

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 250, 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.

[Print Page](#)

About Mitel Standard Linux

Mitel® Standard Linux (MSL) is an operating system and software solution for single-site and branch-based enterprises. Mitel Standard Linux supports a suite of managed services and applications delivered from the license servers or available on CD. An MSL server can act either as an internet-facing server with firewall capability (in server-gateway configuration) or as an internal server on the local area network (LAN) (in server-only configuration).

In server-gateway configurations, the MSL server manages the end-user's connection to the Internet by routing Internet data packets to and from the network (which allows all the computers on the network to share a single Internet connection) and by providing security for the network, minimizing the risk of intrusion. When one of the computers on the local network contacts the Internet, or is contacted by an outside machine on the Internet, the MSL server not only routes that connection, but seamlessly interposes itself into the communication. This prevents a direct connection from being established between an external computer on the Internet and a computer on the local network, which significantly reduces the risk of intrusion onto the network.

[Print Page](#)

What's New in This Release

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 (SLS 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 SLS License Server, the SLS uses your ServiceLink ID to provide you with access to licenses, software releases, and upgrades.
- To activate an SLS 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 AMC but the AMC 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-amc.com 216.191.234.91 port 22
- sync.mitel-amc.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	Upgrading To...	Supported
-----------	-----------------	-----------

from...		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.

For a list of new MiCollab functionality, see [What's New in This Release](#) on the Mitel Customer Documentation site.

[Print Page](#)

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 20, Internet Explorer Release 10 or 11, Google Chrome version 46 or higher, and Mozilla® Firefox® 41 or higher. Note that [Flow Through Provisioning](#) and [Reach Through](#) functionality are only supported in Internet Explorer and Firefox browsers.

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.

[Print Page](#)

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. Go to www.mitel.com, and click Login.
2. Log in to Mitel Online.
3. Move your pointer over **Products** and then click **Product Documentation**.
4. In the top menu bar, point to **Applications and Solutions** and then click **MiCollab Mitel Standard Linux**.
5. To view a document, click the document title.
6. To download a document, right-click on the name of the document, and click **Save Target As**.

Note: To view online help, ensure that Compatibility view is enabled for your browser. For example, to enable compatibility view in Internet Explorer 10.0, click **Tools**, click **Compatibility view settings**, and enable **Display all websites in Compatibility view**.

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 Mitel Border Gateway)

- [Remote Phone Configuration Guide](#)

Speech Auto Attendant

- See the [NuPoint UM User 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 Quick Reference Guide](#) : provides basic feature and usage information for the Desktop 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.

Application Management Center (AMC)

- See the online help in your AMC Account

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>.

[Print Page](#)

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

™, ® - Trademark of Mitel Networks Corporation

© Copyright 2021, Mitel Networks Corporation

All rights reserved

[Print Page](#)

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)

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 \(includes Speech Auto Attendant\)](#)
5. [Perform MiCollab Client Service Administration](#)
6. [Configure Vidyo Settings](#)
7. [Configure Service Info E-mail](#)

[Print Page](#)

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](#)

[Print Page](#)

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**.

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.

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.

View Licensing Information

The MiCollab administrator portal opens at the **Licensing Information** page, which displays details about user licensing for your applications.

Unified Communications and Collaboration (UCC) Bundles

This table lists the installed UCC Licensing bundles.

Column	Description
Bundle	Lists the type of UCC licensed bundle; for example, UCC Entry Level for Enterprise (V4.).Note that you can generate a report that identifies the UCC licensing bundle assigned to each user.
User Licenses	Displays the maximum number of licensed bundles that you can assign.
Currently used	Displays the number of UCC bundles that you have assigned or attempted to assign. When this total is greater than the number of Licenses, it is displayed in red to indicate over provisioning. If required, you can purchase extra license bundles from your Authorized Reseller.

Note: This table just shows the tally of the of the available licenses. To determine the licensing part numbers that are being used use to achieve the current level of licensing, you must access the Application Management Center and view the licenses that are assigned to the ULM.

Application User Totals

This table lists the installed applications and the user licensing information for each application. The totals in this table include the user licenses in the available UCC License Bundles plus any "al la carte" licenses that you may have purchased.

Column	Description
Application	Lists the installed applications.
User Licenses	Displays the maximum number of licensed users that you can assign to each application or service.
Currently Used	<div>Displays the number of licenses that you have assigned or attempted to assign. When this total is greater than the User Licenses, it is displayed in red to indicate over provisioning (also see Voice Mailbox Over Provisioning). If required, you can purchase extra licenses or uplifts from your Authorized Reseller.</div> <div>Note: SIP phones appear in the Teleworker license count regardless of whether they are registered to the ICP.</div>

Effect of Adding or Removing UCC Licenses

When you add or remove a UCC Licensing bundle, the system updates the UCC Licensing totals. The Application User Totals are also updated to reflect the change.

If you add/delete . . .	The following application user licenses (in use)
-------------------------	--

	increase/decrease by one . . .
UCC Basic License	<ul style="list-style-type: none"> • UCC Basic (includes MiVoice Business user license)
UCC Entry License	<ul style="list-style-type: none"> • UCC Entry • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM • MiTeam Meetings license
UCC Standard License	<ul style="list-style-type: none"> • UCC Standard • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM license • One Teleworker license • MiCollab Client deskphone, web client, and softphone or mobile client • Vidyo client license • MiCollab Audio, Web and Video Conferencing license • MiTeam Meetings license
Premium UCC License	<ul style="list-style-type: none"> • UCC Premium • Multi-device user license • NuPoint UM mailbox, Standard UM, and Advanced UM license • MiCollab Audio, Web and Video Conferencing license • Three Teleworker licenses • MiCollab Client deskphone, web client, softphone, and mobile client • Vidyo client license • MiTeam Classic license • MiTeam Meetings license
NuPoint UM mailbox (when "al la carte" NuPoint licenses are available)	<ul style="list-style-type: none"> • NuPoint UM mailbox
NuPoint UM mailbox (when "al la carte" NuPoint licenses are not available but UCC license bundles are)	<ul style="list-style-type: none"> • UCC Entry (or Standard, or Premium depending on availability) • NuPoint mailbox

Voice Mailbox Over Provisioning

You are allowed to restore a database to a destination system even though the database may contain more voice mailboxes than the system licensing can support. Over provisioning of voice mailboxes is allowed in order to give you time to purchase additional licenses from the Applications Management Center (AMC). If the system is in an over provisioned state:

- A warning message appears in the Users and Services application that indicates that you need to

purchase additional NuPoint UM user licenses.

- You cannot add new voice mailboxes if the current mailbox count has reached the system NuPoint UM user licensed limit or if the system is in an over provisioned state. You will also be unable to add mailboxes from the NuPoint UM telephone user interface.
- You cannot log into the NuPoint UM web console.
- You cannot log into the MiCollab Audio, Web and Video Conferencing administration application.
- You can log into the NuPoint UM Telephone User Interface (TUI), but you will be unable to access the administrative options.

To return the NuPoint UM application to its normal state, purchase additional licenses or delete the extra mailboxes. You must reduce the number of mailboxes to be equal to, or lower than, the number of available licenses.

[Print Page](#)

Install Blades

This panel shows the currently installed Blades along with their version numbers.

Software application blades can be installed in one of three ways:

- From a CD/DVD-ROM or USB device by logging into the server console as the admin user (except for MiCollab)
- From a CD/DVD-ROM through the server manager Blades panel
- Via the Mitel software download center (swdlgw.mitel.com) and content distribution network (swdl.mitel.com).

To obtain the software entitlements for your server ARID any firewalls must allow outgoing ssh connections on port 22:

- to the Mitel Applications Management Center (AMC), blades.mitel-amc.com with static IP: 216.191.234.91.
- to the SLS licensing server, sync.sls.mitel.com, Current IP: 18.200.183.29.

To obtain download access tokens from the Mitel software download center, any firewalls must allow https connections on port 443 to swdlgw.mitel.com, which has static IP: 99.81.17.20.

