

MITEL

Mitel Standard Linux



Installation and Administration Guide

Release 10.0



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Mitel, Mitel logo, and SX-200 are trademarks of Mitel Networks Corporation.

Linux is a registered trademark of Linus Torvalds.

The terms "ssh" and "Secure Shell" are trademarks of SSH Communications Security Corp.

Trend Micro is a registered trademark of Trend Micro Incorporated.

VMware, VMware vMotion, VMware vCloud, VMware vSphere, ESX, and ESXi are trademarks of VMware Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

See also [Appendix A: Third Party Licenses](#).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

To obtain the source code of third-party components licensed under the GNU General Public License or Lesser General Public License, please email gplrequest@mitel.com.

Mitel Standard Linux
Installation and Administration Guide Release 10.0
June 2013

®,™ Trademark of Mitel Networks Corporation
©Copyright 2013, Mitel Networks Corporation
All rights reserved

ABOUT THIS GUIDE	1
ABOUT MITEL STANDARD LINUX	1
Server-gateway Configuration.....	1
Server-only Configuration.....	2
Server-gateway with Bridged Interface Configuration.....	3
Security for MSL Applications.....	4
WHAT'S NEW IN THIS RELEASE	5
MSL Release 10.0 provides the following new features:.....	5
MSL Release 9.4 SP1 provides the following new features:.....	6
MSL Release 9.4 provides the following new features:.....	6
MSL Release 9.3 provides the following new features:.....	7
MSL Release 9.2 provides the following new features:.....	8
MSL Release 9.1 SP1 provides the following new features:.....	9
MSL Release 9.1 provided the following new features:.....	9
ACCESS THE MSL QUALIFIED HARDWARE LIST	10
AMC LICENSING	11
About the Applications Management Center.....	11
Requesting a New AMC Account.....	12
Accessing your AMC Account.....	12
Finding More Information.....	12
INSTALLING THE HARDWARE	13
General Requirements of the MSL Host Computer.....	13
Hardware Compatibility.....	13
About RAID.....	13
Hardware RAID.....	14
Software RAID.....	14
Firmware or Driver-Based RAID.....	14
MSL Software RAID.....	15
BIOS Settings for RAID.....	15
INSTALLING THE SOFTWARE	16
Collect Site Information.....	16
Installation Notes.....	17

Upgrading from a Previous MSL Version	17
Create Application Record.....	19
Obtain MSL Software.....	19
Download Image from Mitel Online.....	20
Copy Image to CD	20
Copy Image to USB	20
Install MSL Software.....	21
CONFIGURING THE SERVER	22
Restore from Backup?	22
Set Administrator Password	23
Configure Domain Name	23
Configure System Name.....	23
Select Local Network Adapter	23
Enter Local Networking Parameters	24
Enable IPv6 Protocol	25
Select WAN Adapters	25
External Interface Configuration	26
Select Gateway IP Address	26
Select Additional Static IP Address	26
Configure DNS.....	26
Activate/Reboot.....	27
INSTALLING SOFTWARE BLADES.....	28
SERVER ADMINISTRATION AND MAINTENANCE	29
Server Manager.....	29
The Server Manager Menu.....	30
Blades	31
Status.....	33
Online Activation	34
Offline Activation	34
Deactivation	35
Backup	35
View Log Files.....	37
Collect Logs and Diagnostic Data.....	38
Event Viewer	39
System Information	41
System Monitoring	41
System Users.....	41
Digital VPN Certificates for System Users.....	43
Shutdown or Reconfigure	45

Remote Access	46
Local Networks.....	49
Port Forwarding.....	50
Web Server Certificates	51
Client Certificate Management.....	56
Email Settings	57
DHCP	58
Date and Time.....	60
Hostnames and Addresses	63
Domains	64
DNS Forwarder	65
Simple Network Management Protocol (SNMP).....	66
Configure Network Interface Card Settings.....	68
Review Configuration	69
THE SERVER CONSOLE	71
Offline Sync with the AMC	73
Performing Backups	74
Backing up to a USB Device	74
Backing up to a Network File Server.....	74
Verify Backup File.....	75
Restore Configuration Information.....	76
Restore during MSL Re-installation	76
Restore on an Operational System.....	77
Restore from another Running Server	78
Accessing the Linux Root Prompt.....	81
Changing the Administrator Password	82
Resetting the Administrator Password.....	82
TROUBLESHOOTING	83
TECHNICAL SUPPORT.....	83
APPENDIX A: THIRD PARTY LICENSES.....	84
Apache.....	84
Open SSL	87
Original SSLeay License	88
Perl	89

Net-SNMP.....	91
Boutell.Com	98
Fontconfig.....	100
Gnu General Public License	100
GNU Lesser General Public License	110
GLOSSARY	113

About this Guide

The Mitel® Standard Linux Installation and Administration Guide is intended for Resellers who are installing and configuring Mitel Standard Linux (MSL).

 **Note:** Prior to Release 8.2, MSL was called Managed Application Server.

About Mitel Standard Linux

Mitel Standard Linux (MSL) is an operating system and server solution for single-site and branch-based enterprises. MSL provides a base for a suite of managed services and applications delivered from the Mitel Applications Management Center (AMC) or available on CD.

MSL can provide one of the following network configurations:

- **Server-gateway:** functions as an Internet-facing server with firewall capability.
- **Server-only:** functions as an internal server on the local area network (LAN).
- **Server-gateway with Bridged Interface:** functions as an Internet-facing server with firewall capability, and as a bridge to the corporate firewall for data traffic. This configuration requires MSL 9.2 and a minimum of three network interface cards.

Server-gateway Configuration

In the server-gateway configuration, MSL manages the 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 intrusions.

When one of the computers on the local network contacts the Internet, MSL 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.

Throughout this document, the term "MSL" refers specifically to the operating system software that is installed on a computer that hosts the application(s) and subscription services delivered from the AMC.

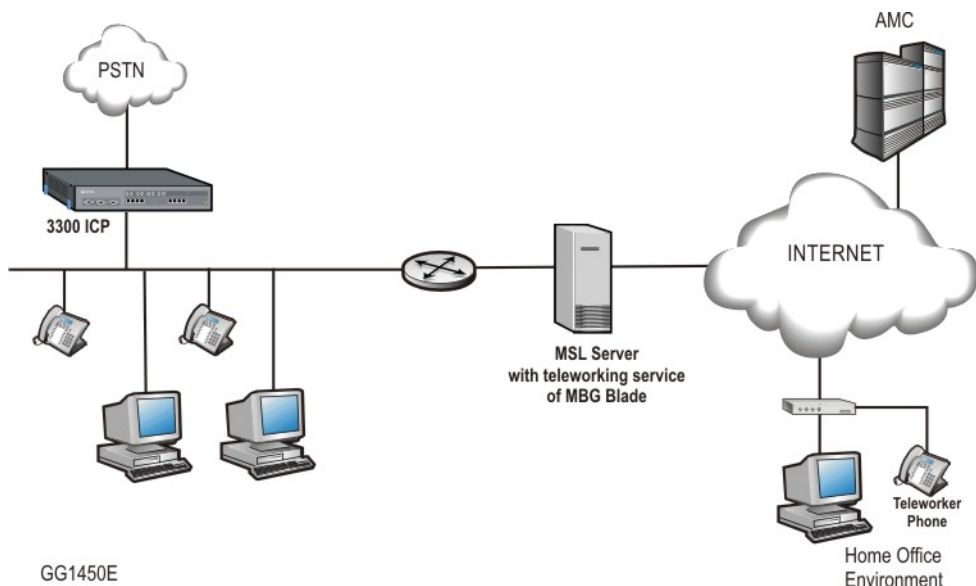


Figure 1. Server-gateway configuration example

Server-only Configuration

When MSL is deployed in server-only mode, it provides the network with services, but not the routing and security functions associated with the role of "gateway". The server-only configuration is typically used for networks that are already behind a separate firewall. In other words, a separate firewall fulfills the role of gateway, providing routing and network security.

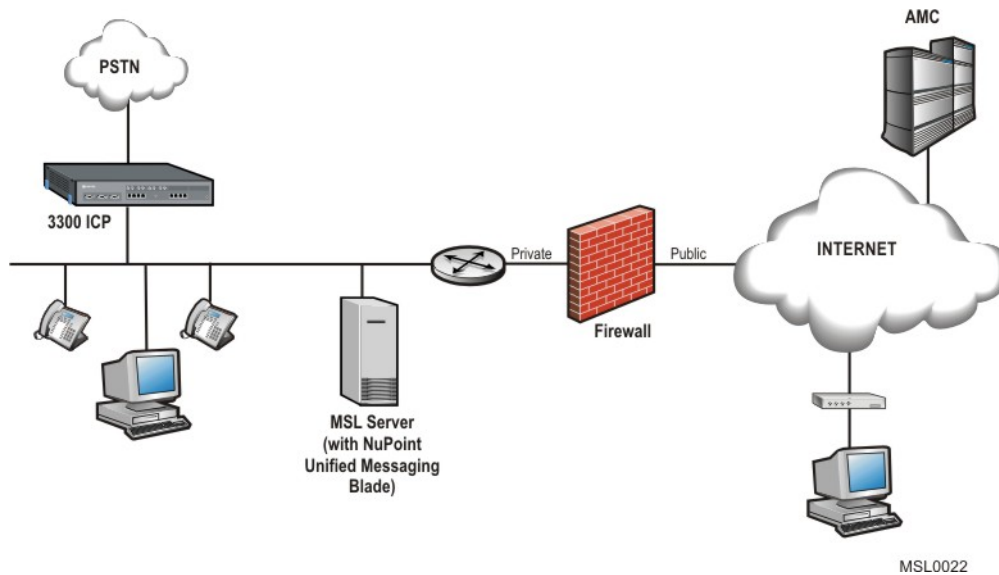


Figure 2. Server-only configuration example

Server-gateway with Bridged Interface Configuration

In this configuration, MSL is deployed parallel to the corporate firewall, providing a public interface to the Internet for VoIP traffic, and a bridged interface to the firewall for all other traffic.

To enable this functionality, the MSL server requires at least three network interface cards. The first NIC connects directly to the LAN, the second connects to the Internet, and the third connects to the WAN interface of the firewall in bridged mode.

When incoming traffic arrives on the server's WAN interface, it is routed to the appropriate network segment. Voice packets are sent directly to the Voice VLAN and data packets are bridged to the firewall's WAN interface. By separating the traffic between the voice and data network segments, QoS for voice calls is improved. This setup also enables a Voice VLAN to be installed into an existing Data VLAN without having to update the firewall rules.

As part of this configuration, you can prioritize voice over data traffic using the Mitel Border Gateway's "Bandwidth Management" feature. Simply program the maximum amount of bandwidth available on the WAN communication links (inbound and outbound). The system employs these settings to establish traffic shaping queues which give priority to voice calls ahead of data traffic.

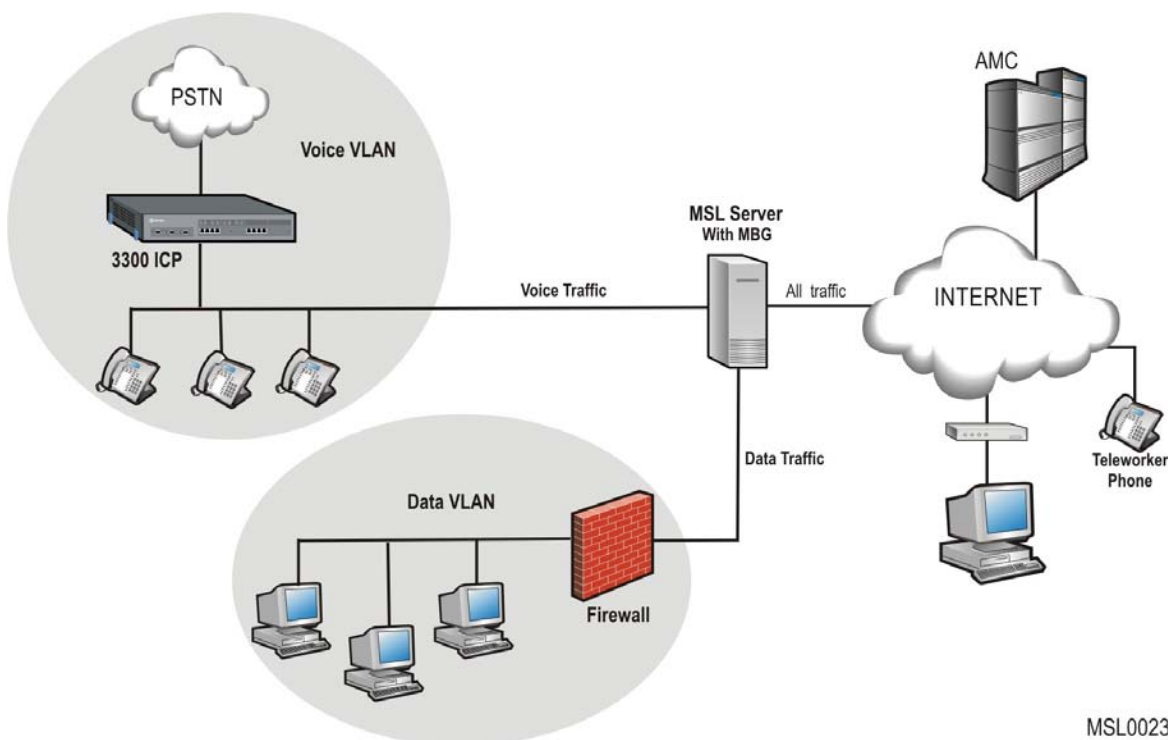


Figure 3. Server-gateway with Bridged Interface configuration example

After installation, MSL can be configured and managed remotely from one of two interfaces:

- The web-based server manager, accessed from the administrator's desktop
- The server console, accessed from the server itself or remotely using an SSH client

Security for MSL Applications

MSL may host many standalone applications with very different features. While it is technically feasible to install several applications on the same MSL, the inherent design of each application may impact co-residency considerations. For example, the Mitel Border Gateway (formerly Teleworker) application is specifically designed for direct connection to the public Internet. Other MSL applications, like Unified Communicator Mobile (formerly Mobile Extension), Live Business Gateway, and NuPoint Unified Messaging (UM), are designed to operate within the enterprise LAN.

Security best practices suggest that highly secure deployments of applications designed to operate within the enterprise LAN should be installed behind a firewall on an MSL server deployed in server- only configuration and not co-resident with applications specifically designed for connection to the public Internet. For this reason Mitel does not recommend that standalone enterprise-only applications and Mitel Border Gateway be installed on the same MSL server.

What's New in this Release

MSL Release 10.0 provides the following new features:

- **General Enhancements:**

- MSL 10.0 is based on CentOS 6.3 and is available in both i686 (32-bit kernel, 32-bit user space) and x86-64 (64 bit kernel, 32-bit user space) versions. CentOS 6.0 is required to ensure compatibility with recently released hardware servers.
- Clustering has been removed from the interface due to the discontinuation of the NPM 640 system.
- The ETX option has been removed from the a software installation procedure due to the discontinuation of the ETX and APC product variants.

- **Installation and Upgrades:**

- If you select "Restore from Backup?" after installing MSL software, you may now obtain the backup files from another running server in addition to a network drive or removable device. The new option facilitates the replacement of an existing MSL 9.x server (physical or virtual) with a new MSL 10.x server.
- Physical servers running MSL 9.3 or 9.4 can now upgrade to MSL 10 without physical media or console access. Use the new MSL Remote Fresh Install (RFI) blade to automatically upgrade to Release 10 from the Blades panel while maintaining configuration settings.

Note: The RFI blade requires sufficient disk space for a backup. If your system has insufficient disk space, the blade will be unavailable on the Blades panel.

- **Security Enhancements:**

- Increased resistance to cross-site request forgery and scripting attacks.
- Communications between the MSL server and the AMC now use SSHv2 for improved security.
- SNMP security enhancements: Administrators may now choose between SNMPv2c and SMNPv3. SNMPv3 is the latest version of the SNMP protocol and introduces authentication and encryption for network management communications.
- For increased security, you can use SSL client certificates to authenticate VPN connections for remote users.

- **Alarm Enhancements:**

- The Event Viewer panel has been enhanced to make it easier to determine the reason for alarms. New settings enable you to clear a single event (as opposed to all events) and display only new events (as opposed to both new and cleared events). Also, the "Start" and "End" date fields have been made to easier to use.

- **MSL Backup Enhancement:**

- You can now perform network backups to Linux servers that support secure FTP (SFTP). Previously, you were limited to performing network backups to Windows servers using the SMB/CIF protocol.

- **Integration with Hosted and Cloud-based Systems:**

- Support for configuration of OAuth 1.0 and OAuth 2.0 protocols for application interaction with cloud-based systems like Google Gmail and Google Calendar.

- The destination port for outbound SMTP can now be set to 587 (TLS), in addition to 465 (SSL) or 25 (clear text). The use of secure ports is required by some hosted email service providers such as Google Apps.

MSL Release 9.4 SP1 provides the following new features:

- **Server Manager Enhancements:**

- The email settings can now be configured to support a direct connection to an SMTP relay (smart host) such as Google Apps using secure port 465.
- The new "Log Collector" utility allows you to create an archived file of system-level logs and then save the file to another location such as your local PC.

MSL Release 9.4 provides the following new features:

- **General Enhancements:**

- MSL 9.4 is based on CentOS 5.7 and is available in both i686 (32-bit kernel, 32-bit user space) and x86-64 (64 bit kernel, 32-bit user space) versions.
- **ServiceLink upgrades (from the "Blades" panel) are available for both versions effective with the following releases:**
 - 32-bit: Rel 9.1.24.0 and later
 - 64-bit: Rel 9.2.21.0 and later

- **MSL Backup Enhancements:**

- Network backups can now be made to a specific sub-directory on the MSL server. Previously, backups were always placed in the root directory.
- When restoring backup files on an operational system, the following prompt no longer appears: "Do you wish to restore from backup?" The prompt still appears when you perform a restore during the software installation process.
- In previous releases, after you restored a backup configuration the default gateway address displayed incorrectly. This problem has been corrected.

