receive an unavailable message.

NOTE: If you are installing web licenses on a system that has been running with only audio licenses, then the users must restart Microsoft Outlook for this change to take effect.

Instant Messaging Service

This service provides the Instant Messaging server to be used with Connect Client for Windows and with the Connect client. For the number of IM clients that Service Appliances can support, refer to the *Specifications*. For detailed explanations and usage of available features for each application, see the *Connect Client User Guide*.

Single Dial-in Number and Web Address

Multiple Service Appliances on the network can function with a single dial-in number and single Fully Qualified Domain Name (FQDN).

You specify the single dial-in number as a system-wide and global conference extension. For more information, see *Integrating the Service Appliance with the Mitel System*. When the conference host or participant dials this number, the call gets automatically routed to the preferred Service Appliance, if this Service Appliance is available or not overloaded. For Service Appliance capacities, see the *Specifications*.

A system-wide global conference URL can also be configured in **System** > **Additional Parameters**. The system-wide URL must be FQDN of first collaboration appliance configured in the system.

NOTE: A preferred Service Appliance is the Service Appliance that a Mitel user is manually assigned to by the administrator. The system does not assign a Service Appliance automatically to a user.

For example, if you assign an FQDN, such as “conference.acme.com” to the first Service Appliance you install, your users will only need to remember one URL. When the conference hosts enter the system-wide URL, conference.acme.com, they get connected to their preferred Service Appliance.

The preferred SA-specific global conference URL is also included in the conference invitations created by the conference portal and Microsoft Outlook.The global conferencing URL is available in MiVoice Connect Director at **Administration** >**System** > **Additional Parameters**.

Service Appliance Failover

The Service Appliance is designed to provide high availability. The system is set up so that you can assign each Service Appliance a primary and backup server to manage the unit. If the primary server fails or is otherwise unavailable, the backup server takes over call management without interrupting conferencing services. The SA also uses a dual-port Ethernet card. The ports are designated as primary and secondary, and use the same IP address. You must connect both ports on the SA to the same network to protect against a port or cable failure.

Complete Failure Scenario

In a single Service Appliance deployment configuration, the system will not have any fail-over capabilities.

In a system with multiple Service Appliance, the system can ensure that a conference starts even if the preferred SA is not available.

When the conference is scheduled to start, the system checks to see if the user's preferred SA is available and not overloaded. If the preferred SA is unavailable or overloaded, the new conference will be hosted on a different Service Appliance. A conference started on a non-preferred Service Appliance offers the same functionality as a conference started on the preferred Service Appliance.

Because the system uses floating licenses, you do not need to deploy fail-over licenses. The system tracks the number of ports in use at the system level and not at the appliance level.

When IM users are assigned to a Service Appliance that goes down, only the users assigned to that particular Service Appliance are affected. Other users can continue to use IM.

Conferencing and Instant Messaging Resiliency

Each Service Appliance must be able to reach the Headquarters server in order to provide full functionality.

If connectivity to the Headquarters server is down, users can still perform the following tasks:

- Hear other users.
- Use all the audio controls.
- Join and attend started conferences. The user can use the direct conference URL or enter the access code in the Join Access field.
- Start and stop desktop sharing.
- Use the Instant Messaging Service (as long as the user has logged in during the previous three days and there are no user changes in Director).

NOTE: If connectivity to the Headquarters server or DVS assigned to the IM user is down, the user cannot log in to the IM service.

However, if connectivity to the Headquarters server is down, users cannot perform the following tasks:

- Access the conference portal
- Start and stop a recording, or access meeting recordings
- Access web pages that may be linked from the meeting user interface
- Create meetings
- Start and stop meetings
- Configure conferencing by using MiVoice Connect Director

Service Appliance Logs and Records

The Service Appliance provides audio and web conference data to the Mitel system that is collected in the call detail record (CDR) database. The Mitel system can collate the data and issue various types of reports about Service Appliance activity. The Service Appliance also maintains data log files that can be used for troubleshooting. Virtual service appliance report is available in MiVoice Connect Director.

Upgrading Service Appliance Data in System CDR Database

If the Mitel system is upgraded to ST13 or 14, a separate script must be run to upgrade the Service Appliance data in the Mitel system CDR database. To run the script, perform the following steps:

1. Navigate to the following directory: `\Program Files\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\`
2. Double-click/run the following script: `cdr_upgrade_for_upgrade_-from_ST12_to_ST13_or_later.wsf`
3. Wait for the script to finish running.

   NOTE: Running this script will impact database performance.

Integration with Connect Client and Microsoft Office

Conferencing integrates with Microsoft Outlook to provide integrated one-click conference scheduling in conjunction with user calender appointments. See the *Connect Client User Guide* for more details.

NOTE: The use of delegates and the limitations are as follows:

- In Outlook, only the original delegate that created the meeting can modify.
- A second delegate can modify a meeting if the meeting was created in Connect Client and the delegate was listed as an organizer during meeting creation

This option is available only on Windows

Host and Participant Desktop Requirements

Participants in web conferences will need to meet minimum software and browser requirements.

Participant desktop and laptop systems are not required to meet any minimum hardware requirements except for an acceptable broadband Internet connection.

Internet Browsers

Web Conference users require one of the following Internet browsers:

- Microsoft Internet Explorer 10.0 and 11.0
- Microsoft Edge 25.10586.0.0
- Google Chrome 49 and 50.0.2661.102
- Safari 8 and 9.1 on Mac OS
- Mozilla Firefox 45 and 46.0.1 - on Windows and Mac OS

NOTE: On a Mac, while the Presenter is in focus, you may need to click twice to trigger a button on the Conference Viewer. After the Conference Viewer has focus, then it works normally and only requires a single click to trigger a button.

Microsoft Office Integration

The following is required when the Microsoft Office integration feature is used:

- Microsoft Office 2010 32-bit SP1 on Windows
- Microsoft Office 2010 64-bit SP1 on Windows
- Microsoft Office 2013 32-bit SP1 on Windows
- Microsoft Office 2013 64-bit SP1 on Windows
- Microsoft Outlook 2011 on Apple OS X

To enable one-click conference scheduling from Microsoft Outlook, the Outlook calender integration must be installed from Connect Client. For more information, see the *Connect Client User Guide*.

Planning and System Design

This chapter guides you through the planning process for deploying Service Appliances on your network.

Recommendations

The following recommendations will assist you in designing your Mitel system to use conferencing capabilities:

- Ensure you determine the need for audio conferencing, web conferencing and Instant Messaging services
- Ensure you determine licensing requirements
- Ensure you determine the placement of Service Appliances within the Mitel system topology, including external web access and security considerations
- Ensure you determine WAN considerations, quality and bandwidth.

Determining Your Conferencing Needs

The single management system makes it easy for you to effectively and cost-efficiently provide conference and IM services for your users. The conferencing solution is flexible, which allows you to install a single Service Appliance unit to provide services company-wide or multiple units deployed regionally to handle services for local users. This can save on long-distance costs when your regions are in remote locations.

In determining how best to deploy Service Appliances in your environment, consider the following:

- The number of simultaneous conferences you want to support.
- The types of conferences you expect to support
- The number of IM sessions you expect to support
- The topology of your network
- Load balancing
- Failover (redundancy)

Determining the Number of Service Appliances to Deploy

Among the factors to consider in determining how many Service Appliances to deploy are the capabilities of the SA100, SA400, and the Virtual Service Appliance. Table 1 provides information about the maximum number of participants Service Appliances can support by conference type. For additional information, see *Chapter 3, Network Requirements and Preparation* .

Table 3.1:Maximum Number of Participants Supported Per Conference Type

Conference Type	SA100 Maximum Conference Ports	SA400 Maximum Conference Ports	Small Virtual Service Appliance	Large Virtual Service Appliance	IM Only
G.711	50	200	50	200	N/A
G.722 (High Definition)	15	15	15	60	N/A
G.729	50	50	50	200	N/A
Web Conference Sessions (secured/unsecured)	50	100	50	200	N/A
IM	500 (Sessions)	2000 (Sessions)	500	2000	2000

The examples below show how you can use the information in the table to determine your deployment needs:

- **Example 1:** In your planning you determine that you require the capacity for 125 concurrent, standard audio (G.711) audio sessions. To determine how many SA100 devices your system requires, divide the number of audio sessions you determine that you require by the maximum number of conferences the SA100 supports; for example, 125 ÷ 50 = 2.5. To satisfy the requirement for your network, you would install three SA100s.
- **Example 2:** You determine that you require 20 high definition individual audio (G.722) sessions and 90 standard audio sessions. An SA100 can support no more than 15 HD sessions, with up to 35 standard sessions simultaneously. To determine how many SA100s you need, assign the first 15 HD conference sessions and the first 35 standard conference sessions to one SA100. That leaves 5 HD conference sessions and 55 standard conference sessions to be supported. You can combine the remaining 5HD conference sessions with 45 standard conference sessions to achieve the capacity for a second SA100. That leaves 10 standard conference sessions, which can be supported by a third SA100. Consequently, you will need three SA100 to satisfy this scenario.
- **Example 3:** You determine that you require the capacity for 150 concurrent HTTPS web conference sessions. The SA100 supports up to 50 HTTPS web conference sessions simultaneously. To determine how many SA100s you need, divide the total number of required HTTPS conference sessions by the maximum number of HTTPS conferences the SA100 supports; for example, 150 ÷ 50 = 3. You need three SA100s to satisfy the requirement in this scenario.
- **Example 4:** You determine that you require 600 configured IM sessions. The SA100SA100 supports up to 500 IM sessions simultaneously. To determine how many SA100 devices you need to satisfy this requirement, divide the total number of IM sessions by the number of simultaneous IM sessions the SA100 supports; for example, 600 ÷ 500 = 1.2. You need two SA100s to satisfy this requirement.

System Topology

The topology in which your Mitel system is installed can be a factor in determining how you deploy Service Appliances. For Mitel systems installed over multiple sites (a site is an area managed by a Mitel server), whether those sites are in the same building or spread across diverse geographical regions, it may be more effective and efficient to install Service Appliances at specific sites. For example, if your experience includes inconsistent WAN connections, limited WAN bandwidth or known WAN quality issues, installing Service Appliances at regional sites and implementing load balancing can minimize the effect the WAN has on conference calls.

Similarly, if your Mitel system is servicing users in different cities or countries and many of the conferences are held at local sites, you can save on long distance charges by installing Service Appliances at the local sites to handle local conferences. Other advantages of installing Service Appliances at local sites include:

- Savings on inter-site bandwidth
- Better quality audio and web sessions

NOTE: For optimal performance, Mitel recommends that you do not install Service Appliances in a network where latency exceeds 100 ms. To operate Service Appliances optimally, network latency and jitter must be minimized. Mitel also recommends that the ping lag time between Service Appliances and the Mitel headquarters server does not exceed 200 ms. This lag time affects how quickly web pages refresh.

For more information about setting up a remote service appliance, see *Configuring a Remote Service Appliance and a Proxy Web Portal*.