Note: Verify the IP address for swdlgw.mitel.com with a DNS lookup before adding it to any firewall rules as the server IP may change over time.

To download software from the content delivery network, https connection on port 443 to swdl.mitel.com must be allowed. Static IP addresses cannot be guaranteed by the content delivery network therefore any firewall rules must allow access to the FQDN. The CDN IP addresses may change depending on which location in the world the download is taking place to ensure the fastest speed as possible for that geolocation.

Software blades allow applications and services to run on the server.

You can download and install the blade in a single step, or you can download it for installation at a later time. The first option ties up your computer for a short period of time. The second option, which is known as “caching,” enables you to initiate the download and then use your computer for other purposes.

To install Blades from the server:

1. Under **ServiceLink** , click **Blades** .
2. Click **Update List** to retrieve the latest list of available blades from the Mitel software download center.
3. Scroll through the list and locate the blade for the feature that you are adding to the system.
4. Do one of the following:
 - To install a new blade immediately, click the Install link beside it.
 - To download a blade for installation at a later time, click the Cache link beside it. Complete the installation process by clicking the Install link.

Installing a blade creates new menu items in the navigation menu to allow you to administer the blade.

Note: For MiVoice Business Virtual or MiVoice Business - ISS, install the **ServiceLink** blade first and then install the **MiVoice Business** blade. For a MiVoice Business system deployed on an EX controller, install the **ServiceLink** blade first, followed by **Blade-ExPlatform** and the **MiVoice Business** blade.

5. After you install a blade, launch the associated online help from the application blade. The online help provides information on how to program and use the blade.

Note: To install blades from CD/DVD-ROMs, insert the CD/DVD-ROM and click **Update List**.

View ServiceLink Status

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

You must activate ServiceLink before you can view status information .

Online Activation

To activate ServiceLink online:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. Under **ServiceLink** , click **Status** .
3. Enter your **Application Record ID** (also called Service account ID).
4. If the Internet is accessed via a proxy, enter:
 - Address of proxy
 - If AMC is used, the proxy server must be configured to forward TCP packets on the incoming port to the AMC address (sync.mitel-amc.com) on port 22.
 - If SLS is being used, enter the proxy address as **sync.sls.mitel.com** . This field is mandatory in case of SLS.
 - TCP port used to connect to proxy
5. Click **Activate** to synchronize with 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. License expiration dates and any service entitlement changes made to your license server account are updated at this time.

Offline Activation

The following procedure describes how to perform offline activation from the server manager using a maintenance PC.

If your MSL server has a USB drive, you may also perform offline activation from the server console. Refer to the MSL Installation and Maintenance Guide for instructions.

Note: When an offline system is upgraded to MSL 10.0, it will receive a Major alarm indicating that the AMC synchronization process has failed. To disable auto-synchronization and prevent further alarms, re-do the Offline Activation procedure. The original alarm can then be cleared manually.

To activate ServiceLink offline with AMC:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. In the server manager of the maintenance PC, under **ServiceLink** , click **Status** .
3. Enter your **Application Record ID** (also called Service account ID).
4. Select **Enable offline license generation** .
5. Click **Activate** to request an offline licensing file.
6. The Operation status report page is displayed. Click **Download license request file** .
7. In the file download dialog, click **Save** and save the zip file to a portable storage medium on the

maintenance PC.

8. Remove the portable storage device and go to an Internet-connected PC.
9. On the Internet-connected PC, extract the contents of the zip file to a temporary folder.
10. Open the folder and double-click the **sync.bat** file to execute handshake and synchronization with the AMC.
Synchronization occurs with the AMC and the sync.bat file creates a license.zip file containing license files from the AMC. (If you receive a security warning during this process, click **Run**.)
11. Save the **license.zip** file to the portable storage device.
12. Remove the storage device from the Internet-connected PC and return to the maintenance PC. Insert the storage device in the maintenance PC.
13. In the server manager of the maintenance PC, under **ServiceLink**, click **Status**.
14. Beside **Upload license file**, click **Browse**.
15. In the file upload dialog, browse to the **license.zip** file that was created by executing the sync.bat file, then click **Save** to select the file to be uploaded.
16. Click **Upload license file** to install the synchronized license key file and activate the purchased options.

To activate ServiceLink offline with SLS:

1. Obtain an **Application Record ID** (or service account ID) from your authorized reseller.
2. In the server manager of the maintenance PC, under **ServiceLink**, click **Status**.
3. Enter your **Application Record ID** (also called Service account ID).
4. Select **Enable offline license generation**.
5. Click **Activate** to request an offline licensing file.
6. The **Operation status report** page is displayed. Click **Download license request file**.
7. In the file download dialog, click **Save** and save the zip file to a portable storage device on the maintenance PC.
8. Remove the portable storage device and go to an Internet-connected PC.
9. Access the license server through **Mitel MiAccess** portal.
10. Click **Licenses & Services** option from the left menu, **License Server** home page opens.
11. Use the **Search product/ end customer** option and find your system.
12. In the **Licenses & Service** home page, click **Upload request** from the left menu. Browse to locate the zip file downloaded in **Step 6**, and upload offline license request, and click **Upload Request**.
13. Scroll to the bottom of the page to download and save latest **license zip file**. Save the license.zip file in a portable storage device.
14. Remove the storage device from the Internet-connected PC and return to the maintenance PC.
15. Insert the storage device in the maintenance PC.
16. Log into the server manager of the maintenance PC.
17. In the server manager of the maintenance PC, under **ServiceLink**, click **Status**.
18. Click **Sync** to generate an offline license request. The **Upload license file** and **Download licensing refresh file** buttons are displayed.
19. Beside **Upload license file**, click **Browse**.

20. In the file upload dialog, browse to the **license.zip** file on your PC and upload the latest license zip file containing the licenses to the server manager. Click **Save** to select the file to be uploaded.
21. Click **Upload license file** to install the synchronized license key file and activate the purchased licenses.

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 licence server and then reactivate your ServiceLink account using either the online or offline method.

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.

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.

[Print Page](#)

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, an Amazon S3 storage bucket or a network file server that supports SFTP or SMB/CIF)
- 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.

Notes :

- 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: 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.

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.
- Three file-sharing protocols are supported:
 - SMB/CIFS
 - Secure File Transfer Protocol (SFTP)
 - HTTPS to an AWS S3 (storage bucket)

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. The **Network Backups** page is displayed .

5. From the **Backup Destination Type** drop-down list, select the type of network backup.

- If you select **SMB/CIFS** , then specify the following details.

Field	Description
IP Address	IP address of the network file server where you have stored the database
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. Sets the SMB domain of the user name. If the server's NetBIOS name, then instead of the domain SAM, the server's (SAM) is used for authentication.
Sharename	The file-share name. The shared folder must have permissions set to "Full
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. The Sharename.
Maximum number of backup files to keep	Select the maximum number of backup files to keep (1-999) on the server. reaches this maximum count, the earliest version is deleted.

- If you select **SFTP** , then specify the following details.

Note: If you are backing up to an MSL server, enter the IP address and the user name and password of the "root" user and leave the remaining fields blank.

Field	Description
IP Address	IP address of the network file server.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
(Optional) Sub Directory	Name of the sub-folder in which to store the backup files. The sub-directory system accessed through the SFTP protocol.
Maximum number of backup files to keep	Select the maximum number of backup files to keep (1-999) on the server. reaches this maximum count, the earliest version is deleted.

- If you select **AWS S3**, then specify the following details.

Field	Description
AWS Access Key ID	To enable programmatic calls to AWS, you must provide your AWS access the Key ID and Secret Access Key. Enter your access key ID here.
AWS Access Key	The secret access key portion of your AWS access key credential set.
AWS S3 Region	The AWS region used to access your storage bucket. Stored objects (back
AWS S3 Bucket Name	Your storage bucket name.
(Optional) Sub Directory	The sub directory (also known as an object prefix) will be prepended to the bucket.
(Optional) IAM Role ARN	The Amazon Resource Name (ARN) of an AWS Identity and Access Mana configured storage bucket. Example: arn:aws:iam::827611302152:role/Back
(Optional) Maximum number of	Select the maximum number of backup files to keep (1-999) on the server.

backup files to keep reaches this maximum count, the earliest version is deleted.

