A MITEL
PRODUCT
GUIDE

MiCollab MSL Server Manager

Release 10.2

December 2025

Mitel
Powering connections

Notices

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

Trademarks

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

Contents

Getting Started 1

This chapter contains the following sections:

1.1 About MiCollab

MiCollab is a software and hardware solution that allows you to

- install multiple Mitel applications on a single server, and
- manage the server and the installed applications from this web-based administrator portal.

MiCollab and the installed applications provide services (voice mail, for example) to the users on a Mitel MiVoice Business, MiVoice Office 400, MiVoice 5000, or MiVoice MX-ONE communication platforms. In addition, MiCollab provides users with a personal web-based end-user portal (MiCollab End User Portal) that allows them to modify the settings of their installed applications.

Several configurations of MiCollab are supported. Refer to the *MiCollab Engineering Guidelines* for details about these configurations. The server settings that you need to configure from this administrator portal depend on your application requirements and your network configuration.

1.2 What's New in This Release

MSL Release 12.0

MSL Release 12.0 provides the following new features:

- MSL Release 12.0 now supports TLS 1.3 along with TLS 1.2

> **Note**: TLS 1.1 and TLS 1.0 are no longer regarded as secure and not supported by MSL 12.0

MSL Release 11.0

MSL Release 11.0 provides the following new features:

- The server manager **Shutdown or Reconfigure** panel has been renamed to **Shutdown or reboot**. The Reconfigure option in that panel has been removed.
- The server manager **Web Server** panel has a field for entering Subject Alternate Names (SANs) for the server, when generating a Certificate Signing Request.
- The server manager **Hostnames and addresses** panel does not comprise invalid host names section, and the **Review configuration** panel does not comprise server names section such as mail.domain, ftp.domain, www.domain, and so on.
- When running MSL on EX platform, the option to restore from removable media or another running server are not available.
- MiCollab and MBG supports licensing through the Licenses & Services Application (License Server). The Mitel Licenses & Services Application manages the software licensing and entitlement of the Software Assurance Program. After you obtain a ServiceLink ID or Serial ID from the License Server, the License Server uses your ServiceLink ID to provide you with access to licenses, software releases, and upgrades.
- To activate an License Server Serial ID the following connections must be allowed through any firewalls.
  - FQDN: sync.sls.mitel.com, Current IP: 18.200.183.29 Port: 22 Protocol: SSH
  - Customer must verify current IP before creating firewall rules as the IP address may be subject to occasional change.
- **Supported Upgrade Methods**: MSL 11.0 is available only as a 64-bit distribution. Migration from a 32-bit to a 64-bit system requires a fresh software installation, either manually or using the new Remote Fresh Install blade.
- The application blade software is no longer downloaded from the License Server but the License Server still provides software licensing. MSL 11.0 uses the Mitel Software Download Center, supported by a global content distribution network to increase speed and reliability of downloads. The following outbound connections must be allowed through your firewall: License entitlement: register.mitel-sls.com 216.191.234.91 port 22 sync.mitel-sls.com 216.191.234.91 port 22 Access token for content delivery network: swdlgw.mitel.com 99.81.17.20 port 443 (occurs during available blade software list update) Content delivery network for blade software download: swdl.mitel.com port 443 (IP address based on location)
- Note: For the Akamai FQDN swdl.mitel.com, the static IP address ranges cannot be guaranteed by the Content Delivery Network. Thus, any firewall rules should allow the FQDN. The following table outlines the supported upgrade methods: Upgrading from… Upgrading To... Supported Upgrade Methods 10.x releases (32-bit or 64-bit) 11.0 (64-bit) Fresh Install from CD/DVD/USB Remote Fresh Install 9.x releases (32-bit) 11.0 (64-bit) Fresh Install from CD/DVD/USB Cloud Platform Support: The following features are supported on the Azure platform: Hostname: The default hostname will be the lower case VM name. Any invalid hostname characters, such as periods or underscores, will be translated to hyphens Networking: MSL supports auto-provisioning of network elements, such as NICs, public/private IP addresses, gateways, routing and DNS On every reboot, which includes following a restore operation, the VM networking is analyzed and auto-provisioned if any changes are detected. Supports auto-registration of the VM hostname in a private DNS zone linked to the virtual network of the primary (first) NIC. Only the primary (first) private IP linked to the NIC is registered. So, if the configuration console changes the hostname, the private DNS entry will be updated accordingly when the reboot occurs. Supports custom data when creating a VM. Note:Refer to Cloud Platform Support in the Mitel Standard Linux Installation and Maintenance Guide for more information. Backup and Restore using AWS S3 buckets: Now, backups to the network file server and restoration of the backed up files stored in the network File Server can be processed using HTTPS through Amazon Web Services Simple Storage Service (that is, AWS S3). Note: Refer to Backup and Restore topics for more details.

1.3 Logging In

The Username and Password for the administrator portal are set from the server console during installation. The *MiCollab Installation and Maintenance Guide* provides complete instructions.

Instructions for logging into the administrator portal are also provided below:

1. Open your browser.

> **Note**: The following browsers are supported: Microsoft Edge 115 or higher, Google Chrome version 115 or higher, and Mozilla® Firefox® 115 or higher. Note that Flow Through Provisioning and Reach Through functionality are only supported in Firefox browser.

2. Enter the following URL:

   https://<Fully Qualified Domain Name of the MiCollab server>/server-manager
3. A security alert may appear. Click **Yes** to accept the security certificate.
4. Enter your Username and Password and click **Login**.

   - Default Username is "admin"
   - Password is set during installation

> **Note**: The default timeout for a Server Manager session is two hours.

5. You will be prompted to change the password immediately on first login. Enter and verify the new password and click **Change Password**.
6. Click **OK** to login to the Server Manager.

Click the Help link in the administrator portal for instructions about performing administration tasks and adding users. When you add a new user, the system is configured to automatically send a Welcome e-mail to the user's e-mail address. The Welcome e-mail provides the user with his or her account information and the URL of the MiCollab End User Portal :

https://<Fully Qualified Domain Name of the MiCollab server>/portal

> **Note**: For more information about the End User Portal, refer to the online help provided in the portal interface.

1.4 About the MiCollab Administrator Portal

This web-based portal allows you to

- configure server settings

- administer the Mitel applications that are installed on the MiCollab server
- maintain the server

1.5 About the Documentation Set

All Mitel product documentation is available at Mitel Online. You must be a registered user.

To access product and technical documentation on Mitel Online:

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From the left menu, select **Docs Center**.
3. Click **Applications** > **Collaboration** and then select **MiCollab**.
4. To view a document, click the document title.
5. To download a document, right-click on the name of the document, and click **Save Target As**.

> ℹ **Note**: To view online help, ensure that Compatibility view is enabled for your browser.

MSL Documentation

- **MSL Installation and Administration Guide**: provides platform requirements, software installation instructions and maintenance and troubleshooting procedures
- **Server Manager Online Help** (this online help): provides the administrator with instructions for configuring the MSL server

MiCollab Documentation

- Installation and Maintenance Guide: provides platform requirements, software installation instructions and maintenance and troubleshooting procedures.
- Platform Integration Guide*:* provides instructions on how to configure the MiVoice Business, MiVoice Office 250, MiVoice 5000, and MiVoice MX-ONE communication platforms to support the MiCollab applications.
- Engineering Guidelines: highlight specific areas of the product that you must consider before installation. Use them to plan site installations.
- Administrator Portal Online Help: (this online help) provides the administrator with instructions about configuring the MiCollab server and maintaining the applications.
- MiCollab End User Portal Online Help: provides end users with instructions about setting up and using their MiCollab applications.

End-User Guides

- Messaging User Guide
- TUI Quick Reference Guide
- Competitive TUI Voice Mail User Guide
- Competitive TUI Quick Reference Guide

MBG (formerly MiVoice Border Gateway)

- Remote Phone Configuration Guide

MiCollab Client

Engineering and Administrator Documentation

- MiCollab Client Advanced Engineering Guidelines: provides system requirements, configuration information, network diagrams, virtualization information, performance recommendations, system capacities.
- MiCollab Client Administrator Guide: includes PBX configuration information, Unified Communications specifications and hardware configuration information, and configuration information for integrated applications.
- MiCollab Client Administrator Online Help: provides a high-level overview of the provisioning process with links to task-related instructions. The task-related instructions provide detailed descriptions for fields and options.

End-user documentation

- MiCollab Client end-user online help: provides basic feature and usage information for the PC Client, Web Portal, MAC Client, and Mobile Client.
- Online Help for supported clients: embedded in the user interfaces, the help systems describe the interface elements, supported features, and provide task-related instructions

MiCollab Audio, Web and Video Conferencing (formerly Mitel Collaboration Advanced)

- Web Conferencing and Remote Support Installation Manual: provides installation instructions and maintenance procedures.
- MiCollab Audio, Web and Video Conferencing User Guide: contains end user information and procedures for Mitel Collaboration Advanced.
- MiCollab Audio, Web and Video Conferencing Online Help: provides administration and programming procedures.

License Server

- See the online help in your License Server Account

1.6 Contacting Technical Support

Contact Mitel Technical Support if you require technical assistance. Before you call, check this Help system for tips and solutions. If you are unable to find a solution, please have the following information ready when you call:

- The MiCollab MSL software revision
- The nature of the problem
- What you were doing with the application when the problem occurred
- Troubleshooting results

For information about contacting Mitel Technical Support, access Mitel Online at http://www.mitel.com.

1.7 Disclaimer, Trademarks, and Copyright

Disclaimer

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.

Copyright

Performing Administration Tasks 2

This chapter contains the following sections:

- Configure the Server Settings
- Administer the Applications
- Maintain the Server
- Assign Local Administrator User

2.1 Configure the Server Settings

1. Configure Server Date and Time
2. Configure Remote Access Settings
3. Install and Upgrade Applications
4. Install Blades
5. Grant Network Privileges
6. Configure Port Forwarding
7. Add Hostnames and Addresses
8. Configure Email settings
9. Configure Internal DHCP server
10. Configure Proxy Settings
11. Manage Client Certificates
12. Install Web Server Certificate (optional)
13. Manage TLS Protocol
14. Configure PPTP Settings (Client-to-Server VPN)
15. Add ICPs
16. Change LDAP Directory Settings
17. Configure SNMP support
18. Manage Domains
19. Set System Information Access
20. Configure Traffic Shaping
21. Review Server Configuration
22. Configure MiCollab Settings
23. Set MiCollab Language
24. Run MiCollab Client Integration Wizard (if required)
25. Configure Flow Through Provisioning or Add or Edit Network Elements if Flow Through Provisioning is not supported
26. Run the Reconcile Wizard (if required)
27. Configure IDS on MiCollab (optional)

2.2 Administer the Applications

1. Provision Users and Services
2. Perform MiCollab Audio, Web and Video Conferencing Administration
3. Perform MBG Administration

   or Remote MBG Administration
4. Perform NuPoint UM Administration
5. Perform MiCollab Client Service Administration
6. Configure Service Info E-mail

> **Note**: For details on MBG administration, navigate to the online help from the MBG application.

2.3 Maintain the Server

1. Configure MSL Web Services
2. View ServiceLink Status
3. View Log Files/Collect Log Files
4. View Event Logs
5. View System Information
6. Access System Monitoring Tools
7. Manage System User Accounts for Remote Access
8. Backup or Restore Server Data
9. Shutdown or Reconfigure Reboot

2.4 Assign Local Administrator User

You can assign the "Local Administrator" login to a single system user who can then perform a subset of the MiCollab administrative functions. Local Administrator permission allows adding/editing users, phones, and services. The account name " local-admin" is created when MiCollab is installed. To assign a user to this account, modify the existing information.

Two email pseudonyms are automatically created for the Local Administrator user: < firstname.lastname> and < firstname_lastname>.

The Local Administrator will access the Administrator Portal in the same way as the System Administrator, but will see a limited subset of administrative tasks.

To assign Local Administrator privileges:

1. In the server manager menu, under **Administration**, click **System users**.
2. Click the Modify link associated with the local-admin account.
3. Enter the name and address information for the Local Administrator user. (Note: Department information is not linked to the "Department" field in the User Services and Provisioning application.)
4. Click **Save**.

> ℹ **Note**: Newly-created accounts are locked until the password is entered/changed.

To set or reset the Local Administrator password:

1. In the server manager menu, under Administration, click **System users**.
2. Click the Reset password link associated with the local-admin account. Passwords must contain at least one upper case letter, one lower case letter, one number, and one non-alphanumeric character, and be at least 7 characters long.
3. Enter the new password and then confirm by entering again.
4. Click **Save**.

To lock the Local Administrator from account access:

1. In the server manager menu, under Administration, click **System users**.
2. Click the Lock account link associated with the local-admin account.
3. Click **Lock** to confirm.

> ℹ **Note**: A locked account is unable to log in or collect email. You can unlock the account by resetting the password.

To view local-admin user's access logs:

1. In the server manager menu, under Administration, click **View log files**.
2. In the **Choose a log file to view** list, select **httpd/ admin_access_log**.
3. In the **Filter Pattern** field, enter **local-admin** and then click **Next**. There may be multiple httpd/ admin_access_log.yyyymmddhhmmss files. The timestamp indicates the ending timestamp for the logs in that file.

ServiceLink (On-Premise Only) 3

This chapter contains the following sections:

3.1 Install and Upgrade Applications

ℹ **Note**: ServiceLink is not supported for MiCollab deployments in MiCloud Flex on GCP (Google Cloud Platform) environment.

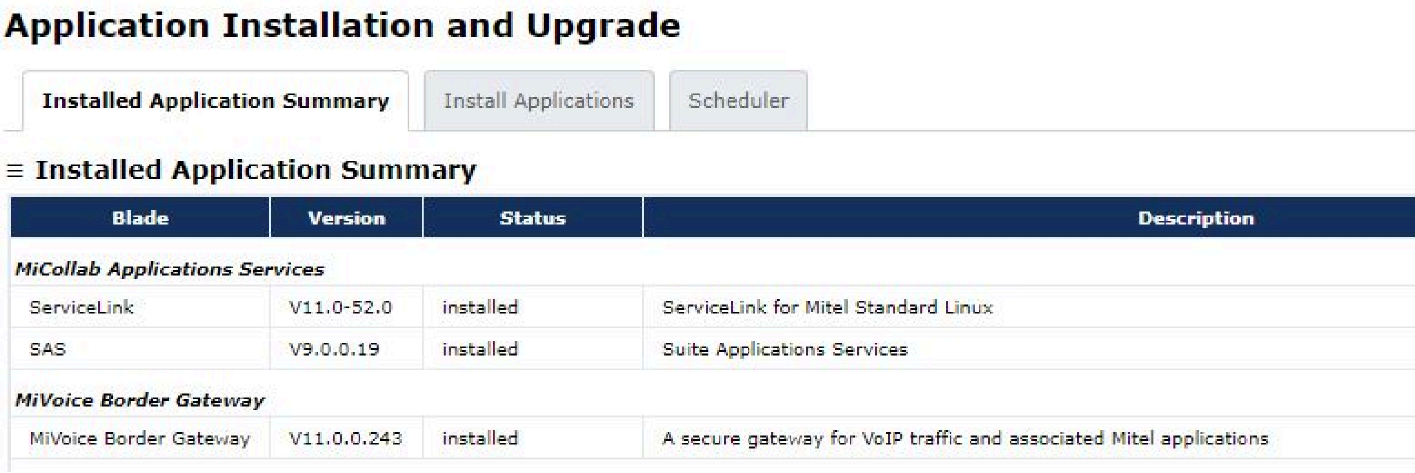
Description

Use this panel to upgrade and install MiCollab software for applications, services and security update blades.

ℹ **Note**:

- Ensure that the MiCollab server is NOT processing calls during an upgrade. Upgrading should be done outside of business hours.
- For Virtual MiCollab and MiVoice Business Express systems that are installed in a VMware environment, you can only use this panel to perform upgrades within the same release (for example, from Release 7.1 to 7.1 SP1). For major upgrades (for example from Release 7.0 to 7.x or from Release 7.x/8.x to 9.0) you **must** deploy a new OVA file. Refer to the *MiCollab Installation and Maintenance Guide* or *MiVoice Business Express Deployment Guide* for instructions.
- Downgrading MiCollab software to a previous (lower) release (for example, from Release 7.1 to 7.0) is not supported.
- All new MiCollab installations from R9.2 onwards will have MiCollab Client in an integrated mode by default.

Installed Application Summary Tab



Application Installation and Upgrade

≡ Installed Application Summary

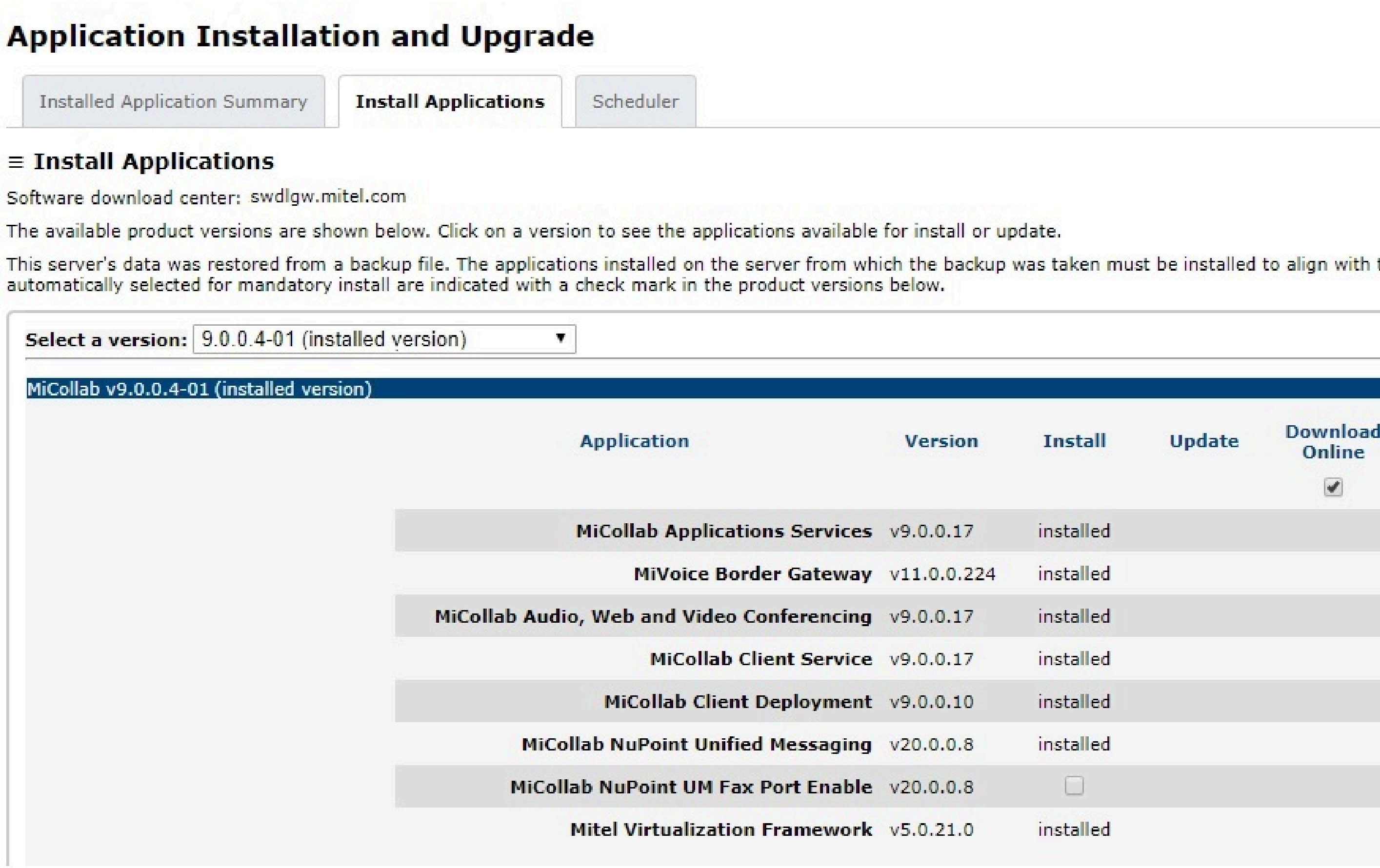
Blade	Version	Status	Description
MiCollab Applications Services			
ServiceLink	V11.0-52.0	installed	ServiceLink for Mitel Standard Linux
SAS	V9.0.0.19	installed	Suite Applications Services
MiVoice Border Gateway			
MiVoice Border Gateway	V11.0.0.243	installed	A secure gateway for VoIP traffic and associated Mitel applications

The Installed Application Summary tab lists the MiCollab applications, services and security update blades that are currently installed on the server.

Note: In case of a download error due to network time-out or network error, the Admin again needs to start the downloading process manually. Downloads will not continue for that single file which ran into an error, but if some downloads were successful before the error, the download will not be repeated once the download resumes.