Load Balancing

Conferencing supports load balancing. The Mitel system manages all calls in the system including conference calls from a single source. That means that when a conference is initiated, Conferencing can assess conference resources and shift the conference to an available Service Appliance if the local unit does not have sufficient resources.

Redundancy

The Service Appliance supports failover in cases where a unit loses connectivity or fails. In the event of a loss of network connectivity or unit failure, the Mitel system will redirect new conference calls to another Service Appliance unit if resources are available.

NOTE: Instant Messaging feature does not support *"Load Balancing"* and *"Redundancy"*. If the service appliance fails, the users configured for IM services cannot use the IM feature.

Licensing Requirements

Audio conferencing and web conferencing services are enabled through keyed licenses for Audio Conference ports and web conference ports. Licenses enable concurrent access to the services, rather than per user or per appliance. Instant Messaging is enabled in all Connect Client access levels.

For example, you have a single SA100 which supports 50 G711 audio conference streams and 50 web sessions (secured/unsecured). To run a concurrent audio/secure web conference for 30 participants would require 30 Audio Conference and 30 web conference licenses.

To be a conference host on the system, you must be added as a user, which requires at least a mailbox license.

Network Requirements and Preparation

Use the information in this chapter to determine specific network requirements for the Service Appliance 100 and the Service Appliance 400. After determining the network requirements, you will be ready to configure your network appropriately.

Network Requirements for SA100, SA400 and VSA

Conferencing services require that the underlying network meet all Mitel recommendations. Refer to the *MiVoice Connect Planning and Installation Guide* for more information for recommendations about deploying a telephony system on your network. Consider the following items when planning your system for audio and web conferences:

- Audio conference streams:
  - Delivers adequate bandwidth for toll-quality calls.
  - Meets the latency and jitter requirements for toll-quality calls.
  - Meets the packet loss requirements for toll-quality voice.
  - Bandwidth management to prioritize your voice traffic over your data traffic.
  - Proper configuration of the Admission Control feature for each site.
- Web conference streams:
  - Delivers adequate bandwidth for the typical application you expect users to share.
  - Maintains a ping lag of not more that 100 ms between Service Appliances and the Mitel Headquarters server.

Supported Codecs and Bandwidth

The following table shows the codecs that the SA100 supports.

Table 4.1:SA100 Codecs and Concurrent Audio Streams

Codec	Bandwidth	Sampling Rate	Max Audio Streams	Max SRTP Streams
G711 (both a-law and µ-law)	64 kbps	8 kHz	50	50
DV14/ADPCM	32 kbps	8 kHz	50	50
Linear (L16/8000)	128 kbps	8 kHz	50	No Support
Wideband Linear (L16/16000)	256 kbps	16 kHz	50	No Support
G722	64 kbps	16 kHz	15	15
G.729	8 kbps	8 KHz	50	50

the following table shows the codecs that the SA400 supports.

Table 4.2:SA400 Codecs and Concurrent Audio Streams

Codec	Bandwidth	Sampling Rate	Max Audio Streams	Max SRTP Streams
G.711 (both a-law and u-law)	64 kbps	8 kHz	200	200
DV14/ADPCM	32 kbps	8 kHz	200	200
Linear (L16/8000)	128 kbps	8 kHz	200	200
Wideband Linear (L16/16000)	256 kbps	16 kHz	200	200
G.722	64 kbps	16 kHz	15	15

Network Bandwidth Requirements for Web Conference Sessions

Audio and web data are handled separately by the Service Appliance. Content for web sessions is generated from the computer that is sharing and sent to the Service Appliance managing the conference for distribution to conference participants. For most content, the Service Appliance broadcasts the data to the other web participants. (Content sharers can also send a file to the Service Appliance that the Service Appliance makes available to conference participants to download and open on their devices.) All content that is shared directly with participants appears through the conference Web Viewer. Direct content is provided using the Presenter, the whiteboard, or files downloaded to the sharing device. The bandwidth of this content forms the basis of the network bandwidth requirement for conferencing discussed in this section.

NOTE: A presenter is someone who has permission to present data to others in a conference. The conference host can give the presenter permissions to a participant. The host has all presenter permissions by default. Only the conference host controls the audio conference.

The network bandwidth a conference consumes is the product of the content bandwidth (plus overhead) times the number of participants receiving the content and can be expressed as follows:

$Conf_{BW}$ = Content Mbps × P

where $Conf_{BW}$ is the total bandwidth the conference uses, Content Mbps is the content bandwidth expressed as a rate, and P is the number of participants receiving web content.

For example, in standard operating mode, the Presenter supports bandwidths of up to 250Kbps. An SA100 operating at full capacity (50 HTTPS web ports) would generate the following bandwidth on the network:

$Conf_{BW}$ = 250 Kbps × 50

$Conf_{BW}$ = 12.5 Mbps

NOTE: The bandwidth requirements are as follows:

- Share Full Screen = 8 Mbps per presenter × 250 Kbps for each additional participant

- Share Area = 3.5 Mbps + 250 Kbps
- Share Window = 250 Kbps per participant

IP Addressing

The Service Appliance requires an IP address with a permanent lease or a static IP address. Either of the following methods may be used to assign network parameters:

- DHCP from a network server (default out-of-the-box option)
- A static IP configured through the maintenance port on the back of the Service Appliance.

The Service Appliance also requires a fully qualified domain name (FQDN) during configuration in MiVoice Connect Director. When configuring the service appliance, you must plan to use the following FQDNs:

- You must have an FQDN for each deployed service appliance
- You must configure you internal and external DNS server to point to the service appliance.
- The FQDNs must map correctly, both internally and externally, to the IP address of the service appliances.

See *Chapter 5, Installing Services Appliances on page 41* for more information about configuring the IP address.

Time Services

The Service Appliance requires a connection to time services in order to support Conferencing services.

The address of the NTP server can be provided to the Service Appliance through DHCP option 004 (if DHCP is used) or configured statically.

See the *MiVoice Connect Planning and Installation Guide* for detailed instructions on selecting an NTP public server if you do not run an NTP server within your organization.

Network Security

This section discusses network security concerns that can come up when you deploy Service Appliances.

Internal Firewall

Service Appliances can be deployed in the DMZ, allowing external participants to access web conferences. Positioning in the DMZ places the Service Appliance in a privileged security position within the customer's network infrastructure. Proactive security policies and strict management of evolving Internet security risks are essential to maintain network security.

Security Considerations

As security threats evolve new vulnerabilities may be discovered that require immediate resolution. Mitel provides upgrades to the appliance software and updates for critical security patches. If required, these upgrades are distributed independently from the standard release cycle for software upgrades.

Should critical security patches be required to the appliance operation or file systems, a mini-installer is used to implement immediate fixes to the platform images. This allows customer IT departments to quickly protect their networks without having to complete an entire release upgrade.

Hotfixes and patches for the appliance are incorporated into the next build or release.

Procedures to apply security patches to the appliance operating system and applications are described in the MiVoice Connect Maintenance Guide and are also distributed through e-mail or other customer notification pathways such as the Mitel support website.

Deployment Scenarios

The Service Appliance 100 and Service Appliance 400 may be deployed both internal to the LAN or externally in a company DMZ.

Deployment scenarios may include multiple installations of appliances in a Mitel system.

However, in any multi-appliance deployment scenario, if one appliance is accessible for external access then all appliances must be accessible for external access.

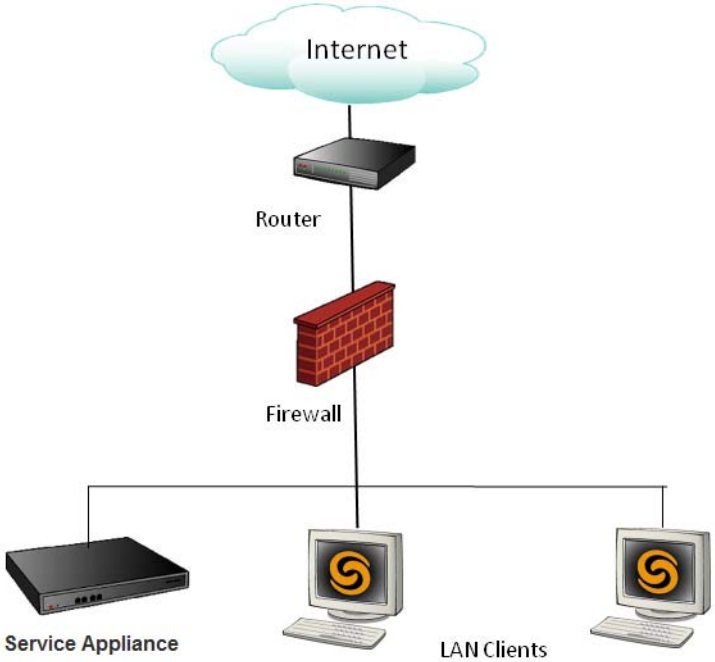
Deploying a Service Appliance in the LAN

In the scenario where a Service Appliance is deployed on the trusted internal network, the following requirements apply:

- The network requires port-forwarding through the firewall which is restricted to web ports (80-unsecure & 443-HTTPS). Alternatively, a reverse-proxy server can be used instead of port-forwarding but this requires the provision of an additional server.
- The network requires DNS configuration both internally to resolve internal addresses and externally to resolve to external addresses.
- Alternatively, a network can be configured with DNS configured for external addressing only and a host file configured to handle traffic internally.

The following figure shows deploying a service appliance in the LAN.

Figure 4.1: Deploying a Service Appliance in a LAN

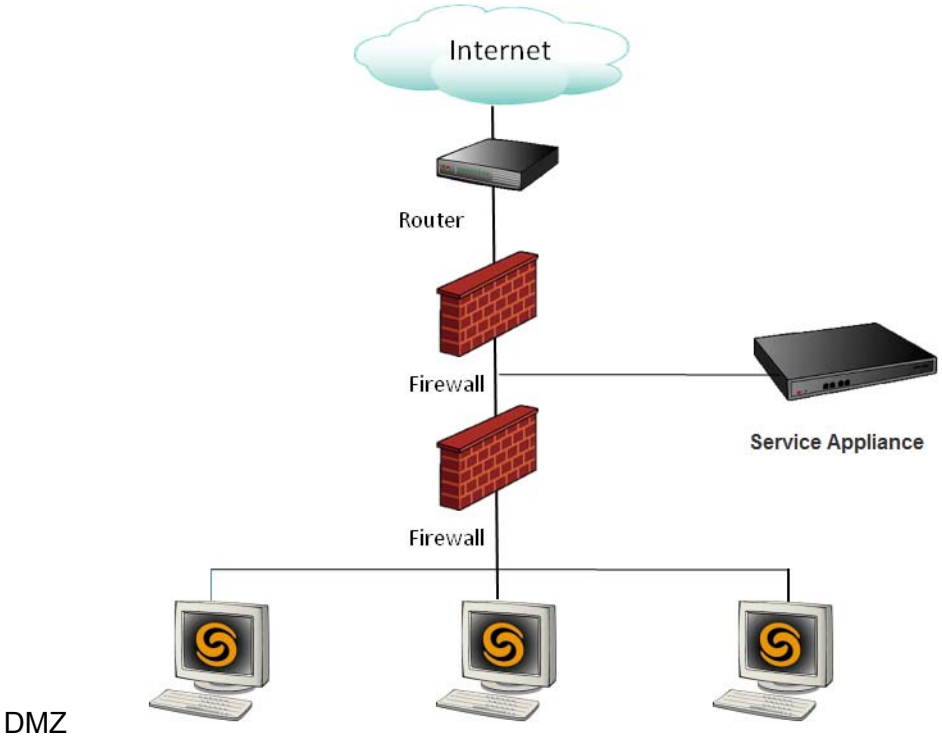


Deploying a Service Appliance In the DMZ

Deploying the Service Appliance in the demilitarized zone (DMZ) is the preferred method to facilitate external traffic. This requires the firewall between the DMZ and the LAN to be properly configured for Voice Switch ports as shown in Figure 2 .