Note: AWS requires that all incoming requests are cryptographically signed. The "signature" includes a date/time stamp. Therefore, you must ensure that your PC's date and time are correctly set. If you do not do this, AWS rejects the request if the date/time in the signature is too far off of the date/time recognized by the AWS service. The PC displays 403-forbidden error status if the date/time is more than 15 minutes off the correct time.

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.

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 the **Save** button to validate your server configuration. If validation is successful the Backup Now button will appear.

8. Click the **Backup Now** button to perform an immediate backup.

The backup file is saved to the network file server. The file is identifiable by its extension, either .tgz (not encrypted) or .aes256 (encrypted).

To perform an immediate backup:

1. 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 **Perform**.
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"

To access the Server Console :

1. On the Putty client screen, enter the IP address of the PPC Server Manager.
2. Enter the login ID and password. It is the same as the credentials the user enters in the browser version of Server Manager.

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.

6. MSL displays an estimate of the size of your backup. Click **Proceed**.
7. When the backup is complete, remove the USB device at the prompt. Click **Continue**.
8. 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* installation in the *MSL Installation and Administration Guide*.

[Print Page](#)

Restore Server Data

You can restore a server backup file stored on a network file share. Three file-sharing protocols are supported:

- Samba (SMB)/Common Internet File System (CIFS)
- Secure File Transfer Protocol (SFTP)
- HTTPS to Amazon Web Services Simple Storage Service (that is, AWS S3)

NOTE: You must not restore the database backup file created from the following systems and vice-versa.

- MiVoice Business System Administration Tool (all platforms)
- Server Manager (other platforms)

Before you begin

Ensure that you have placed the backup file (in *.tgz* format) in an accessible AWS S3 storage bucket or in a folder on a network file share that supports SFTP, SMB/CIFS.

To restore the server database backup file

1. Under **Administration**, click **Restore**.
2. The **Restore from Network** page is displayed.
3. From the **Restore Source Type** drop-down list, select the type of network restore.

- If you select **SMB/CIFS**, then specify the following details.

Field	Description
IP Address	IP address of the network file server where you have stored the database backup files.
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. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then instead of the domain SAM the server's local Security Account Manager (SAM) is used for authentication.
Sharename	The file-share name. 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. The sub-directory is relative to the share.

- If you select **SFTP**, then specify the following details.

Field	Description
IP Address	IP address of the network file server where you

	have stored the database backup files.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. The sub-directory is relative to the root of the file system accessed through the SFTP protocol.

- If you select **AWS S3**, then specify the following details.

Field	Description
AWS Access Key ID	To enable programmatic calls to AWS you must provide your AWS access key credential set that consists of the Key ID and secret Access Key. Enter your access key ID here.
AWS Access Key	The secret access key portion of your AWS access key credential set.
AWS S3 Region	The AWS region used to access your storage bucket. Stored objects (backup files) will be read from this region.
AWS S3 Bucket Name	Your storage bucket name.
(Optional) Sub Directory	The sub-directory (also known as an object prefix) will be searched for matching backup file names.
(Optional) IAM Role ARN	The Amazon Resource Name (ARN) of an AWS Identity and Access Management (IAM) role with access to the configured storage bucket. Example: arn:aws:iam::827611302152:role/Backup.

NOTE: AWS requires that all incoming requests are cryptographically signed. The "signature" includes a date/time stamp. Therefore, you must ensure that your PC's date and time are correctly set. If you do not do this, AWS rejects the request if the date/time in the signature is too far off of the date/time recognized by the AWS service. The PC displays 403-forbidden error status if the date/time is more than 15 minutes off the correct time.

4. Click **Next**.
5. The system validates and lists all the database backup files available in the specified location on the network in the **Select backup file** drop-down list.
6. In the **Select backup file** drop-down list, select the database backup file you want to restore.
7. If the database backup file was encrypted when creating the backup, then enter the password in the **Encryption Password** field.
8. Click **Next**. A confirmation message is displayed.
9. Click **Yes** to restore the database. The system reboots and restores the database upon restart.

NOTE: The **Restore from Network** page displays only the last restore status of the server.

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 ("journal" file for MiVoice Business system).
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. For example, 'eth[01]:' is a regular expression that would match either 'eth0:' or 'eth1:'.
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.

Notes :

- 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.

[Print Page](#)

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).

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

- An "Alarm State" link is displayed next to each application name on the Server Manager (under Applications). Clicking this link opens the Event viewer and displays alarm details.

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.

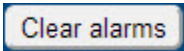

Note: Events may also be cleared automatically by the applications.

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.	<input type="checkbox"/> set connection <input type="checkbox"/> set registration <input type="checkbox"/> one-way audio
Value	Value associated with the event	<input type="checkbox"/> established <input type="checkbox"/> rejected <input type="checkbox"/> lost <input type="checkbox"/> MAC address (for one-way audio)
Severity	Level of severity associated with this alarm	<input type="checkbox"/> Cleared (green): No alarms have been raised since the alarms were last cleared. <input type="checkbox"/> Indeterminate (turquoise): The cause of the alarm cannot be determined at this time. <input type="checkbox"/> Warning (blue): Indicates an "information only" alarm. <input type="checkbox"/> Minor (yellow): Indicates a fault which affects service. This may result in a major degradation in service and requires attention to minimize customer complaints. <input type="checkbox"/> Major (orange): Indicates a fault which will cause a major degradation in service and requires attention as soon as possible. <input type="checkbox"/> 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. 

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.

[Print Page](#)

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** .

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 the access for 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.

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.

Notes :

- 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](#).
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](#).

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

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 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.

5. Select **Remember my sign-in info**, and then click **Save**.
6. Click **Connect** to test the connection

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.

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.

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

[Print Page](#)

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.

Note: The recommended method to monitor disk latency for a VM is to set up a monitoring alarm in vCenter. To do this, right-click the VM, select Alarm, New Alarm; give the alarm a name that contains the VM name, assign 'VM Max Total Disk Latency' as the key of the IF condition and finish defining the alarm as needed. Some recommended parameters from VMware is defining the alarm with 25ms threshold and violation duration of 30 seconds. Email action can be specified so the appropriate contacts can be notified when problem is detected. Disk latency monitoring is a best-effort task within the guest operating systems because the correct measurement information is not available in guest OS and therefore it's impossible for MVF to monitor disk latency the same way VMware could.

MVF does monitor various symptoms associated with disk performance issues and creates an MSL alarm whenever MVF detects slow disk responses. Slow disk response is what MVF can tell at best. The root cause for lack of response may be actual disk latency, heavy cpu load on the vSphere host, heavy cpu load on the VM itself and many other reasons combined.

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.
vCPU Speed (MHz)	<p>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.</p> <p>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.</p>

Managing Storage Monitoring

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

To manage the storage monitoring settings:

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

Setting	Description
File System Monitoring	<p>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.</p> <p>The following errors are monitored:</p> <ul style="list-style-type: none"> • File system errors: Errors related to storage degradation • CPU Starvation: When the monitoring process is not dispatched within a specified

	<p>time (default is 5 seconds).</p> <ul style="list-style-type: none"> • High I/O Latency: When I/O operations exceed the pre-determined duration of 5 seconds.
Reboot on Read-Only State	<p>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.</p> <p>Notes :</p> <ul style="list-style-type: none"> • File System Monitoring must be enabled before this feature can be employed. • 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).	<ul style="list-style-type: none"> • 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.
Current Dimensions	Indicates whether the currently configured application resource dimensions are supported.	<ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 1. Revert to the default configuration for your deployment. For details, see Default Configurations. 2. Contact Mitel Product Support for assistance.
AMC Connectivity	Indicates whether the Virtual Machine can connect to the Mitel Application Management Center	<ul style="list-style-type: none"> • Connected - Your Virtual Machine can connect to the AMC. • Error - Your Virtual Machine cannot connect

	(AMC) for licensing purposes.	to the AMC. Check the networking configuration and Application Resource ID (ARID). See the <i>Mitel Standard Linux Installation and Maintenance Guide</i> 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 ESXi 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** .