Field	Description
Blade	Abbreviated name of blade
Version	Version number of currently installed application blade
Status	Installation status (installed)
Description	Full name of application. In some cases a brief descript ion of the application is also provided
Documentation	Link to documentation (if provided)

Install Applications Tab



Application Installation and Upgrade
Installed Application Summary
Install Applications
Scheduler

≡ **Install Applications**

Software download center: swdlgw.mitel.com

The available product versions are shown below. Click on a version to see the applications available for install or update.

This server's data was restored from a backup file. The applications installed on the server from which the backup was taken must be installed to align with t automatically selected for mandatory install are indicated with a check mark in the product versions below.

Select a version: 9.0.0.4-01 (installed version) ▾

MiCollab v9.0.0.4-01 (installed version)

Application	Version	Install	Update	Download Online
				☑
MiCollab Applications Services	v9.0.0.17	installed		
MiVoice Border Gateway	v11.0.0.224	installed		
MiCollab Audio, Web and Video Conferencing	v9.0.0.17	installed		
MiCollab Client Service	v9.0.0.17	installed		
MiCollab Client Deployment	v9.0.0.10	installed		
MiCollab NuPoint Unified Messaging	v20.0.0.8	installed		
MiCollab NuPoint UM Fax Port Enable	v20.0.0.8	□		
Mitel Virtualization Framework	v5.0.21.0	installed		

Use the Install Applications tab to perform the following functions:

- Select the PBX type with which this server will interact (the first time you access the tab)
- View application information for unique MiCollab software releases.
- Determine the current status of your applications, services and security patches
- Install new applications, services and security update blades
- Upgrade existing applications (service pack updates), services and security patches

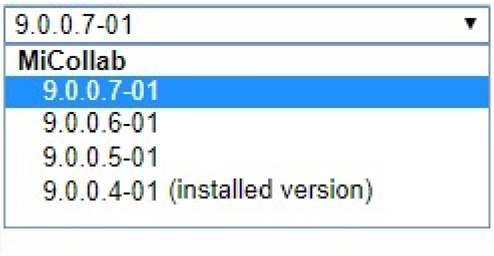
Selecting a MiCollab Version and Determining its Software Status

Use this procedure to select a MiCollab software version and determine the current status of its applications, services and security patches. By default, the system displays information pertaining to the currently installed MiCollab software version.

To select a MiCollab software version and determine the status of its applications, services and security patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.

3. To view licensed applications, services and security patches for a particular MiCollab software release, make a selection from the **Select a version** drop down menu:



9.0.0.7-01 ▼

MiCollab
9.0.0.7-01
9.0.0.6-01
9.0.0.5-01
9.0.0.4-01 (installed version)

The system downloads application information from online Software Download Center (SWDLC) and displays it in a table. Note that application information for the currently installed MiCollab version is displayed by default.

Field	Description
Application	The name of the application, service or security patch.
Version	This field lists the latest version of application software that is available for this version of MiCollab .
Install	If this field contains the word **installed**, the latest version of application software is currently installed on the system. If this field contains a blank check box, new application software is available for installation. To install it, select the check box and click the **Install** button. If this field contains a preselected check mark, new application software will be installed when you click the **Install** button.
Update	If this field contains a preselected check mark, updated application software will be installed when you click the Install button.
Download Online	Use this field to specify whether the software is to be downloaded from Software Download Center (the de fault) or locally from CD/DVD or USB. To download fr om SWDLC, select the check box. To download locally, clear the check box.

4. To view application information for a different version of MiCollab software (if available), make a selection from the **Select a version** drop down menu.

To download software from SWDLC, the firewall should allow the following connections and URLs:

- Access token for contact delivery network

  - swdlgw.mitel.com port 443 (occurs during available blade software list update)

- Content delivery/blades Akamai

  - swdl.mitel.com port 443 (download of software)

Upgrading and Installing Software

Download Optional Software from MiAccess

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From the left menu, select **Software Download Center**.
3. Under **Navigate by categories**, select **MiCollab** or enter MiCollab in the search box and press Enter.
4. Click **MiCollab**.
5. Click the download icon for the appropriate MiCollab Software Download version.
6. Download the required application .iso files (for example MiCollab NuPoint Unified Messaging) to a network drive or to a folder on your PC. Do not change the names of the files. When you click a link, you are presented with a software Disclaimer.
7. Save the application .iso files to a network drive.
8. Copy the files to CD/DVD or USB (physical or virtual).

Connect CD/DVD/USB

To Physical Systems

- CD/DVD: To connect a CD/DVD to a physical platform, insert the CD/DVD in the drive
- USB: To connect a CD/DVD to a physical platform, connect the USB drive.

To Virtual Systems

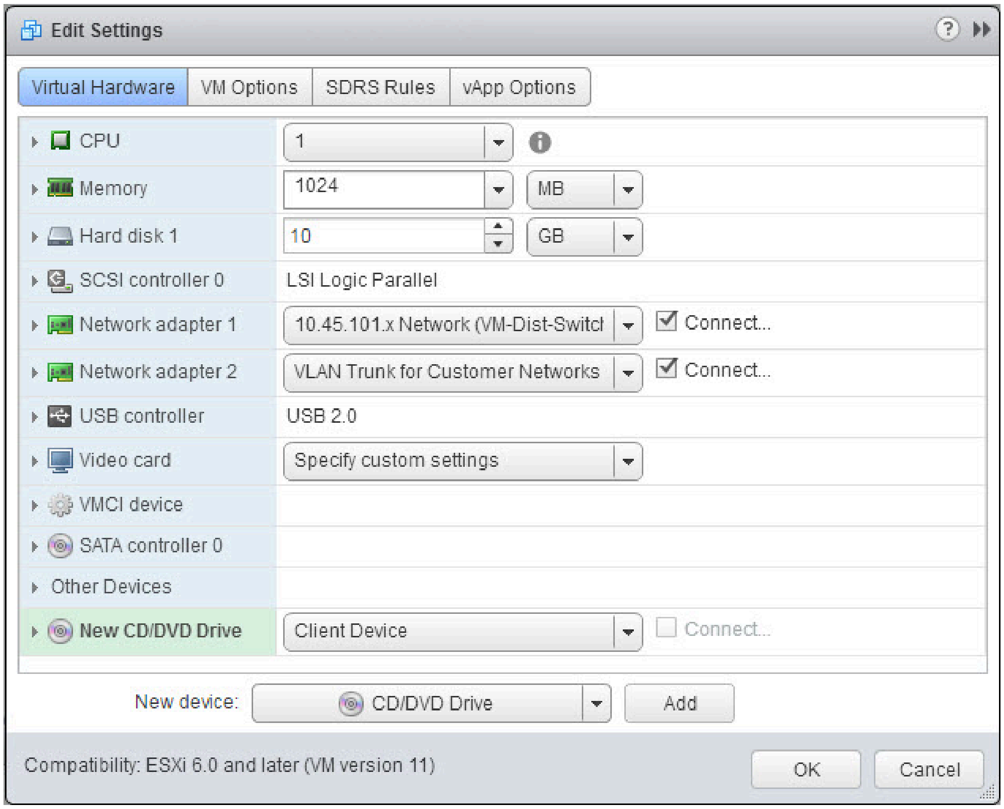
- CD/DVD

Prerequisites:

- Before adding the CD/DVD drive, turn off the virtual machine.
- If the ISO image files are not available on a local or shared datastore, upload them to a datastore from your local system by using the datastore file browser.

To connect a CD/DVD to a virtual platform:

1. In the vSphere Client Application, right-click on the virtual instance (for example: vMiCollab 6.2.3.0 build) and then click **Edit Settings**. The Virtual Machine Properties window opens.
2. Click the **Virtual Hardware** tab.
3. From the New device drop-down menu, select **CD/DVD Drive** and click **Add**. The new drive appears at the bottom of the Virtual Hardware list.



CPU	1		
Memory	1024	MB	
Hard disk 1	10	GB	
SCSI controller 0	LSI Logic Parallel		
Network adapter 1	10.45.101.x Network (VM-Dist-Switcl		☑ Connect...
Network adapter 2	VLAN Trunk for Customer Networks		☑ Connect...
USB controller	USB 2.0		
Video card	Specify custom settings		
VMCI device			
SATA controller 0			
Other Devices			
New CD/DVD Drive	Client Device		□ Connect...

New device: CD/DVD Drive

Compatibility: ESXi 6.0 and later (VM version 11)

4. Expand **New CD/DVD Drive** and select the device type.

Option	Action
Client Device	a. Select to connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Web Client. b. From the **Device Mode** drop-down menu, select **Passthrough CD-ROM**. When you turn on the virtual machine, select the media to connect to from the **VM Hardware** panel on the virtual machine **Summary** tab.
Host Device	a. Select to connect the CD/DVD device to a physical DVD or CD device on the host. b. From the **CD/DVD Media** drop-down menu, select the media to connect to. c. From the **Device Mode** drop-down menu, select **Emulate CD-ROM**.
Datastore ISO File	a. Select to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host. b. **Browse** to the file containing the ISO image to connect to and click **OK**.

5. (Optional) Select **Connect At Power On** to connect the device when the virtual machine turns on.
6. (Optional) To change the device node from the default, select a new mode from the **Virtual Device Node** drop-down menu.
7. Click **OK**.

- USB: You can add one or more USB passthrough devices from a client computer to a virtual machine on the virtual machine Summary page in the vSphere Web Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machine resides.

  Prerequisites:

  - Ensure that a USB Controller is present.
  - Ensure that the vSphere Client application has access to the ESXi host on which the virtual machines are running.
  - Upload the ISO image files to the USB device.

  To connect a USB to a virtual platform:

  1. In the vSphere Client Application, right-click on the virtual instance (for example: vMiCollab 6.2.3.0 build) and then click **Edit Settings**. The Virtual Machine Properties window opens.
  2. Click the **Virtual Hardware** tab.
  3. Click the USB icon to the right of **USB Devices** under **VM Hardware** and select an available device from the drop-down menu.

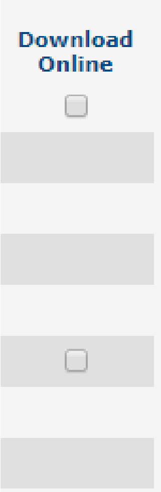
  A Connecting label and a spinner appear, which indicates that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to USB Devices.

Select a Software Download Method

By default, all software is set to download from the Software Download Center (SWDLC). You may, however, download the software from local storage media (CD/DVD or USB). Use this procedure to specify which download method you wish to use for each application, either the SWDLC or local.

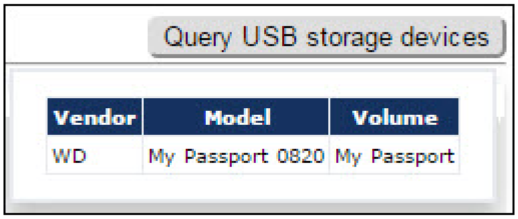
To select the download method for an application:

1. Clear the **Download Online** check box.



Each application now has its own **Download Online** check box. The boxes are cleared, indicating that MSL will attempt to download the application software from local media rather than the SWDLC.

2. Select a download method for each application:
   - To download from local media (CD/DVD or USB), clear the **Download Online** check box for the application.
   - To download from the SWDLC, select the **Download Online** check box for the application.
3. If installing from USB, click **Query USB Storage Devices**.



Vendor	Model	Volume
WD	My Passport 0820	My Passport

The system attempts to detect USB devices connected to the local computer. For each device that is found, the following information is displayed: **Vendor** name, **Model** name, and **Volume** label. When you install or upgrade an application, the system will search these devices for software (ISO files). If a device is not detected, it will not be searched.

Install New Software

The first time you access the Install Applications tab, you will be prompted to select the type of PBX with which the server will interact: MiVoice 5000 , MiVoice Business , MiVoice MX-ONE , or MiVoice Office 400.

To install new applications, services and patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab. If prompted, select the **PBX Type** with which this server will interact and then click **Next**.

   The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.

> **Note**: The MiVoice 5000 , MiVoice MX-ONE , and MiVoice Office 400, are only supported in MiCollab Client Integrated Mode. If you are deploying MiCollab with one of these platforms, run the MiCollab Client Integration Wizard.

3. To display information for a different version of MiCollab software (if available), use the **Select a version** drop down menu.
4. Under the Install column:

Field Contents	Description
	The word installed indicates that the latest version of the application software is currently installed on the s ystem.
	A blank check box indicates that new application sof tware is available. To install it, select the check box and click the Install button.

Field Contents	Description
	A preselected check box indicates that new application software will be installed when you click the Install button.

5. Select the software download method, either from the Online (SWDLC) or local media (CD/DVD or USB).
6. Click **Install** to install the applications/services you have selected.

   Software downloads are queued and installed sequentially from the SWDLC or local media.
7. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed.
8. When installation is complete, click **Clear this report**. The MSL server manager displays the installed applications.
9. Remove the CD/DVD, disconnect the USB, dismount the network share, or dismount the vSphere Datastore.

Upgrade Existing Software

To upgrade existing applications, services and patches:

1. Under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.

   The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.
3. To display information for a different version of MiCollab software (if available), use the **Select a version** drop down menu.
4. Under the Update column, a preselected check box ☑ displays for each currently installed application/service that will be upgraded with new software when you complete this procedure.
5. Select the software download method, either from the SWDLC preselected check boxes.

   Software downloads are queued and installed sequentially from the SWDLC or local media.
6. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed.
7. When installation is complete, click **Clear this report**. The MSL server manager displays the installed applications.
8. Remove the CD/DVD, disconnect the USB, or dismount the vSphere Datastore.

Note: You can install and upgrade software simultaneously.

Scheduler tab

Use the **Scheduler** tab to configure the server to download the latest available application updates at a specific date and time. Only applications available online on the SWDLC are downloaded. You can schedule the update downloading to be a one-time event, or one that recurs weekly or monthly. Optionally you can choose to receive notifications that will alert you about the available updates.

ℹ **Note**: The scheduler option is available only on a MiCollab or an MiVBX server.

Schedule Summary

Displays the result of the last scheduled event execution.

Scheduling Options

Complete the following steps to create a new scheduled event:

1. Under **ServiceLink**, click **Install Applications**. The **Application Installation and Upgrade** page opens.
2. Click the **Scheduler** tab.
3. In the **Scheduling Options**, select **Enabled** from the **Scheduler service status** drop-down.
4. Select the **Send update notification** check box if you want to be notified about an available update.
5. Configure the date, time, and frequency of downloading updates.
6. Click **Save**. The scheduler displays a confirmation that updates will be downloaded as scheduled by you.

ℹ **Note**: The installation needs to be done manually after the blades are downloaded as per the time scheduled in the scheduler.

3.2 View ServiceLink Status

This panel provides updated ServiceLink status information for this server. License information is downloaded from the license server as part of the synchronization protocol.

You must activate ServiceLink before you can view status information. The status is a result of a successful or non-successful online or offline synchronization with the server from which the license information is downloaded.

MiCollab solutions with MiVoice MX-ONE, MiVoice 5000, MiVoice Office 400, and MiVoice Business will be licensed through the License Server.

Online Activation

To activate ServiceLink online:

1. Obtain an Application Record ID (service account ID) or ServiceLink ID (Serial ID) from your authorized reseller.
2. Under **ServiceLink**, click **Status**.
3. In the Service Link Activation Page, enter your **Application Record ID** (also called Service account ID) or **ServiceLink ID.**

4. Enter:

   - Address of proxy

     - Address of proxy
     - when using the License Server
   - TCP port

     - when using a proxy with different port (valid for License Server)

> **Note**: The proxy server must be configured to forward TCP packets on the incoming port to the License Server address which is sync.mitel-sls.com on port 22. This is not an optional field.

5. Click **Activate** to synchronize with the license server and activate ServiceLink.

Following successful activation, MSL periodically reconnects to the License Server (every 24 hours by default) via a secure, encrypted connection to synchronize ServiceLink status information. New configuration instructions, such as services you have added or deleted to your License Server account, are updated at this time.

Manual Synchronization

Although the system automatically synchronizes with the license server on a periodic basis (every 24 hours by default), you can force an immediate synchronization at any time. This is useful to check the network connection between MSL and the license server, attempt to clear major alarms that are generated if the automatic sync process fails, or to obtain up-to-date ServiceLink configuration information from the license server. This procedure can be performed on systems that have been activated either online or offline.

To manually synchronize with the license server:

1. Under **ServiceLink**, click **Status**.
2. Click the **Sync** button.

Deactivation

If the system hardware has been changed or replaced, you will need to deactivate your ServiceLink account, reset your Hardware ID, re-enter your Application Record ID and then reactivate your ServiceLink account. Use the MSL server manager to complete all steps with the exception of resetting your Hardware ID, which must be done on the licence server.

To deactivate ServiceLink:

1. Under ServiceLink, click **Status**.
2. Click the here link to access the deactivation screen.
3. Click **Deactivate**.

> **Note**: Following deactivation, you must reset your hardware ID on the license server and then reactivate your ServiceLink account using either the online or offline method.

Administration 4

This chapter contains the following sections:

4.1 MSL Web Services

Mitel Standard Linux includes a Representational state transfer (REST) API that provides a secure web services framework using the OAuth 1.0 protocol. This "Web Services" interface is intended to support the features and functions currently available in the traditional Mitel administrative interfaces.

In its initial release, the Web Services interface supports MiCloud Management Portal (MMP) management integration. MiCloud Management Portal (MMP) is a web-based customer provisioning application that employs the Multi-instance MiVoice Business to deliver multi-customer communications services for service providers. Hosted from the data center, MiCloud Management Portal (MMP) is intended as the primary management tool for customers and end-users to access and modify services.

By default, the Web Services panel includes a single registered web services client for MiCloud Management Portal (MMP). Do not change this configuration in any way. Do not modify the existing consumer information or tokens, and do not attempt to add a new consumer.

The administrator can create a new web services consumer. A consumer is a vendor of a particular web services client. The credentials entered are used in the client to begin the OAuth authentication process.

You can use the Web Services panel to enable/disable the interface. To enable/disable the MSL Web Services interface:

1. Under **Administration**, click **Web services**.
2. Under Manage web service availability, click **Start** to enable or **Stop** to disable the web services interface.

ℹ **Note**: The expired consumer tokens must be manually renewed from the Web Services interface. Periodically check the **Approved tokens** table to **Modify**, **Renew**, or **Revoke** the tokens that are representing an approved client for the web service.

4.2 Backup Server Data

There are two main methods for backing up system data (including all server configuration data, application configuration data, user settings, messages, and greetings):

- Server Manager **Backup** (to backup data to a local workstation or a network file server that supports SFTP or SMB/CIF), and
- Server Console **Perform Backup** (to backup to a USB device or to a network file server)

If you are planning to restore a pre-existing MiCollab 1.1 backup, we recommend that you verify the file beforehand.

ℹ **Note**:

- If your MiCollab system is integrated with a directory service, ideally you should back up both the MiCollab database and the directory server database at the same time.
- You can use different filenames for backup files, but the filename must not contain spaces and the file extension must be **.tgz**. (Note that all backup files of systems prior to Release 9.0 will be titled "smeserver.tgz".)
- The content of the system's /root directory will be included in the backup. To minimize the backup size, delete any temporary unwanted files that administrators might have created during system support activities. Do not delete the content of hidden files and directories such as /root/.ssh and /root/.bash* which are required for proper server functionality.
- The backup file does not include OAuth 1.0 data. Accordingly, if you have implemented Google Apps integration with OAuth 1.0, you must re-enter the data after performing a restore procedure. (Note that OAuth 2.0 data *is* included in the backup file.)
- To ensure that MiCollab has consistent Network Element (ICP) information, you must use one of these backup procedures. Restoring backups made from inside the individual applications may cause incorrect Network Element data to be presented to the MiCollab server.
- To restore the data, you must transfer the backup file to a storage medium (CD/DVD or USB storage device).
- If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you should back up both the MiCollab server database and the MBG server database at the same time.
- You cannot restore a MiCollab database backup to a Virtual MiCollab Release 2.1 deployment. For Virtual MiCollab Release 2.1 deployments you must use VMware tools to perform backups and restores. See the *MiCollab Installation and Maintenance Guide* for instructions. However, it is recommended that you continue to take scheduled MiCollab database backups from a Virtual MiCollab Release 2.1 deployment, because MiCollab database restores are supported in MiCollab Release 2.2 and later.

Server Manager "Backup"

Backup to Desktop

Use this procedure to save your system backup to a file or device on your desktop computer or maintenance PC if your MiCollab system has only one application installed .

A "Backup to desktop" saves all of the data to a single, large compressed file and is therefore limited by the file system and browser of the client operating system. For example, if you are backing up data to a Windows client that uses the FAT32 file system (the default for many older versions of Windows), you are limited to a maximum file size of 4 GB; newer Windows operating systems that use the NTFS file system have a much larger capacity. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored. For this reason, we recommend that you use the Verify Backup File option in the MSL server console to ensure the backup was successful.

1. Under **Administration**, click **Backup**.
2. Select the **Backup to desktop** option.
3. Click **Perform**. MSL prepares the system for backup.