NOTE: The Service Appliance will not function if it is positioned in the DMZ and network traffic initiated from the trusted zone to the Service Appliance goes through NAT (Network Address Translation). The Service Appliance will display a **Lost Communication** status in MiVoice Connect Director.

Figure 4.2: Deploying a service appliance in



Requirements

In the scenario where a service appliance is deployed in the DMZ, the following requirements apply:

- Enable routable traffic between the DMZ and LAN. Network Address Translation (NAT) can not be used for network traffic between these points.
- Adequate bandwidth between DMZ and LAN with a minimum of voice latency and jitter.
- DNS (Domain Name System) configuration to resolve both internal and external addresses. A DNS configured to external addressing only, with a host file configured to handle traffic internally, may be used as an alternative. The Service Appliance must be able to resolve the HQ Fully Qualified Domain Name (FQDN) using the DNS server configured for it.
- If a Service Appliance is made available from the Internet, all other Service Appliances need to be accessible and addressable from the Internet.
- The network requires port-forwarding through the firewall which is restricted to web ports (80-unsecure HTTP and 443-secure HTTPS).

To deploy a Service Appliance in the DMZ, follow these steps:

1. Configure your firewall to allow traffic from the IP address assigned to the Service Appliance to go through.
2. Ensure that the ports the Service Appliance supports are open. See the ports usage tables in the *MiVoice Connect Maintenance Guide* for information about the ports.
3. Set parameters for the range of ports for audio packets and the range of trusted IP address you want the Mitel system to recognize as valid from Service Appliances deployed in the DMZ.
4. Ensure that ports 80 and 443 are enabled from the WAN to the DMZ to ensure that uses can access the Service Appliance.

5. Ensure that the Service Appliance can communicate with the LAN by pinging the Service Appliance.

Best Practice Tests

You can use the following tests to verify the operation of the service appliance:

1. Configure a user for Conferencing.
2. Create a test conference and verify that audio users can join from both the LAN and WAN.
3. Verify users can join a web conference from both the LAN and WAN.
4. After the service appliance status is green on MiVoice Connect Director, go to any Mitel Phone and press the **Conference** button. The call should be routed to Conferencing, and you should be able to hear the conferencing prompts.

Site Requirements and Preparation

This chapter provides information about preparing your site for Service Appliance installation, including concerns such as physical space, environment, and cabling.

Recommendations

The following recommendations will assist you in planning and preparing your site for the Mitel system:

- Hire a cabling contractor to install your racks, patch panels, and cabling.
- Have two RJ-48C cables ready for each Service Appliance.
- Use surge protector or UPS.
- For remote deployment, your network should have 384 kbps bandwidth or better available between the FTP server and the remote Service Appliance for downloading upgrade software.

Specifications

Table 4 provides the specifications for the SA100 and the SA400:

NOTE: For Virtual Service Appliance specifications, see *Virtual Service Appliance Specifications*.

Table 5.1:SA100 and SA400 Specifications (Sheet 1 of 3)

Specifications	SA100	SA400
Application capacity		
Audio conferencing	Up to 50 simultaneous audio conferencing ports (including 15 HD calls)	Up to 200 simultaneous audio conferencing ports (including 15 HD calls)
Web conferencing	Up to 50 simultaneous secure Web conferencing ports (HTTPS)	Up to 100 simultaneous secure Web conferencing ports (HTTPS)
Instant Messaging	Up to 500 IM clients	Up to 2000 IM clients
Number of conferences	Up to 16 conferences	Up to 64 conferences
Hours of conference data	Up to 1000 hours of conference data	Up to 1000 hours of conference data
Networking/storage		
Hard Disk	2 x 500 GB	2 x 500 GB
RAID level	Level 1 (Mirror)	Level 1 (Mirror)

Table 5.1:SA100 and SA400 Specifications (Continued) (Sheet 2 of 3)

Auto-sensing, 10/100/1000 Ethernet interfaces	2	2
Ethernet fail-over	Yes	Yes
Maintenance		
Serial connector (DB9)	Yes	Yes
Power-on indicator	Yes	Yes
Hard drive activity indicator	Yes	Yes
Diagnostic indicators	Yes	Yes
System status indicator	Yes	Yes
Fan status indicator	Yes	Yes
System identification button	Yes	Yes
USB connectors	2	2
Slide-out system Identification panel	Yes	
Retention clip	Yes	Yes
Mechanical		
19" rack mount	Yes	Yes
Dimensions (HxWxD)	1.67 in (4.3 cm) x 17.09 in (43.4cm) x 15.5 in (39.4 cm)	1.7 in (4.3 cm) x 17.2 in (43.7 cm) x 23.5 in (59.7 cm)
Weight	17.8 lb (8.06 kg)	37 lb. (17 kg)
MTBF	53200 hours	60500 hours
Power/ Consumption Rates		
Power	250 Watts	650 Watts
Redundant power supplies		Yes
Input power	108 Watts @368.5 BTU per hour	280 watts@956 BTU per hr
AC input voltage	100-240 VAC	100-240 VAC
Rated Input Current	3A (115 V) to 1.5A (230 V)	8A (115 V) to 4A (230 V)
Rated Input Frequency	50-60 Hz	50-60 Hz
Consumption/dissipation	1039 BTU per hour maximum	2218 BTU per hour maximum

Table 5.1:SA100 and SA400 Specifications (Continued) (Sheet 3 of 3)

Environmental		
Operating temperature	10º to 35º C (50º to 95º F)	10º to 35º C (50º to 95º F)
Operating humidity	8% to 90% (non-condensing)	8% to 90% (non-condensing)
Storage temperature	-40º to 65º C	-40º to 70º degrees C

SA100 Specifications

The specifications in this section apply to the SA100.

Front Panel

This section provides information about the SA100 front panel. The below figure and the following table provide information about the SA100 front panel. In addition, a bezel is shipped with the unit that you can attach to the front panel and lock. The bezel blocks access to jacks on the front panel.

Figure 5.1: SA100 Front Panel Indicators and Connectors

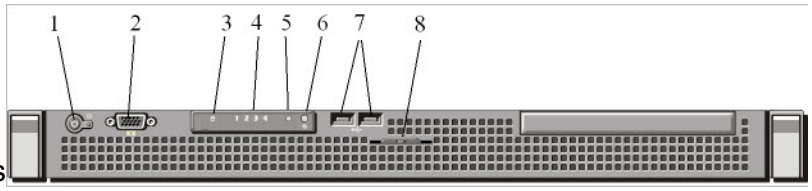


Table 5.2:SA100 Front Panel Indicators and Connectors (Sheet 1 of 2)

Item	Indicator, Button, or Connector	Description
1	Power-on indicator/power button 	The power-on indicator lights when the system power is on. The power button controls the internal power supply output to the system. When the system bezel is installed, the power button is not accessible.
2	VGA Connector	Not used.
3	Hard drive activity indicator	Lights up when the hard drive is in use.
4	Diagnostic indicator lights	The four diagnostic lights display error codes during system startup.
5	System status indicator	Lights blue during normal system operation. Lights amber when the system needs attention due to a problem.

Table 5.2:SA100 Front Panel Indicators and Connectors (Continued) (Sheet 2 of 2)

Item	Indicator, Button, or Connector	Description
6	System identification button	These front and back panel buttons can be used to locate a particular system within a rack containing multiple appliances. When a button is pushed, both front and back indicators light until the button is pushed again, allowing the specific appliance to be easily located.
7	USB Connectors (2)	Allows you to connect USB devices to the unit for system recovery. The ports are USB 2.0-compliant.
8	Slide-out system Identification panel	The top contains the product ID, part number and serial number. The bottom contains two MAC addresses for the two internal NICs.

Back Panel

This section provides information about the SA100 back pane. Figure 4 and Table 6 provide information about the SA100 back panel.

Figure 5.2: SA100 Rear Panel indicators and Connectors

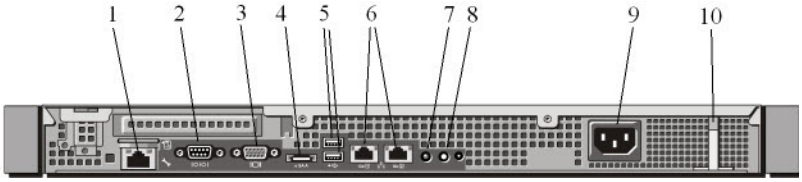


Table 5.3:SA100 Back Panel Indicators and Connectors (Sheet 1 of 2)

Item	Indicator, Button, or Connector	Description
1	iDRAC6 Enterprise port	Not used.
2	Serial connector (DB9)	Connects a serial device to the system. Used to configure static IP address.
3	VGA Connector	Not used.
4	eSATA	Not used.
5	(2) USB Connectors	Allows you to connects USB devices to the unit for system recovery. The ports are USB 2.0-compliant.

Table 5.3:SA100 Back Panel Indicators and Connectors (Continued) (Sheet 2 of 2)

Item	Indicator, Button, or Connector	Description
6	(2) Ethernet Connectors 	Supports 10base-T, 100base-T and 1000base-T connections.
7, 8	System identification button and indicator light 	These front and back panel buttons can be used to locate a particular system within a rack containing multiple appliances. When a button is pushed, both front and back indicators light until the button is pushed again, allowing the specific appliance to be easily located.
9	Power supply connector	Allows you connect power to the unit.
10	Retention clip	Secures the power cable.

Power Cable

Each SA100 ships with a power cable. If you do not receive the correct power cable for your environment, contact your Mitel partner or Mitel technical support.

NOTE: Mitel recommends that you connect the SA100 to a reputable surge protector or uninterruptable power supply (UPS).

Ethernet Ports

The SA100 uses an auto-sensing, 10/100/1000 Ethernet interface. Two RJ-48C Ethernet connections (GB1 and GB2) are provided to provide fault-tolerant deployment. The ports use the same MAC Ethernet address and IP address but are independent of each other and can be used in any sequence. However, when both ports are connected, only one will be active at a time. Should the active interface lose the link, the other interface is made active. You must use Category 5 or higher cabling.

The SA100 provides two methods of fault tolerance. To protect against Ethernet switch failure, connect Ethernet ports GB1 and GB2 to separate Ethernet switches. To protect against port or cable failure, connect LAN1 and LAN2 to separate ports on the same Ethernet switch.

