Mitel SIP Teleworker via MBG on MiVoice Office 400

DEPLOYMENT GUIDE

Version 1.1

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

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

TRADEMARKS

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

© Copyright 2018, Mitel Networks Corporation

All rights reserved

Mitel SIP Teleworker via MBG on MiVoice Office 400
Version 1.1 – 05.2018

Table of Contents

Overview ... 4

Introduction ... 4

Abbreviations ... 4

Preconditions ... 5

AMC licenses ... 9

Create ARID for MBG ... 10

Customer Data ... 18

Prepare MiVoice Office 400 ... 21

MiVoice Border Gateway Installation / Configuration ... 30

Install MBG virtual appliance - ESXi ... 30

Trusted Networks (for MBG) ... 69

MSL: Enter ARID ... 70

MSL: Manage Web server certificate ... 73

Certificates ... 73

Let's Encrypt ... 74

Request a "Let's Encrypt" SSL Certificate ... 75

Verify the installed certificate ... 82

Uninstall a Let's Encrypt SSL Certificate ... 83

Other Third party Certificate ... 84

Create a Certificate Signing Request ... 84

Upload and install a Certificate ... 88

MBG: System configuration: Network profile ... 92

MBG: System configuration: Settings ... 95

MBG: System configuration: Port ranges ... 99

MBG: Service configuration: ICPs ... 101

MBG: Administration: File transfer ... 104

Web proxy for SSP access ... 109

Mitel SIP phone: Start-up ... 112

Set config-server in phone GUI ... 113

Set config-server in the TUI ... 116

Login screen ... 119

Maintenance ... 121

Overview

Introduction

The user of a SIP terminal can work remotely (teleworker) i.e. behind an MiVoice Border Gateway (MBG). When doing so, the user has access to all the normal features of the MiVoice Office 400 communication server, including the XML applications on the phones. Additionally, the user has access the Self Service Portal (SSP) and is able to change his personal configuration there.

For registration, two sets of SIP credentials are needed. These need to be configured both on the MiVo400 communication server and on the MBG. The Mitel SIP terminal receives the appropriate credentials in the configuration file.

MiVoice Office 400 supports the export of the teleworker SIP terminal data for the MBG configuration. With this, the “Bulk Provisioning” of the MBG can be executed and the SIP terminals are configured in the MBG. All other MBG configurations needs to be done manually.

Abbreviations

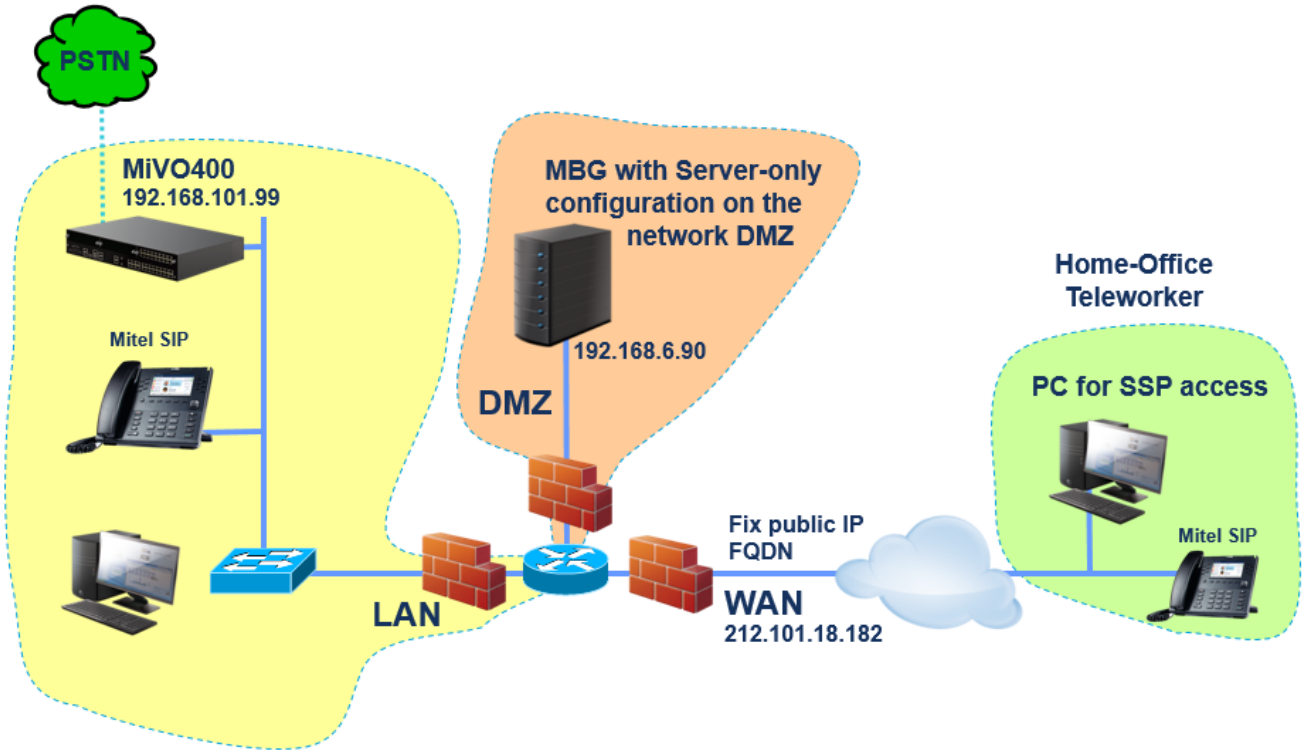
Abb.	Description
AMC	Applications Management Center (License server for MBG,…)
ARID	Application Record ID
CSR	Certificate Signing Request
GUI	Graphical user interface
ICP	IP Communication Platform (e.g. MiVoice Office 400)
MBG	MiVoice Border Gateway
RCS	Redirect and Configuration Server
SSP	MiVO400 Self Service Portal
TUI	Terminal user interface

Preconditions

The following pre-requisites must be in place before starting to configure the teleworker solution.

- **MiVoice Office 400** software must be **R6.0 or higher**
- MiVoice Border Gateway (**MBG**) software must be **10.1 or higher**

Mitel SIP Phone Teleworker with MiVO400



- **FQDN for the MBG** system (e.g.: mbg.mycompany.com) must be resolvable externally to the public IP of MBG.
- A **second FQDN for MiVO400 Self Service Portal (SSP)** access (e.g.: ssp.mycompany.com) must be resolvable externally to the public IP of MBG and internally to the MiVO400 IP.
- A 3rd party signed **certificate** if not using Let's Encrypt (the CSR is generated under MSL "Web Server" certificate view)
- Mitel SIP Phone of type 6800i family or 6900 family

Firewall rules

All involved firewalls have to match the following settings

WAN to DMZ

From external to MBG in the DMZ
Open (and forward) the following ports:

Port	Type	Protocol	Comment
80	tcp	HTTP	for Mitel SIP phone configuration over HTTP including first "startup.cfg", MBG root CA files and language files
69	udp	TFTP	(OPTIONAL only if http can't be used) for Mitel SIP phone configuration over TFTP including first "startup.cfg", MBG root CA files and language files
443	tcp	HTTPS	for MiVO400 SSP access via Remote Proxy Server
4430	tcp	HTTPS	XML listen port for Mitel SIP phones (4430 is default value)
5061	tcp	SIP TLS	Teleworker to MBG
20000 - 21999*	udp	RTP / SRTP	Voice Communication. Must match with the port range setting on MBG

* 20000 is for Teleworker Network Analyzer.

DMZ to WAN

From MBG in the DMZ to external
Open the following ports:

Port	Type	Protocol	Comment
22	tcp	SSH	MBG to Mitel AMC, for licensing and blade visibility
53	udp	DNS	look up IP address on public DNS server
80	tcp	HTTP	Let's Encrypt Certificate
123	udp	NTP	Time server access
443	tcp	HTTPS	Let's Encrypt Certificate

DMZ to LAN
Open the following ports:

Port	Type	Protocol	Comment
80	tcp	HTTP	XML to MiVO 400
53	udp	DNS	look up IP address on corporate DNS server
69	udp	TFTP	MBG to MiVO400 (to get first startup.cfg and language files)
443	tcp	HTTPS	MBG to MiVO400 (for real configuration and XML, plus MiVO400 SSP access via Remote Proxy Service)
5060	tcp	SIP	MBG to MiVO400 (for SIP signaling)
5061	tcp	SIP/TLS	MBG to MiVO400 (for SIP signaling if TLS is required in the LAN)
5004 - 5131	udp	RTP	Voice Communication (Standard media switch / EIP module)
3000 - 3023	udp	RTP	Voice Communication (Mitel SIP phones)
16230 - 16399	udp	RTP	Voice Communication (SIP-DECT)
30000 - 30023	udp	RTP	Voice Communication (MiVoice 5300 IP phones)
40000 - 40499	udp	RTP	Voice Communication (ViApp media server)

LAN to DMZ
Open the following ports:

Port	Type	Protocol	Comment
22	tcp	SSH	(OPTIONAL) if SSH access to MBG is required
443	tcp	HTTPS	Web configuration for admin MBG
5060	tcp	SIP	MiVO400 to MBG (MSIP Teleworker)
5061	tcp	SIP/TLS	MiVO400 to MBG (for SIP signaling if TLS is required in the LAN)

20000 - 21999	udp	RTP	Voice Communication. Must match with the port range setting on MBG

Remote (Teleworker) Site
No special requirements for home deployments as home routers normally allow outgoing connections.
In the case that the solution is deployed at a remote site fronted by a managed firewall, the remote site firewall rules must allow the phones to reach:

Teleworker-LAN to WAN
Open the following ports:

Port	Type	Protocol	Comment
21	udp	FTP	to FTP firmware server
53	udp	DNS	look up IP address on public DNS server
123	udp	NTP	Time server access
80	tcp	HTTP	for Mitel SIP phone configuration over HTTP including first "startup.cfg", MBG root CA files and language files
69	udp	TFTP	(OPTIONAL only if http can't be used) for Mitel SIP phone configuration over TFTP including first "startup.cfg", MBG root CA files and language files
443	tcp	HTTPS	to RCS (rcs.aastra.com) if RCS is used for deployment
4430	tcp	HTTPS	XML menus and keys for Mitel SIP phones
5061	tcp	SIP TLS	Mitel SIP phone to MBG (for SIP signaling)
20000 - 21999*	udp	SRTP	Voice Communication. Must match with the port range setting on MBG

* 20000 is for Teleworker Network Analyzer.

AMC licenses

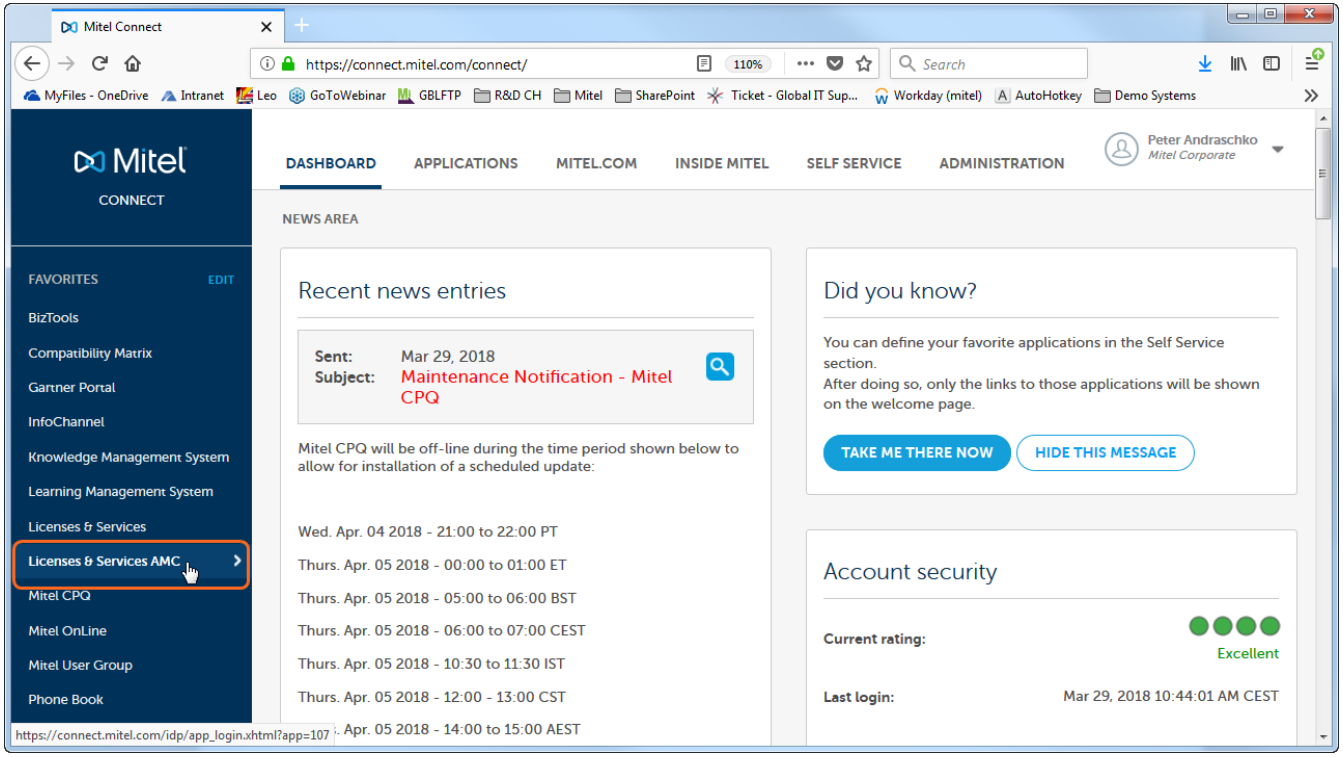
MiVoice Border Gateway Products

Quantity	Article No.	Product	Remark
1	54005339	MiVoice Border Gateway Virtual	MBG Virtual Appliance
5	54004572	MBG Teleworker Service x1	For Mitel SIP phone as Teleworker
	54004573	MBG Teleworker Service User x10	
	54004574	MBG Teleworker Service User x25	
	54004575	MBG Teleworker Service User x50	
	54004577	MBG Teleworker Service User x100	
	54004491	MBG: 1 SIP Trunking Channel License	Option: To use MBG as Proxy between IPC and SIP provider
	54009229	SWA Std 1y MiV BG System	
	54007973	SWA Std 3y MiV BG System	
	54007981	SWA Std 5y MiV BG System	
	54009232	SWA Std 1y MiV BG Telewk User	
	54007974	SWA Std 3y MiV BG Telewk User	
	54007982	SWA Std 5y MiV BG Telewk User	
	54009230	SWA Std 1y MiV BG SIP Connect	
	54007971	SWA Std 3y MiV BG SIP Connect	
	54007979	SWA Std 5y MiV BG SIP Connect	

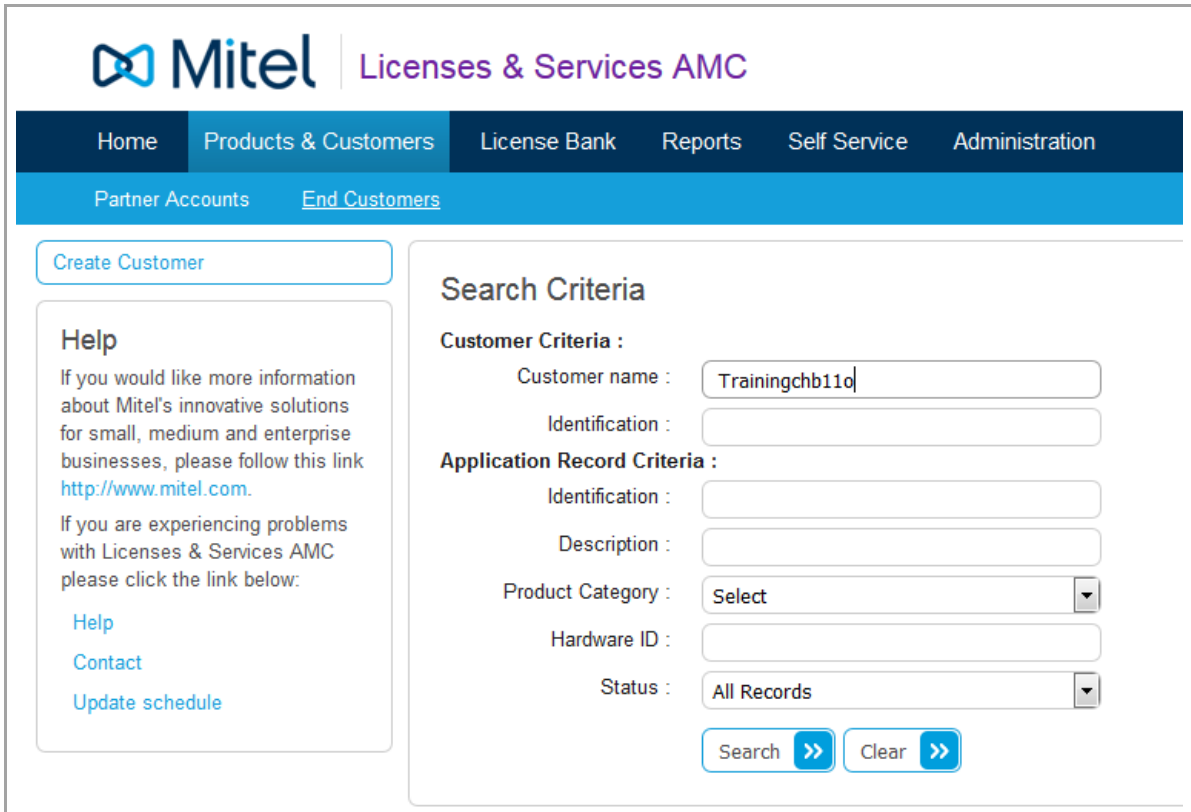
Create ARID for MBG

After ordering the necessary MiCollab/MBG licenses via Mitel CPQ, these licenses are automatically transferred to the license bank of AMC.

A technician/partner has to do the following steps:



Login to Mitel connect and select "License server AMC"

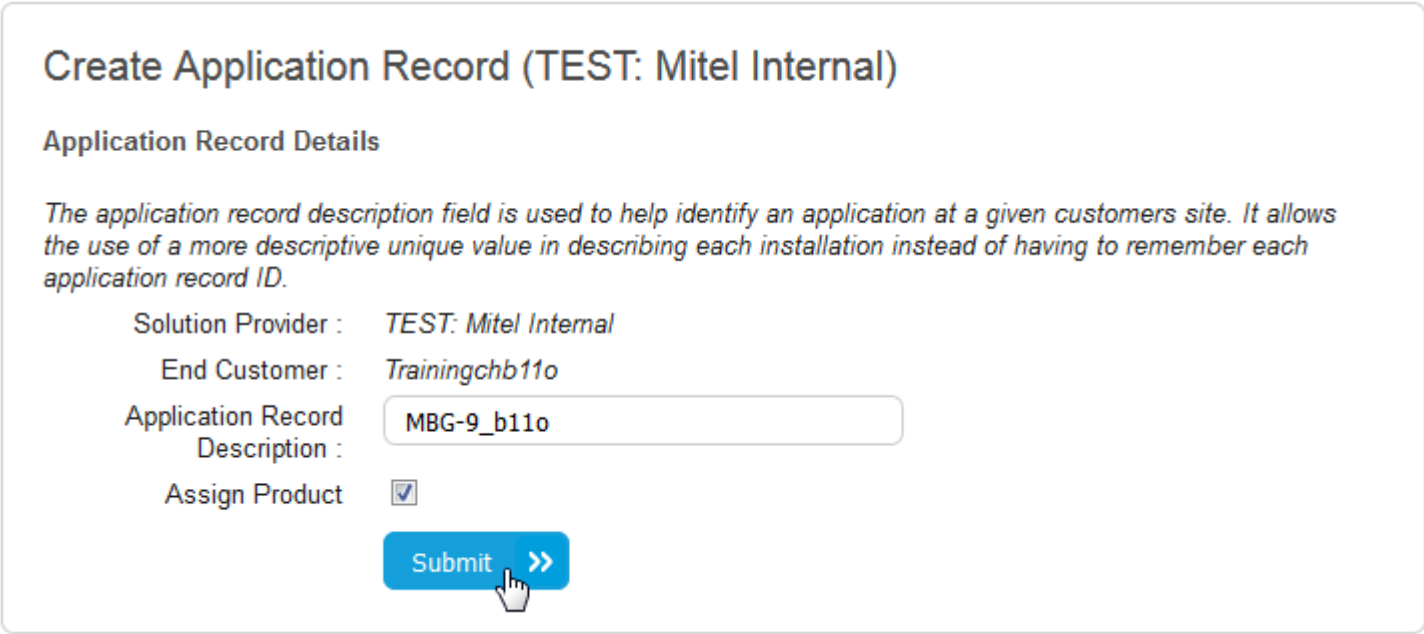


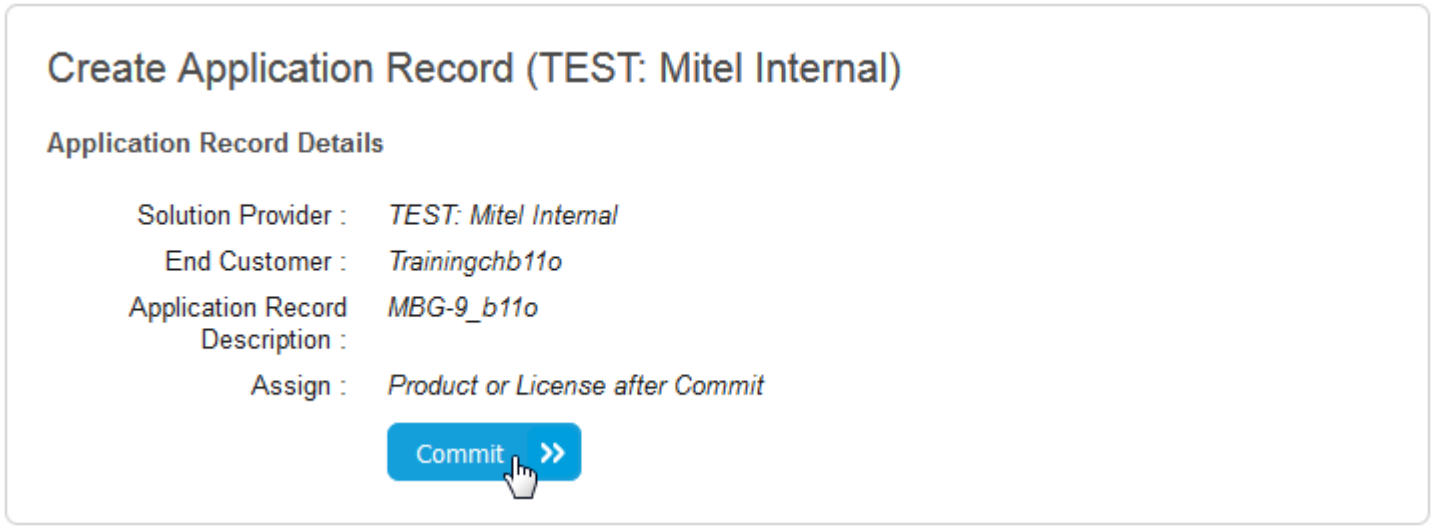
Select "Customer"

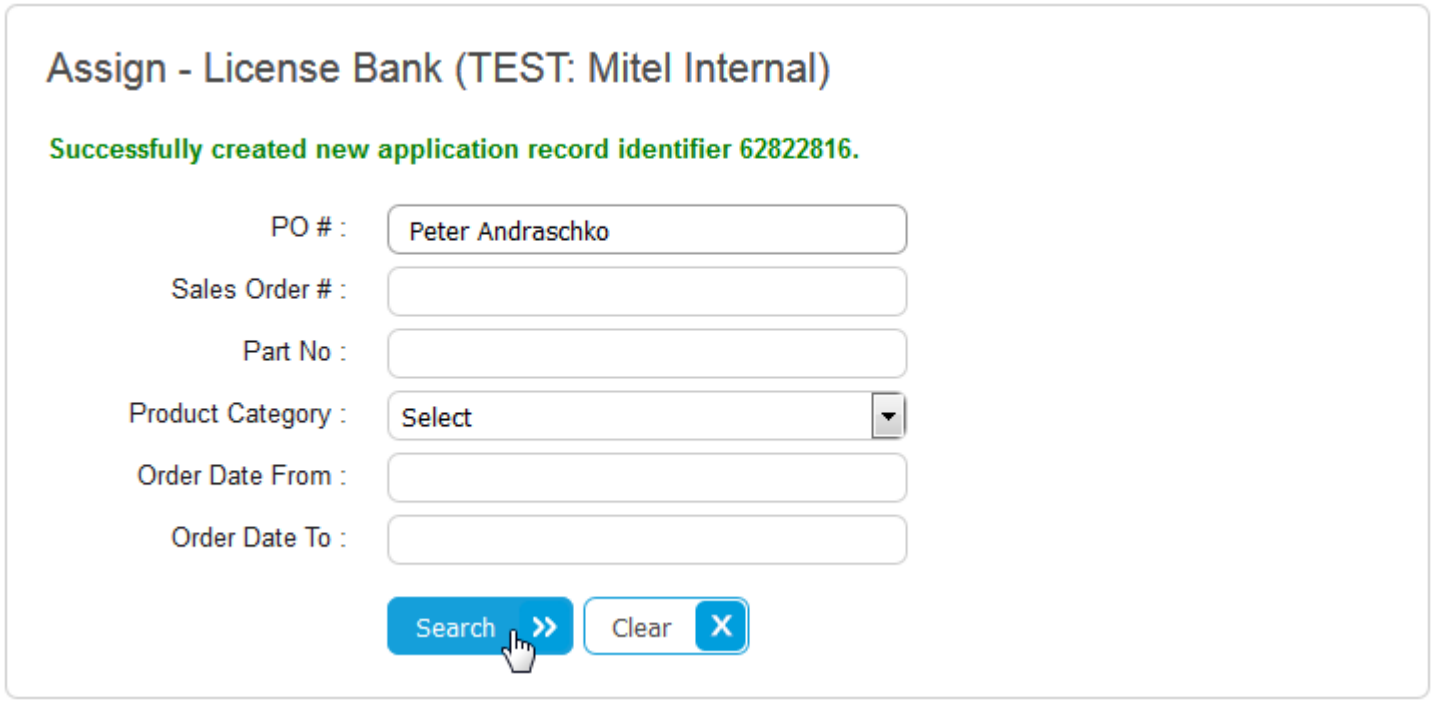
and "Search" for your customer

or

create a new customer

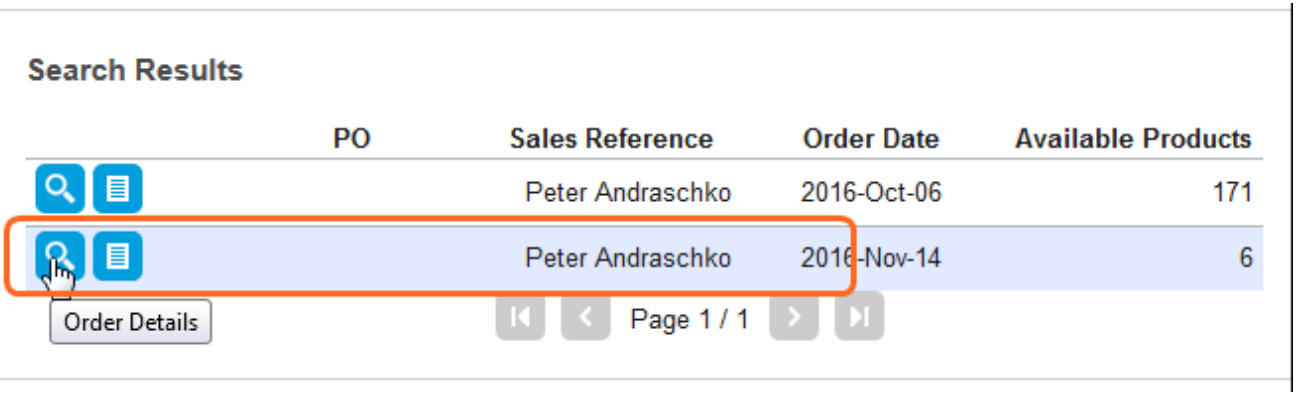
	Click "Create App Record"
	Enter a description, select "Assign Product" and click "Submit".


Create Application Record (TEST: Mitel Internal)
Application Record Details
Solution Provider : TEST: Mitel Internal
End Customer : Trainingchb11o
Application Record Description : MBG-9_b11o
Assign : Product or License after Commit
Commit



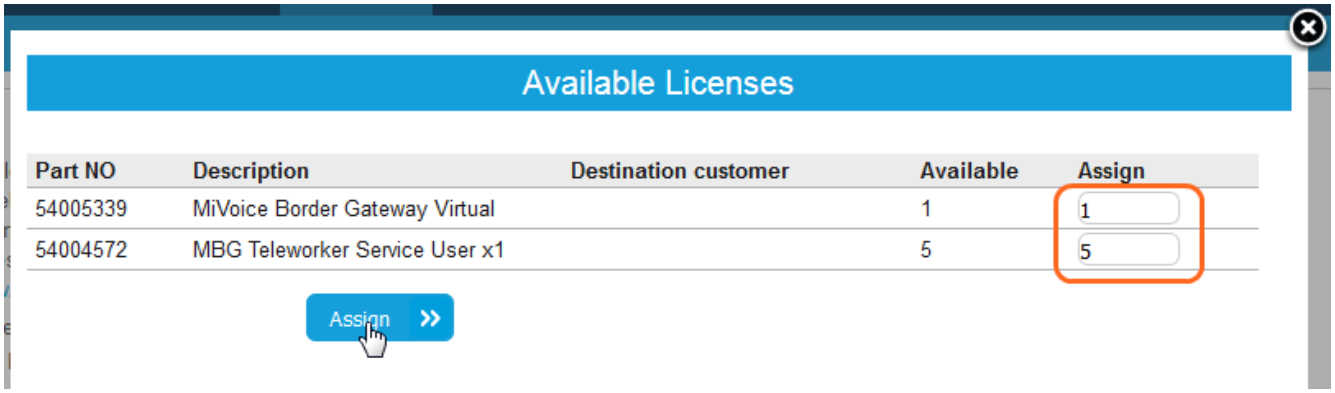
The ARID is successfully created.
Store this ARID in the customer data file for MBG.

Enter your purchase order number or your sale order number to search for your licenses.

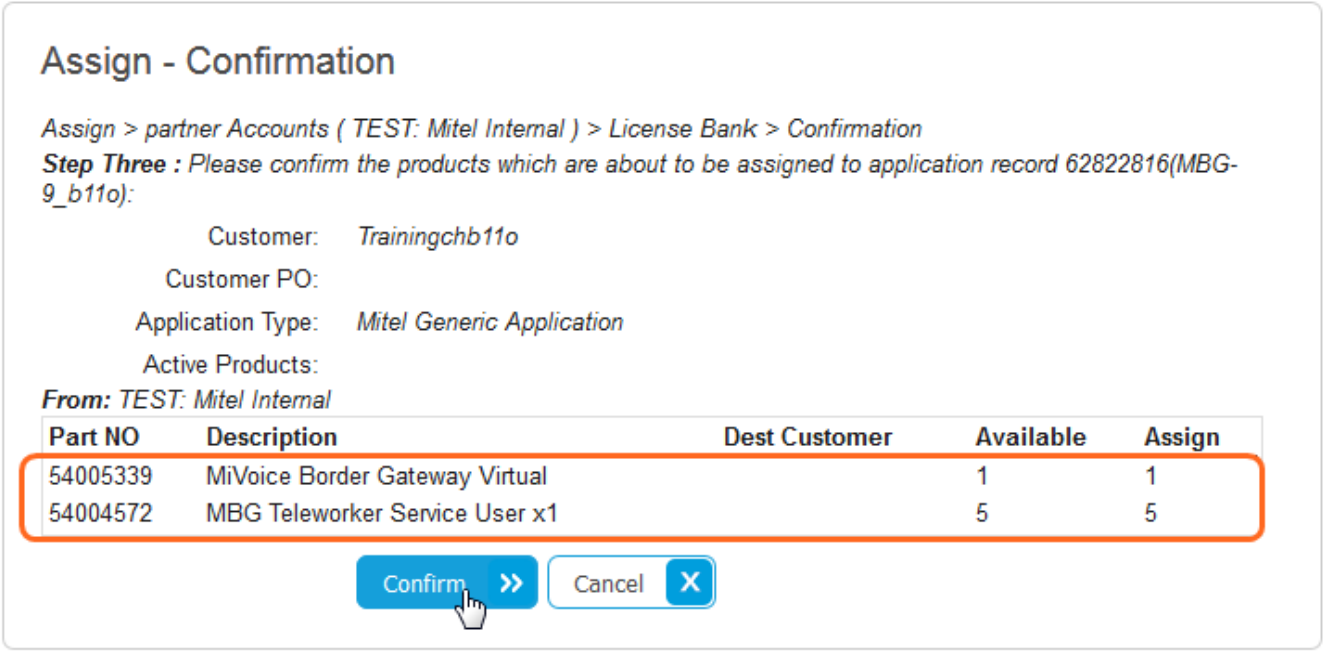


Filter your purchase orders and open the order details by clicking the "magnifying glass"

.



For the MBG server the ARID needs this licenses assigned.



"Confirm"

Assignment Confirmation - Transaction Report

REQUIRED: The assignment date of your licenses is still within the first 30 days of SWA service assignment.
You can apply SWA by clicking this link.