Notes :

- 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	<p>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.</p> <p>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</p>
USER-SUMMARY.tmp	<p>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.</p> <p>This report is presented in two formats:</p> <ul style="list-style-type: none"> • 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 operation 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, a 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, an 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 $4 + 4 + 4 + 4 + 4 \div 16 = 1.25$. 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 $2 + 2 + 2 + 2 + 2 \div 8 = 1.25$, which will cause an event to be registered.
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)	<p>If "Yes" is displayed, the system checks to determine if hyperthreading is enabled on the ESXi host.</p> <p>Note: This parameter can only report on Intel processors that support hyperthreading. It cannot report on AMD or other non-Intel processors.</p>
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.

About Remote Access

You can access the MiCollab Mitel 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](#)

[Print Page](#)

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](#).

Enable VPN Access

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:

- [Creating the connection](#)
- [Configuring the connection](#)

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.

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.

[Print Page](#)

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** .

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

[Print Page](#)

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.

Note: If you are behind a firewall, please make sure it allows passage through the ports used by the syslog server.

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.

Notes:

- 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 now 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.

[Print Page](#)

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 MiCollab MSL 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 MiCollab MSL 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](#)

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.

Notes :

- 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 AWW 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 MiCollab MSL 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	Description
-------	-------------

Name	
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 <i>not</i> 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.

- 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:

- Log into the MiCollab MSL Server Manager.
- Under **Security**, click **Web Server**.
- Click the **Web Server Certificate** tab.
- Click **Modify Request**.
- Update the field values as required in order to modify your certificate signing request (CSR).
- 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:

- Log into the MiCollab MSL Server Manager.
- Under **Security**, click **Web Server**.
- Click the **Web Server Certificate** tab.
- 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 MiCollab 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 authorization 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 Certificate 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	<p>Date and time when the certificate expires.</p> <p>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.</p> <p>Certificate already expired: CRITICAL</p> <p>Expires in less than 1 week: CRITICAL</p> <p>Expires in less than 3 weeks: MAJOR</p>

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 an 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

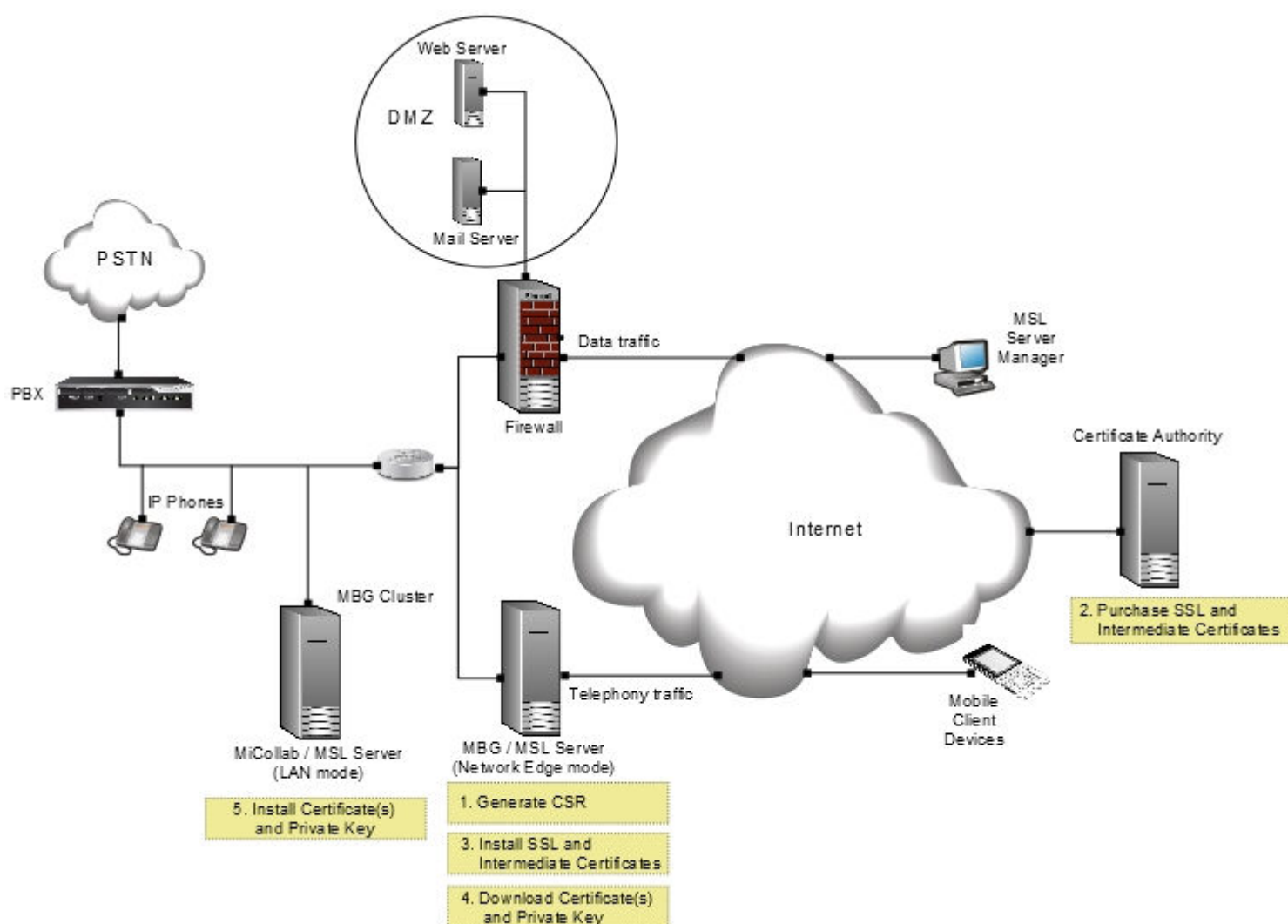
You can import third-party SSL certificates in either PEM or PKCS#12 format:

- **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 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.



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.
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 organization 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 name in the Organization field, and the DBA (doing business 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 Resources." If applicable, you may enter the DBA (doing business as) name in this field.
Common Name	<p>Enter the common name for the service to which you plan to apply your certificate. A web browser checks this field. It is required.</p> <p>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.</p> <p>The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com).</p>

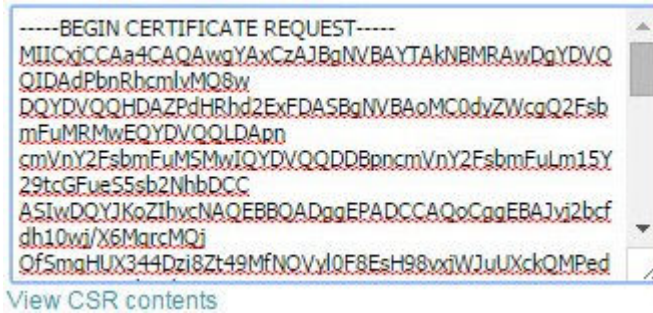
6. Check to ensure that you have entered all the required information correctly before you generate the CSR. If you need to make changes, regenerate the file. Do NOT modify the text of the generated file in a text editor such as Notepad.
7. Click **Generate Certificate Signing Request**. The system generates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



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**.

Notes :

- ☐ 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 Servers

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** .
5. 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** .
6. 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** .
7. Click **Install Web Server Certificate** .
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.
9. 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 authorization 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 Certificate 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	<div>Date and time when the certificate expires.</div> <div>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.</div> <div>Certificate already expired: CRITICAL</div> <div>Expires in less than 1 week: CRITICAL</div> <div>Expires in less than 3 weeks: MAJOR</div>

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 MiCollab MSL 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 MiCollab MSL 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 MiCollab 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 authorization 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-signed certificates.
	OU: name of the organizational unit
	CN: server hostname
	Authority/ emailAddress : email address of the Certificate 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.
Expires	<p>Date and time when the certificate expires.</p> <p>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.</p> <p>Certificate already expired: CRITICAL</p> <p>Expires in less than 1 week: CRITICAL</p> <p>Expires in less than 3 weeks: MAJOR</p>

[Print Page](#)

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 Trust** 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.