- **Installation Enhancements:**

- USB storage devices may now be formatted with the NTFS file system in addition to FAT32 and EXT3. This allows for file sizes larger than 4 GB.
- It is no longer possible to switch (upgrade or downgrade) between the 32-bit and 64-bit kernel versions of MSL. If you attempt to do so, you will receive an error message.
- On an initial installation, when you configure the server parameters you are now prompted to "Enter Local Subnet Mask" rather than "Select local subnet mask."

- **Server Console Enhancements:**

- There is no longer a need to log in a second time after selecting "Access Server Manager" from the Server Console menu.
- In previous releases, if you upgraded a software blade from the Server Console, the new software version would be displayed irrespective of whether the upgrade was successful. This problem has been corrected and the actual software version now displays in all circumstances.
- When you initiate a reboot, shutdown or reconfigure from the Server Console or Server Manager, you will be prompted to confirm your selection. In previous releases, these actions occurred immediately.

- If you configure a Corporate DNS server address, you can now specify whether it should perform name resolution for all domains, or only for non-local domains.
- **Server Manager Enhancements:**
 - It is now possible to download SSL certificates and private key files from one MSL server and upload them to another.
 - Regular patterns can now be used in the “Filter Pattern” and “Highlight Pattern” fields on the View Log Files panel. In addition, log download performance has been optimized for faster viewing of large logs.
 - A new “cache” option has been added to the Blades panel. It enables you to download software blades for installation/upgrade at a later time.
 - The System Information panel now indicates whether the MSL Kernel Version is 32-bit or 64-bit.
 - Cluster management has been made easier: You can now remove a cluster simply by clearing its Cluster IP address, and you can update a password in the server manager and have the change replicated across the cluster nodes.
- **Virtualization Enhancements:**
 - OVA files for all Mitel Virtual appliances now include the Mitel Virtual Framework (MVF) blade. This software blade manages optional VMware features like Site Recovery Manager and High Availability. See your application documentation for instructions on how and when to update this blade.
 - If the MAC address of the network interface card in a single-NIC system changes (for example, if you create a new virtual machine (VM) and then restore a backup from a previous VM), MSL 9.4 recognizes and stores the changed address. In previous releases, you may have had to step through the "Configure this Server" option to make MSL recognize the updated NIC. Note: This feature may not be effective for physical hardware with multiple NICs. If networking does not respond properly, you may still have to step through the "Configure this Server" option to reset the addresses.

MSL Release 9.3 provides the following new features:

- **Installation Enhancements:**
 - CD boot screens now indicate when the 64-bit MSL version is being installed.
 - A USB device can now be used to install/upgrade MSL software.
- **Internet Protocol Version 6 (IPv6) Support:**
 - Server Console: Local Networks and WAN Interface configuration screens now have the ability to accept IPv6 addresses.
 - Server Manager: The server manager can be accessed via IPv6. Along with Local Networks and WAN configuration screens, the Review Configuration screen now displays IPv6 information. IPv6 access to System Monitoring and SSH are also provided.
- **Remote SSH Access Security Improved:**
 - Secure shell access is extended to remote management networks in addition to local networks. This enables external administrators, such as Mitel Product Support personnel, to access the system in relative security and avoid using the “Allow public access” option.

- **AMC Synchronization Improvements:**
 - Online Sync: If an AMC synchronization has not been successfully completed within 24 hours, a Major alarm is raised.
 - Offline Synch: Offline systems that migrate to MSL 9.3 will generate a Major alarm indicating that AMC synchronization has failed. To disable auto-synchronization and prevent further alarms, re-do the offline activation procedure.
- **Download Manager:**
 - MSL software can now be downloaded from Mitel OnLine using the optional Download Manager, an ActiveX application installed through your web browser. In addition, you can still use HTTP to download software.

MSL Release 9.2 provides the following new features:

- **Installation Enhancements:**
 - Server and APC (ETX) installations are now packaged in one image. You can select either package at the initial boot.
 - Rescue mode images are supplied for file recovery in case of MSL failure
 - Hardware detection and memory test utilities now appear as options at boot time
 - When MSL detects a system with multiple hard disks, such as NuPoint with a storage array, it prompts you to include/exclude each drive in the MSL partition.
 - MSL displays an error message if it cannot detect a hard drive (usually caused by incompatible SCSI/SAS hardware).
- **Server Manager Enhancements:**
 - ServiceLink AMC Synchronization: Offline synchronization support has been added for deployments that do not have USB capability. Also, it is now possible to perform an online synchronization via a proxy by entering the proxy's IP address and connection port.
 - Time Server Connectivity: A Query button has been added to the NTP/Date and Time screen to ensure that network connection to the time server is valid.
 - System Information Enhanced: The System Information option now provides hardware manufacturer and product name/model information.
 - Network Interface Card Settings: The NIC Settings screen provides an interface to configure NIC speed for deployments that need to override the default setting of "auto-negotiate".
- **Server Console Enhancements:**
 - The server console now includes a "Restore from backup" menu item that provides an "on demand" restore option. You can restore from a backup that was saved to either a removable device (USB/CD), or to a network file share. This option reboots the server and then displays the "Do you want to restore from backup?" prompt.
- **Alarm Enhancement:**
 - Event Viewer: The Event Viewer panel is enhanced with configurable start and end dates for searches (the default time period is the previous 7 days), and the ability to enter regular expressions (regex) in the Text filter field.

- E-mail Settings: MSL 9.2 extends alarm capabilities to configurable email notification. Emails are sent to the configured administrator email account if alarms meet or exceed the user-selected severity.

MSL Release 9.1 SP1 provides the following new features:

- **MSL Backup Enhancements:**
 - **Desktop backup** handles larger data sets, with more accurate reporting of pre-compressed backup size
- **Scheduled Network Backup now supports:**
 - daily, weekly, and monthly backups
 - configurable backup storage – set a maximum number of backup files to keep on server
 - “Backup Now” button for immediate backup
- Certificate Signing requests for submission to third-party certificate authorities are now generated with 2048-bit keys
- RAID Array events are now forwarded to the “Forwarding address for administrative email”, if configured, or delivered to admin-raidreport@<domain name>.

MSL Release 9.1 provided the following new features:

- **Scheduled Network Backups:** setup a schedule for automatic network backup
- **Web Server Certificates Panel:** generate Certificate Signing Requests and import third-party signed SSL certificates
- **Offline Synchronization Menu:** Provides an offline method to synchronize with the AMC.
- **Keyboard Selection:** Installation procedure allows for selection of non-US keyboards
- **Improved Backup Verification Handling:** MSL offers a "Try again" screen if the USB device is not detected.
- **‘memtest’ Utility Improvements:** use the memtest utility to test server memory even on the most recent CPUs.
- **MAS Applications Installation from CD/DVD:** When installing application blades, MSL recognizes MAS deployments and routes the installation to a MAS-specific process. (The CD/DVD installation procedure for non-MAS applications remains the same.)
- **Update Mitel Applications Suite Panel:** For MAS deployments only, MSL now provides a dedicated menu in the server console for updating the MAS application.

Access the MSL Qualified Hardware List

To access the MSL Qualified Hardware List:

1. Log in to Mitel OnLine.
2. Point to **Support** and then click **Product Documentation**.
3. Point to **Applications and Solutions**, and then select **Mitel Standard Linux** from the drop-down list.
4. Click **Qualified Hardware List**.


AMC Licensing

About the Applications Management Center

The Mitel Applications Management Center (AMC) is an online service accessed via the Internet that provides licensing, monitoring, management, and a variety of other services for installations of Mitel software applications. The AMC is also the procurement and provisioning interface for AMC-delivered products and services. As a reseller of Mitel products, you receive a unique licensing account on the AMC system. By logging in to the AMC with the user name and password you are given when you obtain your account, you can view a list of your AMC-enabled products, check their status, and add or drop services from any of them.

When you place a new order for Mitel products with Customer Services, the order information is entered into the AMC system. The AMC places the purchased licenses into your licensing account. Before you can install application software, there are four steps to follow:

- In your AMC account, create an Application Record for the MSL-based system and take note of the Application Record ID.

 **Note:** Each Application Record represents one physical hardware device (server or controller).


- Assign all application licenses to the MSL Application Record.
- Assign all User and Device licenses to the appropriate 3300 ICP Application Record.
- Install the MSL-based software and register with the AMC to activate the license.

When the installation of the MSL operating system is complete, it generates a unique Hardware ID. When connected to the AMC through the Internet, you must enter the Application Record ID (also called Service Link ID) that you created for this installation. MSL uses the Hardware ID and the Application Record ID to identify itself to the AMC. Upon synchronization with the AMC, purchased software and options become available.

After online registration, MSL will connect to the AMC regularly via a secure, encrypted connection to synchronize or "sync". When you add or delete services using your AMC account, MSL receives its new configuration instructions from the AMC at the next sync. You can force an immediate sync by clicking the **Sync** button on the **Status** page of the server manager. You can also use Sync to check that connectivity between the server and the AMC has been restored after a network problem.

The most important services provided by the AMC for the MSL family of products are:

- Licensing
- Software blade downloads
- Software Updates (security patches)

 **Note:** If your server is behind an additional firewall, that firewall must be configured to allow outbound SSH packets on TCP port 22 to permit server communication with the AMC.

Requesting a New AMC Account

To request an AMC account, send an email containing the following information to amc_accounts@mitel.com:

- Name of your certified Technician
- Full company name
- Company mailing address
- Phone 1/Phone2
- Fax number
- Admin email (address of the person who should receive notification of service expiry dates)
- Tech email (address of the person who should receive notification of update releases and other technical notices)
- Company URL (if any)
- Your Mitel SAP account number
- Specify if you would like your user ID and password delivered to you by fax, phone, or both (for security reasons user IDs and passwords are not sent by email).

Please allow two business days for your AMC account to be created.

Accessing your AMC Account

To access your account for the first time:


1. Go to the Mitel web site (<http://www.mitel.com>) and log in to your Mitel OnLine account.
2. In the menu bar, point to Purchasing and then click AMC.
3. Sign in with your unique AMC ID and password to establish your "single sign on". On subsequent visits, you access your AMC account directly after signing in to Mitel OnLine.

For information about using the AMC, click the online [Help](#) link in your AMC account.

Finding More Information

To access documentation/software from the Internet:

1. Log in to Mitel OnLine.
2. Point to **Support**.
3. Do one of the following:
 - Click **Product Documentation** to access documentation
 - Click **Software Downloads** to access MSL software

 **Note:** You must be a registered user to access documentation and software downloads through Mitel OnLine.

Installing the Hardware

MSL software relies upon the host computer meeting the documented hardware standards. Mitel Networks Corporation reserves the right to limit support for hardware configurations that we determine to be incompatible with MSL software. Please note that future applications from Mitel may be certified and supported only on specific hardware platforms that provide the requisite speed and performance.

General Requirements of the MSL Host Computer

Hardware requirements for the MSL host are generally dictated by the requirements of the applications that it hosts. Here are some general notes:

- The amount of available RAM is one of the most important considerations for performance as it reduces the load on the disks. If a tradeoff is required, extra RAM is usually more beneficial than a faster CPU.
- For a dedicated connection in a server-gateway configuration, the server requires two Ethernet adapters (also called network adapters or network interface cards). For a server-gateway with a bridged interface, the server requires three Ethernet adapters (one for the LAN, another for the WAN, and a third for the bridged connection to the WAN interface of the firewall). For a server-only configuration, only one Ethernet adapter is needed.
- The software supports most external modems; internal modems are not supported.

To test server memory before installing MSL, or to debug possible memory problems, see Troubleshooting on page 83.

Hardware Compatibility

Please refer to the **MSL Qualified Hardware List** available at Mitel OnLine for a complete list of supported servers along with a matrix that provides the correct MSL version for all MSL-compatible applications. Mitel recommends servers from this list only and reserves the right to limit support for other hardware configurations.


About RAID

MSL supports disk redundancy, also called RAID Level 1. Disk redundancy ensures that all data is written to two separate hard disks installed in the server. If the primary disk fails, the mirror disk will continue as if nothing had happened. All of the data is protected.

If a disk failure occurs while using MSL software RAID, email notification is sent immediately to the administrative forwarding address configured on the MSL server. If the forwarding

address has not been configured, the email is sent to `admin-raidreport@<domain name>`, which must be a valid email account your domain's email server. If neither of these addresses is valid, the notification is not delivered. For this reason, we strongly recommend that you configure an [administrative forwarding address](#).


Disk redundancy can be accomplished using either the MSL operating system software RAID, or an actual hardware RAID controller.

 **Note:** Although RAID improves data reliability, to fully protect your system you should perform a backup on a periodic basis. For details, see [Perform Backup](#) on page 74.

Hardware RAID

A hardware implementation of RAID uses special-purpose RAID controller hardware. On a desktop system this can be a PCI or PCI-e expansion card. Most hardware implementations provide a cache that generally improves RAID performance. In most systems the write cache is battery-protected, so pending writes are not lost when power fails. Hardware implementations provide guaranteed performance, add no overhead to the local CPU system, and can support many operating systems since the controller presents a virtual single logical disk to the operating system. You configure a RAID array in the controller where you will install MSL. MSL sees this array as a single disk.

MSL is compatible with the recommended hardware-based RAID controllers. The RAID array that will store MSL must be configured before installing MSL.

 **Note:** MSL RAID drive failure notification is not active when hardware RAID is used. To enable drive failure notification, additional RAID adapter-specific software must be installed.

Software RAID

Software implementations of RAID are now supplied by many operating systems. A software layer sits above the disk device drivers and provides an interface between the logical and physical drives. Software RAID must run on a host server attached to storage, and the server's processor must dedicate processing time to run the RAID software. Processing time required for RAID1, which MSL uses, is negligible. An advantage of software RAID is that it allows RAID disks to be easily moved from one computer to another, which is very useful when hardware fails.

Firmware or Driver-Based RAID

To supply a RAID controller that is cheaper than Hardware RAID, some manufacturers have introduced Firmware RAID, which is not a RAID controller chip but is simply a standard disk controller chip with special firmware and/or drivers. During early-stage bootup, the RAID is implemented by the firmware. When a protected-mode operating system kernel (such as MSL) is loaded, the drivers take over. The bulk of RAID processing is done by the host computer's CPU, not by the "RAID controller" itself. Most embedded RAID devices are Firmware/Driver-based RAID controllers and have been used on many entry-level servers.


Firmware/driver-based RAID, known as "dmraid" in MSL, is NOT supported.

MSL Software RAID

The MSL system uses Linux software RAID, which has proven reliability and supportability. The MSL RAID configuration utility also includes management, monitoring, and reporting capabilities. Moreover, if a hardware problem occurs, the system can usually be rescued by moving the disks to another system. This is not the case for hardware- or firmware-based RAID.

To enable software RAID1 support, you must have two disks that are the same size or that are capable of having partitions of the same size. These disks can be SCSI, IDE, Serial ATA (SATA), or Serial Attached SCSI (SAS) drives. When the MSL installer detects a server with two fully functional disks, it will configure the disks into a RAID Level 1 array, which is subsequently controlled by the MSL operating system. You can install MSL software on a single disk and then insert a second (blank) disk at a later date to create a mirrored pair (use the “Manage Disk Redundancy” option in the server console to activate the second disk).

If two disks are installed that are not configured into an existing hardware-controlled array, the MSL installation automatically creates an MSL-controlled RAID1 array.

 **Note:** MSL does not support RAID Level 0 (disk striping), because it does not provide data protection. MSL does not support RAID Level 5 (disk striping with parity) because of the poor performance and reliability of software implementations of RAID5. If you are seeking RAID5 support, Mitel recommends you consider one of the many hardware implementations, which will provide both protection and performance.

BIOS Settings for RAID

The BIOS for each server can be unique. As a result, we must analyze the SATA/RAID controller settings on a server-by-server basis. This process is part of the MSL hardware qualification program, and involves testing new servers and recommending the appropriate BIOS settings for various SATA/RAID controllers. See the MSL Qualified Hardware List available at Mitel OnLine.

This process is part of the MSL hardware qualification program.

Each server BIOS is different and we analyze the SATA/RAID controller settings, on a server-by-server basis, in the MSL hardware qualification program. As new servers are tested, recommendations will be made about BIOS settings to use when dealing with various SATA/RAID controllers. See the MSL Qualified Hardware List available at Mitel OnLine.

Installing the Software

Installation of MSL consists of the following tasks:

- Collect Site Information (this page).
- Read [Installation Notes](#) on page 16.
- [Create Application Record](#) on page 19.
- [Obtain MSL software](#) on page 19.
- [Install MSL Software](#) page 21.
- [Configure MSL](#) on page 22.
- Launch the [Server Manager](#) on page 29.