Maintenance Cable

The SA100 provides a maintenance port that you can connect a terminal to using a DB-9, female-to-female, null-modem connector. You can use the maintenance port to assign the unit IP address parameters when DHCP is not used.

SA400 Specifications

The SA400 has the following characteristics:

- Sealed appliance
- Optimized for resiliency and security

- Designed to run Mitel services such as integrated Audio Conferencing, Web Conferencing, and Instant Messaging
- Can store up to 2000 hours of conference data—including reports, recordings, and library files—without backup (up to 1000 hours with backup active)
- Can be deployed anywhere, including in corporate DMZ
- Tested with well-known security tools for potential application and network vulnerabilities
- Managed entirely through MiVoice Connect Director
- Offers approximately 4x the capacity of the SA100
- Can be used with SA100(s) in the same system
- Licenses for the SA100 can also be used for the SA400 (audio and web conference licenses are unchanged)

SA400 Key Features

The SA400 provides the following key features:

- Processors: 2 Intel Hex-coreCPUs, Series 5600/5500 series, with QPI up to 6.4 GT/s
- Memory: up to 192-GB DDR3 1333/1066/800 MHz ECC registered DIMM/48-GB unbuffered DIMM. By default, the unit is shipped with 6 GB RAM
- RAM: 6 GB
- Hard drives: two Seagate Constellation.2 500-GB SATA 6.0 7200 64-MB 2.5-inch mirrored drives
- Left slot (full-height/full-length): one (x16) PCI-E 2.0 + 1 UIO
- Right slot (low-profile): 2-GB LAN optional (AOC-PG-i2+)
- Ethernet controller: Intel 82576 dual-port gigabit processor
- Hard drive bays: eight 2.5-inch bays (for customized storage). By default, the unit is shipped with two mirrored drives.
- Power supply: two 650-Watt, high-efficiency, redundant supplies

Front and Back Panels

The SA400 is one rack-unit (RU) high and can be installed in a standard 19-inch (48.26-cm) rack. Figure 5 shows the rear view of the SA400.

Figure 5.3: Rear View of SA400

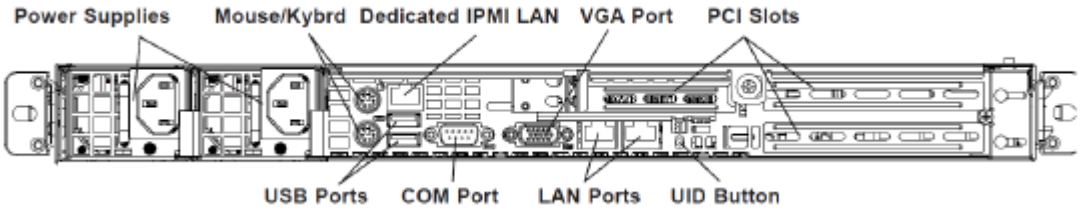


Figure 6 shows the front view of the SA400.

Figure 5.4: Front View of the SA400 with Bezel Attached

The front panel of the SA400 includes the following light indicators (left to right):

- Overheating/fan failure: Flashing = Fan failure. On continuously = Appliance overheated.
- Network activity on LAN2: Flashing = Network activity on LAN2.
- Network activity on LAN1: Flashing = Network activity on LAN1.
- DVD-ROM/hard drive activity: Flashing green = Hard drive activity. Flashing amber = Hard drive rebuilding. Solid red = Hard drive failure.
- Power to internal power supply units: Illuminated = System operating. Not illuminated = No power to internal power supply units.

Connection Specifications

The following table provides the connection specifications for the SA-400.

Table 5.4:Connection specifications

Port	Connection
Ethernet	• ETH0 • ETH1
Console	Serial

Power Input Specifications

The SA400 includes dual power supplies. To operate properly, you must plug both power supplies into an AC power source.

NOTE: If only one power supply is plugged in, a loud audio warning tone sounds when you turn on the SA400. The audio warning tone persists until you plug in both power supplies.

The power supplies have the following ratings:

- Rated Output Power: 650W
- Rated Output Voltages: +5 V (25 A), +3.3 V (12 A), +12 V (54 A), +5 VSB (3 A)

Virtual Service Appliance Specifications

One of the benefits of virtual deployments is that scale is essentially determined only by the compute power and memory of the host virtual environment. So a single virtual switch instance could in theory seamlessly scale from very small to very large capacities. A virtual service appliance has no inherent capacity, but its capacity is determined at initial run-time, based on its virtual machine's configuration.

NOTE: The Virtual Service Appliance OVA file must be deployed using VMWare vSphere client on a vSphere ESXi server, version 5.0 or higher.

Table 7 lists the audio capacity for various scales of virtual deployments.

Table 5.5:Virtual Service Appliance Audio Capacity (Sheet 1 of 2)

Scale of Audio Deployment	G.711/G.729	G.722	Maximum No. of Conferences
Small	50	15	25

Table 5.5:Virtual Service Appliance Audio Capacity (Continued) (Sheet 2 of 2)

Scale of Audio Deployment	G.711/G.729	G.722	Maximum No. of Conferences
Large	200	60	500

Table 8 describes the web capacity for various scales of virtual deployments.

Table 5.6:Virtual Service Appliance Web Capacity

Scale of Web Deployment	Max. Participants per Conference	Maximum No. of Conferences
Small	50	25
Large	200	100

Table 9 describes the IM capacity for various scales of virtual deployments.

Table 5.7:Virtual Service Appliance IM Capacity

Scale of IM Deployment	No. of IM Users
Small	500
Large	2000
IM only	2000

NOTE: Existing licenses for the SA100 and SA400 can also be used for a Virtual Service Appliance.

Environmental Requirements

To ensure optimum operating conditions for the Service Appliance, verify that the operating environment is adequately ventilated, free of gas or airborne particles, and isolated from electrical noise.

Installing Service Appliances

This chapter provides information about mounting Service Appliances in a rack, assigning the units an IP Address, and connecting it to the network.

NOTE: Unless otherwise specified, the instructions in this chapter apply to both the SA100 and the SA400.

Preparing for Installation

The section lists things that are recommended and required to install a Service Appliance.

- Computer mounting rack capable of supporting 1U equipment.
- Adequate clearance in the front and back of the rack to allow adequate ventilation.
- Surge protector or UPS.
- IP address to assign to Service Appliance.
- Mitel recommends that you assign a static IP address to all Service Appliances.
- IP address of the gateway that you want the Service Appliances to use.
- Subnet address that you want the Service Appliances to use.
- Computer with a terminal emulation program installed.
- DB-9 female-to-female, null-modem, serial cable.
- The IP network between the main and remote sites meets the bandwidth, latency, jitter, and packet loss requirements for a multisite installation.
- The IP network between the main and remote site has quality of service in place such that voice is prioritized ahead of data.
- You have appropriate firewall provisions in place, including VPN if applicable.
- All power and environmental requirements are met.

Verifying the Contents of the Box

This section lists the items you should receive in your Service Appliance package. Inspect the package carefully before you open it and contact the shipper if it is damaged. If items are missing from the package, contact your Mitel partner or Mitel technical support. The items in the box include the following:

- Service Appliance
- Either one power cord for the SA100 or two power cords for the SA400
- Rack mounting kit
- Front bezel kit
- MiVoice Connect Quick Install Guide
- Product Information Guide

Location Guidelines

Except when they are specified separately, these guidelines apply to both the SA100 and the SA400:

- Operating temperature: 10° to 35° C (50° to 95° F)
- Operating humidity: 8% to 90% non-condensing
- Adequate ventilation after the Service Appliances are installed

Installation

Follow the procedures in this section to install the Service Appliance.

Mounting the Service Appliance

The Service Appliance is shipped with a rack mounting kit that includes mounting instructions. The kit is designed to accommodate different types of equipment racks. Use the kit instructions to attach the rails to the Service Appliance and mount the unit in the rack.

NOTE: Ensure there is ample space between the front panel and back panel of the Service Appliance and any other surface to allow ample ventilation for the unit.

Connecting AC Power to the SA100

Service Appliances are shipped with a power cable that are appropriate for the location to which they are shipped. If you receive the wrong cable with the unit, contact your Mitel partner or Mitel technical support.

NOTE: Electrical surges in the AC line can damage unprotected equipment. Mitel recommends that you use an AC surge protector or a UPS to connect a Service Appliance to the AC line.

Press the power button on the front panel (see *SA100 Specifications*) to turn the unit on. The LED in the power button comes on and the SA100 performs its start-up process. The fan spins up and a sequence of numbers flash on the LED block on the front panel. The fan will quiet down and a solid LED appear when the process is complete. The process takes about 30 seconds. If the fan does not come on or the numbers do not flash, ensure that the power cord is plugged into the power source and the power source is working. If the appliance still fails to power on, contact your Mitel partner or Mitel technical support.

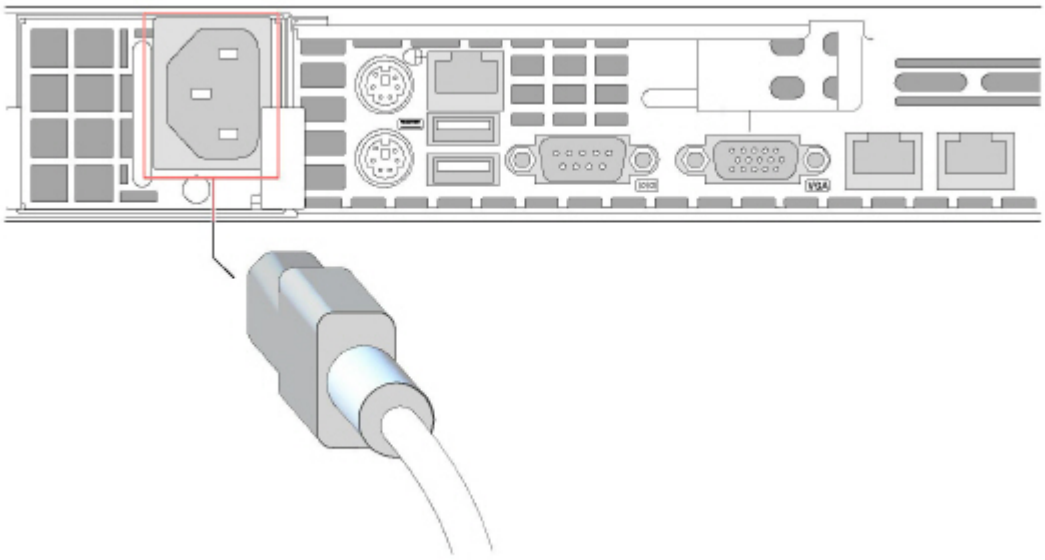
Connecting AC Power to the SA400

There are two power connections on the rear panel of the SA400 to ensure failover functionality.