   The "Operation status report" is displayed with the estimated backup size, along with the "Backup Encryption" option.
4. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. The encrypted backup file is identifiable with an .aes256 extension.

> ℹ **Note**: You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

5. Click **Download Backup File**.
6. When prompted to Open or Save, click **Save**.
7. In the file download window that appears:

   - Name the file and then select the location where the file will be saved. Note the backup filename must not contain spaces; otherwise, you will get an error when you attempt to restore it.
   - Click **Save**. After saving, you can copy the backup file to a CD/DVD or USB storage device, if required. The backup file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

Schedule Backups to Network File Server

Use this option to:

- perform immediate system backups to a Network File Server
- schedule daily, weekly, or monthly system backups to a Network File Server

Use this option if your system has more than one application installed.

Note:

- You can only have one backup scheduled on the server. To cancel an existing backup schedule, select **Disabled** and then click **Save**.
- If you are backing up to an MSL server, configure it to accept access from the backup server. See Configure Network Privileges for details.
- Two file-sharing protocols are supported:
  - SMB/CIFS
  - Secure File Transfer Protocol (SFTP)

To perform a backup to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Specify the following details.

Field	Description
IP Address	IP address of the network file server where you have stored the database backup file.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
Domain or Workgroup Name	Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.

Field	Description
Sharename	The file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/ shared folder as an SMB/CIFS resource. The shared folder must have permissions set to "Full Control."
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.

ℹ **Note**: If you are backing up to an MSL server, enter its IP Address and the Username/Password of the "root" user. Leave the remaining fields blank..

5. (Optional) Select the **Maximum number of backup files to keep** (1-999) on the server. When the number of stored files reaches this maximum count, the oldest version is deleted.
6. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.

ℹ **Note**: You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

7. Click **Backup Now** to test your server configuration by performing an immediate backup.

   The backup file is saved to the network file server. The file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

To perform an immediate backup, Click **Backup Now**.

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Save**.

4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example:

   mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).

   - For Daily backups, select a time of day (hour, minute, AM/PM)
   - For Weekly backups, select a time of day, and day of the week
   - For Monthly backups, select a time of day, and day of month
   - To disable regularly scheduled backups, click **Never.**
5. Click **Save**.

Server Console "Perform Backup"

You can save your system backup to a USB storage device (such as a memory stick or hard drive) or to a network file server that supports SFTP (typically a Linux server, including MSL) or SMB/CIF (typically a Windows server). Any USB storage device that is formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux) is compatible.

The backup file size limit via USB or network backup is set by the destination file system: 4 GB for a FAT32, 2 TB (terabyte or trillion bytes) for NTFS, and 16 GB to 16 TB for ext3 (depending on file system block size). The current MSL ext3 block size is 4096 bytes which allows file sizes of 2TB.

Optionally, you can encrypt the backup file if you are saving it to a USB device from the server console. This option is not available if you are saving the backup file to a network file server from the server console.

1. Access the server console.
2. Log in as " admin".
3. From the console, select the option to **Perform backup**.
4. Select a destination for the backup file:

   - Backup to a USB device.
   - Backup to a network file server.

Backing up to a USB Device

1. Select **Backup to a USB device**.
2. At the prompt, insert the USB device (if not already in place) and click **Next**.
3. When prompted, enter a filename for the backup file (default is ' mslserver') and click **Next**. Note the backup filename must not contain spaces; otherwise, you will get an error when you attempt to restore it. The file extension, either .tgz (unencrypted) or .aes256 (encrypted), is automatically added.
4. (Optional) To encrypt the backup file, enter an encryption password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Next**.

> **Note**: You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

5. MSL displays an estimate of the size of your backup. Click **Proceed**.
6. When the backup is complete, remove the USB device at the prompt. Click **Continue**.
7. Re-mount the USB and verify that the backup was performed successfully using the Verify Backup Data procedure.

Backing up to a Network File Server

> **Note**: If you are backing up to an MSL server, enter its IP address and the username/password of the "root" user. Leave the remaining fields blank.

1. Select **Backup to a network file server**.
2. Enter the **IP address** of the file server where the backup will be stored.
3. Enter the **domain** or workgroup name of the server. (For example, mitel.com.)
4. Enter the name of the **shared folder** where the backup file will be stored. (For example, "Backups".) The shared folder must have permissions set to "Full Control".
5. Enter an **Optional Sub Directory** for the backup file. The specified directory must exist in the share folder. The field accepts multi-level directories; for example"MAS/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.
6. Enter the **username** to use when connecting to the backup server.
7. Enter the **password** to use when connecting to the backup server.
8. Click **Next**. A progress bar indicates backup status. When the backup is complete, file verification is performed automatically.

Verify Backup Data

When backing up to a USB device or when using a pre-existing backup file, it is important to verify the file before starting a restore procedure. If your backup file cannot be verified, then it cannot be used to restore system information.

To verify a backup file:

1. Access the server console at the MiCollab server or from a maintenance PC.
2. Log in as " admin".
3. From the console, select the option to **Verify backup file**.
4. At the prompt, insert your storage medium. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it first.) A list of all storage devices found on your system is displayed.
5. If more than one storage device is connected to your system, select the device containing the backup file.
6. If more than one backup file is contained on the storage device, select the file you want to verify.
7. Click **OK**. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again. See the *MiCollab Engineering Guidelines* for a list of supported USB devices.

Restore (Disaster Recovery Situations)

When recovering from a disaster situation, it is necessary to reinstall MSL operating system software. Follow the instructions for Disaster Recovery in the *MiCollab Installation and Maintenance Guide MSL Installation and Administration Guide*.

4.3 View Log Files

Use this panel to view/download log files and to collect log files and diagnostic data.

View/Download Log Files

To assist in troubleshooting, you can either view or download the log files generated by the services running on your server.

To view/download the log files:

1. Under **Administration**, click **View log files**.
2. Under View Log Files, choose a log view. Most system services write their logs to the "messages" file.
3. Enter a **Filter Pattern** to view online the lines of the log that contain that text. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
4. Specify a **Highlight Pattern** to mark in bold the specified text in any logs that the text appears. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.
5. From **Operation**, select **View log file** or **Download**.
6. Click **Next**. If you selected **View log file**, the log files are displayed.

Note: The system automatically updates the list every 5 seconds with any new logs.

Collect Log Files and Diagnostic Data

This utility allows system-level logs to be collected for the server platform and then saved to another location such as your local PC. Logs can be selected for collection from specific applications.

To collect and save log files:

1. Under **Administration**, click **View log files**.

2. Under Collect log files & diagnostic data, select which categories you wish to collect. To minimize the size of the log file, uncheck categories you do not require.

Note: Coredump log files can be very large and take a long time to collect. It is recommended that you uncheck the "Coredump files" category.

3. Click **Start**. A progress indicator appears while the logs are being collected.

Note: You can navigate to other screens without interrupting the process.

4. When the log collection process finishes, the indicator changes to "Complete / 100%" and the archived log file is listed on the screen. Depending on which type of web browser you are using, a copy of the file will be downloaded automatically or you will be prompted to save it.
5. You can manage the list of archived log files as follows:

   - To save and encrypt a file, click **Encrypt Download**, enter a **Password**, and then re-enter it. Create a strong password by using a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Continue**. An encrypted tar file with the filename "sosreport-<file>.tar.gz.aes256" is saved to the **Downloads** folder.
   - To save a file without encrypting it, click **Download**. A tar file with the filename " sosreport-<file>.tar.gz" is saved to the **Downloads** folder.
   - To delete a file, click **Delete**, and then click **OK**. The archived log file is deleted from the server.

After saving an archived log file, send it to Mitel Product Support for analysis. If the file is encrypted, also send the password. Without it, the file cannot be decrypted.

Note:

- To decrypt an encrypted log file, transfer the file to a Linux system, access a console on the system, and then enter the following command: **openssl enc -aes-256-cbc -d -in filename -out newfilename**. **openssl** - This is the openssl command. **enc** - This indicates the symmetric cipher routine being used.
- When prompted, enter the password used to encrypt the file. If you only have access to a Windows system, use a Unix emulator such as CygWin to perform these steps.
- Archived log files are automatically deleted from the server after 72 hours.
- You can also manage the archived log files from the MSL shell. The files are located on the server in /var/cache/e-smith/ logcollector.
- For MSL-based versions of MiVoice Business , collecting logs is a multi-step process:

  1. In the MSL Server Manager, access the View logs files screen and select the **Collect MCD logs** check box.
  2. In the MiVoice Business System Administration Tool, access the System Diagnostics form, run the System Diagnostics and package the log files.
  3. In the MSL Server Manager, access the View logs files screen and click **Start** to collect the logs.
- For an EX controller, the SOS report contains the Notification file that consists of EX events along with the EX configuration data.

4.4 View Event Logs

You can display the current alarm state of the system and view the application event logs for some applications (such as MBG).

ℹ **Note**: Some deployments may display a Critical alarm after initial installation. Follow the instructions below to clear the alarm.

Alarm Notification

The header bar of the MSL server manager contains an "Alarm Status" label which indicates the system alarm severity level. For example, if the system has a service-affecting fault, the label will display "Minor" with a yellow background. Clicking the label opens the Event Viewer.

View Application Event Logs

To view application event logs:

1. To access the Event Viewer, do one of the following:
   - Click the **Alarm Status** severity indicator.
   - Under **Administration**, click **Event viewer**.
2. Select the number of events that you want to display per page from the **Events per Page** drop-down menu.
3. The **Boundary dates and times** are populated automatically by the system. To enter non-default values:
   - Under **Start** and/or **End**, click the **Manual** box.
   - Enter a new **Date** (YYY-MM-DD) and/or **Time** (HH:MM:SS).
4. Select the **Severity filter**. All logs with the selected alarm severity or higher will be displayed.
5. In the **Text filter** field, enter any text that you want the logs to be filtered against. Only logs that contain the specified text will be displayed. The filter is applied against the log data in the "Application", "Event type", "Value" and "Description" fields.
6. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
7. Select the **Show Cleared Events** box if you want to view both cleared and new events. Clear the box if you only want to view new events.

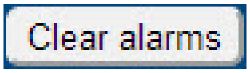
   ℹ **Note**: Events may also be cleared automatically by the applications.

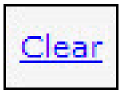
8. Select the **Auto Reload** box if you want the system to automatically reload the events each time you open the page.
9. Click **Reload**. The event logs are displayed.

Field	Description	Possible Values
Clear	Click to clear this ietm.	
Application	Application name	
Event Type	Event that was occurring or attempting to occur when the alarm was set.	• set connection • set registration • one-way audio
Value	Value associated with the event	• established • rejected • lost • MAC address (for one-way audio)

Field	Description	Possible Values
Severity	Level of severity associated with this alarm	• **Cleared** (green): No alarms have been raised since the alarms were last cleared. • **Indeterminate** (turquoise): The cause of the alarm cannot be determined at this time. • **Warning** (blue): Indicates an "information only" alarm. • **Minor** (yellow): Indicates a fault which affects service. This may result in a major degradation in service and requires attention to minimize customer complaints. • **Major** (orange): Indicates a fault which will cause a major degradation in service and requires attention as soon as possible. • **Critical** (red): Indicates a total loss of service which demands immediate attention. The "Indeterminate", "Warning" and "Cleared" states are informational only
Date and Time	Timestamp of the alarm	
Description	A comma-separated list of identifiers that pertain to the alarm; may contain MAC and IP addresses as well as Reason for alarm.	(various) Click the **Refer to...** link to open the application that is affected by this alarm.

Clear Alarms

- To clear all alarms, click **Clear alarms**. 

- To clear an individual alarm, click **Clear** for the item. 

4.5 About SDS Distribution Errors

Flow Through Provisioning synchronizes user and services data updates between the MiCollab database and MiVoice Business system databases in a sharing network. If you make an update in the MiCollab USP database and the update is not successfully shared to all the other elements in the sharing network, a distribution error is sent to the MiCollab SDS Distribution Errors application. If the number of distribution errors exceeds an SDS alarm threshold, a data distribution alarm is generated in the Event Viewer application.

The SDS Distribution Error application allows you to view and manage distribution errors and pending updates:

- **Distribution Errors** are updates that could not be applied to the destination elements.
- **Pending Updates** are updates that have not yet been applied to the destination elements.

From this application, you can:

- reload the list of distribution errors
- export the errors to a file
- delete updates
- retry failed updates
- filter errors in the list.

Launching the SDS Distribution Error Application

ℹ **Note**: The SDS Distribution Error application is only available if Flow Through Provisioning has been enabled between MiCollab and MiVoice Business platforms.

1. Under **Administration**, click **SDS Distribution Errors**.
2. Resolve any distribution errors.

Field Descriptions

Parameter	Description
	Click to select a record
	Click to display the details for the record.
Action ID	A unique number sequence that identifies the transaction of a specific shared form distribution attempt.

Parameter	Description
To	Indicates the destination network element for the membership data. ℹ **Note**: This field displays the name of the destination network element as it appears in the Network Elements form of the MiVoice Business system.
Date/Time	Displays the date and time that a distribution transaction was attempted.
Last Retried	Displays the date and time of the most recent failed update retry.
Action	Specifies the configuration action type (for example: add, modify, or delete).
MiVB Form Name	Identifies the name of the MiVoice Business form from which the data distribution originated.
Error Type	The types of distribution error messages include: • Transport errors - failures of data update event delivery • Application errors - failures of data update transaction at destination • Concurrency error - conflicting data update information at the destination because • a change was made to a record but the original record on the remote system(s) was not in sync with the original record on the local (master) system, or • a change was made at the same time by two or more administrators on the same record. • Transport and Concurrency Error • Application and Concurrency Error
Reason	Displays an error message.
Status	Displays the status of the update: • Idle - awaiting Retry operation • Retry Pending - administrator has retried the update and a system response is pending. • Pending - automatic update has been sent and a response is pending. ℹ **Note**: The status field is updated approximately every 30 seconds.

Parameter	Description
Count	The Count in the lower left corner of the Distribution Error screen displays the total number of error listed.

4.6 View System Information

System Information for your server can be viewed under **Administration** > **System Information** panel.

The System Information panel provides hardware manufacturer and product name/model information. This panel also provides a summary of networking parameters, server details, and domain information.

The following system parameters are displayed in this panel:

- **System Vital** - hostname, IP address, kernel version, and so on. For example, this panel indicates whether the MSL Kernel Version is 32-bit or 64-bit.
- **Memory Usage** - Server-wide memory utilization statistics, size and the usage of random-access memory.
- **Mounted Filesystem** - list of the mounted partitions, root, directory (mount point), size, and available storage
- **Network Usage Information** - the amount of data sent and received by your system network interfaces, network interface throughput.
- **Hardware Information** - server manufacturer/model, number of processors/model, CPU speed, cache size, and so on.

4.7 Access System Monitoring Tools

To enable access to system monitoring tools:

1. Under **Administration**, click **System Monitoring**.
2. In the **Access to system monitor display** field, select one of the following:
    - **Private**: to allow access only for private networks (local networks only)
    - **Public**: to allow public access to entire Internet (visible to anyone on the Internet)
    - **Disabled**: to disable access
3. Click **Save**.

To view the system monitor display, click **System monitor display**.

4.8 System Users

4.8.1 Manage User Accounts for Remote VPN Access

You can add, modify, lock, or remove user accounts for Virtual Private Network (VPN) client access. When you create a new system user account, the account is locked. You must reset the password to enable access to the account.

To add a system user account for VPN client access:

1. Under **Administration**, click **System users**.
2. Click **Add user account**.
3. Enter the **Account name**, **First name**, and **Last name**. The account name should contain only lower-case letters, numbers, hyphens, periods, underscores and should start with a lower-case letter. For example "betty", "hjohnson", and "mary-jane" are all valid account names, but "3friends", "John Smith", and "henry:miller" are not.
4. Set **VPN Client Access** to **Yes**.
5. Click **Add**.
6. Click **Reset Password** and reset the password for the account. By default, passwords must be at least 8 characters. See Password quality requirements.
7. From the list of users, you can modify or remove a user account (by clicking **Modify** or **Remove** next to the user name), or set the user's password. User accounts are locked out and cannot be used until you set the initial password for each account.

4.8.2 Manage Multiple Admin Accounts

You can create additional administrative accounts which have complete Server Manager access. This setting allows multiple users to have administrative access to the server without having to share the primary **admin** user account password.

The primary system **admin** account has privileges to create and modify any system account, including password resets of the sub-admin accounts. Additional sub-admins can only modify their own account information and do not have privileges to create additional administrative accounts.

Note:

- It is strongly recommended that only a single admin user perform any system modification at one time to prevent concurrency issues.
- Any logs produced, by operations performed by the logged in user, are recorded with the user login name for audit trail purposes.

To provide a system user account with Admin access:

1. Under **Administration**, click **System users**.
2. Click **Add user account**.
3. Enter the **Account name**, **First name**, and **Last name**. The account name should contain only lower-case letters, numbers, hyphens, periods, underscores and should start with a lower-case letter. For

example "betty", "hjohnson", and "mary-jane" are all valid account names, but "3friends", "John Smith", and "henry:miller" are not.

4. Set **Admin User Access** to **Yes**.
5. Click **Add**.
6. Click **Reset Password** and reset the password for the account. By default, passwords must be at least 8 characters. See Password quality requirements.

> ℹ **Note**: Only ASCII characters are supported for sub-admin passwords.

7. From the list of users, you can modify or remove a user account (by clicking **Modify** or **Remove** next to the user name), or set the user's password. User accounts are locked out and cannot be used until you set the initial password for each account.

Locking (Disabling) User Accounts

When an account is locked, the user will no longer be able to access server resources such as the VPN. To unlock the user account, reset the password using the Reset password link.

Changing User Passwords

Administrators can change user and/or administrator passwords by using the Reset password link for that user's account on the Users panel. This entry overrides any previous password entered. Passwords can contain any combination of printable characters, including upper- and lowercase letters, numbers, and punctuation marks. By default, passwords must be at least 8 characters. See Password quality requirements.

> ℹ **Note**: There is no way to recover a forgotten password for a user. If this occurs, a new password must be set.

4.8.3 Digital Certificates for VPN Connections

For increased security, you can use SSL client certificates to authenticate VPN connections.

To implement this feature for a user, you must download a certificate from MSL, import the certificate to the user's computer, and then set up the user's VPN connection.

Downloading the Certificate from MSL

Use this procedure to download the user's digital certificate from MSL, the certificate authority (CA).

To download a certificate from MSL:

1. Log in to the server manager remotely from a Windows PC.
2. In the server manager under Administration, click **System Users**.
3. Find an existing user (or set up a new user and reset the password).
4. Click **Download VPN certificate**.
5. Click **Save** or **Save as** and save the file to a location on your computer.

Importing the Certificate

Use this procedure to import the user's digital certificate to the user's computer.

> **Note**: The following procedure outline how to import a certificate to Internet Explorer 9 in a Microsoft Windows environment. For instructions to perform these procedures on a different browser, refer to your product documentation.

To import a certificate to the user's computer:

1. In Internet Explorer, click **Tools > Internet Options**.
2. On the Content tab, click **Certificates**.
3. Click **Import**.
4. The Certificate Wizard opens. Click **Next**.
5. Browse to the location of the stored certificate file.

> **Note**: The file may not be visible until you specify files with extension .pfx or .p12.

6. Click **Open** and then click **Next**.
7. In the Password dialog, click **Next** to continue. Do not enter a password for the private key.
8. In the Certificate Store dialog, select **Automatically select the certificate store based on the certificate type**.
9. Click **Next**. If Windows prompts you for confirmation to install the certificate, click **Yes**.
10. Click **Finish** to complete the certificate import.

Setting Up the VPN Connection

Use the following procedures to set up a VPN connection on the user's computer:

- Windows 7 VPN Setup
- Windows 10 VPN Setup

Windows 7 VPN Setup

Creating the Connection

To create a VPN connection on a Windows 7 computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the Connection Option list, select **Connect to a Workplace**.
4. Select **No, create a new connection** if prompted, and then click **Next**.
5. Select **Use my Internet connection**.
6. Enter the server **IP address** or **host name**.
7. Enter a **Destination name** for your VPN connection.
8. Select **Don’t connect now; just set it up** and then click **Next**.

9. Enter your **User name**. Password is not required if you are using certificate for authentication.
10. Click **Create** and then click **Close**.

Configuring the Connection

To configure a VPN connection on a Windows 7 computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. In the left-hand menu, click **Change adapter settings**.
3. Right-click your VPN name and then click **Properties**.
4. On the Networking tab, select **Internet Protocol Version 4** and then click **Properties**.
5. Click **Advanced**.
6. Clear the **Use default gateway on remote network** check box.
7. Click **OK** twice to return VPN Connection Properties dialog.
8. On the Security tab, in the Type of VPN list, select **Point to Point Tunneling Protocol (PPTP)**.
9. Under Authentication, select **Use Extensible Authentication Protocol (EAP)**.
10. In the EAP list, select **Microsoft: Smart Card or other certificate**.
11. Click **Properties**.
12. Under “When connecting” select **Use a certificate on this computer** and then select **OK**.
13. Choose whether to validate the server certificate. When selected, Windows prompts users to confirm that they're connecting to the correct server and that the certificate is valid. If you choose to enable validation, clear the **Connect to these servers** check box.
14. Click **OK** until you return to the Control Panel > Network Connections dialog.
15. Right-click on your VPN name and then click **Connect** to test the connection.

