A MITEL
PRODUCT
GUIDE

Mitel Standard Linux

Installation and Administration Guide

Release 11.0

Jan 2022

Mitel
Powering connections

Notices

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

Trademarks

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

Contents

About this Guide 1

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 2

This chapter contains the following sections:

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/DVD.

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 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.

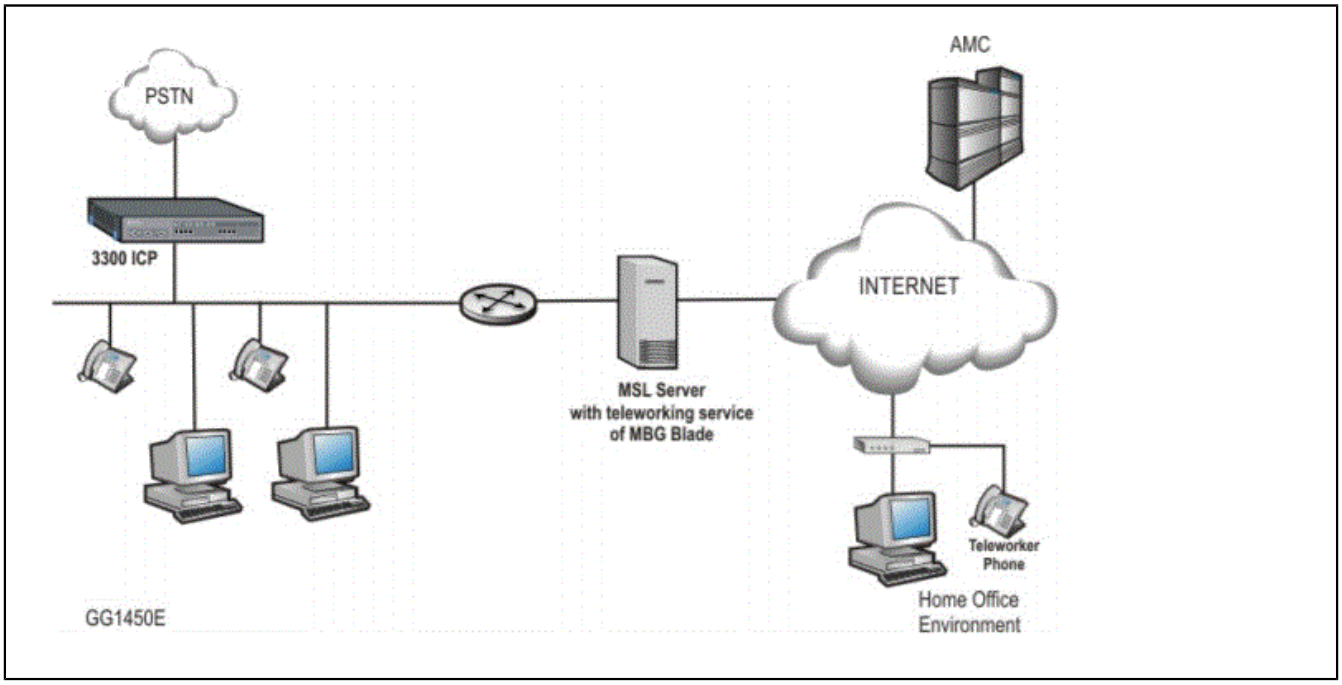


Figure 1: Server-gateway configuration example

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.

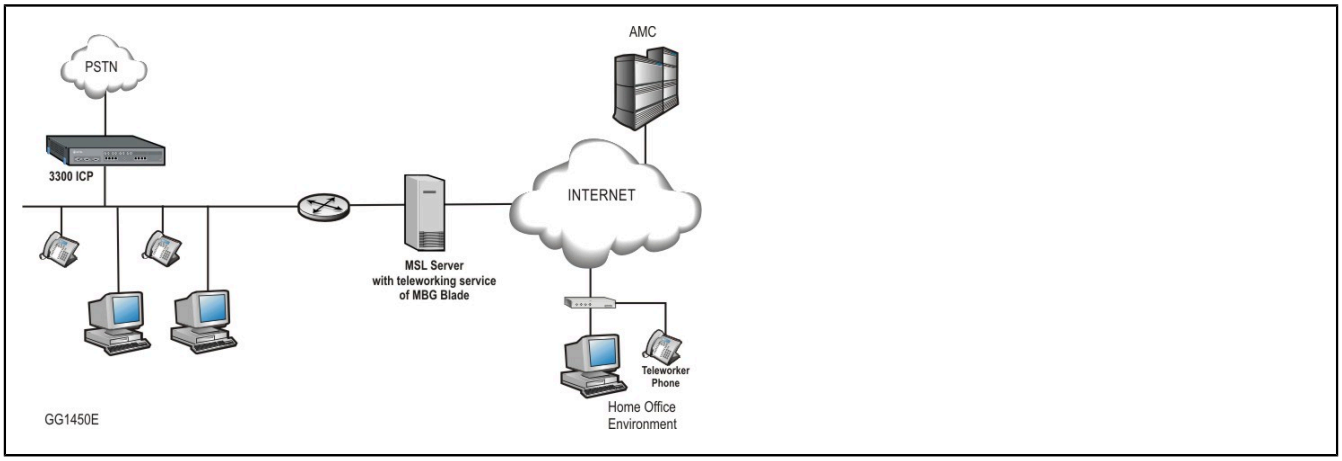


Figure 2: Server-only configuration example

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.

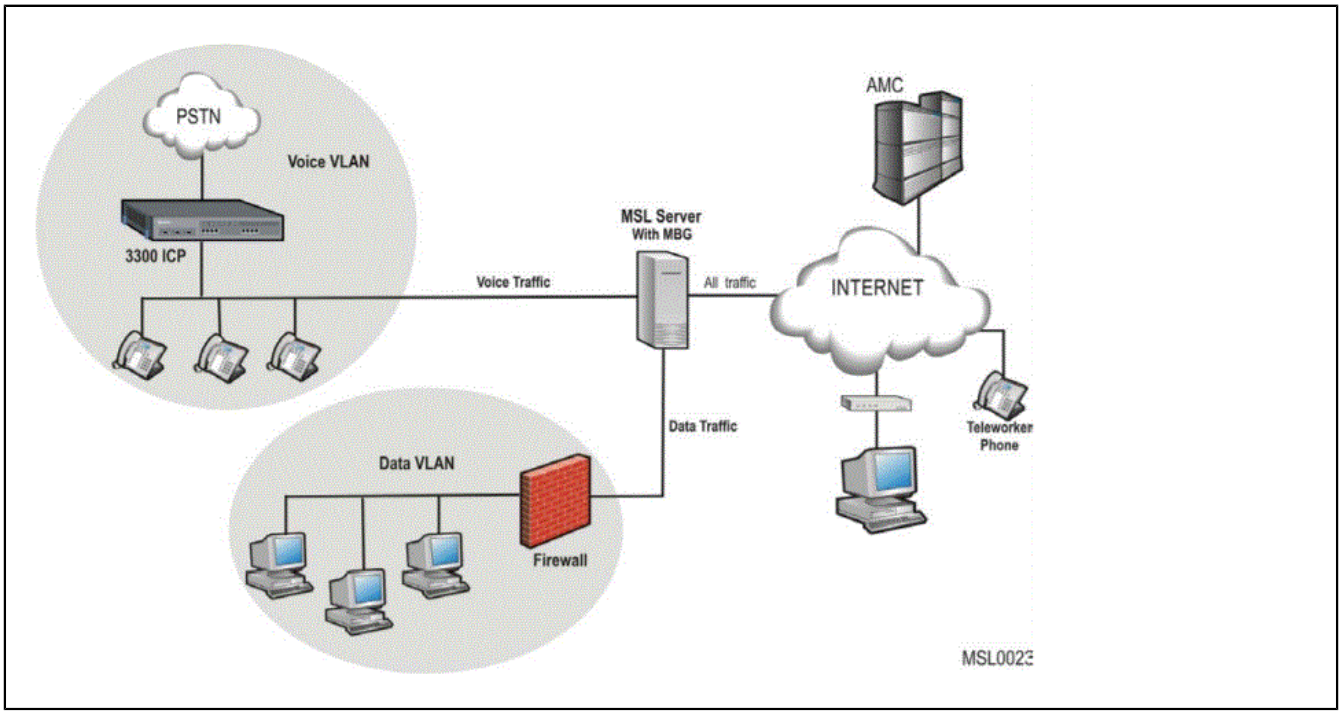


Figure 3: Server-gateway with Bridged Interface configuration example

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

2.1 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 MiCollab Mobile Client, 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 MiVoice Border Gateway be installed on the same MSL server.

2.2 Cloud Platform Support

Virtual Machine images will be produced to support deployment on multiple cloud platforms.

Azure Platform

The following features are supported on the Azure platform:

- Auto-provisioning of required MSL VM configuration. Provisioning data is obtained from the Azure platform and provided custom configuration values.
    - **Hostname**: The default hostname will be the lower case VM name. Any invalid hostname characters, such as periods or underscores, will be translated to hyphens.
    - **Networking**: MSL supports auto-provisioning of network elements, such as NICs, public/private IP addresses, gateways, routing and DNS.
    - On every reboot, which includes following a restore operation, the VM networking is analyzed and auto-provisioned if any changes are detected.
    - Supports auto-registration of the VM hostname in a private DNS zone linked to the virtual network of the primary (first) NIC. Only the primary (first) private IP linked to the NIC is registered. So, if the configuration console changes the hostname, the private DNS entry will be updated accordingly when the reboot occurs.

Networking Auto Configuration

Alternatives for auto-configuration of multiple NICs with optional multiple IP configurations.

Constraints:

- The primary private IP address on the primary interface (eth0) is always the LAN interface.
- Auto-provisioning of the network configuration will occur during each boot process if any VM networking changes are detected.

Configuration rules based on private/public IP configuration of additional NICs:

MSL currently supports up to 3 NIC adapters, which can be configured as the MSL LAN, WAN, and LAN2 interfaces. The WAN interface can have a second IP address assigned to it which will be configured as an IP address alias which we will call WAN2 for the purpose of this document.

The three possible NICs are referred to below as NIC0, NIC1 and NIC2, and the name directly correlates to the order in which the NICs are attached to the VM.

Note:

The Azure documentation refers to NIC0 as the primary NIC and the first private IP address assigned to a NIC as the primary IP.

The result of the MSL automatic network configuration follows and is based on the number of NIC adapters attached to the VM and the Azure private/public IP configuration of each NIC.

In all cases:

- NIC0 primary IP will always be configured as the LAN interface
    - VM host name registered with primary IP in linked private DNS zone if auto-registration is enabled

One NIC attached:

- NIC0 is default gateway

Two NICs attached:

- NIC0 is default gateway if NIC1 has no public IP
- NIC1 is
    - WAN and default gateway if it has public IP
        - WAN2 (alias) if it has second public IP
    - LAN2 if no public IP

Three NICs attached:

- NIC0 is default gateway if neither NIC1 or NIC2 have a public IP

- First additional NIC with 2 public IPs becomes
  - WAN and default gateway
  - WAN2 (alias)
- If no additional NIC with 2 public IPs found, first additional NIC with public IP becomes
  - WAN and default gateway
- First remaining additional NIC becomes
  - LAN2
- Remaining NICs (if any) are ignored

Custom Metadata Entries

Description of custom data that is supported when creating a VM.

- The custom data entry must be in valid JSON data format.
- The custom data must be entered into the Azure portal "Custom data" text field, located under the Advanced tab when creating a VM.
- If you are using the Azure CLI to create the VM, enter the custom data using the --custom-data option.
- **Note**: The system-password value is mandatory.

Note:

Providing invalid JSON custom data, will result in failure to auto-provision the VM. Access the serial console to configure the VM manually, if deployment takes more than 5 minutes.

Key	Example Values (must be JSON formatted)	Description
"domain-name"	"az.ucs.mitel.io"	Domain name to configure in the VM. If omitted the default internal Azure DNS name will be used

Key	Example Values (must be JSON formatted)	Description
"timezone"	"US/Eastern"	See Zone List for list of supported timezone strings.
"system-password"	"password"	The initial root/admin password configured in the VM. On first login to server manager you will be prompted to change the password.
"remote-networks"	["216.191.234.70/32","174.112.94.135/32"]	JSON list of network/mask pairs allowed to access the server manager and connect via ssh. The mask can be in integer (CIDR) or dotted decimal IP format.

Example JSON formatted option string:

```
{
"domain-name": "az.ucs.mitel.io",
"remote-networks": [
"216.191.234.70/32",
"174.112.94.135/32"
],
"system-password": "password",
"timezone": "US/Eastern"
}
```

Note:

See **MiVoice Business Subscription Azure Deployment Guide** for more details.

2.3 List of Timezone entries

Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
Africa/Douala
Africa/El_Aaiun
Africa/Freetown
Africa/Gaborone
Africa/Harare
Africa/Johannesburg
Africa/Juba
Africa/Kampala
Africa/Khartoum

Africa/Kigali
Africa/Kinshasa
Africa/Lagos
Africa/Libreville
Africa/Lome
Africa/Luanda
Africa/Lubumbashi
Africa/Lusaka
Africa/Malabo
Africa/Maputo
Africa/Maseru
Africa/Mbabane
Africa/Mogadishu
Africa/Monrovia
Africa/Nairobi
Africa/Ndjamena
Africa/Niamey
Africa/Nouakchott
Africa/Ouagadougou
Africa/Porto-Novo
Africa/Sao_Tome
Africa/Timbuktu
Africa/Tripoli
Africa/Tunis
Africa/Windhoek
America/Adak
America/Anchorage
America/Anguilla
America/Antigua
America/Araguaina
America/Argentina/Buenos_Aires
America/Argentina/Catamarca
America/Argentina/ComodRivadavia
America/Argentina/Cordoba
America/Argentina/Jujuy
America/Argentina/La_Rioja
America/Argentina/Mendoza
America/Argentina/Rio_Gallegos

America/Argentina/Salta
America/Argentina/San_Juan
America/Argentina/San_Luis
America/Argentina/Tucuman
America/Argentina/Ushuaia
America/Aruba
America/Asuncion
America/Atikokan
America/Atka
America/Bahia
America/Bahia_Banderas
America/Barbados
America/Belem
America/Belize
America/Blanc-Sablon
America/Boa_Vista
America/Bogota
America/Boise
America/Buenos_Aires
America/Cambridge_Bay
America/Campo_Grande
America/Cancun
America/Caracas
America/Catamarca
America/Cayenne
America/Cayman
America/Chicago
America/Chihuahua
America/Coral_Harbour
America/Cordoba
America/Costa_Rica
America/Creston
America/Cuiaba
America/Curacao
America/Danmarkshavn
America/Dawson
America/Dawson_Creek
America/Denver

America/Detroit
America/Dominica
America/Edmonton
America/Eirunepe
America/El_Salvador
America/Ensenada
America/Fort_Nelson
America/Fort_Wayne
America/Fortaleza
America/Glace_Bay
America/Godthab
America/Goose_Bay
America/Grand_Turk
America/Grenada
America/Guadeloupe
America/Guatemala
America/Guayaquil
America/Guyana
America/Halifax
America/Havana
America/Hermosillo
America/Indiana/Indianapolis
America/Indiana/Knox
America/Indiana/Marengo
America/Indiana/Petersburg
America/Indiana/Tell_City
America/Indiana/Vevay
America/Indiana/Vincennes
America/Indiana/Winamac
America/Indianapolis
America/Inuvik
America/Iqaluit
America/Jamaica
America/Jujuy
America/Juneau
America/Kentucky/Louisville
America/Kentucky/Monticello
America/Knox_IN

America/Kralendijk
America/La_Paz
America/Lima
America/Los_Angeles
America/Louisville
America/Lower_Princes
America/Maceio
America/Managua
America/Manaus
America/Marigot
America/Martinique
America/Matamoros
America/Mazatlan
America/Mendoza
America/Menominee
America/Merida
America/Metlakatla
America/Mexico_City
America/Miquelon
America/Moncton
America/Monterrey
America/Montevideo
America/Montreal
America/Montserrat
America/Nassau
America/New_York
America/Nipigon
America/Nome
America/Noronha
America/North_Dakota/Beulah
America/North_Dakota/Center
America/North_Dakota/New_Salem
America/Ojinaga
America/Panama
America/Pangnirtung
America/Paramaribo
America/Phoenix
America/Port-au-Prince

America/Port_of_Spain
America/Porto_Acre
America/Porto_Velho
America/Puerto_Rico
America/Punta_Arenas
America/Rainy_River
America/Rankin_Inlet
America/Recife
America/Regina
America/Resolute
America/Rio_Branco
America/Rosario
America/Santa_Isabel
America/Santarem
America/Santiago
America/Santo_Domingo
America/Sao_Paulo
America/Scoresbysund
America/Shiprock
America/Sitka
America/St_Barthelemy
America/St_Johns
America/St_Kitts
America/St_Lucia
America/St_Thomas
America/St_Vincent
America/Swift_Current
America/Tegucigalpa
America/Thule
America/Thunder_Bay
America/Tijuana
America/Toronto
America/Tortola
America/Vancouver
America/Virgin
America/Whitehorse
America/Winnipeg
America/Yakutat

America/Yellowknife
Antarctica/Casey
Antarctica/Davis
Antarctica/DumontDUrville
Antarctica/Macquarie
Antarctica/Mawson
Antarctica/McMurdo
Antarctica/Palmer
Antarctica/Rothera
Antarctica/South_Pole
Antarctica/Syowa
Antarctica/Troll
Antarctica/Vostok
Arctic/Longyearbyen
Asia/Aden
Asia/Almaty
Asia/Amman
Asia/Anadyr
Asia/Aqtau
Asia/Aqtobe
Asia/Ashgabat
Asia/Ashkhabad
Asia/Atyrau
Asia/Baghdad
Asia/Bahrain
Asia/Baku
Asia/Bangkok
Asia/Barnaul
Asia/Beirut
Asia/Bishkek
Asia/Brunei
Asia/Calcutta
Asia/Chita
Asia/Choibalsan
Asia/Chongqing
Asia/Chungking
Asia/Colombo
Asia/Dacca

Asia/Damascus
Asia/Dhaka
Asia/Dili
Asia/Dubai
Asia/Dushanbe
Asia/Famagusta
Asia/Gaza
Asia/Harbin
Asia/Hebron
Asia/Ho_Chi_Minh
Asia/Hong_Kong
Asia/Hovd
Asia/Irkutsk
Asia/Istanbul
Asia/Jakarta
Asia/Jayapura
Asia/Jerusalem
Asia/Kabul
Asia/Kamchatka
Asia/Karachi
Asia/Kashgar
Asia/Kathmandu
Asia/Katmandu
Asia/Khandyga
Asia/Kolkata
Asia/Krasnoyarsk
Asia/Kuala_Lumpur
Asia/Kuching
Asia/Kuwait
Asia/Macao
Asia/Macau
Asia/Magadan
Asia/Makassar
Asia/Manila
Asia/Muscat
Asia/Nicosia
Asia/Novokuznetsk
Asia/Novosibirsk

Asia/Omsk
Asia/Oral
Asia/Phnom_Penh
Asia/Pontianak
Asia/Pyongyang
Asia/Qatar
Asia/Qostanay
Asia/Qyzylorda
Asia/Rangoon
Asia/Riyadh
Asia/Saigon
Asia/Sakhalin
Asia/Samarkand
Asia/Seoul
Asia/Shanghai
Asia/Singapore
Asia/Srednekolymsk
Asia/Taipei
Asia/Tashkent
Asia/Tbilisi
Asia/Tehran
Asia/Tel_Aviv
Asia/Thimbu
Asia/Thimphu
Asia/Tokyo
Asia/Tomsk
Asia/Ujung_Pandang
Asia/Ulaanbaatar
Asia/Ulan_Bator
Asia/Urumqi
Asia/Ust-Nera
Asia/Vientiane
Asia/Vladivostok
Asia/Yakutsk
Asia/Yangon
Asia/Yekaterinburg
Asia/Yerevan
Atlantic/Azores

Atlantic/Bermuda
Atlantic/Canary
Atlantic/Cape_Verde
Atlantic/Faeroe
Atlantic/Faroe
Atlantic/Jan_Mayen
Atlantic/Madeira
Atlantic/Reykjavik
Atlantic/South_Georgia
Atlantic/St_Helena
Atlantic/Stanley
Australia/ACT
Australia/Adelaide
Australia/Brisbane
Australia/Broken_Hill
Australia/Canberra
Australia/Currie
Australia/Darwin
Australia/Eucla
Australia/Hobart
Australia/LHI
Australia/Lindeman
Australia/Lord_Howe
Australia/Melbourne
Australia/NSW
Australia/North
Australia/Perth
Australia/Queensland
Australia/South
Australia/Sydney
Australia/Tasmania
Australia/Victoria
Australia/West
Australia/Yancowinna
Brazil/Acre
Brazil/DeNoronha
Brazil/East
Brazil/West