To connect AC power, follow these steps:

1. Insert the female end of the power cord into one of the two power connections on the rear panel of the SA400. See Figure 7 .
2. Insert the other end of the power cord into an AC power source.
3. Repeat Steps 1 and 2 to connect the other power connector with an appropriate, separate AC power source for full failover functionality.
4. The SA400 automatically powers on.
5. As the SA400 starts up, messages display in the terminal emulation software window, if connected.

Figure 6.1: Connecting



Power

Setting the IP Address Manually

This section describes how to set the IP address on the Service Appliance manually. Mitel recommends that you use a static IP address for Service Appliance. You can also use DHCP to assign the unit an IP address. If you choose to use DHCP, you must configure the DHCP server with address information for the Service Appliance prior to turning on the unit. You can use the instruction provided in this section to obtain the Ethernet address of the unit.

NOTE: The Service Appliance is shipped from the factory configured to use DHCP to set IP address. That means that unless otherwise set, the first time the unit is turned on with an Ethernet cable connecting it to the network the unit will seek an IP address from the DHCP server on the network.

To configure the IP address manually, you need the following:

- Valid IP address for the segment in which you want to install the Service Appliance.
- Computer with terminal emulation software installed.
- Null modem DB-9 serial cable.

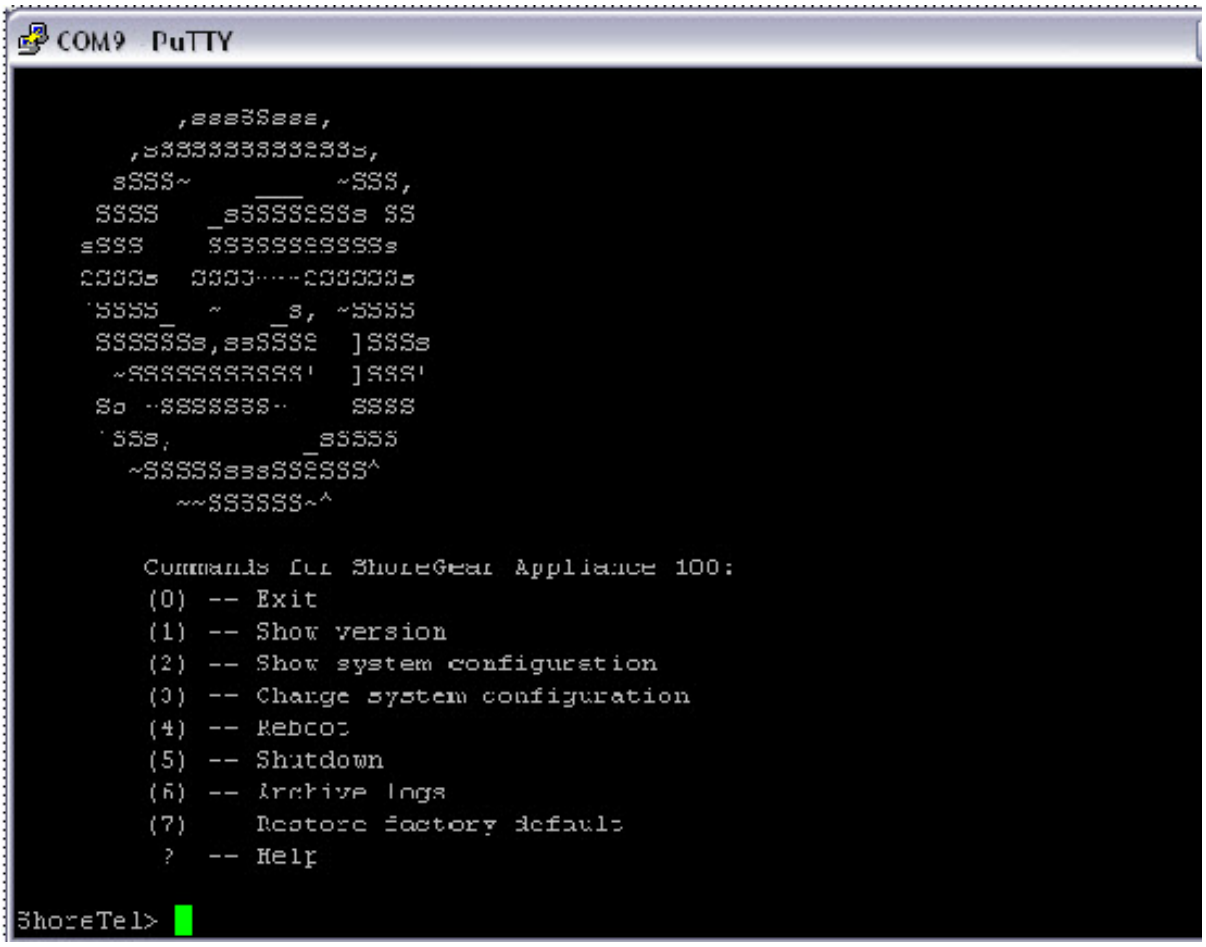
1. Connect the DB-9 serial cable to the serial port on the back panel of the Service Appliance and a computer.
2. Power on the Service Appliance and the computer.

   NOTE: The Service Appliance performs a start-up process when it is turned on. A sequence of numbers flash on the LED panel during start up, and a solid LED appears when the process is complete. The process takes about 30 seconds.
3. On the computer, start a terminal emulation program and set the following parameters:
   - Baud rate: 19200 bps
   - Data Bits: 8
   - Parity: None
   - Stop Bit: 1

– Flow control: None

4. At the Login prompt, type the user ID required to enter the CLI interface and press **Enter**. The default login name is **root**. The Password prompt appears.
5. At the Password prompt, type the password required to enter the CLI interface and press **Enter**. The default password is **ShoreTel**.
6. At the Linux prompt, type **stcli** and press **Enter**. The command-line interface as shown in Figure 8

Figure 6.2: Command Line Interface



NOTE: You can change the default CLI user name and password for the Service Appliance in MiVoice Connect Director. Refer to the MiVoice Connect System Administration Guide for more information.

7. Type **3** and press **Enter** to change the system configuration. The **Change System Configuration Menu** appears as listed in Table 10

Table 6.1:Change System Configuration Menu

Command	Description
(0)	Return to previous menu
(1)	Change IP address of the switch
(2)	Change IP subnet mask
(3)	Change gateway IP address
(4)	Change server IP address
(7)	Enable/disable DHCP
(8)	Change network speed and duplex mode
(D)	Set/change domain name
(F)	Set/change optional image server IP address
(M)	Set/change management IP address
(N)	Set/change management subnet mask
(P)	Set/change primary DNS IP address
(S)	Set/change secondary DNS IP address
(*)	Display current configuration
?	Display Help

Using DHCP to Set the IP Address

You can use DHCP to assign IP address information to the Service Appliance. If you want to use DHCP to configure the Service Appliance, be sure to configure the DCHCP server with information for the Service Appliance before you connect the unit to the network and turn it on. Doing so makes it easier to locate the unit on the network after the IP address is assigned.

To set DHCP to assign IP address information to a Service Appliance, follow these steps:

1. Specify a permanent lease for the Service Appliance.
2. Provide the Ethernet address of the Service Appliance to the DHCP server
3. You can use a terminal emulator as described in *Setting the IP Address Manually* to obtain the Ethernet address from the Service Appliance.
4. Ensure that the NTP server IP address is passed to the Service Appliance.

Refer to the documentation for the DHCP server for instructions on how to configure the DHCP server to set parameters on a network device.

Connecting the Service Appliance to the Network

Service Appliances are equipped with two Ethernet ports. The second port provides fault-tolerant protection by providing a second circuit for the unit to communicate with the network should a failure occur within the first circuit. You can connect both ports to the same network or connect the second port to a remote network. The first method provides protection in case cable or port fails. The second method provides protection in case the Service Appliance cannot communicate with the gateway to which it is assigned.

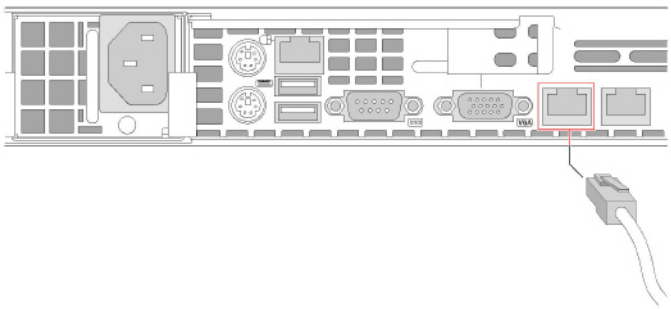
Connect Service Appliances to a device in your network, such as a switch, using the straight-through Ethernet cable provided with the Service Appliance.

NOTE: If you are using the Secure Remote Voice feature (a way to remotely generate a control signal prompted by an audible voice command), connect the second Ethernet port (ETH1) to an external network.

To connect the Ethernet ports, follow these steps:

1. Insert one end of the Ethernet cable to the network device.
2. Insert the other end of the Ethernet cable to the left Ethernet port (ETH0) on the rear of the Service Appliance. For the location of the ETH0 port on the rear of the SA400, see Figure 9 .
3. To implement failover with the unit, plug another Ethernet cable into the ETH1 port on the back of the Service Appliance and the other end into a different LAN segment.

Figure 6.3: Connecting the Ethernet Cable to the



SA400

Installing the Bezel

A locking front bezel and key are included with the Service Appliance. The bezel and fits over the front panel, blocking access to all items on the panel. Refer to the MiVoice Connect Quick Install Guide shipped with the unit for bezel installation instructions.

Configuring the Unit for Operation

After you have mounted the Service Appliance in a rack and connected it to the network, you must configure the Mitel system to use the unit. MiVoice Connect Director is used to configure the Mitel system to use the Service Appliance. For information about using MiVoice Connect Director to add a new Service Appliance, see the *Chapter 6, Configuring the Service Appliance on page 51*.

For information about using MiVoice Connect Director, refer to the *MiVoice Connect System Administration Guide*.

Installing the Virtual Service Appliance

The Virtual Service Appliance ISO file must be deployed by using VMware vSphere client on a vSphere ESXi server or Microsoft Hyper-V.

Refer to the *Installing the DVS Software: Linux* section in the *MiVoice Connect Planning and Installation Guide* for information about creating a new virtual machine for Virtual Service Appliance.

Table 6.2:Table 11: Virtual Service Appliance Requirements

Scale of Requirements	Processor	Virtual Cores	RAM per Virtual Machine	Disk Space	Network
Small	Intel Xeon E3-1275 v5 3.60 GHz	4	2 GB	100 GB	100 Base-T or Gigabit Ethernet
Large	Intel Xeon CPU E5-2630 v4 2.2 Ghz	8 a	6 GB	100 GB	Gigabit Ethernet
IM Only	Intel Xeon E3-1275 v5 3.60 GHz	2	2 GB	20 GB	Gigabit Ethernet

[a]The above numbers are the recommended guideline. You can allocate fewer virtual processor cores, but monitor the performance load to ensure that CPU utilization is less than 75 percent.

Configuring the Service Appliance

This chapter describes the procedures you must complete to configure and register your service appliance with the Mitel system. In this chapter, a service appliance can be an SA100, an SA400, or a Virtual Service Appliance (VSA).