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).

Notes :

- 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 MiCollab MSL 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.

Notes :

- 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.

Configure MiCollab Language

This page allows you to configure the following settings:

- **System Language** : Select the language of the Telephone User Interfaces (TUIs) for the MiCollab application end-users. End-users can also set their own prompt language on the Settings page of their MiCollab End User Portal. After the initial installation of a new system, the System Language defaults to US English.
- **NuPoint UM Prompt Languages** : Select the other languages for the NuPoint UM prompts. When users call into the NuPoint UM system through the Message Center auto attendant or Receptionist application, they are asked to select the language of the NuPoint UM prompts for the duration of their call. Users can select either the primary prompt language or one of the other languages. The primary (first) language is determined by the System Language setting above; the other languages are determined by the settings in these fields. For example, the primary system language could be English (United Kingdom); the second language; French (Canada), the third language Swedish (Sweden), and so on.

You must record your corporate "Welcome" greeting in all the selected languages for incoming calls to the NuPoint UM system. When an external caller connects with the voice mail hunt group pilot number, the system plays your bilingual or multi-lingual corporate greeting and then prompts the caller to select the desired language. For example:

System "Welcome" Greeting: "Welcome to Mitel Networks, Bienvenue à Mitel Networks".

System Prompt: "For Service in English press 1; Pour le service en français, appuyez sur 2".

Users should also record their mailbox greetings in the required languages. When a caller reaches a user's mailbox, the system plays the mailbox greeting. For example: "You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message".

- **Use NuPoint UM Mnemonic English Prompt** : When the System Language or Secondary NuPoint UM Prompt Language is set to English (United States), check this box if you want the NuPoint UM voice mail system to use English mnemonic prompts. By default, the system uses English numeric prompts.

Change System Language

To change the system language:

1. Under **Configuration**, click **MiCollab Language**.
2. Select the desired language from the **System Language** drop-down box.
3. If you set the system to use "English (United States)", you can choose to use numeric (default) or mnemonic prompts for NuPoint UM voice mail:
 - Check the **Use NuPoint Mnemonic English Prompt** box if you want the voice mail system to prompt users to enter letters to select actions. For example, "Press P to play";
 - Clear the box if you want the voice mail system to prompt users to enter numbers to select actions. For example "Press 7 to play".

Note: The **Use NuPoint Mnemonic English Prompt** box is only presented if the NuPoint UM application is installed.

4. Click **Save**.

The following conditions apply to the System Language :

- The Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it overrides the MiCollab system language setting and the MiCollab secondary NuPoint UM prompt language setting. Note that the LCOS

language overrides the Line Group language and the MiCollab System language.

- The language of the Call Director application is not controlled by the system language setting.
- MiVoice Business phone displays are not controlled by the system language setting.
- For MiCollab Audio, Web and Video Conferencing, the Telephone User Interface language (TUI) is set on a system-wide basis for all users (that is, each user cannot set his or her own TUI language for MiCollab Audio, Web and Video Conferencing).
- The MiCollab End User Portal login page is displayed to the user in the language of the user's browser. If the browser language is not supported, the login page is displayed in the system language.
- The prompt language for call flows in Call Director default to the MiCollab language setting. However, users can set the prompt language for a call flow independently of the MiCollab language setting through the **Action** menu in the Call Director application.
- The System Language setting does not control the language used by the MiCollab End User Portal or Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports two languages: UK English and NA English. To change the Speech Auto Attendant language:
 1. Under **Applications**, click **NuPoint Web Console**.
 2. Under **Auto Attendant**, click **Misc. Parameters**.
 3. Select the desired **Primary Language**, and then click **Save**.
 4. Under **Auto Attendant**, click **Data Source**.
 5. Click **Force Update**.
- The **Use Nupoint Mnemonic English Prompt** box is displayed only when either System Language or Secondary NuPoint UM Prompt Language is set to English (United States).
- MiCollab Client supports additional languages that are not supported by MiCollab. However, MiCollab Client users can use these additional languages when MiCollab Client is deployed as an application on MiCollab, even though these languages are not supported by MiCollab.

Configure NuPoint UM Prompt Language

To configure a prompt language for the NuPoint UM system:

1. Ensure NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" is assigned to the users' voice mailboxes.
2. Under **Configuration**, click **Application Suite Language**.
3. Select the desired languages from the **NuPoint Prompt Language** drop-down box.
4. Record a bilingual or multilingual corporate greeting for the NuPoint UM system hunt group pilot number through the NuPoint UM administrator mailbox. Record the greeting in the "System Language" followed by the same greeting in the other selected languages; for example: "Welcome to Mitel Networks, Bienvenue à Mitel Networks; Bienvenido a Mitel Networks; Willkommen bei Mitel Networks".
4. Call into the NuPoint UM system hunt group pilot number and ensure that the prompts are played correctly.
5. Instruct mailbox users to record bilingual (or multilingual) greetings for their mailboxes as required. Again, users should record their mailbox greetings in the "System Language" followed by the same greeting in the other languages; for example: "You have reached the voice mailbox of Jean Julian, please leave a message; Vous avez atteint la boîte aux lettres de Jean Julien, s'il vous plaît laissez un message; Usted ha llegado al buzón de voz de Jean Julian, por favor deje un mensaje; Sie sind auf der Sprachmailbox von Jean Julian erreichen, hinterlassen Sie bitte eine Nachricht".

The following conditions apply to the other NuPoint UM prompt languages:

- NuPoint UM FCOS feature bit 51 "Do Not Switch Languages for Outside Caller" must be assigned to the users' voice mailboxes.
- The NuPoint UM Line Group language setting and LCOS language setting use the MiCollab system default language. In the interface, the Line Group language setting is set to "undefined" and the LCOS language setting is set to "default". If you set the system language in the Line Group, it will override MiCollab system language setting and the MiCollab NuPoint UM prompt language.
- The "NuPoint Prompt Language" field is only displayed if NuPoint UM is installed.
- This prompt language feature does not apply to Speech Auto Attendant (SAA).
- Callers select the desired language for NuPoint prompts at the system-level only, not at the mailbox level.
- The system plays the languages in the order of the language choices. For example, if you selected the English as the "System Language" and then French, the system generated prompt plays: *"For service in English, press 1; Pour le service en français, appuyez sur 2."*
- This feature applies to calls to the NuPoint UM voice mail hunt group pilot number. The caller only selects the prompt language once, before the first system prompt is played.
- Mailbox owners are not prompted to select a prompt language when they log into their mailboxes.
- In MiCollab, the language selection prompts are system generated. MiCollab does not provide you with the ability to record and import a custom language selection prompt.
- An "SAA Warning" is displayed in the server manager interface if the "System Language" or one of the other language selections is not English.