CET
CST6CDT
Canada/Atlantic
Canada/Central
Canada/Eastern
Canada/Mountain
Canada/Newfoundland
Canada/Pacific
Canada/Saskatchewan
Canada/Yukon
Chile/Continental
Chile/EasterIsland
Cuba
EET
EST
EST5EDT
Egypt
Eire
Europe/Amsterdam
Europe/Andorra
Europe/Astrakhan
Europe/Athens
Europe/Belfast
Europe/Belgrade
Europe/Berlin
Europe/Bratislava
Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Busingen
Europe/Chisinau
Europe/Copenhagen
Europe/Dublin
Europe/Gibraltar
Europe/Guernsey
Europe/Helsinki
Europe/Isle_of_Man
Europe/Istanbul

Europe/Jersey
Europe/Kaliningrad
Europe/Kiev
Europe/Kirov
Europe/Lisbon
Europe/Ljubljana
Europe/London
Europe/Luxembourg
Europe/Madrid
Europe/Malta
Europe/Mariehamn
Europe/Minsk
Europe/Monaco
Europe/Moscow
Europe/Nicosia
Europe/Oslo
Europe/Paris
Europe/Podgorica
Europe/Prague
Europe/Riga
Europe/Rome
Europe/Samara
Europe/San_Marino
Europe/Sarajevo
Europe/Saratov
Europe/Simferopol
Europe/Skopje
Europe/Sofia
Europe/Stockholm
Europe/Tallinn
Europe/Tirane
Europe/Tiraspol
Europe/Ulyanovsk
Europe/Uzhgorod
Europe/Vaduz
Europe/Vatican
Europe/Vienna
Europe/Vilnius

Europe/Volgograd
Europe/Warsaw
Europe/Zagreb
Europe/Zaporozhye
Europe/Zurich
GB
GB-Eire
GMT
GMT+0
GMT-0
GMT0
Greenwich
HST
Hongkong
Iceland
Indian/Antananarivo
Indian/Chagos
Indian/Christmas
Indian/Cocos
Indian/Comoro
Indian/Kerguelen
Indian/Mahe
Indian/Maldives
Indian/Mauritius
Indian/Mayotte
Indian/Reunion
Iran
Israel
Jamaica
Japan
Kwajalein
Libya
MET
MST
MST7MDT
Mexico/BajaNorte
Mexico/BajaSur
Mexico/General

NZ
NZ-CHAT
Navajo
PRC
PST8PDT
Pacific/Apia
Pacific/Auckland
Pacific/Bougainville
Pacific/Chatham
Pacific/Chuuk
Pacific/Easter
Pacific/Efate
Pacific/Enderbury
Pacific/Fakaofo
Pacific/Fiji
Pacific/Funafuti
Pacific/Galapagos
Pacific/Gambier
Pacific/Guadalcanal
Pacific/Guam
Pacific/Honolulu
Pacific/Johnston
Pacific/Kiritimati
Pacific/Kosrae
Pacific/Kwajalein
Pacific/Majuro
Pacific/Marquesas
Pacific/Midway
Pacific/Nauru
Pacific/Niue
Pacific/Norfolk
Pacific/Noumea
Pacific/Pago_Pago
Pacific/Palau
Pacific/Pitcairn
Pacific/Pohnpei
Pacific/Ponape
Pacific/Port_Moresby

Pacific/Rarotonga
Pacific/Saipan
Pacific/Samoa
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Truk
Pacific/Wake
Pacific/Wallis
Pacific/Yap
Poland
Portugal
ROC
ROK
Singapore
Turkey
UCT
US/Alaska
US/Aleutian
US/Arizona
US/Central
US/East-Indiana
US/Eastern
US/Hawaii
US/Indiana-Starke
US/Michigan
US/Mountain
US/Pacific
US/Pacific-New
US/Samoa
UTC
Universal
W-SU
WET
Zulu

What's New in this Release 3

This chapter contains the following sections:

3.1 MSL Release 11.0

MSL Release 11.0 provides the following new features:

- The server manager “Shutdown or Reconfigure” panel has been renamed to “Shutdown or reboot”. The Reconfigure option in that panel has been removed.
- The server manager “Web Server” panel has a field for entering Subject Alternate Names (SANs) for the server, when generating a Certificate Signing Request.
- The server manager “Hostnames and addresses” panel does not comprise invalid host names section, and the “Review configuration” panel does not comprise server names section such as mail.domain, ftp.domain, www.domain, and so on.
- When running MSL on EX platform, the option to restore from removable media or another running server are not available.
- MiCollab and MBG supports licensing through the Licenses & Services Application (SLS License Server). The Mitel Licenses & Services Application manages the software licensing and entitlement of the Software Assurance Program. After you obtain a ServiceLink ID or Serial ID from the SLS License Server, the SLS uses your ServiceLink ID to provide you with access to licenses, software releases, and upgrades

- To activate an SLS Serial ID the following connections must be allowed through any firewalls.
  - **FQDN**: sync.sls.mitel.com, **Current IP**: 18.200.183.29 **Port**: 22 **Protocol**: SSH
  - Customer must verify current IP before creating firewall rules as the IP address may be subject to occasional change.
- **Supported Upgrade Methods**: MSL 11.0 is available only as a 64-bit distribution. Migration from a 32-bit to a 64-bit system requires a fresh software installation, either manually or using the new Remote Fresh Install blade.
  - The application blade software is no longer downloaded from the AMC but the AMC still provides software licensing. MSL 11.0 uses the Mitel Software Download Center, supported by a global content distribution network to increase speed and reliability of downloads.

    The following outbound connections must be allowed through your firewall:

    License entitlement:

    - register.mitel-amc.com 216.191.234.91 port 22
    - sync.mitel-amc.com 216.191.234.91 port 22

    Access token for content delivery network:

    - swdlgw.mitel.com 99.81.17.20 port 443 (occurs during available blade software list update)

    Content delivery network for blade software download:

    - swdl.mitel.com port 443 (IP address based on location)

    Note:

    For the Akamai FQDN swdl.mitel.com, the static IP address ranges cannot be guaranteed by the Content Delivery Network. Thus, any firewall rules should allow the FQDN.

- The following table outlines the supported upgrade methods:

Upgrading from…	Upgrading To...	Supported Upgrade Methods

10.x releases (32-bit or 64-bit)	11.0 (64-bit)	Fresh Install from CD/DVD/USB Remote Fresh Install
9.x releases (32-bit)	11.0 (64-bit)	Fresh Install from CD/DVD/USB

Cloud Platform Support

The following features are supported on the Azure platform:

- **Hostname**: The default hostname will be the lower case VM name. Any invalid hostname characters, such as periods or underscores, will be translated to hyphens
- **Networking**: MSL supports auto-provisioning of network elements, such as NICs, public/private IP addresses, gateways, routing and DNS
- On every reboot, which includes following a restore operation, the VM networking is analyzed and auto-provisioned if any changes are detected.
- Supports auto-registration of the VM hostname in a private DNS zone linked to the virtual network of the primary (first) NIC. Only the primary (first) private IP linked to the NIC is registered. So, if the configuration console changes the hostname, the private DNS entry will be updated accordingly when the reboot occurs.
- Supports custom data when creating a VM.

Note:

Refer to Cloud Platform Support on page 5 for more details.

Backup and Restore using AWS S3 buckets

- Now, backups to the network file server and restoration of the backed up files stored in the network File Server can be processed using HTTPS through Amazon Web Services Simple Storage Service (that is, AWS S3).

Note:

Refer to the Backup and Restore sections under the Server Manager menu for more details .

3.2 MSL Release 10.6

MSL Release 10.6 provides the following new features:

- The audit logs in /var/log/secure have been enhanced to include entries for viewlogfile operations.
- You can now create multiple administrator accounts from the System Users panel. Additional admin accounts will have full server manager access.
- New installations will have the TLSv1.0 protocol disabled by default. The protocol can be enabled if required from the Web Server panel. Existing customers have the option to disable the TLSv1.0 protocol from the Web Server panel. It is not disabled by default on upgrade to this release.
- Two Mitel root CA certificates have been added to the Trust Store and are visible in the Certificate Authority Trust tab. The new Mitel root CA certificate is commonly known as Mitel Products Root CA and will be used in new products with release 10.6 and later.

3.3 MSL Release 10.5

MSL Release 10.5 provides the following new features:

- **Updates for MiCollab Implementations**:
  - The Install Applications tab in the MiCollab server manager has been changed to enable you to install and upgrade application software from removable USB devices in addition to the AMC.
  - The first time you access the Install Applications tab in the MiCollab server manager, you are prompted to select the type of PBX with which the server will interact. Support has been added for a new PBX type, the MiVoice Office 400.
  - The following options have been removed from the MiCollab server console menu: Upgrade MiCollab Software and Install MiCollab Software. All software maintenance must now be done in the MiCollab server manager on the Application Installation and Upgrade panel.
- **Syslog Enhancement**: MSL records event notification messages and sends these to a local syslog server. You can enhance this functionality by configuring the system to accept messages from remote hosts or send its own messages to remote hosts.
- **Web Certificate Enhancement**: When SSL certificates do not contain the proper chain of trust configuration, MSL will display an error message on the Manage Web Server Certificates panel.
- **AMC Synchronization Update**: The Enable Online Sync check box has been removed from the Status panel in the server manager. To switch to Online Sync mode from Offline sync mode, you must deactivate the ARID on the Status panel, clear the

Hardware ID in the AMC (you may need to contact AMC support to complete this task) and use the online procedure to reactive.

- **Supported Upgrade Methods**: MSL 10.5 is available in 32- and 64-bit distributions. Migration from a 32-bit to a 64-bit system requires a fresh software installation, either manually or using the new Remote Fresh Install blade. The following table outlines the supported upgrade methods:

<table>
<tr><th>Upgrading from…</th><th>UPgrading To...</th><th>Supported Upgrade Methods</th></tr>
<tr><td>9.x and earlier releases (32-bit)</td><td>10.5 (32-bit)</td><td>Fresh Install from CD/DVD/USB
Remote Fresh Install</td></tr>
<tr><td rowspan="5">10.0 releases (32-bit)
Fresh Install from CD/DVD/USB
Remote Fresh Install
Upgrade from CD/DVD/USB
ServiceLink
Fresh Install from CD/DVD/USB
Remote Fresh Install</td><td>10.5 (32-bit)</td><td>Upgrade from CD/DVD/USB
ServiceLink</td></tr>
<tr><td>10.5 (64-bit)</td><td>Fresh Install from CD/DVD/USB
Remote Fresh Install</td></tr>
<tr><td>10.0 SP1 (64-bit hybrid)</td><td>10.5 (64-bit)</td></tr>
<tr><td rowspan="2">10.1 and later releases (32-bit)</td><td>10.5 (32-bit)</td></tr>
<tr><td>10.5 (64-bit)</td></tr>
<tr><td>10.1 and later releases (64-bit full)</td><td>10.5 (64-bit)</td><td>Upgrade from CD/DVD/USB
ServiceLink</td></tr>
</table>

Consult your application documentation to confirm the exact upgrade steps you should follow. In some cases, you will be required to upgrade MSL before upgrading the application. In other cases, you will be required to upgrade the application software first.

3.4 MSL Release 10.4

MSL Release 10.4 provides the following new features:

- MiCollab Installation Improvement: The Install and Upgrade Applications panel has been changed to enable you to display application information for particular MiCollab software releases. Previously, information for all available releases was displayed, which sometimes resulted in delays obtaining updates from AMC.
- Data Encryption: You now have the option to encrypt MSL backups and log files using a symmetric cipher (256 bit AES in CBC mode). To use this feature, simply provide a password when performing a backup or saving a log file and the system will encrypt your data. The password must be entered again to decrypt the data.
- NTP Query Results: When you run a query to verify that the connection to your network time protocol server is configured, the status of the last eight NTP messages is presented in alphabetic format in the Reach field, with a "Y" indicating that a message was successful and an "X" indicating that a message was unsuccessful. Previously, this information was displayed as octet values, which was difficult to comprehend.
- PCI DSS Compliance: By default, MSL supports the use of early TLS (TLS v1) for communications security. To migrate to the latest TLS version, you must upgrade your client softphones and devices and then clear the Allow TLS v1.0 field on the Web Server screen. After these steps are complete, your system will be in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

3.5 MSL Release 10.3

MSL Release 10.3 provides the following new features:

- General Improvements:
  - Kernel Update: MSL 10.3 is based on CentOS 6.6, providing improved security and server compatibility
  - Full 64-bit version: MSL 10.3 provides a full 64-bit distribution for improved memory management. Migration from a 32-bit to a 64-bit system requires a fresh software installation, either manually or using the new Remote Fresh Install blade. The following table outlines the available upgrade methods:

Upgrading from…	Upgrading To...	Supported Upgrade Methods

9.x and earlier releases (32-bit)	10.3 (32-bit)	• Fresh Install from CD/DVD/ USB • Remote Fresh Install
10.0 releases (32-bit)	10.3 (32-bit)	• Upgrade from CD/DVD/USB • ServiceLink
	10.3 (64-bit)	• Fresh Install from CD/DVD/ USB • Remote Fresh Install
10.0 SP1 (64-bit hybrid)	10.3 (64-bit)	• Fresh Install from CD/DVD/ USB • Remote Fresh Install
10.1 and later releases (32-bit)	10.3 (32-bit)	• Upgrade from CD/DVD/USB • ServiceLink
	10.3 (64-bit)	• Fresh Install from CD/DVD/ USB • Remote Fresh Install
10.1 and later releases (64-bit full)	10.3 (64-bit)	• Upgrade from CD/DVD/USB • ServiceLink

Consult your application documentation to confirm the exact upgrade steps you should follow. In some cases, you will be required to upgrade MSL before upgrading the application. In other cases, you will be required to upgrade the application software first.

- MiCollab Installation Improvement: The Install Applications panel, which previously allowed only AMC software download, now provides the option to install or upgrade software from local media. In the future, this feature will be enhanced to enable local downloads from a network share or USB drive.
- SFTP Restore: Since MSL 10.0, it has been possible to perform network backups to Linux servers that support secure FTP (SFTP). However, to restore an SFTP backup, users had to copy it to a removable device such as USB key, and then select the "Restore" from Backup option from the server console. With MSL 10.3, it is now possible to restore an SFTP backup directly from a network file server.

- Virtual Environment Enhancements:
  - If you are deploying to VMware vCenter server, you can now configure the MSL settings (such as the DNS and interface IPs) as part of the initial OVF deployment. This eliminates the need to use the server console for this purpose.
  - You will be forced to change the administrator password the first time you power on a system in a VMware environment. This requirement ensures that any password information stored in the virtual appliance cannot be used to access the server.
  - The Mitel Virtualization Tool now includes a Storage Monitoring utility that you can use to detect file system errors and take corrective action such as issuing an email notification or rebooting the system.
- Security Enhancements:
  - To address security vulnerabilities, MSL will distribute security patches through the Blades panel. You will be notified by Mitel Product Support whenever a new patch is available.
  - Increased protection against dictionary-based attacks, and enhanced cookie security.
  - To facilitate client access to MSL, you can now import third-party SSL certificates in PKCS#12 format as well as PEM format.
- Performance Enhancements (invisible to users):
  - The Linux CFS process scheduler has been returned to maximize CPU utilization and improve voice quality performance.
  - To prevent LDAP file system corruption in the event of an unexpected shutdown, the backend database has been configured to use shared memory rather than files.

3.6 MSL Release 10.1

MSL Release 10.1 provides the following new features:

- Both MSL 10.1 and MSL 10.0 SP2 are based on CentOS 6.5. The MSL 10.1 release is available in i686 (32-bit kernel, 32-bit user space) and x86-64 (64 bit kernel and user space) versions. CentOS 6.0 is required to ensure compatibility with recently released hardware servers.
- Integration with Hosted and Cloud-based Systems: Support for the OAuth 1.0 protocol has been discontinued with the release of MSL 10.1. If you are currently using OAuth 1.0 and upgrade to the latest MSL software, you should reprogram API access for your application using an OAuth 2.0 Service Account. After you have done this, the OAuth 1.0 tab will be removed from the server manager interface. If you are installing new software (including install/database restore) only OAuth 2.0 is available for configuration.

- Web Services: MSL supports the Web Services framework, a Representational state transfer (REST) API that enables management integration through the Oria Provisioning Portal.
- Networking enhancements:
  - IPv6 in IPv4 Tunnel: The MSL Server Manager has a new screen which enables you to encapsulate IPv6 packets for transmission across an IPv4 network such as the internet. The screen also allows you to program the external interface of the tunnel with an IPv6 address, which allows it to be addressable by IPv6 traffic on the internet. Both of these functions require the MSL server to be operating in server-gateway mode.
  - Trusted networks and network routes: The “Local Networks” screen in the MSL Server Manager has been renamed “Networks” and now allows you to add trusted networks and routes for both IPv4 and IPv6 protocols. You may define subnetworks using either a subnet mask or a prefix in CIDR format.
  - Remote Management: You can now configure remote access and secure shell (SSH) settings for both IPv6 and IPv4 networks.
  - Default Gateway: It is now possible to specify an IPv6 default gateway address when you originally install and configure the MSL software using the server console.
- Event/alarm notification has been added to top of the MSL Server manager interface.
- Most of the Mitel product portfolio has been rebranded. These changes are reflected as follows on the MBG interface:

Old Product Name	New Product Name
5000 Communications Platform	MiVoice Office
Mitel Communications Director	MiVoice Business
MiCollab	MiCollab
NuPoint Unified Messaging	MiCollab NuPoint Unified Messaging
Speech Auto Attendant	MiCollab Speech Auto Attendant
Mitel Collaboration Advanced	MiCollab Audio, Web and Video Conferencing

Unified Communicator Advanced	MiCollab Client
Unified Communications Advanced Mobile	MiCollab Mobile Client
Unified Communications Server	MiCollab Client Service
Mitel Border Gateway	MiVoice Border Gateway
Unified Communicator 360	MiVoice Conference Unit
Mitel Enterprise Manager	MiVoice Enterprise Manager

3.7 MSL Release 10.0

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/CIFS 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 Contacts 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.

3.8 MSL Release 9.4 SP1

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.

3.9 MSL Release 9.4

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 be 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- 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.

3.10 MSL Release 9.3

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 the re-sync interval (24 hours by default), a Major alarm is raised.

Offline Sync: 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.

3.11 MSL Release 9.2

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.

3.12 MSL Release 9.1 SP1

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>.

3.13 MSL Release 9.1

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 MiCollab Panel: For MAS deployments only, MSL now provides a dedicated menu in the server console for updating the MAS application.

Accessing the MSL Qualified Hardware List

4

Effective June 30, 2019, Mitel discontinued testing and documenting compatibility of specific server hardware models with Mitel Standard Linux (MSL) and making recommendations. Refer to the *Hardware Compatibility* section in this guide to select the hardware to run your MSL based applications.

Licensing 5

This chapter contains the following sections:

This section provides instructions on how to assign licenses to the system via the **AMC** and the **Mitel Licenses & Services Application (SLS Licenses Server)**.

MiCollab and MBG solutions are licensed as a base package with a series of optional, add-on application user packages and system feature options. There are several base packages available depending on the required deployment model. Add-on user packages allow the licensed number of users to access the base package functionality.

5.1 About Licensing

AMC Licensing

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.

5.2 Request 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.

5.3 SLS Licensing

MSL supports licensing through the **Licenses & Services Application** (SLS License Server) for MiCollab and MBG Solutions with MiVoice MX-ONE, MiVoice Office 400 and MiVoice 5000. The Mitel Licenses & Services Application manages the software licensing and entitlement of the Software Assurance Program. After you obtain the ServiceLink ID or Serial ID from the SLS License Server, the SLS uses your ServiceLink ID to provide you with access to licenses, software releases, and upgrades.

The Mitel Licenses & Services Application allows licensing keys to be automatically created at all times (24 hours a day, 7 days a week) through remote license keys generation. The Licenses & Services Application is also the procurement and provisioning interface for SLS-delivered products and services.

As a reseller of Mitel products, you receive a unique licensing account on the Licenses & Services Application. By logging in to the Mitel Licenses & Services Application with the username and password via the MiAccess Portal, you are given when you obtain your account, you can view a list of your SLS-enabled products, check their status, and add services to any of them. When you place a new order for products, the order information is entered into the Mitel Licenses & Services Application which can be accessed through the MiAccess Portal. The SLS places the purchased licenses into your licensing account for use in creating a record.

To create a record in the SLS License Server:

- Select/Find Voucher
- Register voucher including SWA

You must install MiCollab and then register it with the License and Services Application online. When you install MiCollab, MSL generates a unique Hardware ID of the server. When you connect to the License and Services Application over the Internet, MSL uses the Hardware ID and the ServiceLink ID/ Serial ID to communicate with the SLS to obtain licensing information (also called sync).