Collect Site Information

The following table lists the information you need to enter during installation and configuration. For efficient installation, we recommend that you gather this information beforehand:

Item		Notes	Your Information
Server Configuration			
1.	Administrator Password	For password strength, choose a password that contains a mix of upper and lower case letters, numbers, and punctuation characters, and that is not a dictionary word.	
2.	Domain Name	Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 23.	
3.	System Name		
4.	IP address of your MSL server	The local, static IP address of the server where you are installing MSL.	
4b.	IP address of your external NIC(s)	The IP address of your external Ethernet connection.	
4c.	Alias IP for your external NIC	A second, alias IP address used for applications that require a server with two IPs (like Mitel Collaboration Advanced)	
5.	External Interface Connection	Cable Modem? You need to know if the ISP requires an Account Name OR an Ethernet address as identification in DHCP requests	
		DSL Connection? You need to know the username and password for authentication	
		Direct Connection? You need to know the static IP address	

Item		Notes	Your Information
6.	Gateway IP Address	The IP address that your MSL server will use to access the network.	
7.	DNS Server IP Address	Enter the IP address of your corporate DNS server. Note: If your DNS is supplied by your ISP, leave this setting blank.	
8.	Application Record ID #	The number generated when you created an Application Record ID for this product in your AMC account.	
<p>“Local Network” Access</p> <p>If your ICP or some of your users are not on the same subnet as the MSL server, you need to classify them as “Local Networks” and then allow them access. Both IPv4 and IPv6 networks are supported.</p>			
1.	IP Address	The IP address of the network for which you want to allow access	
2.	Subnet	The subnet mask for the range of IPv4 addresses you wish to allow.	
3.	Router Access	The address of the router/gateway you will use to access the network (or subnet) to which you are granting access	

Installation Notes

- If you are upgrading from a previous release of MSL software, see [Upgrading from a Previous Version](#) on page 17.
- If you are performing a fresh install, see [Install the Software](#) on page 21.

Upgrading from a Previous MSL Version

Mitel Standard Linux provides an upgrade path for most software versions. If you have previously installed a server and now want to upgrade, you can do so while preserving configuration data. Follow the installation instructions and choose the **upgrade** option after the previous installation is detected. As a precaution, you should always perform a backup of the system prior to performing this upgrade.

MSL can be upgraded in one of three ways:

ServiceLink Upgrade

The ServiceLink update option is the easiest way to upgrade MSL; it is available in the Blades panel on the server manager. For more information, see [Upgrade the MSL Blade](#).

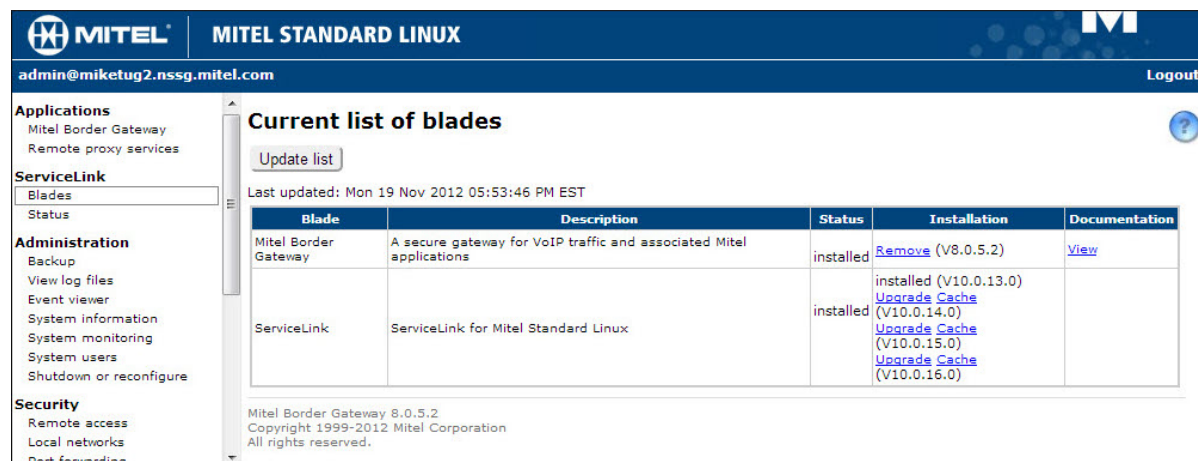


Figure 4. ServiceLink option in Blades Panel

Note that some applications do not support this option, and that it is not available for major upgrades (for example, upgrading from MSL 9.x to MSL 10.x). If the ServiceLink update option update is not visible on the Blades panel, then you cannot use it for your implementation.

CD or USB Upgrade

You can upgrade from physical media for most MSL software releases. Boot from the MSL CD or USB flash drive and select the “upgrade” option during the install. Although configuration and application data is maintained, a backup is recommended. For more information, see [Install the MSL Software](#).

Fresh Install

Major software upgrades (e.g. upgrading from MSL 9.x to MSL 10.x) generally require a fresh software installation. This entails backing up the database, installing the new MSL version from a CD or USB flash drive, and restoring the database. For more information, see [Install the MSL Software](#).


Notes:

- Ensure that your current software applications are compatible with the new MSL version and that they support the Upgrade option.
- You cannot change the primary domain name during an upgrade.

If the MSL server was not shut down cleanly before attempting an update, you may see an error message such as "One or more of the file systems for your Linux system was not unmounted cleanly". You will not be able to proceed with an upgrade. (You could proceed with a clean install but you would lose your configuration data.) If you want to upgrade and keep existing configuration data, terminate the current upgrade attempt, reboot the MSL server, and then shut it down cleanly. Proceed with the upgrade.

Upgrading with the Remote Fresh Install Blade

Physical servers running MSL 9.3 or 9.4 can upgrade to MSL 10 without the need for physical media or console access.

 **Note:** The RFI blade requires sufficient disk space for a backup. If your system has insufficient disk space, the blade will *not* be listed on the Blades panel.

To perform a remote fresh install:

1. Perform a backup through the server manager (this step is optional but recommended). See [Backup](#) on page 35.
2. In the server manager, under ServiceLink, click **Blades** and then click **Update List**.
3. Locate the **Remote Fresh Install** blade and click [Install](#) link beside it.
4. Accept the software license agreements when prompted.

The system automatically backs up the database, installs the software, and restores the database. After this process is complete, you are prompted to reboot the server.

5. In the server manager, under Administration, click **Shutdown or reconfigure**, select **Reboot** and then click **Perform**.
6. When the reboot is complete, log back in to the server console and confirm that the configuration data has been restored. If there is a problem, restore from the backup. See [Restore on an Operational System](#) on page 77.
7. Select the option to **Register for Service Link** to perform a sync with the AMC.
8. Reinstall your application software. See [Installing Software Blades](#) on page 28.

Upgrading from a Previous Version and adding RAID1

If you enabled software mirroring with a previous version of the software, you can upgrade without problems, provided an upgrade path is available. However, if you are upgrading a previous version of the software that was not installed with software mirroring, and you now want to use software mirroring, perform these steps:

- Perform a backup through the server manager.
- Install the second disk and perform a fresh install of MSL.
- Restore the backed up configuration through the server console.

Create Application Record

Create an Application Record for this MSL installation in your AMC license account. You will use the ID number of this Application Record to activate your MSL license. For information about creating Application Records, refer to the online help in your AMC account.


Obtain MSL Software

Before you can install MSL software, you must download the ISO image of the software from Mitel Online and then copy it to a CD-ROM or USB flash drive.

Download Image from Mitel Online

To download an ISO image of MSL software:

1. Log on to Mitel OnLine.
2. Move your pointer over **Support** and then click **Software Downloads**.
3. Click the name of the application software you want to install. The correct MSL load for your software is included on this page.

 **Note:** Make sure to download the correct MSL kernel version, either 32-bit or 64-bit. You cannot switch versions when performing a software upgrade or downgrade.

4. Click the [MSLx.x.x.iso](#) link.
5. Select a download method: **HTTP** or the **Software Download Manager**.
6. Select a location on your maintenance PC to store the downloaded software ISO images.

Copy Image to CD

To build a CD from the downloaded ISO image:

1. Insert a CD into the CD/DVD ROM drive of the maintenance PC.
2. Navigate to the stored MSL software ISO image and double-click the file. Your CD burner builds the CD.

Copy Image to USB


Use a USB storage device that is formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux).

WARNING: All existing data is erased from the USB drive when you copy an ISO image to it.

Linux Environment

To write the image from a Linux system to a USB flash drive:

1. Open a command prompt and execute the dd command.
 - Command structure: dd if=<source> of=<target>
 - Command example: dd if=msl-9.2.22.0.iso of=/dev/sda

 **Note:** Use the “enum_devices” command to determine the <target> block device of your USB flash drive. This command is available only with MSL, not with other versions of Linux.


Windows Environment

To write the image from a Windows system to a USB flash drive:

- Obtain a USB Image Tool (such as www.alexpage.de/usb-image-tool/) and use it to write the image to the USB flash drive.

Install MSL Software

The following procedure describes how to install MSL software to a workstation from a CD or USB flash drive. As part of this process, you are provided with the option to either erase all disks and perform a fresh install or upgrade the existing software.

 **Note:** If this configuration utilizes a hardware-based RAID 1, 5, or 10 solution, you must read your server vendor installation documentation and then complete the RAID configuration prior to installing MSL software.

CAUTION: The computer on which you install this software will be totally dedicated to being the server. The hard drive of this computer will be erased and re-written with the Linux operating system. This means that while this computer is acting as the server, you cannot use it for any other purpose.


Depending on which install option you select, the installation process may format and erase all attached hard drives. If you have multiple hard drives, be sure to back them up before starting the installation process.

The installation (or upgrade) process rewrites the boot sector on the hard drive. Machines with BIOS boot sector virus detection enabled may fail to boot unattended. This detection should be disabled in the system's BIOS.

To install MSL software on a workstation:

1. If you have a previous version of MSL, back up your configuration and data files using the Backup procedure. See [Performing Backup](#) page 74 for more information.
2. Configure your system to boot from either the CD/DVD ROM drive or the USB drive.
3. Insert the MSL software CD or USB drive you created in the [Obtain MSL Software](#) section.
4. Reboot the computer. The installation script runs automatically and the MSL Installer dialog appears.
5. Select a software installation package:
 - **SL** for a server installation.
 - **Rescue Mode** for a minimal server installation. This option provides a functional Linux environment that allows you to access the files stored on your hard drive even if you cannot run MSL. Select rescue mode only at the direction of Mitel Product Support.
6. Use the arrow keys to select the appropriate keyboard type and then select **OK**.
7. If you are installing from CD, you are prompted to test it. Click **OK** and then **Test** to test the media for validity and readability, or click **Skip** to proceed to the installation. The software installer runs.

MSL detects the installed hard drive(s). If multiple drives are found and they are not already configured in a hardware-based RAID 1, 5 or 10 array, MSL automatically configures them in an MSL software-based RAID 1 array.

-  **Note:** If MSL cannot detect any hard drives (typically because the server has SCSI or SAS hardware that is not compatible with MSL), an error message is displayed.
8. If you do not have a previous version of MSL software, you are offered an **Install** option. Click **Yes** and proceed to Step 9.
 9. If you have a previous version of MSL software, you are offered two choices:
 - **Erase all disks and perform a fresh install.** Select this option if you are performing a major upgrade (i.e. upgrading to Release 10.0 from a previous release), and then proceed to the next step. Because this erases your configuration settings, ensure that you have performed a backup as instructed in Step 1.
 - **Upgrade existing software:** Select this option if you wish to retain your configuration and application data, and then proceed to the next step.
 10. Choose your **Time Zone** from the list.
 11. If you selected **Erase all disks and perform a fresh install**, the screen displays a warning that your disks will be formatted and asks for confirmation. Click **Yes**.
 12. A log of the installation is created and stored in /root/install.log.
 13. Finishing the installation is automatic and takes only a few minutes. At the end of the process, you are prompted to remove the media and then reboot the system.

Configuring the Server

After the system has restarted and is no longer booting from the installation media, you are ready to log in and configure the system. If your ISP provided a summary of configuration choices and network information, refer to it while completing the screens in the configuration section of the server console.

The following steps walk you through the configuration settings as they appear on the screen. For more information about a particular step, refer to the Details section included with each step.

Restore from Backup?

- Click **No** if this is your initial installation of MSL software. Continue with the next configuration step “Set Administrator Password”.
- OR
- Click **Yes** to restore server configuration if you have a backup file and are installing MSL subsequent to an initial installation. You are then prompted to select the location of the backup file—a **network share**, **removable device**, or **another running server**. Once you have located the backup file, you can perform the restore and the MSL installation will be complete. See also [Restore Configuration Data](#) on page 76.

Set Administrator Password

- Enter the Administrator password and then re-enter it for confirmation.


The Administrator password (or System password) is used to access the server manager and the server console as the "admin" user and the Linux shell as the "root" user. Choose a secure, non-trivial password that is at least eight digits in length and contains a mix of numbers, upper and lower case letters, and punctuation characters.

After you have entered and confirmed the password, the MSL software examines the password for strength. If it is found to be weak, you are offered the chance to change it or continue.

Configure Domain Name

- Enter the primary domain name that will be associated with the MSL server. (Default is "mycompany.local".)

Enter the primary domain name that will be associated with this MSL server. This domain will be the default for the web-based server manager. The name must start with a letter and can contain letters, numbers, and hyphens. (For example, mitel.com.)

 **Note:** If you are using the MSL server as a DNS source, changing the domain name will require the server and all clients to reboot, and all references (such as bookmarks) that point to the server will require manual modification.

Configure System Name

- Enter a system name for the server (host name). Enter a unique system name for the server. The name must start with a letter and can contain letters, numbers, and hyphens (for example, Server-1).

Select Local Network Adapter

- Use the keyboard up/down arrows and the space bar to select the adapter(s) to configure as Local.

MSL automatically detects your system's Ethernet adapters and displays them so you can configure them as "Local Network (LAN)" adapters or, in a later step, as "WAN" adapters. In the initial screen, you can configure multiple LAN connections, each consisting of one or more adapters (multiple adapters are bonded together to present a virtual single interface). You must configure at least one LAN connection.

To configure multiple LAN adapters without bonding them, select only the first adapter on this initial screen. After you have configured your WAN connection (if required), you are offered the option of configuring any remaining adapters as LAN or bridged interfaces.

Notes:

- If your application is deployed in a server-gateway configuration, you need to configure at least one adapter as a WAN interface.
- If your application is deployed in a server-gateway with bridged interface configuration, you need to configure one adapter as a LAN interface, another as a


WAN interface, and a third as a bridged interface to the WAN interface of the firewall. For this setup, the server requires a minimum of three NICs.

Enter Local Networking Parameters

- Enter the local IP address for this server, or select from the default parameters provided. The address must be entered in IPv4 format.
- Enter the subnet mask for the local network, or accept the default.

These settings provide information about the internal network so that the server can communicate with other machines on the local network.

If the server is being installed into an existing network, choose an address that is not in use by any other computer on the network.

 **Note:** If you are installing servers at multiple sites within the organization, use different network addresses for each site. This simplifies later troubleshooting and VPN setups.


If the server will be operating in a server-only configuration, and there are other servers on the network, obtain an IP address that is unused in the local network. If your network uses a DHCP server, this address must also be outside of the scope of your DHCP pool.

Enable IPv6 Protocol

- Click **No** to limit the server to IPv4 addresses. Continue with the next configuration step “Select WAN Adapters”.

OR

- Click **Yes** to enable the server to be programmed with both IPv6 and IPv4 addresses. You are then prompted to enter an IPv6 address for the LAN interface.

 **Note:** If the LAN interface does not have an IPv6 address, this field can be left blank. However, some applications (such as MBG) require entry for IPv6 operation.

In addition to the LAN interface, you can configure IPv6 addresses for the WAN interface and gateway. This enables you to deploy MSL in a network environment that supports a mixture of IPv4 and IPv6 network protocols, and to access MSL via its IPv6 interfaces.

The following table lists the options supported by IPv6 in the current release:

Option	Notes
Server Manager access	Use https://<IPv6address>/server-manager.
System Monitor access	Use https://<IPv6address>/monitor.
LAN interface configuration	Support for one IPv6 address only (i.e. you cannot configure any additional LAN interfaces with an IPv6 address at this time). Bonding is supported.
WAN interface configuration	Support for one IPv6 static address. Bonding is supported. (DHCP/PPPoEwith IPv6 is not supported at this time.)
Local Networks	IPv6 network addresses are supported.
SSH access	IPv6 access supported.
Review Configuration	Displays IPv6 configuration.

Other options, such as backup/restore, remote management, MSL firewall, port forwarding, Email, DHCP, Hostnames and addresses, domains and SNMP, are not supported.

Select WAN Adapters

MSL automatically detects any remaining unconfigured Ethernet adapters and displays them here. If your server requires Internet access, you must configure a WAN (external) adapter. If you configure more than one adapter as "WAN", they will be bonded together to present a virtual single interface.

If your server will be operating in a server-only configuration, you don't need to configure a WAN adapter. Press the space bar to clear the selection and proceed to “Select Gateway IP Address”.

If you still have unconfigured adapters at this time, MSL prompts you to configure them as LAN or bridged interfaces. Press **Yes** to configure the remaining adapter(s) or press **No** to leave them unconfigured.

External Interface Configuration

If you have selected an adapter to act as a WAN interface, specify how the WAN adapter will be configured according to your connection setup:

Your setup:	Choose Option:
Cable Modem and your ISP has supplied an account name	1. Use DHCP and send account name.
Cable modem and your ISP has supplied an Ethernet address	2. Use DHCP and send Ethernet address.
Residential ADSL	3. Use PPP over Ethernet
You have a static IPv4 address. If the server supports IPv6, you may also have a static IPv6 address.	4. Use static IP address.


If you select Option 4:

- Enter the IPv4 address that this server will use to access the Internet.
- Enter the subnet mask.
- If prompted, enter the IPv6 address that this server will use to access the Internet.

Select Gateway IP Address

For Internet access:

- Enter your default gateway (router) IPv4 address.
- If prompted, enter your default gateway IPv6 address.

 **Note:** The option to select the Gateway IP Address does not appear if you have configured an external interface (WAN).

Select Additional Static IP Address

If you selected External Interface Configuration option 4 (static IP address), you are prompted to enter an additional IP address and subnet mask now. This option provides a second IP for those applications, like Mitel Collaboration Advanced, which require two different addresses on the same server.