Recipient Details: Assignment

The following is the status of the assignment of the following products onto application record 62822816 **(MBG-9_b11o)**.
Please keep the transaction reference for future reference and communication with the support staff.

Customer Name: Trainingchb11o
Customer PO:

Transaction Reference: **PTQMPVSFNL97GP6A**
Customer Reference:
Date: **Nov 15 2016**

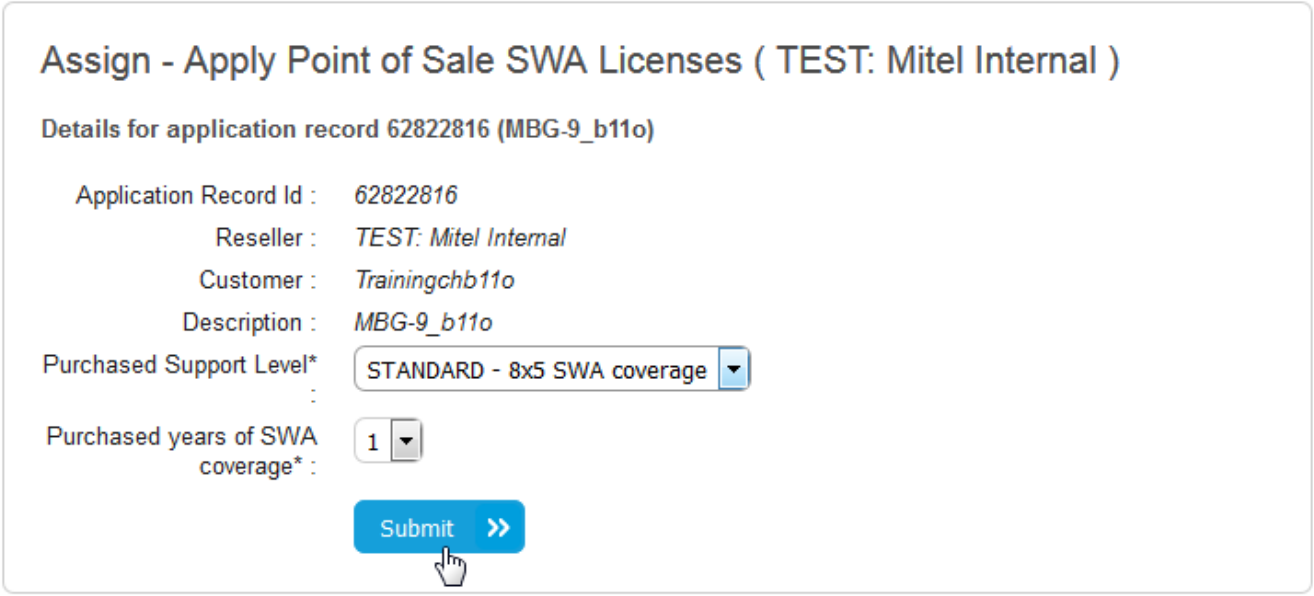
		Overall Status		
		Total Items	**Successes**	**Failures**
Transaction Audit Trail		6	6	0
Product No.	**Description**	**Items**	**Success**	**Failure**
54005339	MiVoice Border Gateway Virtual	1	1	0
54004572	MBG Teleworker Service User x1	5	5	0

Apply SWA » Done »

Hit "Done " to finish the licensing process.

The first 30 days Software Assurance (SWA) is available.

Select "Apply SWA" for proper Software assurance.

<table>
<tr><td> 
</td><td>Please note:
Premium SWA is not supported for MBG together with MiVO 400.
Hit "Submit"</td></tr>
<tr><td>Now the ARID for MBG is ready!</td><td></td></tr>
</table>

Customer Data

Please use this data sheet for your customer project to collect and safe all necessary data.
Entries in red may be replaced by your real data.

Customer / Company Name:	
Address (street):	
ZIP / Postal code	
City:	
Phone no.:	

Contact name:		Phone no.:		email:	
Channel partner:		Phone no.:		email:	

Common data

DDI range:	
internal number range	

MiVoice Office 400 system data

System type	vMiVO400
EID:	49065AE28839FC3400DD20C753521E807ECF
Sales channel:	CH-Freemarket
Host name:	mlx-10
Domain	micollabdemo.com
IP address:	192.168.101.99
DNS	192.168.1.5

User name:	admin	password:	your password

Software version	6.0 (8917a1)
License file:	your licence file
SWA basic until:	14.10.2021
SWA user:	50

ESXi server (VMWare, vSphere, vCentre)

Software version:	6.0		
IP address:	192.168.1.11		
User name:	admin	password:	****

MBG system data

Login credentials	user name	password
	admin	your password
Installed version:	10.1.0.175	
Updated to:		
Domain:	micollabdemo.com	
Host name	mbgchb11o	

	IP address	remarks
WAN	normally not used	
LAN	192.168.6.90	public fix IP: your public IP
Default gateway	192.168.6.1	
DNS server	192.168.1.5	

Trusted networks	subnet mask	gateway	remarks
192.168.1.0	255.255.255.0	192.168.6.1	Management network
192.168.101.0	255.255.255.0	192.168.6.1	LAN network (MiVO400)

ARIDs		remarks
MBG	12707414	

System size	users	
☑	150	Small business (1 vCPUs / 1 GB RAM / 20 GB HDD
☐	500	Enterprise (3 vCPUs / 2 GB RAM / 40 GB HDD

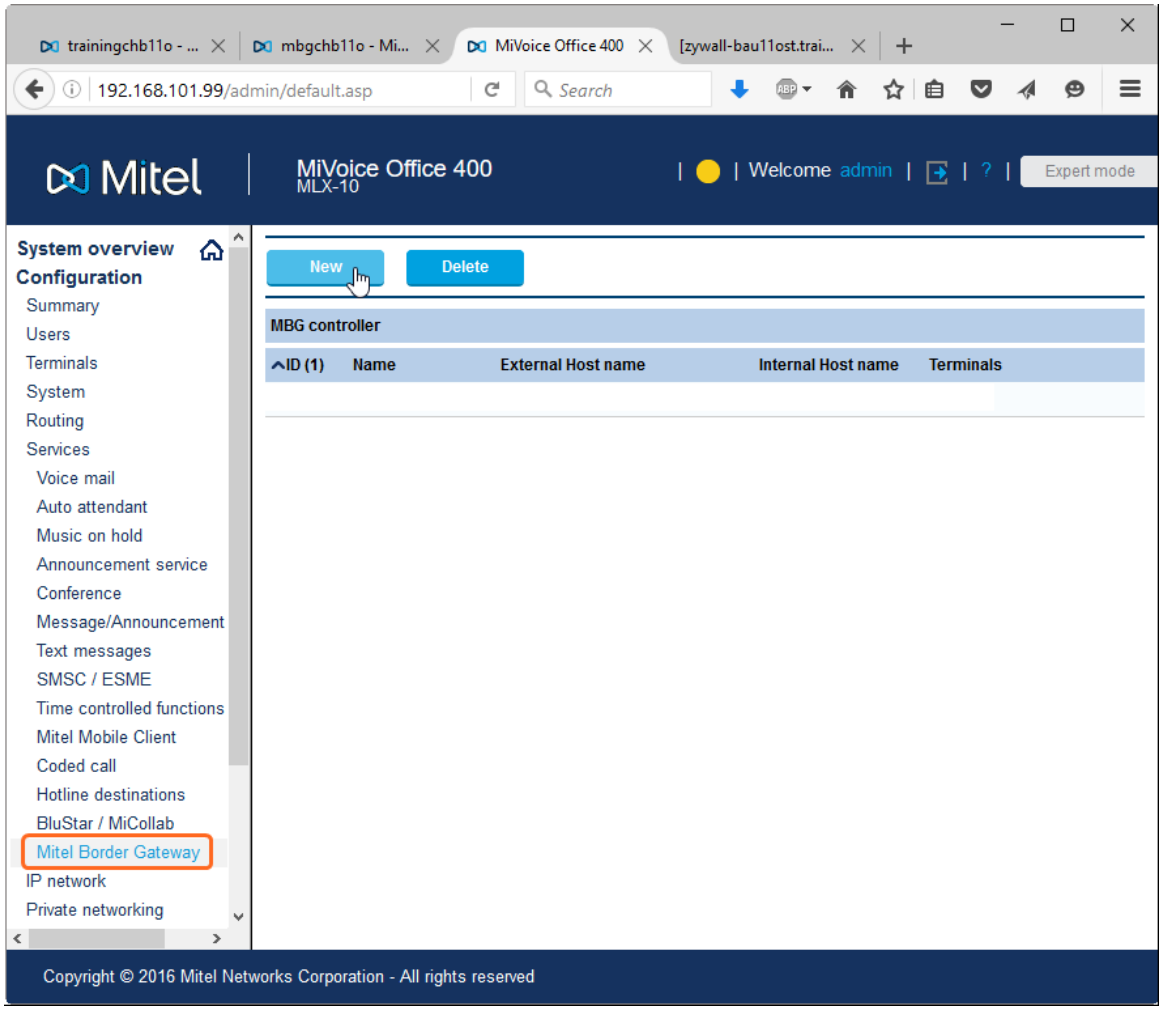
Host name (FQDN)	mbgchb11o.micollabdemo.com	

Certificate authority:		
☐	self-signed certificate	
☑	Let's Encrypt certificate authority	
	Common Name:	mbgchb11o.micollabdemo.com
	Alternate Name(s):	trainingchb11o.micollabdemo.com
☐	external certificate authority:	

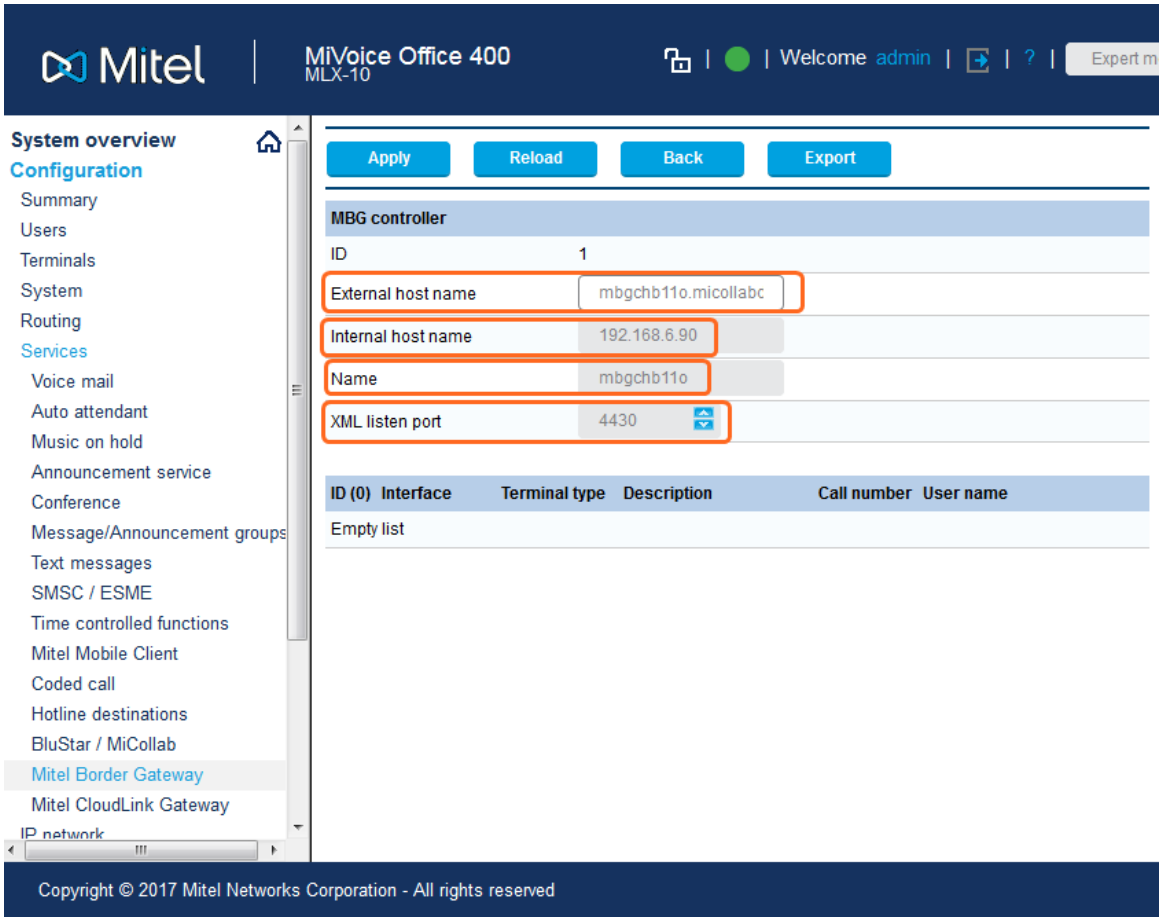
ICP XML listen port:	4430	this is the default port

Prepare MiVoice Office 400

MiVoice Office 400 Release 6.0 or higher is mandatory to use for this teleworker solution.



Add a new MBG

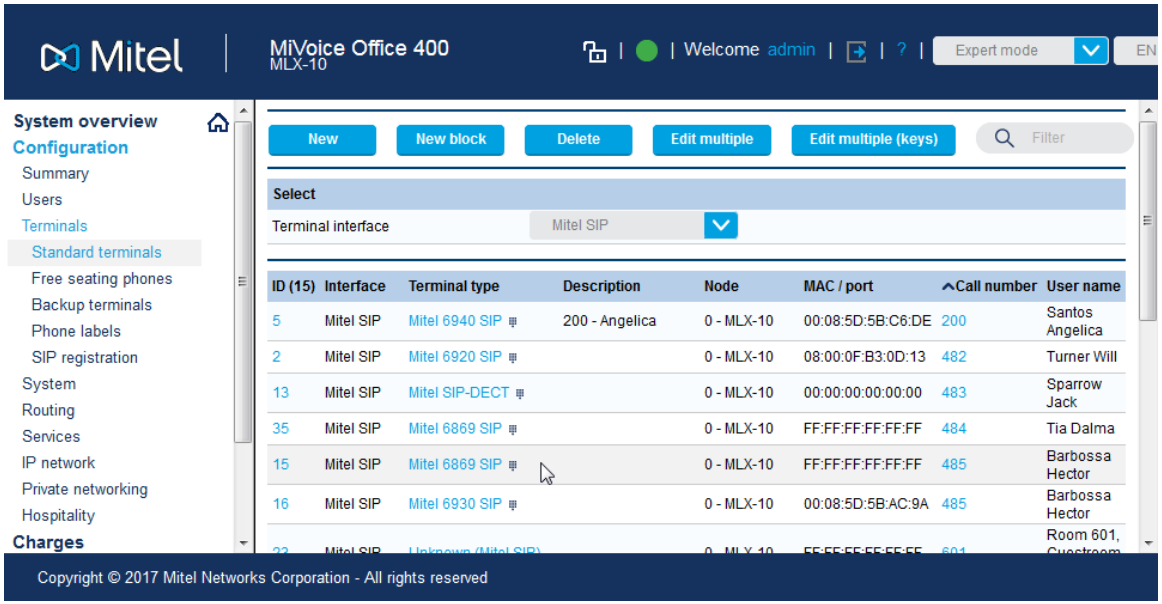


External Host name:
<public reachable FQDN >
e.g.:
mbgchb11o.micollabdemo.com

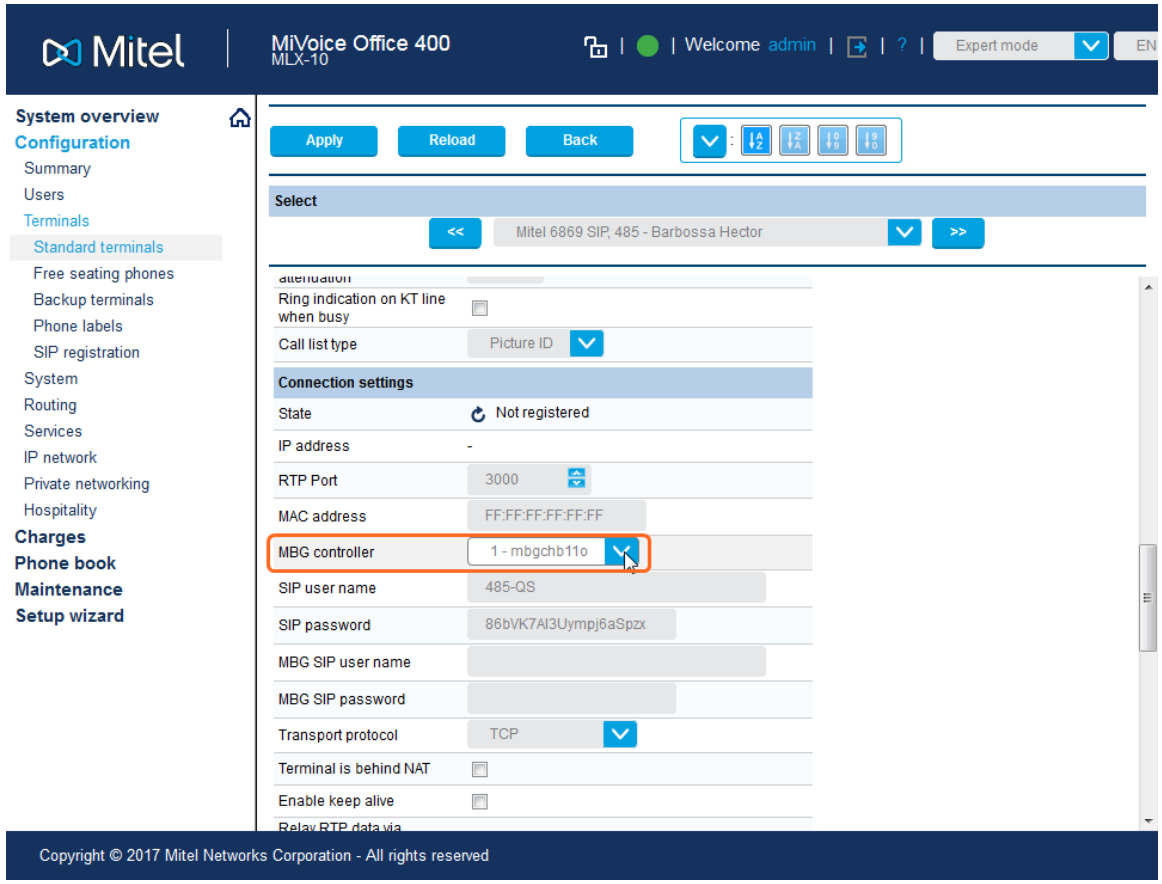
Internal Host name:
<IP address of MBG in DMZ>
e.g.: 192.168.6.90

Name: **<Name of MBG>**
e.g.: mgbchb11o

XML listen port: **4430**
(4430 is the default port on MBG for XML connection)



Go to "Standard terminals" and select the Mitel SIP phone, that should be used as Teleworker terminal.

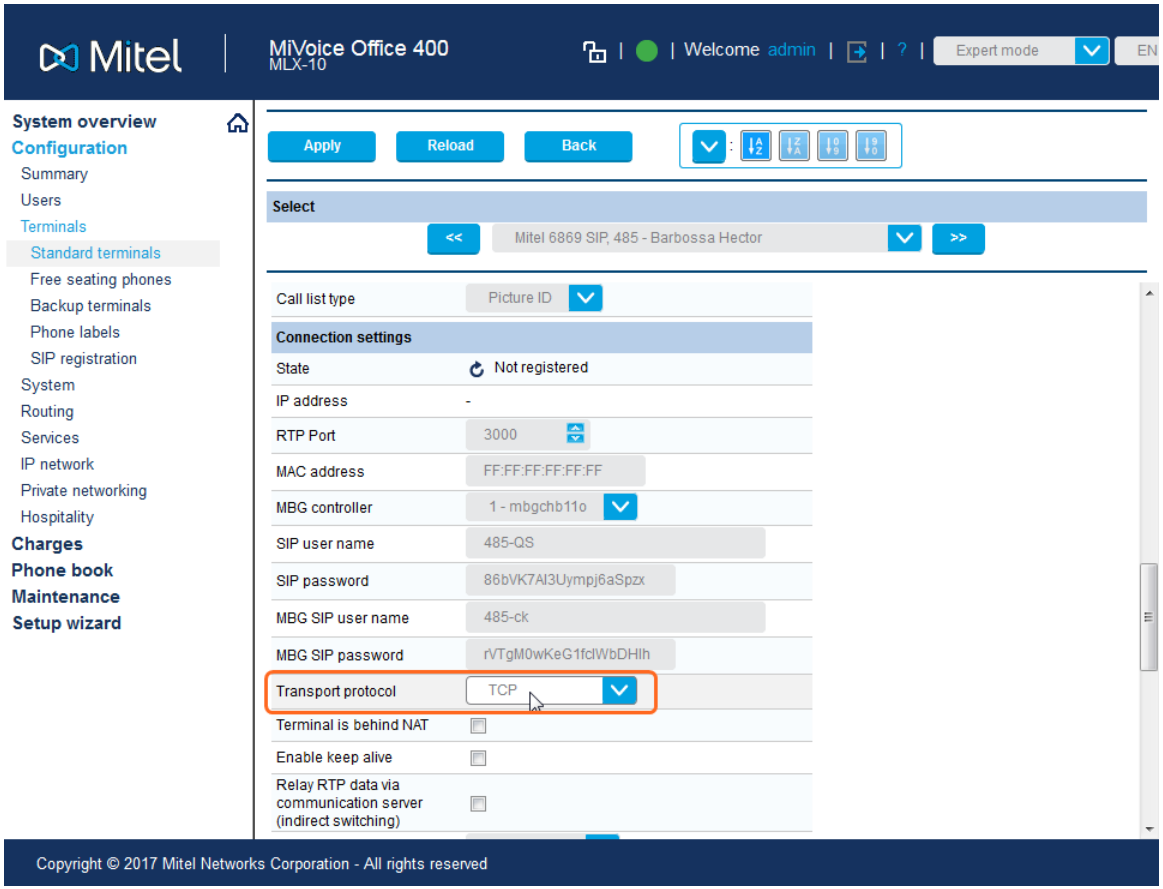


Scroll down to the connection settings.

MAC address must be empty
(i.e. shows FF:FF:FF:FF:FF:FF)

MBG controller:
<select the just created MBG>

Apply



The terminal gets a second set of SIP credentials.

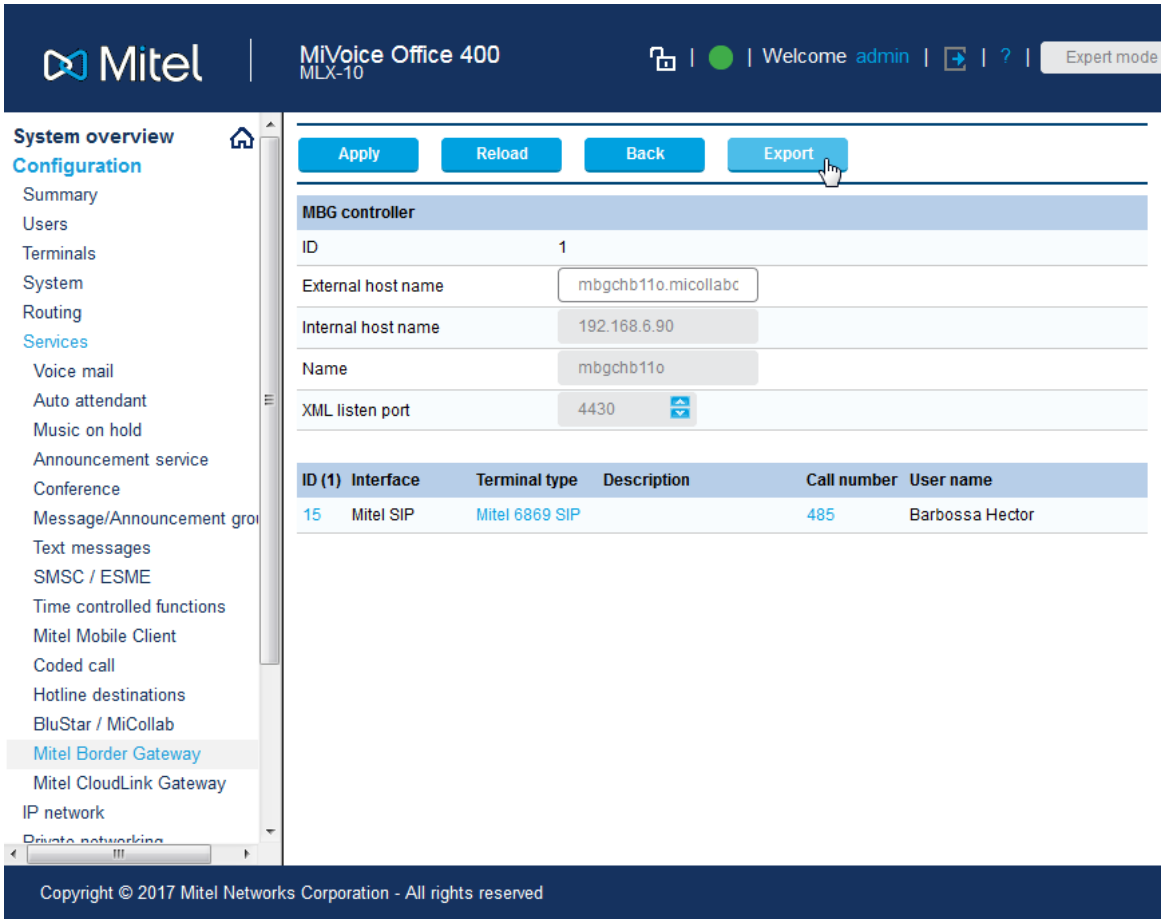
The normal SIP user name is now for the MBG, which registers with this credentials towards MiVO400.

The new "MBG SIP user name" is copied into the config file for the phone, so that the phone can register towards the MBG.

Set "Transport protocol": **TCP**

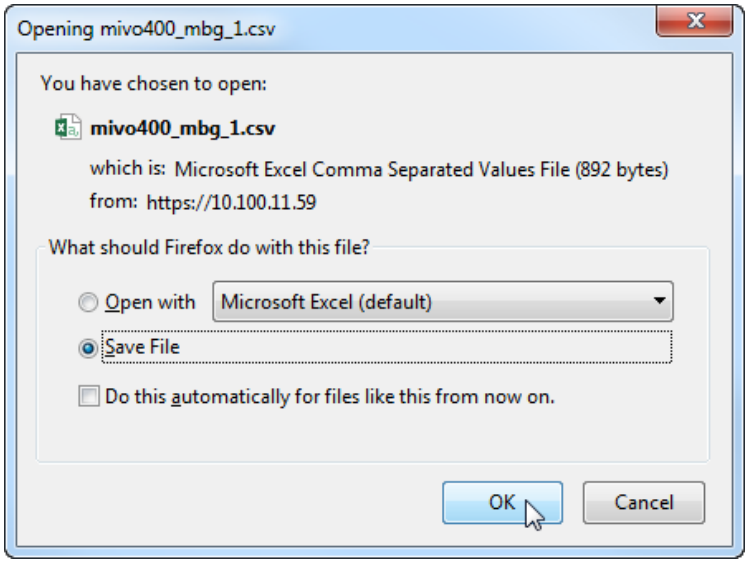
Apply

Do the same for all other Mitel SIP phones which should be used as teleworker set.

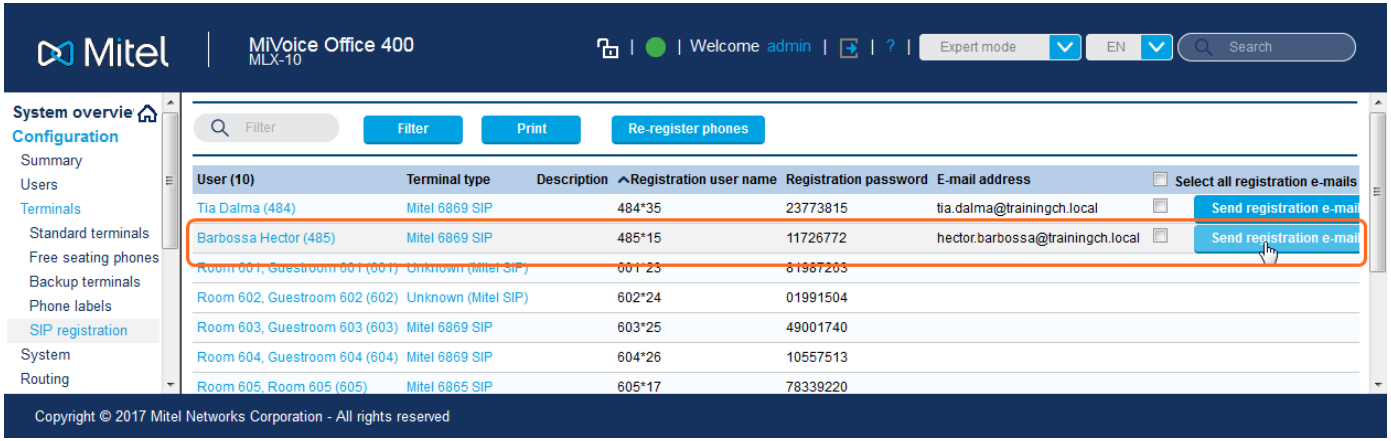


Go back to "Services -> MiVoice Border Gateway"

Export a csv file containing all Mitel SIP Teleworker settings for the MBG.

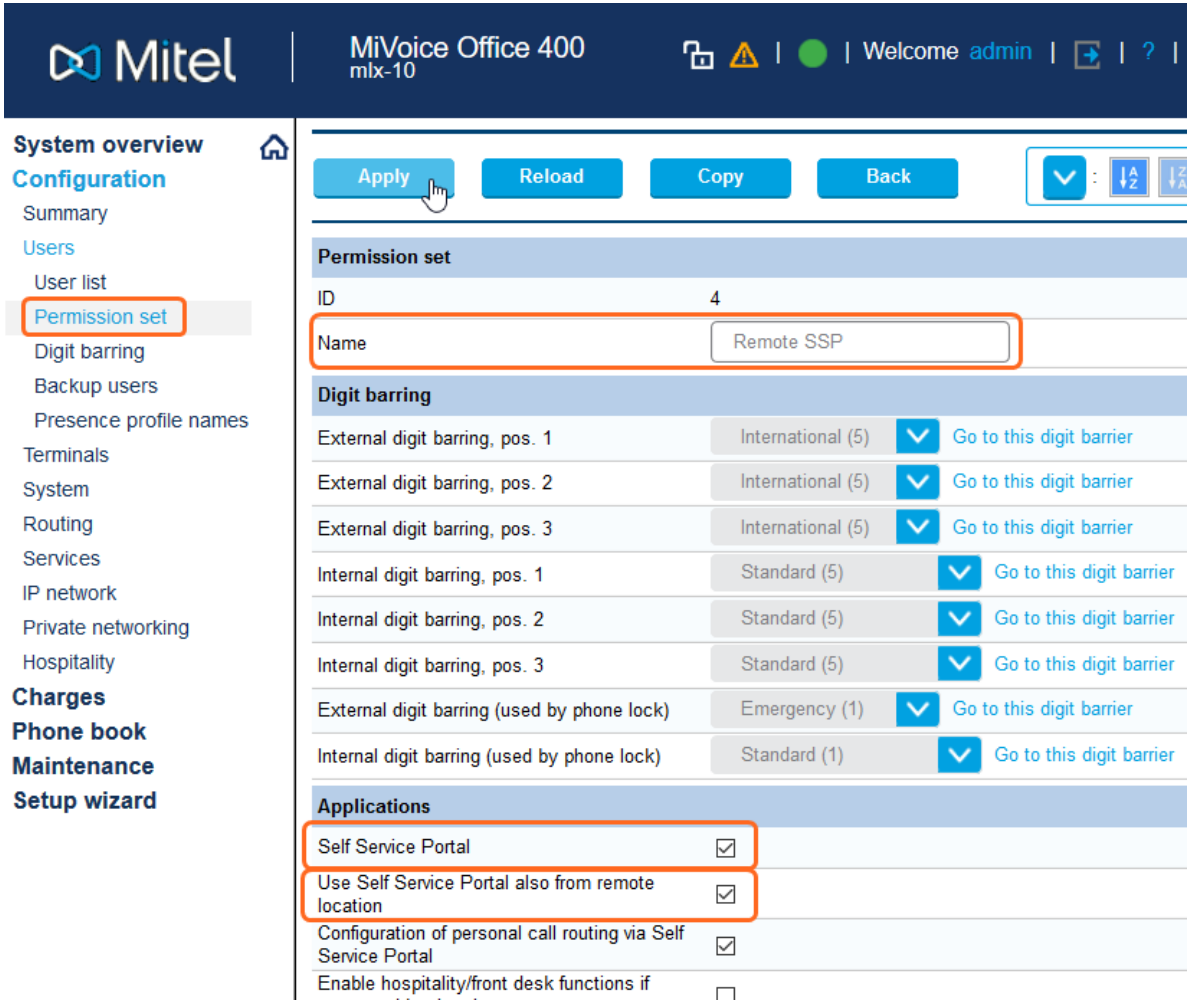


Save the file.



Go to "SIP registration" and send the registration credentials to the user.
(User must have an email address assigned and MiVO400 must be enabled to send out emails.)