Accessing your License Server Account

To access your account for the first time:

Pre-requisites:

- MiAccess user account

- MiAccess privilege to access Licenses & Services. The MiAccess privileges includes:
  - **Application access** - This is read only access
  - **License Manager** - includes voucher registration tasks
  - **Upgrade Manager** - includes release upgrade
  - **Service Manager** - includes SWA renewal and export of licensed product list

1. Go to the Mitel web site (http://www.mitel.com) and log in to your **Mitel MiAccess** account.
2. From the left menu, click **Licenses & Services**.
3. In the Home page, under the **License Bank** tab, you can access the license vouchers.

5.4 Access your AMC Account

To access your account for the first time:

1. Log in to yourMitel MiAccessaccount.
2. From the left menu, click**Licenses & Services AMC**.
3. From the drop-down, select**Add a newLicenses & ServicesAMC login**.
4. Enter your**User ID**and**Password**.
5. Click**Login**. For information about using the AMC, click the Online Help link in your AMC account.

5.5 Requesting a new SLS License Server Account

To request account, send an e-mail to **Mitel MiAccess Support**(MiAccess.support@mitel.com). Every partner or organization account by default has access to Licenses & Services Application in the MiAc-cess portal. In order to get access to **Licenses & Services application** (SLS license server), the following is needed:

- An active MiAccess user account
- MiAccess privilege to access Licenses & Services

5.6 Find More Information

To access documentation/software from the Internet:

1. Log in to your **Mitel MiAccess** account.
2. On the left menu, do one of the following:

   a. Click **eDocs** to access product documentation.
   b. Click **Software Download Center** to access MSL software.

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

Installing the Hardware 6

This chapter contains the following sections:

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. Note that future applications from Mitel may be certified and supported only on specific hardware platforms that provide the requisite speed and performance.

6.1 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.

To test server memory before installing MSL, or to debug possible memory problems, see Troubleshooting on page 115.

6.2 Hardware Compatibility

In order to assist partners and customers to select the hardware to run their MSL based applications on, Mitel publishes the following table showing the CentOS version that their MSL is based upon.

MSL Version	CentOS Version
10.6.23.0	6.10
11.0.50.0	7.6

MSL Version	CentOS Version
11.0.60.0	7.7
11.0.79.0	7.9

6.3 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 104.

6.3.1 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.

6.3.2 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.

6.3.3 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.

6.3.4 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.

6.3.5 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 in your Mitel MiAccess account.

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 MiAccess.

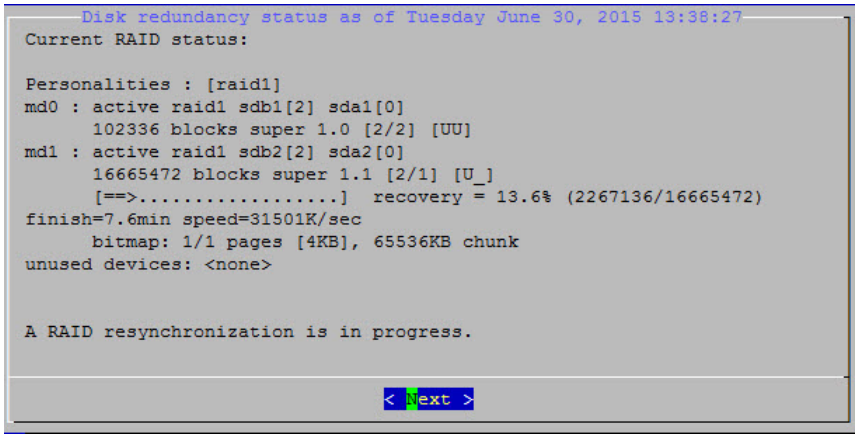
6.3.6 Test the RAID Configuration

Prior to deploying the system, you can test the MSL software RAID configuration to confirm that the system can operate with only one disk.

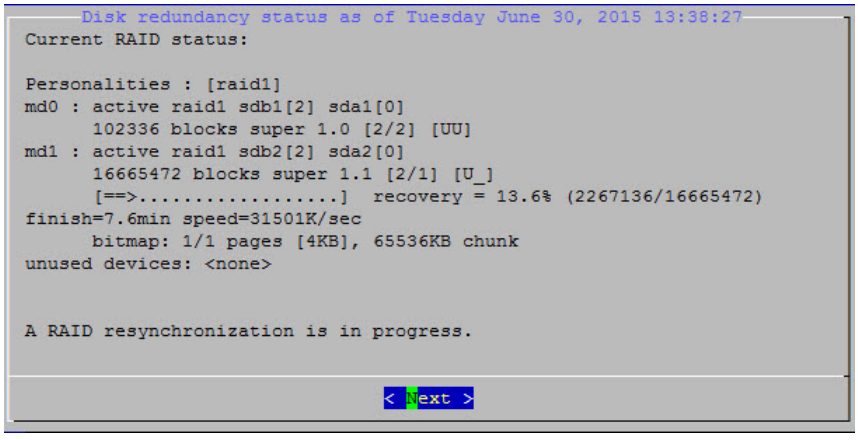
To test the RAID configuration before deployment:

1. Access the server console and log in as "admin".
2. From the console, select the option to **Reboot**, reconfigure or shut down this server.
3. Select **Shutdown** and press **OK**.
4. Remove or disconnect one of the two drives.
5. Restart the system and allow it to fully boot.
6. From the console, select the option to Reboot, reconfigure or shut down this server.
7. Select **Shutdown** and press **OK**.
8. Reconnect the disconnected drive and disconnect the other drive.
9. Restart the system and allow it to fully boot.

10. From the console, select the option to Reboot, reconfigure or shut down this server.
11. Select **Shutdown** and press **OK**.
12. Reconnect the disconnected drive. (Both drives should now be connected.)
13. Restart the system and allow it to fully boot.
14. From the console, select the option to **Manage disk redundancy**.
15. Select **Yes** to activate the unused disk and begin the RAID resynchronization process.



16. Click **Next** to return to the console menu.
17. Wait for a few minutes and select the option to Manage disk redundancy. If synchronization is complete, the screen will indicate that “All RAID devices are in clean state.” If it is incomplete, exit the screen and continue waiting. Depending on the amount of data stored to disk, the synchronization process may take 15 minutes or longer. Accordingly, you may need to exit and re-access the screen several times. (Note that the screen is not updated automatically.)



18. After you receive the message that “All RAID devices are in clean state,” click **Next** to return to the console menu.
19. Click **Exit** from the server console. The system is ready to be deployed.

Installing MSL Software 7

This chapter contains the following sections:

Installation of MSL consists of the following tasks:

- Collect Site Information (this page).
- Read Installation Notes on page 22.
- Create Application Record on page 23.
- Obtain MSL software on page 23.
- Install MSL Software page 24.
- Configure MSL on page 26.
- Launch the Server Manager on page 44.

7.1 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 punctuationcharacters, and that is not a dictionaryword.	

Item		Notes	Your Information
2	Domain Name	Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 26.	
3	System Name		
4	IP address of your MSLserver	The local, static IP address of the serverwhere you are installing MSL.	
4b	IP address of your external NIC(s)	The IP address of your external Ethernetconnection.	
4c	Alias IP for your externalNIC	A second, alias IP address used forapplications that require a server with twoIPs (like Audio, Web and VideoConferencing)	
5	External Interface Connection	Cable Modem? You need to know if the ISP requires an Account Name OR an Ethernetaddress as identification in DHCP requests	
		DSL Connection? You need to know theusername and password for authentication	
		Direct Connection? You need to know the static IP address	
6	Gateway IP Address	The IP address that your MSL server willuse to access the network.	
7	DNS Server IP Address	Enter the IP address of your corporate DNS server. Note: If your DNS is supplied byyour ISP, leave this setting blank.	

Item		Notes	Your Information
8	Application Record ID #	The number generated when you created an Application Record ID for this product in your AMC account.	
“Trusted Network” Access If your ICP or some of your users are not on the same subnet as the MSL server, you need to classify them as "Trusted Networks" and then allow them access. Both IPv4 and IPv6 networks are supported.			
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 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.	

7.2 Installation Notes

- If you are performing a fresh install, see Install MSL Software on page 24.
- If you are upgrading from a previous release of MSL software, see Upgrading MSL Software MSL Software on page 31.

7.3 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.

7.4 Obtain MSL Software

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

7.4.1 Download Image from Mitel MiAccess

To download an ISO image of MSL software:

1. Log on to Mitel MiAccess.
2. Click **Software Download Center** from the left panel.
3. Click the name of the application software or use the **Search downloads by name** field to find the 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.

7.4.2 Copy Image to CD or DVD

For 32-bit installations of MSL, use a CD. For 64-bit installations of MSL, use a DVD.

To build a CD or DVD from the downloaded ISO image:

1. Insert a CD or DVD disc 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/DVD burning software builds the CD or DVD.

Note: The .iso file must be written as an image and not as a file.

7.4.3 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.

7.5 Install MSL Software

The following procedure describes how to install MSL software to a workstation from a CD/DVD 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 on page 104 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/DVD 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**. If you are installing from CD or DVD, 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.

7. If you do not have a previous version of MSL software, you are offered an Install option. Click Yes and proceed to Step 9. If you do have a previous version of MSL software, you will be prompted to perform an upgrade; see Upgrading MSL Software on page 31 for more information .
8. 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.
9. Choose your Time Zone from the list.
10. 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.
11. A log of the installation is created and stored in /root/install.log.
12. 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.

7.6 Configure 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.

7.6.1 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 106.

7.6.2 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.

7.6.3 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.

7.6.4 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).

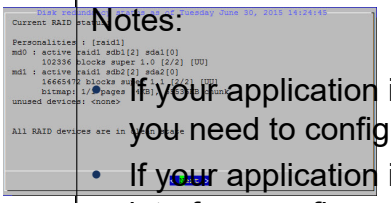
7.6.5 Select Local Network Adapter

- 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.

7.6.6 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.

Note: If you want to disable serving IP addresses from the local range for the local subnet, set a value of zero for the lease time to disable that local range.

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.

7.6.7 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.)
Trusted Networks	IPv6 network addresses are supported.
SSH access	IPv6 access supported.
Review Configuration	Displays IPv6 configuration.
Remote Management access	IPv6 access supported.
Default Gateway	IPv6 network addresses are supported.

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

7.6.8 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.

7.6.9 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.

7.6.10 Select Gateway IP Address

For Internet access:

- Enter your default gateway (router) IPv4 or IPv6 address.

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

7.6.11 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 Audio, Web and Video Conferencing, which require two different addresses on the same server.

7.6.12 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 96 for more information).

You have now provided all information required for MSL configuration.

7.6.13 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 MiCollab.)

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

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

Upgrading MSL Software 8

This chapter contains the following sections:

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 using one of the following procedures:

- Upgrade with CD/DVD/USB—page 31
- Upgrade with ServiceLink—page 31
- Upgrade with Remote Fresh Install Blade—page 32

8.1 Upgrade with CD/DVD/USB Media

You can download the MSL operating system software as an ISO file from Mitel MiAccess, and then copy it to physical media for installation on the server. You can then use it to perform either a "minor" or "major" software upgrade:

- Minor software upgrade: If you are performing a minor software upgrades (for example, upgrading from 9.x to 9.x) you can simply insert the media into the server, boot from the appropriate drive, and select the "upgrade" option during the installation process. Although configuration and application data is maintained, a backup is recommended.
- Major software upgrades: If you are performing a major (for example, upgrading from MSL 9.x to MSL 10.x) you must perform a fresh software. This entails backing up the database, installing the new MSL version from a CD/DVD or USB flash, and then restoring the database.

For more information on upgrading with CD/DVD/USB, 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 un-mounted 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.

8.2 Upgrade with ServiceLink

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.

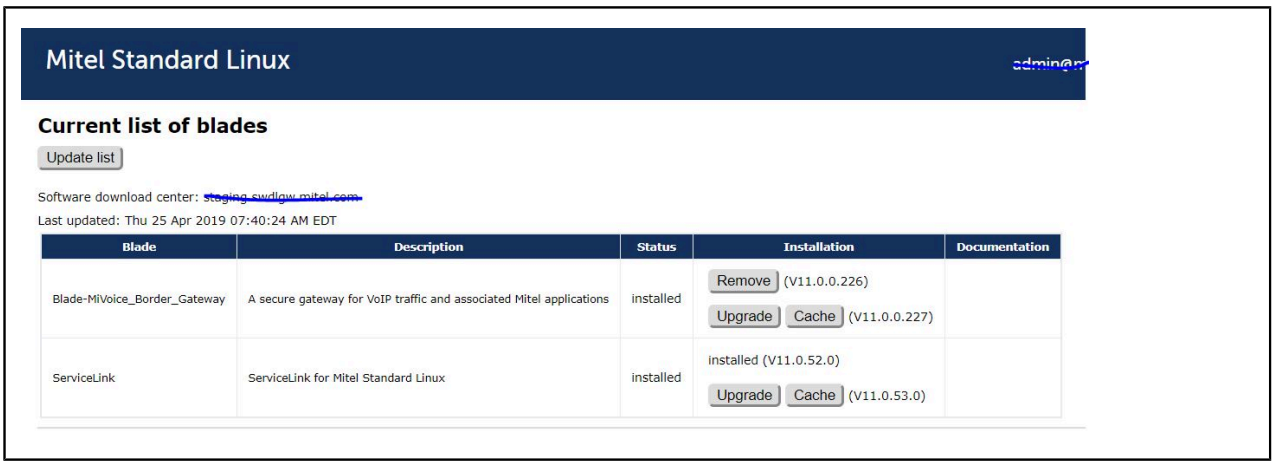


Figure 4: ServiceLink option in Blades Panel

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.

8.3 Upgrade with Remote Fresh Install Blade

You can upgrade a physical servers running MSL 10.x to MSL 11.x or later 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 51.
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.

1. In the server manager, under Administration, click Shutdown or reconfigure, select Reboot and then click Perform.
2. 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 108.
3. Select the option to Register for Service Link to perform a sync with the AMC.
4. Reinstall your application software.

Upgrade from a Previous Version and add 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.

Installing Software Blades 9

This chapter contains the following sections:

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

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

To obtain the software entitlements for your server ARID any firewalls must allow outgoing ssh connections on port 22 to the Mitel Applications Management Center (AMC), blades.mitel-amc.com with static IP: 216.191.234.91.

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

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

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

9.1 Security Software Patch Installation

Periodically, you will be informed by Mitel Product Support that a software patch is available which addresses a security vulnerability. You can download and install the patch from the Blades panel.

Virtualization 10

This chapter contains the following sections:

10.1 Overview

A variety of MSL-based applications, including MiCollab, NuPoint UM, MiCollab Client and MiVoice Border Gateway, can be can be run as virtual appliances in a VMware vSphere or Microsoft Hyper-V environment. For a list of supported applications, please refer to the Virtual Appliance Deployment Guide available at Mitel MiAccess.

10.1.1 Requirements for Virtual Deployments

- For a list of supported servers, refer to the hardware compatibility guides provided by VMware and Microsoft.
- For information concerning hardware and software requirements, deployment considerations, supported features, and configuration guidelines, refer to the Virtual Appliance Deployment Guide available at Mitel MiAccess.
- For additional product-specific restrictions and requirements, plus host and storage performance guidelines, refer to the Mitel application-specific Engineering Guidelines documentation available at Mitel MiAccess.

10.1.2 Software for Virtual Deployments

VMware

For virtual deployments in a VMware environment, MSL software is packaged with the application software and delivered as an OVA file which can be installed on a vSphere client using the Deploy OVF Template wizard. OVA files for the various applications can be downloaded from Mitel MiAccess.

Software updates can be delivered in one of three ways:

- ServiceLink updates through the MSL Server Manager Blades panel (for most applications except MiCollab)
- Server manager Install Applications panel (MiCollab and MiVBX)
- Deploy a new OVA image (for all applications)

Hyper-V

For virtual deployments in a Hyper-V environment, you use the same MSL and application ISO images as for installing during the physical procedures, but you must still purchase the virtual version of the license for the Mitel products.

Software updates are also handled like a physical implementation. For minor release and service pack upgrades, use the Blades panel. For major releases, you must perform a fresh install and restore a product-specific backup. Prior to performing an upgrade, you can clone the virtual appliance or take a snapshot to serve as a backup.

10.1.3 Licensing for Virtual Deployments

When a virtual appliance is powered up, you are prompted to enter your Application Record ID (ARID), just as it would with a physical server. When the AMC receives a virtual appliance ARID, it responds with a Globally Unique Identifier (GUID) for the appliance. The GUID is stored in the database of the virtual appliance and used when performing regular synchronization with the AMC.

If a virtual appliance is upgraded by deploying a new OVA, MSL backup and restore procedures must be used to maintain the GUID and to ensure continued synchronization with the AMC. If the GUID is not maintained, you will need to contact the AMC and have it reset.

The GUID in the virtual environment serves an equivalent purpose to the Hardware ID in the physical environment.

Note: The server hosting the virtual appliance must have continuous Internet access (for both licensing and for application use).

10.2 VMware Implementations

10.2.1 VMWare: Installation

Installation consists of the following tasks:

1. Collect site information
2. Create Application Record
3. Download .ova file from Mitel MiAccess
4. Deploy the virtual appliance
5. Configure MSL
6. Configure the application

Note:
Steps 1-2 and 5-6 are the same for both physical and virtual installations and will not be repeated in this procedure.

Download the OVA File

Download the applicable .ova file from Mitel MiAccess:

1. Launch a web browser on the vSphere Client PC.
2. Log in to Mitel MiAccess.
3. Click Technical and then click Software Downloads.
4. Click the appropriate application name and version for the software you want to install.
5. Review the application Release Notes.
6. Click the appropriate link to download the .ova file.
7. If you agree to the software disclaimer, click “I agree [Download using Software Download Manager]”. (On initial use, you will have to install the Download Manager application.)
8. Save the .ova file to a folder on the vSphere Client PC.

Note:
Some applications, such as NuPoint Unified Messaging, require installation of additional .iso files for optional software.

Deploy the Virtual Appliance in VMware

The .ova file you downloaded from Mitel MiAccess contains the MSL operating system, the application software, and VMware Tools (a suite of utilities to enhance performance).

To deploy the virtual appliance on a vSphere host:

1. Launch the vSphere Client on the network PC:

   a. Click **Start** > **All Programs**.
   b. Click **VMware** > **VMware vSphere Client**.
   c. Enter the hostname or IP address of the Hypervisor ESX/ESXi host server. **OR**

   a. Enter the hostname or IP address of the vCenter Server.
   b. Enter your username and password.
   c. Click **OK**.
2. In the vSphere Client application, click File > Deploy OVF Template. (The .ova file you downloaded is a template file in OVF format.)
3. In the Deploy OVF Template screen, specify the storage location of the .ova file you downloaded.
4. Specify the Source Location for the OVF template file (.ova file extension):

   - To deploy from a file on the local PC or from a network share, click Browse and navigate to the file.
   - To deploy from a URL (if the file is on the Internet or is accessible through a web browser) enter the URL of the file location.
5. Click Next. The OVF Template Details screen appears. The information shown is derived from the .ova file to provide a “check” for correct application and version. Note that the Download size is only an estimate until a deployment configuration is selected later in the process.
6. Click Next. The End User License Agreement screen appears.
7. Click Accept to accept the end-user license agreement, and then click Next. The Name and Location screen appears.
8. Enter a meaningful name for the virtual appliance, or accept the default name, and then click Next. The Deployment Configuration screen appears.
9. Select the resource profile that best matches your site. For example, MiCollab offers “Small Business” for up to 150 users, “Mid-Range” for up to 2500 users, or “Enterprise Multi-application” for up to 5000 users. Your selection determines the hardware resource requirements. Click Next. The following three steps are dependent on your configuration.
10. If you are using the optional vCenter Server, select the appropriate Host/Cluster for this deployment and then click Next.
11. If you are using the optional vCenter Server, select the appropriate Resource Pool for this deployment and then click Next.
12. If multiple Datastores are available, select the Datastore for the vNuPoint instance, and then click Next. The Disk Format screen appears.

13. In the Disk Format screen, select a provisioning format:

    - Thick provision Lazy Zeroed
    - Thick provision Eager Zeroed
    - Thin provision

    Click Next. The Network Mapping screen appears.

14. Configure the network mapping. (This screen is only displayed if the network defined in the OVF template does not match the name of the template on the host to which you are deploying the virtual application.) The required settings are dependent on your deployment configuration:

    - Network Edge (Server-Gateway) Mode: In this configuration mode, the server functions as a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the internal network (LAN) while the other is connected to the external network (Internet). Select the destination LAN and WAN networks for the OVF template. These are the "Associated Networks" that are assigned in the LAN and WAN IP Pools. You must assign the LAN and WAN destinations to different networks.
    - LAN Only (Server-only) Mode: In this configuration mode, the server is only connected to the internal network (LAN). For this mode, only select a destination LAN network for the OVF template.
    - LAN (Optional): This interface can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.