Windows 10 VPN Setup

To create and configure a VPN connection on a Windows 10 computer:

1. Click **Start > Settings**.
2. Click **VPN**, and then click **Add a VPN connection**.
3. Configure the following:

   - For the **VPN Provider**, select **Windows (built-in)**.
   - For the **Connection name**, enter a name of your choice.
   - For the **Server name or address**, enter the server address.
   - For the **VPN type**, select **Automatic**.
   - For the **Type of sign-in info**, select **Certificate**.

   Do not enter a Password. Since you are using a certificate for authentication, It is not required.
4. Select **Remember my sign-in info**, and then click **Save**.
5. Click **Connect** to test the connection

4.8.4 Password Quality Requirements

As an administrator, you can enforce password complexity by setting password complexity rules. The following rules and configuration instructions apply to all system accounts.

Note: The credit value of each field indicates the requirement of the corresponding item in the password. For example,

- Uppercase credit 0 : Uppercase characters may or may not be included in the password.
- Uppercase credit -2: The password must contain a minimum of 2 uppercase characters.
- Uppercase credit 2: If uppercase characters are included in the password, 2 of these characters will have a length credit assigned, which means, each of these 2 uppercase characters will be counted as 2 characters towards the minimum password length. Additional uppercase characters included in the password will not get this credit and will be counted only as 1 towards the minimum password length. Positive credit for a character does not imply that that character must be included in the password.

The following rules and configuration instructions apply to all system accounts by default:

- **Minimum length**: The password must contain at least 8 characters.
- **Uppercase credit**: Specifies the maximum length credit for having uppercase characters in the password. If less than 0, it is the minimum number of uppercase characters required.
- **Lowercase credit**: Specifies the maximum length credit for having lowercase characters in the password. If less than 0, it is the minimum number of lowercase characters required.
- Digit credit: Specifies the maximum length credit for having digits in the password. If less than 0, it is the minimum number of digits required.
- **Non-alphanumeric credit**: Specifies the maximum length credit for having non-alphanumeric characters in the password. If less than 0, it is the minimum number of non-alphanumeric characters required.
- **Minimum character classes**: Specifies the minimum number of character classes required. The four classes are digits, uppercase, lowercase and non-alphanumeric characters.

Note: To require 1 character from each class set this value to 4.

- **Maximum class repeat**: Specifies the maximum number of allowed consecutive characters of the same class. The option is disabled if the value is 0.
- **Maximum repeat**: Specifies the maximum number of same consecutive characters allowed. The option is disabled if the value is 0.
- **Character difference**: Specifies the number of characters in the new password that must not be present in the old password during a password change.
- **User real name check**: Checks whether any words, more than 3 characters long, from the account owner's real name (the "User name" field of the account) are contained in the password, in which case the password is not acceptable.
- **Reset non-compliant password**: Forces password change at logon if the password does not comply with the password quality requirements.
- **Forbidden words**: Specifies space separated list of forbidden words (containing more than 3 characters). These are in addition to the words included in the normal cracklib dictionary check.

4.9 Shutdown or Reboot

To shut down, reboot or reconfigure the server:

1. Under **Administration**, click **Shutdown or reboot** in the main menu.
2. Select one of the following actions:
    - **Reboot** - reboots the server after graceful shutdown.
    - **Shutdown** - shuts down the server for service outage or scheduled down time.
3. Click **Perform** and then confirm your selection. Click **Yes** to initiate the action or click **No** to return to cancel the action.

> ℹ **Note**: Each of these functions take several minutes to complete.

4.10 Mitel Virtualization Diagnostics Tool

The intended use of the Virtualization Diagnostic tool is to pinpoint performance and voice quality issues found when running Mitel applications in a virtual environment. The tool is especially helpful for customers who do not have control of the underlying infrastructure but are interested in determining the cause of problems.

The Diagnostic tool is a component of the Mitel Virtualization Framework (MVF) and includes a "Mitel Virtualization" screen that appears within the MSL Server Manager. The screen enables you to obtain an overview of the virtual machine and MVF properties, manage storage monitoring, receive a diagnostic overview, configure a connection to the vCenter server or ESXi hypervisor, and run the diagnostic tool to generate a variety of log files containing statistical, performance and configuration data.

Supported Applications

To employ the Diagnostics tool, you require the following:

- Operating System: MSL 10.0 or higher
- VMware environment: vSphere 4.1 or higher
- Mitel Virtual Framework: MVF 2.0 or higher

Reviewing the Virtual Machine Properties

The "Virtual Machine Properties" table displays information concerning the Virtual Machine and Mitel Virtual Framework. The information is presented in two columns:

- **Current Dimensions**: Lists the configuration at the time that the current Mitel Virtualization page was loaded. Refreshing the page resets the settings.
- **First Boot Dimensions**: Lists the configuration after the Mitel Open Virtual Appliance (OVA) package has been installed and the settings configured, but before the virtual machine has been powered on for the first time.

To review the virtual machine properties:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtual Machine Properties**, review the following settings:

Setting	Description
MVF Version	The version number of the Mitel Virtualization Framework (MVF), a software package that enable Mitel applications to run in a virtual infrastructure. MVF has the capacity to support multiple operating systems and hypervisor products.
Virtualization Agent Version (VMware Tools)	The version number of VMware Tools, a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.
Hypervisor Version	The version number of the VMware ESXi hypervisor that hosts one or more virtual machines and their "guest" operating systems.
vCPU count	The number of virtual Central Processing Units (vCPUs) configured on this virtual machine.
Memory (MB)	The amount of virtual physical memory available for use by the operating system on this virtual machine.
Disk size (GB)	The virtual disk size available for use by the operating system on this virtual machine.
NIC count	The number of virtual network interface cards configured on this virtual machine.
CPU Reservation (MHz)	The guaranteed minimum allocation of CPU resources for this virtual machine.
Memory Reservation (MB)	The guaranteed minimum allocation of memory resources for this virtual machine.
CPU Limit (MHz)	The upper limit of CPU resources that can be allocated to this virtual machine. This limit is expressed in concrete units (Megahertz) and cannot be exceeded.
Memory Limit (MB)	The upper limit of for memory resources that can be allocated to this virtual machine. This limit is expressed in concrete units (Megabytes) and cannot be exceeded.

Setting	Description
vCPU Speed (MHz)	The speed of the virtual CPU, which is dependant on the speed of your underlying processor. So if you have a 12 cores and a processor speed of 3.36GHz, that means a virtual machine with a single vCPU running a single threaded application can consume 3.36GHz. The setting defines what a single vCPU will consume, not the aggregated amount among multiple vCPUs on a single virtual machine. Accordingly, if you have two vCPUs this figure should be doubled.

Managing Storage Monitoring

Use this tool to detect to degrading storage conditions and take corrective actions.

To manage the storage monitoring settings:

1. Under **Administration**, click **Storage Monitoring**.
2. Under **Storage Monitoring**, enter the following settings:

Setting	Description
File System Monitoring	Use this setting to specify whether file system monitoring is enabled or disabled. If the feature is enabled (the default), the system will check for disk I/O errors every five seconds. If any errors are detected, a warning notification is sent to the "admin" email address configured on the Email Settings screen. The following errors are monitored: • File system errors: Errors related to storage degradation • CPU Starvation: When the monitoring process is not dispatched within a specified time (default is 5 seconds), • High I/O Latency: When I/O operations exceed the configured duration time.

Setting	Description
Reboot on Read-Only State	If this setting is enabled (the default), the system will automatically reboot whenever it enters read-only state. After the system reboots, all disk I/O errors will be cleared and the system will be in read-write state. ℹ **Note**:

Setting	Description
	- File System Monitoring must be enabled before this feature can be employed.

Setting	Description
	• Read-only state occurs when there are I/O errors on the virtual machine disk drives, and is intended to protect the file system from damage.

3. Click **Save**.

Reviewing the Diagnostic Overview

The Virtualization Diagnostic tool constantly monitors the system in order to report on three alarm conditions and the state of the last nightly analysis.

To review the virtualization diagnostics overview:

1. Under **Administration**, click **Virtualization**.
2. Under **Diagnostic Overview**, review the following settings:

Condition	Description	States
Hypervisor Version	Indicates whether or not the version of VMware ESXi Hypervisor is supported. The Hypervisor is also known as the Virtual Machine Monitor (VMM).	• **Supported** - Your ESXi version is supported and no changes are required. • **Unsupported** - Your ESXi version is not supported and you must switch to a supported version in order to restore monitoring functionality. For example, if you are running ESXi 4.0 or earlier, you must upgrade to version 4.1 or later.

Condition	Description	States
Current Dimensions	Indicates whether the currently configured application resource dimensions are supported.	• **Supported** - Your configuration is supported and no changes are required. • **Unsupported** - Your configuration is not supported due to a setting (vCPU count, Memory, Disk size, or NIC count) being out of boundaries. To resolve any performance issues, do the following: **a.** Revert to the default configuration for your deployment. For details, see Default Configurations. **b.** Contact Mitel Product Support for assistance.
License Server Connectivity	Indicates whether the Virtual Machine can connect to the Mitel License Server for licensing purposes.	• **Connected** - Your Virtual Machine can connect to the License Server. • **Error** - Your Virtual Machine cannot connect to the License Server. Check the networking configuration and Application Resource ID (ARID). See the *Mitel Standard Linux Installation and Maintenance Guide* for more information.
Last Nightly Analysis	Indicates the date and time that the last nightly analysis was completed, and whether any problems occurred while it was being run. Upon successful completion, the nightly analysis generates the following log file: NIGHTLY-REPORT-YYYY-MM-DD.txt	YYYY/MM/DD & Problems (if any)

Configuring the Virtualization Diagnostics Credentials

To enable the Virtualization Diagnostics tool to collect statistics for the virtual machine and the host, and then use the statistics to generate log files, you must enter credentials for the vCenter server or ESXi hypervisor.

The information collected depends on the credentials entered:

- Admin login to vCenter - full range of features and statistics.
- Read-only login to vCenter - subset of features and statistics.
- Read-only login to ESXi - subset of features and statistics.
- No credentials - Allocation and Reservation & Limits information only.

Note: For optimum results, enter credentials for the vCenter. Entering credentials for the ESXi may result in connectivity problems if settings are changed on the hypervisor.

Enter New Credentials

To enter the virtualization diagnostics credentials:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, enter the following settings:

Setting	Description
FQDN or IP address	Enter the Fully Qualified Domain Name or IP address of the vCenter or ESXi hypervisor.
Username	Enter the username required to access the vCenter or ESXi hypervisor.
Password	Enter the password required to access vCenter or ESX i hypervisor.
Nightly Analysis Time	Specify the one-hour period during which the nightly analysis will be run each day. Select hours between 0-1 and 23-24. Upon successful completion, the nightly analysis generates the following log file: NIGHTLY-REPORT-YYYY-MM-DD.txt.

3. Click **Save**.

Once a connection is established, the system will obtain performance statistics for the virtual machine and the host, and you may click the **Run Diagnostics** button in order to manually generate log files and an online report. For more information, see Manually Generated Log Files.

Note: For a newly installed system, wait for it to collect statistics for at least 15 minutes before clicking the **Run Diagnostics** button.

Remove Current Credentials

To remove the virtualization diagnostics credentials:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, click **Remove**.

You may now enter new credentials.

Note: Without credentials, the system will not collect statistics or generate log files for virtualization diagnostics.

Reviewing the Log Files

The system generates log files containing performance and configuration data plus statistical events.

To view and/or download the log files:

- See View Log Files.

Automatically Generated Log Files

The following log files are generated automatically by the system on a periodic basis.

Report Name	Description
NIGHTLY-REPORT-YYYY-MM-DD.txt	This report contains the previous day's detailed performance and configuration information, and is generated daily in the Nightly Analysis Time you have specified. The system retains seven reports, deleting the oldest file after seven days.
VM-STATS-YYYY-MM-DD.csv	This report contains virtual machine statistics for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.
HOST-STATS-YYYY-MM-DD.csv	This report contains host system statistics for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.
ALL-CONFIG-YYYY-MM-DD.csv	This report contains all CPU, performance and network configuration statistics concerning the host and virtual machine for the previous week. The system polls for new data every 15 minutes and deletes existing data after seven days.

Manually Generated Log Files

A number of log files are created when you request them.

To manually generate the log files and an online report:

1. Under **Administration**, click **Virtualization**.
2. Under **Virtualization Diagnostics**, click **Run Diagnostics**.

Note:

- For a newly installed system, allow it to collect statistics for at least 15 minutes before you click the **Run Diagnostics** button.
- If you repeatedly click the **Run Diagnostics** button, you may exceed the storage capacity of the host server's hard drive.

Report Name	Description
USER-REPORT-YYYY-MM-DD-HH-MM-SS.txt	This report is similar to the NIGHTLY-REPORT-YYYY-MM-DD.txt report, but contains detailed performance and configuration information for the previous week (rather than a single day), collected from the moment you click the **Run Diagnostics** button. The report file is retained for seven days and then deleted. In the event you cannot resolve a problem by yourself, Mitel Product Support will request that you obtain this log file and send it to them. For details, see View/Download Log Files
USER-SUMMARY.tmp	This report is an abbreviated version of USER-REPORT-YYYY-MM-DD-HH-MM-SS.txt report. It contains performance and configuration overviews for each day of the previous week. This report is presented in two formats: • Displayed on the Mitel Virtualization screen. This report is retained until you navigate away from the screen. • Recorded in the log files. This file is retained until the **Run Diagnostics** button is clicked again.
VM-EVENTS-YYYY-MM-DD.csv	The report contains 15 days' activity regarding the oper ation of the Virtual Machine. This file is retained until the Run Diagnostics button is clicked again.

Log File Contents

Although the log files are primarily intended for use by Mitel Product support, you may use them to troubleshoot basic issues with the following issues:

- **Performance Problems**: The system analyzes performance data and if it detects five consecutive "out of bounds" events, an problem will be reported. For example, if the virtual machine waits longer than two seconds to be serviced by the host, five times in a row, the system will report a "CPU Ready" error. Note that system events are registered every twenty seconds.

- **Configuration Problems**: The system checks configuration data and statistical events on an ongoing basis. If a problem is found, and error is logged immediately.

See Analysis Tuning Parameters for detailed information concerning the system settings which control the generation of log file problems.

Performance Problems	Description
CPU Ready (seconds)	The virtual machine has exceeded the maximum amount of time that it can wait to be run on the physical CPU(s). The default is 2 seconds.
CPU Usage (percent)	The virtual machine has exceeded its CPU capacity limit, which is expressed as a percentage of the total amount available. For example, with a limit of 50%, if the virtual machine has four CPUs with 2 GHz processors, and you are running an application that requires 6 GHz (75% of capacity), the limit has been exceeded by 25%. The default is 50%.
Disk Latency (seconds)	The virtual machine has exceeded the maximum amount of time permitted for a SCSI command to be issued by the guest operating system to the virtual machine hard disk. The default is 0.02.
Network Usage (MB)	The virtual machine has exceeded the maximum network utilization (combined transmit and receive rates, in Megabytes per second). The default is 50.0 MB.
Memory Swapped (MB)	The virtual machine has exceeded the maximum amount of memory, in Megabytes, that can be swapped into memory from disk. The default is 0 MB.
Memory Use (MB)	The virtual machine has exceeded the maximum amount of memory capacity that it can use, expressed as a percentage of the total amount available. For example, if the virtual machine has 4 GHz of memory, and you are running an application that requires 3 GHz (75% of capacity), an event will be registered. The default value is 50%.
Number of Packets Dropped (average)	The virtual machine has exceeded the maximum number of received packets that can be dropped at the network interface. The default value is 0.
Disk Usage (MB)	The virtual machine has exceeded the maximum amount of data, in Megabytes per second, that can be read from the virtual machine hard disk. The default value is 30 MB.
Configuration Detections	Description (Yes/No)
High VM-to-host CPU ratio	If "Yes" is displayed, the ESXi host has exceeded the virtual CPU to host CPU ratio, which is 0.79 by default. For example, if five virtual machines with 4 GHz vCPUs are powered on, and the host has 8 physical/16 logical cores, then the ratio is 4 + 4 + 4 + 4 + 4 ÷ 16 = 1.25. Since 1.25 exceeds 0.79, a potential configuration issue is detected.
High VM-to-host Memory ratio	If "Yes" is displayed, the ESXi host has exceeded the virtual memory to host memory ratio, which is 1.20 by default. For example, if five VMs are powered on, each using 2 GHz of memory, and the host has 8 GHz of physical memory, then the ratio is 2 + 2 + 2 + 2 + 2 ÷ 8 = 1.25, which will cause an event to be registered.

Performance Problems	Description
Snapshots Present	If "Yes" is displayed, the system checks to determine if snapshots are supported on the virtual machine. Because snapshots create considerable disk I/O load, use of this feature may degrade the voice quality of calls.
Low CPU Speed (MHz)	If "Yes" is displayed, the maximum speed of the virtual CPU, which is dependant on the speed of the underlying processor on the ESXi host, has been exceeded.
No Hyperthreading (Ignore if running on non-Intel processor)	If "Yes" is displayed, the system checks to determine if hyperthreading is enabled on the ESXi host. **Note**: This parameter can only report on Intel processors that support hyperthreading. It cannot report on AMD or other non-Intel processors.
vMotion occurred	If "Yes" is displayed, the system checks to determine if vMotion is enabled on the ESXi host.
Low CPU Reservation (MHz)	If "Yes" is displayed, the guaranteed minimum allocation of CPU resources for this virtual machine has been exceeded.
Low Memory Reservation (MB)	If "Yes" is displayed, the guaranteed minimum allocation of memory resources for this virtual machine has been exceeded.

Security 5

This chapter contains the following sections:

5.1 Remote Access

5.1.1 About Remote Access

You can access the MiCollabMitel Standard Linux network, either from a computer on the internal network, or from a computer outside the site on the Internet. You can also access the computer network securely from a remote computer.

- PPTP Settings
- Remote Management
- Secure Shell Settings
- Managing Digital Certificates

5.1.2 PPTP Settings (Client-to-Server VPN)

The Point-to-Point Tunneling Protocol (PPTP) is used to create client-to-server Virtual Private Networks (VPNs).

The IP addresses for PPTP clients are allocated from within the local subnet range managed by the DHCP server. The addresses are taken from the last portion of the range, and the number used depends on the “Number of PPTP clients” that you program.

For example, if you program “10” as the “Number of PPTP clients” for local subnet 192.168.1.10 to 192.168.1.100, then the last ten addresses in the range (.11 to .100) will be allocated to PPTP clients for VPNs.

If necessary, you can increase the total number of addresses available to all clients by modifying the local subnet range. For details see Configure DHCP Server.

VPN access and configuration

To enable VPN access:

1. Under **Security** click **Remote access**.
2. Under **PPTP Settings** in the Remote Access panel, enter the number of individual PPTP clients that will be allowed to connect to the server simultaneously. This can be the total number of remote PPTP clients in the organization, or, if you have a slow connection to the Internet and do not want all of those PPTP clients to connect at the same time, enter a lower number. Enter 0 to deny PPTP connections.
3. Click **Save**. The server is now ready to accept PPTP connections.

Setting Up a VPN Connection on Clients

Use the following procedures to set up a VPN connection on each user's computer:

> **Note**: The following procedures outline how to create and configure a VPN connection in Microsoft Windows 7. For instructions to perform these procedures in another operating system, refer to your product documentation.

To create a VPN connection on the user's computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the Connection Option list, select **Connect to a Workplace**.
4. Select **No, create a new connection** if prompted, and then click **Next**.
5. Select **Use my Internet connection**.
6. Enter the server **IP address** or **host name**.
7. Enter a **name** for your VPN connection.
8. Select **Don’t connect now; just set it up** and then click **Next**.
9. Enter your **user name**. Password is not required if you are using certificate for authentication.
10. Click **Create** and then click **Close**.

To configure a VPN connection on the user's computer:

1. Click **Start > Control Panel > Network and Sharing Center**.
2. In the left-hand menu, click **Change adapter settings**.
3. Right-click your VPN name and then click **Properties**.
4. On the Networking tab, select **Internet Protocol Version 4** and then click **Properties**.
5. Click **Advanced**.
6. Clear the **Use default gateway on remote network** check box.
7. Click **OK** twice to return VPN Connection Properties dialog.
8. On the Security tab, in the Type of VPN list, select **Point to Point Tunneling Protocol (PPTP)**.
9. Under Authentication, select **Use Extensible Authentication Protocol (EAP)**.
10. In the EAP list, select **Microsoft: Smart Card or other certificate**.
11. Click **Properties**.
12. Under “When connecting” select **Use a certificate on this computer** and then select **User simple certificate selection**.
13. Choose whether to validate the server certificate. When selected, Windows prompts users to confirm that they're connecting to the correct server and that the certificate is valid. If you choose to enable validation, clear the **Connect to these servers** check box.