Configure DNS

Select a DNS server option:

- To resolve all names locally, do not enter a Corporate DNS server address, and then click **Next**.
- OR—
- To resolve names using a mix of local and remote resources, enter the Corporate DNS server address, click **Next**, select **localhost**, and then click **Next**. The localhosts file will

resolve names for the local domain (the one configured on the MSL server) while the corporate DNS server will handle all other name resolutions.

—OR—

- To resolve names using only the corporate DNS server, enter the Corporate DNS server address, click **Next**, select **corporate**, and then click **Next**. The corporate DNS server will resolve names for all domains.

Although the MSL server contains a fully functional DNS server, if your network already contains a DNS server you should use it for name resolution.

If you enter a Corporate DNS server address, you must use the Domains panel of the server manager to configure the domain lookups that will be handled by the DNS server (see page 64 for more information).

You have now provided all information required for MSL configuration.

Activate/Reboot

When you have entered all configuration information, you are prompted to activate your changes. Click **Yes** to activate changes.

After activation, you are prompted to enter the **Application Record ID** number. You can enter it now to initiate registration of your licenses or you can bypass this screen and enter it via the server manager later. **Note:** Some applications must supply this number to acquire licenses from the AMC before they can be installed. (For example, NuPoint UM when installed as part of the Mitel Applications Suite.)

At the **Do you wish to install blades from CD-ROM?** prompt, check your application documentation for instructions:

- Click **Yes** to install application CDs. Your application documentation will supply instructions for this step.
- Click **No** to skip this step and complete the boot process.

Installing Software Blades

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

- Using a CD/DVD-ROM at the server console (for example, Mitel Applications Suite)
- Using a CD/DVD-ROM at the server manager Blades panel (for example, standalone NuPoint UM)
- Via the AMC (for example, standalone Mitel Border Gateway)

The documentation supplied with your software application contains installation instructions.

Server Administration and Maintenance


There are two ways to perform server administration, depending on the function you want to perform.

- **Server Manager:** a web-based control panel for performing such tasks as installing applications, configuring the server and its optional features, and managing available services.
- **Server Console:** a text-based control panel built into the MSL server and used for performing functions like reconfiguring network parameters (changing server configuration, for example), testing Internet access, and managing disk redundancy. (See page 71.)

Server Manager

The server manager is accessed using a web browser on the local network by visiting the URL: `http://<IP_address_of_MSL_server>/server-manager`.

Notes:

- Remote access to the server manager is only possible via an encrypted connection, using SSL (https).
 - By default, the server manager is accessible only from the local network. To extend access privileges to other networks, you must program them. Do this while you are physically connected to the local network. For details, see [Remote Management](#) on page 47 and [Local Networks](#) page 49.
 - You should allow access only from local and remote management networks, not from the public network (entire Internet). For details, see [SSH Settings](#) on page 47.
-  **TIP:** If you cannot see the MSL server manager login screen and you have set up Remote Access as instructed, you may need to check the security settings in Internet Explorer. MSL requires the Meta Refresh option to be enabled (default).

To check Meta Refresh:

1. In Internet Explorer, click **Tools > Internet Options**.
2. On the Security tab, click Custom Level...
3. Scroll down to the **Miscellaneous** section and ensure that **Allow META REFRESH** is enabled.
4. Click **OK** to exit.

When the page opens, enter the user name "admin" and the system password, then click **OK**. The server manager appears, as shown in Figure 5. Descriptions of each menu item follow the image.

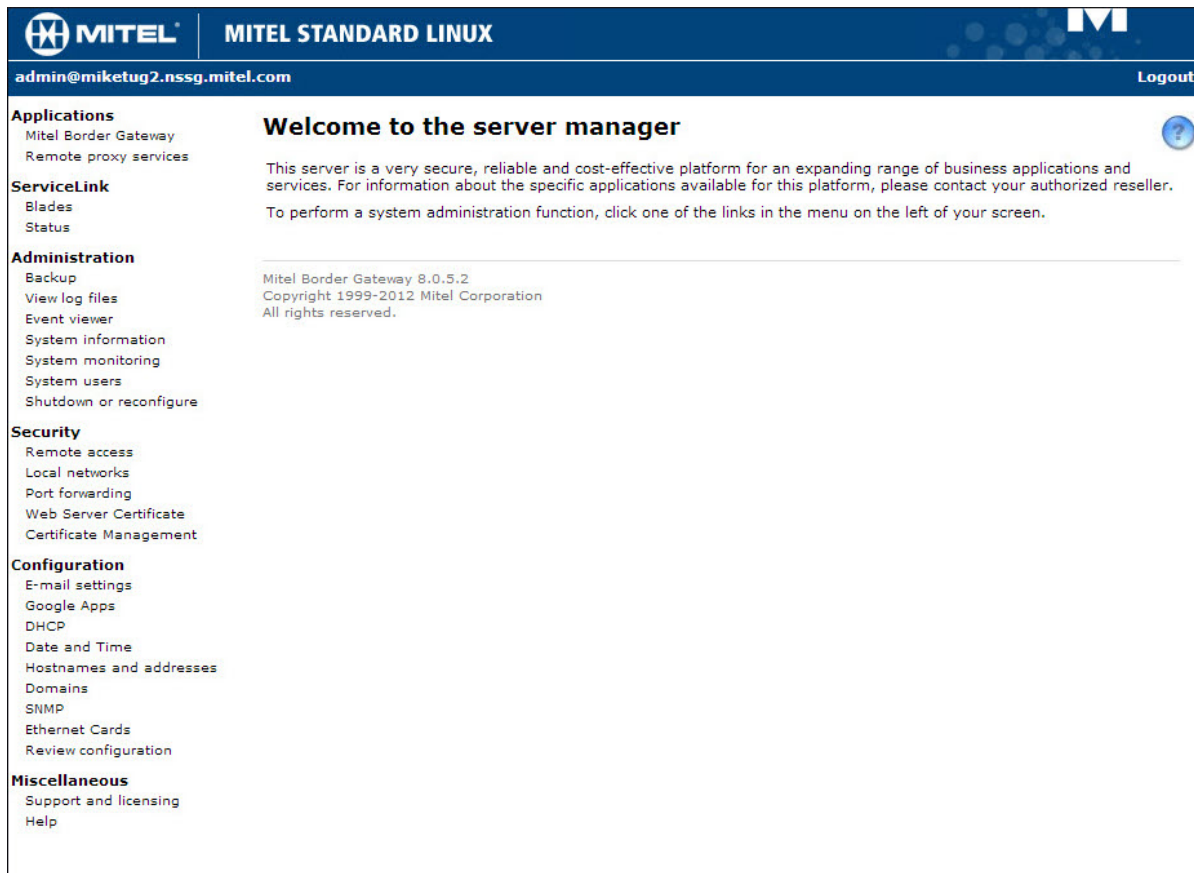


Figure 5. Server Manager

The Server Manager Menu

Section	Menu Item	Use this option to...	For more info, see page
ServiceLink	Blades	view current list of blades and install/cache/upgrade/remove links	31
	Status	view ServiceLink status for this server provided by the AMC	33
Administration	Backup	backup server configuration data (and application data)	35
	View log files	view or download log files generated by the services running on this server	35
	Event viewer	view the current alarm status of the system and a list of recent events	39
	System information	view (and control view access) of networking parameters, server, and domain information	41

Section	Menu Item	Use this option to...	For more info, see page
	System monitoring	view (and control view access) for system monitoring	41
	System users	add, edit, or delete user accounts for users who may access the MSL server	41
	Shutdown or reconfigure	reboot, reconfigure, or shutdown your system	43
Security	Remote Access	review and configure remote access settings (for example, PPTP and SSH)	46
	Local networks	grant local access privileges to other IPv4 and IPv6 networks	49
	Port forwarding	use to modify your firewall rules to provide port forwarding (For server-gateway configurations only.)	50
	Web Server Certificate	use to install third-party security certificate on server (example: certificate purchased from company like VeriSign), and to export the certificate and private key files for use on another server	51
	Certificate Management	Manage client certificate signing requests.	56
Configuration	Email Settings	configure SMTP settings	57
	DHCP	manage/configure the MSL DHCP server	58
	Date and Time	enable/configure network time server	60
	Hostnames and Addresses	view/add hostnames if using the MSL server as a DNS server.	62
	Domains	view/manage virtual domains and corporate DNS settings.	64
	SNMP	configure SNMP support for remote management/monitoring	66
	Ethernet Cards	configure the speed and duplex settings for the Network Interface Cards	68
	Review configuration	view networking parameters, server, and domain information	69
Miscellaneous	Support and licensing	view the MSL License Agreement (EULA)	-
	Help	access online help for MSL configuration	-

Blades

Software blades allow applications and services to run on MSL. For example, the Mitel Border Gateway blade allows your MSL server to run the MBG application (See Figure 6.)

You can use the Blades panel to install, upgrade or remove an application or service that is running on MSL, or to upgrade MSL itself.

You can download and install a software 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.

Note: Some applications may alter the behavior of the Blades panel. For example, Mitel Applications Suite software (Release 2.0 and later) uses the Blades panel as an information-only screen, displaying blade versions and the applications to which they belong. All installation and upgrades are performed using the [server console](#).



Figure 6. Blades Panel

For information about configuring and using application software blades, refer to the documentation for each application.

Install, Upgrade, Cache or Remove a Blade

To install/upgrade/cache/remove a blade:

1. In the server manager, under ServiceLink, click **Blades**. The currently cached list of blades is displayed.
2. Click **Update List** to ensure an up-to-date listing. (Note: If the AMC sync process is disabled, the blades list will not be refreshed. The listing will show only installed blades, blades from CD, and entries from the last sync.)
3. 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](#) or [Upgrade](#) link.
 - To upgrade a blade, click the [Upgrade](#) link beside it.
 - To delete a blade, click the [Delete](#) link beside it.

Each software blade modifies the server manager navigation menu to allow you access to application configuration pages. For details, consult the documentation provided with each application blade.

 **Notes:**

- You can also install blades from a CD. If you have an application distributed in this way, insert the CD before loading the blades panel, or click Update List after inserting the CD.
- If the blade does not have an upgrade link, then you are already running the latest software version or the application does not support ServiceLink upgrades.

Upgrade the MSL Blade

To upgrade MSL:

1. In the server manager, under ServiceLink, click **Blades**.
2. Click **Update List** to ensure an up-to-date listing. Newer MSL versions are listed as ServiceLink blades and include an Upgrade link.
3. Do one of the following for the MSL version you want to install:
 - To download the blade for installation at a later time, click the Cache link beside it. Complete the process by clicking the Upgrade link.
 - To upgrade a blade immediately, click the Upgrade link beside it.

 **Notes:**

- If Mitel Standard Linux does not have an upgrade link, then you are already running the latest software version.
- If you previously used the CD upgrade method to upgrade the server, you may experience difficulty when using ServiceLink to upgrade to a later release due to accumulated driver modules. To avoid a “hang” condition during the upgrade, do the following:
 - Log in to the server as “root.”
 - At the Linux prompt, type **rpm -qa | grep kmod-gfs**. MSL displays all the driver module versions. Example output:

```
kmod-gfs-PAE-0.1.34-2.e15
kmod-gfs-PAE-0.1.31-3.e15
```
 - If there are multiple modules, delete all of them except the most recent one (the first module listed) using the **rpm -e** command. Example input:
rpm -e kmod-gfs-PAE-0.1.31-3.e15
 - You may now upgrade MSL by accessing the Blades panel and clicking the upgrade link.

Status


This panel provides updated ServiceLink status information for this server. Status information is downloaded from the Applications Management Center (AMC) 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**.
4. If the Internet is accessed via a proxy, enter:
 - Address of proxy
 - TCP port used to connect to proxy

 **Note:** 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.

5. Click **Activate**.


Once ServiceLink is activated, the message, “sync completed successfully” is displayed.

 The system automatically resynchronizes with the AMC on a regular basis. If this process fails, a Major alarm is generated. To clear the alarm, you must successfully synchronize with the AMC.

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. See [Offline Sync with the AMC](#) on page 73 for details.

 When an offline system is upgraded to MSL 9.3 or later, it will receive a Major alarm indicating that the automatic 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:

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. 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.

 **Note:** If at a later time you wish to use online activation, click **Status** under **ServiceLink** and then click **Disable offline license generation**. Then see [Online Activation](#) on page 34.

Deactivation

In case of hardware replacement, you need to deactivate ServiceLink.

 **Note:** You will need to reset your hardware ID and re-enter your Application Record ID before you can re-activate.

To deactivate ServiceLink:

1. Under ServiceLink, click **Status**.
2. Click the [here](#) link to access the deactivation screen.
3. Click **Deactivate**.

Backup

There are two methods for backing up system data:

- The server manager offers the **Backup** option to back up data to a local workstation, or to configure and/or schedule backups to a Microsoft or Linux network file server.
- The server console provides the **Perform Backup** option to back up to a USB device or to a Microsoft or Linux network file server – see [Perform Backup](#) on page 74 for more information on the server console option.

Backup to Desktop Option

To back up system and application data to a local workstation:

1. Under Administration, click **Backup**.
2. Select the **Backup to desktop** option and then click **Perform**. MSL prepares the system for backup.
3. The Backup to desktop screen is displayed with your estimated backup size. Ensure that your browser and target file system support downloads of this size and then click **Begin Download**.
4. When prompted to Open or Save, click **Save**.
5. In the file download window that appears, name the file, select the location on the desktop where the file will be saved and then click **Save**. A confirmation message is displayed. After saving, you can copy the backup file to a CD or USB storage device, if required. (CD or USB storage is required for future restore operations.)

 **Notes:**

- "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 FAT file system (the default for many older versions of Windows), you are limited to a maximum file size of 2 GB; Internet Explorer 6 and 7 are limited to 4GB file size. 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 will not 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.
- Do not click Back on the browser when a backup is in progress. Doing so will not terminate the backup, and the system will be unable to inform you when the action is complete.

Configure Backup to Network File Server Option

Use this option to configure/schedule your system backup to Network File Server. Two file-sharing protocols are supported:

- SMB/CIF for Windows servers
- SFTP for Linux servers (including MSL)


 **Notes:**

- You can only have one backup scheduled on the server. To cancel an existing backup schedule, select **Never** and then click **Update**.
- If you are backing up to an MSL server, configure it to accept access from the backup server. See [Local Networks](#) for details.
- To restore an SFTP backup, you must copy it to a removeable device such as USB key, and then select the [Restore from Backup](#) option from the Server Console.


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. Configure the server where the backup file will be stored.

 **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.

- Enter the **IP address** of the file server where the backup will be stored.
- Enter the **Username** to use when connecting to the backup server.
- Enter the **Password** to use when connecting to the backup server. Available storage space is displayed.
- Enter the **Domain** or **Workgroup** name of the server. (For example, mitel.com.)
- Enter the **Sharename** of the shared folder where the backup file will be stored. (For example, "Backups".) The shared folder must have permissions set to "Full Control".

 **Note:** If a sharename is entered, the backup utility will first try to connect to the server/shared folder as an SMB/CIFS resource. If the connection fails, it will then try to connect using SFTP.

- Enter the **(Optional) Sub Directory** where the backup will be stored. If you leave this field blank, the file will be stored at the root of the shared folder. Spaces and multi-level directory names are permitted; for example, "MSL backup" and "MSL backup/2011/October" are valid sub directory names. Dashes (-) are not permitted.
5. Select the **Maximum number of backup files to keep** (1-999) on the server (default is 5). When the number of stored files reaches this maximum count, the oldest version is deleted.
 6. Select the frequency with which you want to perform backups (Daily, Weekly, Monthly, Never). Backup file names will include timestamps in the format: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz
 - To disable regularly scheduled backups, click **Disabled**.
 - 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 the month
 - For **immediate** backup file creation, proceed to the next step.
 7. To test your backup configuration, or to run an immediate backup, click **Backup Now**.

 **Note:** The Backup Now button displays only if you have entered a valid configuration.

8. Click **Save** to save the schedule information.


If the scheduled backup fails, an alarm is raised and can be seen in the [Event Viewer](#) panel.

View Log Files

The messages log file is where most of the system services write log messages. You can view log files to assist in troubleshooting.

To view log files:

1. In the server manager under Administration, click **View Log Files**.
2. Select a log from the dropdown list (for example "messages"). With no filter options entered, you will see the entire log file.

View log files 

This panel allows you to view or download the log files generated by the services running on your server.

Choose a log file to view

You may optionally specify a filter pattern to display only the lines from the log file which match this pattern. If you leave this field blank, all available lines of the log file will be displayed. Note that this option is not used if you download the logfile.

Filter Pattern (optional) **Regular Expression**

You may also optionally specify a highlight pattern to mark in bold any lines from the log file which match the highlight pattern. The highlight pattern is applied to any lines which have already matched the filter pattern. Note that this option is not used if you download the logfile.

Highlight Pattern (optional) **Regular Expression**

You must choose between viewing the logfile in your browser, or downloading the logfile to your computer. If the logfile is particularly large, you may wish to download it instead of attempting to open it in your browser, as this is a problem for some web browsers.

Operation

Next

Figure 7. View Log Files

1. Enter text in the **Filter Pattern** box to view only the lines of the log file containing that text. Check the **Regular expression** box if you want to apply the filter in the format of a regular expression.
2. Enter text in the **Highlight Pattern** box to view the lines of the log file containing that text displayed in bold type. Check the **Regular expression** box if you want to apply the filter in the format of a regular expression.


 **Note:**

- The two filter options can be used together.
 - The filters are case sensitive.
 - The filters are not applied when you Download the log file.
 - A regular expression 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. See [Event Viewer](#) on page 39 for details and examples.
 - The system automatically updates the list every 5 seconds with any new logs.
3. From the Operation list, select **View** or **Download** and click **Next**.