    Contact your Data Center administrator for more details on which Network Mapping to use.

15. Click Next. If you are deploying on vCenter, the Properties screen appears. You can use this screen to configure the MSL operating system parameters. Complete the fields in this screen using the information that you have collected. Mandatory fields are highlighted with a red border.

    - You must specify both the LAN IP and WAN IP addresses. Otherwise, the virtual appliance will not power on. If you are deploying the virtual machine in LAN only (server-only) mode set the WAN IP address to 0.0.0.0.
    - For Network Edge deployments, ensure that the LAN IP and WAN IP addresses are on different subnets and the Gateway IP address is on the subnet of the WAN IP address.
    - You can only use this screen to set the LAN IP and WAN IP addresses for the initial deployment of the appliance. After initial boot-up, you must use the MSL server console interface to modify the LAN IP or WAN IP addresses.

16. Click Next. The Deploy OVF Template Ready to Complete screen appears.
17. If you are using the optional vCenter Server and you are installing MiCollab with Voice, you are prompted to enter MSL configuration information such as the Admin password

and networking properties. (Other applications will take advantage of this feature in future releases.)

18. Click Next to display your deployment settings.
19. Review the information and then click Finish. vSphere deploys the virtual appliance on the server. A progress bar is displayed.
20. When deployment is complete, click Close. The new virtual machine appears in the inventory list in the left-hand pane.

Power On the Virtual Appliance

1. In the vSphere client, right-click the virtual appliance name and then click Power > Power On (or click the Power On icon).
2. Right-click the virtual appliance name again and click Open Console. The MSL server console opens and displays the MSL boot up screens.
3. Application configuration and any additional MSL configuration (if required) is performed in exactly the same way as for a physical server installation.

10.2.2 VMware: Access the Server Manager and Update the Admin Password

For increased server access security when installing virtual appliances, users will be prompted to change the administrator password the first time they use the MSL server manager to access the system. This update ensures that the original password information stored in the virtual appliance cannot be used to access the server.

1. Power On the Virtual Appliance (see above).
2. Access the MSL server manager:

   a. Open a web browser on the local network.
   b. Enter the URL: http://<IP_address_of MSL server>/server-manager.
3. The Change Account Password dialog appears. Enter your old and new passwords, verify your new password, and then click Change Password.

Note:
If desired, you can cancel out of the dialog and use the original administrator password to access MSL. However, the next time you log in through the server manager, you will again receive a prompt to update the password.

10.2.3 VMWare: Backup

To back up the VMware virtual appliance, use the same methods that you would use for a physical server. An MSL backup is required if you are deploying a new OVF, or if you are migrating from a physical to a virtual deployment.

Most application-specific backups, such as the NuPoint UM backup procedure, are also supported. (Note that the NuPoint UM backup does not back up MSL configuration or ARID information. See the NuPoint documentation for backup instructions.)

VMware also supplies optional backup tools including:

- vStorage API for Data Protection (vADP): APIs that third-party backup utilities can use to backup/restore from a central backup server
- VMware Data Recovery: a vCenter plug-in that enables disk-based backup and restore

Note:
VMware snapshots are not supported as a backup method.

All virtual appliances can also be backed up by exporting an OVF template of the virtual appliance. The template is a copy of the virtual appliance in .ova format. To restore the virtual appliance, you deploy the exported OVF file to the vSphere platform.

Check the training material and/or documentation for your application to see which methods are supported/recommended.

Export an OVF Template

To export an OVF Template:

1. In the vSphere client, right-click the virtual appliance name and select Shutdown Guest.
2. Click File > Export > Export OVF Template.
3. Enter the name of the OVF template file and the directory where you want to save it.
4. Select one of the following options:

   a. Physical Media (OVA): to export a single .ova file (recommended)
   b. Web: exports multiple files

5. Select one of the following Format options:

   a. Single File (OVA): to export a single .ova file (recommended)
   b. Folder of Files (OVF): exports multiple files
6. Click OK. MSL automatically configures the NIC address for the new virtual machine.

Note:
For virtual machines with multiple NICs, automatic NIC addressing is not guaranteed. If your virtual machine has multiple NICs and does not function correctly after the OVF export, we suggest that you select the server console option “Configure this Server” to manually configure the NIC addresses.

10.2.4 VMWare: Convert from Physical to Virtual

This task list presents the general steps required to upgrade your virtual machine. For detailed instructions, refer to the Installation and Maintenance Guide for your application.

Notes:

- Ensure that conversion is supported for your deployment configuration BEFORE you begin.
- Conversion requires a service outage and should be scheduled for off hours.

To convert from physical to virtual:

1. Purchase the required “Server to Virtual” licensing and apply it to the Application Record. Make a note of your Application Record ID.
2. If you are converting from MSL 9.2 to 9.3 or later, request a reset of the Hardware ID. (Not required for conversion between two 9.3 or later systems.)
3. Download the latest .ova file from Mitel MiAccess.
4. Deploy the virtual appliance but do not power it up.
5. Back up the physical server using the method recommended in the application documentation.
6. Shut down the physical server, launch the vSphere Client, and power up the virtual appliance.
7. Open the virtual appliance console and, when prompted to “Restore from Backup?”, select Yes.
8. If converting from MSL 9.2, when the restore is complete, access the MSL server manager and click Status. Deactivate and reactivate the ServiceLink so it matches the new AMC GUID. (This step is not required for conversion between two systems that are both running MSL 9.3 or later.)

10.3 Hyper-V Implementations

Deploying Hyper-V involves creating a Virtual Machine (VM) with the correct resource allocation to support the installation of the particular Mitel virtual application. This section provides an overview of the steps for creating the Hyper-V virtual machine on which you can install the Mitel virtual applications. For detailed instructions, refer to the Virtual Appliance Deployment Guide available at Mitel MiAccess.

10.3.1 Limitations

- Hyper-V virtual machines that run Mitel Standard Linux (MSL) do not support connection of USB devices. Accordingly, the MSL software installation must be performed from the CD/DVD-ROM drive.
- Mitel software must be installed using traditional physical ISO images available from Mitel MiAccess. OVA images cannot be used. After creating the virtual machine, use the ISOs to install the MSL operating system and application software as you would on a physical system.
- Once the software has been installed and licensed, Hyper-V must maintain online connectivity to the AMC and is subject to the same Sync Expiry rules in place for VMware-based deployments.
- To achieve the same performance as VMware, a Hyper-V virtual machine requires twice as many virtual processors.

10.3.2 Hyper-V: Installation

Installing the Mitel application on Hyper-V consists of the following tasks:

1. Create the virtual environment.
2. Install and configure Mitel Standard Linux (MSL) on the virtual machine.
3. Install the Mitel virtual application on the virtual machine.

Create the Virtual Environment

When configuring the virtual environment, adhere to the following guidelines:

- Configure the Guest Hardware with the number of processors, amount of memory and disk size specified in the Virtual Appliance Deployment Guide and the Engineering Guidelines for the application you are installing.

- Recommended settings:
  - Select CentOS Linux 6 (32 bit) as the operating system.
  - Set Virtual Machine Type to Generation 1.
  - Set the CPU priority to High for the voice-sensitive Mitel applications. Lower settings can be used for the other applications.
  - Connect a new Virtual Hard Disk (fixed and correct size).
  - Add the disk to the IDE Device.
- Configure an additional NIC if the Mitel application is being deployed in server-gateway mode. See the Virtual Appliance Deployment Guide for details.
- Before starting the virtual machine and before MSL is installed, modify the Virtual Machine to match resource requirements specified in the Virtual Appliance Deployment Guide for the application you are installing. For example, allocate four vCPUs to a MiCollab implementation.

Hyper-V: Install Mitel Standard Linux

Installing the MSL operating system in Hyper-V is identical to installing it on a physical server. The only limitation is that you can mount the ISO image from a network drive or CD/DVD, but not from a USB device. For instructions, see Install MSL Software.

Hyper-V: Install the Mitel Application

Installing Mitel virtual applications in Hyper-V is very similar to installing on a physical server. For Hyper-V installations, you use the same MSL and application ISO images as for installing during the physical procedures, but you must still purchase the virtual version of the license for the Mitel products. Optional application software can be installed from the Blades panel of the MSL server manager or from an ISO image.

Refer to the installation documentation for the specific Mitel product on Mitel MiAccess for detailed instructions for installing the appliance on a physical server.

10.3.3 Hyper-V: Upgrade

Hyper-V virtual machines are upgraded similarly to physical servers. You will need to upgrade MSL and the application together. You can clone or snapshot the VM as a backup before upgrading.

- For minor release and service pack upgrades, use the Blades panel.
- For major releases, perform a fresh install and restore a product-specific backup.

Server Administration and Maintenance

11

This chapter contains the following sections:

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 102.)

11.1 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:

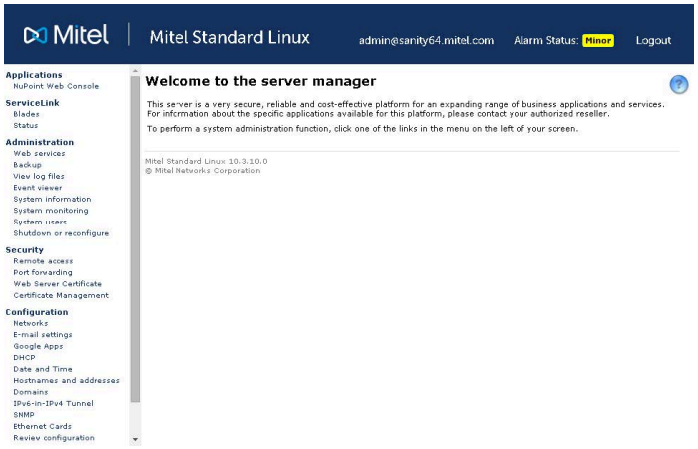
- Remote access to the server manager is only possible via an encrypted connection, using SSL (https).
- By default, the server manager is accessible only from the local network. To extend access privileges to other networks, you must program them. Do this while you are physically connected to the local network. For details, see Remote Managementon page 65 and Networkspage 67.
- You should allow access only from local and remote management networks, not from the public network (entire Internet). For details, see SSH Settingson page 66
- Server Manager login is protected from brute force password attacks. By default, six consecutive failed login attempts within a 10-minute period locks out the IP address of the client for 30 minutes.

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

Figure 5: Server Manager



11.2 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	71

Section	Menu Item	Use this option to...	For more info, see page
	Install Applications	• select the PBX Type with which the MiCollab server will interact (upon first accessing the screen) • view current list of MiCollab applications, services and security patches • install new software and upgrade existing software online or a removable USB/DVD device See the MiCollab online help for more information.	N/A
	Status	view ServiceLink status for this server provided by the AMC	73
Administration	Web Services	MSL includes a Representational state transfer (REST) API that supports the features and functions currently available in the traditional Mitel administrative interfaces. Do not update the settings on this panel.	83
	Backup	backup server configuration data (and application data)	76
	Restore	restore server configuration data (and application data)	80
	View log files	view or download log files generated by the services running on this server	82
	Event viewer	view the current alarm status of the system and a list of recent events	85

Section	Menu Item	Use this option to...	For more info, see page
	System information	view (and control view access) of networking parameters, server, and domain information	87
	System monitoring	view (and control view access) for system monitoring	88
	System users	add, edit, or delete user accounts for users who may access the MSL server	88
	Shutdown or reboot	reboot, reconfigure, or shutdown your system	92
Security	Remote Access	review and configure remote access settings (for example, PPTP and SSH)	92
	Port forwarding	use to modify your firewall rules to provide port forwarding (For server-gateway configurations only.)	96
	Syslog	configure the syslog server to accept events from remote hosts, or send events to remote hosts	96
	Web Server	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 use to enable/disable support for TLS version 1	98

Section	Menu Item	Use this option to...	For more info, see page
	Certificate Management	manage client certificate signing requests.	98
Configuration	Networks	grant trusted local access privileges to other IPv4 and IPv6 networks	113
	Email Settings	configure SMTP settings	117
	DHCP	manage/configure the MSL DHCP server	121
	Date and Time	enable/configure network time server	124
	Hostnames and Addresses	view/add hostnames if using the MSL server as a DNS server.	126
	Domains	view/manage virtual domains and corporate DNS settings.	127
	SNMP	configure SNMP support for remote management/monitoring	129
	Ethernet Cards	configure the speed and duplex settings for the Network Interface Cards	131
	Review configuration	view networking parameters, server, and domain information	132
Miscellaneous	Support and licensing	view the MSL License Agreement (EULA)	-

Section	Menu Item	Use this option to...	For more info, see page
	Help	access online help for MSL configuration	-

11.2.1 Blades

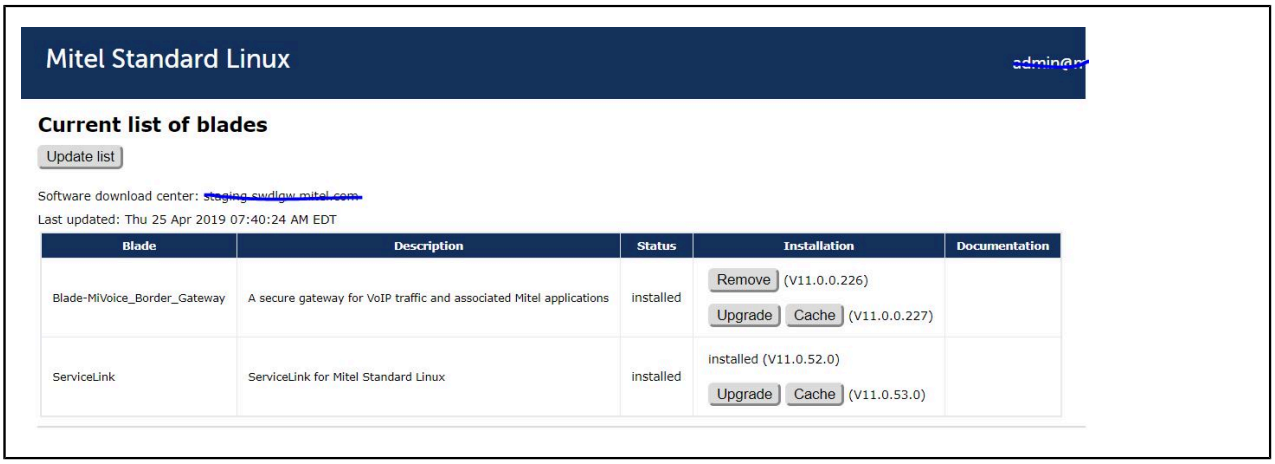
Software blades allow applications and services to run on MSL. For example, the Mitel Border Gateway blade allows your MSL server to run the MBG application (See Figure 6.)

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

You can download and install a software blade in a single step, or you can download it for installation later. 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, in MiCollab deployments, the Blades panel is replaced by the Install Applications panel, which you can use to install and upgrade MiCollab applications and security patches. For more information, refer to the MiCollab online help.

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

1. In the server manager, under **ServiceLink**, click **Blades**. The currently cached list of blades is displayed.
2. Click **Update List** to retrieve the latest list of available blades from the Mitel software download center.
3. Scroll through the list and locate the blade for the feature that you are adding to the system.
4. Do one of the following:
   - To install a new blade immediately, click the **Install** link beside it.
   - To download a blade for installation at a later time, click the **Cache** link beside it. Complete the installation process by clicking the **Install** or **Upgrade** link.
   - To upgrade a blade, click the **Upgrade** link beside it.
   - To delete a blade, click the **Remove** link beside it.
5. Reboot the server (if required for the application blade). 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.

Note:

- You can also install blades from a CD/DVD. If you have an application distributed in this way, insert the disc before loading the blades panel, or click Update List after inserting the disc.
- 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.

> **Note**:
> If Mitel Standard Linux does not have an upgrade link, then you are already running the latest software version.

11.2.2 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.

11.2.3 Online Activation

To activate ServiceLink online:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. Under **ServiceLink**, click **Status**.
3. Enter your **Application Record ID** (also called Service account ID).
4. Address and port number of License Server or proxy:

   - If the AMC license server is being used and no proxy connection is required, leave the address and port fields blank
   - If the AMC license server is being used, but must be accessed via a proxy, enter the proxy address and proxy port number

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.

- If SLS is being used, enter the proxy address as sync.sls.mitel.com and leave the port number blank. This field is mandatory when using the SLS for licensing.

Note:

To activate an SLS Serial ID the following connections must be allowed through any firewalls.

- **FQDN**: sync.sls.mitel.com, **Current IP**: 18.200.183.29 **Port**: 22 **Protocol**: SSH
- Customer must verify current IP before creating firewall rules as the IP address may be subject to occasional change.

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

Following successful activation, MSL periodically reconnects to the license server (every 24 hours by default) via a secure, encrypted connection to synchronize ServiceLink status information.License expiration dates and any service entitlement changes made to your license server account are updated at this time.

11.2.4 Offline Activation

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

If your MSL server has a USB drive, you may also perform offline activation from the server console. Refer to the Offline Sync with the AMC on page 164 for details.

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

To activate ServiceLink offline with **AMC**:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. In the server manager of the maintenance PC, under **ServiceLink**, click **Status**.
3. Enter your **Application Record ID** (also called Service account ID).
4. Select **Enable offline license generation**.
5. Click **Activate** to request an offline licensing file.
6. The Operation status report page is displayed. Click **Download license request file**.
7. In the file download dialog, click **Save** and save the zip file to a portable storage medium on the maintenance PC.
8. Remove the portable storage device and go to an Internet-connected PC.
9. On the Internet-connected PC, extract the contents of the zip file to a temporary folder.
10. Open the folder and double-click the **sync.bat** file to execute handshake and synchronization with the AMC.

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

To activate ServiceLink offline with **SLS**:

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

10. Click **Licenses & Services** option from the left menu, **License Server** home page opens.
11. Use the **Search product/ end customer** option and find your system.
12. In the **Licenses & Service** home page, click **Upload request** from the left menu. Browse to locate the zip file downloaded in Step 6, and upload offline license request, and click Upload Request.
13. Scroll to the bottom of the page to download and save latest license zip file. Save the license.zip file in a portable storage device.
14. Remove the storage device from the Internet-connected PC and return to the maintenance PC.
15. Insert the storage device in the maintenance PC.
16. Log into the server manager of the maintenance PC.
17. In the server manager of the maintenance PC, under ServiceLink, click Status.
18. Click **Sync** to generate an offline license request. The Upload license file and Download licensing refresh file buttons are displayed.
19. Beside Upload license file, click **Browse**.
20. In the **file upload**dialog, browse to the license.zip file on your PC and upload the latest license zip file containing the licenses to the server manager. Click **Save** to select the file to be uploaded.
21. Click **Upload license file** to install the synchronized license key file and activate the purchased licenses.

11.2.5 Manual Synchronization

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

To manually synchronize with the license server:

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

11.2.6 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.

11.2.7 Backup

There are two methods for backing up system data:

- The server manager offers the Backup option to backup data to a local workstation, an Amazon S3 storage bucket, 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 104 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.
3. Click **Perform**. MSL prepares the system for backup and displays the following:
4. The "Operation status report" with the estimated backup size. Ensure that your browser and target file system support downloads of this size.
5. The "Backup Encryption" option.
6. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. The encrypted backup file is identifiable with an .aes256 extension.

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

7. Click **Download Backup** File.
8. When prompted to Open or Save, click **Save**.

9. 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/DVD or USB storage device, if required. (CD/DVD or USB storage is required for future restore operations.) The backup file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

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 NFTS 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. Three file-sharing protocols are supported:

- SMB/CIFS (typically used for Windows servers)
- SFTP (typically used for Linux servers, including MSL)
- HTTPS to an AWS S3 (storage bucket)

Notes:

- You can only have one backup scheduled on the server. To cancel an existing backup schedule, select Disabled and then click Save.
- If you are backing up to an MSL server, configure it to accept access from the backup server. See Networks for details.

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** drop-down list, click **Configure network backup**.
3. Click **Perform**.
4. The **Network Backups** page is displayed.

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

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

Field	Description
IP Address	IP address of the network file server where you have stored the database backup files.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
Domain or Workgroup Name	Domain or workgroup name. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then instead of the domain SAM, the server's local Security Account Manager (SAM) is used for authentication.
Sharename	The file-share name. The shared folder must have permissions set to "Full Control".
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. The sub-directory is relative to the Sharename.

Field	Description
Maximum number of backup files to keep	Select the maximum number of backup files to keep (1-999) on the server. When the number of stored files reaches this maximum count, the earliest version is deleted.

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

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

Field	Description
IP Address	IP address of the network file server.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
(Optional) Sub Directory	Name of the sub-folder in which to store the backup files. The sub-directory is relative to the root of the file system accessed through the SFTP protocol.