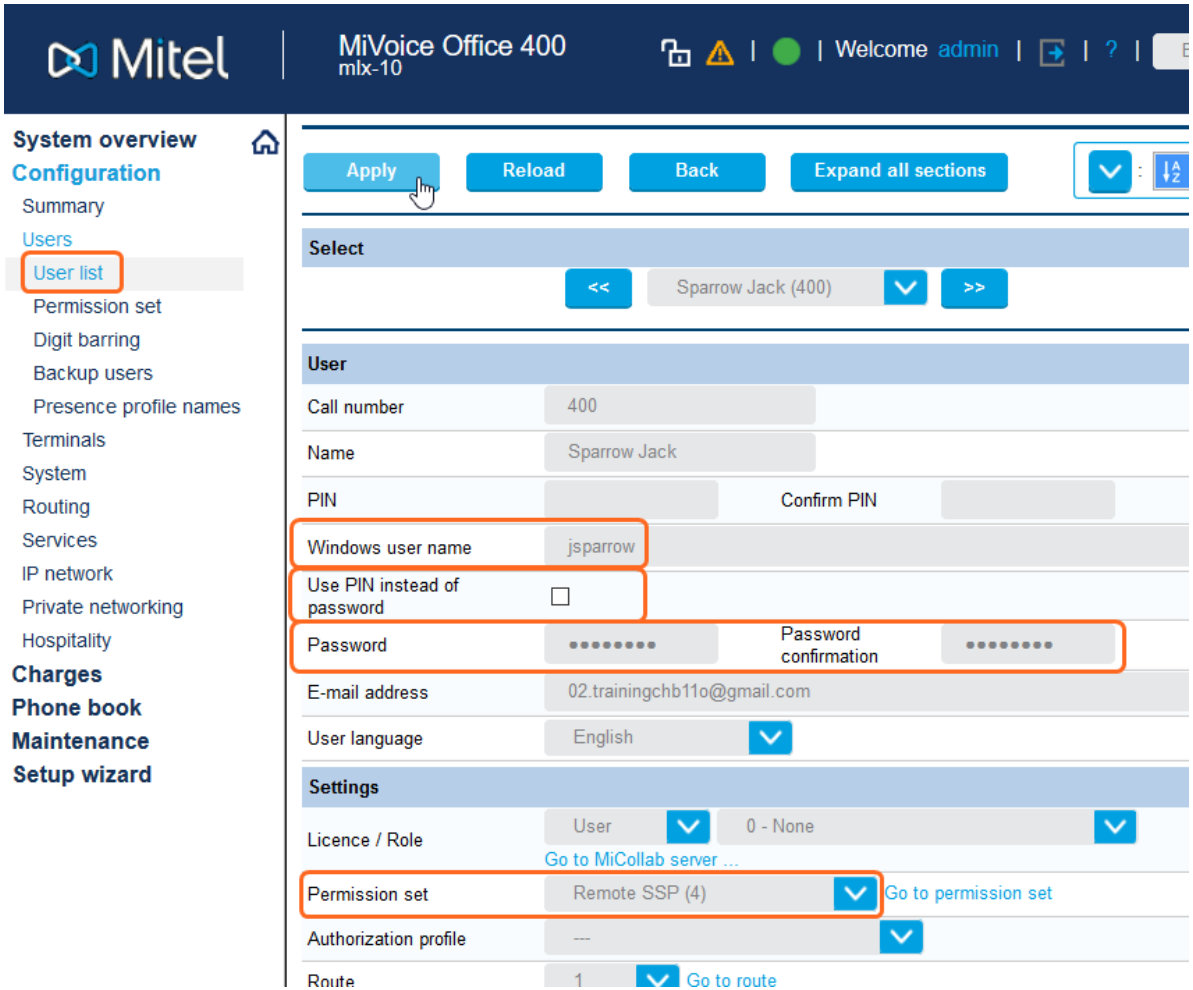
Preparing MiVO400 for an access to the SSP from remote, the following step have to be done:



Create a permission set which authorizes:

- Self Service Portal
- Use Self Service Portal also from remote location

"Apply" the settings



For each user, who wants to access the SSP from remote, set the following parameter:

- Windows user name
- Untick "Use PIN instead of password"
- Set a password.
  The password must be strong!
  - minimum 8 characters
  - uppercase letters A - Z
  - lowercase letters a - z
  - digits 0 - 9
  - special characters:
    ’?’ ’/’ ’<’ ’>’ ’.’ ’,’ ’-’ ’+’ ’*’ ’#’ ’=’ <space>

- Assign the appropriate permission set.

"Apply"

The user finally has to access to the SSP from remote by

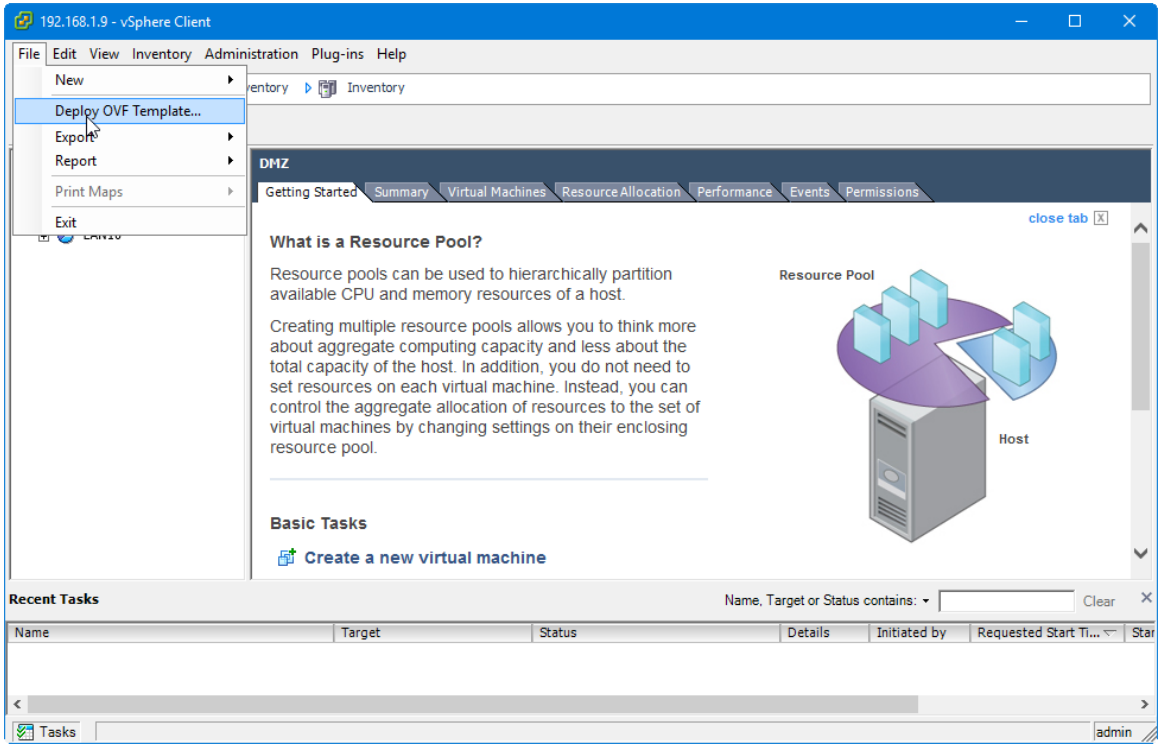
- connecting to URL: https: // <FQDN for SSP> and
- entering the user name and password on the login screen

("call number" and "PIN" are not allowed from remote).

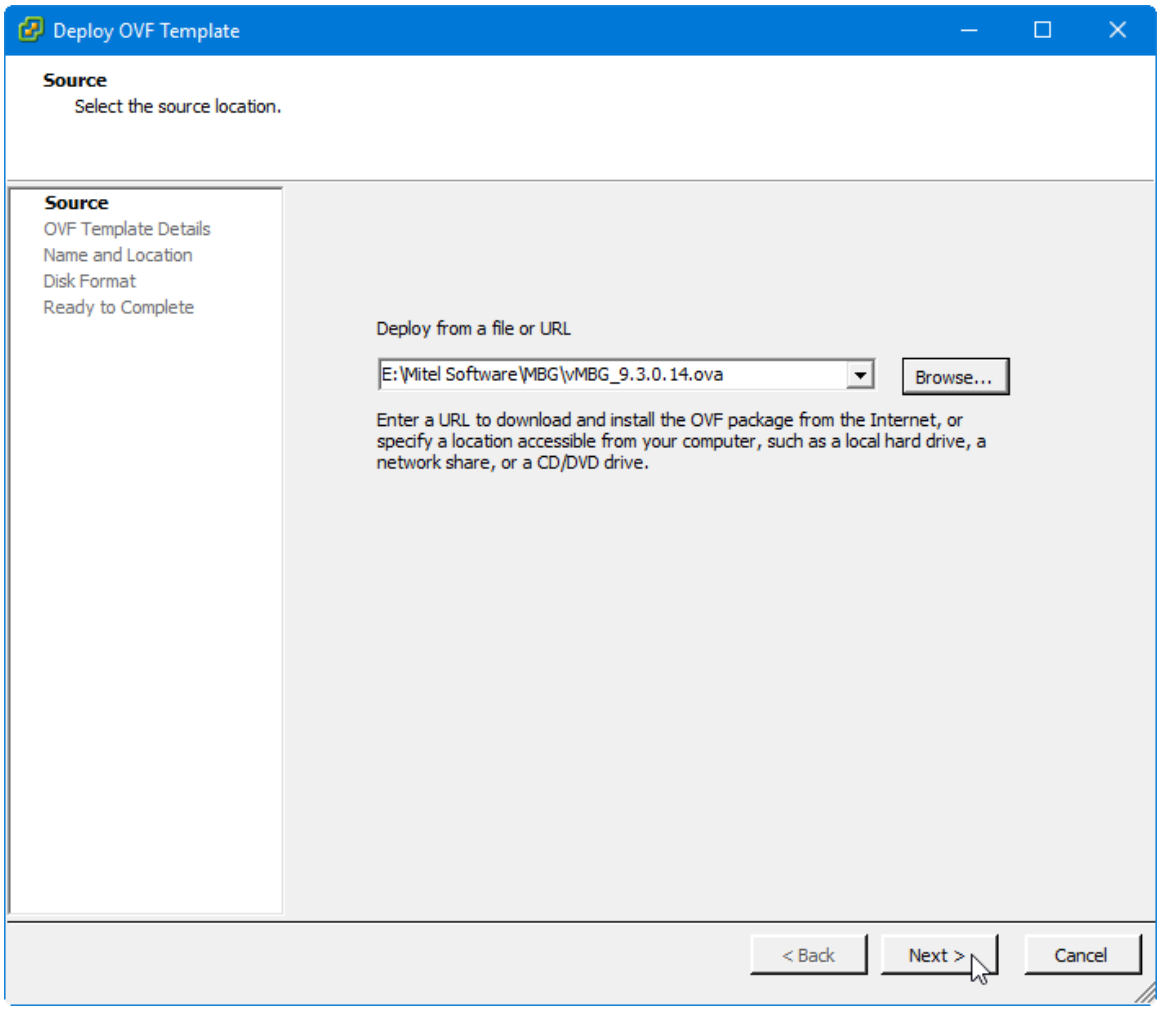
MiVoice Border Gateway Installation / Configuration

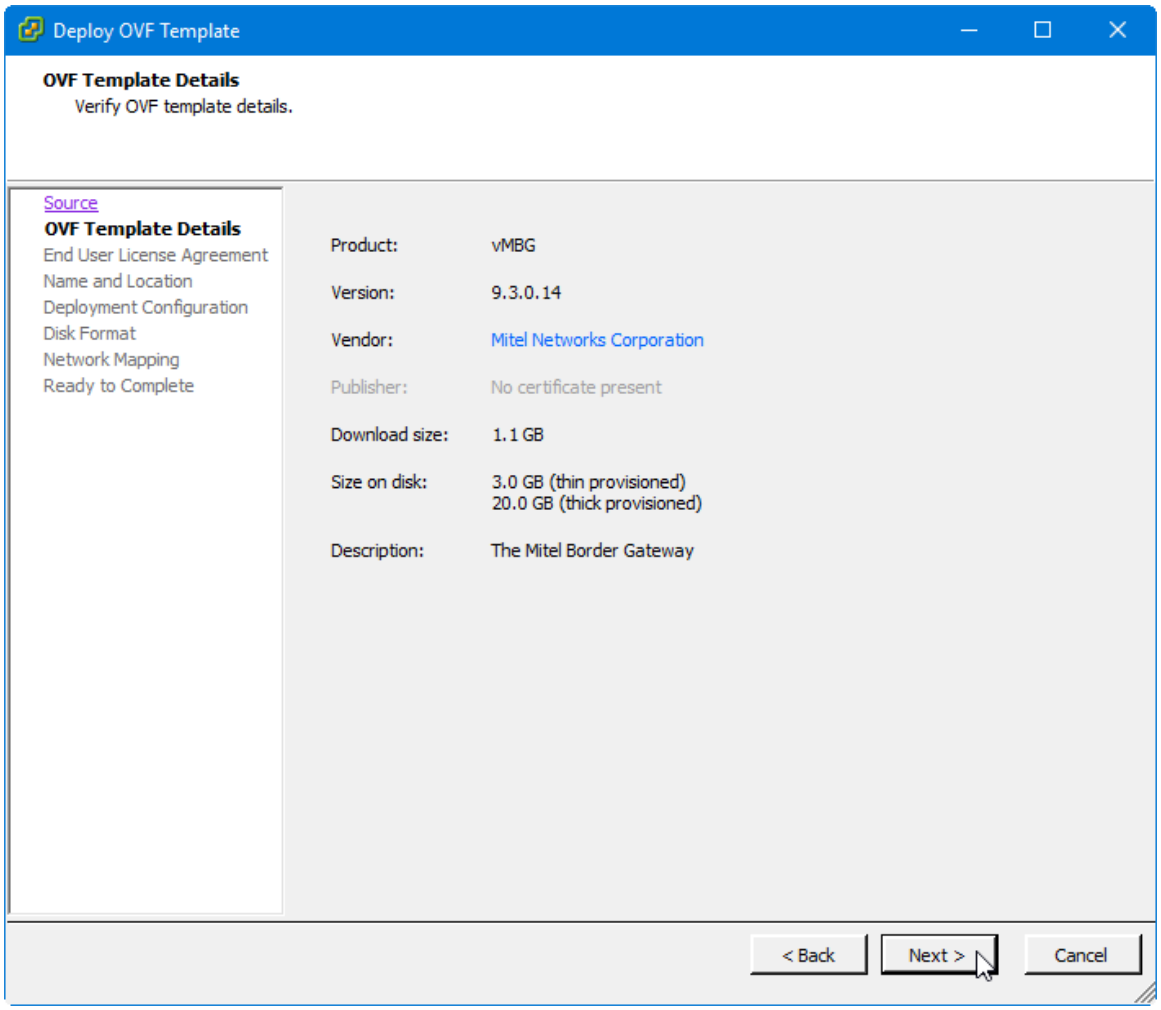
MiVoice Border Gateway Release 10.1 or higher is mandatory to be able to connect Mitel SIP Teleworker with MiVoice Office 400

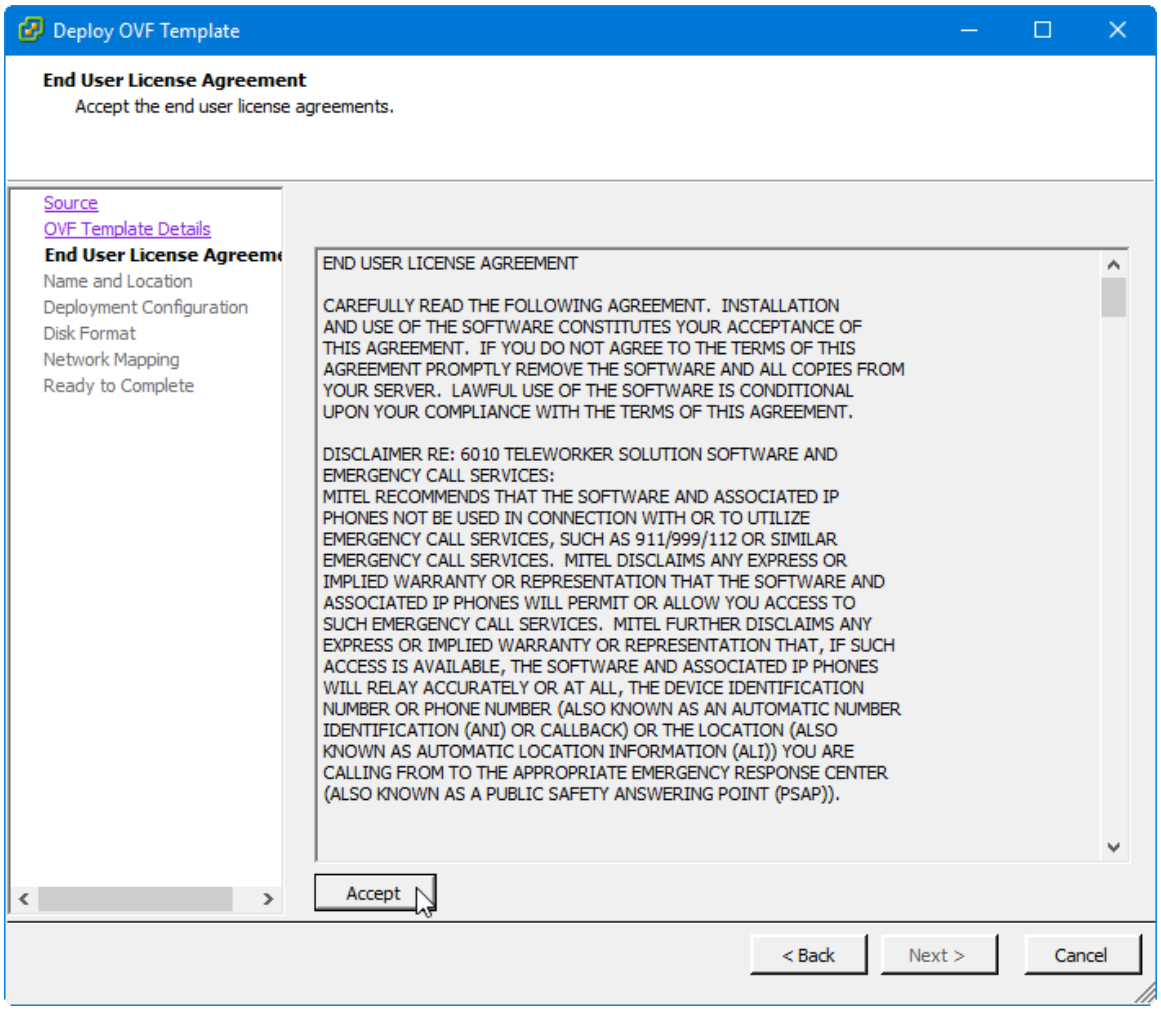
Install MBG virtual appliance - ESXi

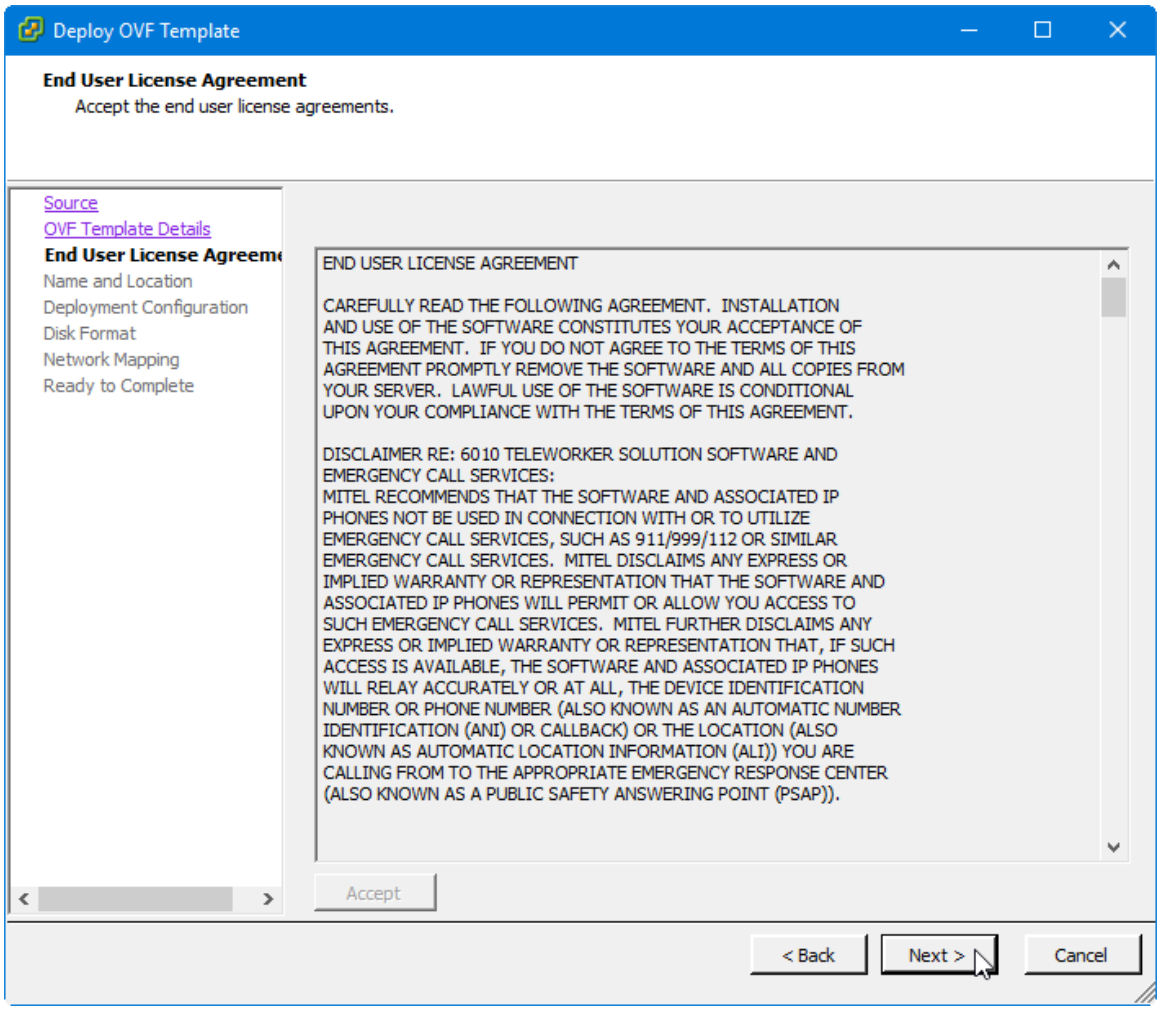


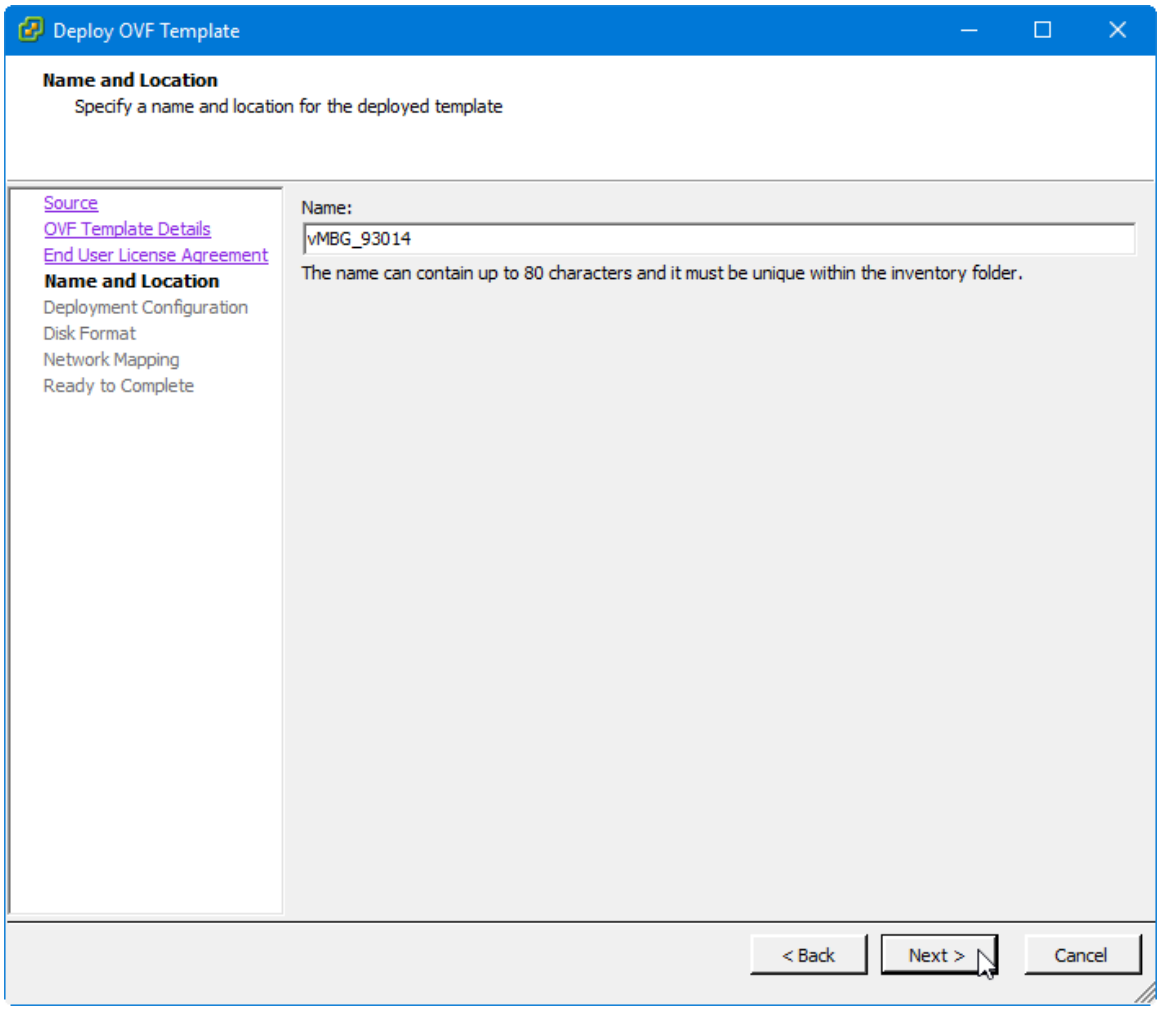
Deploy MiVoice Border Gateway (MBG) via a *.ova file

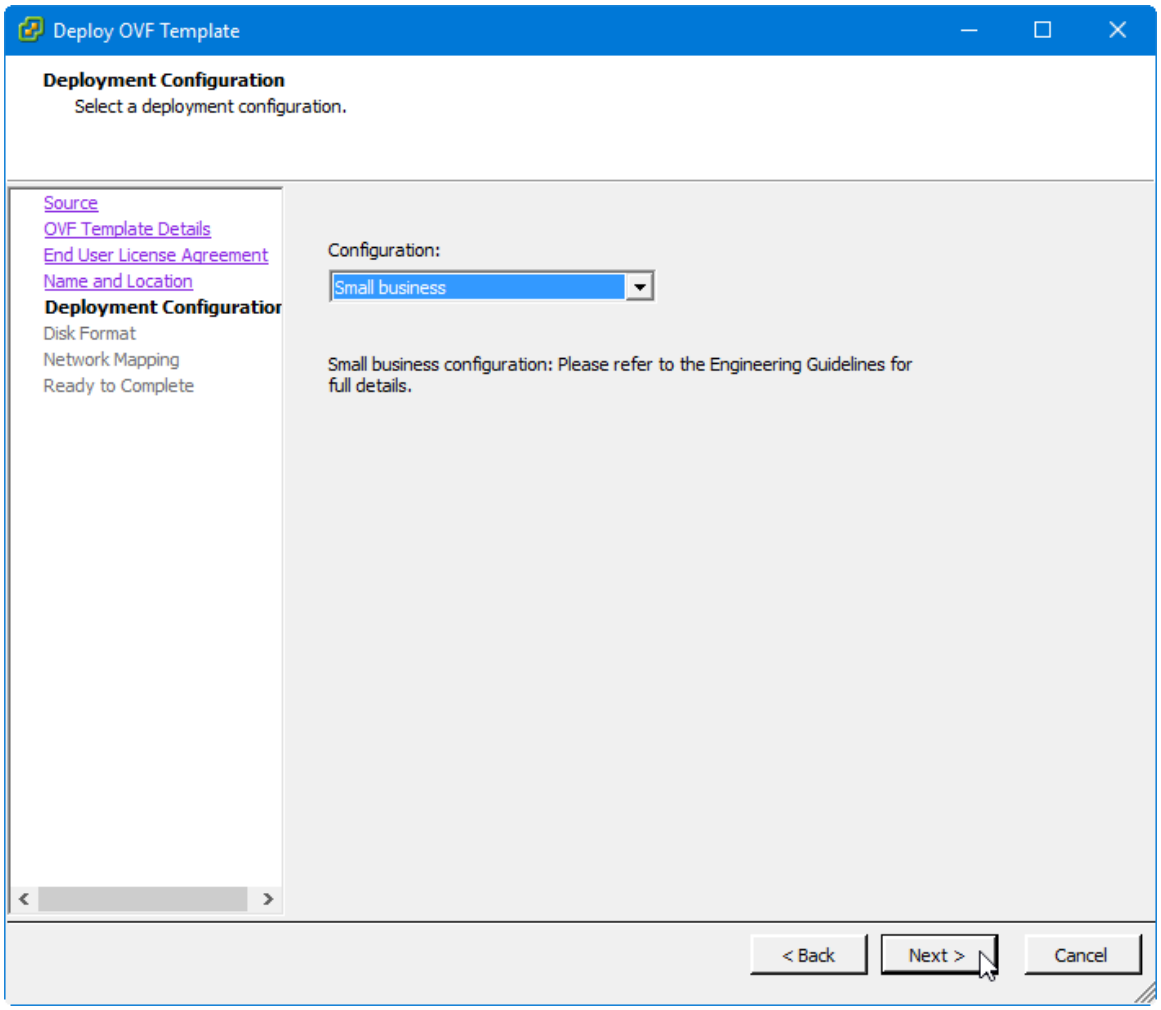

Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete
Deploy from a file or URL
E:\Mitel Software\MBG\vMBG_9.3.0.14.ova
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
< Back
Next >
Cancel

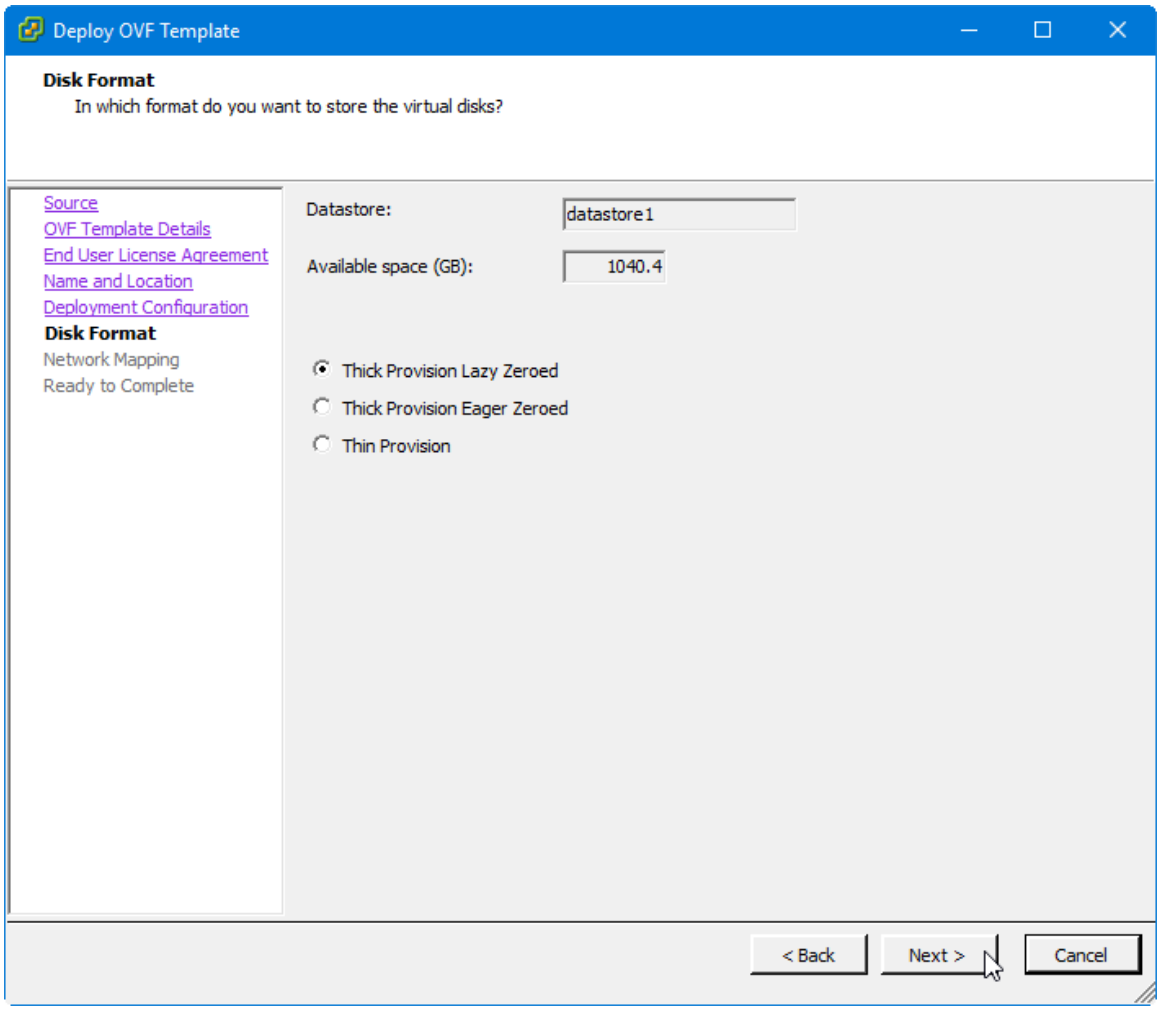

Deploy OVF Template
OVF Template Details
Verify OVF template details.
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
Product: vMBG
Version: 9.3.0.14
Vendor: Mitel Networks Corporation
Publisher: No certificate present
Download size: 1.1 GB
Size on disk: 3.0 GB (thin provisioned)
20.0 GB (thick provisioned)
Description: The Mitel Border Gateway
< Back
Next >
Cancel