Collect Logs 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. In the server manager 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.
 3. Click **Start**. A progress indicator appears while the logs are being collected.
-  **Note:** The log collection process can take a few minutes. 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 a file, click **Save** (or respond to the prompt), navigate to the location you wish to store the file, and then click **Save**. A tar file with the filename "sosreport-<file>-tar.bz2" is saved to the specified 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.

 **Notes:**

- 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`.

Event Viewer

MSL monitors system status every 60 seconds and stores the information in a log file. Some applications, like Mitel Border Gateway, allow you to view events from the past hour, 24 hours, or 7 days. For detailed information about log information, refer to the MSL online help. The alarm states are:

- Cleared (green): No alarms have been raised since the alarms were last cleared.
- Minor (yellow): Indicates a fault which affects service to a user or users. This may result in a major degradation in service and requires attention to minimize customer complaints.
- Major (orange): Indicates a fault which will cause a major degradation in service and requires attention as soon as possible.
- Critical (red): Indicates a total loss of service which demands immediate attention.
- Warning (blue): Indicates an "information only" alarm.

 **Notes:**

- Some applications do not support Event Viewer.
- Some deployments may display a Critical alarm after initial installation. Follow the instructions below to clear the alarm.

View Application Event Logs

To view application event logs:

1. 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 set automatically by the system. To set 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 alarm **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.

Regular expression examples:


/a/ Exact match of the character "a".

/^a/ Exact match of the character "a" at the beginning of a line.

/a\$/ Exact match of the character "a" at the end of a line.

./a/ Match any character that precedes the character "a" (wildcard).

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.
8. Check 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.
10. Click **Clear alarms** to clear the alarms.

 **Note:** Severity of "Indeterminate" indicates an "information only" alarm.

Clear Alarms

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

System Information

To view the system information page:


- Under Administration, select **System Information** to view System Vital, Network Usage, Memory Usage, Mounted Filesystem, and Hardware Information.

System Monitoring

Viewing monitoring graphs can help you analyze the system's performance.

To enable access to the System Monitor display:

1. Under Administration, select **System monitoring**.
2. In the **Access to system monitor display list**, select one of the following to enable System Monitoring:
 - **Private** – allows access to your private network including networks that you have configured in the “Remote Access” panel
 - **Public** – allows access from anywhere
 - **Disabled** – to disable access
3. Click **Save** to save your selection.
4. Click **System monitor display** to view system information graphs. Click on the graphs for more detailed system information.

 **Note:** Traffic Analysis graphs are available only if SNMP is enabled.

To view the System Monitor display in the server manager:

1. Under Administration, click **System monitor**.
2. Click **System Monitor Display**. Your system graphs appear. Click any graph for detailed information.

To view the System Monitor display in a web browser:

1. Open a web browser on the local network (if private access is enabled) or the Internet (if public access is enabled).
2. Enter the system monitor URL: `https://<IP_address_of MSL server>/monitor/`

System Users

You can add, modify, lock, or remove user accounts for 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.



Figure 8. System Users

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. (Optional) Update the directory information (**Department**, **Company**, etc.).
5. Set **VPN Client Access** to **Yes**.
6. (Optional) Select **Group memberships**.
7. Click **Add**.
8. Click **Reset Password** and reset the password for the account. Passwords must be at least 7 characters long and must contain:
 - upper case letter
 - lower case letter
 - number
 - non-alphanumeric character
9. 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.

Disabling User Accounts

When an account is disabled, the user will no longer be able to access server resources such as the VPN. To re-enable the user account, reset the password using the [Reset password](#) link in the System Users panel.

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.

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

Digital VPN Certificates for System Users

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 **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

Setting up a VPN connection on the user's computer is a two-step process. First you create the VPN connection, then you configure it with the digital certificate.

 **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**.

Shutdown or Reconfigure

If you need to shut down or reboot the server, use the **Shutdown or reconfigure** panel to ensure that the shutdown sequence occurs gracefully, preserving all configuration and information on the server.

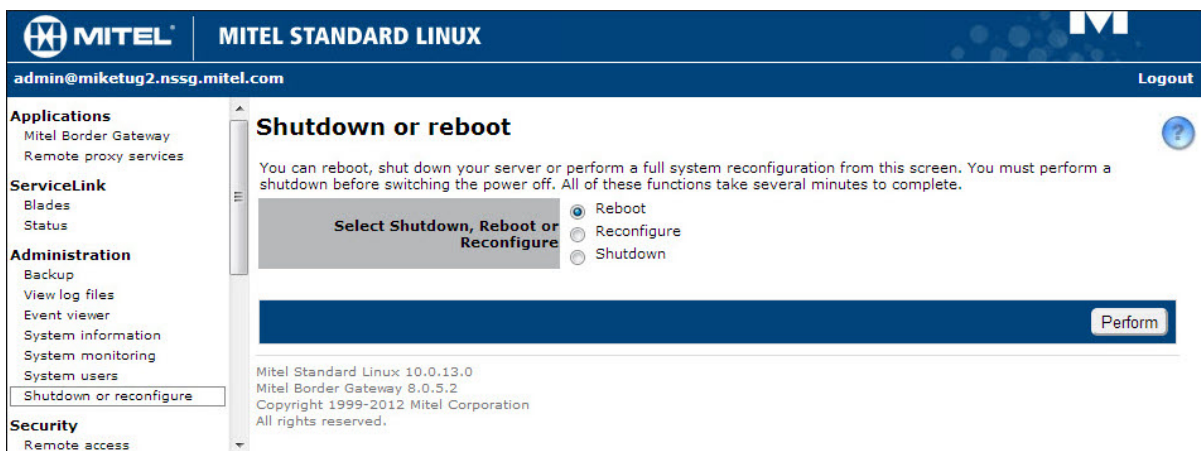


Figure 9. Shutdown or reconfigure

- **Reboot:** reboots the server after graceful shutdown.
- **Reconfigure:** reaffirms all settings (forced reset – may be requested by Product Support).
- **Shutdown:** turns off the server for service outage or scheduled down time.

Click **Perform** and then confirm your selection. Click **Yes** to initiate the action or click **No** to return to cancel the action.

Remote Access

MSL provides several ways to access the underlying operating system, 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. All of these operations are configured using the Remote Access panel in the server manager.

Change remote access settings

PPTP Settings
 You can allow PPTP access to your server. You should leave this feature disabled by setting the value to the number 0 unless you require PPTP access.

Number of PPTP clients

Remote Management
 It is possible to allow hosts on remote networks to access the server manager or login via secure shell by entering those networks here. Use a subnet mask of 255.255.255.255 to limit the access to the specified host. Any hosts within the specified range will be able to access the server manager using HTTPS. To allow secure shell access from hosts in the specified range you must also configure the Secure Shell Settings accordingly.

Network	Subnet mask	Number of hosts	Remove
0.0.0.0	0.0.0.0	4294967296	<input type="checkbox"/>

To add a new remote management network, enter the details below.

Network

Subnet mask

Secure Shell Settings
 You can control Secure Shell 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.

Secure shell access

Allow administrative command line access over secure shell

Allow secure shell access using standard passwords

Mitel Border Gateway 8.0.5.2
 Copyright 1999-2012 Mitel Corporation
 All rights reserved.

Figure 10. Remote Access

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 [DHCP](#) on page 58.


To enable VPN access:

16. Under **PPTP Settings** in the Remote Access panel, enter the **Number of 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 here. Enter 0 to deny PPTP connections.
17. Click **Save**. The server is now ready to accept PPTP.

To connect using PPTP:

1. Install the protocol on each remote Windows client - Click Network Control Panel (you may need to have the original Windows installation CD available). Client PCs should be rebooted if prompted.
2. Create new connections - In the Dial-Up Networking panel, enter the external IP address of the server to which you want to connect.

When you are finished, initiate a PPTP connection by double-clicking the appropriate icon in **the Dial-Up Networking** window. When you open the Network Neighborhood window, the server workgroup is listed there.

 **Note:** Establish the connection to the Internet before you initiate the PPTP connection. This may involve double-clicking one **Dial-Up Networking** icon to start the Internet connection, then double-clicking a second icon to start the PPTP connection. To shut down, disconnect the PPTP connection first, then disconnect from the ISP.

WARNING: To protect the network, MSL enforces the use of 128-bit encryption for PPTP connections. If you are unable to establish a PPTP connection to the server, visit <http://windowsupdate.microsoft.com/> and download the appropriate update. The contents of the page will appear differently depending upon the version of Windows you are using. You may need to search for Virtual Private Networking or a Dial Up Networking 128-bit encryption update. You may need to install the 40-bit encryption update first, and then install the 128-bit encryption update. Note that with Microsoft's ActiveUpdate process, if you are not presented with the choice for this update, it may already be installed in your system.

Remote Management

- Enter the Network IP address and subnet mask to enable remote management.

Remote management allows hosts on the specified remote 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. (Using 255.255.255.255 allows access from a specific host or limits access to a specific host.) If your mask allows a range of IP addresses, any hosts within that range can access your server manager using HTTPS. (See also [Local Networks](#).)

Secure Shell Settings

Use the Secure Shell Settings section to control SSH access to your server.

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.


About SSH (Secure Shell)

SSH (secure shell) provides a secure, encrypted way to log in to a remote machine across a 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 provides 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 MSL, 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 the Secure Shell Settings:

1. Select an access option:
 - **No Access** – (Default) SSH access not allowed.
 - **Allow access only from local and remote management networks** – This 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 enables you to access the server from anywhere on the Internet. Employ a strong SSH password with this option in order to enhance security.


 **Note:** 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.

2. Program the configuration options:
 - **Allow administrative command line access over secure shell** - This allows someone to connect to the server and log in as "root" with the administrative password. The user has 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 to **No**.
 - **Allow secure shell access using standard passwords** - If you choose **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 the copying of an SSH key from the client to the server.
3. Click **Save**.

Using an SSH Client

Once SSH is enabled, you can 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. The interface opens in the server console. From here you can change the server configuration, access the server manager 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 server manager) 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.

Local Networks

When you configured the server, you provided it with the information to deduce its own local network and identify machines on this network as being eligible for access to its services. You can also allow other networks to access your server as if they were a local network. As with [Remote Management](#), they receive server manager access, but as a Local Network, they can also access other MSL services like SNMP and System Monitoring.


If the MSL server is being deployed on a simple network with only one subnet, you do not need to enter any additional information here.

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.

 **Note:** You can also use the [server console](#) to show, add, and delete local networks.

To extend privileges to one or more additional networks:

1. For an IPv4-only server, click **Add network**.
—or—
For an IPv6-enabled server, click **Add IPv4 network** or **Add IPv6 network**.
2. In the **Network Address** field, enter the IPv4 or IPv6 address of the network to designate as "local".
3. In the **Subnet Mask** field (IPv4 only), enter the mask to apply to the Network Address.
4. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
5. Click **Add**.

 **Note:** When you add or change Local Network information, updates to permissions files may take up to 15 seconds. When a newly-added local network attempts a connection before permissions have been updated, it receives a "403: Forbidden" error message.

Depending on the architecture of the network infrastructure, the instructions for configuring the client machines on an additional network may be different than the instructions outlined in this handbook. For more information about adding another network, contact your Mitel authorized reseller.

Port Forwarding

Port Forwarding allows you to modify your firewall rules so that the port you select 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.

WARNING: Misuse of this feature can compromise the security of your network.

To create a port forwarding rule:

1. Under Security, click **Port forwarding**. A list of your current forwarding rules appears.
2. Click **Create Portforwarding rule**.
3. In the **Protocol** field, select the traffic to which you want to apply the rule (TCP or UDP).
4. In the **Source Port** field, enter the number of the port that is to be forwarded.
5. In the **Destination Host IP Address**, enter the IP address of the machine to which the traffic from the Source Port is to be forwarded.
6. In the **Destination Port** field, enter the port on the Destination Host to which the traffic is to be forwarded.
7. Click **Next**.
8. To confirm your port forwarding configuration, click **Add**.

To remove a port forwarding rule, select the appropriate line in the rule table and click the **Remove** link.

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

Web Server Certificates

About SSL Certificates

An SSL certificate is a digital certificate that authenticates the identity of a web site and encrypts information sent to the server from client stations using Secure Sockets Layer (SSL) technology.

The screenshot shows the 'Manage Web Server Certificate' page in the Mitel Standard Linux web interface. The page is titled 'Manage Web Server Certificate' and displays the following information:

The following web server certificate is currently installed:

Issuer:	miketug2.nssg.mitel.com
Certificate Name:	miketug2.nssg.mitel.com
Alternate Name(s):	*.nssg.mitel.com 10.38.200.253 miketug2 miketug2.nssg.mitel.com nssg.mitel.com
Valid From:	Jul 31 16:30:13 2012 GMT
Expires:	Jul 29 16:30:13 2022 GMT

If you would like to install a web server certificate that is issued by a third-party Certificate Authority (CA), you must first generate a Certificate Signing Request (CSR) which you can then send to the Certificate Authority.

Once the Certificate Authority has issued you a web server certificate, you can upload it using the 'Upload and install' option below. This option may also be used if you want to import a private key and web server certificate from a different server.

To download the currently installed web server certificate and private key, select the 'Download' option below. The resulting file will be a ZIP file containing the private key, the current web server certificate, and an intermediate certificate if one is installed.

Select operation to perform:

- Generate a new Certificate Signing Request (CSR)
- Upload and install a web server certificate
- Download the current web server certificate

Perform

Mitel Standard Linux 10.0.13.0
Mitel Border Gateway 8.0.5.2
Copyright 1999-2012 Mitel Corporation
All rights reserved.

Figure 11. Web Server Certificate

A default self-signed SSL certificate is provided with the server. When you first log in to the server manager, a Security Alert warning dialog is displayed that asks you to accept the server as a trusted web site. To proceed with the log in, you must accept the default self-signed certificate that is assigned to the server.

You can prevent this Security Alert warning from appearing by doing one of the following:

- by purchasing a Secure Sockets Layer (SSL) certificate from a third-party Certificate Authority and then importing the certificate and, if necessary, the private keys into the server.

OR

- by installing the default self-signed certificate locally on your workstation.

Using Third-Party SSL Certificates

To prevent the "Certificate Error: Navigation Blocked" page from appearing on client stations on the local network, purchase a Secure Sockets Layer (SSL) certificate for the MSL server and then import it onto the MSL server.

If your MSL server is deployed in a server-only (LAN) configuration with an MBG Web Proxy Server in the demilitarized zone (DMZ), the remote clients connect through the Web Proxy to the MSL server on the LAN. To prevent the "Certificate Error: Navigation Blocked" page warning from appearing on these remote client stations, purchase a Secure Sockets Layer (SSL) certificate for the MBG Web Proxy server and then import it onto the MBG Web Proxy server. **Note:** This configuration will always require a trusted certificate to prevent web browser security alerts for remote Internet users.


Currently Installed Web Server Certificate

If a certificate is currently installed on the server, the details are listed as follows:

Field Name	Details
Issuer	<p>Lists the following information for the certificate authorization company that issued the certificate:</p> <p>C: country code (2-letter ISO country code)</p> <p>ST: state or province</p> <p>L: locality name (for example: city name)</p> <p>O: name of the certificate authorization authority; "XYZ Corporation" is the name that appears for Mitel self-signed certificates.</p> <p>OU: name of the organizational unit</p> <p>CN: server hostname</p> <p>Authority/emailAddress: email address of the Certificate Authority</p>
Subject	<p>Lists the following information for the certificate holder:</p> <p>C: country code (2-letter ISO country code)</p> <p>ST: state or province</p> <p>L: locality (for example, city name)</p> <p>O: organization name (your company name)</p> <p>OU: organizational unit (for example, department name)</p> <p>CN: MSL server hostname</p>
Not before	Date and time when the certificate takes effect.
Not after	Date and time when the certificate expires.


Generating a Certificate Signing Request

You need a certificate signing request (CSR) in order to obtain an SSL certificate from a Certificate Authority (CA). The CSR can be generated locally or on a different computer.

 **Note:** If you generate the CSR on a different server, you must obtain the private key file from that machine and import it to the local MSL server. For instructions on how to obtain the private key file from an MSL server, refer to [Downloading Certificates](#) on page 55.

To generate a CSR:

1. Under **Security**, click **Web Server Certificate**.
2. Select **Generate a new Certificate Signing Request (CSR)**, and then click **Perform**.
3. Enter the information required to generate a certificate signing request (CSR). If you have previously generated a CSR, the previously entered values are displayed. Beginning with Release 9.1.24, CSRs are generated with 2048-bit keys.

 **Note:** When completing the fields, capitalize the first letter only (for example Ontario, not ONTARIO).

Field Name	Enter
Country Name (2 letter code)	2 letter code of your country
State or Province Name	full name of your state or province
Locality Name	name of your city, town, or village
Organization Name	name of your company
Organizational Unit Name	organization unit or department name
Common Name	fully-qualified hostname of your server including the domain name (for example, msl.mitel.com); wild cards are permitted (for example, *.mitel.com)
Subject Alternate Name (virtual host in LAN)	<p>This information needs to be entered in the CA web form. If requesting a certificate for Web Proxy in the DMZ, this entry is the FQDN of the MSL server in the LAN. If requesting a certificate for the MSL server in the LAN, this entry is the MSL server IP address.</p> <p>Note: If the trusted certificate does not have a Subject Alternate Name equal to the LAN server FQDN, remote web browser access to the LAN server will generate Security Alerts because the certificate does not include name of the server used in the URL. If the trusted certificate does not have a Subject Alternate Name equal to the LAN server IP address, local web browser access to the LAN server with that IP address will generate Security Alerts because the certificate does not include the IP address used in the URL.</p> <p>If one Web Proxy in the DMZ is going to proxy for several MSL servers in the LAN, the trusted certificate in the web proxy needs to have a Subject Alternate Name for each MSL server.</p> <p>Certificate Authorities will contact the administrator of the domain listed in a CSR. The information used by the organization to register an internet FQDN will be used to contact the organization.</p>

1. 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.
2. Click **Generate Certificate Signing Request**. The system generates a CSR file.
3. Copy the text of the CSR file.
4. Access the web site of a Certificate Authority company (for example, VeriSign) and purchase a certificate. During the transaction process, you will be prompted to provide your CSR file. You will also be required to enter a **Subject Alternate Name** (virtual host in LAN) in the CA web form.
 - If requesting a certificate for Web Proxy in the DMZ, this entry is the FQDN of the MSL server in the LAN. If the trusted certificate does not have a Subject Alternate Name equal to the LAN server FQDN, remote web browser access to the LAN server will generate Security Alerts because the certificate does not include the name of the server used in the URL.
 - If requesting a certificate for an MSL server in the LAN, this entry is the MSL server IP address. If the trusted certificate does not have a Subject Alternate Name equal to MSL server IP address, local web browser access to the MSL server in the LAN with that IP address will generate Security Alerts because the certificate does not include the IP address used in the URL.