Field	Description
Maximum number of backup files to keep	Select the maximum number of backup files to keep (1-999) on the server. When the number of stored files reaches this maximum count, the earliest version is deleted.

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

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

Field	Description
(Optional) Maximum number of backup files to keep	Select the maximum number of backup files to keep (1-999) on the server. When the number of stored files reaches this maximum count, the earliest version is deleted.

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

6. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers, and symbols, plus both upper and lower case characters.

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

7. Click the **Save** button to validate your server configuration. If validation is successful the Backup Now button will appear.
8. Click the **Backup Now** button to perform an immediate backup.

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

To perform an immediate backup:

1. Click **Backup Now.**

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.

2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).
   - For Daily backups, select a time of day (hour, minute, AM/PM)
   - For Weekly backups, select a time of day, and day of the week
   - For Monthly backups, select a time of day, and day of month
   - To disable regularly scheduled backups, click **Never**
5. Click **Save**.

If the scheduled backup fails, an alarm is raised and can be seen in the Event Viewer panel.

11.2.8 Restore Server Data

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

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

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

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

Before you begin

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

To restore the server database backup file

1. Under **Administration**, click **Restore**.
2. The **Restore from Network** page is displayed.

3. From the **Restore Source Type** drop-down list, select the type of network restore.

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

Field	Description
IP Address	IP address of the network file server where you have stored the database backup files.
Username	User name to use when connecting to the network file server.
Password	Password to use when connecting to the network file server.
Domain or Workgroup Name	Domain or workgroup name. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then instead of the domain SAM the server's local Security Account Manager (SAM) is used for authentication.
Sharename	The file-share name. The restore utility will try to connect to the server/shared folder as an SMB/CIFS resource. The shared folder must have permissions set to "Full Control".

Field	Description
(Optional) Sub Directory	Name of the sub-folder where you have stored the database backup file. The sub-directory is relative to the share.

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

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

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

Field	Description
AWS Access Key ID	To enable programmatic calls to AWS you must provide your AWS access key credential set that consists of the Key ID and Secret Access Key. Enter your access key ID here.

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

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

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

8. Click **Next**. A confirmation message is displayed.
9. Click **Yes** to restore the database. The system reboots and restores the database upon restart.

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

11.2.9 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 drop-down list (for example “messages”). With no filter options entered, the entire log file is displayed.

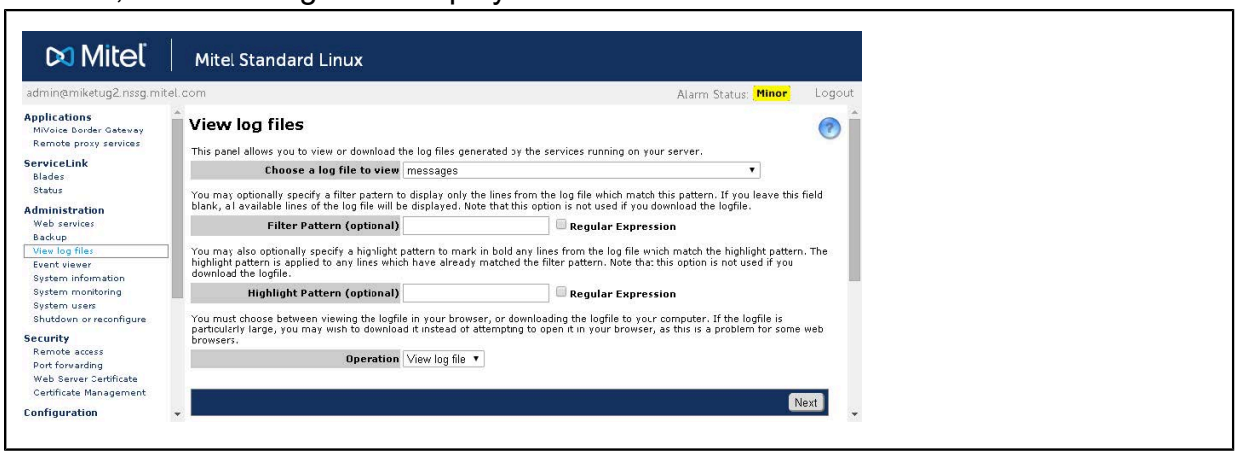


Figure 6: View Log Files

3. 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.
4. 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 56 for details and examples.
- The system automatically updates the list every 5 seconds with any new logs.

5. From the Operation list, select View or Download and click Next.

11.2.10 Web Services

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

By default, the Web Services panel includes a single registered web services client for Oria, a web-based customer provisioning application. Do not change this configuration in any way. Do not modify the existing consumer information or tokens, and do not attempt to add a new consumer. You can use the Web Services panel for one purpose only: to enable/disable the interface.

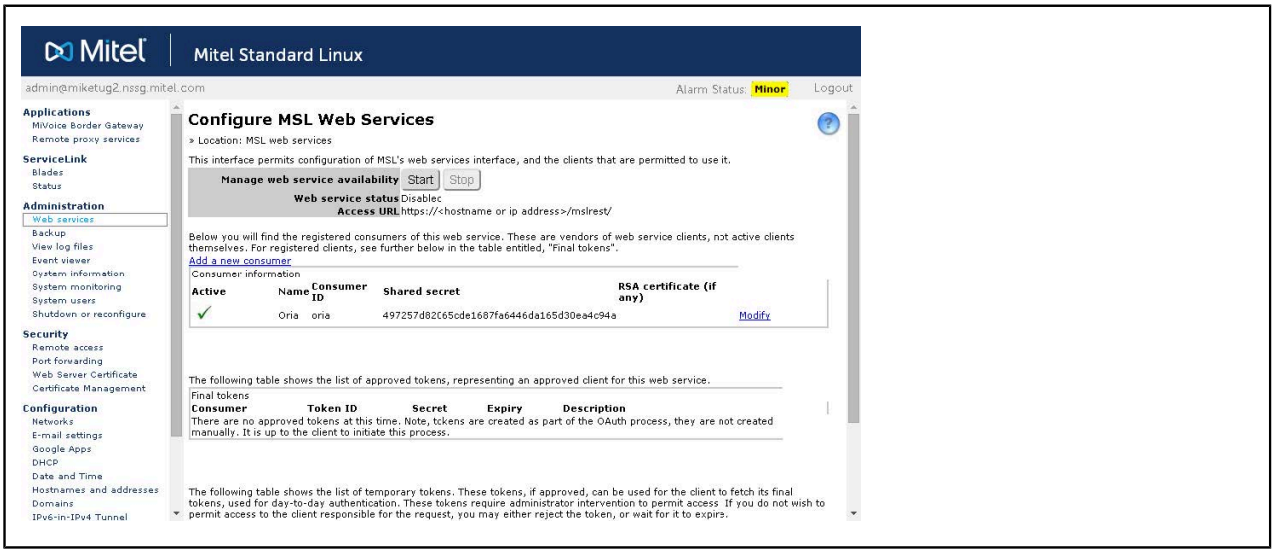


Figure 7: Logs and Diagnostic Data

To enable/disable the MSL Web Services interface:

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

11.2.11 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.

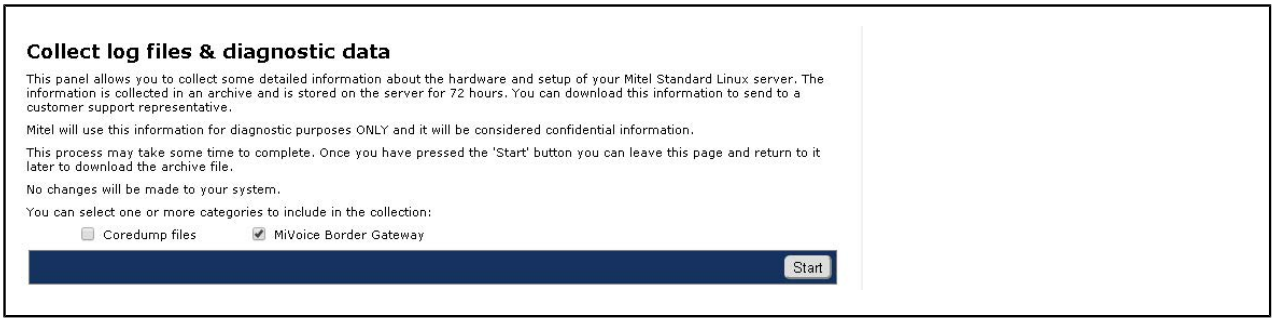


Figure 8: Logs and Diagnostic Data

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 and encrypt a file, click Encrypt Download, enter a Password, and then re-enter it. Create a strong password by using a mix of characters, numbers and symbols, plus both upper and lower case characters. Click Continue. An encrypted

tar file with the filename "sosreport-<file>.tar.gz.aes256" is saved to the Downloads folder.

- To save a file without encrypting it, click Download. A tar file with the filename "sosreport-<file>.tar.bz2" is saved to the Downloads folder.
- To delete a file, click Delete, and then click OK. The archived log file is deleted from the server.

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

Notes:

- To decrypt a log file, transfer to file to a Linux system, access a console and enter the following command: openssl enc -aes-256-cbc -d -in filename -out newfilename. When prompted, enter the password used to encrypt the file. If you only have access to a Windows system, use a Unix emulator such as CygWin to perform these steps.
- Archived log files are automatically deleted from the server after 72 hours.
- You can also manage the archived log files from the MSL shell. The files are located on the server in /var/cache/e-smith/logcollector.

11.2.12 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.

You can access the Event Viewer from the Server Manager menu or by clicking the Alarm Status button located the header bar. The Alarm Status button indicates the severity level of the most serious system alarm. For example, if the system has a service-affecting fault, the label will display "Minor" with a yellow background.

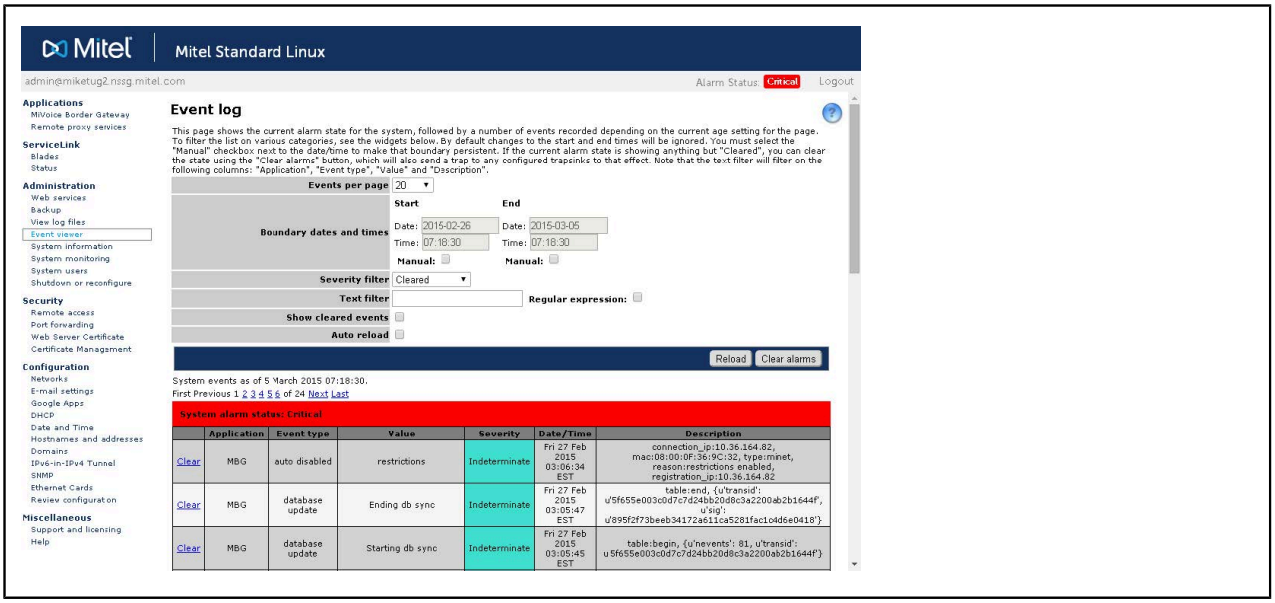


Figure 9: Event Viewer

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. To access the Event Viewer, do one of the following:

   a. Under **Administration**, click **Event viewer**.

   b. Click the **Alarm Status** button.
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** check box if you want to view both cleared and new events. Clear the box if you only want to view new events.
8. Select the **Auto Reload** check 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.

11.2.13 System Information

Access this screen to obtain the following:

- System Vital Information - hostname, IP address, kernel version, etc.
- Network Usage Information - network interface throughput.
- Hardware Information - server manufacturer/model, number of processors/model, CPU speed, cache size, etc.
- Memory Usage - size and usage of random-access memory.
- Mounted Filesystem - list of the mounted partitions.

To view system information for your server:

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

11.2.14 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/

11.2.15 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.

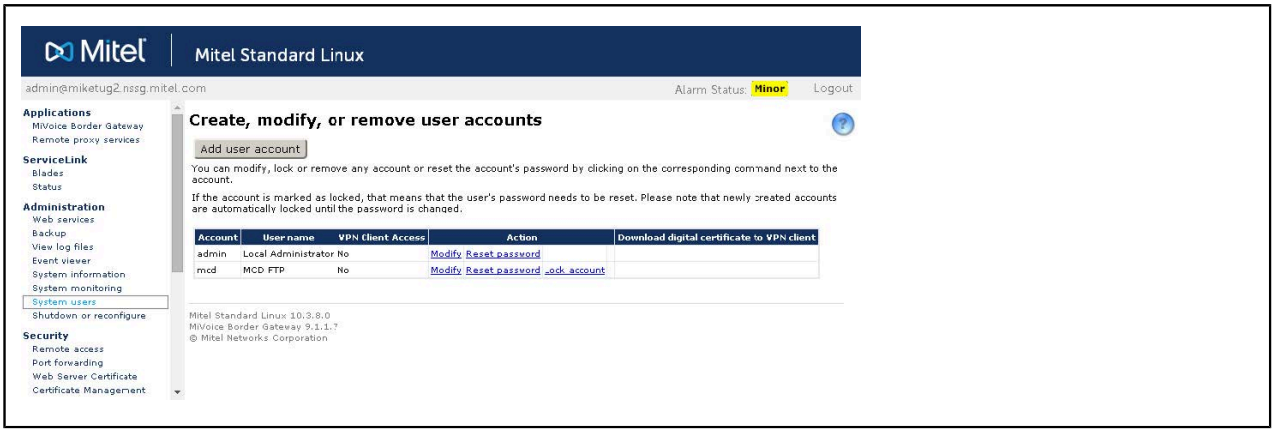


Figure 10: System Users

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. Click Add.

7. 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

8. 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.

11.2.16 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 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**.

11.2.17 Shut Down or Reboot

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

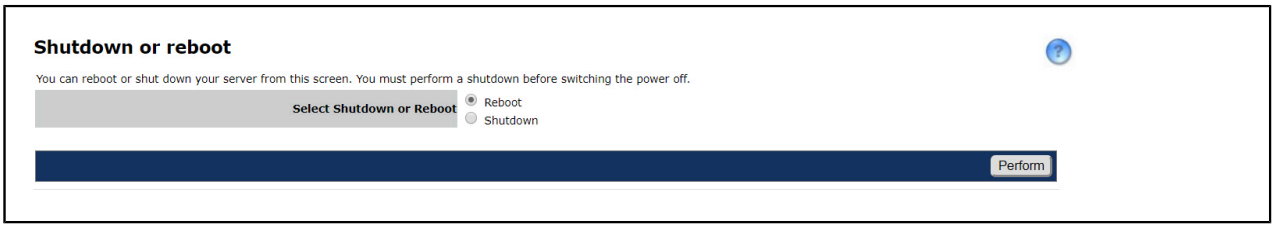


Figure 11: Shutdown or reboot

- Reboot: reboots the server after graceful shutdown.
- 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.

11.2.18 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.

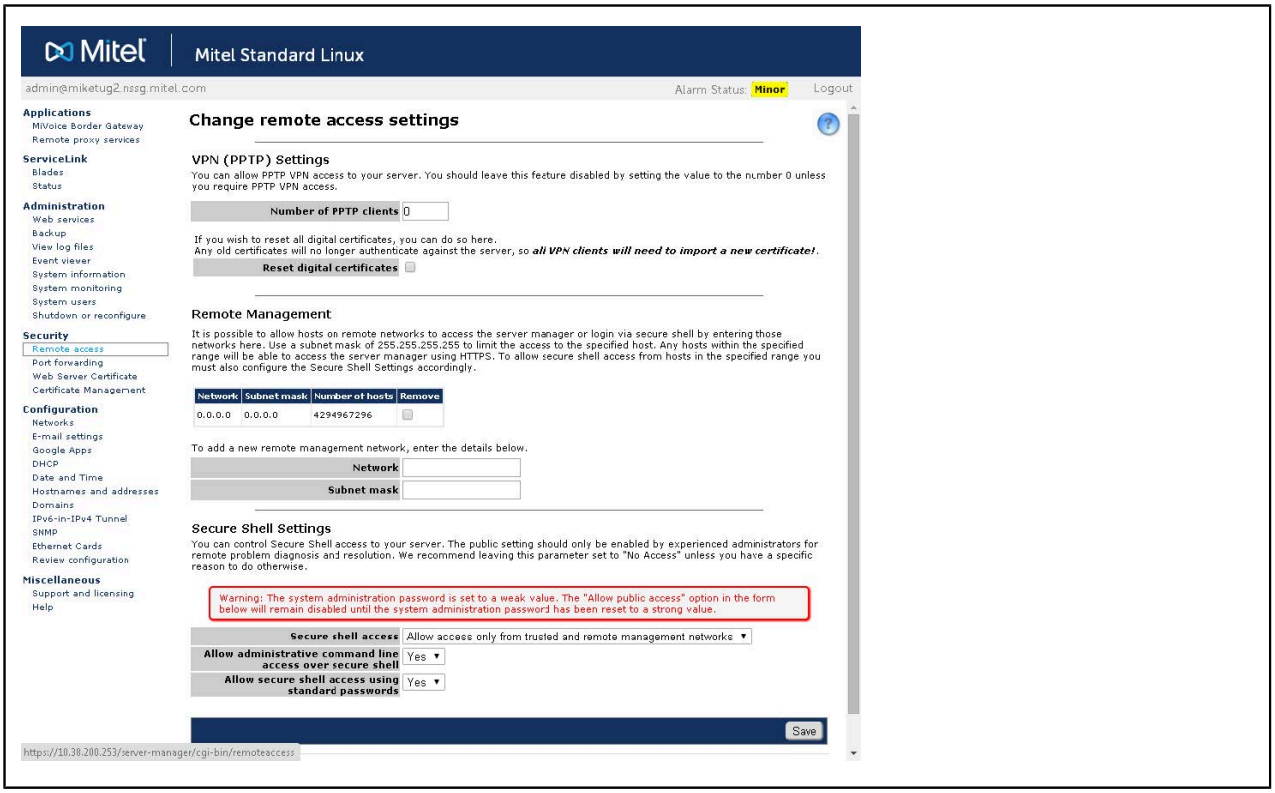


Figure 12: Remote Access

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 87.

To enable VPN access:

1. 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.
2. 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/DVD 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 IPv4 or IPv6 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 for IPv4 networks or a CIDR prefix of /128 for IPv6 networks. Using 255.255.255.255 or /128 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 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 an IPv4 or IPv6 network, or to copy files from a local machine to a server. Programs such as telnet and FTP transmit passwords in plain, unencrypted text across the network or the Internet. SSH 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 trusted and remote management networks – This option enables you to access the server from trusted local networks and remote management networks. To add a remote management network, see Remote Management.
   - Allow public access (entire Internet) – This option enables you to access the server from anywhere on the Internet. It is selectable only if you have configured a strong SSH (admin) password. If you have weak password and attempt to select this option, you will receive the following warning: "The system administration password is set to a weak value. The "Allow public access" option in the form below will remain disabled until the system administration password has been reset to a strong value."

   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

Several 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.

11.2.19 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(s) 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(s) field, enter the port on the Destination Host to which the traffic is to be forwarded.
7. To enable Secure Network Address Translation, select SNAT.
8. Click Next.
9. 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.

11.2.20 Syslog Server

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

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

Receiving Messages from Remote Hosts

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

To start receiving syslog event messages from remote hosts:

1. Under Security, click Syslog.
2. Under Accept syslogs from remote hosts, do the following:

   a. In the Accept remote syslog on UDP field, click Enable.
   b. (Optional) In the Accept remote syslog on TCP field, click Enable. In the Listen Port field, enter a port number (for example, 514), and then click Save.

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

3. To stop receiving syslog event messages from a remote host:

   a. Under Security, click Syslog.
   b. Under Accept syslogs from remote hosts, locate the protocol you wish to disable (UDP or TCP).
4. Click Disable.