14. Click **OK** until you return to the Control Panel > Network Connections dialog.
15. Right-click on your VPN name and then click **Connect**.

Remote Management

Remote management allows hosts on the specified remote IPv4 and IPv6 network(s) to access the server manager of your MSL server. To limit access to the specified host, enter a subnet mask of 255.255.255.255 for IPv4 networks or a CIDR prefix of /128 for IPv6 networks. If your mask allows a range of IP addresses, any hosts within that range can access the server manager using HTTPS. See also Grant Access Privileges to Trusted Local Networks.

To add a remote management network:

1. Under **Security**, click **Remote access**.
2. Scroll to the Remote Management section.
3. In the **Network** field, enter the IP address of the remote host for which you want to allow access.
4. In the **Subnet mask** field, enter a mask to limit the range of access (255.255.255.255 limits access to the specified IP address).
5. Click **Save**.

Secure Shell Settings

About the Secure Shell

Use the Secure Shell Settings section to control access to your server. The public setting should only be enabled by experienced administrators for remote problem diagnosis and resolution. We recommend leaving this parameter set to "No Access" unless you have a specific reason to do otherwise.

⚠ **Warning**: Before allowing secure shell access to the server using standard passwords, please ensure you set a secure admin/root password on the server. With a weak password, an internet- facing server can be compromised very quickly.

Configuring SSH (Secure Shell)

SSH (secure shell) provides a secure, encrypted way to log in to a remote machine across an IPv4 or IPv6 network, or to copy files from a local machine to a server. Programs such as telnet and ftp transmit passwords in plain, unencrypted text across the network or the Internet. SSH and its companion program SCP provide a secure way to log in or copy files. For more information about SSH Communications Security and its commercial products, visit http://www.ssh.com/.

OpenSSH, included with the MSL server, is a version of the SSH tools and protocol. The server provides the SSH client programs as well as an SSH server daemon and supports the SSH2 protocol.

To configure SSH:

1. Under **Security**, click **Remote access**.
2. Scroll to the Secure Shell Settings section.

3. Select a Secure shell access option:

   - **No Access** – (Default) SSH access not allowed.
   - **Allow access only from trusted and remote management networks** – This option enables you to access the server from local networks and remote management networks. To add a remote management network, see **Remote Management**.
   - **Allow public access (entire Internet)**– This option enables you to access the server from anywhere on the Internet. It is selectable only if you have configured a strong SSH (system admin) password. If you have weak password and attempt to select this option, you will receive the following warning: "The system administration password is set to a weak value. The "Allow public access" option in the form below will remain disabled until the system administration password has been reset to a strong value."

4. Program the configuration options:

   - **Allow administrative command line access over secure shell** - This option allows someone to connect to the server and log in as "root" with the administrative password. The user would then have full access to the underlying operating system. This can be useful if someone is providing remote support for the system, but in most cases we recommend setting this option to No.
   - **Allow secure shell access using standard passwords** - If you set this option to Yes, users will be able to connect to the server using a standard user name and password. This may be a concern from a security point of view, in that someone wishing to break into the system could connect to the SSH server and repeatedly enter user names and passwords in an attempt to find a valid combination. A more secure way to allow SSH access is called RSA Authentication and involves copying an SSH key from the client to the server.

5. Click **Save**.

Once SSH is enabled, connect to the server by launching the SSH client on the remote system. Ensure that it is pointed to the external domain name or IP address for the server. In the default configuration, you will be prompted for your user name. Enter "admin" and the administrative password. You will be in the server console. From here you can change the server configuration, access the Administrator Portal through a text browser or perform other server console tasks.

> ℹ **Note**: By default, only two user names can be used to log in remotely to the server: "admin" (to access the server console) and "root" (to use the Linux shell). Regular users are not permitted to log in to the server.

Obtaining an SSH Client

A number of different free software programs provide SSH clients for use in a Windows or Macintosh environment. Several are extensions of existing telnet programs that include SSH functionality. Two different lists of known clients can be found online at http://www.openssh.com/windows.html and http://www.freessh.org/.

A commercial SSH client is available from SSH Communications Security at: http://www.ssh.com/products/ssh/download.html. Note that the client is free for evaluation, academic, and certain non-commercial uses.

5.2 Configure Port Forwarding

Port Forwarding allows you to modify your firewall rules so that the port you need is opened, and forwarded to another port on another host. This is typically done to provide network services from a server inside of your private LAN, permitting incoming traffic to directly access one of your private hosts.

⚠ **CAUTION**: Misuse of this feature can compromise the security of your network.

In the Administrator Portal, under **Security**, click **Port forwarding**. On the panel that appears, a table lists the current port forwarding rules.

To create a port-forwarding rule for TCP or UDP traffic:

1. Under **Security**, click **Port forwarding**.
2. Click **Create Port forwarding rule**.
3. Enter the following information:
   - **Protocol**: select either TCP or UDP.
   - **Source Port**: enter the number of the port that is to be forwarded.
   - **Destination Host IP Address**: enter the IP address of the machine to which the traffic on the Source Port is to be forwarded.
   - **Destination Port**: enter the port on the Destination Host to which the traffic is to be forwarded.
   - **SNAT**: select to enable Secure Network Address Translation.
4. Click **Add**.

To remove a port forwarding rule, select the rule from the table of current rules and click **Remove**.

ℹ **Note**: Port Forwarding is not available in a server-only configuration.

5.3 Configure Syslog

MSL includes a syslog server for message logging. When a system event occurs, such as a failed authentication attempt or login failure, the affected service generates a message which is recorded in a log file. You can examine these messages in the Log File Viewer.

You can enhance this functionality by enabling the local system to accept syslog messages from remote hosts, and by enabling the local system to send its own syslog messages to remote hosts.

Receiving Messages from Remote Hosts

You can configure the local syslog server to accept event messages from other syslog servers, provided that they are in list of trusted networks. The event messages can be received over UDP (using port 514) and TCP (using a configured port).

To start receiving syslog event messages from remote hosts:

1. Under **Security**, click **Syslog**.
2. Under **Accept syslogs from remote hosts**, do the following:
   a. In the **Accept remote syslog on UDP** field, click **Enable**.
   b. (Optional) In the **Accept remote syslog on TCP** field, click **Enable**. In the **Listen Port** field, enter a port number (for example, 514), and then click **Save**.

The local system can now receive syslog event messages from remote hosts.

To stop receiving syslog event messages from a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Accept syslogs from remote hosts**, locate the protocol you wish to disable (UDP or TCP).
3. Click **Disable**.

Sending Messages to Remote Hosts

You can configure the local syslog server to forward its own event messages to one or more other syslog servers.

To start sending local syslog event messages to a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Forward local syslogs**, click **Add remote syslog destination**.
3. In the **Configure syslog** screen, do the following:
   a. In **Facility**, select type of program or subsystem that is logging the message. By default, the **auth** facility code (security/authorization messages) is selected. You may also select **authpriv** (messages generated internally by syslogd) or any other facility code. For a complete list of facility code descriptions, see RFC 3164.
   b. In **Destination Host (ip:port)**, enter the IP address and port number of the remote syslog server.

   > **Note**:
   >
   > - A port number is required only if TCP is selected as the transport.
   > - You can enter multiple destination hosts, provided that they use the same facility and port number. Use commas to separate the individual entries.

   c. In **Protocol**, select the transport, either **UDP** or **TCP**.
4. Click **Next**, and then click **Add**.

   The local system will new forward syslog event messages to the designated remote host(s).

To stop sending local syslog event messages to a remote host:

1. Under **Security**, click **Syslog**.
2. Under **Forward local syslogs**, locate the host you wish to disable.
3. Click **Remove** twice.

5.4 Certificates

5.4.1 About SSL Web Server Certificates

Overview of SSL Web Server Certificates

An SSL web server certificate authenticates the identity of a web site and encrypts information passed between the web server and the web client using Secure Sockets layer (SSL) technology.

A default self-signed SSL certificate is provided with the MSL server at no additional cost. You can instruct remote users to install this certificate in their workstations in order to prevent the “Certificate Error: Navigation Blocked” message from appearing when they attempt to log in to the MiCollabMitel Standard Linux Server Manager.

For enhanced security and ease of use, obtain a signed SSL certificate from a third-party Certificate Authority (CA). Two options are available:

- **Let's Encrypt**: Let’s Encrypt is a free, automated, and open Certificate Authority. It enables you to obtain a valid SSL certificate simply by providing your domain settings and then clicking a button. The acquired certificate is monitored and renewed automatically. This service is supported on single-server, standalone MSL systems that are accessible to the Internet.
- **Other 3rd-Party**: An alternative third-party Certificate Authority issues an SSL certificate upon request, typically for a fee. Companies such as Entrust and GoDaddy provide such services. To obtain a generic SSL certificate, you must first generate a Certificate Signing Request (CSR) on the MSL system and send it to the CA. The CA will then return a package containing your web server certificate, plus any intermediate certificates that are required to maintain the certificate key chain. Optionally, you can download the SSL certificate and private key from the local MSL server, and upload these files to other servers in your domain.

As with the self-signed SSL certificate, a third-party SSL certificate enables remote users to log in to the MiCollabMitel Standard Linux Server Manager without receiving an error message. It also allows MiCollab Mobile Client users to establish connections and receive their deployment configurations.

For more information and programming instructions, see:

- Manage Let's Encrypt Third-Party SSL Web Server Certificates
- Manage Alternate Vendor Third-Party SSL Web Server Certificates
- Manage Self-Signed SSL Web Server Certificates

5.4.2 Manage Third-Party Certificates from Let's Encrypt

Let’s Encrypt is a free, automated, and open Certificate Authority (CA). It enables you to obtain a valid web server certificate simply by providing your domain settings and then clicking a button. The acquired certificate is uploaded, installed, monitored and renewed automatically. You do not need to generate a certificate signing request (CSR) or go through the manual process of installing the certificate. These steps are handled by the CA and the local MSL server, and are invisible to you.

Note:

- To use this service, the MSL server must be accessible to the Internet, either directly or through a proxy.
- The service is currently not supported on servers under the following deployment configurations:
- Any server behind a MiVoice Border Gateway Web Proxy version earlier than v9.4.
- MiCollab with AWV in server-only (LAN) mode behind a MiVoice Border Gateway in server-gateway mode on the network edge with 2nd WAN IP address configured on the MBG Web Proxy for MiCollab Audio, Web and Video Conferencing if the MBG Web proxy version is earlier than v9.4.0.25.
- The service is supported on any MSL system that meets the following criteria:
- Each FQDN configured in the certificate request must be resolvable from the external Let's Encrypt server.
- An https request to each resolved FQDN above with a URL of the form https://FQDN/.well-known/acme-challenge/CHALLENGE_TOKEN must reach and be responded to by the server on which the Let's Encrypt certificate request has been made.
- When you request an SSL certificate from the Let's Encrypt service, you must provide a Common Name and, optionally, Subject Alternative Names as fully qualified domain names (FQDNs) that are resolvable to addresses on the public network. When the Let's Encrypt servers issue an HTTP request to a resolved FQDN (such as https://mbg.mitel.com/.well-known/acme-challenge/random_file_name), this request must be able to reach the MSL server on port 80 on which the certificate request is being made. Accordingly, the MSL server must be accessible to the Internet, either directly or through a proxy.

Programming Steps

To implement a Let's Encrypt SSL certificate, complete the following procedures:

- Request a Let's Encrypt SSL Certificate
- Modify a Let's Encrypt SSL Certificate (required only if you wish to update your credentials)
- Uninstall a Let's Encrypt SSL Certificate (required only if you wish to resume using the default self-signed certificate)
- Verify the Installed Let's Encrypt SSL Certificate

Request a Let's Encrypt SSL Certificate

To request a Let's Encrypt SSL certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Get Certificate**.

5. Enter the information required to request the SSL certificate from the Let's Encrypt system:

Field Name	Description
Status	Indicates the status of the certificate, either enabled (successfully installed and active) or disabled (not successfully installed and inactive)
Contact E-Mail	Enter the email address of the administrator who Let's Encrypt should contact to deal with issues of certificate recovery or registration.
Common Name	Enter the common name to which you plan to apply your certificate. A web browser checks this field. It is required. The common name must be entered as a fully-qualified domain name (FQDN) that is publicly resolvable. Do *not* enter a domain name with a wild card character (e.g. *.example.com) because Let's Encrypt does not support wild card certificate requests.
Alternate Name(s)	Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied. The FQDNs must be publicly resolvable.

6. Click **Get Certificate**. The Let's Encrypt system generates the certificate and returns it to the MSL system for automatic installation. If there are any problems with the certificate request or installation, an error message is displayed. If there are no problems, the Status field displays "enabled," indicating that the certificate has been successfully installed and is now active.

Modify a Let's Encrypt SSL Certificate

To modify a Let's Encrypt SSL certificate request:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Modify Request**.
5. Update the field values as required in order to modify your certificate signing request (CSR).
6. Click **Get Certificate**. The Let's Encrypt system generates the SSL certificate and returns it to the MSL system for automatic installation. If there are any problems with the certificate request or installation, an error message is displayed. If there are no problems, the Status field displays "enabled," indicating that the certificate has been successfully installed and is now active.

Uninstall a Let's Encrypt SSL Certificate

To uninstall a Let's Encrypt SSL certificate and resume using the self-signed certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Remove Certificate**. The MSL system uninstalls the Let's Encrypt SSL certificate and returns to using the default self-signed certificate.

Verify the Installed Let's Encrypt SSL Certificate

To view details regarding currently installed web server certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate: C: country code ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority OU: name of the organizational unit CN: server hostname Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid From	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires. **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

5.4.3 Manage Third-Party Certificates from an Alternate Certificate Authority

To enable remote client stations to log in and MiCollab Mobile Client users to establish connections, you can purchase an SSL certificate from a alternate third-party Certificate Authority and then import it onto the MSL server.

If you have an MSL application server deployed in LAN mode with an MBG / Web Proxy server in the demilitarized zone (DMZ) or network edge, your remote clients will connect to the MSL server through the MBG / Web Proxy server. For this configuration, purchase an SSL certificate for the MBG / Web Proxy server and then share the certificate and private key file with the LAN-based MSL servers.

If you have MSL application servers deployed in LAN mode behind a corporate firewall, your remote clients will connect to the MSL servers through the firewall. For this configuration, purchase a unique SSL certificate for each MSL server.

Supported Formats

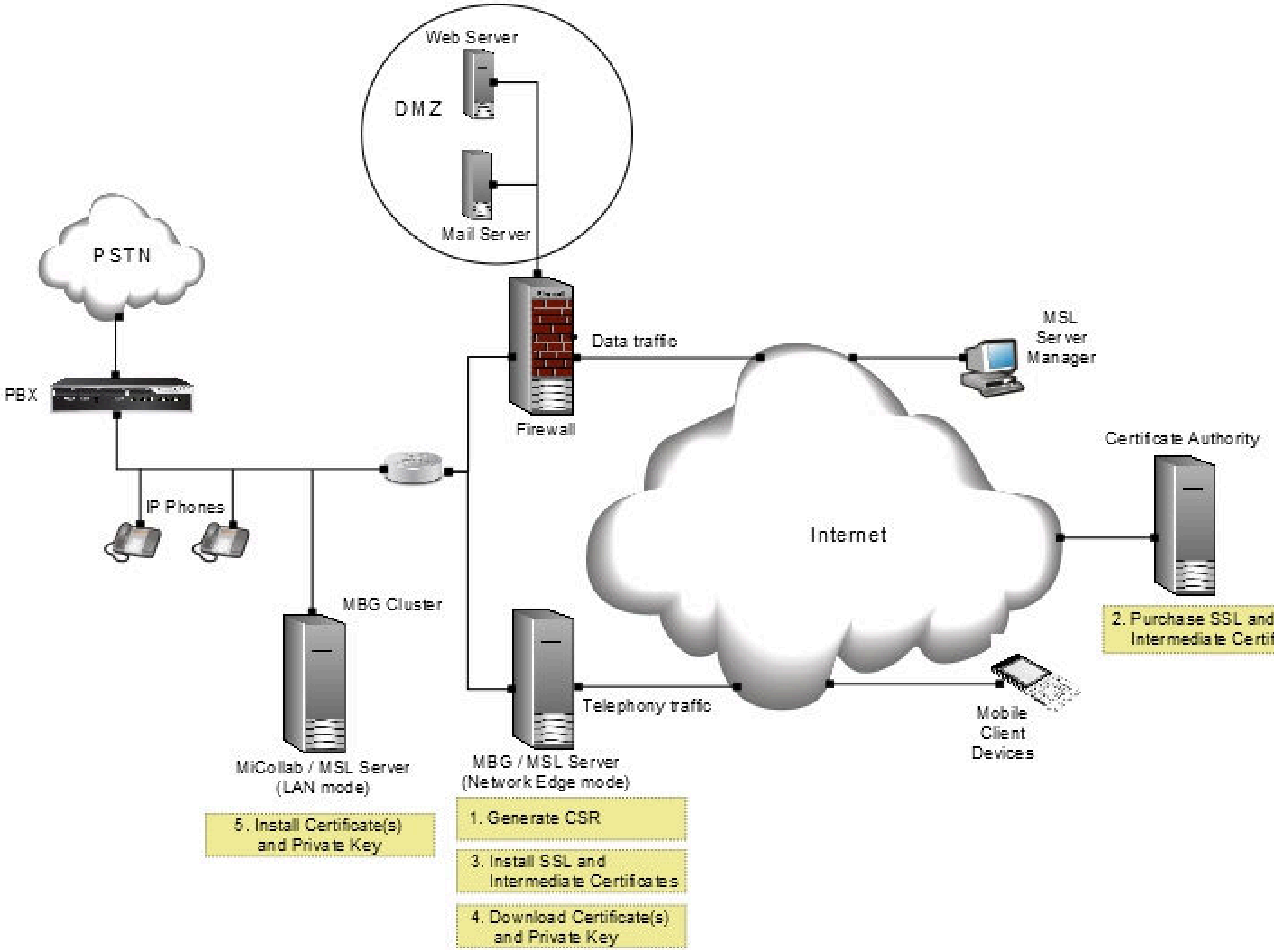
You can import third-party SSL certificates in either PEM or PKCS#12 format:

- **PEM** certificates typically have extensions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format. Apache and similar servers use PEM format certificates. Several PEM certificates, including the private key, can be included in a single file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files.
- **PKCS#12** or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as .pfx and .p12. PFX files are typically used on Windows machines to import and export certificates and private keys.

MSL supports the SHA-2 cryptographic hash function, along with variants such as SHA-256.

Configuration Example

The illustration, below, demonstrates the five basic steps that must be completed to implement a third-party SSL certificate when you have an have an MSL application server in LAN mode with an MBG / Web Proxy on the network edge. First, generate the certificate signing request (CSR) on the MBG / Web Proxy. Second, submit the CSR to the CA, complete the online registration forms and purchase your web server certificate and intermediate certificates. Third, install the certificates on the MBG / Web Proxy (the MSL server that was used to generate the CSR). Fourth, download the certificates and private key from the MBG / Web Proxy. Fifth, install the certificates and private key on the MSL application server on the LAN. The application server can be equipped with Mitel software such as MiVoice Business, MiCollab Client, Open Integration Gateway, Oria or, as illustrated below, MiCollab.


Web Server
DMZ
Mail Server
PSTN
PBX
Firewall
Data traffic
MSL Server Manager
Certificate Authority
IP Phones
Internet
2. Purchase SSL and Intermediate Certif
MBG Cluster
Telephony traffic
Mobile Client Devices
MiCollab / MSL Server (LAN mode)
MBG / MSL Server (Network Edge mode)
5. Install Certificate(s) and Private Key
1. Generate CSR
3. Install SSL and Intermediate Certificates
4. Download Certificate(s) and Private Key

Programming Steps

To implement a third-party SSL certificate, complete the following procedures:

- Generate a CSR and Purchase the SSL Certificate OR Enroll for a web server certificate issued by Enterprise CA using SCEP
- Install the SSL Certificate Files on the MSL Server
- Install the SSL Certificate Files on other MSL Servers (required only if your deployment has LAN-based MSL application servers accessed via an MBG / Web Proxy)
- Uninstall the SSL Certificate (required only if you wish to resume using the default self-signed certificate)
- Verify the Installed SSL Certificate

Enroll for a web server certificate issued by Enterprise CA using SCEP

To automatically enroll for a web server certificate issued by a local Enterprise CA using the Simple Certificate Enrollment Protocol (SCEP), select the Enterprise CA - SCEP Enrollment option.