 **Notes:**

- If one Web Proxy in the DMZ is going to proxy for several MSL servers in the LAN, the trusted certificate in the web proxy needs to have a Subject Alternate Name for each MSL server.
 - Certificate Authorities will contact the administrator for the domain used in a CSR. The information used by the organization to register an internet FQDN will be used to contact the organization.
5. Paste the text of your CSR file into the designated box.

After you complete the transaction, the Certificate Authority sends you an SSL certificate. (They may also send an intermediate certificate.)

6. Upload the SSL certificate to a location that is accessible to the MSL server.

Installing a Third-Party Certificate

You can purchase a web server certificate from a third-party Certificate Authority (CA) and then install it on the server. After you install the certificate, the Security Alert warnings no longer appear because the server portals will be identified as trusted web sites by the Certificate Authority.

1. Under **Security**, click **Web Server Certificate**.
2. Select **Upload and install a web server certificate**, and then click **Perform**.
3. Select the SSL certificate:
 - Beside the SSL Certificate field, click Browse.
 - Navigate to the SSL certificate, select it and click Open.
4. 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.
5. If the CSR was created on a different server, import its private key pair:
 - Beside the **SSL Private Key** field, click **Browse**.
 - Navigate to the SSL Private Key file, select it and click **Open**.
 6. Click **Install Web Server Certificate**.

Verifying the Installed Certificate

To download the installed certificate:

1. In the Server Manager, under **Security**, click **Web Server Certificate**.
2. Verify that the certificate name and issuer are displayed on the page.

Downloading the Installed Certificate

Use this procedure to download the web server certificate, the intermediate certificate (if installed), and the private key file that corresponds to the current SSL server certificate. The downloaded file is in ZIP format.

To download the installed certificate:

1. In the Server Manager, under **Security**, click **Web Server Certificate**.
2. Select **Download the current web server certificate**, and then click **Perform**.
3. Click **Save**, navigate to the location you wish to store the file, and then click **Save**.

The downloaded file is in ZIP format. After unzipping the file, you can upload the contents (certificates and private key files) to another MSL server.

Installing the Default Self-Signed Certificate on Local Workstation

The advantage of using the default self-signed certificate is that there is no additional cost; however, all users must install the certificate locally on their workstations to prevent the Security Alert warnings from appearing. The level of protection supplied by this method is somewhat lower than that of the purchased certificate.

The following procedure describes how to install the self-signed certificate on a workstation that is running Internet Explorer 8 on Windows XP. For other versions of Internet Explorer and/or Windows operating system, see "Certificate Errors" in the Internet Explorer help.

1. When you attempt to access the MSL login page, a "Certificate Error: Navigation Blocked" page is displayed. The warning states "There is a problem with this web site's security certificate".
2. Click the "Continue to this website" link to proceed to the MSL login page.
3. In the Internet Explorer command bar, click **View**, and then click **Security Report**. An "Untrusted Certificate" error dialog opens.
4. Click **View Certificates**.

5. Click **Install Certificate**.
6. Click **Next** to navigate through the **Certificate Import Wizard** windows.
7. Accept the default, "Automatically select the certificate store based on the type of certificate," and click **Next**.
8. Click **Finish** on the Completing the Certificate Import Wizard window.
9. Click **Yes** on the Root Certificate Store window to add the certificate to the Root Store.
10. Click **OK** to close each window you have opened during this procedure.

Client Certificate Management

To securely authenticate client connections, some applications may request a security certificate signed by the MSL server using a Mitel Certificate Authority (CA). You can manage Certificate Signing Requests (CSRs) and issued certificates using the Certificate Management panel.

The screenshot shows the 'Manage Certificates' interface. On the left is a sidebar with categories: Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area has the following sections:

- Manage Certificates**: Introduction text and a help icon.
- CA Signing Certificate Details**:

Issuer	Issuer: C=CA, ST=ON, O=Mitel Networks, OU=VoIP, CN=Mitel 6000 CA/emailAddress=security@Mitel.com
Subject	Subject: CN=ServiceLink Account ID: 45415305/emailAddress=admin@miketug2.nssg.mitel.com, O=XYZ Corporation
Not before	Jul 31 16:34:31 2012 GMT
Not after	Jul 29 16:34:31 2022 GMT
- Queued CSRs**: States 'There are no pending CSRs in the queue at this time.'
- Approved Certificates**:

Certificate ID	Subject
5006988a-207a-4b9a-abe4-fdfc64cfb082	CN=MBG:miketug2.nssg.mitel.com_1, CN=IP:10.38.200.253
- Revoked Certificates**: States 'There are no revoked certificates at this time.'

At the bottom, it says 'All rights reserved.' and '1'.


Figure 12. Certificate Management

To approve a CSR:

1. Under **Security**, click **Certificate Management**. Certificate requests waiting for approval appear under the heading **Queued CSRs**.
2. Click the **Certificate ID** link.
3. After confirming the requester, do one of the following:

- Click **Cancel** to return to the Certificate Management main screen without approving/rejecting the request
- Click **Reject** to reject the CSR. The requester will be notified of the rejection
- Click **Approve** to approve the CSR

To revoke an approved CSR:

Generated certificate numbers are unique. If you need to re-issue a certificate for a specific requester (for example, in the case of hardware failure or theft), then you must first revoke the existing certificate.  **Note:** Do not use this option to disable a set.

1. Under **Security**, click **Certificate Management**. Approved CSRs appear under the heading Approved Certificates.
2. Click the **Certificate ID** link and then click **Revoke**. The requester can now make another request.

 **Note:** The MSL server is limited to accepting 50 concurrent CSRs.

Email Settings


To configure email settings:

1. Click the **Change** button beside the setting you want to change.
2. Configure one or more of the following settings and then click **Save**:
 - **SMTP Server:**
 - **Server to use for outbound SMTP:** The server can deliver outgoing messages via a corporate or Internet service provider's SMTP server, or can deliver messages directly to their destination by looking up mail exchanger records in DNS. If you are using a specific SMTP server, specify its hostname or IP address in this field. Otherwise, leave this field blank. Click **Save** to access other SMTP Server settings.
 - **Destination Port for Outbound SMTP:** If you have specified a Server to use for outbound SMTP, select one of the following:
SMTP Port 25 (use cleartext; default)
SMTP port 587 (TLS encryption)
SMTP Port 465 (SSL encryption).
 - **Mail Server User ID:** If you are using secure SMTP (port 465 or 587), enter the user ID required by the SMTP server. This ID must be configured and licensed in the SMTP server.
 - **Mail Server Password:** If you are using secure SMTP (port 465 or 587), enter the password required by the SMTP server. This password must be configured in the SMTP server.
 - **SMTP email injection restrictions:** This setting controls which networks will be allowed to send mail through this server via SMTP. Choose from one of the following three settings:
 - **Localhost only** – accept email only from applications installed on the server (default setting).

- **Accept only from local networks** – accept email from 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 email.
- **Forwarding address for administrative email:** By default, email 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 email address in this field.
- **E-mail sent for events:** Select the system events for which you want to receive email notifications — Cleared, Indeterminate, Warning, Minor, Major, Critical. By default, Major and Critical are preselected.

DHCP

Use the 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.

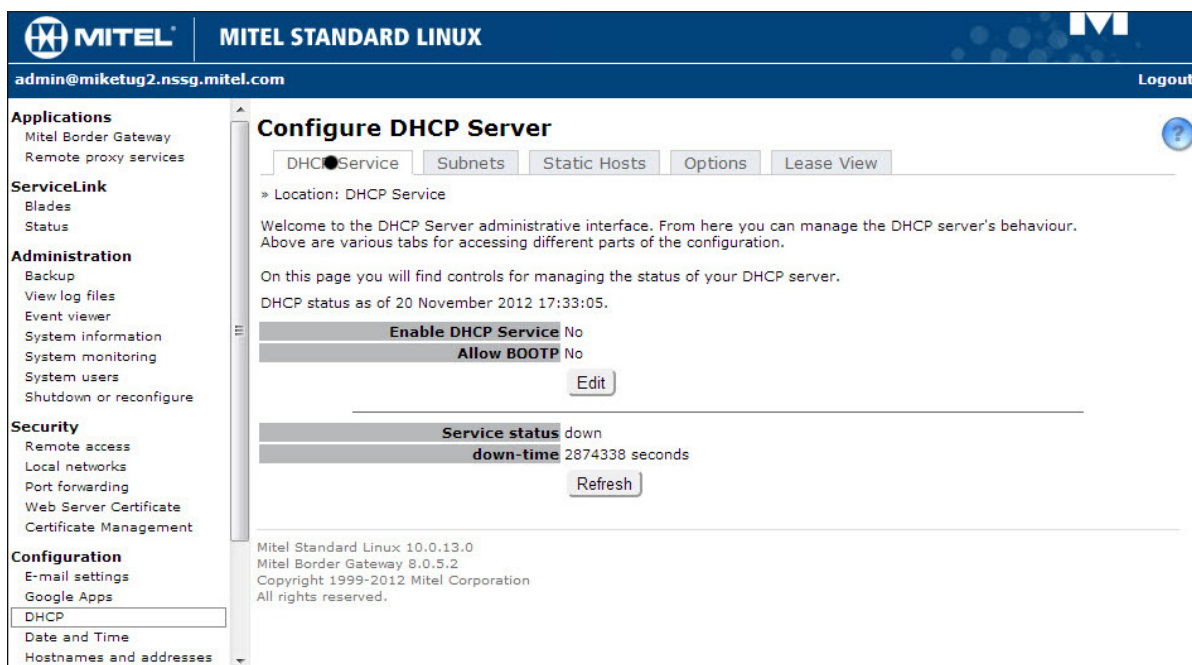


Figure 13. DHCP Settings

To enable DHCP:

1. On the DHCP Service tab, click **Edit**.
2. Click **Enable DHCP Service** to enable the internal DHCP server. Note: Do not enable this server if a DHCP server already exists on the network.
3. Click **Allow BootP** to allow network clients to obtain IP addresses using the Bootstrap Protocol.
4. Click **Update** to enable the settings.

To disable DHCP:

1. On the DHCP Service tab, click **Edit**.
2. Clear **Dable DHCP Service** to disable the internal DHCP server.
3. Click **Update** to enable the settings.

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
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 **Delete**.

To add a subnet range:

 If you enable DHCP and add a subnet, you must then provide a subnet range.

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

To remove a subnet range:

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

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. (For example, host.mitel.com)
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 remove a static host:

1. On the Static Hosts tab, click the Remove link associated with the host you want to remove.
2. Click **Delete**.

To add DHCP Options:

1. On the Options tab, click **Add option**.
2. In the **Scope** field, select the scope to which to apply this option. (Global, Subnet, Range, or Host)
3. Select the **option type** for this option (Standard, Vendor, or Site-local).
4. Do one of the following:
 - For **Standard** options, select an option number from the list.
 - For **Vendor** options, select a vendor option from the list.
 - For **Site-local** options, enter an option number between 224 and 254.
5. Click **Next**.
6. Configure the DHCP option as required.
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.

To remove a DHCP option:

1. On the Options tab, click the Remove link associated with the option you want to remove.
2. Click **Delete**.

Date and Time

Use the Date and time panel to manage configure server date and time. You can use a network time server or you can set the date and time manually. A time server is a device on the Internet that communicates the time to other computers over the Internet using the Network Time Protocol (NTP). Many organizations provide Internet time servers for free.

The screenshot shows the 'Date and time configuration' page in the Mitel Standard Linux web interface. The page is titled 'Date and time configuration' and includes a sidebar with navigation menus. The main content area is divided into several sections:

- Settings Summary:**
 - Current Time: Tue Nov 20 17:38:07 EST 2012
 - Time Zone: America/Montreal
 - Network Time Enabled
 - Server: centos.pool.ntp.org
 - NTP Server: centos.pool.ntp.org
- Set system TimeZone:**
 - The system global TimeZone controls the conversion between internal time (UTC) and displayed local time, and also determines when Daylight Savings Time applies.
 - Time Zone: America/Montreal
- Configure Network Time Server:**
 - The server is periodically synchronizing the system clock to the network time protocol (NTP) server specified below. To synchronize to a different NTP server, enter a different hostname or IP address in the field below.
 - NTP Server: centos.pool.ntp.org
 - Disable Network Time Server**
 - Choose this option to stop synchronizing the system clock to the NTP server. When the NTP service is disabled, you can set the system date and time manually from this page.

The page also includes a 'Save' button at the bottom right and a 'Query' button next to the NTP Server field.

Figure 14. Setting Date and Time


To configure a network time server:

1. In the **Set system Time Zone** list, select your time zone.
2. Select **Configure Network Time Server**.
3. Enter the **domain name** or **IP address** of the NTP Server.
4. Click **Save**.

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://support.ntp.org/bin/view/Servers/WebHome>. You should always use a secondary time server (also called a stratum 2 server) to lighten the load on the primary time servers.


To set the date and time manually:

1. Select **Disable Network Time Server**.
2. In the **Set system Time Zone** list, select your time zone.
3. Select **Set Date and Time** and enter month, day, year, hours and minutes information.
4. (Optional) Select **Enable System Clock Adjustment** to adjust system time gain rate.
5. Click **Save**.

 **Note:** The server manager will reset the time automatically during daylight savings time.

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

1. Click **Disable Network Time Server** and then click **Save**.
2. Enter time zone, date, and time information.
3. Click **Save**.

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

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 to issue the **ntpq -c peers Linux** command.

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).

NTP Server Query results for: centos.pool.ntp.org

remote	refid	st	t	when	poll	reach	delay	offset	jitter
205.189.158.228	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
192.75.12.10	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
208.80.96.70	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
127.127.1.0	.LOCL.	10	l	30	64	377	0.000	0.000	0.000

2. 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 the NTP server.

NTP Server Query results for: centos.pool.ntp.org

remote	refid	st	t	when	poll	reach	delay	offset	jitter
205.189.158.228	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
192.75.12.10	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
208.80.96.70	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
*127.127.1.0	.LOCL.	10	l	30	64	377	0.000	0.000	0.000

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: * indicates that the system time is being synchronized with the NTP server

	<p># indicates that the host is selected for synchronization, but distance from the host to the server exceeds the maximum value.</p> <p>o indicates that the host is selected for synchronization, and the PPS signal is in use.</p> <p>+ indicates the host included in the final synchronization selection set.</p> <p>x indicates that the host is the designated false ticker by the intersection algorithm.</p> <p>. indicates that the host is selected from the end of the candidate list.</p> <p>- indicates a host discarded by the clustering algorithm.</p> <p>blank indicates a host is discarded due to high stratum and/or failed sanity checks.</p>
refid	The current source of the synchronization for the remote host.
st	The stratum used by the remote host. The lower the number, the closer you are to the time source. Stratum 16 indicates that the system is not synchronized with a time server.
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 used between two polls.
reach	The number of times the other NTP server has been contacted successfully.
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.

Hostnames and Addresses

Use this page to manage hostnames and their corresponding IP addresses for the **internal** DNS server. If you have programmed an IP address into the DNS forwarding address on the [Domains](#) page, then MSL forwards DNS requests to that **external** IP address for resolution and ignores any entries on this page. To disable DNS forwarding, enter an empty string as the [DNS Forwarder](#) address.

The screenshot shows the 'Hostnames and addresses' configuration page in the Mitel Standard Linux web interface. The page title is 'Hostnames and addresses' and it includes a sub-header 'Current list of hostnames for mycompany.local.' Below this is a table with the following data:

Hostname	Location	IP Address	Ethernet address	Action
ftp.mycompany.local	Self	192.168.173.1		Modify Remove
mail.mycompany.local	Self	192.168.173.1		Modify Remove
msl-9114.mycompany.local	Self	192.168.173.1		Modify Remove
proxy.mycompany.local	Self	192.168.173.1		Modify Remove
wpad.mycompany.local	Self	192.168.173.1		Modify Remove
www.mycompany.local	Self	192.168.173.1		Modify Remove

Figure 15. Hostnames and addresses

To add a hostname/address listing to the file:

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. (This list is populated by entries made on the Domains page.)
5. In the **Location** list, select visibility (Local, Remote, Self).
6. Click **Next**.
7. Confirm the details and then click **Add**.

To edit the location of a hostname:

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

To remove the hostname of a network device:

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

Domains

This form allows you to configure other virtual domains in the network. You can also define a Domain Name Service (DNS) to be associated with the MSL server, if required (also called a "DNS Forwarder" address).