Sending Messages to Remote Hosts

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

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

1. Under Security, click Syslog.
2. Under Forward local syslogs, click Add remote syslog destination.
3. In the Configure syslog screen, do the following:

   - In Facility, select type of program or subsystem that is logging the message. By default, the auth facility code (security/authorization messages) is selected. You may also select authpriv, a more secure version. For a complete list of facility descriptions, see RFC 3164.
   - In Destination Host (ip:port), enter the IP address and port number of the remote syslog server.

   Note:

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

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

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

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

1. Under Security, click Syslog.
2. Under Forward local syslogs, locate the host you wish to disable.

3. Click Remove twice.

11.2.21 Web Server Certificate Management

About SSL Web Server Certificates

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

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

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

Let's Encrypt

Let’s Encrypt is a free, automated, and open Certificate Authority. It enables you to obtain a valid SSL certificate simply by providing your domain settings and then clicking a button. The acquired certificate is monitored and renewed automatically.

The service is currently not supported on servers under the following deployment configurations:

1. Any server behind a MiVoice Border Gateway Web Proxy version earlier than v9.4.
2. MiCollab with AWV in server-only (LAN) mode behind a MiVoice Border Gateway in server-gateway mode on the network edge with 2nd WAN IP address configured on the MBG Web Proxy for MiCollab Audio, Web and Video Conferencing if the MBG Web proxy version is earlier than v9.4.0.25.

The service is supported on any MSL system that meets the following criteria:

1. each FQDN configured in the certificate request must be resolvable from the external Let's Encrypt server.
2. an https request to each resolved FQDN above with a URL of the form https://FQDN/.well-known/acme-challenge/CHALLENGE_TOKEN must reach and be responded to by the server on which the Let's Encrypt certificate request has been made.

Alternate 3rd-Party

An alternative third-party Certificate Authority issues an SSL certificate upon request, typically for a fee. Companies such as Entrust and GoDaddy provide such services. To obtain a generic SSL certificate, you must first generate a Certificate Signing Request (CSR) on the MSL system and send it to the CA. The CA will then return a package containing your web server certificate, plus any intermediate certificates that are required to maintain the certificate key chain. Optionally, you can download the SSL certificate and private key from the local MSL server and upload these files to other servers in your domain.

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

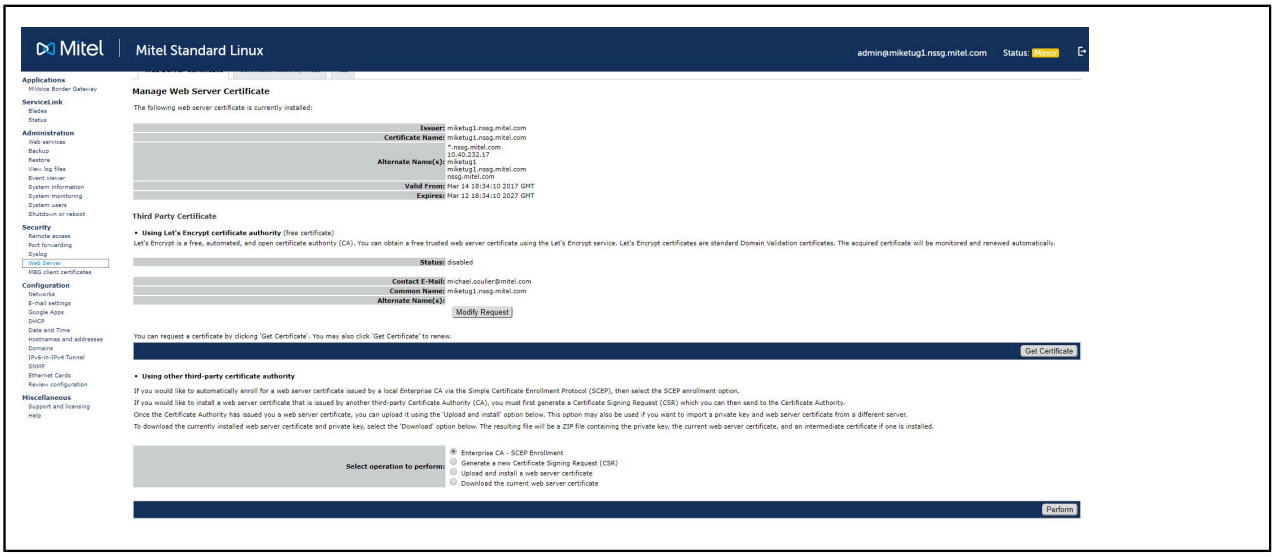


Figure 13: Web Server Certificate

Manage Third-Party Certificates from an Alternate Third-Party Certificate Authority

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

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

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

You can automatically enroll for a web server certificate issued by a local Enterprise CA using the Simple Certificate Enrollment Protocol (SCEP). Select the Enterprise CA - SCEP Enrollment option from the MSL Web Server panel.

11.2.22 Certificate Authority Trust

The Certificate Authority (CA) Trust tab allows the administrator to upload an additional root CA certificate in PEM format to the list of trusted CA certificate store on MSL.

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

By default, the Mitel Networks Root CA and Mitel Products Root CA certificates are added to the Trust Store. These are visible in the Certificate Authority Trust tab.

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

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

Note:
The certificate must be in PEM format.

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

Supported Formats

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

PEM certificates typically have extensions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format. Apache and similar servers use PEM format certificates. Several PEM certificates, including the private key, can be included in a single file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files.

PKCS#12 or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as .pfx and .p12. PFX files are typically used on Windows machines to import and export certificates and private keys.

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

Configuration Example

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

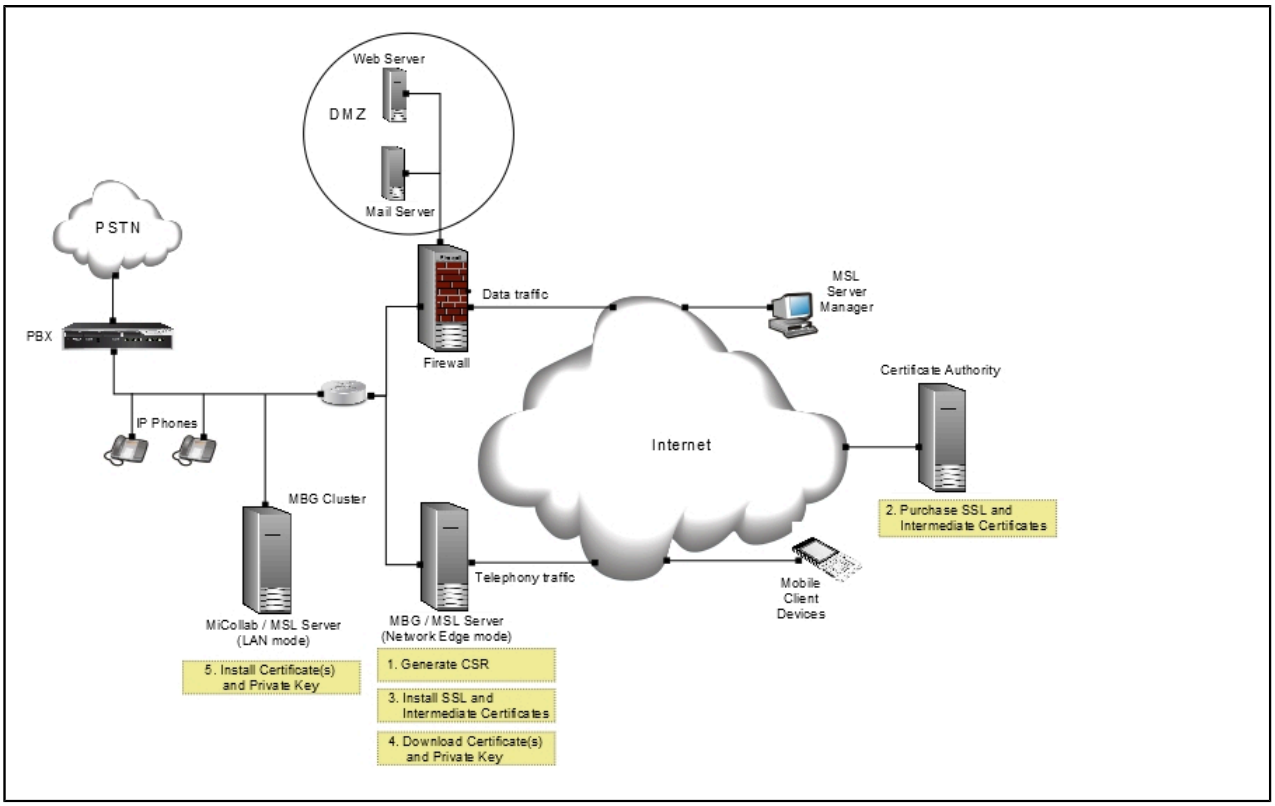


Figure 14: Web Server Certificate – Configuration Example

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

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

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

1. Log into the **MSL Server Manager**.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Enterprise CA - SCEP Enrollment** option.
5. Click **Perform**.
6. Fill out the **SCEP** form:

   - **CA Address**: the FQDN or IP address of the SCEP server
   - **URI Path**: the URI to use in SCEP communication (defaults to Windows SCEP URI for clients)
   - **Enrollment Password**: the enrollment challenge password if required
   - **Common Name**: the Common Name to use in the Certificate Signing Request (CSR) (defaults to the system hostname)
   - **Alternate Name(s)**: the Subject Alternate Name(s) to include in the CSR
7. Click **Get Certificate**.
8. Upon submitting the form, the data is validated and access to the SCEP server is verified. On successful verification, the SCEP enrollment is initiated to request a certificate, a progress status of the SCEP transaction is provided.

   - If the enrollment request is rejected, check the SCEP server for the details of the failure.
   - If the enrollment request is in pending state, the administrator of the SCEP server needs to approve or deny the certificate request.
9. Reload the MSL server manager for the newly acquired web server certificate to take effect.

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

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

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

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

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

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

   - Select the number of domains you wish to protect:
     - Single domain: Select this option if your implementation has one MSL server on a single domain (for example, www.domain.com and domain.com).
     - Multi-domain: Select this option if your implementation has multiple MSL servers on a specific number of domains (for example, www.domain.com and domain.com, plus three sub-domains).
     - Multi-domain and wildcard: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (for example, www.domain.com and domain.com, plus an unlimited number of sub-domains).
   - Enter your account and contact details in the CA web form:
     - Login Name and Password.
     - Name, Email Address, and Telephone Number.
     - Organization Name and Address.
     - Domain Name.

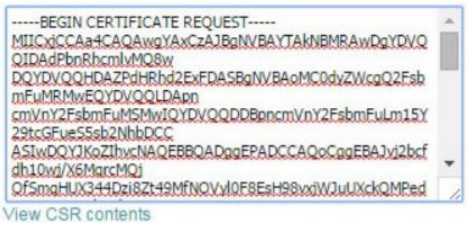
     Note:
     Some CAs may prompt you to enter the Subject Alternate Names (SANs) or wildcard domain in this step. For more information on these entries, see below.

     - Web Server Software.

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

     - Hashing Algorithm.

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



View CSR contents

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

    - **Subject Alternate Name (SAN)**: Enter the domain name for each service (or “virtual host”) in the LAN that you want to include in this certificate. For example,

if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied. Note: You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.

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

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

Note:

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

13. Contact the administrator for the domain used in a CSR. The administrator is identified using information supplied when your organization originally registered its internet FQDN.
14. Upload the certificate files to a location that is accessible to the MSL server.

Install a Third-Party SSL Certificate on the MSL Server

Use the following procedure to install the certificate files that you received from the alternate third-party Certificate Authority onto the MSL server that generated the CSR.

To install the SSL certificate files on the MSL server:

1. Log into the MSL Server Manager for the system that was used to generate the CSR.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload** and install a web server certificate, and then click **Perform**.
5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the **SSL certificate**, select it and click **Open**.
   - If you also received an Intermediate SSL certificate, select it, click **Browse**.
   - Navigate to the **Intermediate SSL certificate**, select it and click **Open**.

Note:

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

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

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

Install the Third-Party SSL Certificate on other MSL Servers

If your deployment includes LAN-based MSL application servers accessed via an MBG / Web Proxy server, use the following procedure to install the certificate files on them. This is a two-step process. First, you must download the web server certificate, intermediate

certificates (if installed), and private key file corresponding to the SSL server certificate from the MBG / Web Proxy. Second, you must upload these files to the LAN-based MSL server.

Download certificates

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

1. Log into the MSL Server Manager for MBG / Web Proxy (the system that was used to generate the CSR)
2. Log into the MSL Server Manager for the system that was used to generate the CSR.
3. Under **Security**, click **Web Server**.
4. Click the **Web Server Certificate** tab.
5. Select **Download the current web server certificate**, and then click **Perform**.
6. Click **Save**, navigate to the location you wish to store the file, and then click Save. The downloaded file is in ZIP format. It includes the web server certificate, intermediate certificates (if installed), and private key file.
7. Unzip the files and upload them to a location that is accessible to the other MSL servers in your network.

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

11.2.23 Upload certificates

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

1. Log into the MSL Server Manager for a LAN-based MSL server.
2. 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**.
   - If you also received an **Intermediate SSL certificate**, select it, click **Browse**.
   - Navigate to the Intermediate SSL certificate, select it and click **Open**.

4. Import the private key pair created on the other MSL server:
   - Beside the **SSL Private Key** field, click **Browse**.
   - Navigate to the SSL Private Key file, select it and click **Open**.
5. Click **Install Web Server Certificate**.
6. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.

Note:

- To prevent fraudulent use of your certificates, delete the certificate and private key files from any media they are stored on.
- Some services, such as the MiCollab Client Service, are restarted automatically as soon as you install the certificate. This removes the need for you to restart the server manually.

Uninstall the Third-Party SSL Certificate

To uninstall an alternate third-party CA SSL certificate and resume using the self-signed certificate:

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

Verify the Third-Party SSL Certificate

To view details regarding currently installed alternate third-party CA certificate:

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

Field Name	Details

Issuer	Lists the following information for the certificate authorization company that issued the certificate: C: country code (2-letter ISO country code) ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority OU: name of the organizational unit CN: server hostname Authority/emailAddress: email address of the Certificate Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid from	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires.

Managing Let’s Encrypt Third-Party Certificates

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

Note:

- To use this service, the MSL server must be accessible to the Internet, either directly or through a proxy.
- This service is only supported on single-server, standalone implementations of applications that use the MSL operating system such as MiVoice Border Gateway and NuPoint Unified Messaging. This service is not supported on MiCollab Server or MiCollab Virtual Appliance deployments.
- When you request an SSL certificate from the Let's Encrypt service, you must provide a Common Name and, optionally, Subject Alternative Names as fully qualified domain names (FQDNs) that are resolvable to addresses on the public network. When the Let's Encrypt servers issue an HTTP request to a resolved FQDN (such as https://mbg.mitel.com/.well-known/acme-challenge/random_file_name), this request must be able to reach the MSL server on which the certificate request is being made. Accordingly, the MSL server must be accessible to the Internet, either directly or through a proxy.

Request a Let's Encrypt SSL Certificate

To request a Let's Encrypt SSL certificate:

1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Click **Get Certificate**.
5. Enter the information required to request the SSL certificate from the Let's Encrypt system:

Field Name	Enter
Status	Indicates the status of the certificate, either enabled (successfully installed and active) or disabled (not successfully installed and inactive)
Contact E-Mail	Enter the email address of the administrator who Let's Encrypt should contact to deal with issues of certificate recovery or registration.

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

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

Modify a Let's Encrypt SSL Certificate

To modify a Let's Encrypt SSL certificate request:

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

Uninstall a Let's Encrypt SSL Certificate

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

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

Verify the Installed Let's Encrypt SSL Certificate

To view details regarding currently installed web server certificate:

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

Field Name	Details
Issuer	Lists the following information for the certificate authorization company that issued the certificate: C: country code (2-letter ISO country code) ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority OU: name of the organizational unit CN: server hostname Authority/emailAddress: email address of the Certificate Authority
Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.

Alternate Name(s)	The FQDNs of each service (or “virtual host”) included in the certificate.
Valid from	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires.

11.2.24 Manage Self Signed SSL Certificates

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

The self-signed SSL certificate has the following disadvantages:

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

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

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

Install the Default Self-Signed SSL Certificate on Local Workstation

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

1. Open Internet Explorer.

2. When you attempt to access the MSL Server Manager login page, a **Certificate Error: Navigation Blocked** page is displayed. The warning states "There is a problem with this web site's security service".
3. Click the **Continue to this website** link to proceed to the MSL login page.
4. In the Internet Explorer command bar, click **View**, and then click **Security Report**. An **Untrusted Certificate** error dialog opens.
5. Click **View Certificates**.
6. Click **Install Certificate**.
7. Click **Next** to navigate through the Certificate Import Wizard windows.
8. Accept the default, “Automatically select the certificate store based on the type of certificate,” and click **Next**.
9. Click **Finish** on the Completing the Certificate Import Wizard window.
10. Click **Yes** on the Root Certificate Store window to add the certificate to the Root Store.
11. Click **OK** to close each window you have opened during this procedure.

Verify the Installed Default Self-Signed Certificate

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

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

Field Name	Details
Issuer	Lists the following information for the certificate authorization company that issued the certificate: C: country code (2-letter ISO country code) ST: state or province L: locality name (for example: city name) O: name of the certificate authorization authority; "XYZ Corporation" is the name that appears for Mitel self-signed certificates OU: name of the organizational unit CN: server hostname Authority/emailAddress: email address of the Certificate Authority

Certificate Name	The Common Name that identifies the fully qualified domain name associated with the certificate.
Alternate Name(s)	The FQDNs of each service (or "virtual host") included in the certificate.
Valid from	Date and time when the certificate takes effect.
Expires	Date and time when the certificate expires.

11.2.25 Manage TLS Protocol

By default, MSL supports the use of early TLS (TLS v1) for communications security. To migrate to the latest TLS version, you must upgrade your client softphones and devices and then disable support for the TLS v1 protocol using the procedure outlined below. After these steps are complete, your system will be in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Figure 15: TLS Setting

Disable Support for TLS v1

To disable support for the TLS v1 protocol:

1. Log into the MSL Server Manager.
2. Under Security, click Web Server.
3. Click the TLS tab.
4. To disable support for TLS v1, clear Allow TLS v1.0. Your system is now in compliance with PCI DSS.

Note:

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

11.2.26 MBG Client Certificates

Note:
The option to MBG client certificates is only visible with MBG installed.

The MSL server includes its own unique certificate authority (CA), named “Mitel Networks,” which is associated with the Mitel root CA. You can use this service to issue digital certificates to applications that require securely authenticated connections, such as MiContact Center.

To begin the process of obtaining a certificate, the client application issues a certificate signing request (CSR) to the Mitel Networks CA on the MSL server. For details on how to do this, consult your application documentation. When the MSL server receives the CSR, it will appear in a queue on the Certificate Management panel. You must then approve the CSR and issue the certificate by following the procedure found below. After these steps are complete, authenticated connections will be possible.

If necessary, you may also reject CSRs that are pending approval, and revoke certificates that have previously been approved.

Note:

- Before approving a CSR, you should establish the requester's identity by telephone or email. If you approve a CSR without being certain of the requester's identity, you may open a security breach in your network.
- The MSL server is limited to accepting 50 concurrent CSRs.

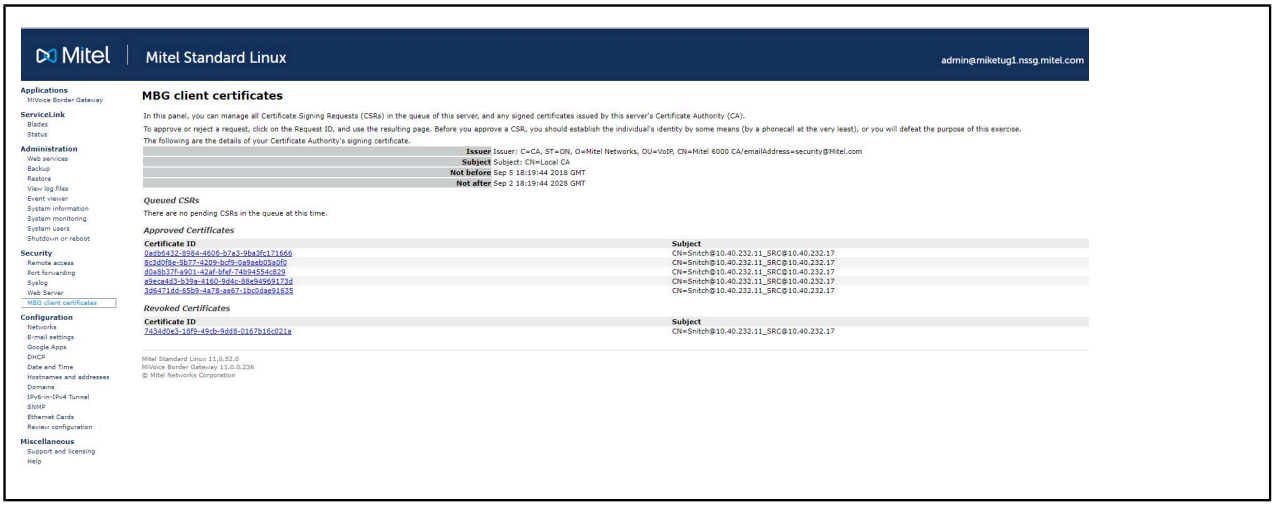


Figure 16: Certificate Management

Approve or Reject a CSR

To approve or reject 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. Note that if you reject the request, the requester must regenerate it.
   - Click **Approve** to approve the CSR. The approved CSR is listed as a certificate under the heading Approved Certificates.