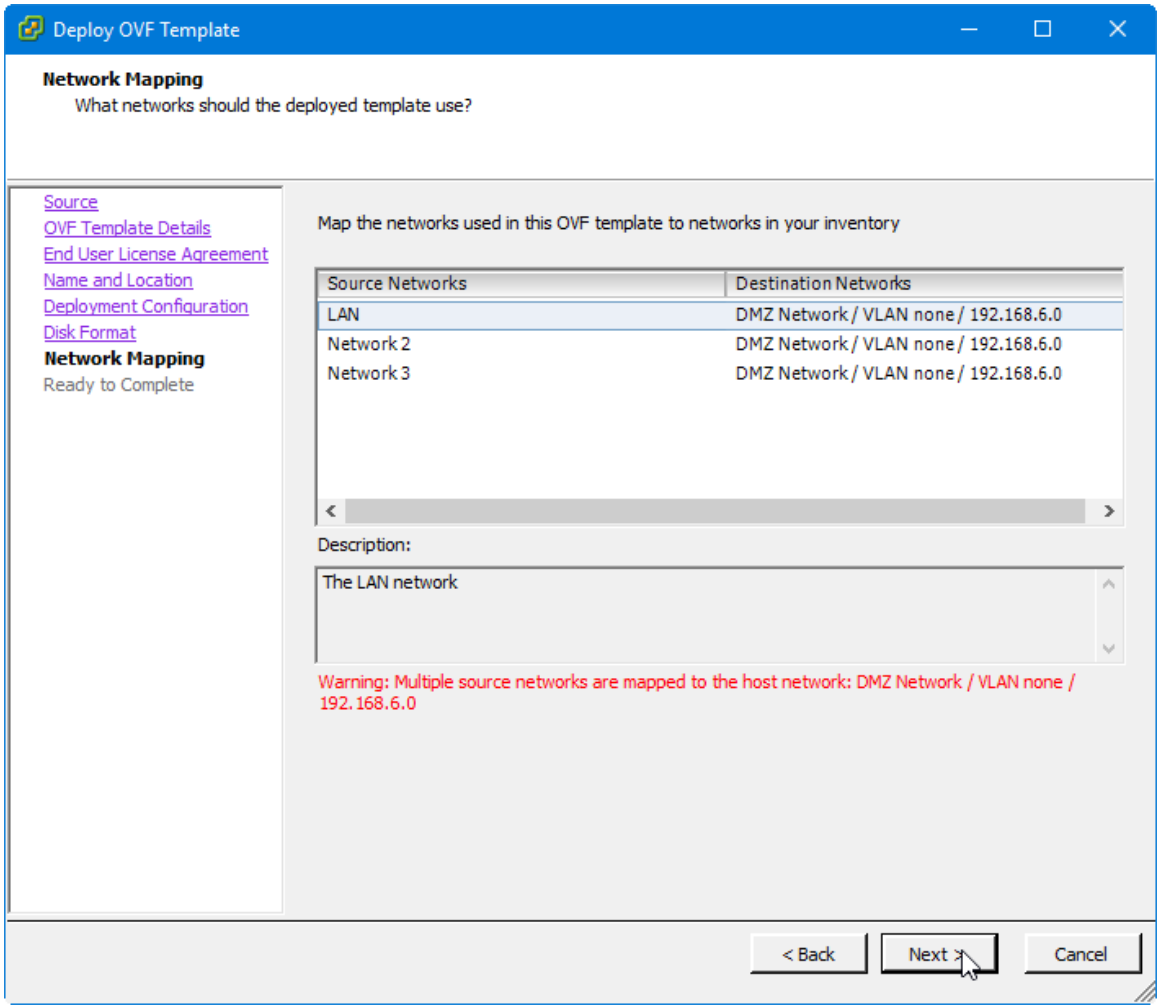

Deploy OVF Template
End User License Agreement
Accept the end user license agreements.
Source
OVF Template Details
End User License Agreeme
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
END USER LICENSE AGREEMENT
CAREFULLY READ THE FOLLOWING AGREEMENT. INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.
DISCLAIMER RE: 6010 TELEWORKER SOLUTION SOFTWARE AND EMERGENCY CALL SERVICES:
MITEL RECOMMENDS THAT THE SOFTWARE AND ASSOCIATED IP PHONES NOT BE USED IN CONNECTION WITH OR TO UTILIZE EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES. MITEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT THE SOFTWARE AND ASSOCIATED IP PHONES WILL PERMIT OR ALLOW YOU ACCESS TO SUCH EMERGENCY CALL SERVICES. MITEL FURTHER DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT, IF SUCH ACCESS IS AVAILABLE, THE SOFTWARE AND ASSOCIATED IP PHONES WILL RELAY ACCURATELY OR AT ALL, THE DEVICE IDENTIFICATION NUMBER OR PHONE NUMBER (ALSO KNOWN AS AN AUTOMATIC NUMBER IDENTIFICATION (ANI) OR CALLBACK) OR THE LOCATION (ALSO KNOWN AS AUTOMATIC LOCATION INFORMATION (ALI)) YOU ARE CALLING FROM TO THE APPROPRIATE EMERGENCY RESPONSE CENTER (ALSO KNOWN AS A PUBLIC SAFETY ANSWERING POINT (PSAP)).
Accept
< Back
Next >
Cancel

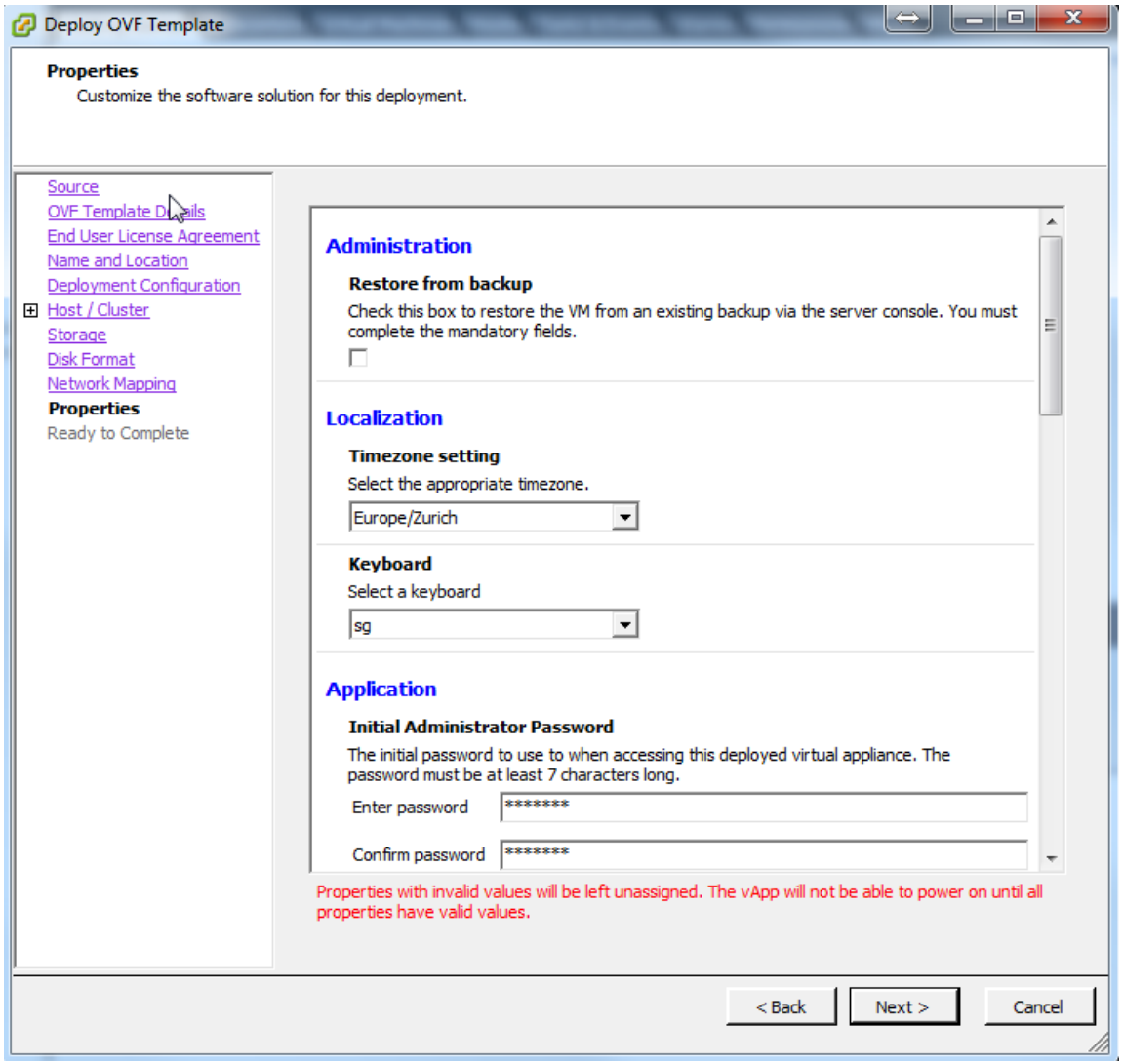

Deploy OVF Template
End User License Agreement
Accept the end user license agreements.
Source
OVF Template Details
End User License Agreeme
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
END USER LICENSE AGREEMENT
CAREFULLY READ THE FOLLOWING AGREEMENT. INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.
DISCLAIMER RE: 6010 TELEWORKER SOLUTION SOFTWARE AND EMERGENCY CALL SERVICES:
MITEL RECOMMENDS THAT THE SOFTWARE AND ASSOCIATED IP PHONES NOT BE USED IN CONNECTION WITH OR TO UTILIZE EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES. MITEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT THE SOFTWARE AND ASSOCIATED IP PHONES WILL PERMIT OR ALLOW YOU ACCESS TO SUCH EMERGENCY CALL SERVICES. MITEL FURTHER DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT, IF SUCH ACCESS IS AVAILABLE, THE SOFTWARE AND ASSOCIATED IP PHONES WILL RELAY ACCURATELY OR AT ALL, THE DEVICE IDENTIFICATION NUMBER OR PHONE NUMBER (ALSO KNOWN AS AN AUTOMATIC NUMBER IDENTIFICATION (ANI) OR CALLBACK) OR THE LOCATION (ALSO KNOWN AS AUTOMATIC LOCATION INFORMATION (ALI)) YOU ARE CALLING FROM TO THE APPROPRIATE EMERGENCY RESPONSE CENTER (ALSO KNOWN AS A PUBLIC SAFETY ANSWERING POINT (PSAP)).
Accept
< Back
Next >
Cancel


Deploy OVF Template
Name and Location
Specify a name and location for the deployed template
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
Name:
vMBG_93014
The name can contain up to 80 characters and it must be unique within the inventory folder.
< Back
Next >
Cancel


Deploy OVF Template
Deployment Configuration
Select a deployment configuration.
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuratior
Disk Format
Network Mapping
Ready to Complete
Configuration:
Small business
Small business configuration: Please refer to the Engineering Guidelines for full details.
< Back
Next >
Cancel

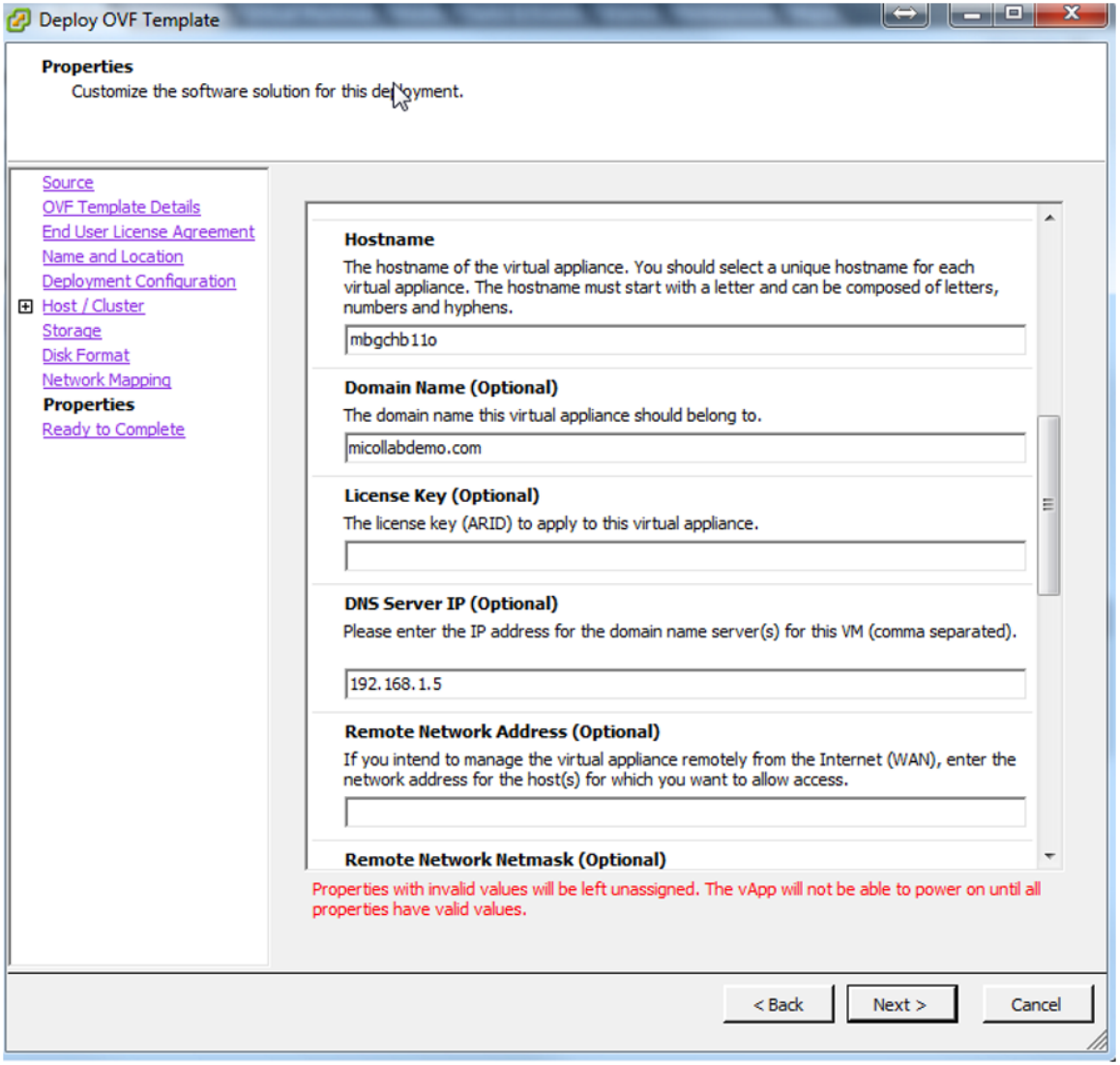

Deploy OVF Template
Disk Format
In which format do you want to store the virtual disks?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
Datastore:
datastore1
Available space (GB):
1040.4
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
< Back
Next >
Cancel


Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
LAN
DMZ Network / VLAN none / 192.168.6.0
Network 2
DMZ Network / VLAN none / 192.168.6.0
Network 3
DMZ Network / VLAN none / 192.168.6.0
Description:
The LAN network
Warning: Multiple source networks are mapped to the host network: DMZ Network / VLAN none / 192.168.6.0
< Back
Next >
Cancel

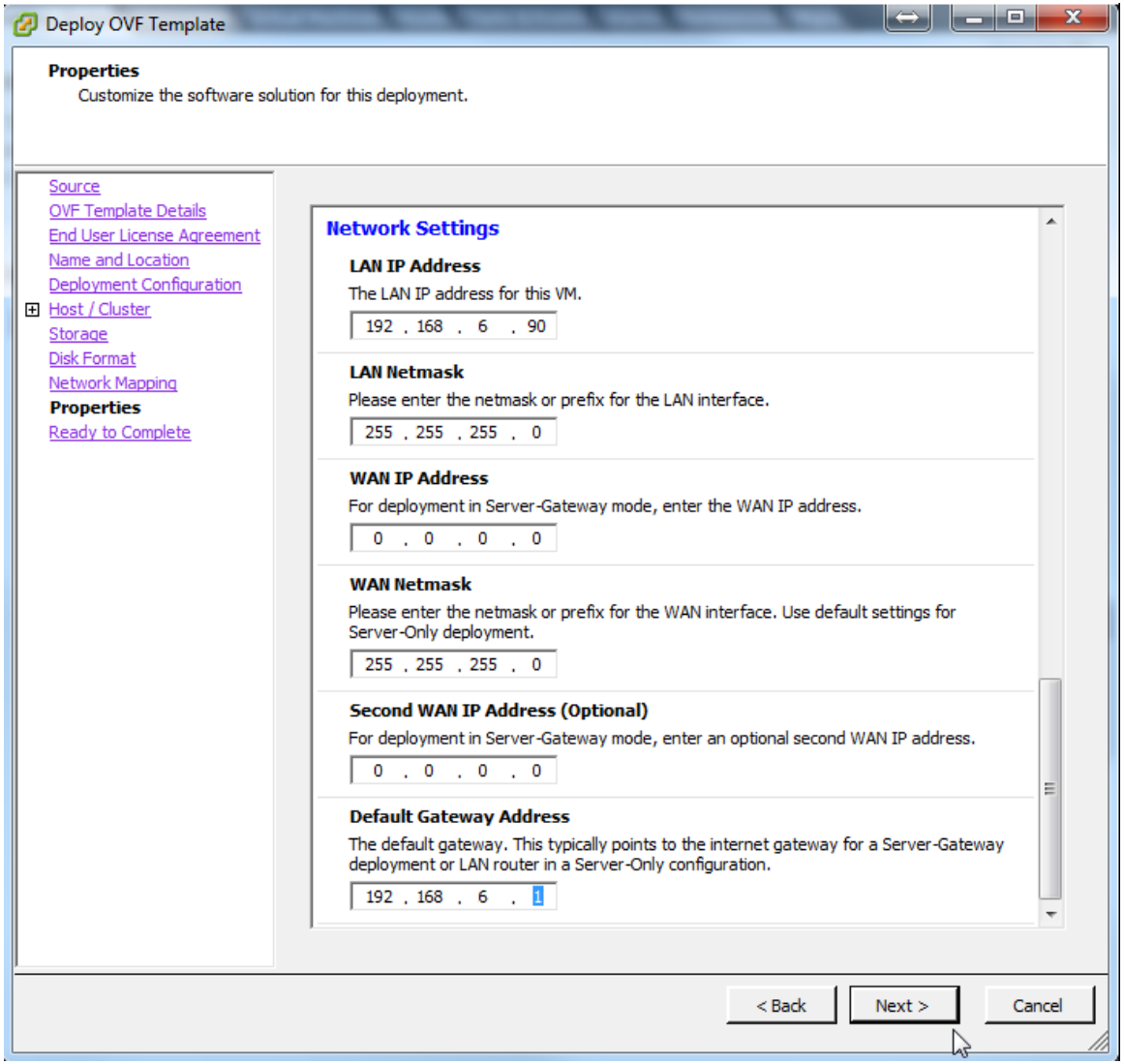


If you have VMware vCenter license you can directly edit some initial settings now:

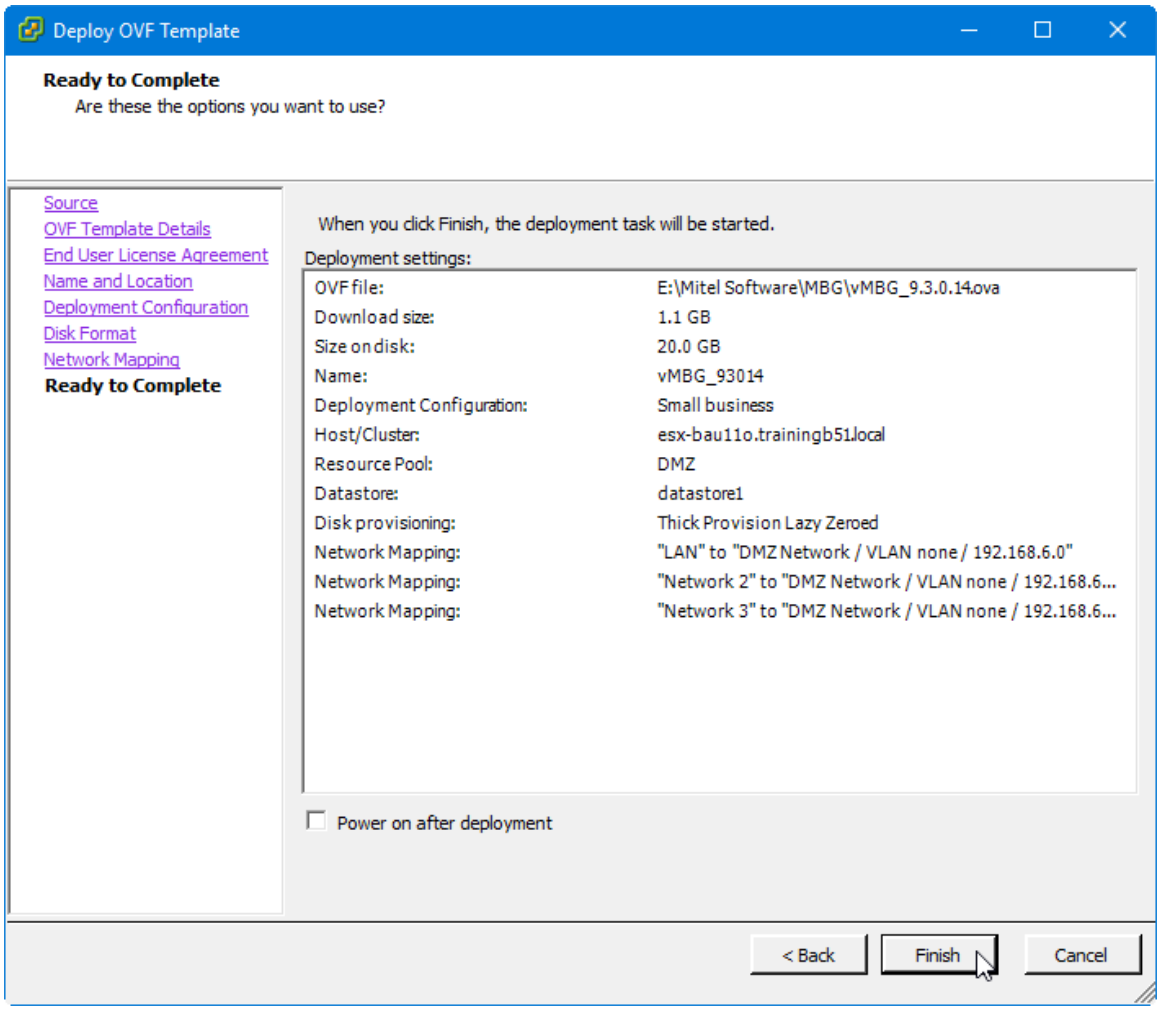
- Time zone
- Keyboard layout
- Admin password

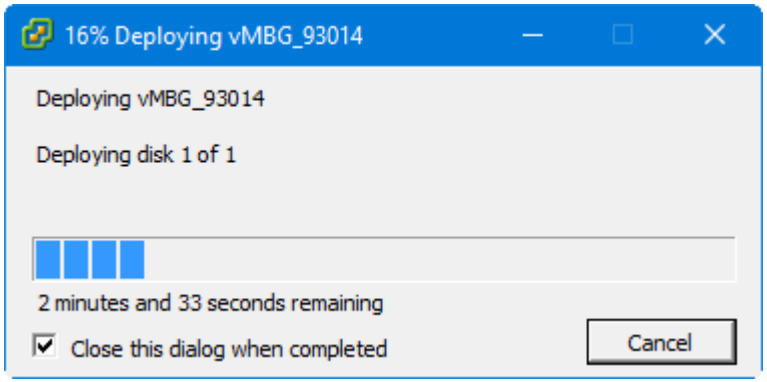


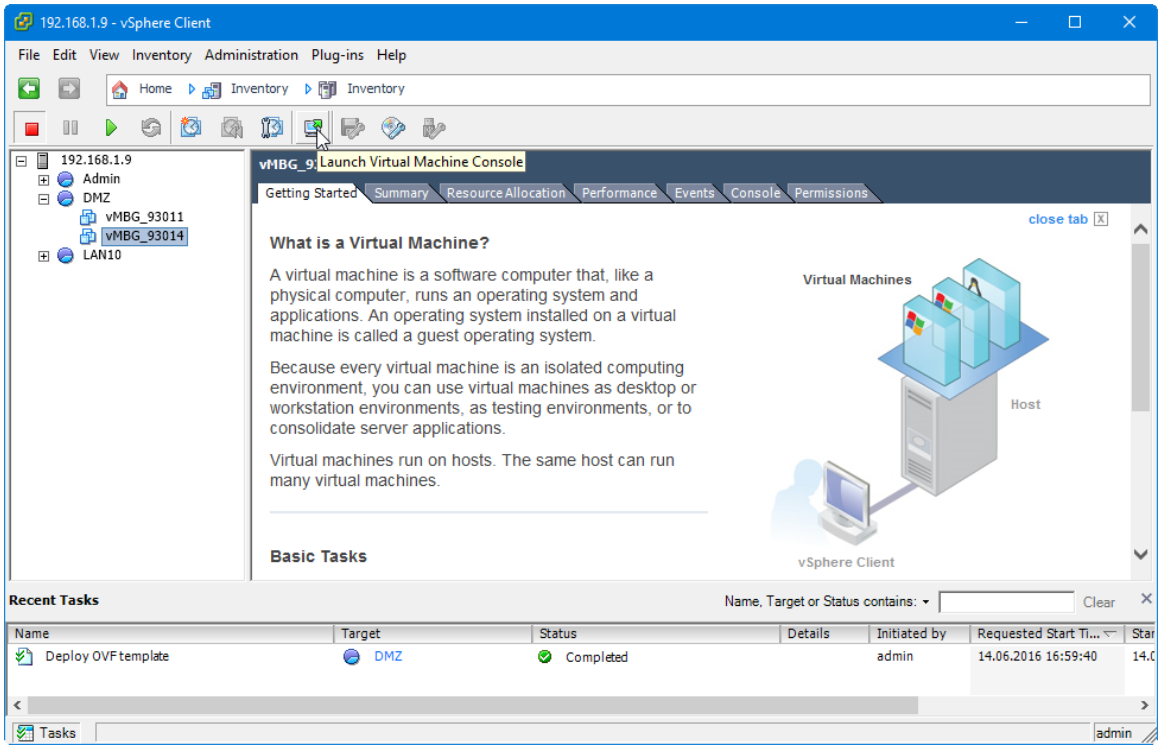
- Hostname
- Domain
- DNS server

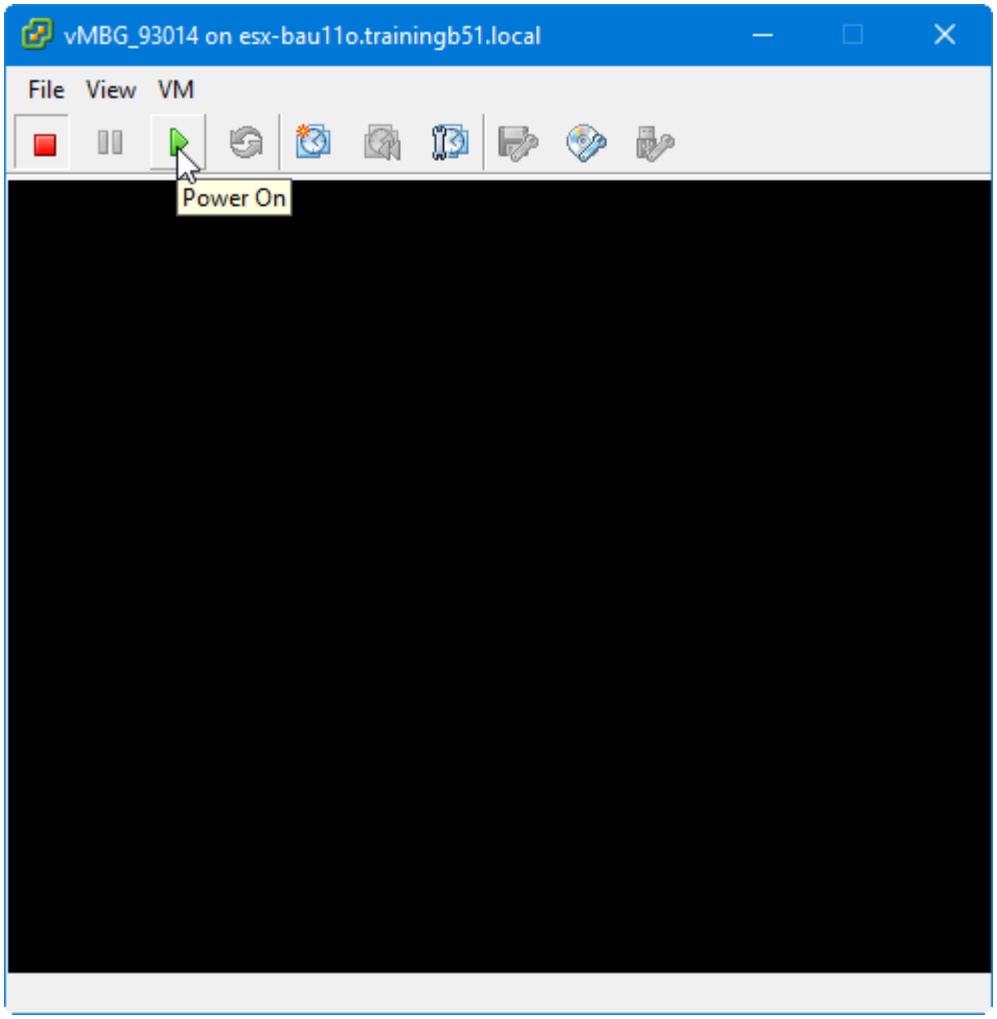


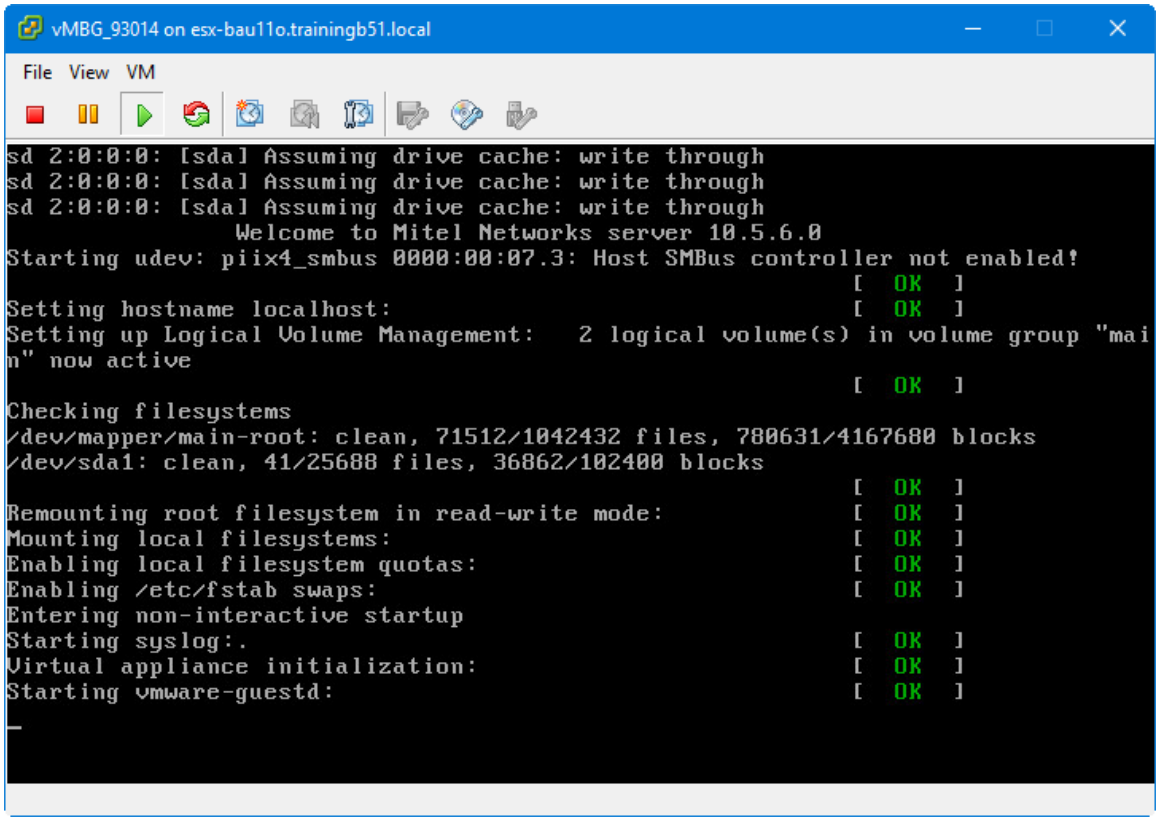
- IP address
- Netmask
- Gateway

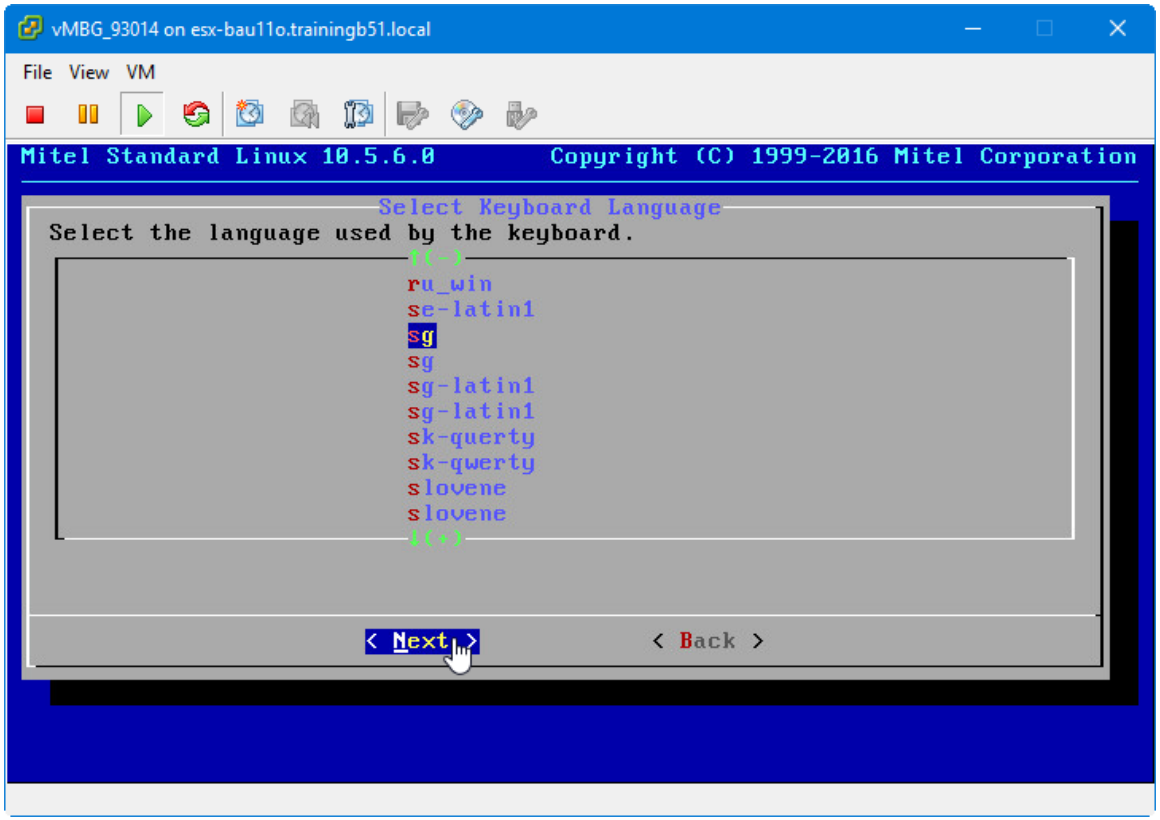

Deploy OVF Template
Ready to Complete
Are these the options you want to use?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Disk Format
Network Mapping
Ready to Complete
When you click Finish, the deployment task will be started.
Deployment settings:
OVF file: E:\Mitel Software\MBG\vMBG_9.3.0.14.ova
Download size: 1.1 GB
Size on disk: 20.0 GB
Name: vMBG_93014
Deployment Configuration: Small business
Host/Cluster: esx-bau11o.trainingb51.local
Resource Pool: DMZ
Datastore: datastore1
Disk provisioning: Thick Provision Lazy Zeroed
Network Mapping: "LAN" to "DMZ Network / VLAN none / 192.168.6.0"
Network Mapping: "Network 2" to "DMZ Network / VLAN none / 192.168.6...
Network Mapping: "Network 3" to "DMZ Network / VLAN none / 192.168.6...
Power on after deployment
< Back
Finish
Cancel