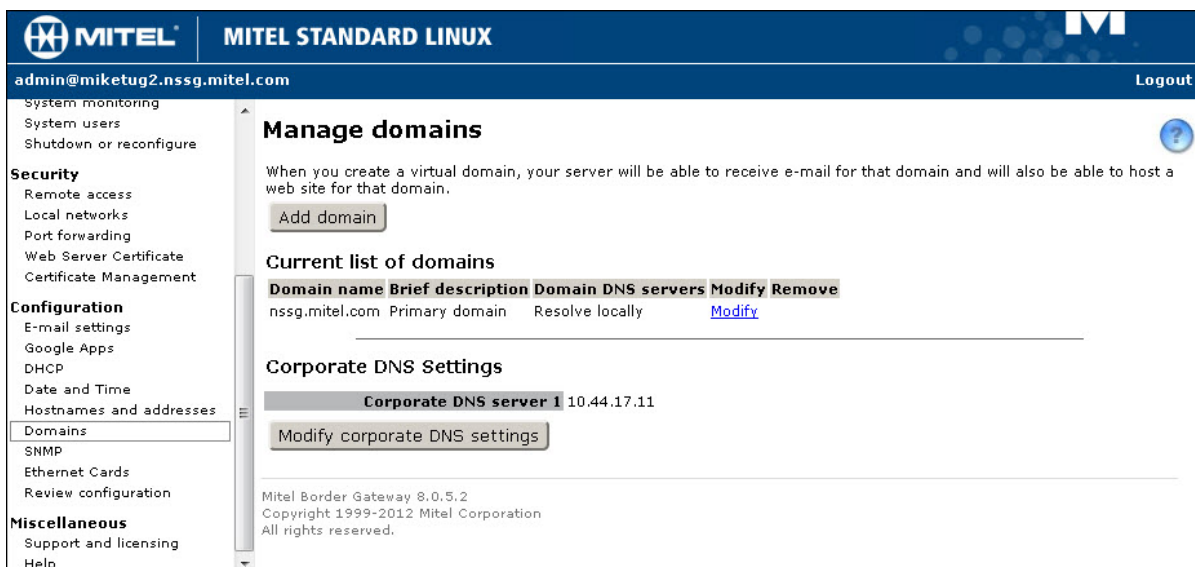


Figure 16. Domains

To configure a virtual domain:

1. Under Configuration, click **Domains**.
2. Click **Add Domain**.
3. Enter the **Domain Name** and a brief description.
4. In the **Domain DNS Servers** field, select how this is resolved:
 - **Resolve locally**
 - **Internet DNS servers**
 - **Corporate DNS servers**


The default will be correct for most networks.

5. Click **Add**.


DNS Forwarder

If you want to override the internal DNS server in the MSL server, you can enter the IP address of the preferred DNS server here.

1. Under Configuration, click **Domains**.
2. Click **Modify Corporate DNS settings**.
3. Enter the **Primary corporate DNS server** IP address. You can also enter a **Secondary corporate DNS** server address if applicable.

 **Note:** Do not enter the address of your ISP's DNS servers because the MSL server is capable of resolving all Internet DNS names without this additional configuration

4. Click **Save**.

 **Note:** By default, the MSL server uses itself as a DNS resolver and cache. When resolution is required, MSL first checks the DNS settings to see if you have overridden the default by programming a forwarder. If not, MSL then checks your Hostnames and Addresses entries to see if the requested host name is listed there. If not, MSL proceeds to access DNS root servers on the Internet for resolution.

Simple Network Management Protocol (SNMP)

MSL supports Simple Network Management Protocol (SNMP) for retrieval of network information and statistics. Enabling SNMP allows access to the following options:

- System Monitoring subsystem for monitoring link use
- Remote access to System Monitoring. For reports, SNMP creates the following URL:

https://<server IPv4 address>/monitor/

 **Note:** The default access for this URL is "disabled".

To enable SNMP:

1. Access the server manager.
2. Under Configuration click **SNMP**.
3. In the **Service Status** list, select **Enabled** to support SNMPv1, SNMPv2c, and SNMPv3.

SNMP Configuration Options

Use the following options to configure SNMP on the SNMP page of the server manager:

SNMPv2c community string for read-only access - a string that your SNMPv2c clients will use to monitor the server. The default string is "public". For security, chose a string other than the default.

SNMPv2c network access setting – controls remote access. Choose from one of the following four settings:

- **Localhost only** – the 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 local networks** – allows access to all networks that are configured in the "Local Networks" panel. These networks may not be on the same subnet as the server (that is, they may be attached via a router).
- **All local plus remote access list** – allows access to all local networks plus the networks listed in the "Remote Access" panel.

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. See [Adding an SNMPv3 User Backups](#) on page 67.

System Contact Address – the email address or user name of a local user responsible for MSL. The default is the Admin forwarding address for the Email service, or, if not set, the local admin account.

System Location – a string that identifies the location of the system.

Vital Process Monitoring – enable this option to monitor processes like the web server or mail server.

Monitor Disk Usage – enable this option to monitor disk space usage on your server's root partition.

Diskspace Threshold – a percentage of remaining disk space that, when reached, reports its value at the Object ID indicated in the panel. Enter a numerical value between 0 and 100 followed by the % sign, or enter an absolute value in bytes. The default value is 5%.

Monitor CPU usage – enable this option to monitor the server's use of the CPU.

One minute CPU threshold, Five minute CPU threshold, and Fifteen minute CPU threshold – enter server load average thresholds for each time period or leave these set to the default values of 5, 4 and 3 respectively. (You can think of load average as a percentage of system utilization. For example: a load average of 2.5 during one minute of operation means the CPU was overloaded by 250% for that particular minute. A fifteen minute load average of .5 would mean that the CPU had a 50% load; in other words, it was only busy for half of the time.)

Trap community string – a string used when sending trap messages. Leave this field blank to make the string default to the one entered in the "Community string for read-only access" field.

Trap host or address – an IP address, or addresses, where trap messages will be sent. Leave this field blank to prevent the transmission of traps.

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 – download the Mitel MIBs if you want to import them into your own network management software. **NOTE:** The MIB files are zipped and in UNIX file format.

Add an SNMPv3 User

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. Access the server manager.
2. Under Configuration click SNMP.
3. Under SNMPv3 Settings , click Configure SNMPv3 Users.
4. Type a User Name (also known as “securityname”) for the SNMPv3 user.
5. Select the **Authentication Type** that matches SNMP manager/agent configuration:
 - MD5
 - SHA1
 - None (no authentication)
6. If you selected an Authentication Type, enter an **Authentication Password** (also known as “authentication passphrase”) at least eight characters long.
7. Select the Privacy Protocol that matches SNMP manager/agent configuration:
 - DES
 - None (no encryption)
8. If you selected a Privacy Protocol, enter a **Privacy Password**.
9. 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.
10. Complete the following fields as required and then click **Add**.

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 (Server-only mode) or
- a "Local" adaptor for connection to the Local Area Network AND a "WAN" adapter for connection to the Wide Area Network (Server-gateway 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).

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

To configure the Speed and Duplex settings of a NIC:

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**.

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

All other settings are read only. See the following table for descriptions of the settings.

Setting	Description
Link detected	Yes: NIC is connected to the network. No: NIC is not connected to the network.
IP Address	IP Address assigned to the Network Interface Card
Netmask	Netmask assigned to the Network Interface Card
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 depend on 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 Configuration

The Review Configuration section of the server manager summarizes how the server is configured. This is the data entered during the installation process and possibly changed later through the server console or the server manager. You can print this report, but you can not make changes from this screen.

The screenshot shows the 'Review configuration' page in the Mitel Standard Linux web interface. The interface includes a top navigation bar with the Mitel logo and 'MITEL STANDARD LINUX' text. Below the navigation bar, the user is logged in as 'admin@miketug2.nssg.mitel.com' and there is a 'Logout' link. A left sidebar contains a menu with categories: ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled 'Review configuration' and contains several sections:

- Networking Parameters:**
 - eth0 (Local): 10.38.200.253/255.255.255.0
 - Internet Visible IP Address (to AMC): 10.38.200.253
 - Gateway: 10.38.200.1
 - Additional local networks: No additional networks defined
 - DHCP server: disabled
- Server names:**
 - DNS server: 10.38.200.253
 - Web server: www.nssg.mitel.com
 - Proxy server: proxy.nssg.mitel.com:3128
 - FTP server: ftp.nssg.mitel.com
 - SMTP, POP, and IMAP mail servers: mail.nssg.mitel.com
- Domain information:**
 - Primary domain: nssg.mitel.com
 - Virtual domains: nssg.mitel.com
 - Primary web site: http://www.nssg.mitel.com
 - Server manager: https://miketug2/server-manager/
 - User password panel: https://miketug2/user-password/
 - Email Addresses:
 - useraccount@nssg.mitel.com
 - firstname.lastname@nssg.mitel.com
 - firstname_lastname@nssg.mitel.com

At the bottom of the page, the following text is displayed: Mitel Standard Linux 10.0.13.0, Mitel Border Gateway 8.0.5.2, Copyright 1999-2012 Mitel Corporation, All rights reserved.

Figure 17. Review Configuration

The Server Console

You can also perform basic MSL configuration using the Server Console. The server console provides basic, direct access to the server. Most server console operations are also available from the server manager.

```

Server console (vmbg-taha.mitel.com)
Welcome to the server console!

Use the Arrow and Tab keys to make your selection, then press Enter.

 1. Check status of this server
 2. Configure this server
 3. Test Internet access
 4. Media Check Mitel CD/DVD
 5. Register for ServiceLink
 6. Install application blades from CD/DVD
 7. Reboot, reconfigure or shut down this server
 8. Offline sync with the AMC
 9. Manage local networks
10. Manage disk redundancy
11. Access server manager
12. View support and licensing information
13. Perform backup
14. Verify a backup file
15. Restore from backup
16. Exit from the server console

< Next >                < Exit >

```

Figure 18. The Server Console

From the Server Console you can see the following information and perform the following tasks:


Option:	Use this option to:
Check status of this server	view uptime information about the server.
Configure this server	view and modify the configuration information entered during installation (Ethernet cards, IPv4 and IPv6 address information, DHCP, DNS, domain names, etc.).
Test Internet access	test your connection by contacting Mitel Corporation via Internet
Media Check Mitel CD	test a Mitel application CD (supported only for applications that have embedded checksum values.)
Register for Service Link	activate ServiceLink on the AMC via text mode browser; (normally you would use the web-based server manager)
Install application blades from CD/DVD	install application software blades from CD. Your application documentation specifies when to use this option.

Option:	Use this option to:
Reboot, reconfigure, or shut down the server	reboot or shut down the server. Configuration settings in effect at the time of reboot are re-applied.
Offline Synch with the AMC	use for AMC activation at sites where the MSL server does not have direct Internet access. (Note: You will need Internet access from another PC/workstation.)
Manage local networks	show, add, or delete “ local network ” access privileges to additional IPv4 and IPv6 networks. Note: For security, we recommend that you be as precise as possible when granting access (for example, enter the IP address of a specific PC or subnet).
Manage disk redundancy	manage configuration of redundant (RAID1) disks.
Access server manager Note: select [+] to access the second page of options.	access the server manager using a text-based browser. This is the same interface to which you can connect remotely using a web browser; this option allows you to perform server manager functions directly from the server console. Use the keyboard arrow keys to navigate the pages. Type 'q' (for quit) to exit the text-based browser. Note: most applications can <u>not</u> be managed using the text-mode browser. The server uses a text-based browser called “ELinks” to access the web-based server manager. ELinks information is available at http://elinks.or.cz/about.html . Note that for security reasons some ELinks features are disabled when you are browsing from the server console (such as the ability to specify an external URL).
View support and licensing information	display the licensing terms.
Perform backup	back up configuration information to a USB device or a network file server. For more information see Performing Backups on page 74.
Verify a backup file	verify previous backup files. For more information, see Verify Backup on page 75.
Restore from backup	restore backup files from a network share, removable device, or another running server. For more information, see Restore Configuration Information on page 76.
Exit from the server console	exit from the Server Console.

Offline Sync with the AMC

If the MSL server is not directly connected to the Internet, you can still perform an activation using the “Offline Sync with the AMC” option. This option allows you to:

- copy Application Record information to a portable storage device
- insert the storage device in an intermediate PC and use it to connect to the AMC and send/receive activation information
- use the storage device to update the MSL server with the received activation information

 When an offline system is upgraded to MSL 9.3 or later, it will receive a Major alarm indicating that the automatic synchronization process has failed. To disable auto-synchronization and prevent further alarms, re-do the Offline Sync procedure. The original alarm can then be cleared manually.

To perform an offline sync:

1. Access the server console from the server itself or remotely using an SSH client.
2. Log in as "admin".
3. Select the option to perform **Offline Sync with the AMC**.
4. On the Offline sync screen, select **create** to prepare the removable storage device for use with offline sync.
5. When prompted, insert a portable storage device and then select **Next**.
6. When prompted, enter your Application Record ID and then select **Next**.
7. When prompted, remove the storage device and take it to a PC with Internet connectivity.
8. Insert the storage device in the remote PC and navigate to the storage drive location.
9. Search the main directory for a file called **sync.bat** and double-click it. A script runs that sends your sync information to the AMC and receives licensekey information in return.
10. To verify the sync, navigate to the **sync.log** file in the **sdata** directory of the storage drive location. Double-click sync.log to open and check for “completed successfully” message.
11. Remove the storage device from the remote PC and go to the MSL server.
12. Select the option to perform **Offline Sync with the AMC**.
13. On the Offline sync screen, select **read**.
14. When prompted, insert the storage device and select **Next**. The MSL server reads the activation information from the storage device and signals successful completion.
15. Select the option to **Exit from the server console**.

You have successfully performed an offline activation.

Performing Backups

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 (Linux, including MSL) or SMB/CIF (Windows). Any USB storage device that is formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux) is compatible.

Notes:

- You can also use the server manager [Backup](#) option to back up data to your desktop or network file server.
- If you are backing up to an MSL server, configure it to accept access from the backup server. See [Local Networks](#) for details.
- To restore an SFTP backup, you must copy it to a removeable device such as USB key, and then select the [Restore from Backup](#) option from the Server Console.


To perform backup:

1. Access the server console from the server itself or remotely using an SSH client.
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**. The backup is performed.
3. Enter a name for the backup file and then click **Next**. The name cannot contain spaces.
4. When the backup is complete, remove the USB device when prompted.
5. Verify that the backup was performed successfully using the [Verify Backup File](#) 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 the **Optional Directory Path** where the backup will be stored. If you leave this field blank, the file will be stored at the root of the shared folder. Spaces and multi-level directory names are permitted; for example, "MSL backup" and "MSL backup/2011/October" are valid sub directory names. Dashes (-) are not permitted.
6. Enter the **username** to use when connecting to the backup server.
7. Enter the **password** to use when connecting to the backup server. Estimated backup size and available storage space are displayed.
8. Click **Proceed**. A progress bar indicates backup status. When the backup is complete, file verification is performed automatically.
9. Click **Continue**.


 **Note:** By default, the backup file is named **mslserver.tgz**. For MSL Release 9.0 and later, you can change the filename but it must maintain the .TGZ extension. Backup files created in releases prior to 9.0 are all named **smeserver.tgz**. If you prefer to save incremental backups, you can rename the file each time (for example, JuneBkp.tgz, JulyBkp.tgz, etc.). For MSL Release 9.0 and later, you can store multiple backup files on the same media and MSL will prompt you to select the file to restore. If you store multiple files on the same media, ensure that there is enough free space available before attempting to store another backup.

Verify Backup File

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

To verify a backup file:

1. Access the server console from the server itself or remotely using an SSH client.
2. Log in as "admin".
3. From the console, select the option to **Verify a 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.)
5. If more than one storage device is connected to your system, select the device that contains 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.

 **Note:** Not all USB memory devices are compatible. Our testing with MAS applications indicates that the Verbatim, GXT, and Kingston brands consistently work well. See the *MAS Engineering Guidelines* for a list of supported USB devices.

Restore Configuration Information

You can restore application and configuration data when you re-install the MSL server software, or on an operational system.

The system backup files can be restored from portable media such as a USB storage device, from a network file server, or from a running server you wish to replace.

Notes:

- Ensure that your verified backup file has the .tgz file extension.
- USB storage devices that are formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux) are compatible for restore.
- You may receive a Windows popup error message when copying your backup to the formatted USB device. Some Windows security applications on the PC where the backup file is stored may add a data stream to this filename to mark it as a "downloaded" file. This results in an error message warning that the backup file contains more than one data stream. This warning can be safely ignored. Click **Yes** and proceed.

Restore during MSL Re-installation


To restore configuration data when you re-install MSL:

1. Copy the backup file to a removable device or network share drive, or arrange access to a running server you wish to replace.
2. Access the server console and log in as "admin".
3. Re-install MSL software by inserting the MSL software CD and selecting the option to **Reboot** from the console menu. Your server must be set to boot from the CD-ROM device.
4. During installation, select the option to **Erase all disks and perform fresh install**. When installation is complete, you are prompted to remove the CD or USB media and then reboot the system.
5. After rebooting the server, you are prompted "Do you wish to restore from backup?" Click **Yes**.
6. Select the location of the backup file:
 - **Restore from removable device**
If you select this option, you will be prompted to insert the removable device (USB or CD) containing the backup file. MSL discovers the backup file (or files) and displays them. Select the backup file you wish to restore and follow the prompts to install it.
 - **Restore from network share**
If you select this option, you will be prompted to select a network interface to use for the restore (LAN or WAN), the address and netmask of the local MSL server, the

address, gateway and domain name of the backup server, the folder name containing the backup file, and the username and password required to log in to the backup server.

- **Restore from another running server**
If you select this option, you will be prompted to pull configuration and application data from an existing physical or virtual server and restore it to a new server. See [Restore from another Running Server](#).
7. After responding to all prompts, click **Next** to restore the backup data.