[Print Page](#)

Configure Networks

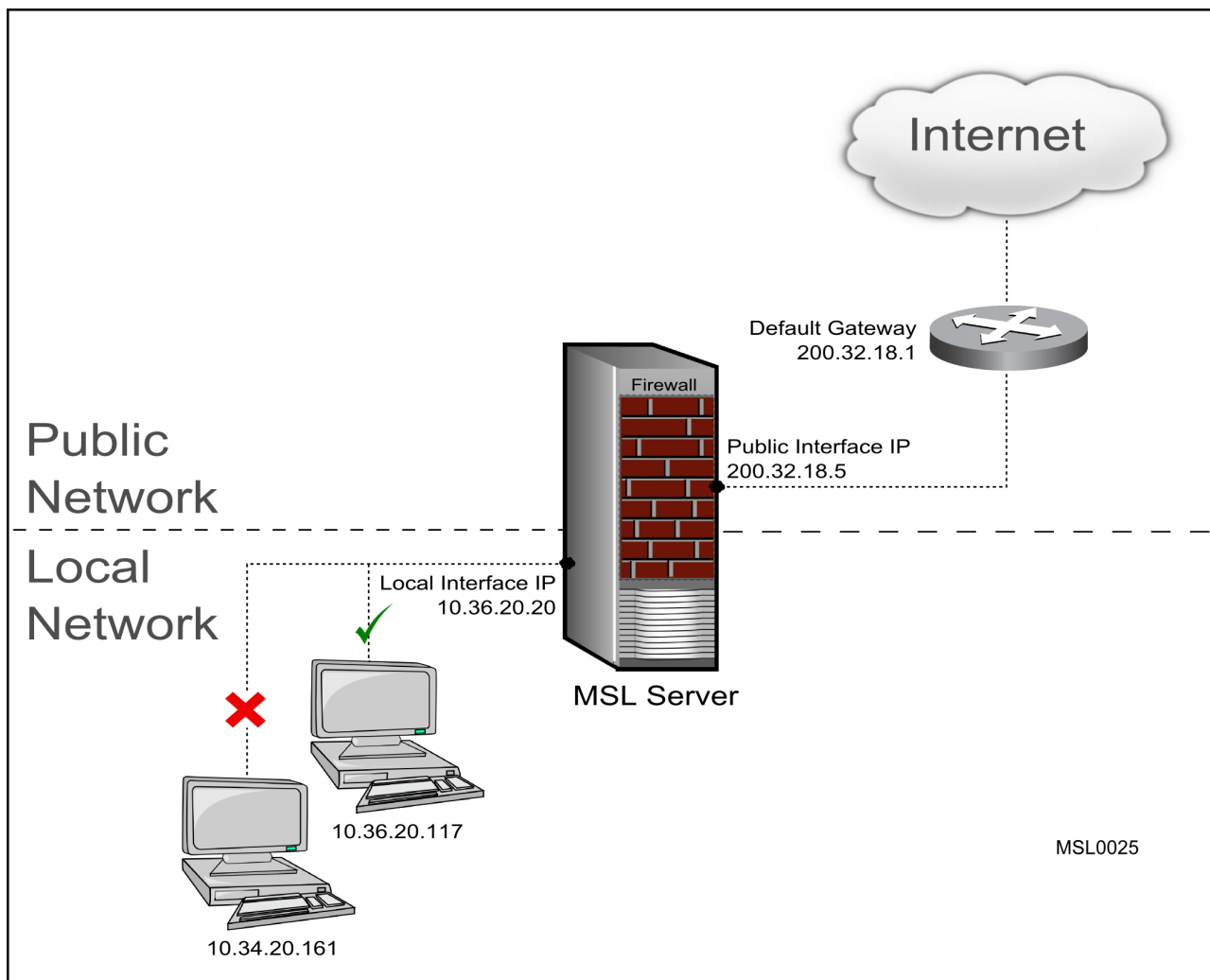
Grant Access Privileges to Trusted Local Networks

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.

For MiVoice Business systems, after an upgrade or installation, the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 networks are added by default that provides access to all MiVoice Business network services on these networks.

Example of Default Routing Configuration

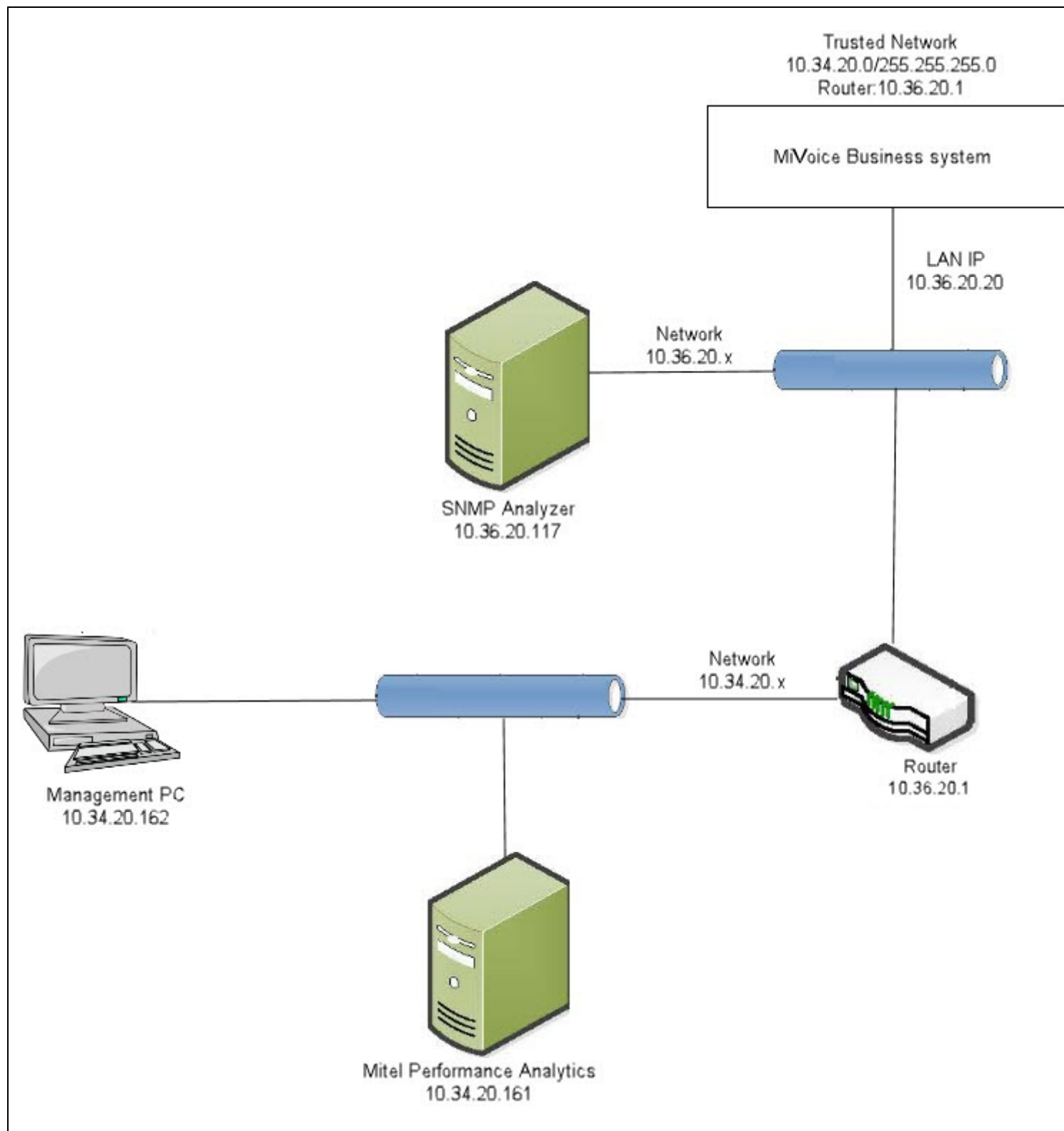
In the example illustrated below, the LAN interface of the MSL server has an IP address of 10.36.20.20. Accordingly, the server will accept traffic only from the 10.36.20.x network while blocking traffic from all other subnets on the LAN.