16% Deploying vMBG_93014
Deploying vMBG_93014
Deploying disk 1 of 1
2 minutes and 33 seconds remaining
Close this dialog when completed
Cancel


192.168.1.9 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.1.9
Admin
DMZ
vMBG_93011
vMBG_93014
LAN10
Launch Virtual Machine Console
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual machines run on hosts. The same host can run many virtual machines.
Virtual Machines
Host
vSphere Client
Basic Tasks
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti...
Deploy OVF template DMZ Completed admin 14.06.2016 16:59:40
Tasks
admin

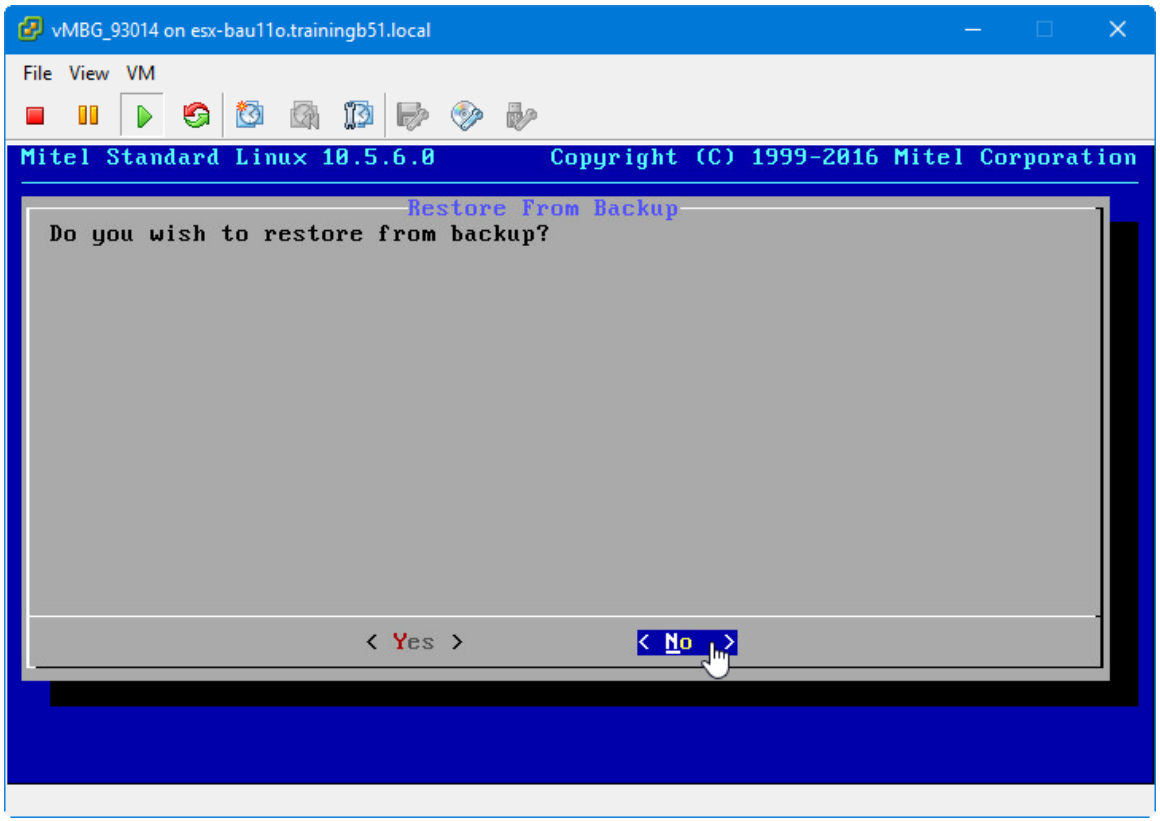

vMBG_93014 on esx-bau11o.trainingb51.local
File
View
VM
Power On

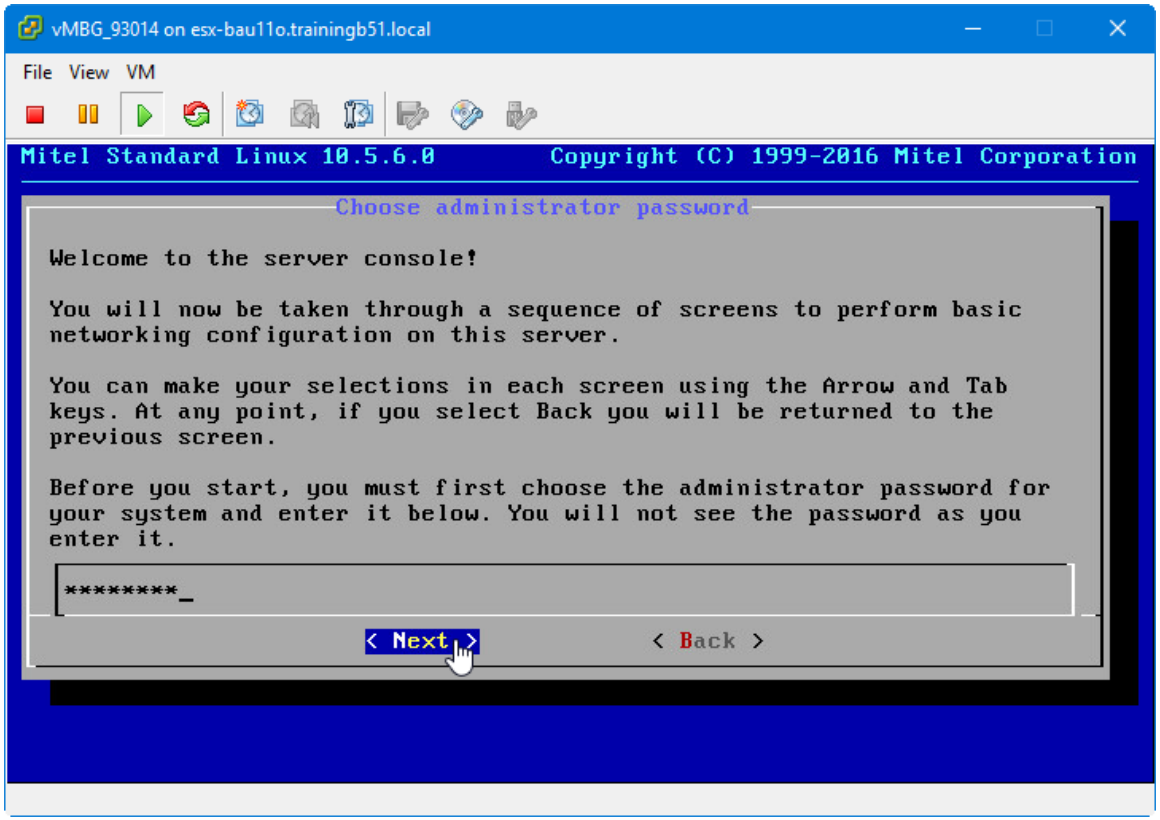

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:0:0: [sda] Assuming drive cache: write through
Welcome to Mitel Networks server 10.5.6.0
Starting udev: piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!
[OK]
Setting hostname localhost: [OK]
Setting up Logical Volume Management: 2 logical volume(s) in volume group "mai
n" now active
[OK]
Checking filesystems
/dev/mapper/main-root: clean, 71512/1042432 files, 780631/4167680 blocks
/dev/sda1: clean, 41/25688 files, 36862/102400 blocks
[OK]
Remounting root filesystem in read-write mode: [OK]
Mounting local filesystems: [OK]
Enabling local filesystem quotas: [OK]
Enabling /etc/fstab swaps: [OK]
Entering non-interactive startup
Starting syslog:. [OK]
Virtual appliance initialization: [OK]
Starting vmware-guestd: [OK]

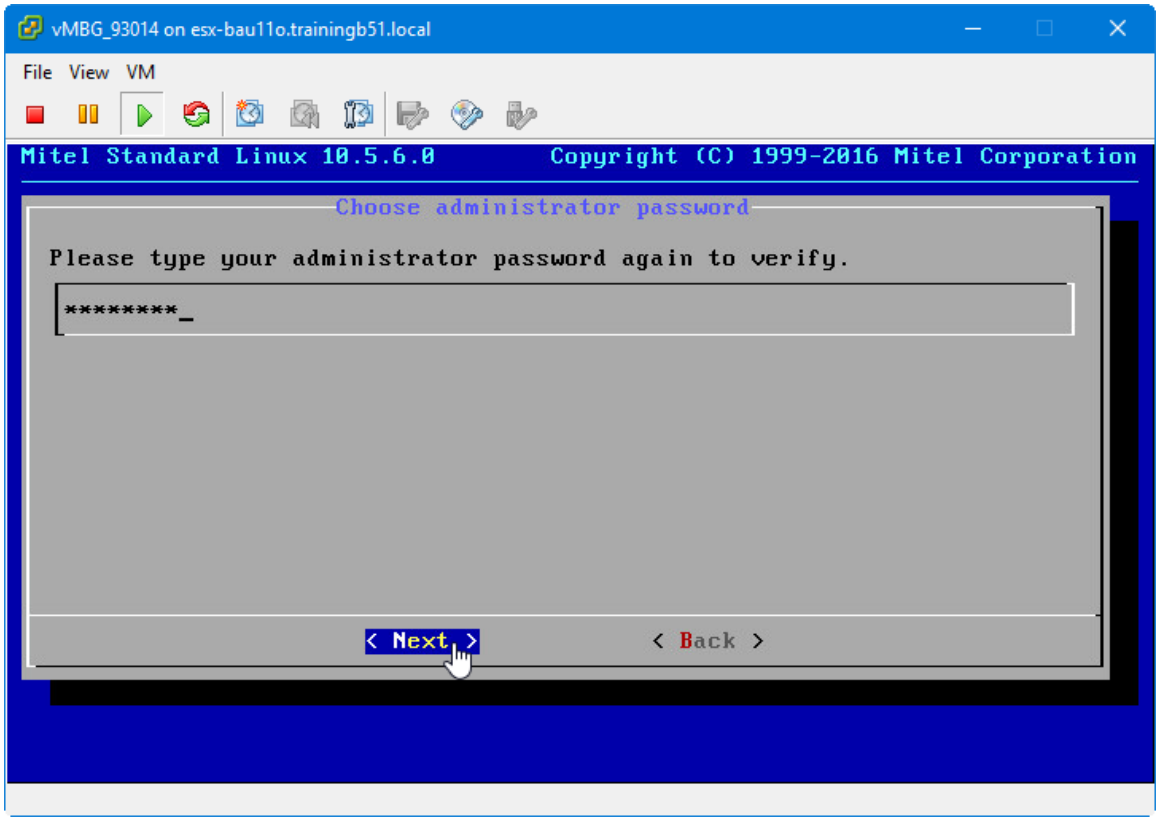


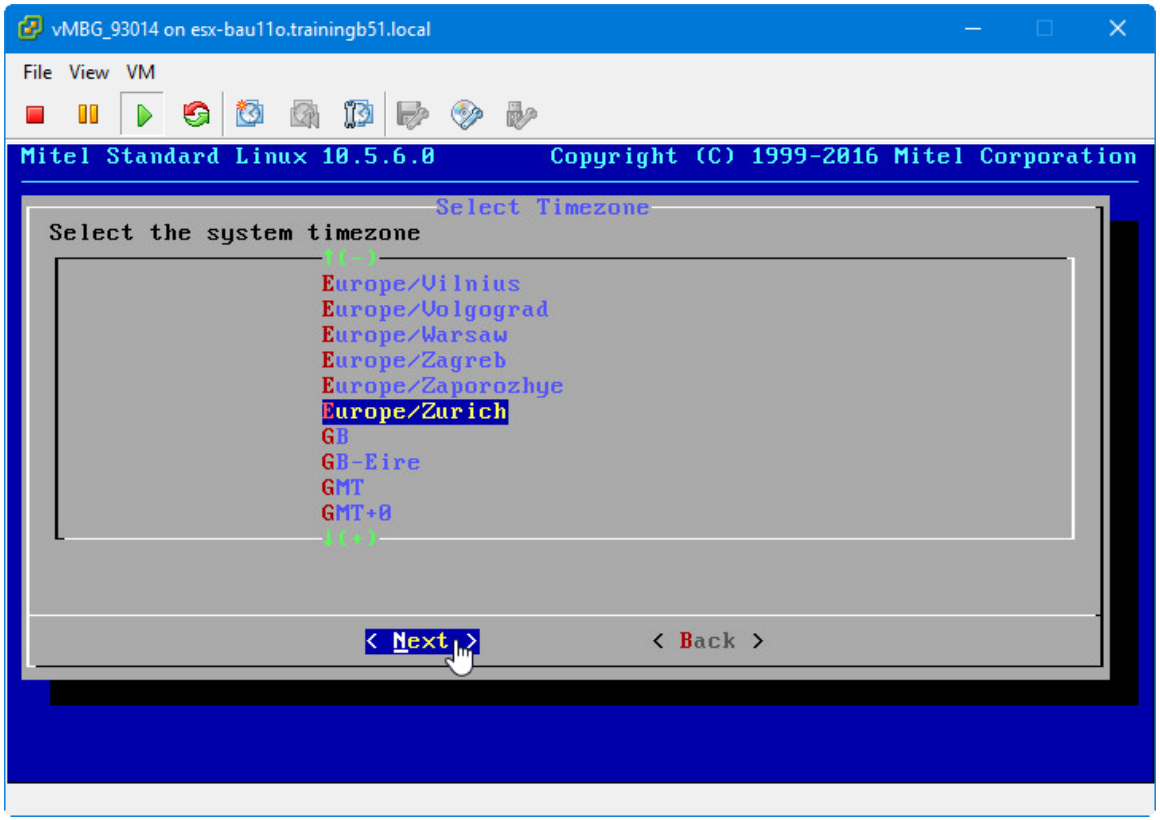
If you do not have the vCenter licenses you have to do the initial settings here in the console:

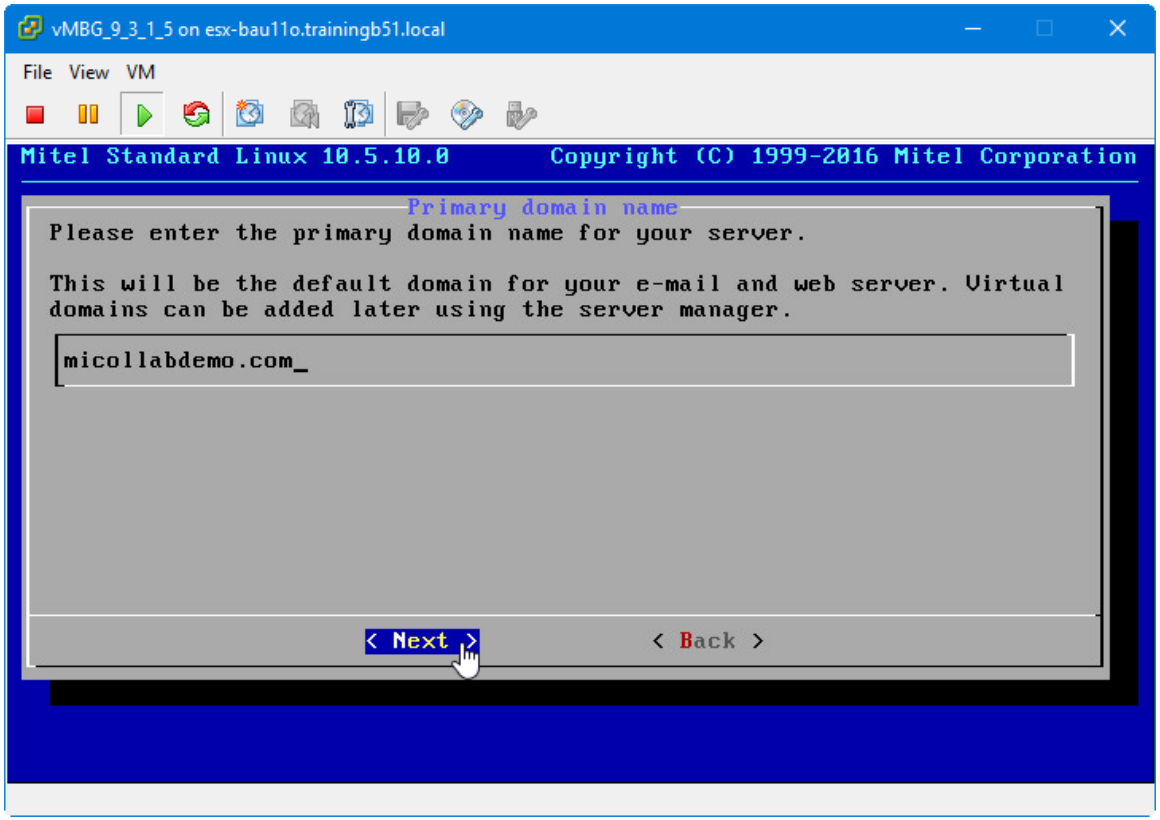
Select your keyboard layout:
e.g.
sg = SwissGerman

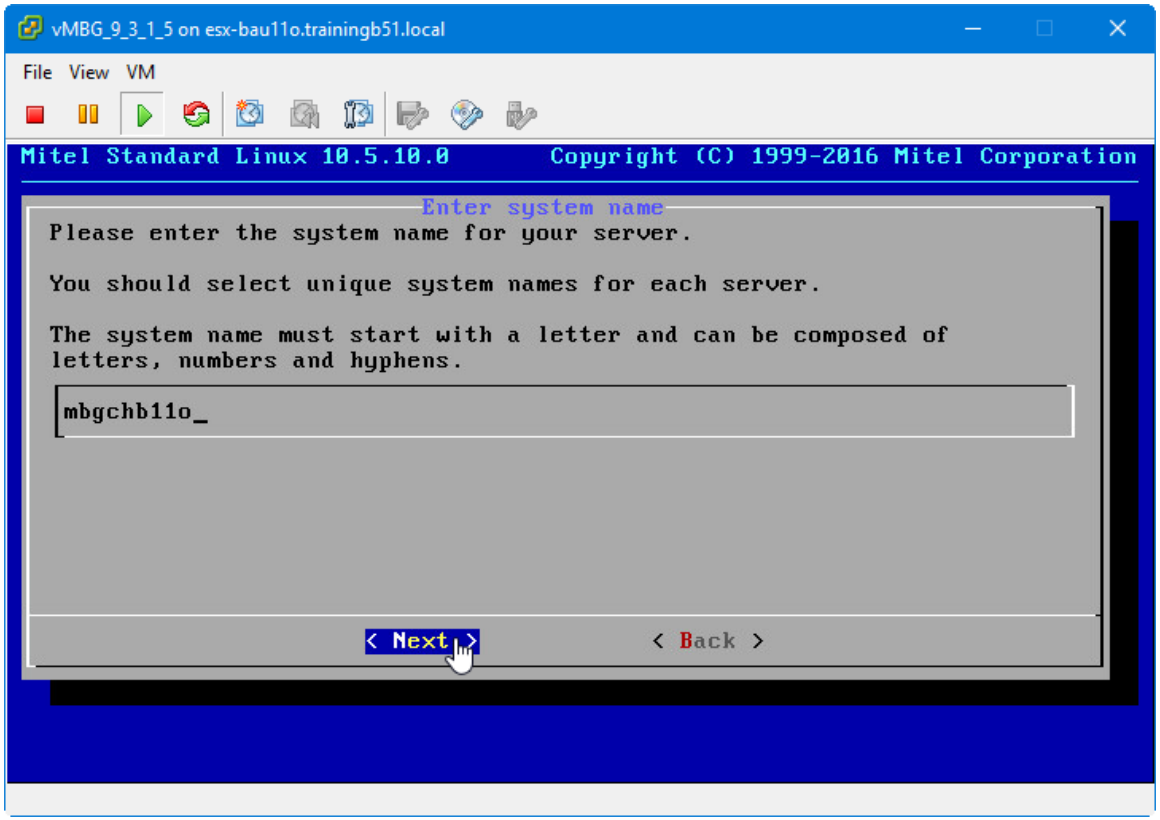

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Restore From Backup
Do you wish to restore from backup?
< Yes >
< No >

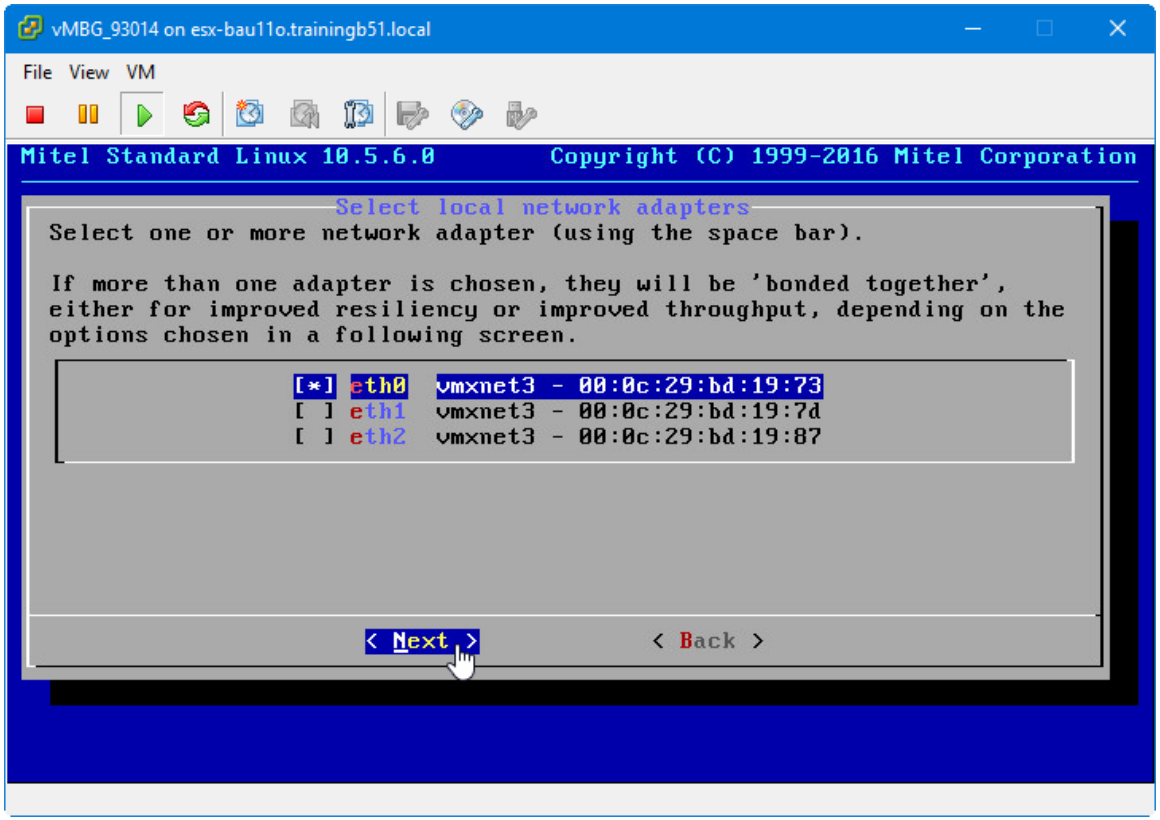

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Choose administrator password
Welcome to the server console!
You will now be taken through a sequence of screens to perform basic networking configuration on this server.
You can make your selections in each screen using the Arrow and Tab keys. At any point, if you select Back you will be returned to the previous screen.
Before you start, you must first choose the administrator password for your system and enter it below. You will not see the password as you enter it.
****
< Next >
< Back >

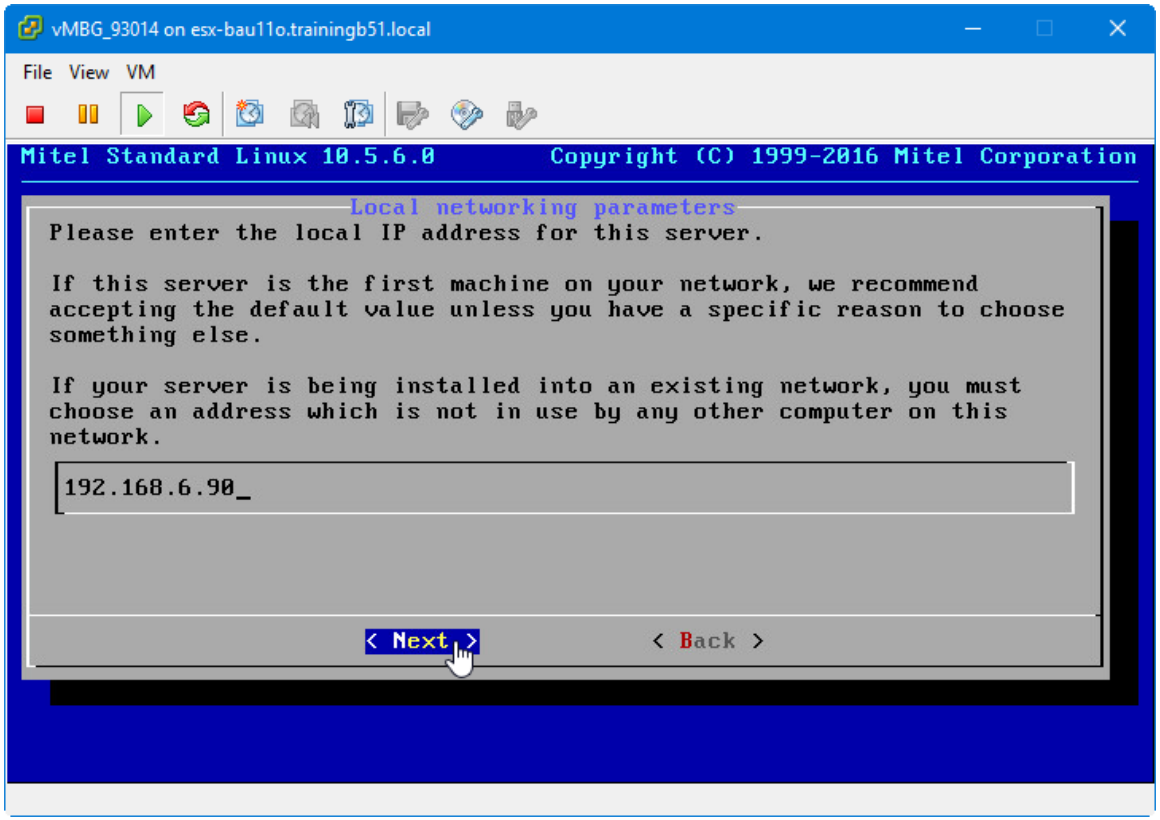

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Choose administrator password
Please type your administrator password again to verify.
********_
< Next >
< Back >

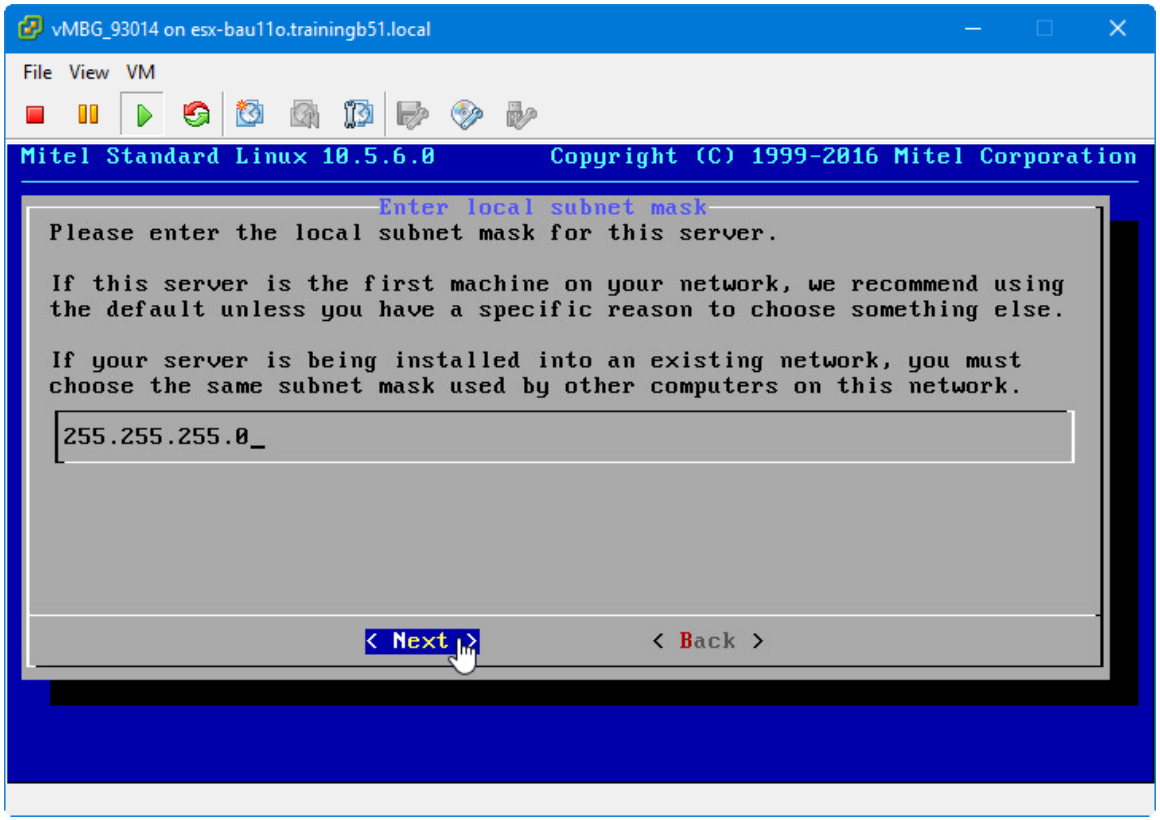

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Select Timezone
Select the system timezone
Europe/Vilnius
Europe/Volgograd
Europe/Warsaw
Europe/Zagreb
Europe/Zaporozhye
Europe/Zurich
GB
GB-Eire
GMT
GMT+0
< Next >
< Back >