To enroll for a web server certificate issued by a Enterprise CA using SCEP, do the following:

1. Log into the **MSL Server Manager**.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Enterprise CA - SCEP Enrollment** option.
5. Click **Perform**.
6. Fill out the SCEP form:
    - **CA Address**: the FQDN or IP address of the SCEP server
    - **URI Path**: the URI to use in SCEP communication (defaults to Windows SCEP URI for clients)
    - **Enrollment Password**: the enrollment challenge password if required
    - **Common Name**: the Common Name to use in the Certificate Signing Request (CSR) (defaults to the system hostname)
    - **Alternate Name(s)**: the Subject Alternate Name(s) to include in the CSR
7. Click **Get Certificate**.
8. Upon submitting the form, the data is validated and access to the SCEP server is verified. On successful verification, the SCEP enrollment is initiated to request a certificate, a progress status of the SCEP transaction is provided.
    - If the enrollment request is rejected, check the SCEP server for the details of the failure.
    - If the enrollment request is in pending state, the administrator of the SCEP server needs to approve or deny the certificate request.
9. Reload the MSL server manager for the newly acquired web server certificate to take effect.

Generate a Certificate Signing Request (CSR) and Purchase the SSL Certificate

You need a certificate signing request (CSR) in order to purchase an SSL certificate from an alternate third-party Certificate Authority (CA).

To generate a CSR and purchase the third-party SSL certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Generate a new Certificate Signing Request (CSR)**, and then click **Perform**.
5. Enter the information required to generate a certificate signing request (CSR). If you have previously generated a CSR, the previously entered values are displayed.

Note: When completing the fields, use first capital letters only (for example Ontario, not ONTARIO).

Field Name	Description
Country Name (two letter code)	Enter the two-letter International Organization for Standardization- (ISO-) format country code for the country in which your organization is legally registered. Examples are, CA for Canada and US for United States.
State or Province Name	Enter the full name of state or province where your organization is located. Do not abbreviate. The first letter of the name entered must be a capital with remaining letters lower case. For example, you would enter "Ontario" for Mitel Corporation.

Field Name	Description
Locality Name	The Locality Name is the city, town, route used in the mail address of the organization that is submitting the CSR. Enter the full name of the city in which your or ganization is located. Do not abbreviate.
Organization Name	The Organization Name is the name used in the mail address of the organization / business submitting the CSR. Enter the name under which your organization / business is legally registered. The listed organization must be the legal registrant of the domain name in the trusted certificate request. If you are enrolling as an individual, please enter the certificate requestor's nam e in the Organization field, and the DBA (doing busi ness as) name in the Organizational Unit field.
Organizational Unit Name	Enter the organization unit or department name. Use this field to differentiate between divisions within an organization. For example, "Engineering" or "Human R esources." If applicable, you may enter the DBA (doing business as) name in this field.
Common Name	Enter the common name for the service to which you plan to apply your certificate. A web browser checks this field. It is required. The common name can be entered as a fully qualified domain name (FQDN) or as a domain name with a wild card character (e.g. *.example.com) in order to generate a wild card certificate request. The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com).

6. Check to ensure that you have entered all the required information correctly before you generate the CSR. If you need to make changes, regenerate the file. Do NOT modify the text of the generated file in a text editor such as Notepad.
7. Click **Generate Certificate Signing Request**. The system generates a CSR file.
8. Copy the text of the CSR file.

9. Access the web site of a Certificate Authority and purchase a certificate. You will be prompted to do the following:

> **Note**: Each Certificate Authority has unique requirements. Accordingly, you may not be prompted for all of the steps listed below, and some of the field names may vary.

a. Select the number of domains you wish to protect:

- **Single domain**: Select this option if your implementation has one MSL server on a single domain (eg. www.domain.com and domain.com).
- **Multi-domain**: Select this option if your implementation has multiple MSL servers on a specific number of domains (eg. www.domain.com and domain.com, plus three sub-domains).
- **Multi-domain and wildcard**: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (eg. eg. www.domain.com and domain.com, plus an unlimited number of sub-domains).

b. Enter your account and contact details in the CA web form:

- **Login Name** and **Password**.
- **Name**, **Email Address**, and **Telephone Number**.
- **Organization Name and Address**.
- **Domain Name**.

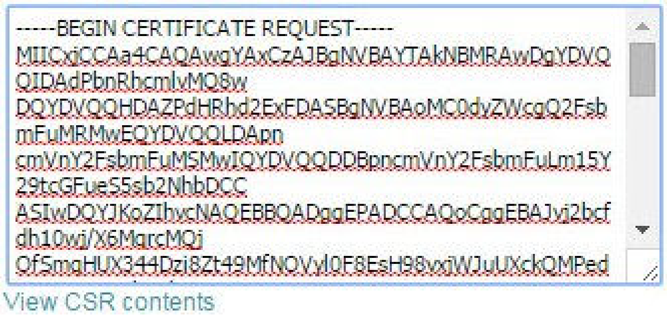
> **Note**: Some CAs may prompt you to enter the Subject Alternate Names (SANs) or wildcard domain in this step. For more information on these entries, see below.

- **Web Server Software**.

> **Note**: Select **Apache**. Other options are *not* supported on the MSL platform.

- **Hashing Algorithm**.

c. Paste the text of the CSR file into the CA web form.



```
-----BEGIN CERTIFICATE REQUEST-----
MIICxjCCAa4CAQAwgYAxCzAJBgNVBAYTAkNBMRAwDgYDVQ
QIDAdPbnRhcmlvMQ8w
DQYDVQQHDAZPdHRhd2ExFDASBgNVBAoMC0dyZWcgQ2Fsb
mFuMRMwEQYDVQQLDApn
cmVnY2FsbmFuMSMwIQYDVQQDDBpncmVnY2FsbmFuLm15Y
29tcGFueS5sb2NhbDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJvj2bcf
dh10wj/X6MqrcMQj
OfSmqHUX344Dzi8Zt49MfNOVyl0F8EsH98vxjWJuUXckQMPed
```

d. If you have purchased a certificate for multiple domains or a wildcard domain, enter the following in the CA web form:

- **Subject Alternate Name** (SAN): Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied.

Note: You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.

- **Wildcard**: To consolidate your domain and unlimited sub-domains into a single SSL certificate, enter a wildcard domain name. For example, if your deployment includes numerous MSL application servers on the LAN (for example, MiCollab, MiVoice Business, MiCollab Client, MiCollab Unified Messaging, generic MSL, and Oria), you can include them all by entering an FQDN such as *.mitel.com.

10. Complete the purchase transaction. The Certificate Authority will do the following:

- Send you the certificate files.

  These include your SSL server certificate and, if required, intermediate certificates. An intermediate certificate is a subordinate certificate issued to establish a certificate chain that begins at the CA's trusted root certificate, carries through the intermediate and ends with your own SSL server certificate. Some CAs provide a single intermediate certificate while others provide multiple intermediate certificates. There should be no need to open and inspect the files, provided that they are in the correct format and that the intermediate certificates have been bundled into a single file by the CA. Consult the documentation provided by your Certificate Authority for instructions to obtain, unzip and identify exactly which files you need to use.

Note:

- If your CA requires you to open a number of intermediate certificates and assemble them into a single bundled file, perform this task with a text editor that employs Unix line formatting. Do not use an editor that employs Windows line formatting such as Notepad.
- The intermediate certificate is required for MiCollab Mobile Client deployments; without it, client connections will fail and users will be unable to download their deployment configurations.
- Contact the administrator for the domain used in a CSR.

  The administrator is identified using information supplied when your organization originally registered its internet FQDN.

11. Upload the certificate files to a location that is accessible to the MSL server.

Install the SSL Certificate Files on the MSL Server

Use the following procedure to install the certificate files that you received from the alternate third-party Certificate Authority onto the MSL server that generated the CSR. The Upload and install a web server certificate option supports only certificates and keys based on RSA algorithm for upload.

To install the SSL certificate files on the MSL server:

1. Log into the MSL Server Manager for the system that was used to generate the CSR.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.

4. Select **Upload and install a web server certificate**, and then click **Perform**.

> **Note**:
>
> This option only supports certificates and keys based on RSA algorithm for upload.

5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the SSL certificate, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the Intermediate SSL certificate, select it and click **Open**.

> **Note**:
>
> - In some cases, the CA will provide multiple intermediate certificates. Consult the CA's documentation to determine which of these certificates you should use and, if necessary, how to assemble them into a single bundled file.
> - The intermediate certificate is required for MiCollab Mobile Client deployments; without it, client connections will fail and users will be unable to download their deployment configurations.

7. Click **Install Web Server Certificate**. If there is a problem with the certificate chain of trust, MSL will display an error message instructing you to take corrective action. You may need to contact your CA for assistance.
8. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence. Perform this step at a time of low system activity.

> **Note**: Some services, such as the MiCollab Client Service and WebRTC, are restarted automatically as soon as you install the certificate. This removes the need for you to restart the server manually.

Install the SSL Certificate on other MSL Severs

If your deployment includes LAN-based MSL application servers accessed via an MBG / Web Proxy server, use the following procedure to install the certificate files on them. This is a two-step process. First, you must download the web server certificate, intermediate certificates (if installed), and private key file corresponding to the SSL server certificate from the MBG / Web Proxy. Second, you must upload these files to the LAN-based MSL servers.

Download certificates

To download the SSL certificate files from the MBG / Web Proxy:

1. Log into the MSL Server Manager for MBG / Web Proxy (the system that was used to generate the CSR).
2. Under **Security**, click **Web Server**.

3. Click the **Web Server Certificate** tab.
4. Select **Download the current web server certificate**, and then click **Perform**.
5. Click **Save**, navigate to the location you wish to store the file, and then click **Save**. The downloaded file is in ZIP format. It includes the web server certificate, intermediate certificates (if installed), and private key file.
6. Unzip the files and upload them to a location that is accessible to the other MSL servers in your network.

> **Note**: Exercise caution when transferring your certificate files and private key to the other system. If your private key is stolen, it can be used to establish fraudulent connections to your applications. For optimum security, delete the files from any media they are stored on as soon as you have completed the upload process.

Upload certificates

To upload the SSL certificate files to a LAN-based MSL server:

1. Log into the MSL Server Manager for a LAN-based MSL server.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.

   > **Note**:
   >
   > This option only supports certificates and keys based on RSA algorithm for upload.

5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the SSL certificate, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the Intermediate SSL certificate, select it and click **Open**.
7. Import the private key pair created on the other MSL server:
   - Beside the **SSL Private Key** field, click **Browse**.
   - Navigate to the SSL Private Key file, select it and click **Open**.
8. Click **Install Web Server Certificate**.
9. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence. Perform this step at a time of low system activity.

   > **Note**: Some services, such as the MiCollab Client Service and WebRTC, are restarted automatically as soon as you install the certificate. This removes the need for you to restart the server manually.

10. To prevent fraudulent use of your certificates, delete the certificate and private key files from any media they are stored on.

Uninstall the SSL Certificate

To uninstall SSL certificate and resume using the self-signed certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Uninstall the third-party web server certificate**, and then click **Perform**. The MSL system uninstalls the SSL certificate and returns to using the default self-signed certificate.

Verify the Installed SSL Certificate

To view details regarding currently installed web server certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate:
	C: country code
	ST: state or province
	L: locality name (for example: city name)
	O: name of the certificate authorization authority
	OU: name of the organizational unit
	CN: server hostname
	Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid From	Date and time when the certificate takes effect.

Field Name	Details
Expires	Date and time when the certificate expires. **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

5.4.4 Manage Self Signed SSL Certificates

A default self-signed SSL certificate is provided with the MSL server at no additional cost. Remote users can add it to their local workstations. This prevents the “Certificate Error: Navigation Blocked” message from appearing when the users attempt to log in to the MiCollabMitel Standard Linux Server Manager.

The self-signed SSL certificate has the following disadvantages:

- The protection supplied by the self-signed SSL certificate is somewhat lower than that of a third-party SSL certificate.
- The self-signed SSL certificate can only be used to prevent the “Certificate Error: Navigation Blocked” message. For MiCollab Mobile Client deployments, you *must* purchase and install a third-party SSL certificate. If you fail to do this, your MiCollab Mobile Client users will not receive their deployment configurations and will be unable to establish connections.

The following procedure applies to Internet Explorer 11. For other browser versions refer to the browser help.

Note: If you are using Windows Vista or Windows 7, you will need to run Internet Explorer as an administrator to install the security certificate. To do this, right-click the Internet Explorer icon, and select **Run as Administrator**. This task needs to be done even if you are logged in as an administrator.

Install the Default Self-Signed SSL Certificate on Local Workstation

To install the default self-signed certificate on a local workstation:

1. Open Internet Explorer.
2. When you attempt to access the MiCollabMitel Standard Linux Server Manager login page, a "Certificate Error: Navigation Blocked" page is displayed. The warning states "There is a problem with this web site's security service".
3. Click "Continue to this web site (not recommended)".
4. To the right of the domain name address in the address bar, click Certificate Error. The Untrusted Certificate warning appears.
5. Click **View Certificates**.
6. Click **Install Certificate**.

7. In the Certificate Import Wizard, click **Next** to accept the default settings.
8. Click **Place all certificates in the following store** and then click **Browse**. Select **Trusted Root Certification Authorities** and then click **OK**.
9. Click **Next** and then **Finish**. A security warning appears, asking if you want to install the certificate.
10. Click **Yes**. The certificate import is confirmed. Click **OK**.
11. Click **OK** to close the **Certificate** dialog.

Note: After you have installed the security certificate, a second security certificate error may appear stating that the security certificate presented by the website was issued for a different website's address. This is a temporary problem and the error should be ignored. Click "Continue to this website" to access the Web View interface.

Verify the Installed Default Self-Signed SSL Certificate

To view details regarding currently installed default, self-signed web server certificate:

1. Log into the MiCollabMitel Standard Linux Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. View details at the top of the page:

Field Name	Details
Issuer	Lists the following information for the certificate auth orization company that issued the certificate: C: country code ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority; "XYZ Corporation" is the name that appears for Mitel self-si gned certificates. OU: name of the organizational unit CN: server hostname Authority/ emailAddress: email address of the Certificat e Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in this certificate.
Valid From	Date and time when the certificate takes effect.

Field Name	Details
Expires	Date and time when the certificate expires. ℹ **Note**: Events are raised prior to, and on the date of expiry of the certificate. Ensure to regularly check the event viewer or configure email alerts. • Certificate already expired: **MAJOR** • Expires in less than 1 week: **MINOR** • Expires in less than 3 weeks: **WARNING**

5.4.5 Manage TLS Protocol

For MiCollab 8.1 or later, by default, MSL supports the use of TLS v1.1 and v1.2 for communications security. For earlier releases, MSL supports the use of TLS v1.0 by default. To migrate to the latest TLS version, you must upgrade your MiCollab for PC Client and MiCollab for Mobile Client to MiCollab 8.1 or later, and then disable support for the TLS v1.0 protocol using the following procedure. After these steps are complete, your system will be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

ℹ **Note**:

- With MSL 10.6 release and later, new installations have the TLSv1.0 protocol disabled by default. The protocol can still be enabled, if required, from the **Web Server** panel.
- Existing customers have the option to disable the TLSv1.0 protocol from the **Web Server** panel.
- It is not disabled by default on upgrade to MSL 10.6 release.

Disable Support for TLS v1

To disable support for the TLS v1 protocol:

1. Log into the MiCollabMitel Standard Linux Server Manager for a LAN-based MSL server.
2. Under **Security**, click **Web Server**.
3. Click the **TLS** tab.
4. To disable support for TLS version 1.0, clear **Allow TLS v1.0**.

   Your system is now in compliance with PCI DSS.

Note:

- If you disable support for TLS version 1.0, users who employ older web browser such as Internet Explorer 9 or 10 will be denied Server Manager access. To resolve this problem, users should switch to using a newer browser or enable TLS version 1.2 in their existing browsers. In Internet Explorer, the TLS settings are located under Options > Advanced > Security.
- Some services, such as the MiCollab Client Service, are restarted automatically whenever you update the **Allow TLS v1.0** setting. This ensures that the services are updated correctly.

TLS v1.3 Support

From MiCollab 10.1 onwards, the following interfaces support TLS 1.3:

From MiCollab Server to:

- Microsoft Exchange Server (Office 365)
- Google Calendar
- Apple Push Server
- Firebase Cloud Messaging (FCM)
- External Directory

From MiCollab Clients *(iOS, Android, PC, Mac, Web)* to**:**

- MiCollab Server

From NuPoint UM Server to:

- Microsoft Exchange Server (Office 365)
- Google Email
- NuPoint UM End User Web Portal
- NuPoint UM Server

Additionally, OAuth 2.0 (Microsoft Graph) is the only Office 365 authentication method currently supporting TLS 1.3 for Calendar Integration. Other Office 365 protocols continue to use TLS 1.2.

Note: No specific configuration is required on the MiCollab side to enable TLS 1.3. It is enabled by default, and the system automatically falls back to TLS 1.2 if the remote interface does not support TLS 1.3.

5.4.6 Certificate Authority Trust

The **Certificate Authority** (CA) **Trust** tab allows the administrator to upload additional root CA certificates, in PEM format, to be added to the list of trusted CA certificates on MSL.

Some customers have their own enterprise root CA certificates, used to sign the certificate that will be installed on the MSL web server. To install a certificate signed by an untrusted CA, the root CA certificate must first be uploaded to and trusted by the server.

To upload a new root CA certificate to the CA trust bundle:

1. In the **Certificate Authority Trus**t tab, click **Choose File**.
2. Browse to the location of the certificate, and click **Open**.

> **Note**: The certificate must be in PEM format.

3. Click **Install Root CA Certificate**.

By default, the following two Mitel root CA certificates are added to the Trust Store. These are visible in the **Certificate Authority Trust** tab.

- The legacy root CA certificate is named **Mitel Networks Root CA**. This is used to complete a full chain of trust between Mitel legacy equipment and applications such as MBG.
- The new Mitel root CA certificate is named **Mitel Products Root CA** and will be used in new products going forward.

Configuration 6

This chapter contains the following sections:

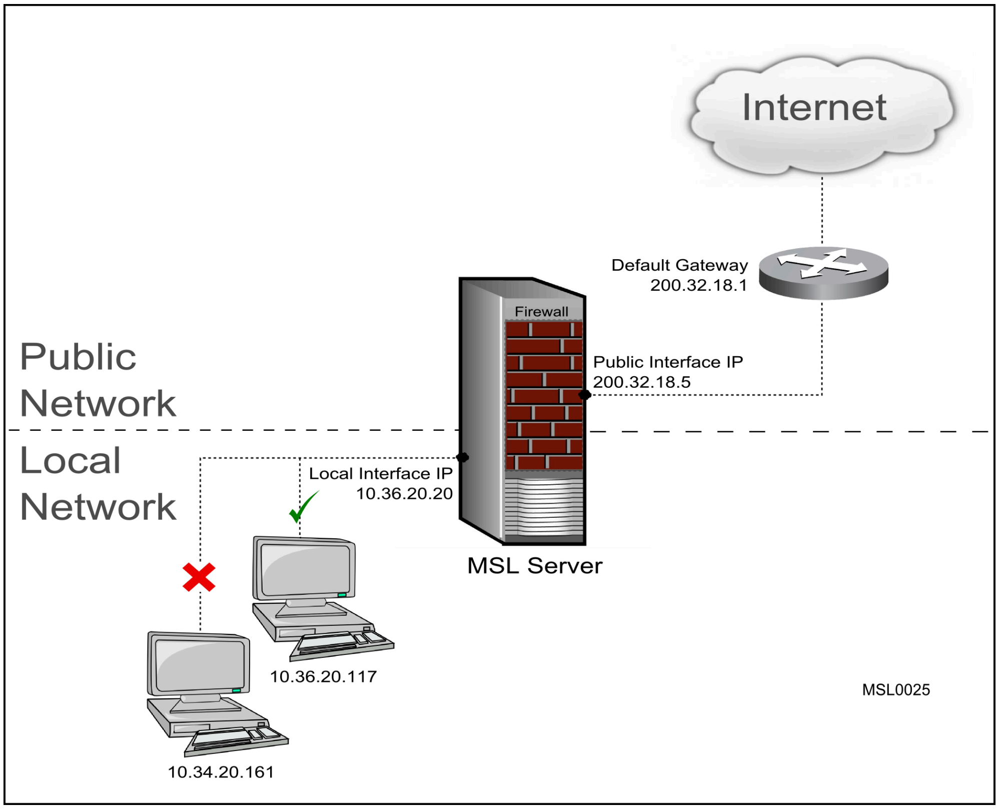
6.1 Configure Networks

Grant Access Privileges to Trusted Local Networks

By default, several MSL services, including server manager access, SSH and system monitoring, are accessible only from computers that are located on the same network where the MSL server is installed. If you need to manage the server from a different subnet on the LAN, then you must configure the other subnet as a "Trusted Network." This configuration opens the firewall and allows access to the services on the MSL server.