Example of MiVoice Business Configuration

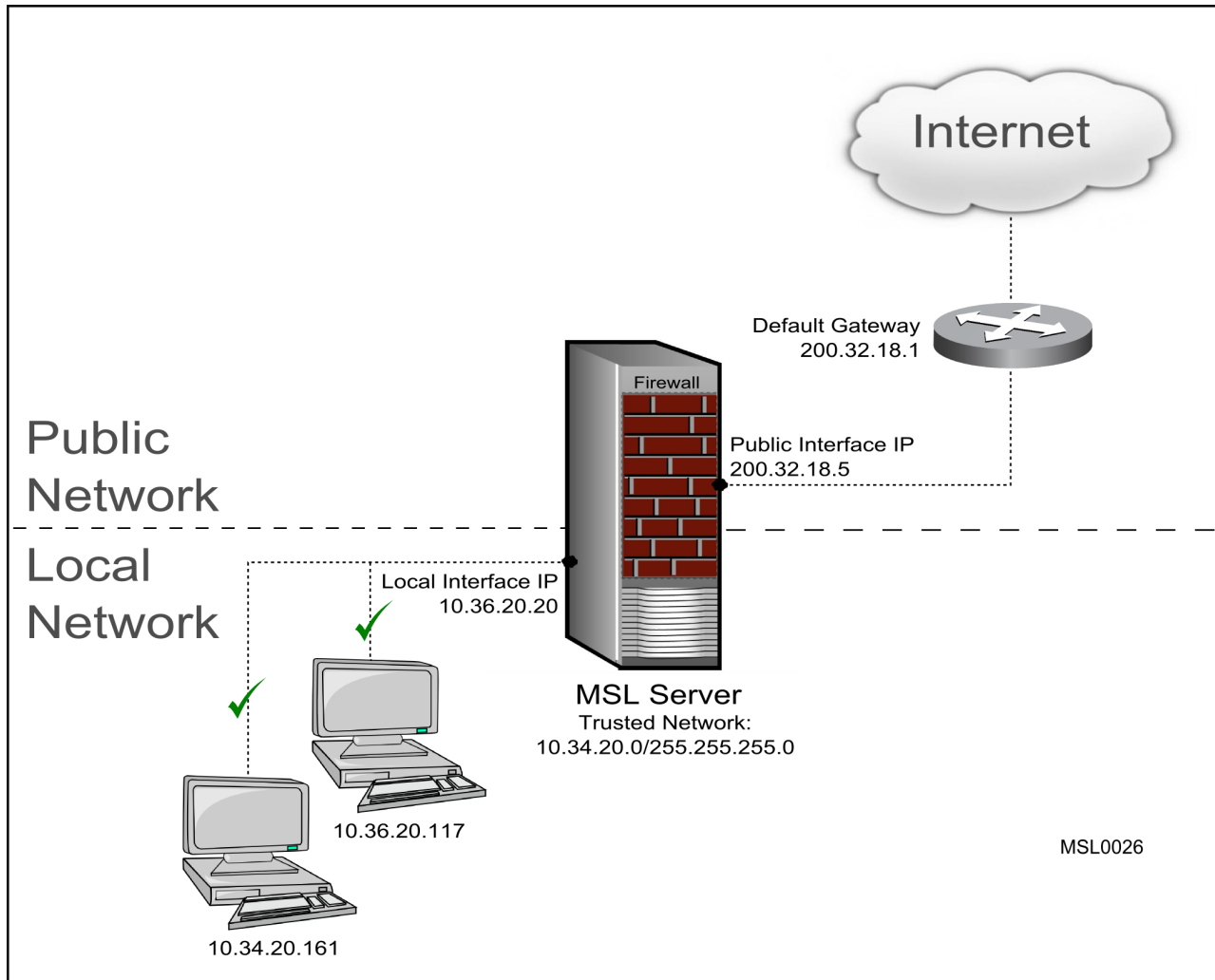
In the example illustrated below, the MiVoice Business system has been configured an IP address of 10.36.20.20 on its LAN interface and with a "trusted network" of 10.34.20.0/255.255.255.0. Accordingly, the

MiVoice Business system will accept MiVoice Business network services from both the 10.36.20.x and 10.34.20.x subnets.



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 10.34.20.x subnets.



Notes :

- If PCs that requires access to the MiVoice Business system are on the same local network as the MiVoice Business system, then you do not need to add trusted networks.
- 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](#) to control access to HTTP and SSH services to specified networks..
- Use [Remote Management](#) to restrict management access to the server.

- Use **Trusted Networks** to provide full access to the trusted network.
- SNMP is accessible only by adding a trusted network. Ensure that [SNMPv2c network access setting](#) is enabled.
- 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 left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.

Note: If you are using the Mitel Performance Analytics (MPA) application for analyzing the MiVoice Business system, then:

- Enable [Secure Shell](#) for trusted and remote management networks.
 - Add trusted network for the MPA with **Network** as 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](#)).

Notes :

- 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**.

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	<p>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).</p> <p>If using a specific SMTP server, specify its hostname or IP address. Otherwise leave this field blank.</p>
Destination port for outbound SMTP	<p>If you have specified a server to use for outbound SMTP, select the destination port for outbound SMTP messaging:</p> <ul style="list-style-type: none">• Port 25 (use cleartext; default)• Port 465 (SSL encryption)• Port 587 (TLS encryption)
Mail Server User ID	<p>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.</p>
Mail Server Password	<p>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.</p>
SMTP e-mail injection restrictions	<p>Controls which networks will be allowed to send mail through this server via SMTP. Choose from one of the following three settings:</p> <ul style="list-style-type: none">• 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
Forwarding address for administrative e-mail	<p>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.</p> <hr/> <p>Note: RAID array event notifications are sent to this e-mail address. We recommend that you configure a valid address here.</p>
E-mail sent for events:	<p>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.</p>

Setting up Cloud Service Provider

The Cloud Service Provider (CSP) panel is the home for the CSP OAuth provisioning. Currently that includes support for two Service Providers:

- [Google](#)
- [Microsoft](#)

You can provision access delegation to user data in the Service Provider using OAuth 2.0, an open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.

OAuth 2.0 allows users to share specific data with applications (for example, contact lists) while keeping their usernames, passwords, and other information private. With OAuth 2.0, user data is protected using access tokens. Applications that use OAuth 2.0 require an authorization code generated in MSL.

For more information on OAuth refer to the official website oauth.net

About Google 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 OAuth 2.0 protocol.

OAuth 2.0 is a relatively simple protocol. To begin, you register your application with Google in order to create 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.

Gadget Service

For MiCollab Audio, Web and Video Conferencing implementations, you should configure the public address of [gadget service](#). This enables users to obtain the a gadget which they can use to transform their Google Calendar events into MiCollab Audio, Web and Video Conferencing conferences with a single click.

[Print Page](#)

Configure OAuth 2.0 for Installed Applications

Use this procedure to configure a secure connection between integrated applications such as MiCollab Client and Google Apps such as Google Contacts or Google Calendar using the OAuth 2.0 protocol.

If OAuth 2.0 authorization is successful then Google will grant an access token to the application on the Mitel Standard Linux server. These tokens can be re-issued when they expire or if the project is changed in any way.

Create an API Project and Client ID in Google

1. Access the Google API console:
 - a. Open a web browser and navigate to <https://code.google.com/apis/console>.
 - b. Enter the domain administrator **Email** and **password** to log in.
2. Create a new project and give it a name such as "NuPoint Advanced UM." Remain in the project.
3. Enable Google APIs for the project:
 - a. Open the side menu and select **API Manager**.
 - b. Select a Google API such as "Calendar API" and click **Enable API**.
 - c. Repeat for all Google APIs you want to support.
4. Create the OAuth 2.0 Client ID and Secret for the project:
 - a. Open the side menu and select **API Manager** and **Credentials**.
 - b. Under **New Credentials**, select **OAuth client ID**.
 - c. Follow the prompts to create a new ID and then click **Create**. Set a **Product name** if prompted.

Note: Select **Other** as the Application type.
 - d. Click **OK**.
 - e. Google provides a **Client ID** and **Client secret**. Record them and the **Product name** for use in the next procedure.

Note: The preceding instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help: <https://developers.google.com/console/help/>

Generate an Authorization Code in MSL

This procedure involves copying your OAuth 2.0 credentials (client ID and matching secret) from the Google APIs console to MSL, which generates an authorization code and then grants an access token. The application on the MSL server employs the access token to integrate with Google services.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Cloud Service Provider > Google**.
3. Select the **Installed Applications** tab.
4. Under **Step 2**, copy and paste the following from the Google APIs console:
 - **Product Name**
 - **Client ID**
 - **Client secret**

5. Click **Save and Generate Authorization Code**. The authorization code is generated and displayed. Remain on the Installed Applications tab in the MSL Server Manager.
6. Under **Step 3**, do the following:
 - a. Copy the authorization code.
 - b. Click the link provided to access the Google API console.