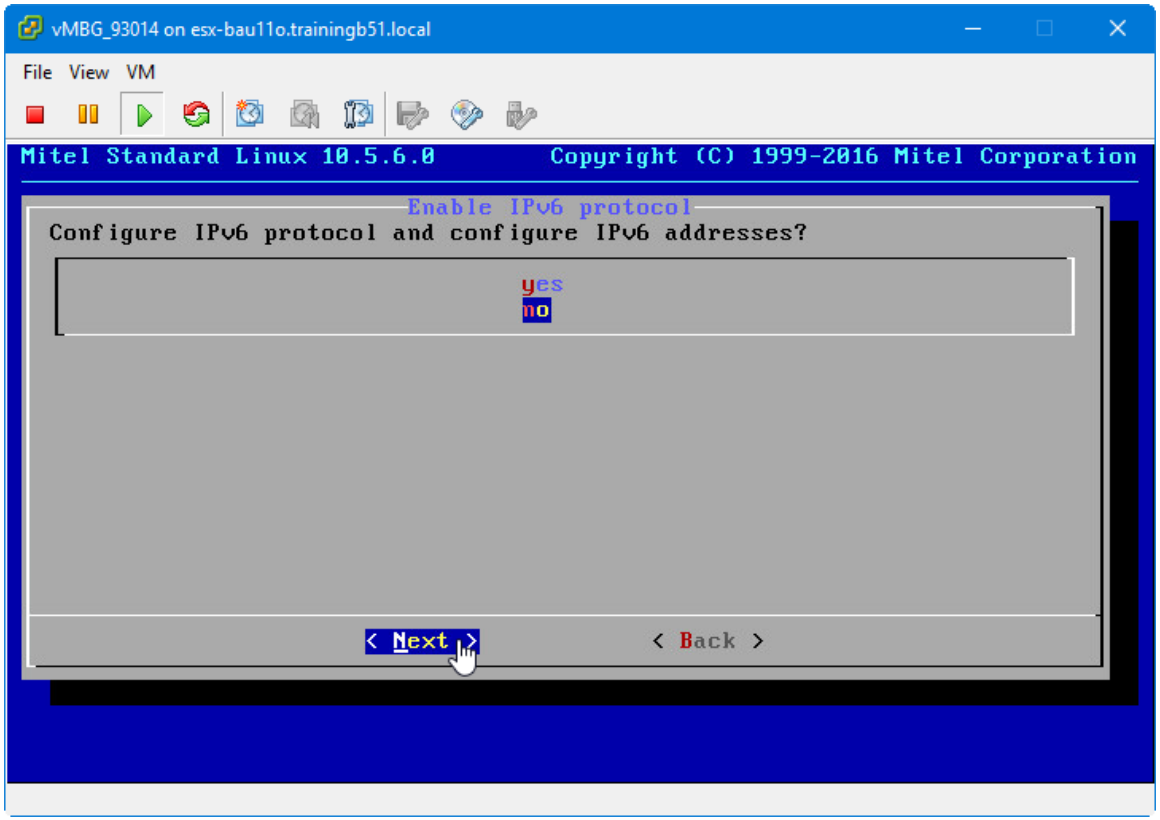

vMBG_9_3_1_5 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.10.0 Copyright (C) 1999-2016 Mitel Corporation
Primary domain name
Please enter the primary domain name for your server.
This will be the default domain for your e-mail and web server. Virtual domains can be added later using the server manager.
micollabdemo.com_
< Next >
< Back >

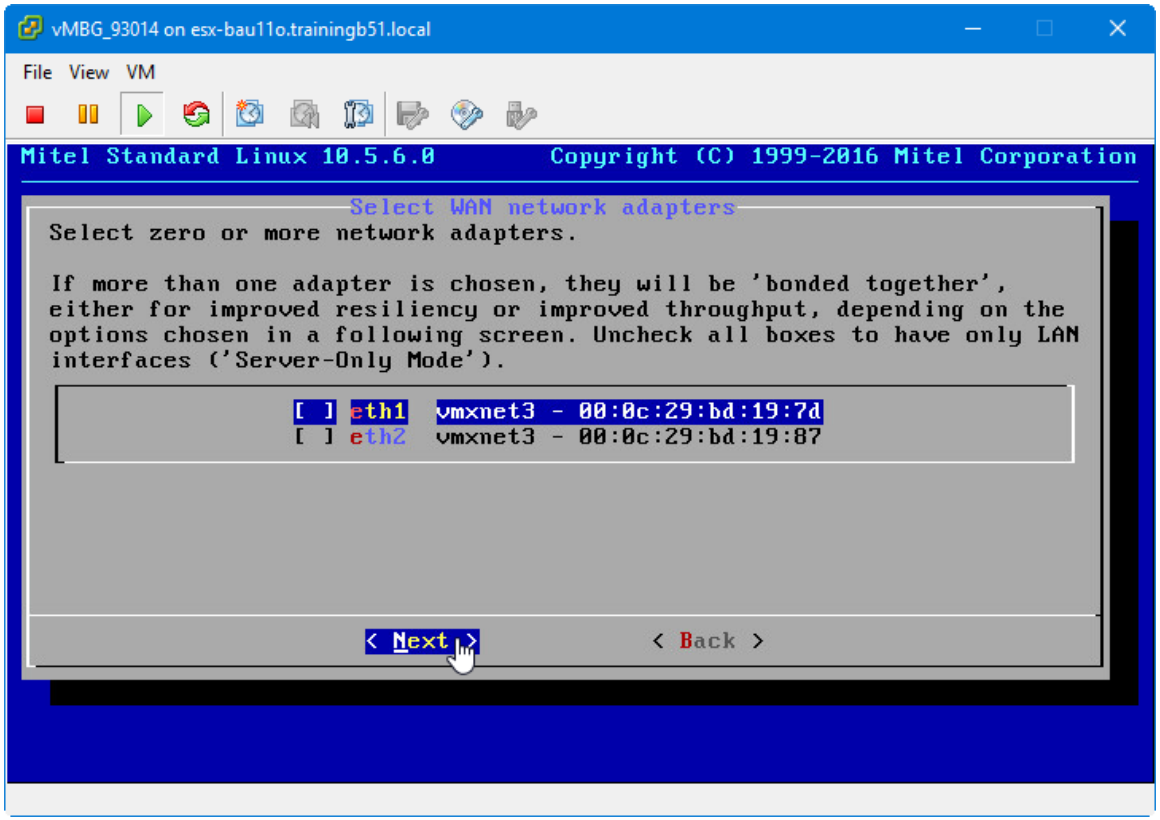

vMBG_9_3_1_5 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.10.0 Copyright (C) 1999-2016 Mitel Corporation
Enter system name
Please enter the system name for your server.
You should select unique system names for each server.
The system name must start with a letter and can be composed of letters, numbers and hyphens.
mbgchb11o_
< Next >
< Back >


vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Select local network adapters
Select one or more network adapter (using the space bar).
If more than one adapter is chosen, they will be 'bonded together', either for improved resiliency or improved throughput, depending on the options chosen in a following screen.
[*] eth0 vmxnet3 - 00:0c:29:bd:19:73
[ ] eth1 vmxnet3 - 00:0c:29:bd:19:7d
[ ] eth2 vmxnet3 - 00:0c:29:bd:19:87
< Next >
< Back >

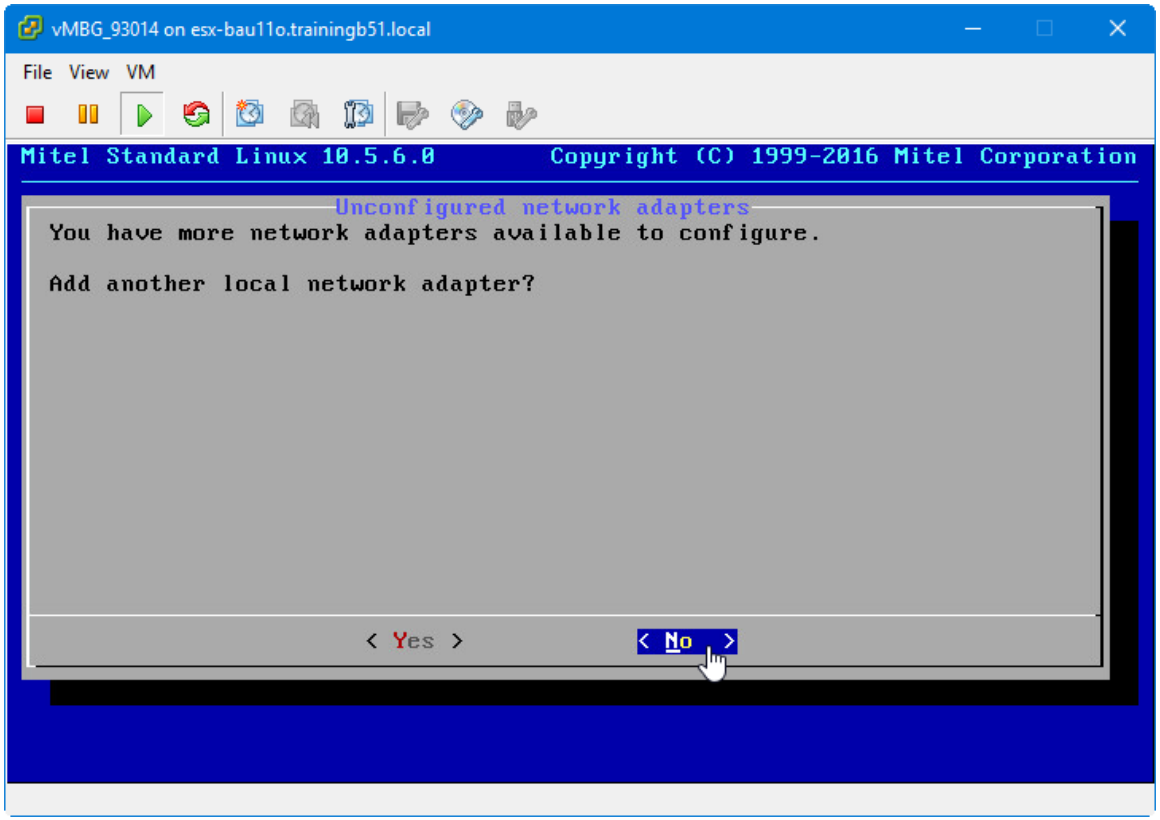

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Local networking parameters
Please enter the local IP address for this server.
If this server is the first machine on your network, we recommend accepting the default value unless you have a specific reason to choose something else.
If your server is being installed into an existing network, you must choose an address which is not in use by any other computer on this network.
192.168.6.90_
< Next >
< Back >

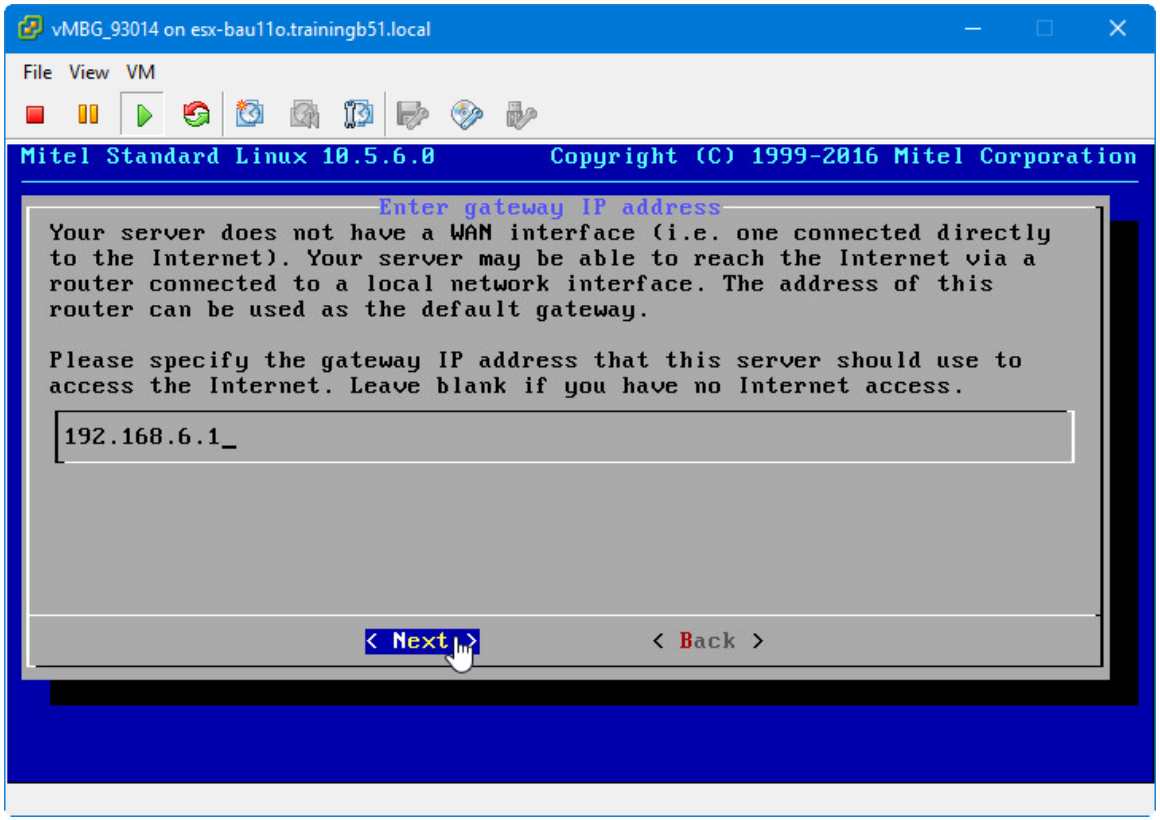

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Enter local subnet mask
Please enter the local subnet mask for this server.
If this server is the first machine on your network, we recommend using the default unless you have a specific reason to choose something else.
If your server is being installed into an existing network, you must choose the same subnet mask used by other computers on this network.
255.255.255.0_
< Next >
< Back >

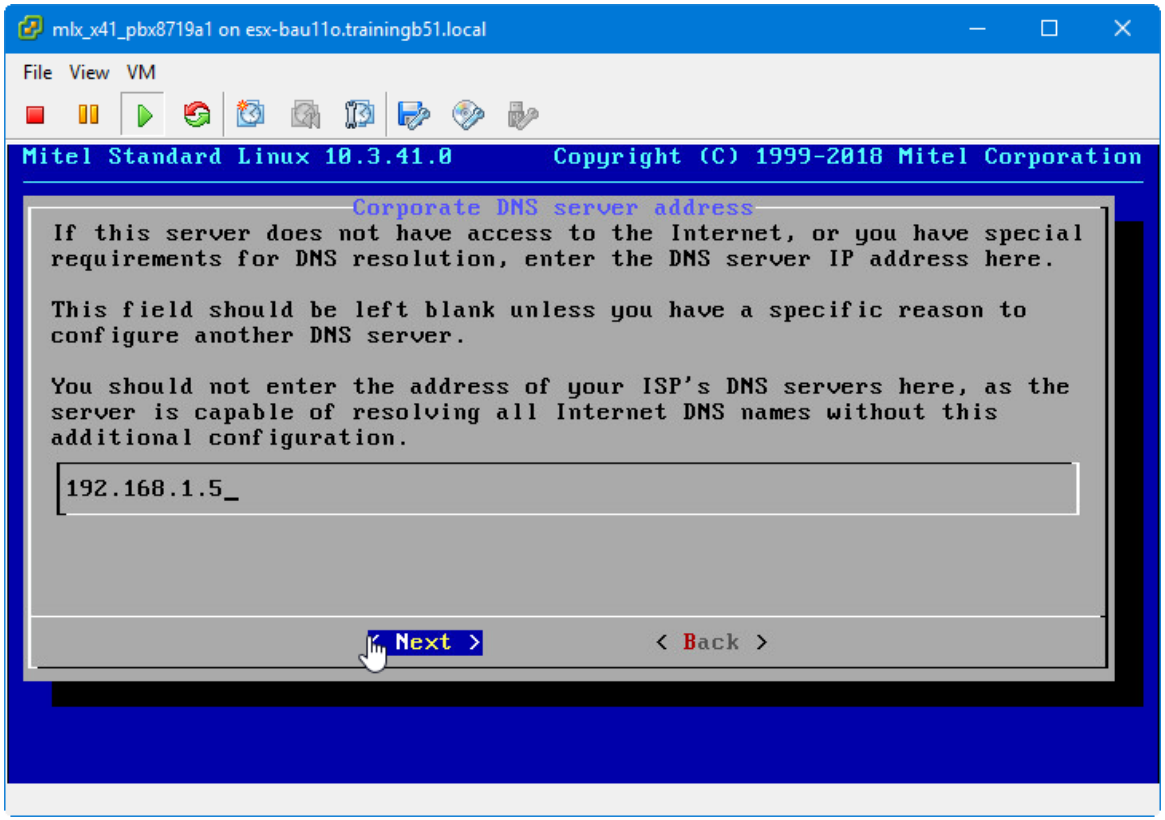

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0
Copyright (C) 1999-2016 Mitel Corporation
Enable IPv6 protocol
Configure IPv6 protocol and configure IPv6 addresses?
yes
no
< Next >
< Back >



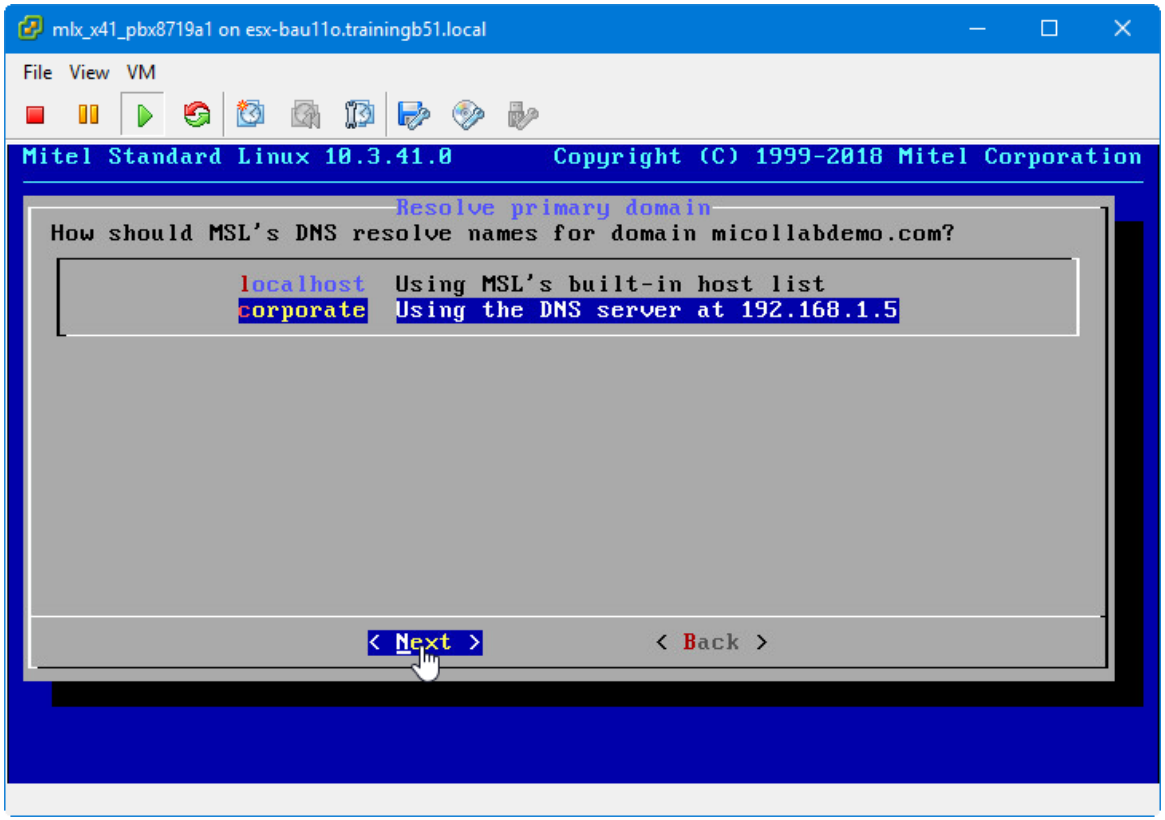
No other network adapter is used.
So just hit "Next".

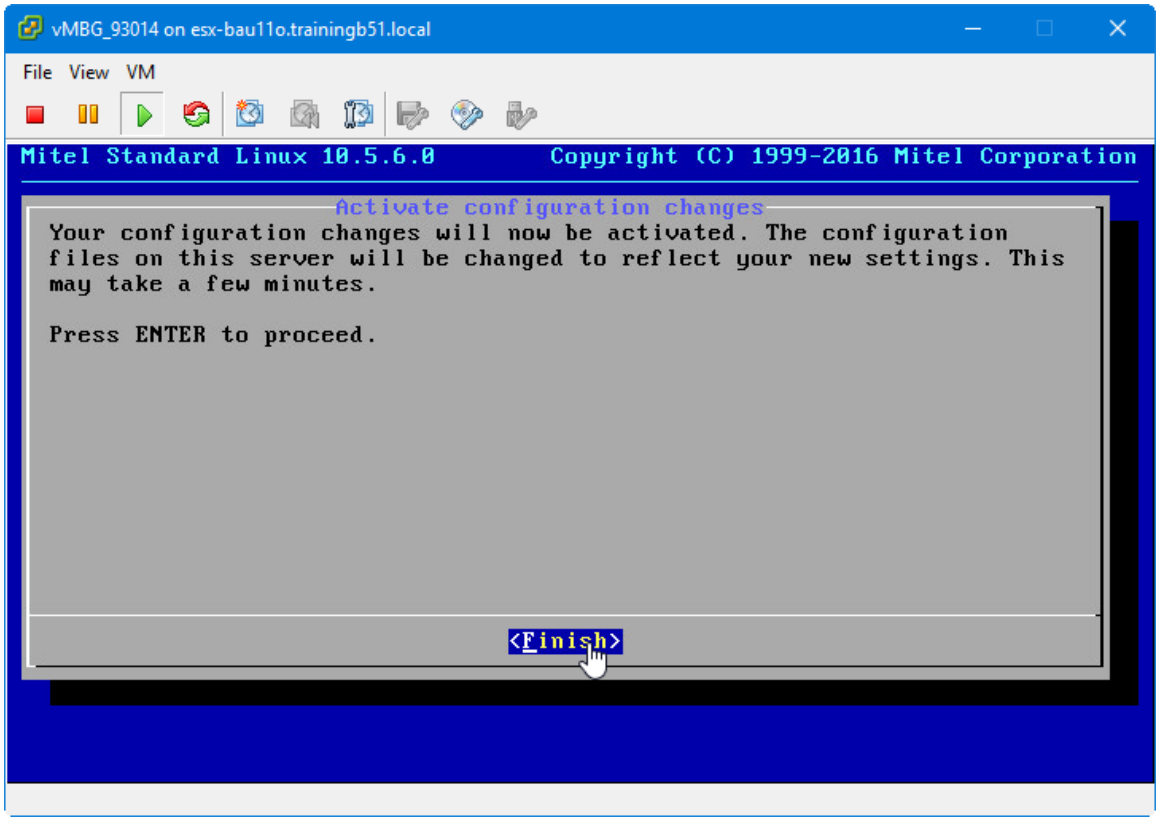

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Unconfigured network adapters
You have more network adapters available to configure.
Add another local network adapter?
< Yes >
< No >

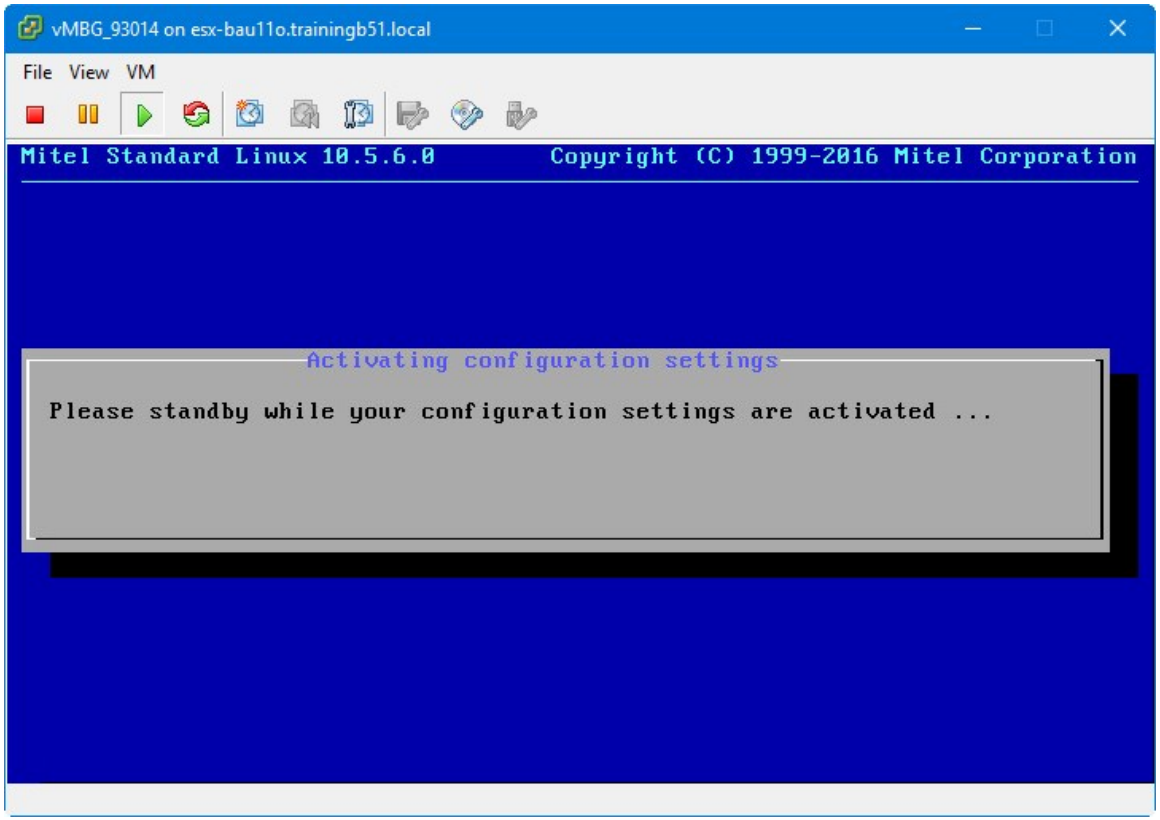

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Enter gateway IP address
Your server does not have a WAN interface (i.e. one connected directly to the Internet). Your server may be able to reach the Internet via a router connected to a local network interface. The address of this router can be used as the default gateway.
Please specify the gateway IP address that this server should use to access the Internet. Leave blank if you have no Internet access.
192.168.6.1_
< Next >
< Back >

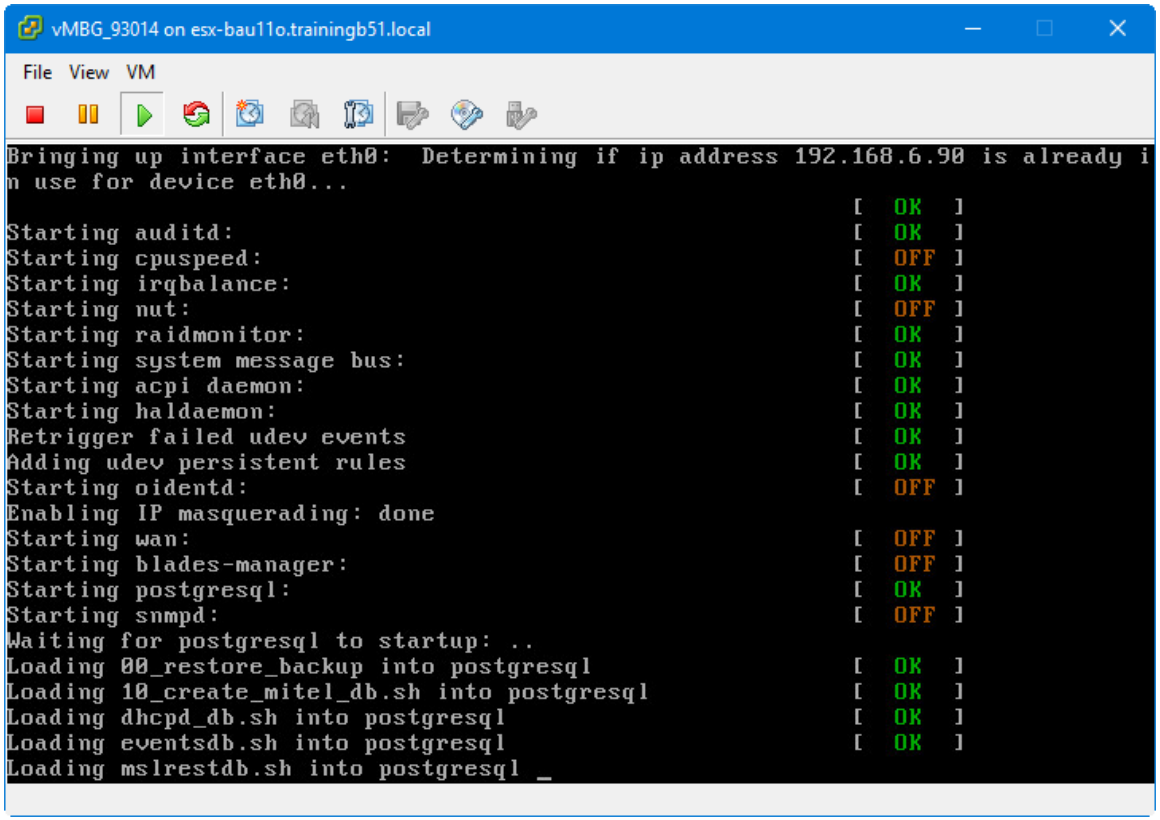


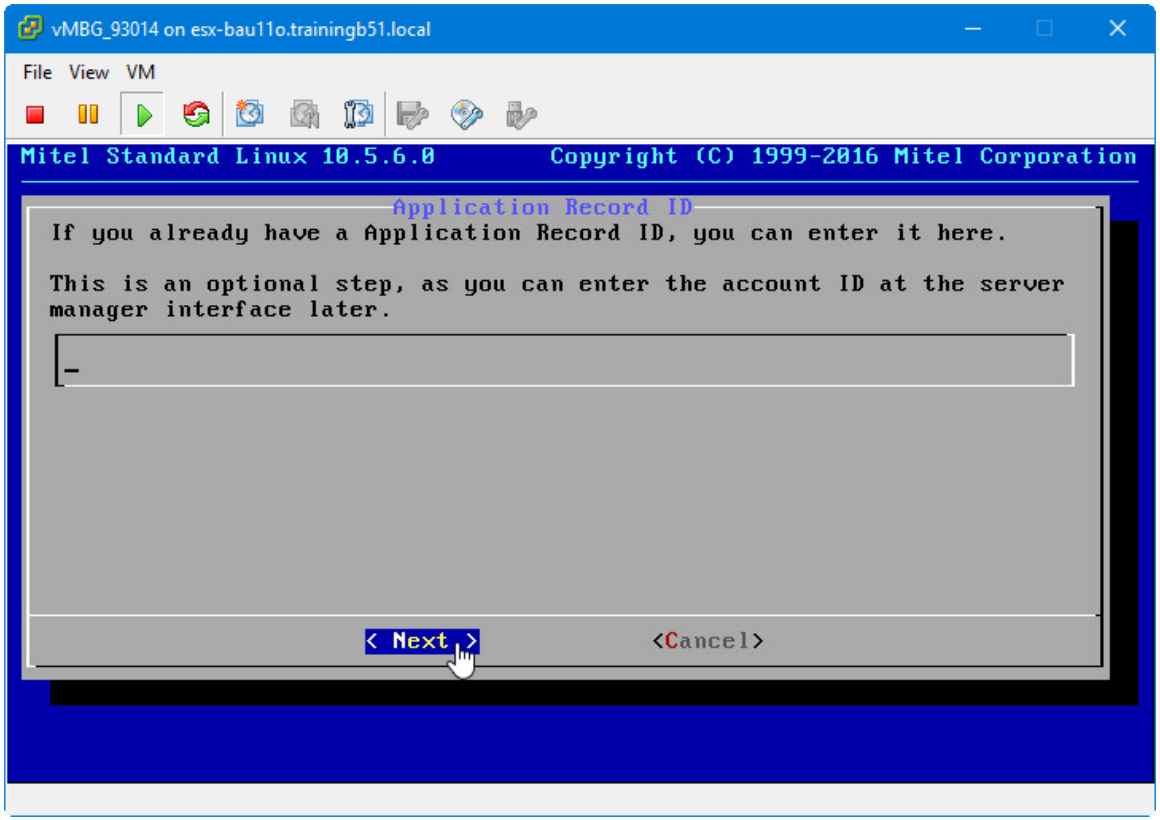
Enter your corporate DNS server here.


mlx_x41_pbx8719a1 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.3.41.0 Copyright (C) 1999-2018 Mitel Corporation
Resolve primary domain
How should MSL's DNS resolve names for domain micollabdemo.com?
localhost Using MSL's built-in host list
corporate Using the DNS server at 192.168.1.5
< Next >
< Back >

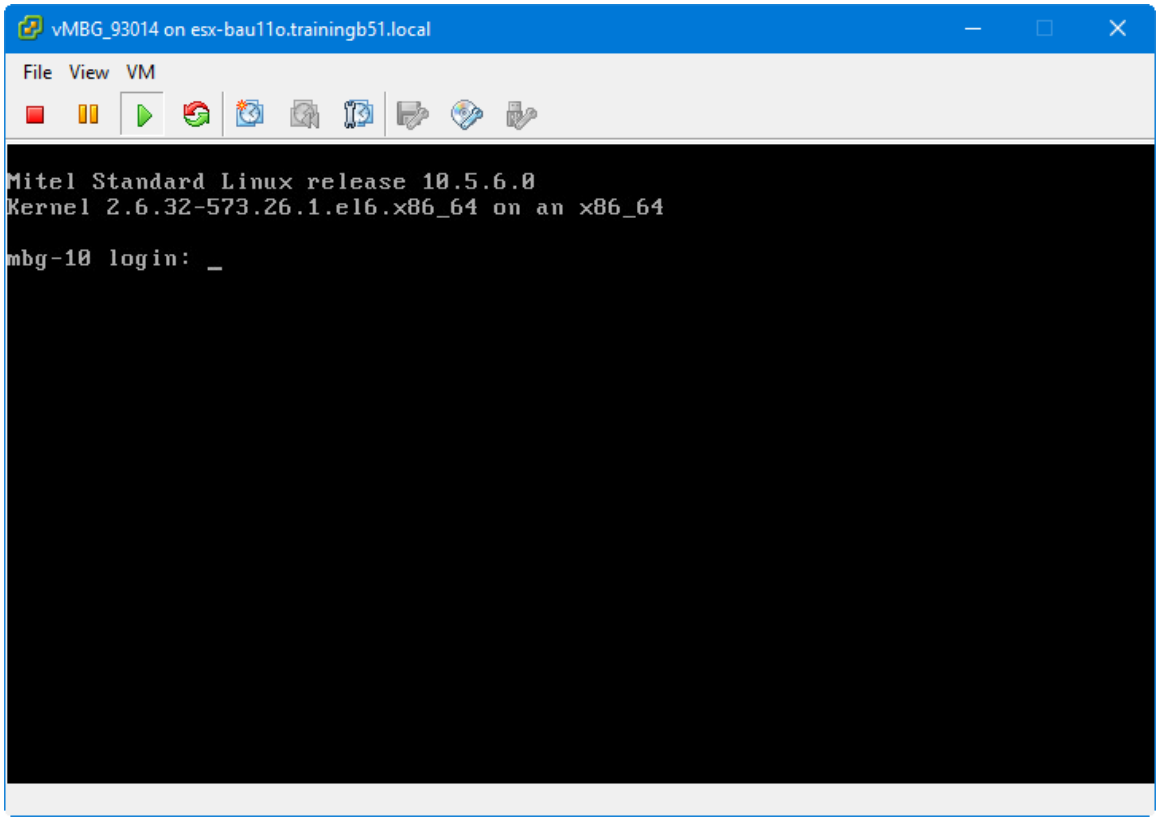

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Activate configuration changes
Your configuration changes will now be activated. The configuration files on this server will be changed to reflect your new settings. This may take a few minutes.
Press ENTER to proceed.
<Finish>


vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Mitel Standard Linux 10.5.6.0 Copyright (C) 1999-2016 Mitel Corporation
Activating configuration settings
Please standby while your configuration settings are activated ...