A progress bar displays while the restore is in progress. When it completes, MSL reboots the server to activate the restored configuration.
 8. When the reboot is complete, log back in to the server console.
 9. Select the option to **Register for Service Link** to perform a sync with the AMC.

 **Note:** If hardware has been changed/replaced, you will need to deactivate your ServiceLink account, reset your Hardware ID, re-enter your Application Record ID (or service account 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 AMC. For more information on Hardware IDs, see the online help provided with your AMC account.

10. Reinstall your application software.

Restore on an Operational System

To restore configuration data on an operational system:

1. Copy the backup file to a removable device or network share drive, or arrange access to a running server you wish to replace.
2. Access the server console and log in as “admin”.
3. From the console, select the option to **Restore from backup**.
4. A warning appears, indicating that if you continue the MSL server will reboot and the current application and configuration files will be overwritten. Click **Reboot Now** to continue.
5. After the reboot is complete, select the location of the backup file:
 - **Restore from removable device**
If you select this option, you will be prompted to insert the removable device (USB or CD) containing the backup file. MSL discovers the backup file (or files) and displays them. Select the backup file you wish to restore and follow the prompts to install it.
 - **Restore from network share**
If you select this option, you will be prompted to select a network interface to use for the restore (LAN or WAN), the address and netmask of the local MSL server, the address, gateway and domain name of the backup server, the folder name containing the backup file, and the username and password required to log in to the backup server.
 - **Restore from another running server**
If you select this option, you will be prompted to pull configuration and application

data from an existing physical or virtual server and restore it to a new server. See [Restore from another Running Server](#).


6. After responding to all prompts, click **Next** to restore the backup data.

A progress bar displays while the restore is in progress. When it completes, MSL reboots the server to activate the restored configuration.

7. When the reboot is complete, log back in to the server console and perform a sync with the AMC if necessary.

Restore from another Running Server

If you are replacing an existing MSL 9.x server (physical or virtual), you can pull configuration and application data from it while it's still running and restore the data to a new MSL 10.x or later server. The restore process automatically shuts down the old server.

 **Note:** This procedure is of particular use for virtual implementations, as it enables users to easily replace an existing virtual machine with a new one. If any problems arise, the original implementation can be restored with minimal downtime.

Conditions

- Installing the same ARID on new physical hardware will require a Hardware ID reset.
- If the two servers are on:
 - **connected networks** (i.e. they have the same IP address range and there is no router between them), both servers must have the same subnet mask applied.
 - **different networks:**
 - MSL will request a gateway/router IP address to use for access.
 - When the restore is complete, the new server must be reconfigured for its own network because it will have inherited the network configuration of the original running server.

Warning! Booting up the original server again after the restore procedure will result in IP address conflicts.

About IP Addressing

The IP address of the new server must be distinct from the original running server, at least for the duration of the migration.

For example, if the two servers are on a connected network, the new server will need a *temporary* IP address from the same network range. When the migration is complete, the new server will reboot with the IP address of the old server and will be usable immediately.

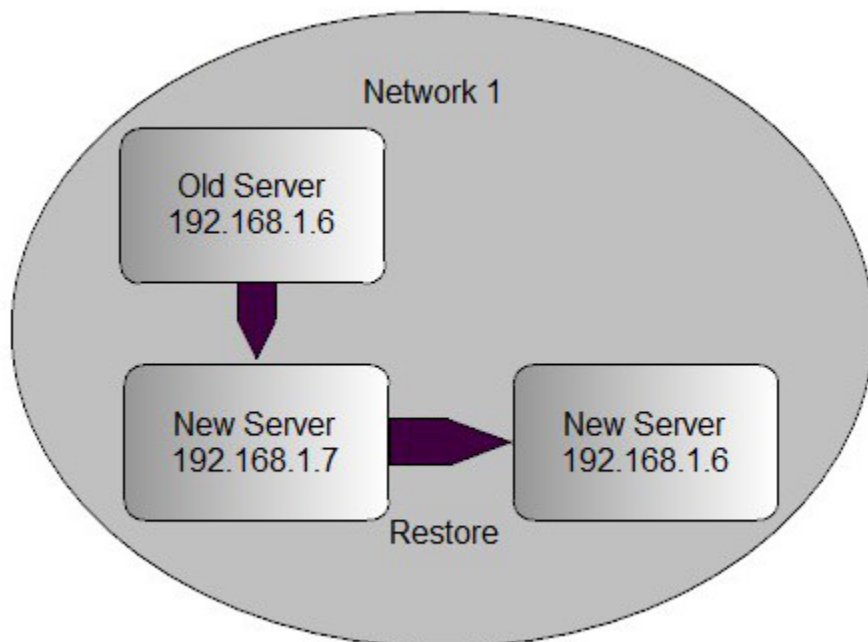


Figure 19. IP Addressing — Two Servers on a Single Network

If the new server is on a different network, it will need a permanent IP address in the range of that network. MSL will prompt you for a gateway IP address that it can use to access the old server. When migration is complete, the new server will reboot with the IP address of the old server, which will not be reachable on the new server's network. You must select the console option to "Reconfigure this server" and enter the correct IP address (i.e. the same one that was used for the migration).

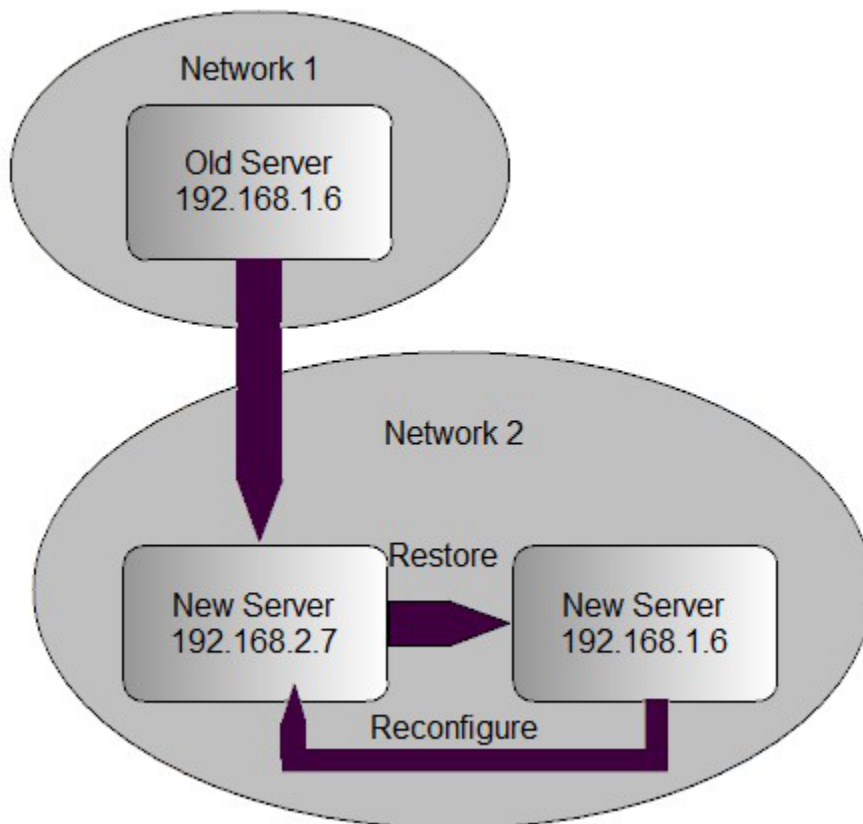



Figure 20. IP Addressing — Two Servers on Two Networks

To restore from another running server:

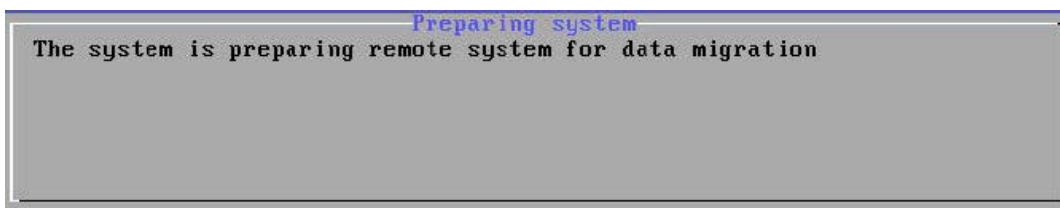
1. [Install MSL software](#) on the new server.
2. In the MSL server console of the new server, when prompted to "Restore from backup?", select **Yes**.
3. When prompted, select **Restore from another running server**.
4. If your system has more than one **network adapter**, select the adapter to use for the restore procedure. (This will usually be the LAN adapter.)
5. Enter the local **IP address** of the new server.
6. Enter the appropriate **subnet mask** for this server.

 **Note:** If the two servers are on the same, connected network, they must have the the same subnet mask.

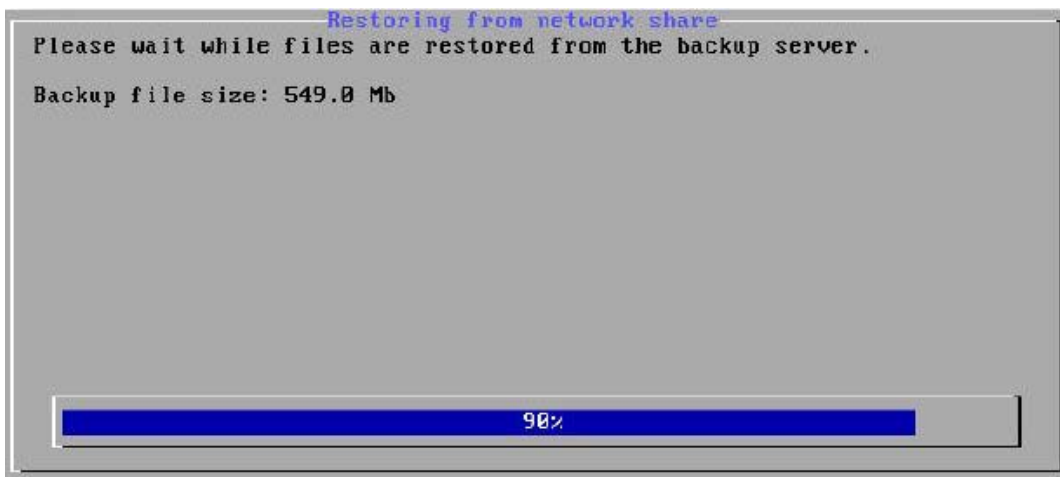
7. Enter the **IP address** of the existing server.
8. If the two servers are on different IP networks, MSL will prompt for the **gateway IP address** to use to access the existing server. (This prompt does not appear if both servers are on the same, connected network.)
9. When prompted, enter the "admin" **password** for the existing server.

10. MSL does the following:

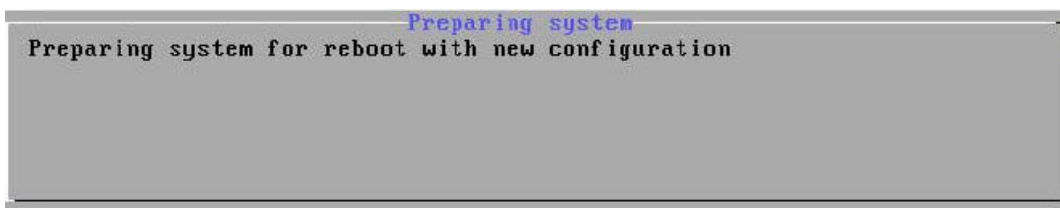
- Configuration and application data is backed up from the existing server.



- Configuration and application data is restored to the new server.



- The existing server is shut down.




11. On the new server, the restore is confirmed. Press **Enter** to reboot and activate your restored configuration settings.
12. If the two servers are on different networks, reconfigure the new server's network settings to reflect its network information, rather than the inherited data from the running server.
13. Reinstall application software.

Accessing the Linux Root Prompt

To perform advanced modifications to the configuration of the server, you can access the Linux operating system underlying MSL software by logging in as user "root".


WARNING: Making changes and customizations to the server from the Linux command prompt may invalidate the support agreement. Contact your Mitel authorized reseller before making any such customizations.

By default, the password for the "root" user is the same as the password used by the "admin" user account. Ensure that you log out from the root account when you are finished.

 **Note:** Remote administrative access is disabled by default and must be specifically enabled through the [Remote Access](#) panel of the server manager.

Changing the Administrator Password

By default, the "admin" and "root" users share a single Administrator password which is set during the initial MSL installation. Use the following procedure to change the "admin" password to a unique value.

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


To change the Administrator password for the "admin" user:

1. In the server manager under Administration, click **System users**.
2. Click the **Reset password** link associated with the "admin" account (the user name for this account is "Local User").
3. Type the new password in the second field. 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.
4. Verify the new password by entering it again in the third field.
5. Click **Save**.

After you change the "admin" password, the system will prompt you for the revised password as soon as you attempt to access another feature in the server manager. When you see the "Authorization Failed" message, click **OK**, enter the new password, and then press **Enter**.


Resetting the Administrator Password

If you forget the Administrator password belonging to the "admin" and "root" users, you can reset it with the following procedure.

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

To reset the Administrator password for the "admin" and "root" users:

1. Open a terminal session to the server.
2. Physically shut down the server and start it up again.
3. When the GRUB boot loader splash screen appears, press the "a" key.
The load process stops, enabling you to append arguments to the kernel boot line.
4. In the kernel boot line, type " single" (note the leading space) and then press **Enter**.

5. When the bash shell prompt appears, do the following:
 - Type "passwd root", enter a new password, and then press **Enter**.
 - Type "passwd admin", enter a new password, and then press **Enter**.
-  **Note:** Although you can enter unique "root" and "admin" passwords, typically you would enter the same value for both users.
6. Type "exit" and press **Enter** to resume the boot sequence.

Troubleshooting

You can use this utility to test RAM memory on a new server, or when debugging a problem server.

To run the memory test (memtest):

1. Configure your system to boot from either the CD/DVD ROM drive or USB drive.
2. Insert the MSL software CD or USB drive containing MSL software.
3. Reboot the computer. The installation script runs automatically and the MSL Installer dialog appears.
4. Select **Memory Test Utility**. Diagnostic test results are displayed on screen.

Technical Support

If you are a Mitel authorized reseller and require support, call +1-613-271-7614 (in the United States and Canada, call 1-866-472-9999) and ask for technical support. You can also visit our Web site at <http://www.mitel.com/>. Please have your Application Record ID number ready when you contact support.

Appendix A: Third Party Licenses

Parts of Mitel Standard Linux are licensed under open-source licenses. By accepting the Mitel EULA, you are also accepting all open-source software terms and conditions.

Apache

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for

informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Open SSL

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

5. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
6. Redistributions in binary form must reproduce the above copyright.

Perl

Definitions

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

- place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
- use the modified Package only within your corporation or organization.
- rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
- make other distribution arrangements with the Copyright Holder.

You may distribute the programs of this Package in object code or executable form, provided

that you do at least ONE of the following:

- distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
- accompany the distribution with the machine-readable source of the Package with your modifications.
- give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
- make other distribution arrangements with the Copyright Holder.

You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS

IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;

OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY

EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS

``AS

IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;

OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS

IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;

OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS

IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Boutell.Com

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002, 2003, 2004 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002, 2003, 2004 Greg Roelofs.

Portions relating to gdtf.c copyright 1999, 2000, 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org).

Portions relating to gdft.c copyright 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, 2003, 2004, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to GIF compression copyright 1989 by Jef Poskanzer and David Rowley, with modifications for thread safety by Thomas Boutell.

Portions relating to GIF decompression copyright 1990, 1991, 1993 by David Koblas, with modifications for thread safety by Thomas Boutell.

Portions relating to WBMP copyright 2000, 2001, 2002, 2003, 2004 Maurice Szmurlo and Johan Van den Brande.

Portions relating to GIF animations copyright 2004 Jaakko Hyvätti (jaakko.hyvatti@iki.fi)

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either

express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in the current release, the authors also wish to thank Hutchison Avenue Software Corporation for their prior contributions.

Fontconfig

Copyright © 2001,2003 Keith Packard

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Keith Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Keith Packard makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

KEITH PACKARD DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL KEITH PACKARD BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Gnu General Public License

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation’s users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a

network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY

AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

- a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or
- b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

- a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.
- b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

- a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.
- b) Accompany the Combined Work with a copy of the GNU GPL and this license document.
- c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

- d) Do one of the following:
 - 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.
 - 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.
- e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.
- b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Glossary

AMC	Applications Management Center
Blade	A software module that can be downloaded from the AMC
ICP	IP Communications Platform
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MAS	Prior to Release 8.2, MSL was called “Managed Application Server” or “MAS”. With the Release of 8.2, the name has changed to Mitel Standard Linux. (Note: The MAS acronym now refers to the Mitel Applications Suite product.)
MSL	Mitel Standard Linux
PPTP	Point-to-Point Tunneling Protocol
RAID1	Disk redundancy
SCSI	Small Computer Systems Interface
ServiceLink	A service supplied by the Applications Management Center (AMC) that allows applications and services to be delivered to the MSL server
SSH	Secure shell. A secure, encrypted way to log in to a remote machine across a network, or to copy files from a local machine to a server
VPN	Virtual Private Network

www.mitel.com



Global Headquarters	U.S.	EMEA	CALA	Asia Pacific
Tel: +1(613) 592-2122	Tel: +1(480) 961-9000	Tel: +44(0)1291-430000	Tel: +1(613) 592-2122	Tel: +61(0) 2 9023 9500
Fax: +1(613) 592-4784	Fax: +1(480) 961-1370	Fax: +44(0)1291-430400	Fax: +1(613) 592-7825	Fax: +61(0) 2 9023 9501

For more information on our worldwide office locations, visit our website at www.mitel.com/offices

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel to be accurate as of the date of its publication, is subject to change without notice. Mitel assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.
© Copyright 2011, Mitel Networks Corporation. All Rights Reserved.