Revoke a Certificate

To revoke an approved certificate:

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.

11.2.27 Networks

Grant Access Privileges to Trusted Local Networks

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

Example of Default Routing Configuration

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

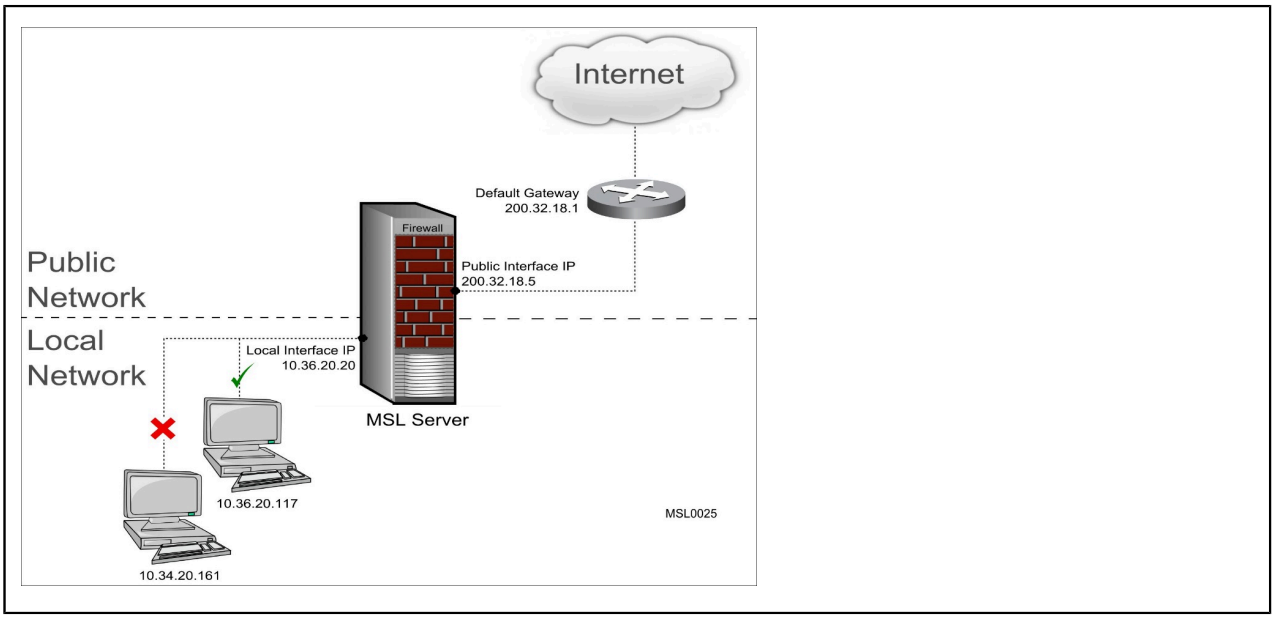


Figure 17: Default Routing Configuration

Example of Trusted Network Configuration

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

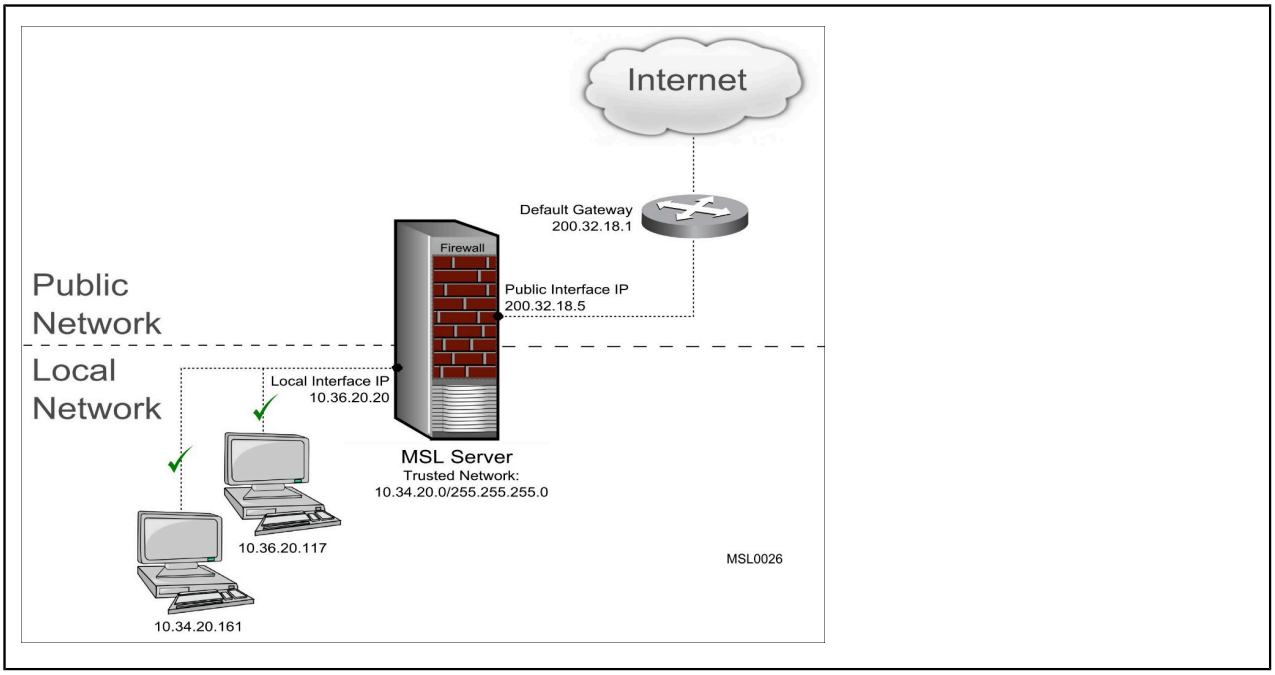


Figure 18: Routing Configuration with Trusted Network

Note:

- If only one network is being serviced by the server, you do not need to add any 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.
- Depending on the architecture of your network infrastructure, the instructions for configuring the clients on an additional network may be different than the following instructions. For more information about adding networks, contact your authorized Mitel Reseller.
- To control access to the server from computers on remote networks, see Remote Management and Secure Shells Settings.
- You can also use the server console to show, add, and delete trusted local networks.

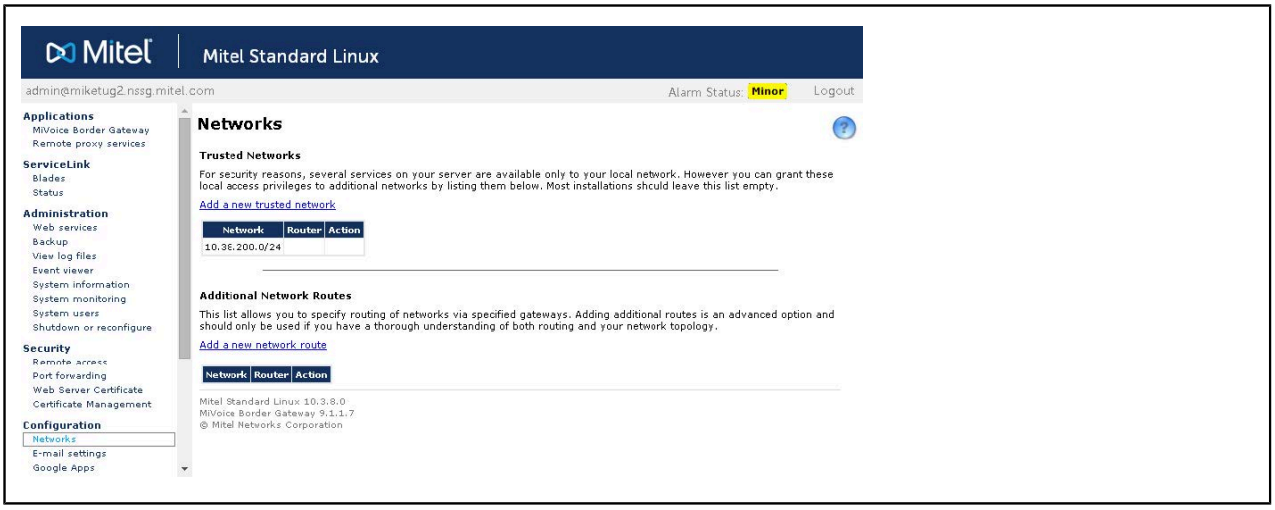


Figure 19: Networks

To extend privileges to one or more additional networks:

1. Click **Add a new trusted 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 or network prefix length field, enter the dot-decimal subnet mask or CIDR network prefix to apply to the Network Address. If this field is left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks.
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 trusted local network information, updates to the permissions files may take up to 15 seconds. If you attempt to access the server manager interface from a newly added trusted local network before the permissions have been updated, you will receive a “403: Forbidden” error message.

Add Network Routes

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

Note:

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

To add additional network routes:

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

11.2.28 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.

Note:
The \ character is not supported for a password.

- 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 trusted networks – accept email from trusted local networks that are directly connected to the LAN. (These networks are on the same subnet as the server's private interface.)
  - Accept from anywhere - accept all 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 pre-selected.

11.2.29 Google Apps

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

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

All applications that access Google must be registered through the Google APIs Console and must configure access using the Open Standard for Authentication 2.0 (OAuth 2.0) protocol. OAuth 2.0 allows users to share specific data with applications (for example, contact lists) while keeping their usernames, passwords, and other information private. With OAuth 2.0, user data is protected using access tokens. Applications that use OAuth 2.0 require an authorization code generated in MSL.

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

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

- **Installed Application** - Select this option if the application is to be installed on a mobile device, tablet or computer. The registration process results in a client ID and a client secret, which you embed in the source code of the application. MiCollab Client requires this configuration.
- **Service Accounts** - Select this option if the application employs server-to-server interactions, such as those between a web application and Google Cloud Storage. MiCollab Audio, Web and Video Conferencing and NuPoint Unified Messaging require this configuration.

Configure OAuth 2.0 for Installed Applications

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

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

Create an API Project and Client ID on the Google Authorization Server

Note:
The following instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help.

1. Log in to the **Google Apis** Console:

   a. Open a web browser and navigate to https://code.google.com/apis/console.
   b. Enter the domain administrator Email and password to log in.
2. Create a new project and give it a name such as "NuPoint Advanced UM." Remain in the project.
3. Enable Google APIs for the project:

   a. Open the side menu and select **API Manager**.
   b. Select a Google API such as "Calendar API" and click **Enable API**.
   c. Repeat for all Google APIs you want to support.
4. Create the OAuth 2.0 Client ID and Secret for the project:

   a. Open the side menu and select **API Manager and Credentials**.
   b. Under **New Credentials**, select **OAuth client ID**.
   c. Follow the prompts to create a new ID and then click **Create**. Set a Product name if prompted.

   Note:
   Select Other as the Application type.

   d. Click **OK**.
   e. Google provides a Client ID and Client secret. Record them and the Product name for use in the next procedure.

Generate an Authorization Code in MSL

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

1. Log in to the **MSL Server Manager** as “admin”.
2. In the navigation tree, under **Configuration**, click **Google Apps**.
3. Select the **Installed Applications** tab.
4. Under Step 2, copy and paste the following from the Google APIs console:

   - Product Name
   - Client ID
   - Client secret

5. Click **Save and Generate Authorization Code**. Remain on the Installed Applications tab in the MSL Server Manager.
6. Under Step 3, do the following:

   a. Copy the authorization code.
   b. Click the link provided to access the Google API console.

Allow Access Permission in Google

1. After clicking the link to access the Google API console, log in to your account.
2. Submit the authorization code to allow access in Google. Google grants the access token, which enables MSL to access services in the API project. Note that after the access token is generated, the panel displays its current status (access token ID and expiry time in seconds).

Note:

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

Configure OAuth 2.0 for Service Accounts

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

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

Create API Project and Client ID on the Google Authorization Server

Note:
The following instructions are provided as a guide only. For up-to-date instructions, refer to the Google online help.

1. Log in to the **Google Apps Console**:
   a. Open a web browser and navigate to https://code.google.com/apis/console.
   b. Enter the domain administrator Email and password to log in.
2. Create the Project:
   a. Click the **Create project** button.
   b. Enter the Project name (for example, "NuPoint Advanced UM") and click **Create**. Remain in the project.
3. Enable Google APIs for the project:
   a. Open the side menu and select **API Manager**.
   b. Select a Google API such as "Calendar API" and click **Enable API**.
   c. Repeat for all Google APIs you want to support. Remain in the project.
4. Create the Service Account with Client ID:
   a. Open the side menu and select **Permissions**.
   b. Under the **Service accounts** tab, select **Create service account**.
   c. Enter a **Name**, select **Furnish a new private key** and JSON as the file type, and then select **Enable Google Apps Domain-wide Delegation**. Set a Product name if prompted.
   d. Click **Create and Close**. The service account is created and the file containing the Private Key and Client ID is downloaded. Note: Store the file in a safe location. You will require it to establish your credentials to MSL.
   e. For the service account you just created, click **View Client ID**.
   f. Copy the Client ID and click **Cancel**. You will require the Client ID in the next procedure.

5. Manage API Client Access (API Scopes): Once a service account is created, you must enable the scope of access for a client ID.

   a. Access the Google Admin console:

      i. Open a web browser and navigate to admin.google.com.
      ii. Enter the domain administrator Email and password to log in.

   b. Click **Security**.
   c. Click **Show more** and then click **Advanced settings**.
   d. Under **Authentication**, click **Manage API Client access**.
   e. On the Manage API client access panel:

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

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

6. Upload Credentials to MSL: This procedure involves uploading your OAuth 2.0 credentials (JSON Service Account ID and private key) from your computer to MSL. MiCollab employs these credentials to integrate with publicly available Google Apps.

   a. Log in to the MSL Server Manager as "admin".
   b. In the navigation tree, under **Configuration**, click **Google Apps**.
   c. Select the **Service Account** tab.
   d. Under **Configuration**, upload the following files from your computer:

      - Service Account ID (.json file)
      - Private Key (.p12 file)

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

   e. Click **Upload Credentials**.
   f. Confirm that the Client ID, Email address, and Private Key are correct by comparing them to the corresponding fields in the Google API project.
   g. Click **Apply**. It is now possible to configure a secure connection to publicly-available Google Apps using the OAuth 2.0 protocol for the Service Account client ID.

Note:

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

11.2.30 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.

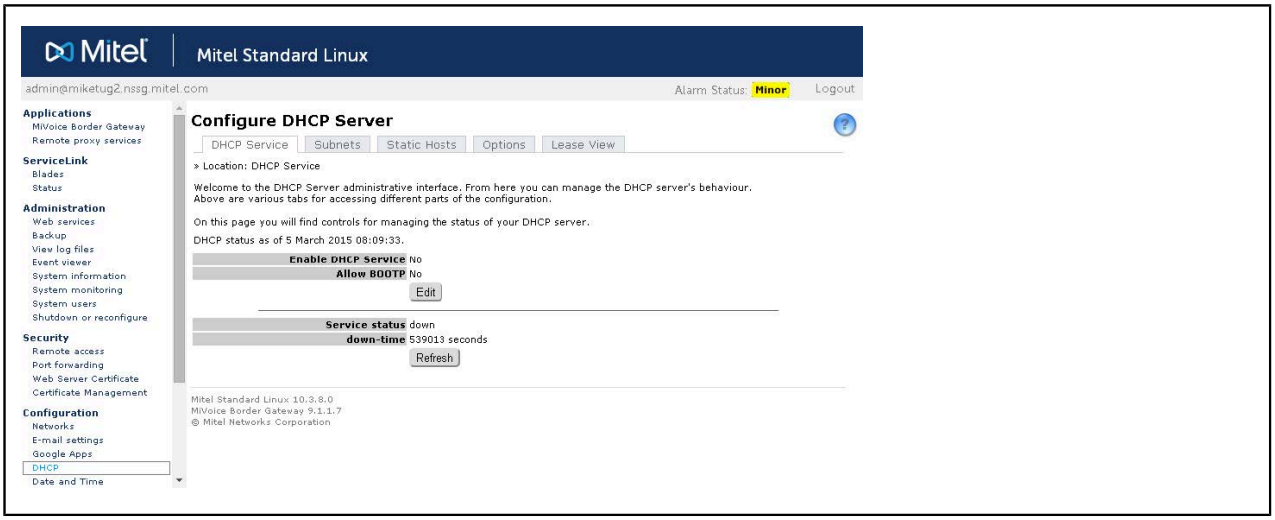


Figure 20: DHCP Settings

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 **Enable 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:

Note:
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**.

11.2.31 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.

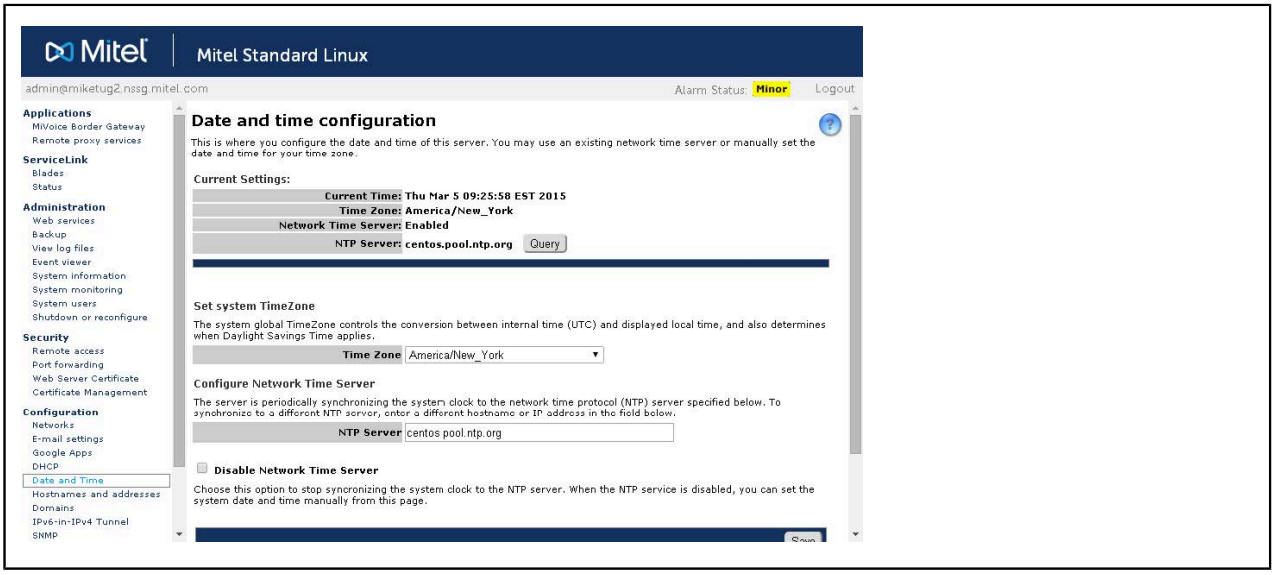


Figure 21: Setting Date and Time

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.

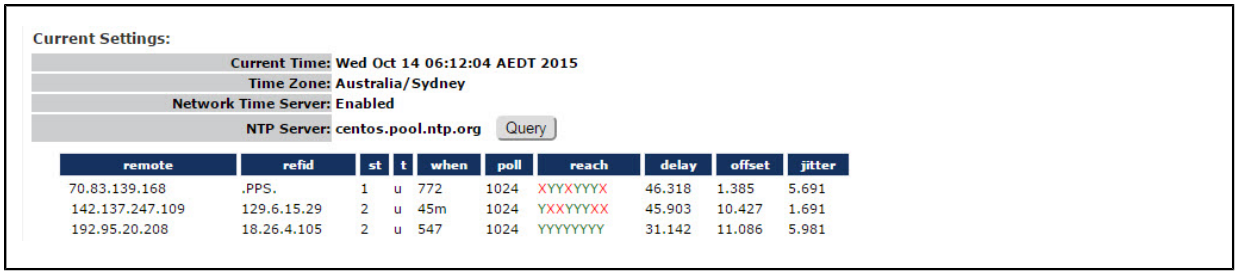
To switch from a Network Time Server to a manual configuration:

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).



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

2. 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.