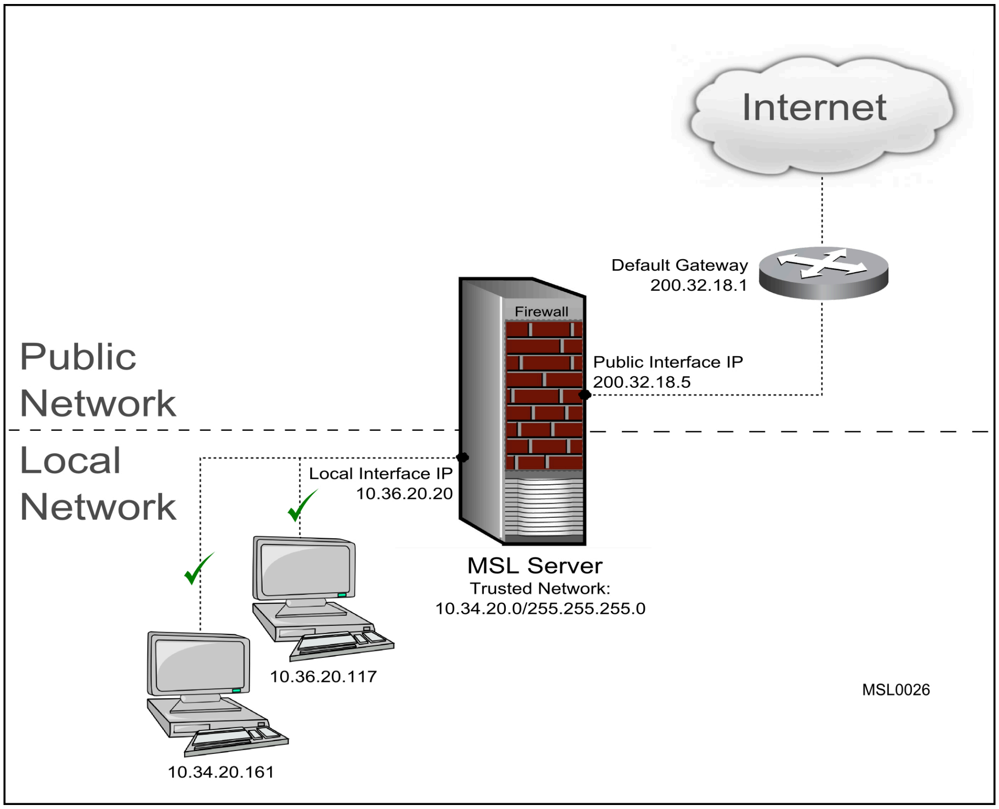
Example of Default Routing Configuration

In the example illustrated below, the LAN interface of the MSL server has an IP address of 10.36.20.20. Accordingly, the server will accept traffic *only* from the 10.36.20.x network while blocking traffic from all other subnets on the LAN.



Example of Trusted Network Configuration

In the example illustrated below, the MSL server has been configured an IP address of 10.36.20.20 on its LAN interface and with a "trusted network" of 10.34.20.0/255.255.255.0. Accordingly, the server will accept traffic from both the 10.36.20.x and 1034.20.x subnets.



Note:

- If only one network is being serviced by the server, you do not need to add any information here.
- Adding a "trusted network" automatically opens the firewall:
  - allows access to the HTTP services on the MSL server
  - allows access to all MiVoice Business network services
- If your server has an IPv6 address configured on its LAN interface, then you can extend privileges to IPv6 networks as well as IPv4 networks. (IPv6 is not supported by MiVoice Business)
- Use the **Secure Shells Settings** topic in **MSL Server Manager** document to control access to HTTP and SSH services to specified networks..
- If you only need to enable traffic to/from remote (or "untrusted") servers but not want them to access MSL services, simply add a network route.
- Depending on the architecture of your network infrastructure, the instructions for configuring the clients on an additional network may be different than the following instructions. For more information about adding networks, contact your authorized Mitel Reseller.

To extend privileges to one or more additional networks:

1. Under **Configuration**, click **Networks**.
2. Click **Add a new trusted network**.
3. In the **Network Address** field, enter the IPv4 or IPv6 address of the network to designate as “local”.

4. In the **Subnet mask or network prefix length** field, enter the dot-decimal subnet mask or CIDR network prefix to apply to the Network Address. If this field is blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.

> ℹ **Note**: If you are using the Mitel Performance Analytics (MPA) application for analyzing the MiVoice Business system, then:
>
> - Refer the **Secure Shells Settings** topic in **MSL Server Manager** document to enable Secure Shells for trusted and remote management networks.
> - Add trusted network for the MPA with **Network** as the IP address of MPA and **Subnet mask or network prefix length** as 255.255.255.255.

5. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
6. Click **Add**.

Add Network Routes

Use this procedure to add new routes to the MSL server's routing table. This configuration opens the firewall and enables traffic to flow to/from remote servers but does *not* grant access to the MSL services (as would adding a trusted network).

> ℹ **Note**:
>
> - The additional network routes are firewalled.
> - Adding additional network routes is an advanced option and should only be used if you have a thorough understanding of both routing and your network topology.

To add additional network routes:

1. Under **Configuration**, click **Networks**.
2. Click **Add a new network route**.
3. In the **Network Address** field, enter the IPv4 or IPv6 address of the network route.
4. In the **Subnet mask or network prefix length** field, enter the subnet mask or CIDR prefix to apply to the Network Address. If this field is left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.
5. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
6. Click **Add**.

6.2 Configure E-mail

This page allows you to configure the server e-mail settings.

1. Under **Configuration**, click **E-mail Settings**.
2. Click the **Change** button beside the setting you want to change.

3. Configure the settings as required and then click **Save**:

Setting	Description
Server to use for outbound SMTP	The server can deliver outgoing messages via a corporate or Internet service provider's SMTP server, or can deliver messages directly to their destination (by looking up mail exchanger records in DNS). If using a specific SMTP server, specify its hostname or IP address. Otherwise leave this field blank.
Destination port for outbound SMTP	If you have specified a server to use for outbound SMTP, select the destination port for outbound SMTP messaging: • **Port 25** (use cleartext; default) • **Port 465** (SSL encryption) • **Port 587** (TLS encryption)
Mail Server User ID	If you are using secure SMTP (port 465 or 587), enter the user ID required by the SMTP server. This ID must be configured and licensed in the SMTP server.
Mail Server Password	If you are using secure SMTP (port 465 or 587), enter the password required by the SMTP server. This password must be configured in the SMTP server.
SMTP e-mail injection restrictions	Controls which networks will be allowed to send mail through this server via SMTP. Choose from one of the following three settings: • **Localhost only** – accept e-mail only from applications installed on the server (default setting). • **Accept only from trusted networks** – accept e-mail from trusted local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.) • **Accept from anywhere** - accept all e-mail

Setting	Description
Forwarding address for administrative e-mail	By default, e-mail to the administrator is sent to the user " admin" at the domain name configured on the server. You can override the default by entering an e-mail address in this field. ℹ **Note**: RAID array event notifications are sent to this e-mail address. We recommend that you configure a valid address here.
E-mail sent for events:	Check the system events for which you want to receive e-mail notifications. The e-mails are sent to the " admin" mailbox. To turn off e-mail notifications clear all the event boxes.

6.3 Cloud Service Provider

6.3.1 Google

6.3.1.1 About Google Apps Integration

When Mitel Standard Linux applications such as NuPoint UM and MiCollab Client require access to user-generated data that is stored in Google Gmail or Google Calendar, they must meet Google's authentication requirements. Google grants access only when the following conditions are met:

- the application provides its authentication information, and
- the user consents to allow the application to view the account information

All applications that access Google must be registered through the Google APIs Console and must configure access using the Open Standard for Authentication 2.0 (OAuth 2.0) protocol.

OAuth 2.0 is a relatively simple protocol. To begin, you register your application with Google in order to creates a client ID. Then your client application requests an access token from the Google Authorization Server, extracts a token from the response, and sends the token to the Google API that you want to access.

When you create a client ID, you must specify the type of application it is for. For integration with Mitel applications, two options are available:

- Installed Application - Select this option if the application is to be installed on a mobile device, tablet or computer. The registration process results in a client ID and a client secret, which you embed in the source code of the application. MiCollab Client requires this configuration.

- Service Accounts - Select this option if the application employs server-to-server interactions, such as those between a web application and Google Cloud Storage. MiCollab Audio, Web and Video Conferencing and NuPoint Unified Messaging require this configuration.

> **Note**: Support for OAuth 1.0 was deprecated with MSL Release 10.1. If you are currently using OAuth 1.0 and upgrade to the latest MSL software, you should reprogram API access for your application using an OAuth 2.0 Service Account. After you have done this, the OAuth 1.0 tab will be removed from the server manager interface. For new software installations, only OAuth 2.0 is available.

6.3.1.2 Google Apps Integration for MiCollab Audio, Web and Video Conferencing

With this release, MiCollab Audio, Web and Video Conferencing can be integrated with Google Apps. This enables users to transform their Google Calendar events into one-time conferences simply by clicking a gadget. In future releases, more features will be added such as the ability to initiate calls from Google Calendar.

Preconditions:

- In the System Options, select **Use HTTPS Only**. You must then configure a third-party SSL certificate in the MSL Server Manager. Note that you may not employ the self-signed certificate; using it will cause Google Apps integration to fail.
- In the Web Conferencing Settings, enter 80 for the **Internal Port** and 443 for the **External Port**.

Administrator tasks

Enable Google Apps Integration with MiCollab Audio, Web and Video Conferencing

The administrator must do the following:

1. Configure OAuth 2.0 for Service Accounts

   When you set up an OAuth 2.0 API project with a service account for the Google Calendar application, you enable MiCollab Audio, Web and Video Conferencing to prove its identity to Google. The two systems can then communicate without involving end users.
2. Configure the Gadget Address

   The gadget address is the publicly accessible FQDN or IP address of the gadget service. After you configure it on the MSL server, users can download the Google- MiCollab Audio, Web and Video Conferencing gadget and transform their Google Calendar events into conferences with a single click. Users will receive a link to the address in their Welcome Email (see next step).
3. Send the Service Information (Welcome) Email

   The Welcome Email contains communications settings such as the user's login credentials, email address and phone number, along with instructions on how to download and configure the Google-

MiCollab Audio, Web and Video Conferencing gadget. You should ensure that the Welcome Email is sent to all new and existing users.

4. Configure the Web Proxy

   You must configure your web proxy server to provide a secure interface between Google on the Internet and the MiCollab server on the LAN. If your enterprise is using MiVoice Border Gateway as a proxy server, access the LAN server proxy list and select **MiCollab** as the LAN server and **Google Calendar Integration to AWV** as the user interface (for configuration details, refer to the *MBG online help*). If your enterprise is using a proxy server from another manufacturer, configure it to forward Google Apps traffic (i.e. traffic that includes "google" as part of the FQDN in HTTPS requests) to the MiCollab server.

End-User tasks

Change the Password and Enable MiCollab Audio, Web and Video Conferencing Conference Functionality

Each user must do the following:

1. In your Welcome Email, click the link to the MiCollab End User Portal : https://< MiCollab server address>/portal
2. Log in to the portal using your account information (ID and password).
3. Change your password:
   - Select **Portal Password**.
   - Enter your old password and your new password in the appropriate fields.
   - Confirm your new password and then click **Save**.
4. In your Welcome Email, click the link to enable MiCollab Audio, Web and Video Conferencing conference functionality in your Google Calendar.
5. Select **Yes** to download and install the gadget.
6. Configure the gadget for use:
   - Click **Permissions** and then, in response to the prompt, click **Allow access**.
   - Enter your **Login ID** and **Password**.
   - Click **Save** to complete the configuration.

To create an MiCollab Audio, Web and Video Conferencing conference, access your Google Calendar, select a one-time or recurring event and click **Collaboration** check box in the gadget.

After setup is complete, you can join the conference simply by clicking on the event. Any changes you make to the event, such as adding more guests or changing the start time, will be reflected in the MiCollab Audio, Web and Video Conferencing conference.

ℹ **Note**:

- If you have just upgraded your system to include Google Apps integration, re-send the Welcome Email to all existing users.
- A conference that was created using the Google- MiCollab Audio, Web and Video Conferencing gadget can be viewed on the My Conferences Tab of the MiCollab Audio, Web and Video Conferencing Web Interface. However, if you edit this conference in the MiCollab Audio, Web and Video Conferencing interface, your updates will *not* be reflected in the Google Calendar.
- The Google- MiCollab Audio, Web and Video Conferencing gadget is available only for English variants of the product.
- To enable Google- MiCollab Audio, Web and Video Conferencing conferencing functionality, you must complete all three steps of the above-noted procedure.
- This feature can be expected to behave differently on different devices and browsers. It is optimized for operation on Google Chrome in a desktop environment. If you are using Internet Explorer and the MiCollab server is not equipped with proper certificates, you will need to install the Mitel Root Certificate in your browser.

  Internet Explorer

  ℹ **Note**: Steps may vary based on your browser, but the intent is to install the Mitel Root Certificate in the **Trusted Root Certification Authorities** store.

  1. Save the Mitel Root Certificate on your PC hard drive.
  2. Launch Internet Explorer.
  3. Select **Tools** and then click **Internet Options**.
  4. Click the **Content** tab and then click the **Certificates** button.
  5. Select **Trusted Root Certification Authorities** and click **Import**. The Certificate Import Wizard opens.
  6. Click **Next**.
  7. Click **Browse** and browse to the **mitelcert.cer** file and click **Open**.
  8. Click **Next**.
  9. Select **Place all Certificates in the following store**.
  10. Click **Browse** and select **Trusted Root Certification Authorities**.
  11. Click **OK**.
  12. Click **Next**.
  13. Click **Finish**.
  14. Click **Yes**. An Import was successful dialog appears.
  15. After the certificate is installed, restart Internet Explorer.
- In some circumstances, a user's Google Calendar may fall out of synchronization with MiCollab Audio, Web and Video Conferencing. For example, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference and then quickly closes their Google Calendar or internet browser, MiCollab Audio, Web and Video Conferencing may fail to create a corresponding conference. Similarly, if the user creates a new Google- MiCollab Audio, Web and Video Conferencing conference while the MiCollab server is being rebooted, a corresponding conference will not be created in MiCollab Audio, Web and Video Conferencing . To correct an out-of-sync error, the user should delete the event in Google Calendar and then recreate it.

6.3.1.3 Google Gadget Configuration

Google provides a framework for users and third parties to implement enhancements to Google Apps called "gadgets." MiCollab Audio, Web and Video Conferencing provides a gadget which users can employ to transform their Google Calendar events into one-time conferences with a simple click.

> ℹ **Note**: For complete instructions concerning how to implement the Google gadget, see the Google Apps Integration for AWV topic.

Address Configuration

Use this procedure to configure the publicly accessible address of the gadget service. Typically, this is external address of the firewall (IP address or FQDN), which should be configured to forward HTTP requests to the gadget service.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Gadget Configuration** tab.
4. Click **Edit**.
5. Enter the **External FQDN or IP address** of the MSL server. Typically, this is the publicly accessible address configured on the enterprise firewall configured to forward requests to the MSL server. The MiVoice Border Gateway can provide this service if it is configured to function as a web proxy for the Google Calendar integration to AWV.

   > ℹ **Note**: Google gadget users will receive a link to this address in their Service Information (Welcome) Email

6. Click **Save**.

6.3.2 Microsoft

6.3.2.1 Configure Microsoft Identity

The OAuth 2.0 protocol is the authentication and authorization method used with the Application identity to access the API permission(s) granted by the tenant administrator.

To configure the Microsoft Identity on MSL, and administer access to the Microsoft resources using the Application identity created in your tenant directory, perform the following on the Microsoft Entra portal:

1. Register an application, see Microsoft help.
2. Obtain the unique Application ID and Tenant ID assigned by Microsoft Entra ID.

Note:

The customer's firewall settings should allow access to the following Microsoft resources:

- outlook.office365.com
- login.microsoftonline.com
- graph.microsoft.com

Perform the following steps under **Cloud Service Provider** to complete the authorization related configuration at MSL:

1. Log in to MSL Server Manager as administrator.
2. Under **Configuration**, click **Cloud Service Provider** > **Microsoft**.
3. Complete the Configuration form:

   - **Tenant directory**

     a. Tenant Name (Optional): Enter a descriptive name for the tenant directory. This field is optional.
     b. Tenant ID: Enter Directory (tenant) ID from the Microsoft Entra ID. This field is mandatory.
   - **Application Identity**

     a. Application Name (Optional): Enter the descriptive name for the application created during application registration. This field is optional.
     b. Application ID: Enter the Application (client) ID from the Microsoft Entra ID. This field is mandatory.
     c. Application Secret: Enter the client secret obtained from the application Certificates & Secrets page. This field is mandatory.

   Note:

   - Certificate-based authentication is not supported at this time.
   - Once the secret is copied, it cannot be retrieved again; if the secret is lost, another one needs to be created.
   - The admin can revoke the secret by deleting it, in which case a new secret is required.
4. Click **Save.**

Note: After a backup restore, the Application Secret will remain intact in the MiCollab if server is restored from an Encrypted backup in the Enterprise. In Google Cloud Platform (GCP), the Application secret will be restored after a backup/restore.

6.4 Configure DHCP Server

Use the Dynamic Host Configuration Protocol (DHCP) panel to configure and manage the behavior of the internal DHCP server.

> **Note**: Do not enable the internal DHCP server if another DHCP server exists on the network.

To enable DHCP:

1. On the **DHCP Service** tab, click **Edit**.
2. Click **Enable DHCP Service** to enable the internal DHCP server.
3. Click **Allow BootP** to allow network clients to obtain IP addresses using the Bootstrap Protocol.

DHCP Configuration

To add a subnet:

1. On the **Subnets** tab, click **Add subnet.**
2. In the **Name** field, enter the name to apply to this subnet.
3. In the **Subnet IP address**, enter the IP address of the subnet to add.
4. In the **Subnet Mask** field, enter the mask to apply to this IP address.
5. (Optional) In the **Router** field, enter the IP address of the router used to access the subnet.
6. Click **Save**.

To remove a subnet:

1. On the **Subnets** tab, click the Remove link associated with the subnet you want to remove.
2. Click **Save**.

To add a subnet range:

If you have enabled DHCP and added a subnet, you must provide a subnet range.

1. On the **Subnets** tab, click **Add range**.
2. In the **Range start** field, enter the IP address at which to start the range of IP addresses available for assignment.
3. In the **Range end** field, enter the IP address at which to end the range.
4. In the **Lease time** field, enter the number of seconds to hold DHCP leases or accept the default setting.
5. Click **Save**.

To add a Static Host:

1. On the **Static Hosts** tab, click **Add Host**.

2. In the **Hostname** field, enter a name for the static host.
3. In the **Host IP** field, enter the static IP address of the host.
4. In the **MAC address** field, enter the MAC address of the host.
5. In the **Client ID (type, value)** field, select a type and enter a corresponding value.
6. Click **Save**.

To add DHCP options:

1. In the **Scope** field, select the scope to apply to this option. (Global, Subnet, Range, or Host)
2. Select the option type for this option (Standard, Vendor, or Site-local).
3. Do one of the following:
4. For **Standard** options, select an option number from the list.
5. For **Vendor** options, select a vendor option from the list.
6. For **Site-local** options, enter an option number between 224 and 254. Click **Next** and then enter **Name**, **Format**, and **value** for the new option.
7. Click **Save**.

To view the state of all dynamic leases:

- On the **Lease View** tab, click **Refresh** to see the most recent version of the list.

6.5 Configure Server Date and Time

You can configure the date and time:

- manually, or
- by configuring the server to obtain the date and time from a Network Time Server on the internet. A network time server communicates the time to other computers over the Internet using Network Time Protocol (NTP).

To set your date and time manually:

1. Under **Configuration**, click **Date and Time**.
2. Click **Set System Time Zone** and select your time zone from the list.
3. Enter the date and time in the fields provided.
4. Select **Enable Network Time Server** to instruct the server to periodically synchronize the system clock to a network time protocol (NTP) server. If you select this option, enter the hostname or IP address of the NTP server in the field provided.
5. Click **Save**.

To obtain the date and time from a Network Time Server:

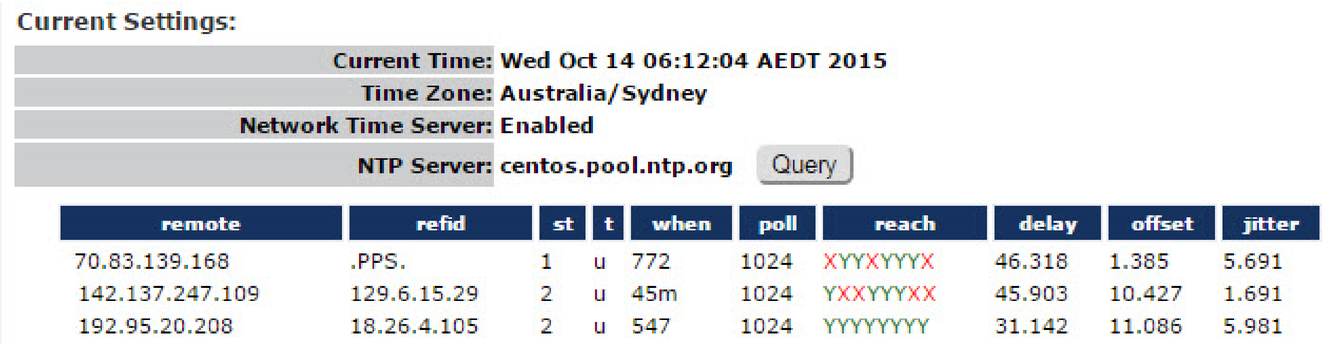
1. Click **Enable Network Time Server**.
2. Enter the hostname or IP address of a Network Time Server.
3. Click **Save**.