Allow Access Permission in Google

1. After clicking the link to access the Google API console, log in to your account.
2. Submit the authorization code to allow access in Google.

Google grants the access token, which enables MSL to access services in the API project. Note that after the access token is generated, the panel displays its current status (access token ID and expiry time in seconds).

Notes :

- After performing a system (MSL) backup and restore, click the **Refresh Access Token** button to refresh the token and activate the expiry timer.
- The access token is valid only for the set of operations and resources described in the token request. For example, if an access token is issued for the Google Calendar API, it will not grant access to the Google GMail API.
- If you regenerate the client ID and secret, you must then regenerate the authorization code in MSL.
- If an access token expires or you wish to change the list of supported services, you can repeat the procedures to [Create an API Project](#) and [Generate an Authorization Code](#).
- OAuth 2.0 data is not included in system (MSL) backups. Accordingly, if you perform a backup and restore procedure, you must then re-enter the OAuth 2.0 data in order to restore the Google Apps integration.

[Print Page](#)

Configure OAuth 2.0 for Service Accounts

Use this procedure to configure a secure connection between Mitel applications such as NuPoint UM and Google Apps such as Google Calendar using the OAuth 2.0 protocol.

With this type of server-to-server interaction, the application has to prove its own identity but end users do not need to be involved.

Create an API Project and Client ID in Google

Note: The following instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help: <https://developers.google.com/console/help/>

Log In to the Google API Console

1. Open a web browser and navigate to <https://code.google.com/apis/console>.
2. Enter the domain administrator **Email** and **password** to log in.

Create the Project

1. Click the **Create project** button.
2. Enter the **Project name** (for example, "NuPoint Advanced UM") and click **Create**. Remain in the project.

Enable Google APIs for the project

1. Open the side menu and select **API Manager**.
2. Select a Google API such as "Calendar API" and click **Enable API**.
3. Repeat for all Google APIs you want to support. Remain in the project.

Create the Service Account with Client ID

1. Open the side menu and select **Permissions**.
2. Under the **Service accounts** tab, select **Create service account**.
3. Enter a **Name**, select **Furnish a new private key** and **JSON** as the file type, and then select **Enable Google Apps Domain-wide Delegation**. Set a **Product name** if prompted.
4. Click **Create** and **Close**. The service account is created and the file containing the Private Key and Client ID is downloaded.
Note: Store the file in a safe location. You will require it to establish your credentials to MSL.
5. For the service account you just created, click **View Client ID**.
6. Copy the Client ID and click **Cancel**. You will require the Client ID in the next procedure.

Manage API Client Access (API Scopes)

Once a service account is created, you must enable the scope of access for your client ID.

1. Access the Google Admin console:
 - a. Open a web browser and navigate to admin.google.com.
 - b. Enter the domain administrator **Email** and **password** to log in.
2. Click **Security**.
3. Click **Show more** and then click **Advanced settings**.
4. Under **Authentication**, click **Manage API Client access**.
5. On the Manage API client access panel:

- a. Paste the client ID in the **Client Name** box.
- b. Enter the following in the **One or More API Scopes** box:
To support Gmail integration (for NuPoint Advanced UM), enter: <https://mail.google.com/>
- c. Click **Authorize**.

The client ID now has access to resources in the specified domains.

Upload Credentials to MSL

This procedure involves uploading your OAuth 2.0 credentials (service account Client ID and Private Key) from your computer to MSL. MiCollab employs these credentials to integrate with publicly available Google Apps.

1. Log in to the MSL Server Manager as "admin".
2. In the navigation tree, under **Configuration**, click **Cloud Service Provider > Google** tab.
3. Select the **Service Account** tab.
4. Under **Configuration**, choose the following files from your computer:
 - **Service Account ID (.json file)**
 - **Private Key (.p12 file)**

Note: The **Private Key (.p12 file)** file is required only for earlier implementations.

5. Click **Upload Credentials**.
6. Confirm that the Client ID, Email address, and Private Key are correct by comparing them to the corresponding fields in the Google API project.

It is now possible to configure a secure connection to publicly-available Google Apps using the OAuth 2.0 protocol for the Service Account client ID.

Notes:

- You can generate another private-public key pair and then upload the private key to the Service Account in MSL.
- OAuth 2.0 data is not included in system (MSL) backups. Accordingly, if you perform a backup and restore procedure, you must then re-enter the OAuth 2.0 data in order to restore the Google Apps integration.

[Print Page](#)

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.

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.

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

6. Click **Save**.

[Print Page](#)

Configure Microsoft Identity

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

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

1. [Register an application](#), see [here](#) for help.
2. Obtain the unique **Application ID** and **Tenant ID** assigned by Azure Active Directory.
3. When you have the **Application ID** and the **Application Secret** (Client secret), [configure Microsoft Identity](#) on MSL.

Configuring Microsoft Identity

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...**
 1. **Tenant Name (Optional)**: Enter a descriptive name for the tenant directory. This field is optional.
 2. **Tenant ID**: Enter Directory (tenant) ID from the Azure Active Directory. This field is mandatory.
 - **Application Identity...**
 1. **Application Name (Optional)**: Enter the descriptive name for the application created during application registration. This field is optional.
 2. **Application ID**: Enter the Application (client) ID from the Azure Active Directory. This field is mandatory.
 3. **Application Secret**: Enter the client secret obtained from the application **Certificates & Secrets** page. This field is mandatory.

Notes:

- 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**.

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.

[Print Page](#)

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.html>. 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.
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).

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 <input type="button" value="Query"/>

remote	refid	st	t	when	poll	reach	delay	offset	jitter
70.83.139.168	.PPS.	1	u	772	1024	XYXYYXX	46.318	1.385	5.691
142.137.247.109	129.6.15.29	2	u	45m	1024	YXXYYXX	45.903	10.427	1.691
192.95.20.208	18.26.4.105	2	u	547	1024	YYYYYYY	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.

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

The following table provides the meaning of the command output:

Command output	Meaning	
remote	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:	
	*	The system time is being synchronized with the NTP server.
	#	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 synchronised with a time server.
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		<p>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.</p> <p>Example: If the field contains XXXXXX YY, the two most recent NTP transactions have been successful while the previous six have failed.</p>
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.

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.

[Print Page](#)

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. To activate this server for ServiceLink, under **ServiceLink** click **Status**, enter the activation code and click **Activate**.
7. To automatically make hostnames available throughout the Internet, under **ServiceLink** click **DNS services**.
8. Click **Publish Globally** to make the hostnames available through the DNS server on the Internet.
9. Click **Next**.
10. 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**.

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** .

[Print Page](#)

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.

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.

Add illustration here

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.
IPv6 Address of the Tunnel (Optional)	<p>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.</p> <p>Note: Your service provider provides this IPv6 address.</p>
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.

Configure SNMP Support

SNMP, or 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: <ul style="list-style-type: none">• 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). Note that the networks in the Remote access panel are typically public, and including them will open your SNMP services to potential attack via the internet.
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. <ul style="list-style-type: none">• 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)

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, an 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.
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	Enter the SNMPv3 trap user name to use when sending trap messages. If you leave this field blank, SNMP traps will be sent using SNMP v2c.
Download Mitel enterprise MIBs	<p>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.</p> <hr/> <p>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.</p>

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	<p>Select the Authentication Type that matches SNMP manager/agent configuration:</p> <ul style="list-style-type: none"> • 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.
Privacy Protocol	<p>Select the Privacy Protocol that matches SNMP manager/agent configuration:</p> <ul style="list-style-type: none"> • 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.

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.

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 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

Support and Licensing

You obtain licenses for the managed services and applications from the license server. Refer to *MSL Installation and Maintenance Guide* for more information on Licensing .

[Print Page](#)