Upgrading the Service Appliance Firmware

Service appliances require a firmware upgrade, which you initiate through MiVoice Connect Director.

Prerequisites

Upgrading the firmware of a service appliance located at a remote site requires a minimum bandwidth of 384 kbps between the appliance and the Mitel Headquarters server providing the upgrade firmware. If the minimum required bandwidth is not available, a remote upgrade may not be possible. The firmware upgrade requires 45 minutes at the minimum bandwidth; higher bandwidth reduces the upgrade time.

Configuration

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Maintenance** > **Status** > **Appliances**.

The list of service appliances and switches is displayed.

3. Select the service appliance you want to upgrade, and select **Upgrade** from the **Command** drop-down list.
4. Click **Apply**.The **Upgrade Switch Firmware** dialog box is displayed.
5. Select the version to which you want to upgrade from the drop-down list, and click **OK**.

The service appliance is upgraded to the selected version.

For more information on MiVoice Connect Director, see the *MiVoice Connect System Administration Guide*.

Configuring the Service Appliance

To configure the service appliance, use the following procedures:

- *Configuring the Network Time Protocol (NTP) Server*
- *Integrating the Service Appliance with the Mitel System*
- *Configuring a Service Appliance in the DMZ*
- *Configuring a Backup Service Appliance Site for the HQ Server*
- *Configuring a Remote Service Appliance and a Proxy Web Portal*

Configuring the NTP Server

The Network Time Protocol (NTP) server is used to synchronize the clock on the service appliance. The NTP server must be configured for every service appliance in a site.

NOTE: This procedure is required only for static IP addresses or DHCP configurations that do not already have a configured NTP server.

To configure NTP:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. Click the name of the site that contains the service appliance, for which you want to configure an NTP server. The information for the selected site is displayed on the **Details** pane.
4. On the **General** tab, in the **network time protocol server** field, enter the **IP address** of the NTP server.
5. Click **Save**.
6. Close MiVoice Connect Director and reboot the service appliance.

The date and time on the service appliance is synchronized with the date and time on the NTP server.

Integrating the Service Appliance with the Mitel System

This section describes how you can set up the Mitel system to use the service appliance.

Adding the Service Appliance to a Mitel Site

After you have installed the service appliance on the network, you must associate the unit with a Mitel site. To obtain the IP and Ethernet addresses for associating the unit with a site, see *Setting the IP Address Manually*.

NOTE: If the service appliance is installed inside the DMZ, ensure the following:

- The routable traffic between the DMZ and LAN is enabled.
- NAT is disabled.

To associate a service appliance with a Mitel site:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed. By default, the first site on the list is selected, and the relevant information is displayed on the details pane.
3. Click **New** on the list pane. The **Details** pane displays the **General** tab for the new site you are about to create.
4. In the **Site** drop-down list, select the site where the service appliance is physically configured.
5. In the **Hardware** type drop-down list, select one of the following:
   - Appliance 100 Collaboration
   - Appliance 400 Collaboration
   - Virtual Appliance Collaboration

6. On the **General** tab, enter the required information to register the service appliance with the Mitel system. See the following table for information about the parameters.
7. Click **Save**. The service appliance is successfully associated with the Mitel site.

Table 7.1:Service Appliance Addition Parameter Field Descriptions (Sheet 1 of 2)

Field	Description
Site (required)	The site where the service appliance is physically configured.
Hardware type	Select the hardware type from the drop-down list.
Name (required)	A name used to identify the service appliance.
Description	Type of service appliance. For example, UCB-VM.
IP address (required)	The IP address assigned to the service appliance. You can click **Find Switches** to select service appliances that are on the same network segment as the Headquarters server.
MAC address (required)	The Ethernet address (MAC address) found on the Mitel label on the back of the unit.
Server to manage switch (required)	The server that you want to use to manage the service appliance.
Is remote service appliance	If selected, indicates that the service appliance is remote.
Local call info number	The external phone number assigned to the service appliance to dial into a conference. **NOTE:** If the **Local Call Info** text is filled out, when displaying meeting info, the Local Call Number will be displayed in the Conference Viewer and Meeting invites.
Backup Section	
Enable daily backup	Enables the service appliance to perform a backup daily, if checked.
IP address	The IP address of the device to which you want the service appliance to back up files.
FTP port (required)	The port number that you want the service appliance to use for backup.
Directory	The URL for the directory to which you want the service appliance to back files up.
Username	The user name the service appliance must use to access the backup directory.
Password (Enter twice)	The password the service appliance must use to access the backup directory in both fields.

Table 7.1:Service Appliance Addition Parameter Field Descriptions (Continued) (Sheet 2 of 2)

Field	Description
Fully qualified domain name (required)	The complete domain name or IP address assigned to the service appliance.
HTTPS	Indicates if HTTPS is enabled or disabled for the appliance.
Extension	The internal extension number assigned to the service appliance to dial into conferences.
Assigned user group	Indicates the user group to which the service appliance is assigned.

Verifying Date and Time Synchronization

1. On the service appliance, open a secure shell (SSH) window.
2. Run the `date` command.
3. Verify that the date and time on the service appliance are synchronized with the date and time on the configured NTP server.

Configuring a Service Appliance in the DMZ

To configure a service appliance in the DMZ, you must configure it to be in compliance with the security parameters required for the network.

To configure the service appliance in the DMZ:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **System** > **Port Configuration**. The Port Configuration page is displayed.
3. In the **First UDP port** field, enter the first port number of the DMZ range that you want the service appliance to use.

The last port number in the range is automatically configured as the first port plus 10000. The default first port value is 1111. The default end port value is 11111 (1111+ 10000). The following table lists the ports that the service appliance supports.

Table 7.2:Service Appliance Port Address Ranges that Support DMZ Installation

Start	Stop	Start	Stop	Start	Stop	Start	Stop
20	–	123	–	5269	–	5455	–
21	–	443	–	5432	–	5457	–
22	–	833	–	5440	–	5461	5470
25	–	2427	–	5446	5450	5555	–
80	–	4308	–	5452	–		
111	–	5060	–	5454	–		

4. On the navigation pane, click **Administration** > **System** > **Trusted IP Ranges**. The **Trusted IP Ranges** page is displayed.
5. Do either of the following:
   - Select one of the default IP address ranges.
   - Click **New** to enter a new trusted IP address range as follows:
     i) Enter a suitable name for the range in the **Name** field.
     ii) Enter the lower limit for the IP address range in the **Low IP address** field.
     iii) Enter the higher limit for the IP address range in the **High IP address** field.
6. Click **Save**. The service appliance is successfully configured in the DMZ.

Configuring a Backup Service Appliance Site for the HQ Server

The service appliance provides services to users associated with the Mitel site where it is installed and to users of any site in the Mitel hierarchy that shares a branch with the installation site. Unless a service appliance is installed or configured on the Mitel Headquarters (HQ) site, all system users may not have access to service appliance services.

To ensure that all system users have access to service appliance services, when there is no unit installed on the Headquarters site, you can configure a backup site containing a service appliance for the Headquarters server. Configuring the backup site with the Headquarters server establishes a hierarchical branch that grants access to service appliance services for all users in the system.

To configure a backup service appliance site for the Headquarters server:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page is displayed.
3. On the list pane, select the **Headquarters site**. The configuration page for the Headquarters site is displayed on the details pane.
4. On the **General** tab, select a backup site in the **Service appliance conference** backup site drop-down list. By default, no backup site is selected.

   NOTE: The backup site can be a logical site.
5. Click **Save**. The backup site is saved for the Headquarters server.

Configuring a Remote Service Appliance and a Proxy Web Portal

Content for conference web pages is managed by the Headquarters server but distributed to endpoints through the local service appliances. When updates are made on the **Conference Options** page (see *Configuring the Conference Options Page*), the updates are first sent to the service appliance, which then distributes them to the endpoints for viewing. Situations where distance or network robustness cause network latency to exceed 100 ms between the Headquarters server and the service appliance can make rendering objects on the endpoints very slow. One possible remedy is to use a service appliance closer to the Headquarters server as a proxy web portal for the distant service appliance.

Because the proxy is closer to the source, the latency that occurs between the Headquarters server and remote service appliances is eliminated, allowing faster rendering of web pages.

First, we configure the proxy web portal by configuring a service appliance close to the source (Headquarters server). Then, you configure a remote service appliance to be used with this proxy web portal.

To configure a remote service appliance and a proxy web portal:

1. Install a service appliance near the Headquarters server, so that the latency between the two is less than100 ms. This automatically operates as the proxy web portal.
2. Identify a service appliance you want to configure as a remote service appliance.
3. Launch MiVoice Connect Director with administrative privileges.
4. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
5. Select the service appliance on the list pane that was identified in Step 2 as the remote service appliance. The details pane displays the relevant details for the selected appliance.
6. To specify that the system should not redirect calls to this service appliance during failover, enable the **Is remote service appliance** option on the **General** tab of the details pane. This selection informs the system to not redirect calls to this service appliance during failover.
7. Click **Save**.The selected service appliance is successfully configured as a remote service appliance.

Requests for the web portal by endpoints using this service appliance are redirected to the proxy web portal. If an appliance cannot perform as the proxy web portal, then the Headquarters server uses the remote service appliance.

Configuring Conferencing for a Service Appliance

To configure Conferencing for a service appliance, use the following procedures:

- *Configuring HTTPS*
- *Configuring Mitel Licenses*
- *Enabling Conferencing for Service Appliance Users*
- *Configuring a Conference Extension*
- *Configuring the Conference Options Page*
- *Integrating Conferencing with Microsoft Exchange*

Configuring HTTPS

Mitel supports HTTPS for securing conference calls. Secure web conferencing uses 2048-bit encryption.

To provide HTTPS security to conference users, you must upload Secure Socket Layer (SSL) certificates on each service appliance for which you want to provide HTTPS security. If you already have an SSL certificate, you can install it on your service appliance. If you do not have an SSL certificate, Mitel recommends that you purchase an SSL certificate from a reputable Certificate Authority (CA). To purchase a certificate, you must create a Certificate Signing Request (CSR) and send it to the CA.

- **NOTE:** If you do not obtain and upload a certificate, the system will automatically create a self-signed SSL certificate and private key.
- A self-signed certificate allows a service appliance to create and participate in HTTPS conferences, but because the certificate is not issued by a third party, HTTPS security is not optimized. When a

self-signed certificate is used, users trying to access the secure conference site will receive a warning message that states the security provided is not guaranteed.

Prerequisites

To configure HTTPS for web conferencing, you must have administrative privileges. For details, see the section on *Configuring Administrators* in the *MiVoice Connect System Administration Guide*.

Configuring HTTPS

Mitel recommends that you enable HTTPS on all of your service appliances. In web conferences where HTTPS is used, service appliances that are not configured to use HTTPS cannot communicate with service appliances that are using HTTPS and are not permitted to join the conference. HTTPS is enabled by default for new service appliances added to the network.

You can upload certificates for a single service appliance or for all of the service appliances currently installed on your systems depending on your certificate agreement.