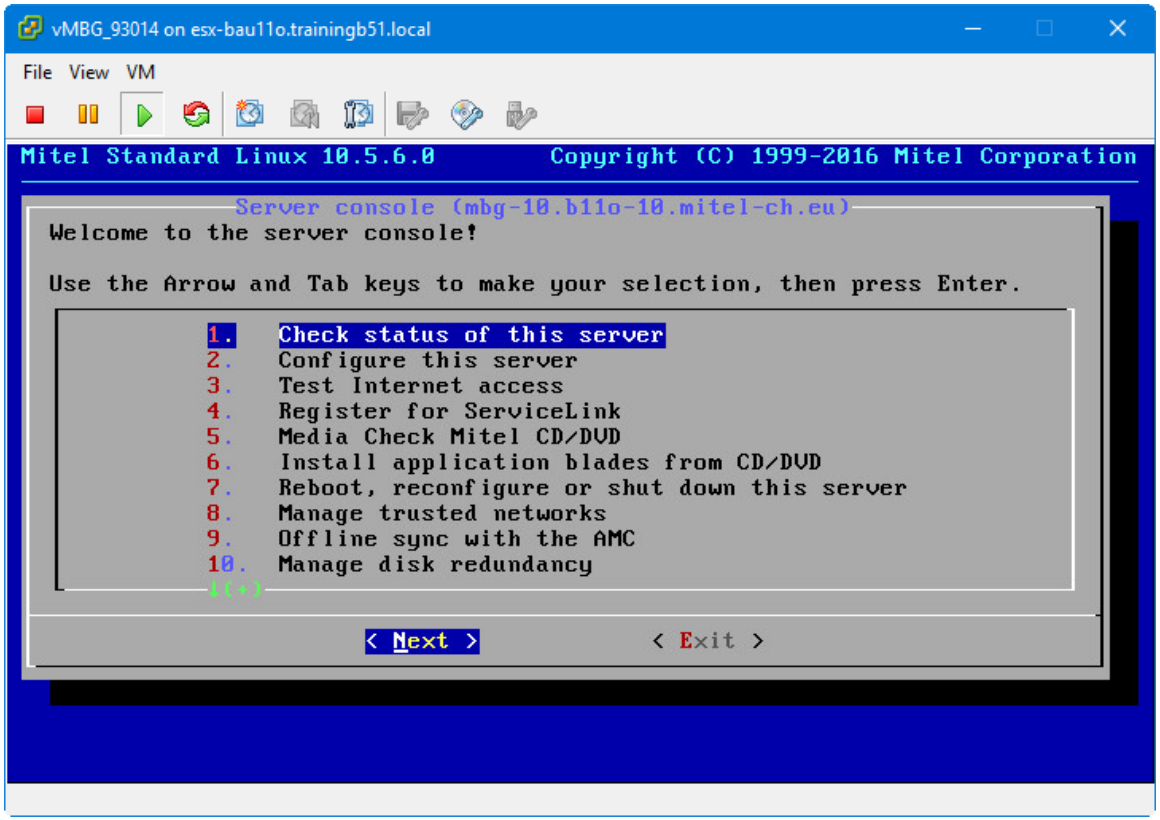

vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Bringing up interface eth0: Determining if ip address 192.168.6.90 is already i
n use for device eth0...
[OK]
Starting auditd: [OK]
Starting cpuspeed: [OFF]
Starting irqbalance: [OK]
Starting nut: [OFF]
Starting raidmonitor: [OK]
Starting system message bus: [OK]
Starting acpi daemon: [OK]
Starting haldaemon: [OK]
Retrigger failed udev events [OK]
Adding udev persistent rules [OK]
Starting oidentd: [OFF]
Enabling IP masquerading: done
Starting wan: [OFF]
Starting blades-manager: [OFF]
Starting postgresql: [OK]
Starting snmpd: [OFF]
Waiting for postgresql to startup: ..
Loading 00_restore_backup into postgresql [OK]
Loading 10_create_mitel_db.sh into postgresql [OK]
Loading dhcpd_db.sh into postgresql [OK]
Loading eventsdb.sh into postgresql [OK]
Loading mslrestdb.sh into postgresql _



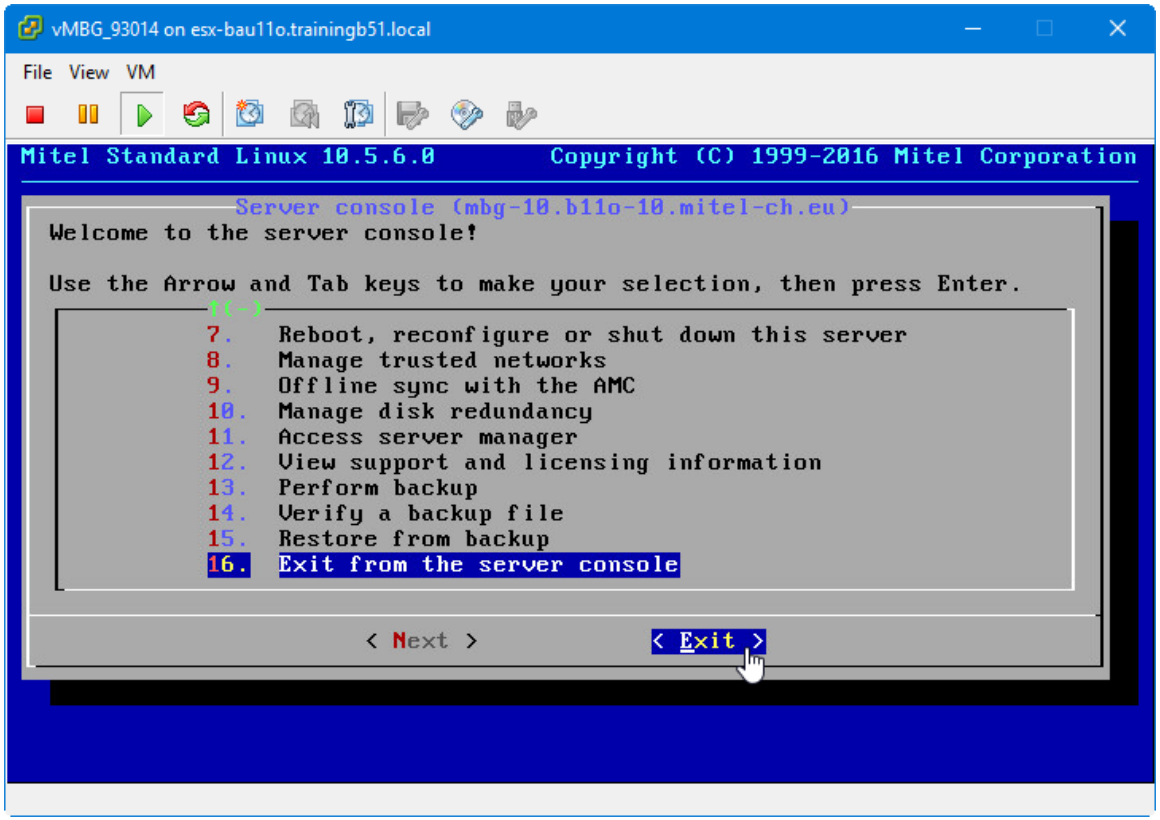
The ARID can be entered later in the Web-GUI.
So just hit "Next"



Login with:
User: admin
Password: *****
(the password was defined at the beginning of this setup)



Next step is to manage trusted networks. Please have a look to the appropriate sub-chapter.

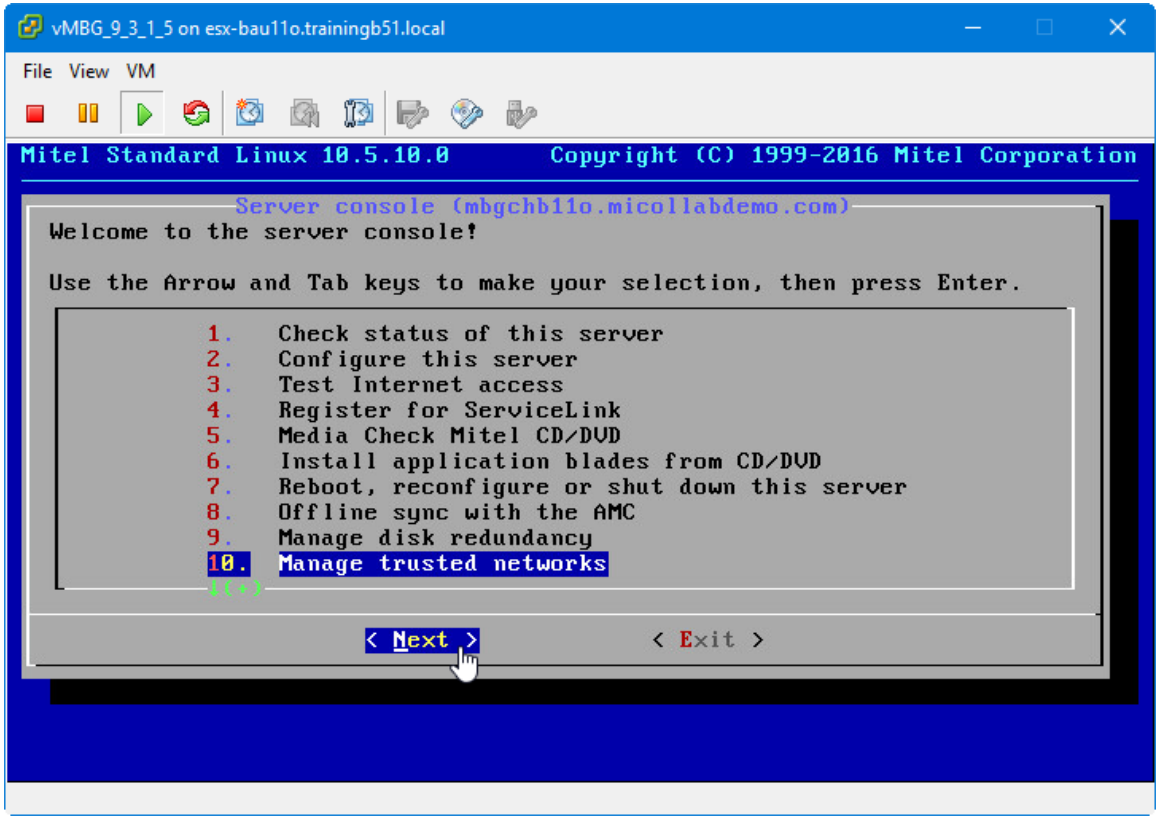


The system is successfully installed :-)

Trusted Networks (for MBG)

To get access to Mitel Standard Linux from another network it has to be trusted:

Add a trusted network for a connection from the MiVO400 to MBG
Optional: Add a trusted network for the connection from the management network to the MBG

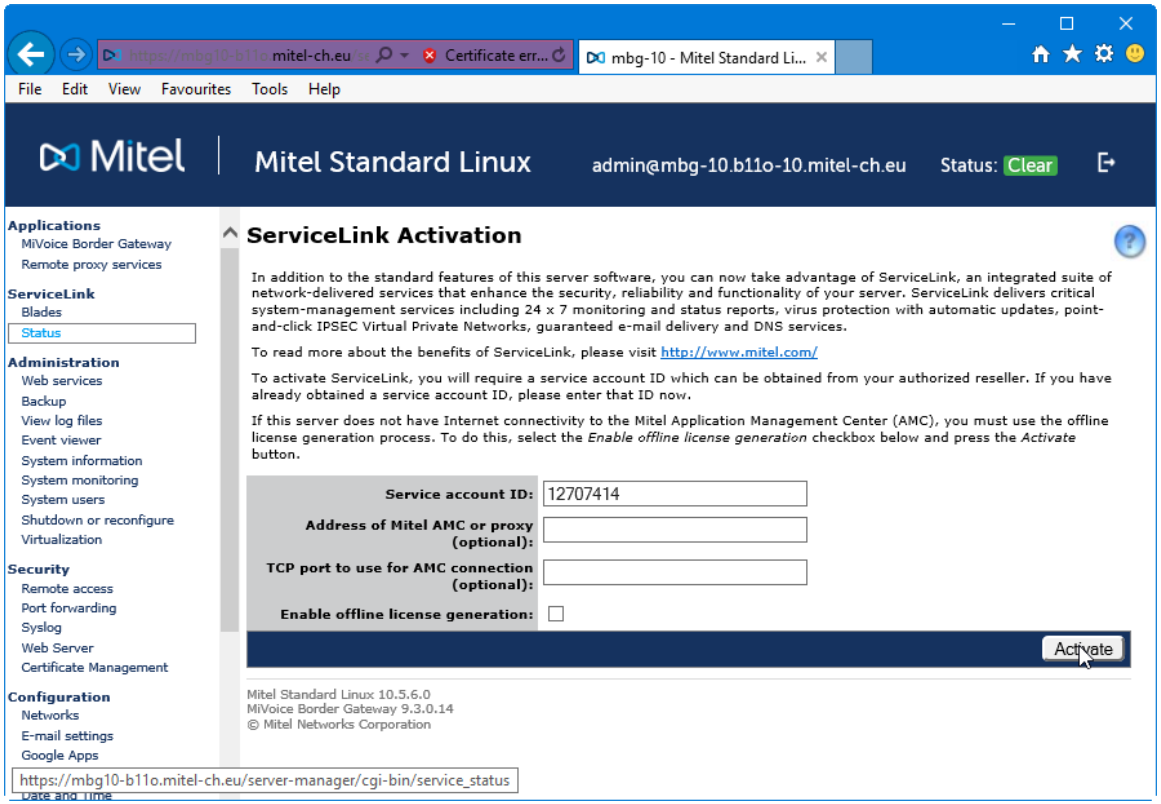


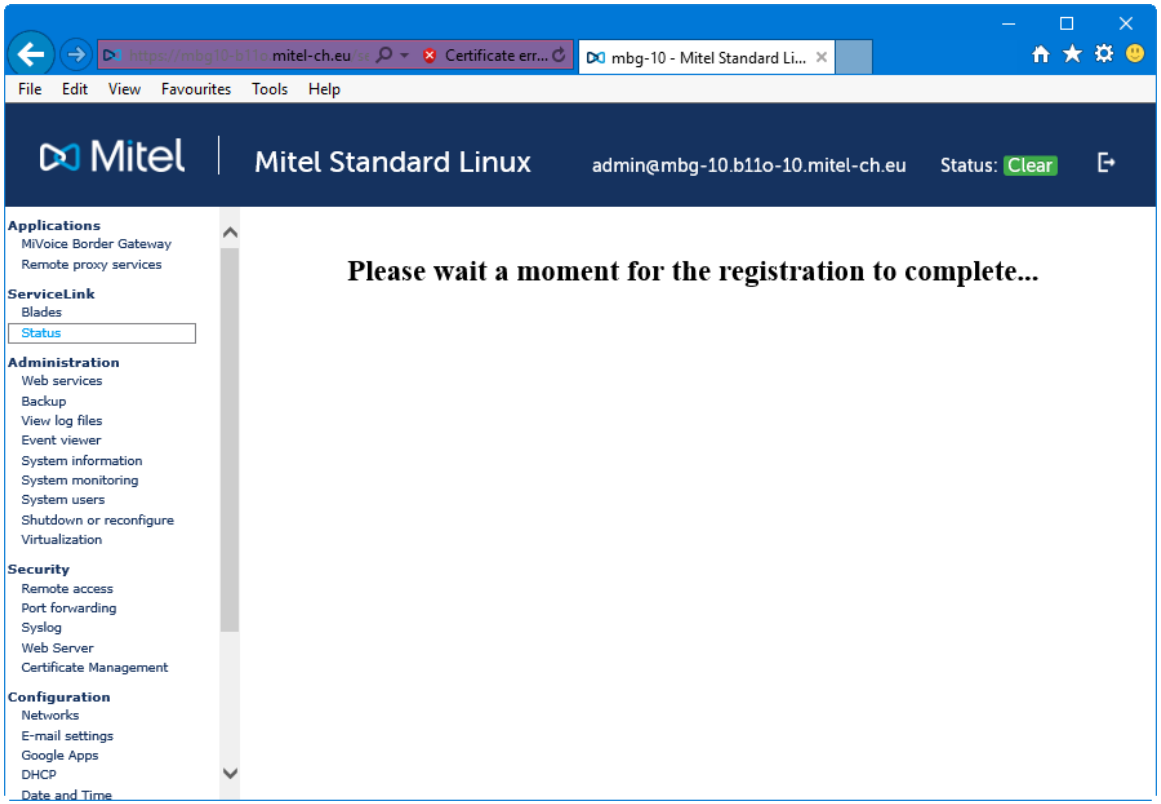
For our training room environment:

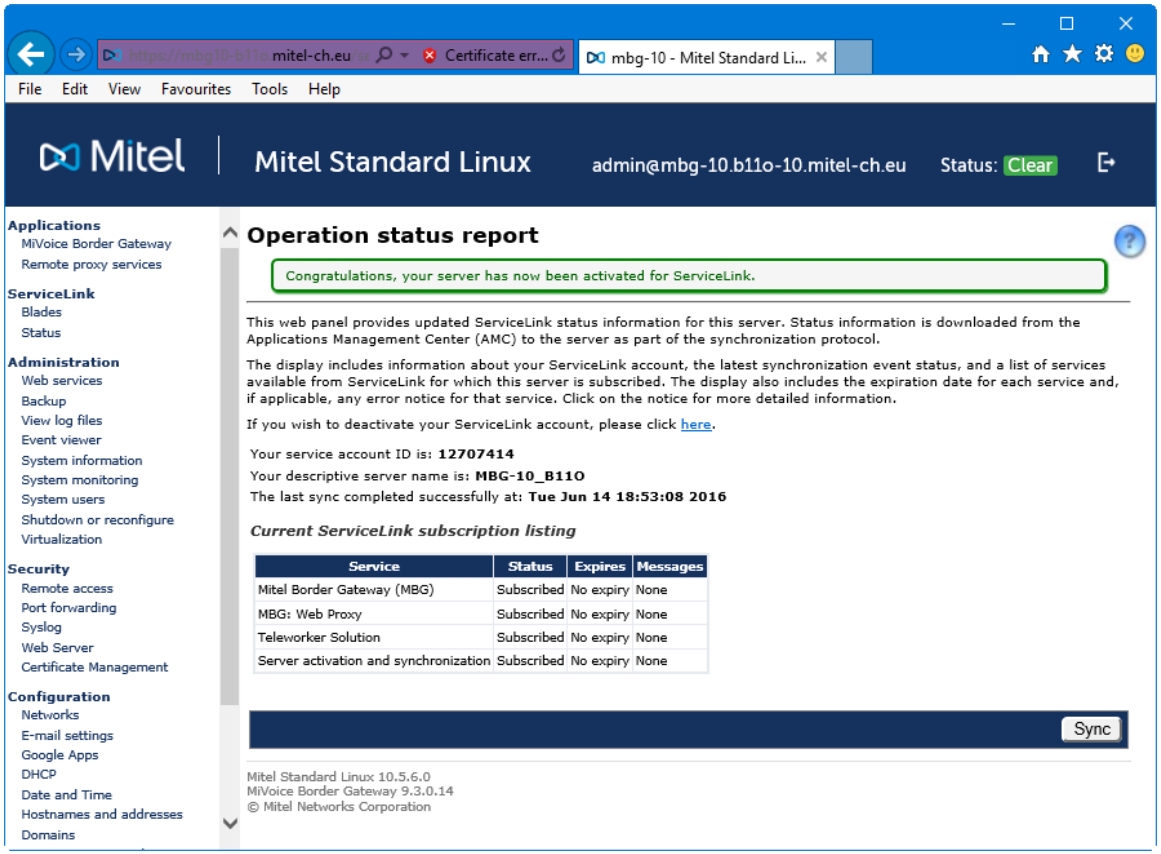
192.168.1.0/24 = management network
192.168.101.0/24 = MiVO400 network
192.168.6.0/24 = own network (DMZ)

MSL: Enter ARID

Service account ID		ARID of the MiVoice Border Gateway from the AMC server
Address of Mitel AMC or proxy	**sync.mitel-amc.com**	Default FQDN of AMC for synchronisation of the purchased licenses
TCP port to use for AMC connection	**22**	Default port




mitel-ch.eu
Certificate err...
mbg-10 - Mitel Standard Li...
File Edit View Favourites Tools Help
Mitel
Mitel Standard Linux
admin@mbg-10.b11o-10.mitel-ch.eu
Status: Clear
Applications
MiVoice Border Gateway
Remote proxy services
ServiceLink
Blades
Status
Administration
Web services
Backup
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reconfigure
Virtualization
Security
Remote access
Port forwarding
Syslog
Web Server
Certificate Management
Configuration
Networks
E-mail settings
Google Apps
DHCP
Date and Time
Please wait a moment for the registration to complete...


mitel-ch.eu
Certificate err...
mbg-10 - Mitel Standard Li...
File Edit View Favourites Tools Help
Mitel
Mitel Standard Linux
admin@mbg-10.b11o-10.mitel-ch.eu
Status: Clear
Applications
MiVoice Border Gateway
Remote proxy services
ServiceLink
Blades
Status
Administration
Web services
Backup
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reconfigure
Virtualization
Security
Remote access
Port forwarding
Syslog
Web Server
Certificate Management
Configuration
Networks
E-mail settings
Google Apps
DHCP
Date and Time
Hostnames and addresses
Domains
Operation status report
Congratulations, your server has now been activated for ServiceLink.
This web 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.
The display includes information about your ServiceLink account, the latest synchronization event status, and a list of services available from ServiceLink for which this server is subscribed. The display also includes the expiration date for each service and, if applicable, any error notice for that service. Click on the notice for more detailed information.
If you wish to deactivate your ServiceLink account, please click here.
Your service account ID is: 12707414
Your descriptive server name is: MBG-10_B11O
The last sync completed successfully at: Tue Jun 14 18:53:08 2016
Current ServiceLink subscription listing
Service | Status | Expires | Messages
Mitel Border Gateway (MBG) | Subscribed | No expiry | None
MBG: Web Proxy | Subscribed | No expiry | None
Teleworker Solution | Subscribed | No expiry | None
Server activation and synchronization | Subscribed | No expiry | None
Sync
Mitel Standard Linux 10.5.6.0
MiVoice Border Gateway 9.3.0.14
© Mitel Networks Corporation

MSL: Manage Web server certificate

MBG needs a web server certificates to be able to establish TLS connections (for SIP and XML) with the teleworker SIP phones.

Certificates

On the MBG a public signed certificate is mandatory for this teleworker solution.

Let's Encrypt

(extract of MBG Online Help)

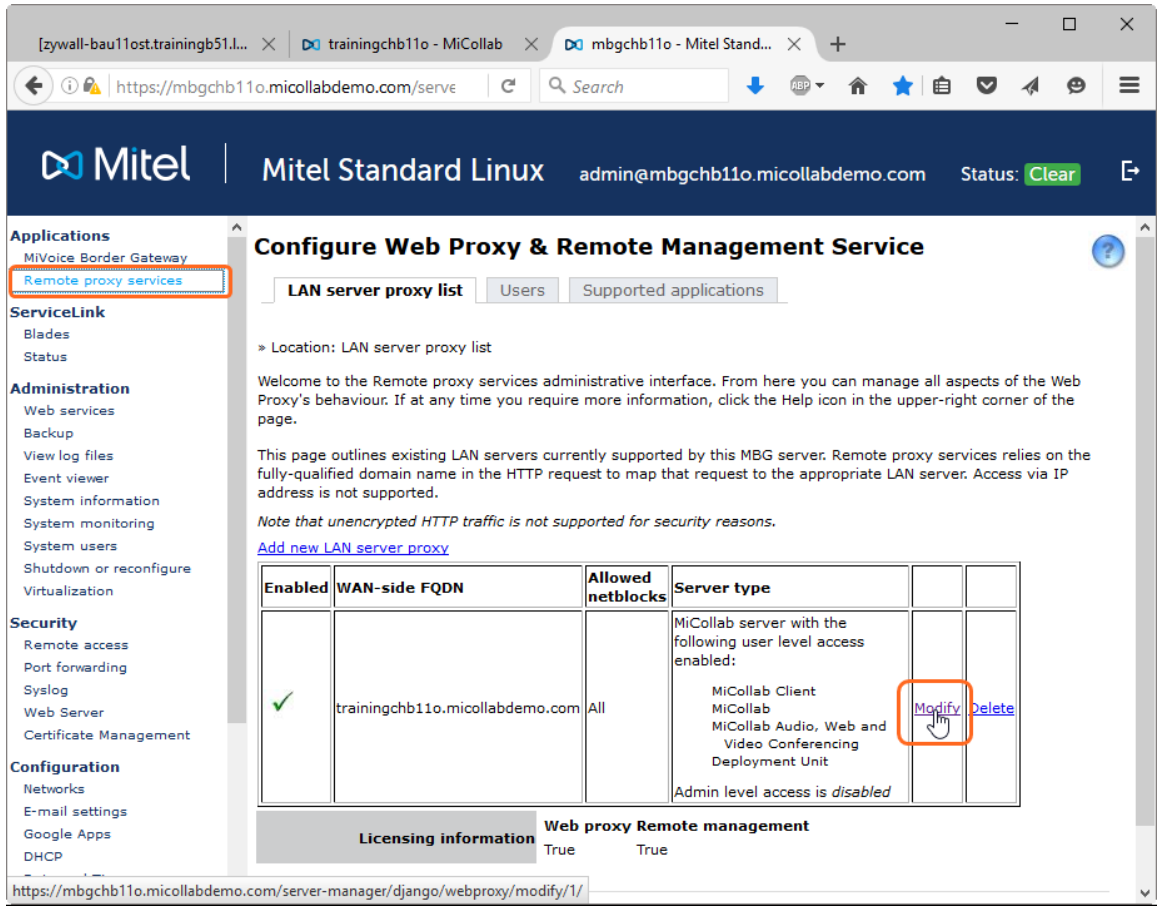
Let’s Encrypt is a free, automated, and open Certificate Authority (CA). It enables you to obtain a valid web server certificate simply by providing your domain settings and then clicking a button.
The acquired certificate is uploaded, installed, monitored and renewed automatically. You do not need to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

Notes:

- To use this service, the MSL server must be accessible to the Internet.
- This service is only supported on single-server, standalone implementations of applications that use the MSL operating system such as MiVoice Border Gateway.

Request a "Let's Encrypt" SSL Certificate

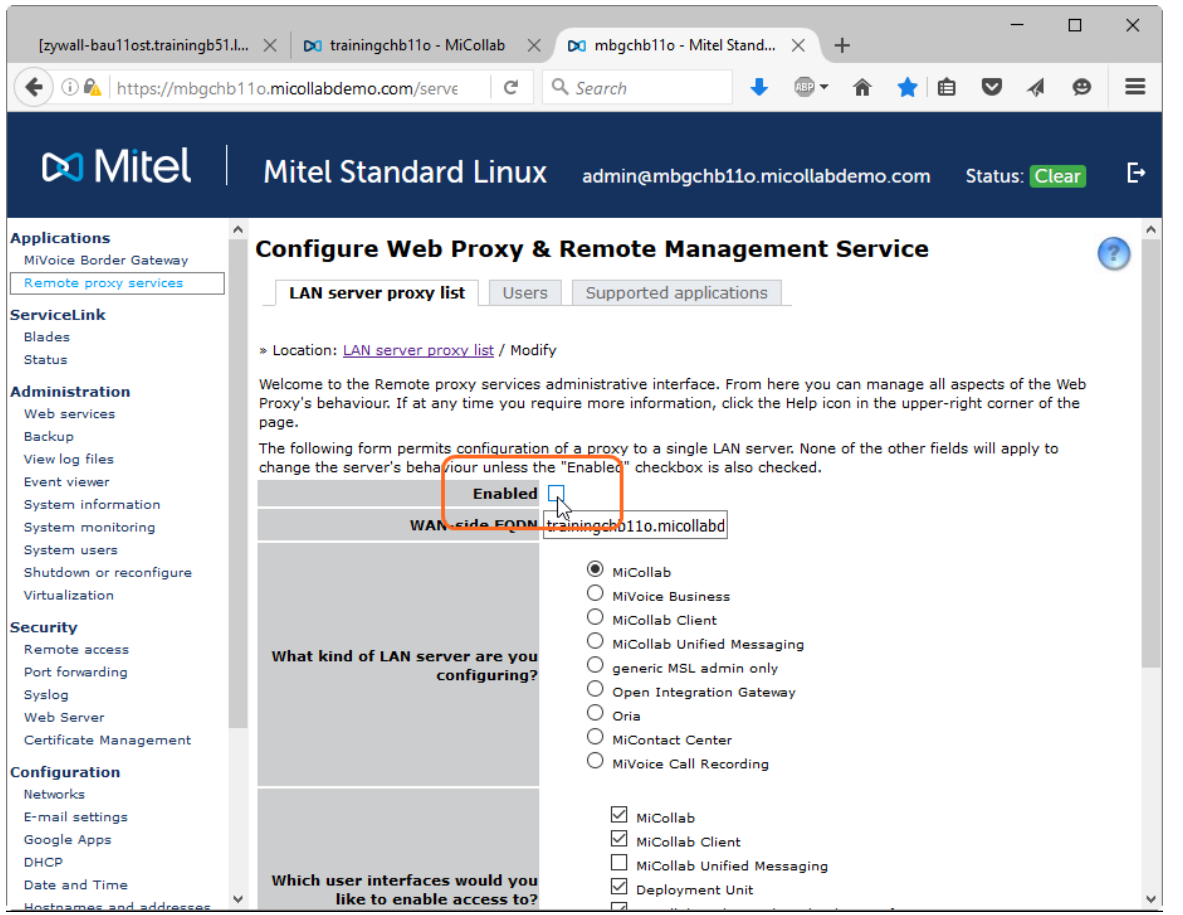
Before requesting a "Let's Encrypt" SSL certificate make sure that the "Remote proxy service" is switched off.