Note:

For more information about using a network time server, visit http://www.ntp.org/. You can also find a list of publicly available time servers at http://www.eecis.udel.edu/~mills/ntp/servers.dita. You should always use a secondary time server (also called a stratum 2 server) to lighten the load on the primary time servers.

To verify that your network time protocol server is set up properly:

1. After you have **saved** the hostname or IP address of a new Network Time Server, click the **Query** button. Clicking the **Query** button issues the **ntpq -c peers** Linux command.

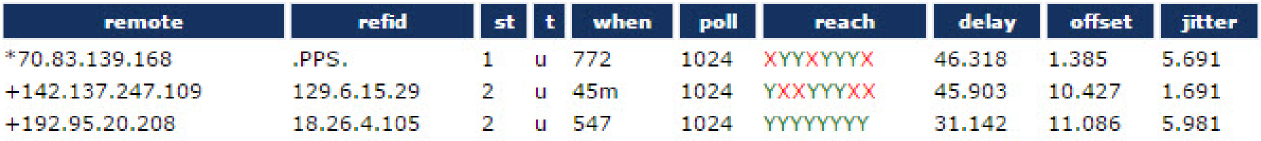


Current Settings:

Current Time:	Wed Oct 14 06:12:04 AEDT 2015
Time Zone:	Australia/Sydney
Network Time Server:	Enabled
NTP Server:	centos.pool.ntp.org

remote	refid	st	t	when	poll	reach	delay	offset	jitter
70.83.139.168	.PPS.	1	u	772	1024	XYYXYYYX	46.318	1.385	5.691
142.137.247.109	129.6.15.29	2	u	45m	1024	YXXYYYXX	45.903	10.427	1.691
192.95.20.208	18.26.4.105	2	u	547	1024	YYYYYYYY	31.142	11.086	5.981

2. The command results are displayed for the NTP server (or for a list of servers if a pool is referenced by the specified hostname or IP address).



remote	refid	st	t	when	poll	reach	delay	offset	jitter
*70.83.139.168	.PPS.	1	u	772	1024	XYYXYYYX	46.318	1.385	5.691
+142.137.247.109	129.6.15.29	2	u	45m	1024	YXXYYYXX	45.903	10.427	1.691
+192.95.20.208	18.26.4.105	2	u	547	1024	YYYYYYYY	31.142	11.086	5.981

3. After a few minutes, press **Query**again. An * appears in front of one of the NTP servers. The * indicates that the system time is being synchronized with that NTP server.

The following table provides the meaning of the command output:

<table>
<tr><th>Command output</th><th colspan="2">Meaning</th></tr>
<tr><td rowspan="2">remote</td><td colspan="2">The hostnames or IP addresses of the remote NTP servers to which the system can be synchronized (based on the pool of available NTP servers). The character that precedes the hostname or IP address indicates the following:</td></tr>
<tr><td>*</td><td>The system time is being synchronized with the NTP server.</td></tr>
</table>

Command output	Meaning	
	#	The host is selected for synchronization, but distance from the host to the server exceeds the maximum value.
	o	The host is selected for synchronization, and the PPS signal is in use.
	+	The host included in the final synchronization selection set.
	x	The host is the designated false ticker by the intersection algorithm.
	.	The host is selected from the end of the candidate list.
	-	A host discarded by the clustering algorithm.
	blank	Indicates a host is discarded due to high stratum and/or failed sanity checks.
refid		The current source of the synchronization for the remote host.
st		The stratum used by the remote host. The lower the number, the closer you are to the time source. Stratum 16 indicates that the system is not synchronized with a time server.

Command output	Meaning	
t		The type of clock used on the NTP server (L stands for local clock; u for an Internet clock).
when		The number of seconds since the last poll.
poll		The number of seconds between NTP transactions. When this time expires, the NTP daemon polls the remote time server. The polling results are displayed in the "reach" field.
reach		The status of the last eight NTP transactions, with each transaction represented by a colored letter. The letter "Y" in green indicates that a response was successfully received from the remote time server. The letter "X" in red indicates that a response was not received. Since this field is a circular log buffer, it is continually refreshed, with the most recent result on the right and the oldest on the left. Example: If the field contains XXXXXXYY, the two most recent NTP transactions have been successful while the previous six have failed.
delay		Indicates the time, in milliseconds, between an NTP request and the answer.
offset		The difference in milliseconds between the time on your local computer and that on the NTP server.

Command output	Meaning	
Jitter		The error rate in your local clock, expressed in milliseconds.

To switch from a Network Time Server to a manual time zone configuration:

1. Click **Disable Network Time Server** and then click **Save**.
2. Select your time zone.
3. Enter the date and time in the fields provided.
4. Click **Save**.

Note: A reboot is required to update any running applications with new date/time information.

6.6 Add or Delete Hostnames and Addresses

You can add or delete devices (servers, computers, printers) to your network by adding the hostname or IP address to the MSL server.

Under **Configuration**, click **Hostnames and Addresses**. The form lists hostnames and addresses of the devices that are currently in the managed network.

Field	Description
Hostname	Displays the hostname of the device.
Location	**Local**: a hostname with an IP on a local network **Remote**: a hostname with an IP on a remote network **Self**: alternative hostname for this host
IP Address	IP address on local network.
Ethernet Address	IP address accessible from Internet.

To add the hostname of a network device:

1. Under **Configuration**, click **Hostnames and Addresses**
2. Click **Add Hostname**.
3. Enter the **Hostname**. The hostname must start with a letter or number and must contain only letters, numbers, and hyphens.

4. From the **Domain** list, select the Domain where this host resides.
5. In the **Location** list, select visibility (Local, Remote, Self).
6. Click **Next**.
7. Confirm the details and then click **Add**.

To edit the location of a hostname:

1. Under **Configuration**, click **Hostnames and Addresses**.
2. In the current list of hostnames, click the Modify link that corresponds to the hostname you want to modify.
3. Edit Location and then click **Next**.
4. Confirm the details and then click **Save**.

To remove the hostname of a network device:

1. Under **Configuration**, click **Hostnames and Addresses.**
2. In the current list of hostnames, click **Remove** in the Action column.
3. Click **Remove**.

6.7 Manage Domains and DNS Settings

This form allows you to define the Domain Name Service (DNS) that will be associated with the MSL server. This name will be the default domain for the email and web server. You can also use this form to configure other virtual domains in the network.

Caution: Do not change the primary domain name after you have set it up. If you do, you will have to reboot the server and all of the clients, and users may have to manually modify items such as Web browser bookmarks that point to the server.

To define the DNS name for the MSL server:

1. Under **Configuration**, click **Domains**
2. Click **Modify Corporate DNS settings**.
3. Enter the primary and secondary DNS server IP addresses if this server does not have access to the Internet, or if you have special requirements for DNS resolution. Leave these fields blank unless you have a specific reason to configure other DNS servers. Do not enter the address of your ISP's DNS servers because the server is capable of resolving all Internet DNS names without this additional configuration.
4. Click **Save**.

To configure other virtual domains:

1. Click **Add Domain**.
2. Enter the **Domain Name** and a brief description.
3. For the web site, you may choose your primary web site or any i-bay as the content.

4. Select whether this domain is **Resolved locally**, passed to the **Corporate DNS servers**, or resolved by the **Internet DNS servers**. The default will be correct for most networks.
5. Click **Add**.

6.8 Configure IPv6 in IPv4 Tunnel

To enable isolated IPv6 hosts and networks to reach each other over an existing IPv4 network infrastructure, you can configure an IPv4-in-IPv6 tunnel. At the tunnel head end, IPv6 packets are encapsulated into IPv4 packets and sent to the remote tunnel destination. At the destination, the IPv4 packet headers are stripped and the original IPv6 packets are forwarded into the IPv6 cloud.

Until the IPv4 and IPv6 protocols are able to run on the same network infrastructure using dual-stack technology, a transitional mechanism such IPv4in-IPv6 tunnelling is required to facilitate communication.

ℹ **Note**: Similar to Port Forwarding, this feature is not available in a server-only configuration. It is only available when the server is operating in server-gateway mode.

Preconditions

- The IPv4 address of the remote endpoint must be reachable via ICMP (Internet Control Message Protocol).
- If you are behind a firewall, please make sure it allows passage of Internet Protocol 41. This protocol is contained in the IPv4 header and indicates that an IPv6 packet is encapsulated within the IPv4 packet.

To configure an IPv4-in-IPv6 tunnel:

1. Under **Configuration**, click **IPv6-inIPv4**.
2. Configure the settings as required and then click **Save**:

Setting	Description
IPv4 Address of the Remote End	Enter the IPv4 address of tunnel destination. This address must be routable on the IPv4 network. Typically, it is the external interface of the router located at the destination.

Setting	Description
IPv6 Address of the Tunnel (Optional)	If the MSL server is functioning as a gateway to the internet, you can configure its external tunnel interface with an IPv6 address. This enables the interface to be addressable by IPv6 traffic. You may configure only one address on this interface. If this field is left blank, no address will be assigned to the external tunnel interface on the MSL server. **Note**: Your service provider provides this IPv6 address.
IPv6 Networks	Enter one or more IPv6 network addresses for the destination. Based on these entries, the system creates a routing table that defines the ultimate destination of the IPv6 packets that are being tunneled. You can enter a single address or a block of addresses (specified by writing a slash (/) followed by a number which defines the length of the network prefix in bits). Use commas to separate multiple entries.

6.9 Configure SNMP Support

SNMP (Simple Network Management Protocol) provides a set of operations and a protocol to permit remote management and remote monitoring of a network device and/or its services. This server currently offers support for remote monitoring via get requests and traps using both IPv4 and IPv6 protocols.

Note: SNMP service is disabled by default.

Configure SNMP Settings

To configure SNMP support:

1. Under **Configuration**, click **SNMP**.
2. Set **Service status** to **Enabled** to support SNMPv1, SNMPv2c, and SNMPv3.

3. Complete the following fields as required and then click **Save**.

Field	Description
SNMPv2c community string for read-only access	Enter the community string that SNMPv2c clients use to monitor this server via get requests and traps. The community string defaults to "public".
SNMPv2c network access setting	Select the network access setting for SNMPv2 services: • Localhost only - Default setting. • Immediate local network only - Allows access to local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.) • All configured trusted networks - Allows access to all networks that are configured in the Networks panel. These networks may not be on the same subnet as the server (that is, they may be attached via a router).
SNMPv3 Settings	To facilitate SNMPv3 communication, you must add a user account to the MSL server that matches an account on the SNMP manager. This "User-based Security Model" (USM) enables unique authentication and encryption settings to be configured for each account. For instructions, see Configure SNMPv3 Users.
System contact address	Specify the email address to which all system notifications should go. • If Email service is enabled, and this field is blank, the address defaults to the Admin forwarding address. • If Email service is not set, the address defaults or to the local-admin account.
System location	Enter a string that identifies the location of the system. (ie. Server room 2, rack 1)

Field	Description
Vital process monitoring	To monitor the server's vital processes, like the web server, secure shell daemon, mail server (with the 6040 blade), and so forth, leave this option at its default of "Enabled". If any problems are detected, an error message and description will be added to the 1.3.6.1.4.1.2021.2.1.100 and 1.3.6.1.4.1.2021.2.1.101 MIB columns, respectively, available via a GET request.
Monitor disk usage	To monitor disk space usage on your server's root partition, leave this option at its default of "Enabled". If any problems are detected, an error message and description will be set in the 1.3.6.1.4.1.2021.9.1.100 and 1.3.6.1.4.1.2021.9.1.101 MIB columns, respectively, available via GET request.
Disk space threshold	If you are monitoring disk space usage on your server's root partition, you need to decide upon a threshold value at which the issue will be flagged at the predefined OID. You may leave this at the default value of 5%, or supply a value. If you supply a value of your own, it may be a numerical percentage of the overall disk space, followed by a percent sign (no spaces), or you may provide an absolute value in bytes.
Monitor CPU usage	To monitor the server's use of the CPU, leave the following setting at "Enabled". If any problems are detected, and error message and description will be set in the 1.3.6.1.4.1.2021.10.1.100 and 1.3.6.1.4.1.2021.10.1.101 MIB columns, respectively, available via GET request.
One minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the one minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.

Field	Description
Five minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the five minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.
Fifteen minute CPU threshold	If you have CPU monitoring enabled, you must choose a threshold value for the fifteen minute load average, above which this server will flag the error at the previously mentioned OID. The value must be a positive real number with no more than two decimal places of precision.
Trap host or address	If you wish to send trap messages to a remote host or hosts, whenever the server boots, the snmpd daemon starts and for authentication failures with the snmpd daemon, enter the hostname or IP address of the host designated to receive these trap messages. If this is left blank, traps will not be sent. To send traps to more than one host, enter the hostnames and/or IP addresses separated by commas.
SNMPv2c Trap community string	Enter the trap community string to use when sending trap messages. If you do not enter a trap community string, the community string for read-only access will be used.
SNMPv3 Trap username	
Download Mitel enterprise MIBs	If you have network management software that you would like to use to monitor this server via SNMP, and would like to import Mitel's enterprise MIBs into it, download them by clicking **Download**. ℹ **Note**: The file you receive is a zip file, so you require appropriate software to open it. Additionally, the MIB files are in Unix file format, so the MS Windows Notepad is not an appropriate application to use in opening them.

SNMP Trap Details

The SNMP trap details are listed below :

```
<application name="sas" oid =".1.3.6.1.4.1.1027.1.7.8">
<TrapSeverity>2</TrapSeverity>
<eventtype name="MOM Startup">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="MOM Crash">
<severity>5</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="LdapFailed">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="IDS status">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="IDS error">
<severity>4</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="SDS Join Started">
<severity>2</severity>
<traptype>status</traptype>
```

```
</eventtype>
<eventtype name="SDS Join Completed">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Device Data Notifications Started">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Device Data Notifications Completed">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="Device Data Notifications Failed">
<severity>4</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="User Sync Started">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
<eventtype name="User Sync Completed">
<severity>2</severity>
<traptype>status</traptype>
</eventtype>
```

```
<eventtype name="Device Sync Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Device Sync Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Device Sync Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Problem Detected">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Startup Error">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Conflicts Detected">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Analysis Started">
```

```
<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Analysis Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Analysis Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype> <eventtype name="Reconcile Execution Started">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Execution Completed">

<severity>2</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="Reconcile Execution Failed">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="SDS Sync Required">

<severity>4</severity>

<traptype>status</traptype>
```

```
</eventtype>

<eventtype name="Unsupported MiVoice Business">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

<eventtype name="User Sync Incomplete">

<severity>4</severity>

<traptype>status</traptype>

</eventtype>

</application>
```

Configure SNMPv3 Users

If you implement support for SNMPv3, you must add at least one user account that matches an account on the SNMP manager. As part of this configuration, you can enable authentication and encryption.

To add an SNMPv3 user:

1. Under **Configuration**, click **SNMP**.
2. Under **SNMPv3 Settings** , click **Configure SNMPv3 Users** .
3. Complete the following fields as required and then click **Add**.

Field	Description
User name	Type a user name (also known as "securityname") for the SNMPv3 user.
Authentication Type	Select the Authentication Type that matches SNMP manager/agent configuration: • MD5 • SHA1 • None (no authentication)
Authentication Password	If you selected an Authentication Type (MD5 or SHA1), you must enter an authentication password (also known as "authentication passphrase") at least eight characters long.

Field	Description
Privacy Protocol	Select the Privacy Protocol that matches SNMP manager/agent configuration: • DES • None (no encryption)
Privacy Password	If you selected a Privacy Protocol (DES), you must enter a privacy password.
Engine ID (Optional)	If the SNMP manager requires a hard-coded Engine ID, enter it here. Otherwise, leave this field blank and the SNMP manager will discover the Engine ID automatically.

6.10 Configure Network Interface Card Settings

This panel allows you to configure the speed and duplex settings for the Network Interface Cards (NIC) that have been enabled in the server. MSL supports the following combinations of NICs:

- a "Local" adaptor for connection to the Local Area Network (LAN-only mode) or
- a "Local" adaptor for connection to the Local Area Network AND a "WAN" adapter for connection to the Wide Area Network (Network Edge mode) or
- a "Local" adaptor for connection to the Local Area Network AND a "WAN" adapter for connection to the Wide Area Network AND a “WAN” adapter bridged to the WAN interface of the firewall (Server-gateway with bridged interface mode).

To configure the Speed and Duplex settings of a NIC:

Note: For virtual deployments, the fields are read-only. You cannot configure the settings from this page.

1. Under **Configuration**, click **Ethernet Cards**.
2. Set the **Auto Configuration** field to **Off**, and then click **Save**.
3. Set the **Speed** and **Duplex** parameters, and then click **Save**. All other settings are read only. See the following table for descriptions of the settings.

Note: Speed and Duplex are read only if the Ethernet card does not support multiple options.

Setting	Description
Link detected	**Yes**: NIC is connected to the network. **No**: NIC is not connected to the network.
MAC Address	Media Access Control address of the Network Interface Card
Driver	Driver (for example: tg3) of the Network Interface Card.
Speed	Data transfer rate. Available settings are determined by the Ethernet card. Only supported settings are displayed.
Duplex	**Half-duplex**: uses only one wire pair with a digital signal running in both directions on the wire. **Full-duplex**: uses two pairs of wires to establish a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device. Full-duplex data transfer provides faster data transmissions than half duplex.
Auto Negotiation	Auto Negotiation is an Ethernet process that allows two connected devices to choose common transmission parameters, such as speed, duplex mode, and flow control. During this process, the connected devices first share these parameters and then choose the fastest transmission mode they both support. Select **On** to apply Auto Negotiation; select **Off** to configure the Speed and Duplex settings.

6.11 Review Server Configuration

To review the server configuration information, under Configuration, click Review configuration. The following data for the MSL server is displayed:

Networking Parameters

- Local Adaptor IPv4 address/subnet mask and optional IPv6 address

- Internet visible IPv4 address and optional IPv6 address
- Gateway IPv4 address and and optional IPv6 address
- Additional trusted local networks
- DHCP server

Server names

- DNS server
- Web server
- Proxy server
- FTP server
- SMTP, POP, and IMAP mail servers

Domain information

- Primary domain
- Virtual domains
- Primary web site
- Server manager
- User password pane
- Email Addresses

Miscellaneous 7

This chapter contains the following sections:

- Support and Licensing
- Panel Requires Upgrade

7.1 Support and Licensing

License Server

MiCollab solutions with MiVoice MX-ONE, MiVoice 5000, MiVoice Office 400, and MiVoice Business will use the Licenses & Services Application (Licenses Server). The License Server can be accessed through the Mitel MiAccess portal.

After you obtain an Application Record ID (ARID) from the License Server, the License Server uses your Application Record ID (ARID) to provide you with access to licenses, software releases, and upgrades.

With the License Server migration, the following changes will be seen:

- All the **new installations** of MiCollab servers connected with a MiVoice MX-ONE, MiVoice 5000, or MiVoice Office 400 will receive their Licenses from the License Server available on MiAccess from the **Licenses & Services** link.
- **All the existing installations** of MiCollab servers connected with a MiVoice MX-ONE, MiVoice 5000, or MiVoice Office 400 would be capable to continue receiving their licenses from the License Server available on MiAccess **until** the site administrator adds or changes licensing (e.g. UCC licenses, SWA, etc) for the customer site.
- The MiCollab administrator **must manually** set the license server FQDN of the License Server for all the MiCollab Solutions with MiVoice MX-ONE, MiVoice 5000, and MiVoice Office 400.

For more information on licensing, see the Installation and Maintenance Guide for the respective PBXs.

About MS Office 365 licensing

The Microsoft Office 365 supported licenses are as follows:

- E3 - Office 365 Basic and Office 365 OAuth2.0
- E5 - Office 365 Basic and Office 365 OAuth2.0
- Office 365 Government GCC - Office 365 OAuth2.0
- O365 Business Premium - Office 365 Basic and Office 365 OAuth2.0
- Office365 Business Standard - Office 365 Basic and Office 365 OAuth2.0

7.2 Panel Requires Upgrade

Server Manager pages display "Panel requires update" if the associated applications must be upgraded to run on the currently installed version of MSL. You will see this message displayed after you upgrade MSL to a new version, but before you have upgraded the installed applications blades to the required version.

For MiCollab and MiVoice Business Express systems, you must upgrade the MiCollab applications from the server conso l e. Refer to the *MiCollab Installation and Maintenance Guide* or the *MiVoice Business Express Deployment Guide* for instructions.

For MSL systems, upgrade the blades from the Blades panel.

Mitel

Powering connections

mitel.com