To configure HTTPS on a service appliance:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. On the list pane, click the service appliance for which you want to configure HTTPS. The **Service Appliance Conference Administration** page is displayed.
4. Click the **HTTPS** tab. The HTTPS page is displayed.
5. In the **Enable HTTPS** section, determine if HTTPS is enabled, as follows:
   - If HTTPS is enabled, you see the message: **HTTPS is currently enabled on this service appliance**.
   - You can disable HTTPS, if required, by selecting the service appliance in the **Disable HTTPS on the following service appliance** drop-down list, and clicking **Go**.
   - If HTTPS is disabled, select the service appliance in the **Enable HTTPS on the following service appliance** drop-down list, and click **Go**.

NOTE: If you select **All** in the **Enable HTTPS on the following service appliance/Disable HTTPS on the following service appliance** drop-down lists, only the service appliances that are currently online are enabled/disabled. HTTPS is enabled by default for new service appliances added to the network. Mitel recommends that all the virtual service appliances on the system must be HTTPS or HTTP, but not a combination of both.

To create a Certificate Signing Request (CSR) to send to the CA, enter the parameters described in Table 14 in the *Create Certificate Signing Request* section.

Table 7.3:CSR Creation Parameter Descriptions (Sheet 1 of 2)

Parameter	Description
Country	Enter the two-character country code for the country where the system is installed. Refer to ISO 3166 for information about country codes.

Table 7.3:CSR Creation Parameter Descriptions (Continued) (Sheet 2 of 2)

Parameter	Description
State or Province	Enter the name of the state or province where the service appliance is installed.
Locality	Enter the name of the city where the service appliance is installed.
Organization	Enter the legal name of the organization or the person requesting the certificate.
Organizational Unit	Enter the name of the department that is requesting the certificate.
Common Name	Enter the fully qualified domain name (FQDN), for which you want the SSL certificate. **NOTE:** If the CSR is for a wild card certificate, you must prepend *. to the common name; for example, *.domain.com.
Email Address	Enter the email address of the administrator handling the certificate.

The Mitel system generates a CSR and a private key. The links to download the CSR and private key are sent to the email address mentioned in the *Create Certificate Signing Request* section.

6. Download the CSR and private key, and send to the CA. The CA sends you the authorized SSL certificate.
7. Do the following in the **Upload CA-Authorized SSL Certificate** section:
   - Select the **This is a wildcard certificate** option only if you want to send the CA-authorized SSL Certificate and private key to all service appliances in the system. If you select this option, the SSL certificate is uploaded even on new service appliances added to the network at a later stage.
   - Click **Choose File** in the **SSL Certificate** field to upload the CA-authorized SSL Certificate. This file is mandatory to complete configuring HTTPS.
   - If you received an Intermediate CA Certificate from the CA, click **Choose File** in the **Intermediate CA Certificate** field to upload the file.
   - If you have a second private key that was not sent to the CA in Step 6, you can click **Choose File** and upload it in the **Private Key** field.
8. Click **Upload**. The CA-authorized SSL certificate is uploaded to the service appliance.
9. In the **Restart the Web Server** section, click **Restart Web Server**. This reboots the service appliance and activates all certificates when the unit restarts.

Configuring Firefox Browser

Before you can use Firefox for Conferencing on service appliances enabled with HTTPS, you must disable the Transport Layer Security (TLS) setting to properly render web conference pages. TLS 1.0 can

downgrade the connection to SSL 3.0, thus weakening security, and hence this must be disabled for Conferencing.

To disable TLS in Firefox:

1. Launch the Firefox browser.
2. Type **about:config** in the address bar. Search for TLS settings by pressing **Ctrl+F**and entering **TLS**. The following TLS settings are displayed:
   - security.tls.version.max
   - security.tls.version.min
3. If the values for the TLS settings are equal to 1.0, right click the parameter, and click **Modify** to change the value to 0.0 or 3.0.
4. Click **OK** to save the setting. Firefox is successfully configured to launch Conferencing.

Configuring Mitel Licenses

Licenses are required for audio and web conferences. You must install an audio conference license and a web conference license for each audio and web conference participant you want the Mitel system to support. Each SA100 can support up to 50 simultaneous audio conference ports, 50 simultaneous web conference ports, and 500 IM clients. Each SA400 can support up to 200 simultaneous audio conference ports, 100 simultaneous secure web conferencing ports (HTTPS), 2000 IM clients.

Each Virtual Service Appliance type Small, Large or IM can support up to (VSA Small = 50 audio \ 50 web \ 500 – IM), (VSA Large = 200 audio \ 200 web \ 2,000 IM) (IM only = 2,000 IM). The actual capacity of a Virtual Service Appliance is determined at initial run-time, based on the configuration of the virtual device. The Mitel system can support up to 1000 audio conference ports, 1000 web ports, 10000 IM users, and up to 5 service appliances.

NOTE: For more information on the capacities for various scales of virtual deployments, see *Chapter 4, Site Requirements and Preparation on page 31*.

Registering and Downloading Conference License Keys

1. Contact your Mitel partner or reseller to purchase the licenses you require.

The Mitel partner or reseller provides you the licenses with the corresponding sales order number. If you do not receive a sales order number, but have the license keys, proceed to the *Installing the Licenses* section, complete the installation, and later register the licenses.

2. On the navigation pane, click **System** > **Security** > **Contact Information**. The **Contact Information form** is displayed.
3. Enter the information about the Mitel partner or reseller, the sales order number, and your primary contact.
4. Click **Now** to register your license. Your request for license registration is sent to Mitel for processing. Your license key is sent instantly to you.

Installing the Licenses

For information on installing the license, see *Installing a License Key* in the *MiVoice Connect System Administration Guide*.

Enabling Conferencing for Service Appliance Users

Conferencing users are Mitel system users with accounts that allow them to schedule and host conferences on a service appliance. For information about configuring Mitel user accounts, refer to the *MiVoice Connect System Administration Guide*.

To enable conferencing for service appliance users:

1. Launch MiVoice Connect Director with administrative privileges.
2. Click **Administration** > **Users**> **Users**. The Users page is displayed.
3. On the list pane, select the service appliance user for whom you want to enable conferencing. The details pane displays the details for the selected user.
4. Click the **Applications** tab.

NOTE: For information about configuring instant messaging, see the *Desktop Installation* chapter, in the *MiVoice Connect Planning and Installation Guide*.

5. In the **Conference Bridge Appliance** drop-down list, select the service appliance associated with the user.
6. Click **Save**. Conferencing is successfully enabled for the selected service appliance user.

NOTE: If you are not running proxy services in your network, we recommend that you disable the **Automatically detect settings Internet** option for Internet Explorer on the machines of conference users. This configuration can cause the Windows Presenter on user machines using a WiFi connection to take up to 30 seconds to load during conferences.

Configuring a Conference Extension

The Mitel system automatically assigns an internal extension to a system-wide conference number that is automatically generated. This is the number that all Mitel users can use to initiate or join a conference. You can change the extension manually and even use an external phone number for the conference extension.

Each service appliance that you install is also automatically assigned a Mitel extension. This number can be used by local users to access the unit to initiate conference calls. You can also change the extension number assigned to the unit.

The UCB global extension does not work, if the configured UCBs are offline. The call routing based on UCB global extension does not work until the offline UCBs are removed. This also applies for voicemail and DRS routing.

This section describes how to modify the extension and add an external number.

To modify the internal extension and add an external number:

1. Launch MiVoice Connect Director with administrative privileges.
2. On the navigation pane, click **Administration** > **Appliances/Servers** > **Platform Equipment**. The **Platform Equipment** page is displayed.
3. On the list pane, select the service appliance for which you want to modify the number. The details pane displays configuration information for the selected service appliance.
4. Select the **Collaboration** tab. In the **Extension** field, add or modify the extension number as required.

5. Select the **General** tab. In the **Local info call in number** field on enter a valid phone number you want to assign to the extension number.

NOTE: Ensure that the number that you enter is properly mapped to a telephony trunk. See the *MiVoice Connect System Administration Guide* for information about setting up trunks.

6. Click **Save**. The list pane displays the updated details for the selected appliance.

Configuring the Conference Options Page

You can configure the **Configuring Options** page to activate a tone that signals a user joining a conference, and set up a link for the conference.

If you access the **Configuring Options** page from a PC running Windows, ensure that your browser allows JavaScript to be downloaded and activated. JavaScript is required to display the **Configuring Options** page.

To configure the Conference Options page:

1. Launch MiVoice Connect Director with administrative privileges.

   NOTE: To add system administrative privileges to an existing user, see *Prerequisites*. To create new users, see the MiVoice Connect System Administration Guide.

2. On the navigation pane, click **Administration** > **Platform Hardware** > **Appliances/Servers** > **Platform Equipment**. The list of servers and service appliances is displayed.

3. Click the service appliance in the list pane, for which you want to configure conferencing. The Service Appliance Conference Administration page is displayed on a new window.

4. Click the **Conference Options** tab. The **Conference Options** page is displayed.

5. To select a logo for the conference, click **Choose File** in the **Logo** field, and select an image from your PC. The **Select File** dialog box is displayed. You can select an image you want to use as a logo for your conference.

6. Select the parameters described in Table 15 to configure the various options for conferencing.

Table 7.4:Conference Options Page Parameters (Sheet 1 of 3)

Parameter	Description
Alert Sound	Configures the alerts for users joining a conference. To enable sound alerts for the audio conference when a user joins the conference, select **Yes**. To disable sound alerts for the audio conference when a user joins the conference, select **No**.

Table 7.4:Conference Options Page Parameters (Continued) (Sheet 2 of 3)

Parameter	Description
Default Conference Type	Configures how a conference starts. You can select one of the following options: • Start the conference only when host joins • Start the conference when anyone joins • Start the conference when anyone joins and make everyone a presenter
Call Me Options	Configures how users to call into a conference. You can select one of the following options: • Enable Call Me • Enable Call Me for authenticated users or when host is present • Disable Call Me
Access Code Options	Configures access code assignments to the host/participant of a conference. If you do not select the following options, access codes are assigned by the MiVoice Connect system to the host and participant: • Enable Custom Host Access Codes • Enable Custom Participant Access Codes You can also configure the **Access Code Length** between a range of 4-12 digits

Table 7.4:Conference Options Page Parameters (Continued) (Sheet 3 of 3)

Parameter	Description
Access Code Error Detection	Configures error handling for access code entry attempts by a user signing into a conference. You can configure to Lock out IP after a number of failed attempts: • 5 • 10 • 30 You can configure the amount of time (seconds) granted to a user attempting to log into a conference: • 10 • 30 • 60 You can configure the amount of time (minutes) to wait before unlocking the IP of a user who has failed to sign in successfully to a conference with a valid access code: • 1 • 5 • 15 • 30

7. Click **Submit** to save your configuration.

Integrating Conferencing with Microsoft Exchange

Mitel provides an add-in that allows users to integrate Microsoft Outlook Calendar with Conferencing through Connect Client for Windows. See *Connect Client User Guide* for information on integration.