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

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 # indicates that the host is selected for synchronization, but distance from the host to the server exceeds the maximum value. o indicates that the host is selected for synchronization, and the PPS signal is in use. + indicates the host included in the final synchronization selection set. x indicates that the host is the designated false ticker by the intersection algorithm. . indicates that the host is selected from the end of the candidate list. - indicates a host discarded by the clustering algorithm. blank indicates a host is discarded due to high stratum and/or failed sanity checks.
refid	The current source of the synchronization for the remote host.
st	The stratum used by the remote host. The lower the number, the closer you are to the time source. Stratum 16 indicates that the system is not synchronized with a time server.
t	The type of clock used on the NTP server (L stands for local clock; u for an Internet clock).
when	The number of seconds since the last poll.

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

11.2.32 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.

Figure 22: 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**.

11.2.33 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).

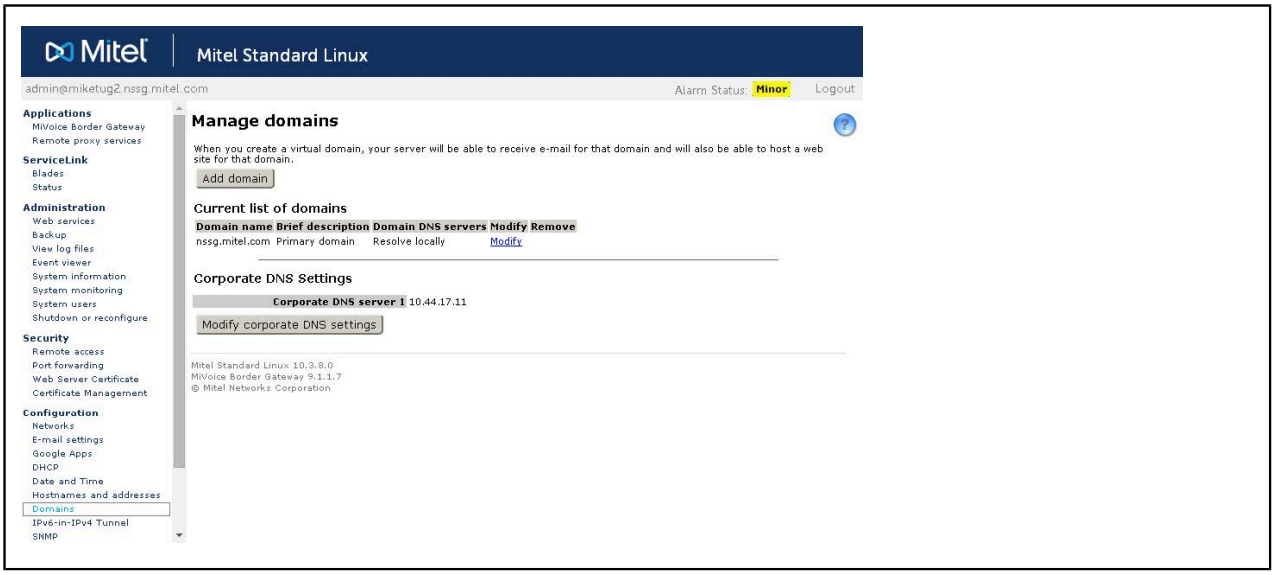


Figure 23: Domains

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.

11.2.34 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.

11.2.35 Simple Network Management Protocol (SNMP)

MSL supports Simple Network Management Protocol (SNMP) for retrieval of network information and statistics.

Note:
SNMP is only supported on a LAN interface, not on a WAN interface.

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 trusted local networks that are directly connected to the LAN. (These networks are on the same subnet as the server’s private interface.)
- **All configured trusted networks** – allows access to all networks that are configured in the “Networks” panel. These networks may not be on the same subnet as the server (that is, they may be attached via a router).

SNMPv3 settings– To facilitate SNMPv3 communication, you must add a user account to the MSL server that matches an account on the SNMP manager. This "User-based Security Model" (USM) enables unique authentication and encryption settings to be configured for each account. See Adding an SNMPv3 User Backups on page 99.

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**.

11.2.36 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.

11.2.37 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.

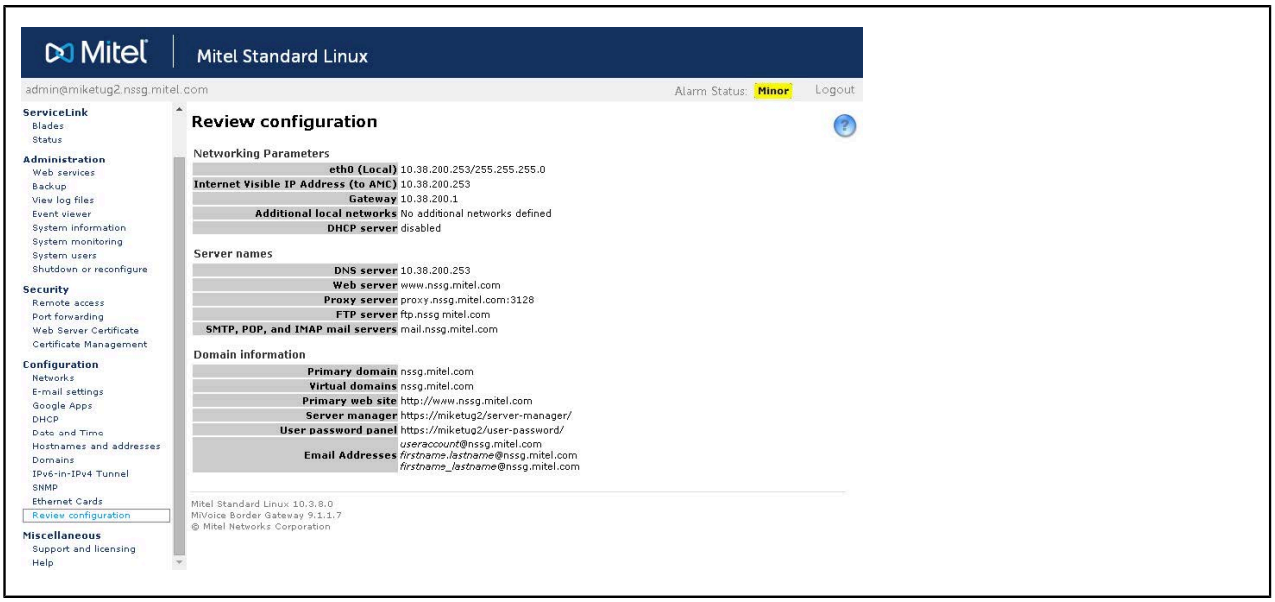


Figure 24: Review Configuration

The Server Console 12

This chapter contains the following sections:

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.

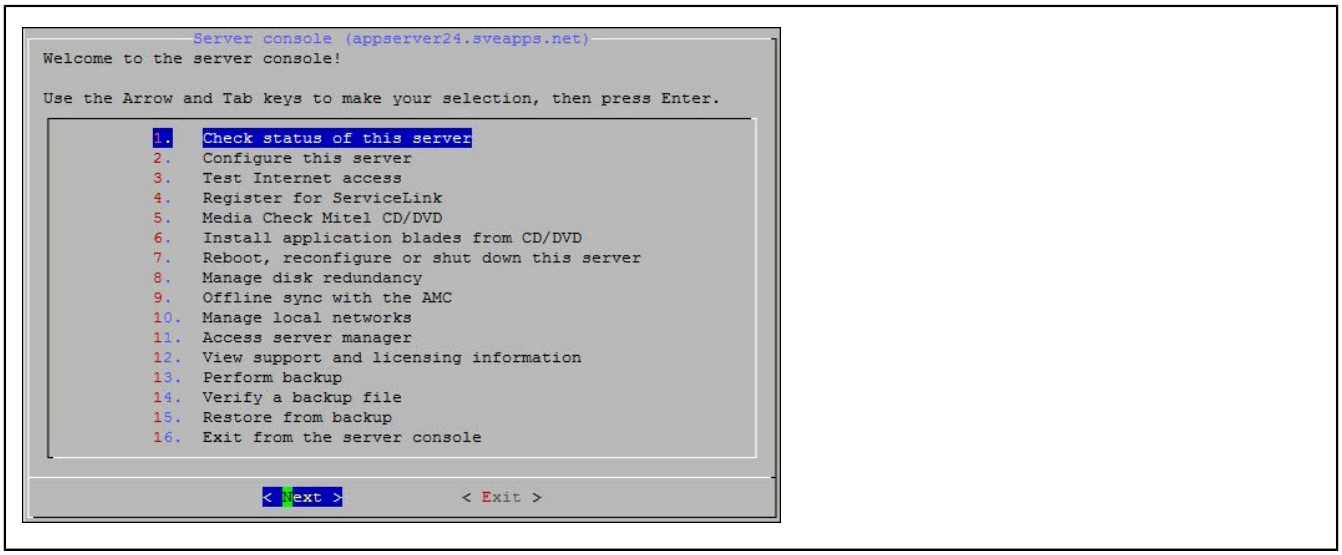


Figure 25: The Server Console

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.

Option:	Use this option to:
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
Register for Service Link	activate ServiceLink on the AMC via text mode browser; (normally you would use the web-based server manager)
Media Check Mitel CD/DVD	test a Mitel application CD/DVD (supported only for applications that have embedded checksum values.)
Install application blades from CD/DVD	install application software blades from CD/DVD. Your application documentation specifies when to use this option.
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.
Manage disk redundancy	manage configuration of redundant (RAID1) disks.
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 trusted networks	show, add, or delete “trusted 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).

Option:	Use this option to:
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 not 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 104.
Verify a backup file	verify previous backup files. For more information, see Verify Backup on page 106.
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 106.
Exit from the server console	exit from the Server Console.

12.1 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 license key 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.

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

Note:

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

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

12.2.1 Backing up to a USB Device

To backup to a USB device, do the following:

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. The file extension, either .tgz (unencrypted) or .aes256 (encrypted), is added automatically.

4. (Optional) To encrypt the backup file, enter an encryption password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Next**.

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

5. MSL displays an estimate of the size of your backup. Click Proceed.
6. When the backup is complete, remove the USB device when prompted. Click Continue.
7. Verify that the backup was performed successfully using the Verify Backup File procedure.

12.2.2 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 backup 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 **sub 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.

12.3 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 MiCollab applications indicates that the Verbatim, GXT, and Kingston brands consistently work well. See the *MiCollab Engineering Guidelines* for a list of supported USB devices.

12.4 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.

Note:

- Ensure that your verified backup file has a .tgz (unecrypted) or .aes256 (encrypted) 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.

12.4.1 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 or DVD 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/DVD 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/DVD) 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.

Note:
When running MSL on EX platform, the option to Restore from removable media or another running server are not available.

- **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. You can restore backups using SMB/CIFS or SFTP.

Note:
If you are using SFTP and do not specify a sub-directory for the backups, the file will be stored in the "/" folder by default.

- 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 **Yes** to restore the backup data.
8. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click **Next** and then **Yes**. A progress bar displays while the restore is in progress.
9. When the restore is complete, click **Reboot Now** to reboot the server and activate the configuration.
10. 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.

11. Reinstall your application software.

12.4.2 Restore on an Operational System

Note:
To do this procedure, you must be connected directly to the physical or virtual system. If you use a remote SSH client, you will lose your connection to the server console and be unable to complete the restore process.

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/DVD) 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. You can restore backups using SMB/CIFS or SFTP.
   - **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 Yes to restore the backup data.
7. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes. A progress bar displays while the restore is in progress.
8. When the restore is complete, click Reboot Now to reboot the server and activate the configuration.
9. When the reboot is complete, log back in to the server console and perform a sync with the AMC if necessary.

12.4.3 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.

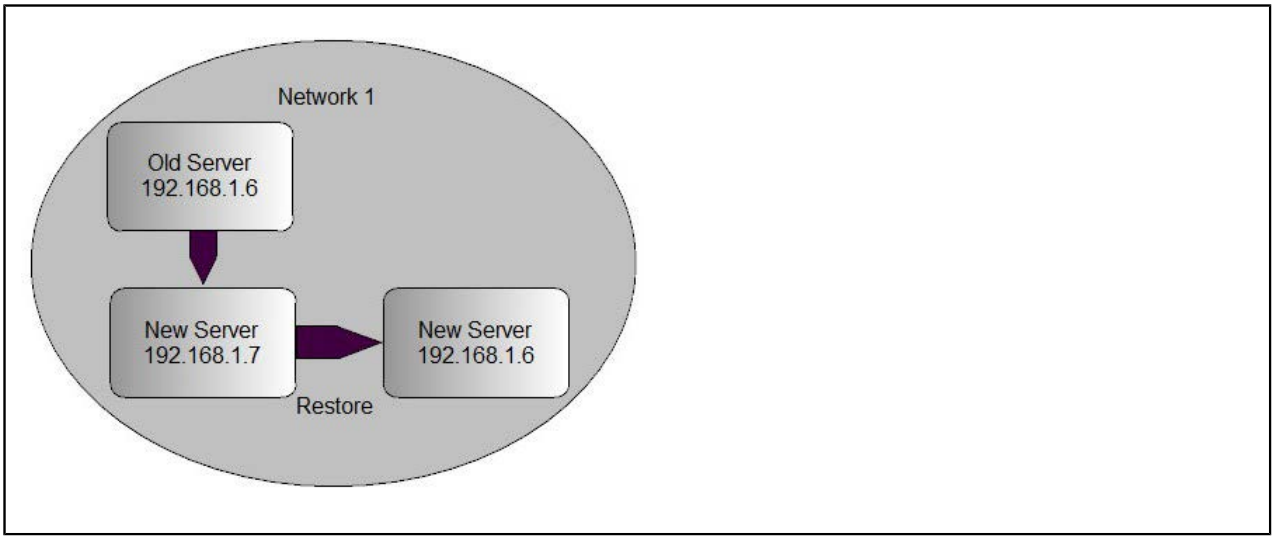


Figure 26: IP Addressing — Two Servers on a Single Network

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).

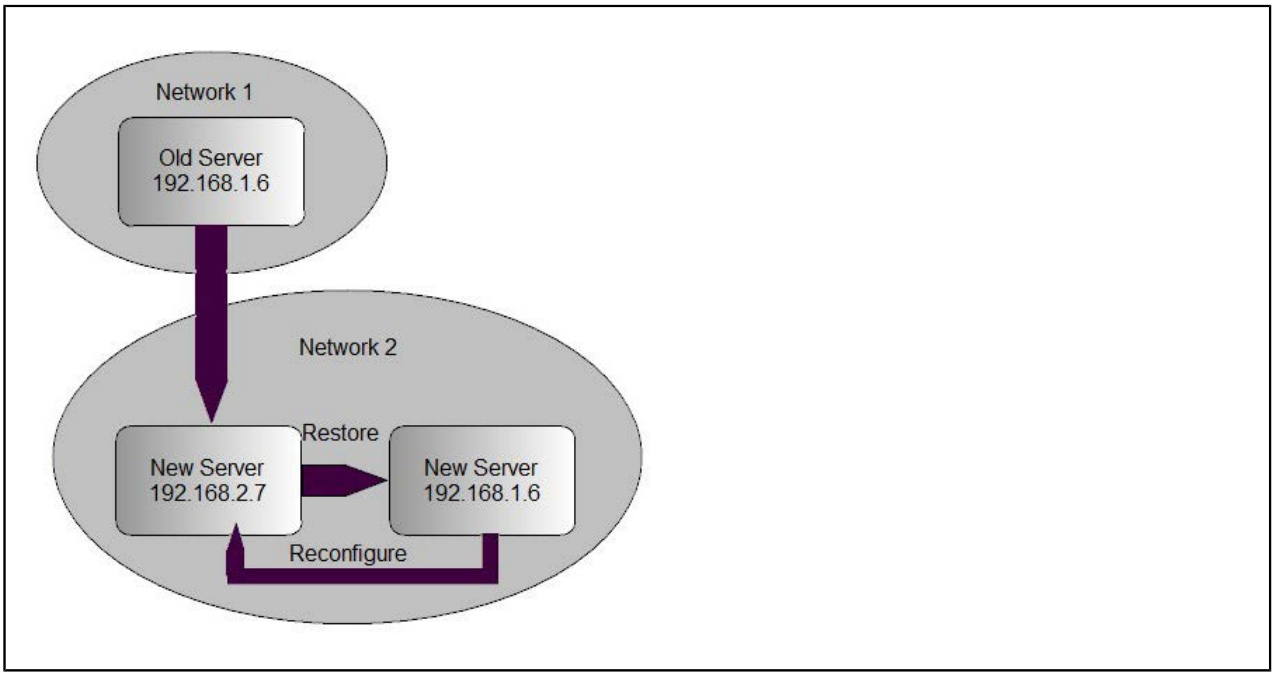


Figure 27: IP Addressing — Two Servers on Two Networks

Restore from a running server

To restore from another running server:

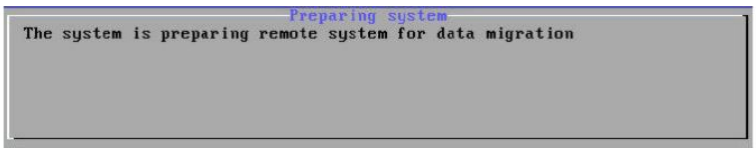
1. Install MSL software on the new server.
2. In the MSL server console of the new server, when prompted to "Restore from backup?", select Yes.
3. When prompted, select Restore from another running server.
4. If your system has more than one network adapter, select the adapter to use for the restore 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.

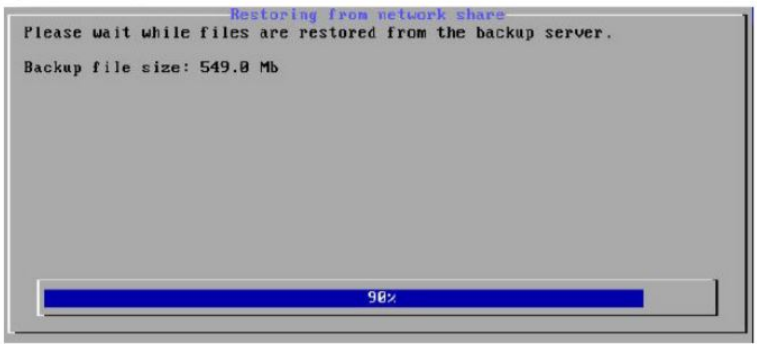
7. Enter the IP address of the existing server.
8. If the two servers are on different IP networks, MSL will prompt for the gateway IP address to use to access the existing server. (This prompt does not appear if both servers are on the same, connected network.)
9. When prompted, enter the “admin” password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

10. MSL does the following:

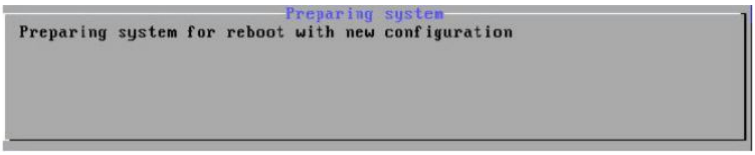
    - Configuration and application data is backed up from the existing server.



    - 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.

Restore in a Cloud Deployment

When performing a restore in a cloud deployment a new VM instance will have its own networking configuration requirements.

- On every boot networking will be checked and auto configuration is performed if changes detected from the last boot.

12.5 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.

12.6 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.

12.7 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 kernal boot line.
4. In the kernal boot line, type " **rw init=/sysroot/bin/sh**" (note the leading space) and then press **Enter**.
5. When the bash shell prompt appears, do the following:

   - Type "**chroot /sysroot**", and then press **Enter**.
   - 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 "**reboot -f**" and press Enter to initiate a system reboot.

Troubleshooting 13

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/DVD 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 14

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 15

This chapter contains the following sections:

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.

15.1 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.

15.2 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 (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

15.3 Original SSLeay License

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

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@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:

15.4 Jarkko Turkulainen License

Copyright (c) 2003 Jarkko Turkulainen. 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.

THIS SOFTWARE IS PROVIDED BY JARKKO TURKULAINEN ``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 JARKKO TURKULAINEN 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.

15.5 OpenOSP License

The Vovida Software License, Version 1.0 Copyright (c) 2000 Vovida Networks, 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:

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. The names "OpenOSP", "OpenOSP server" and "Cisco" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openosp@vovida.org.
4. Products derived from this software may not be called "CISCO" or "OpenOSP", nor may "CISCO" or "OpenOSP" appear in their name, without prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DAMAGES IN EXCESS OF $1,000, NOR FOR ANY 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.

15.6 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 MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

15.7 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 maybe 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.

15.8 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 gdttf.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.

15.9 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.

15.10 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

15.11 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.

15.12 Open Source License for Oracle Berkeley DB

GNU AFFERO GENERAL PUBLIC LICENSE

Version 3, 19 November 2007

Copyright (C) 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 Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are 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.

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.

Developers that use our General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about.

The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

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 Affero 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. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

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 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 work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero 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 Affero 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 Affero 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 Affero 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