When Outlook add-in has been installed, the ShoreTel tab appears in the appointment window of the Microsoft Outlook calendar, which allows you to create meetings with Conferencing. Users can edit, delete, and make exceptions to the conferences that they create in Outlook. Information about Conferences is stored in the Mitel database for the service appliance and used to update the conference user interface.

NOTE: Use of the Outlook add-in is not dependent upon Exchange Server integration.

The connector that Mitel uses to connect service appliances with the Microsoft Exchange server is built into the Mitel server software and implemented through MiVoice Connect Director. The connector is designed to allow one service appliance to serve as an intermediary for the others. This unit will poll the Exchange server periodically and maintain the connection between the Exchange server and the Mitel system, which will update the other appliances as required. Data about the Exchange synchronization polling appears in the service appliance Maintenance page for this unit only.

The connector allows the system to poll the Exchange server for updates to existing conferences. Conference data that has changed in Outlook Calendar is updated in the Connect client. Newconferences are not added to the Mitel database during polling, but about the time they are created in Outlook Calendar. Polling intervals are based on the number of Outlook Calendar users your system supports. For every 500 users, the system adds 30 minutes to the polling interval. For example, for systems that have 500 users the polling interval is every 30 minutes. For systems that have up to 1000 users the polling interval is 60 minutes. For systems that have 5001 users the polling interval is 720 minutes (12 hours).

Enabling the Connector for Microsoft Exchange Integration

You can use the connector for a single Microsoft Exchange Server. Connections with multiple Exchange Servers are not supported. If you are upgrading or migrating the Exchange Server and have multiple Exchange Servers, Mitel recommends that you disable the Exchange connector before you start the upgrade or migration.

Prerequisites for Enabling the Connector

- Configuration of an Exchange user for Conferencing. This must be a privileged user able to query data for other Exchange users.
- Configuration of a Microsoft Exchange Server 2010 or Exchange Server 2013 SP1 and above.
- Exchange e-mail address for end users.

To enable the Connector for a Microsoft Exchange user:

1. Launch MiVoice Connect Director with administrative privileges.
2. Click **Administration** > **System** > **Other System Parameters**. The **Other System Parameters** page is displayed.
3. Select the **Enable Exchange connector** box in the **Service appliance** section.
4. Enter the URL or the IP address of the Exchange Server in the **Exchange server** field in the **Exchange server** section.
5. Enter the user name used for the user's Outlook mailbox in the **Username** field.
6. Enter the password associated with the Outlook user in both **Password** fields.
7. Click **Save**.

   NOTE: The connector uses the Primary SMTP Address of the user to authenticate access to the Exchange Server. If the user or an administrator changes the e-mail address, the connector will not be able to access the account of the user, and the user will not be able to synchronize Outlook with the service appliance.
8. Click **Administration** > **Users** > **Users**. The **Users** page is displayed.
9. Select the user on the list pane, whose Outlook account you configured with the connector. The details pane displays details of the selected user.
10. Enter the Microsoft Exchange Primary SMTP Address assigned to the user in the **Email address** field in the **General** tab.
11. Click the **Applications** tab. The Conferencing and Instant Messaging service appliances can be configured on the **Applications** tab.

12. Select the service appliance that you want the user to use for Conferencing in the **Conference bridge appliance** drop-down list.
13. Click **Save**. Conference sessions are recorded in Microsoft Outlook calendar and the Conference page for the user on the Conferencing portal.

Going Live and Training

This chapter provides the requirements and other information for introducing the Service Appliance 100/SA400, Virtual Service Appliance, and Conferencing services to your organization.

Complete Operational Testing of Service Appliances

After you have installed the Service Appliance, you should test the system to make sure that conferencing and IM services are working properly before making them available to the community. Testing should include the following tasks for both single appliance and multi-appliance installations:

- Verify the Audio Conference service can be accessed on each appliance by dialing the audio conference extension and then by pressing the conference button on a user's IP telephone.
- Verify a user's conference is hosted on their assigned Service Appliance.
- Verify the Global Audio Conference extension routes users to the closest appliance relative to the caller. Verify that once the User enters the conference access code, the call is routed to the appliance that is hosting the conference.
- Verify external callers can access audio conferences through the external numbers established for audio conferencing access.
- Verify default music on hold (MOH) is broadcast from each appliance to a caller using that appliance.
- Verify both internal and external Web participants can access the conference website and enter and participate in Web conferences.
- Verify the Conferencing service can successfully out-dial to selected participants during conferences, both during participant login as well as when directed by the conference host.
- Verify Outlook integration is functioning properly by scheduling and accessing Mitel meetings with Outlook appointments.
- Verify Connect Client integration is functioning properly through the ability to schedule and access Web meetings (both scheduled and Instant) from the Client.
- Verify Instant Messaging Presence, Privacy and IM chat capabilities function correctly.

For multi-appliance installations, the following additional tasks should be accomplished:

- Simulate overloaded conditions to verify a user's conference is distributed to other, less loaded appliances.
- Verify conferencing failover capabilities function correctly by scheduling conferences, disconnecting a user's assigned appliance and then starting the conference.
- Verify IM users assigned to one Service Appliance can successfully initiate IM sessions and exchange presence information with user assigned to other Service Appliances.

Assign Users to Each Service Appliance

Make sure that the Mitel users you want to be able to create and host conferences or use instant messaging services are assigned to a Service Appliance. For information about assigning Mitel users to a Service Appliance, see *Chapter 6, Configuring the Service Appliance on page 51*.

Verify Licensing

To enable Conferencing for all required users and to avoid a potential access lockout, the following should be performed:

- Ensure adequate audio conference and Web conference licenses are purchased to allow all authorized users concurrent access to Conferencing services.
- Ensure each user with IM access has been configured with Connect Client Professional access level, and that a keyed license is entered into the system for each of those access levels. This will ensure the Mitel system does not lock out Administrator access due to inadvertent license violations.

Distribute User Guides

The following end-user information is available:

- The *Connect Client User Guide*: This guide contains detailed information on all features available with Conferencing services and also detailed instructions on each feature's use. This guide is available for download from the Mitel Partner support site and from within MiVoice Connect Director, under the Documentation Menus.
- The *MiVoice Connect Conferencing Quick Reference Guide*: This short guide contains helpful references to quickly enable a user to gain comfort using the most frequently accessed features. This guide is available for download from the Mitel Partner support site and from within MiVoice Connect Director, under the Documentation Menus.

Training

Mitel is committed to ensuring our customers have the tools and knowledge base they need to take full advantage of the capabilities offered with the installation of a Service Appliance and Conferencing features, as well as the entire Mitel system.

It is critical that all users be familiar with Conferencing services before the system is placed into production.

Ensure to consider training needs as personnel staffing changes over time.

Online training for Service Appliance and Conferencing services includes the following:

- Installing, Administering and Using the Service Appliance 100 and Service Appliance 400, an online, virtual live-training class administered by Mitel.
- Using Conferencing, an online self-paced training course designed to familiarize users and administrators with the capabilities and use of all Conferencing features.

For more information, please contact your Mitel-authorized partner or visit the Website http://www.shoretel.com/training.

Backup and Restore

This chapter describes the process for enabling automatic backup of Service Appliance files and data. Should an appliance experience a catastrophic failure or a data corruption, the availability of regular backup files can simplify recovery and minimize the cost of such a failure.

Service Appliance Backup

Mitel recommends that you back up your Service Appliances daily to protect critical data. This feature is not meant as a method of archiving or as a method for retrieving accidentally deleted files.

The files containing user library data, conference recordings and user images, collectively referred to as content files should be backed up on a daily basis.

Backup can occur while conferences are in progress including the files of any conference currently in progress. However, only files that are not being modified will be backed up to protect data integrity.

When the back up process starts, library content upload will be disabled. Library content currently in the process of uploading will be allowed to complete before the back up starts. Once back up is complete, upload of library content is re-enabled. If the user attempts to upload content while the upload is disabled, they will see a message indicating that upload is temporarily unavailable.

Any machine capable of supporting an FTP server can be the target of a backup. The FTP server must be RFC 959 compliant and additionally support the commands MDTM and SIZE. The FTP servers on most versions of Microsoft Windows meet these requirements, including Windows Server 2008 and Windows Server 2012.

If multiple appliances are backing up to the same FTP server, the target directory should be configured differently for each appliance.

An on-demand backup can be performed on demand by establishing an SSH or serial connection to the appliance and then using CMCA ServicesMgr command line interface (svccli) commands.

The backup will only execute if backup is enabled. See the *MiVoice Connect Maintenance Guide* for detailed instructions for executing an on-demand backup.

To avoid bandwidth issues, be aware that Mitel recommends the you install Service Appliances on the same network as the FTP backup server.

NOTE: The Service Appliance can generate more than 1 GB of data files per day and easily have more than 100 GB stored internally.

Before you begin, ensure your system meets the following requirements:

- Ensure that the FTP server is configured to allow the Service Appliance to access and write to it.
- Ensure that port 21 is open and available on the FTP server for the Service Appliance to use. (Port 21 is often blocked.)

For more information about configuring automatic backup for Mitel services and devices, refer to the *Voicemail Model Switches* section in the *MiVoice Connect System Administration Guide*.

To configure the Service Appliance to perform automatic backups using an FTP server, follow these steps:

1. Launch MiVoice Connect Director.
2. Select **Administration** > **Platform Hardware** > **Voice Switches / Service Appliances** > **Primary**. The **Primary Voice Switches/ Service Appliance** page appears.
3. In the Name column, select the **Service Appliance** that you want to configure for backup. The **Edit Service Appliance** page appears.
4. Scroll down to the Backup section and do the following:
   a. Check the **Enable Daily Backup** check box.
   b. In the **IP Address** field, enter the IP address of the FTP server that you want the unit to use for backup.
   c. In the **FTP Port** field, enter port number that you want the Service Appliance to use to connect to the FTP server. The default value is **21**.

      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.
   d. In the **Directory** field, enter the name of the directory to which you want the Service Appliance to back up files on the FTP server. This file will be create the first time a back up is run.
   e. In the **User ID** field, enter the user name that you want the Service Appliance to use to login to the FTP server account for backup.
   f. In the **Password** fields, enter the password the Service Appliance needs to use to login to the FTP.

Service Appliance Restore

There is not a MiVoice Connect Director utility for the purpose of restoring Service Appliance content.

Restore is performed on demand through establishing an SSH or serial connection to the appliance and then using CMCA ServicesMgr command line interface (svccli) commands.

Restoring will copy the content files from the previous backup into the appliance. During restore all appliance services will be stopped.

The restore can occur on non-empty directories, but will not delete files that are in the file system but not part of the last back up. Files that are created after the previous back up remain intact. However, files that have been modified since the previous backup will be replaced by the backup version.

Files that have been deleted since the previous backup will be restored into the appliance but will not be accessible as the database links to deleted files are not maintained. If these files are required, they can be retrieved by establishing an SSH or serial connection to the appliance and retrieving them manually.

Restore procedures are considered non-routine and are not detailed in this guide. For detailed instructions, see the *MiVoice Connect Maintenance Guide*.

Mitel
Powering connections

mitel.com