Go to "Remote proxy services".

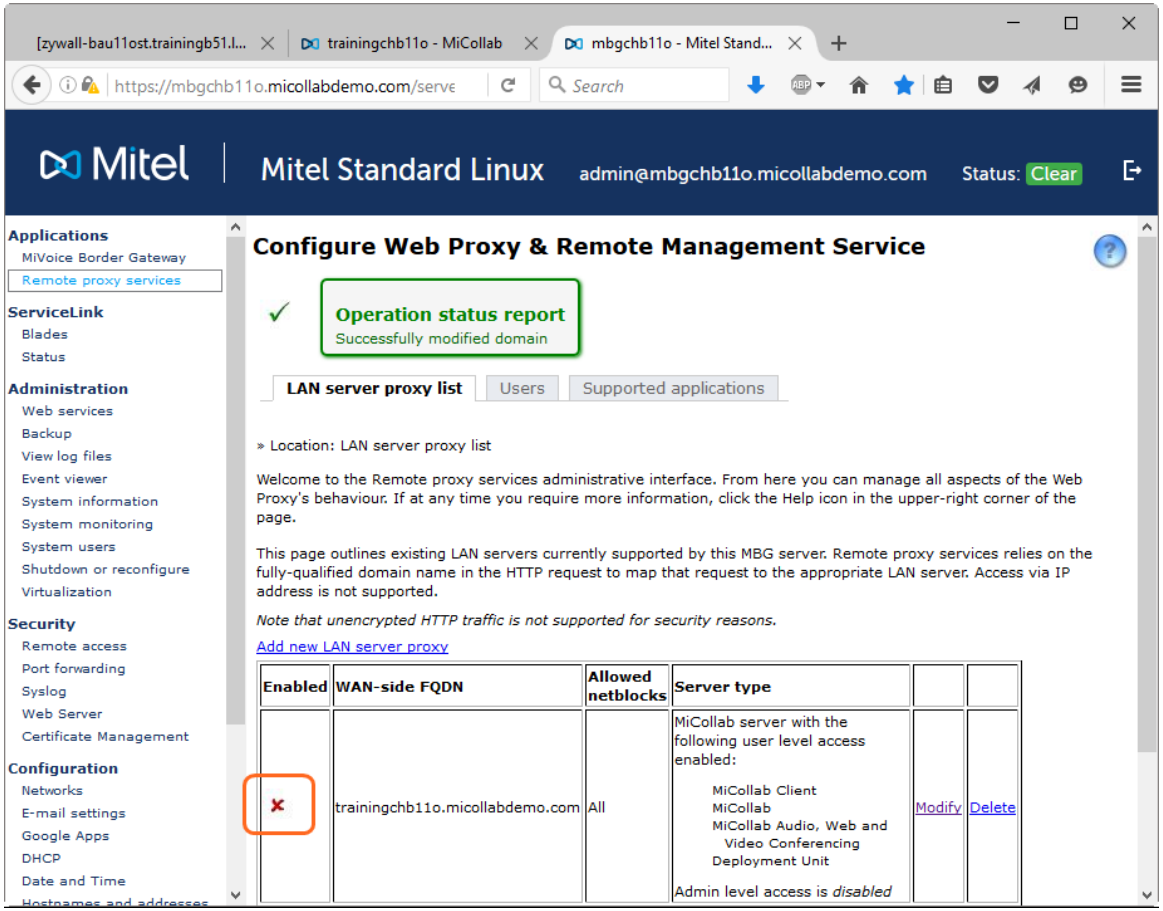
If the service is already configured
(see chapter: "Integrate Audio, Web & Video")

click "Modify"



Remove the "Enabled" tick.

Save

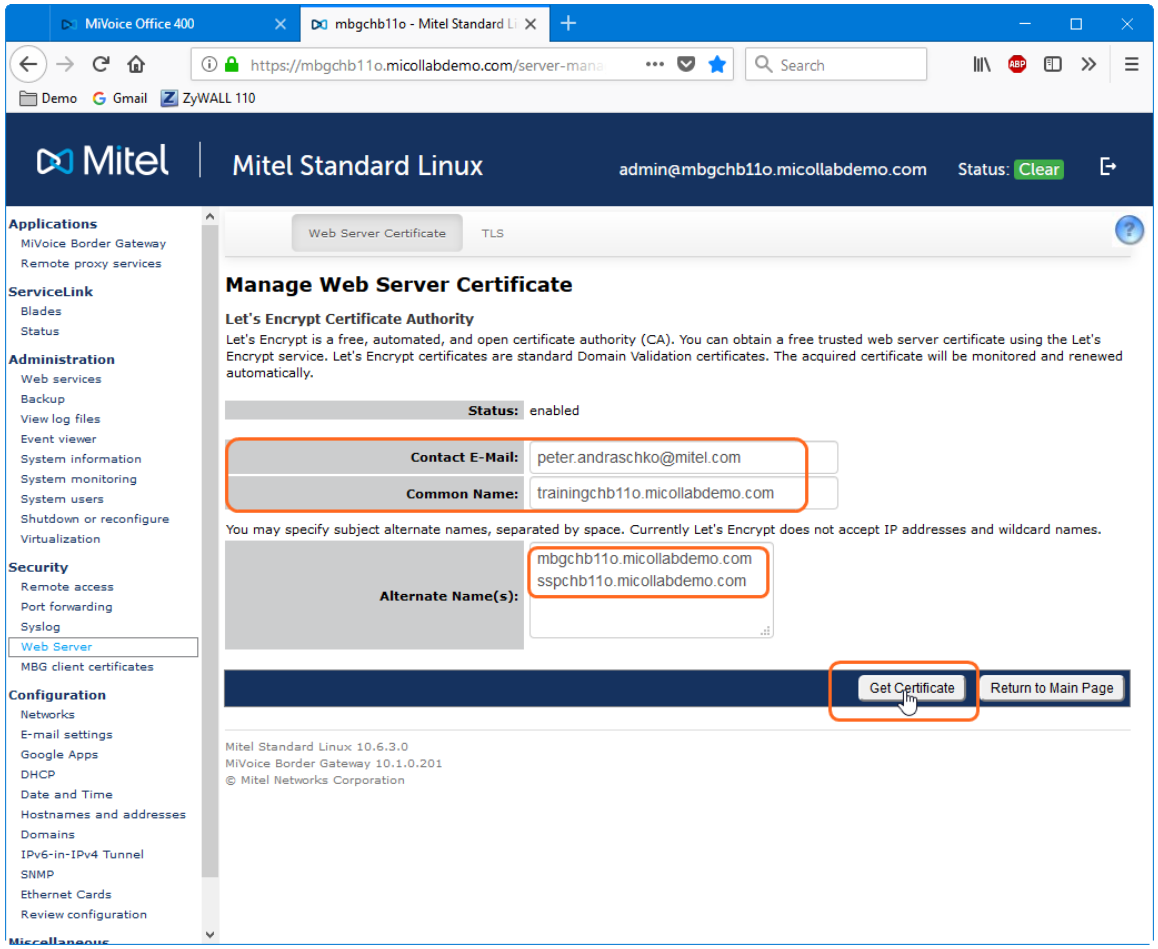


Hint: Don't forget to turn the service on again, after successfully requesting a "Let's encrypt" certificate.

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 **Modify Request**.
5. Update the filed values as required.

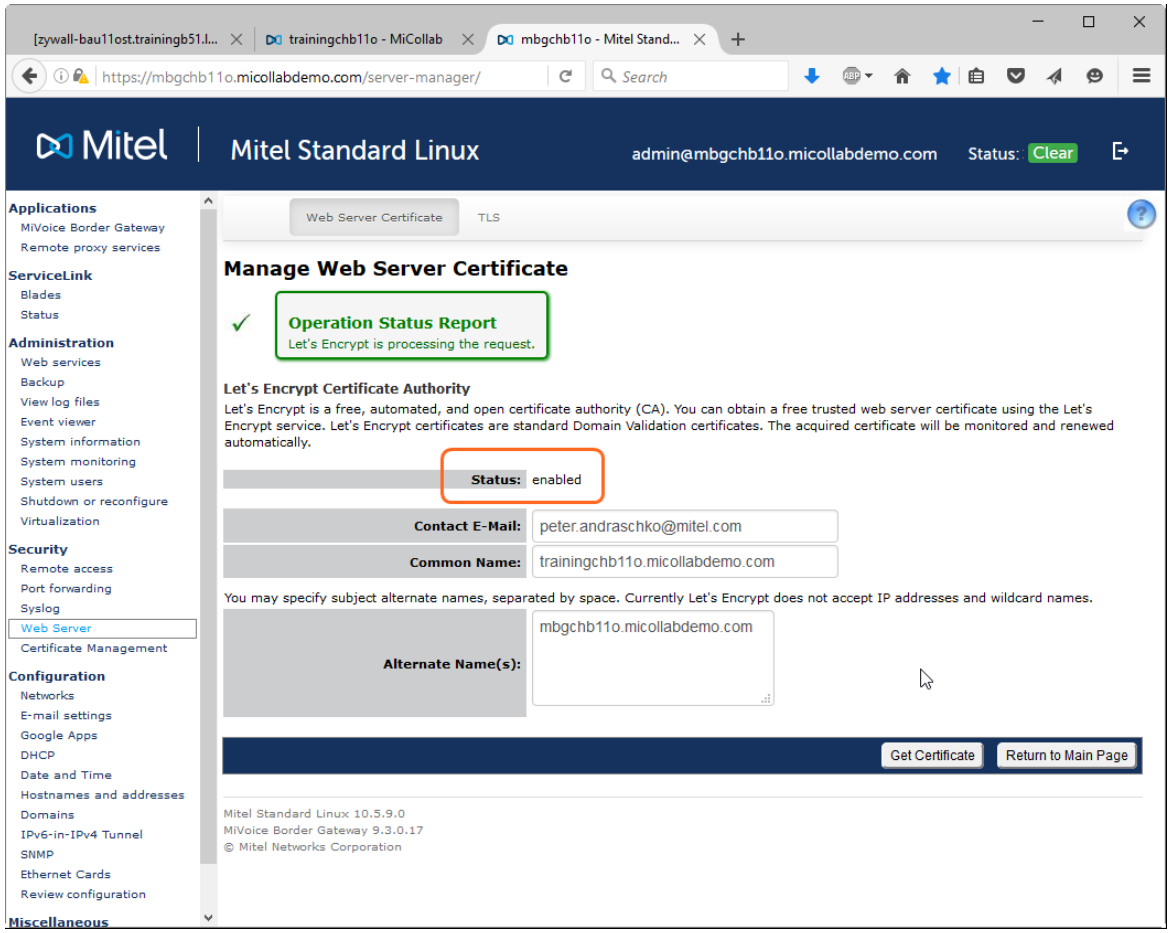
Field Name	Description
Status	Indicates the status of the certificate, either enabled (successfully installed and active) or disabled (not successfully installed and inactive)
Contact E-Mail	Enter the email address of the administrator who Let's Encrypt should contact to deal with issues of certificate recovery or registration.
Common Name	Enter the common name to which you plan to apply your certificate. A web browser checks this field. It is required. The common name must be entered as a fully-qualified domain name (FQDN). 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. **Note**: You may specify subject alternate names, separated by space. Currently Let's Encrypt does not accept IP addresses and wildcard names.

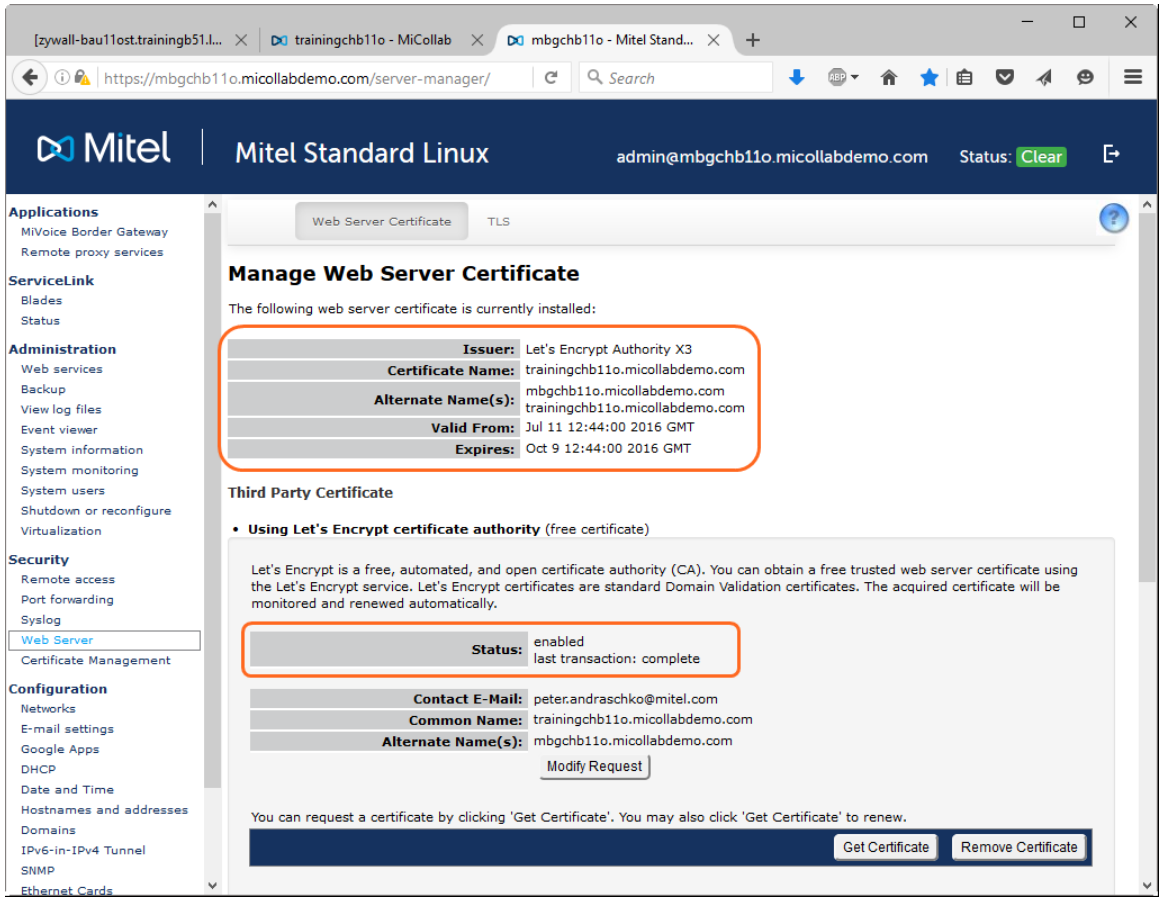


All names (common name and alternate names) have to be resolvable by public DNS.

The system needs the MBG FQDN and the SSP FQDN, plus any MiCollab (In the Alternate Names field.)

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.


[zywall-bau11ost.trainingb51.l...
trainingchb11o - MiCollab
mbgchb11o - Mitel Stand...
https://mbgchb11o.micollabdemo.com/server-manager/
Search
Mitel
Mitel Standard Linux
admin@mbgchb11o.micollabdemo.com
Status: Clear
Applications
MiVoice Border Gateway
Remote proxy services
ServiceLink
Blades
Status
Administration
Web services
Backup
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reconfigure
Virtualization
Security
Remote access
Port forwarding
Syslog
Web Server
Certificate Management
Configuration
Networks
E-mail settings
Google Apps
DHCP
Date and Time
Hostnames and addresses
Domains
IPv6-in-IPv4 Tunnel
SNMP
Ethernet Cards
Review configuration
Miscellaneous
Web Server Certificate
TLS
Manage Web Server Certificate
Operation Status Report
Let's Encrypt is processing the request.
Let's Encrypt Certificate Authority
Let's Encrypt is a free, automated, and open certificate authority (CA). You can obtain a free trusted web server certificate using the Let's Encrypt service. Let's Encrypt certificates are standard Domain Validation certificates. The acquired certificate will be monitored and renewed automatically.
Status: enabled
Contact E-Mail: peter.andraschko@mitel.com
Common Name: trainingchb11o.micollabdemo.com
You may specify subject alternate names, separated by space. Currently Let's Encrypt does not accept IP addresses and wildcard names.
Alternate Name(s): mbgchb11o.micollabdemo.com
Get Certificate
Return to Main Page
Mitel Standard Linux 10.5.9.0
MiVoice Border Gateway 9.3.0.17
© Mitel Networks Corporation



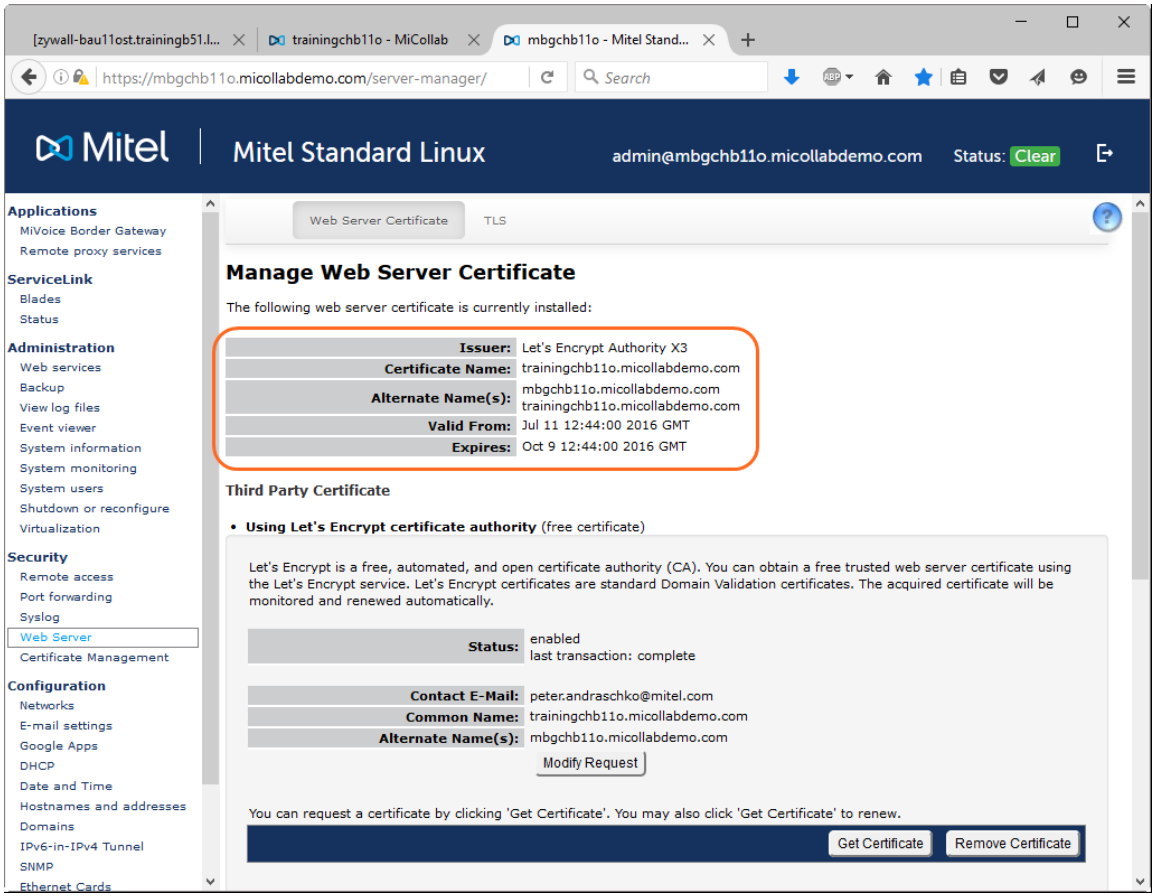
After some seconds the "Let's encrypt" SSL certificate is installed and valid on the MBG server.

Hint: Don't forget to turn the "Remote proxy service" on again, after successfully requesting a "Let's encrypt" certificate

Verify the installed certificate

Currently Installed Web Server Certificate

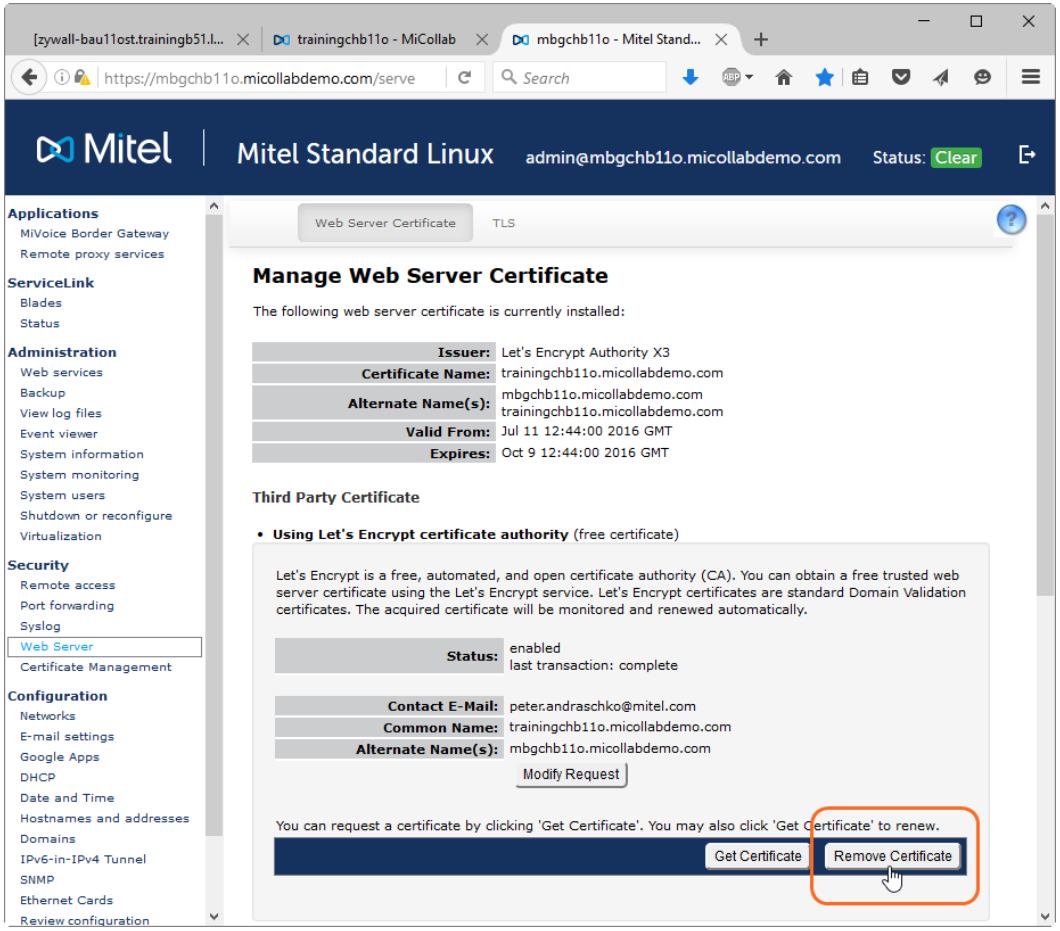
If a web server certificate is currently installed on the MSL server, the details are listed at the top of the Web Server Certificate page.



Uninstall a Let's Encrypt SSL Certificate

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

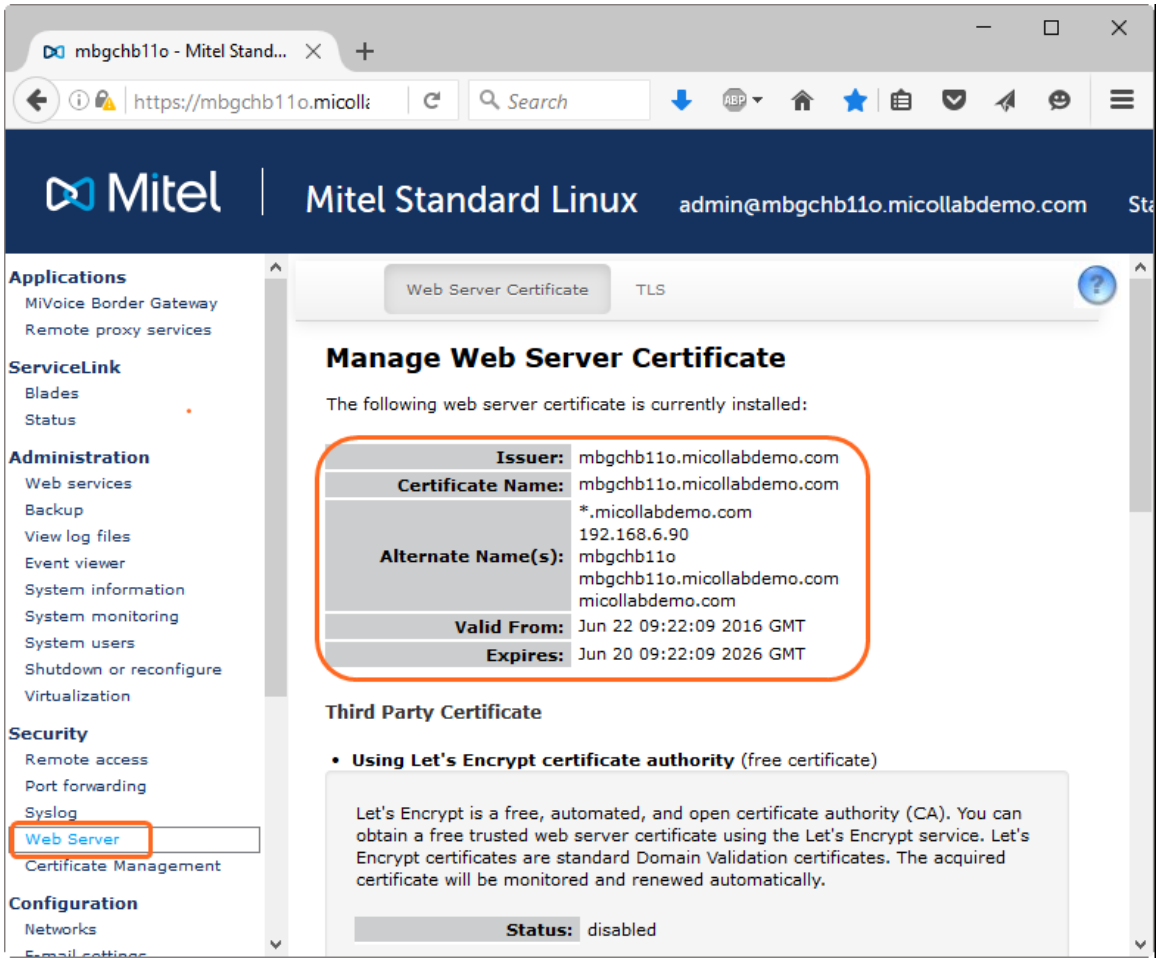
1. Log into the MSL Server Manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Remove Certificate**.



Other Third party Certificate

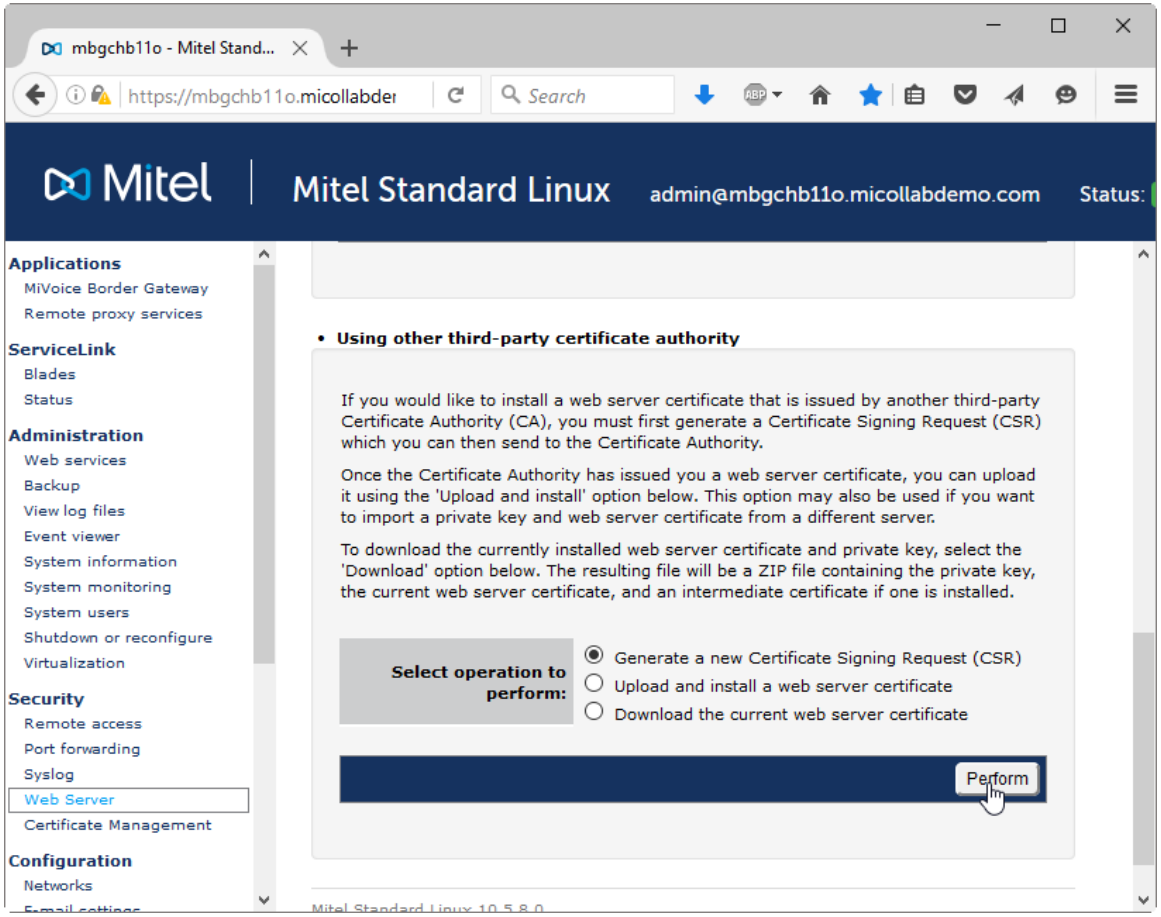
You can also request a public signed SSL certificate from a public CA (like: VeriSign, GoDaddy, Entrust, …)

Create a Certificate Signing Request



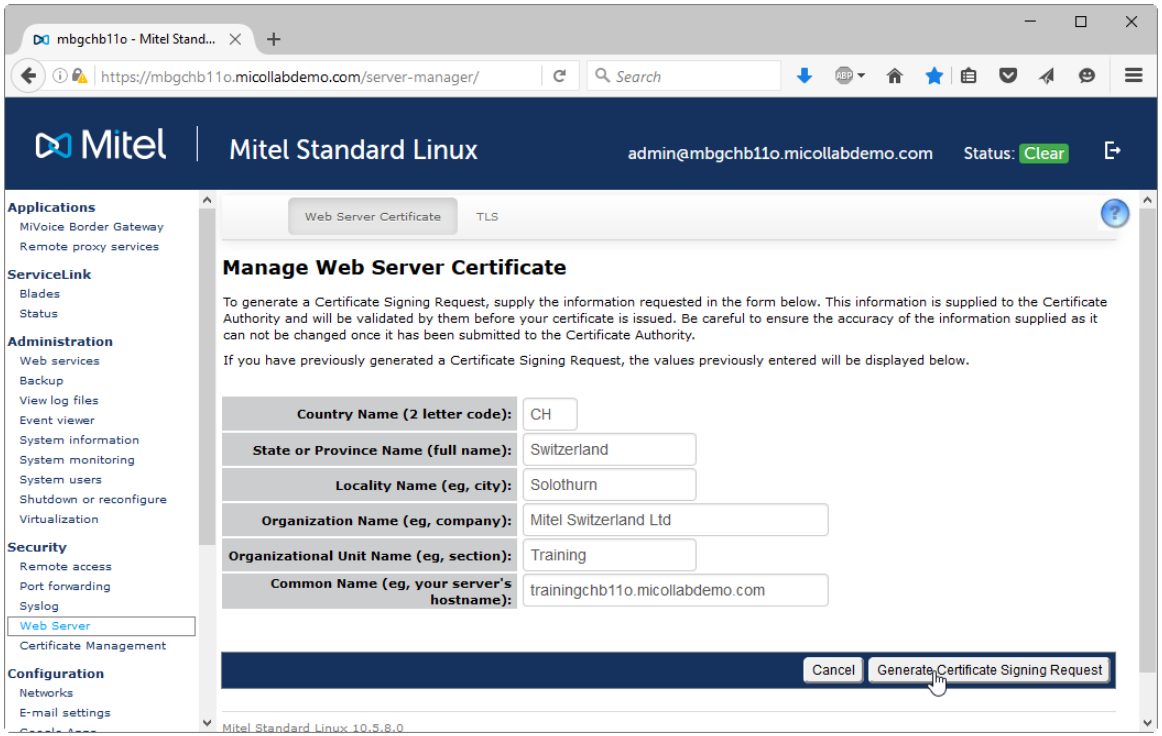
Here you see the default "self-signed" certificate which is automatically created when the MBG is installed.

Scroll down



Select "Generate a new CSR"

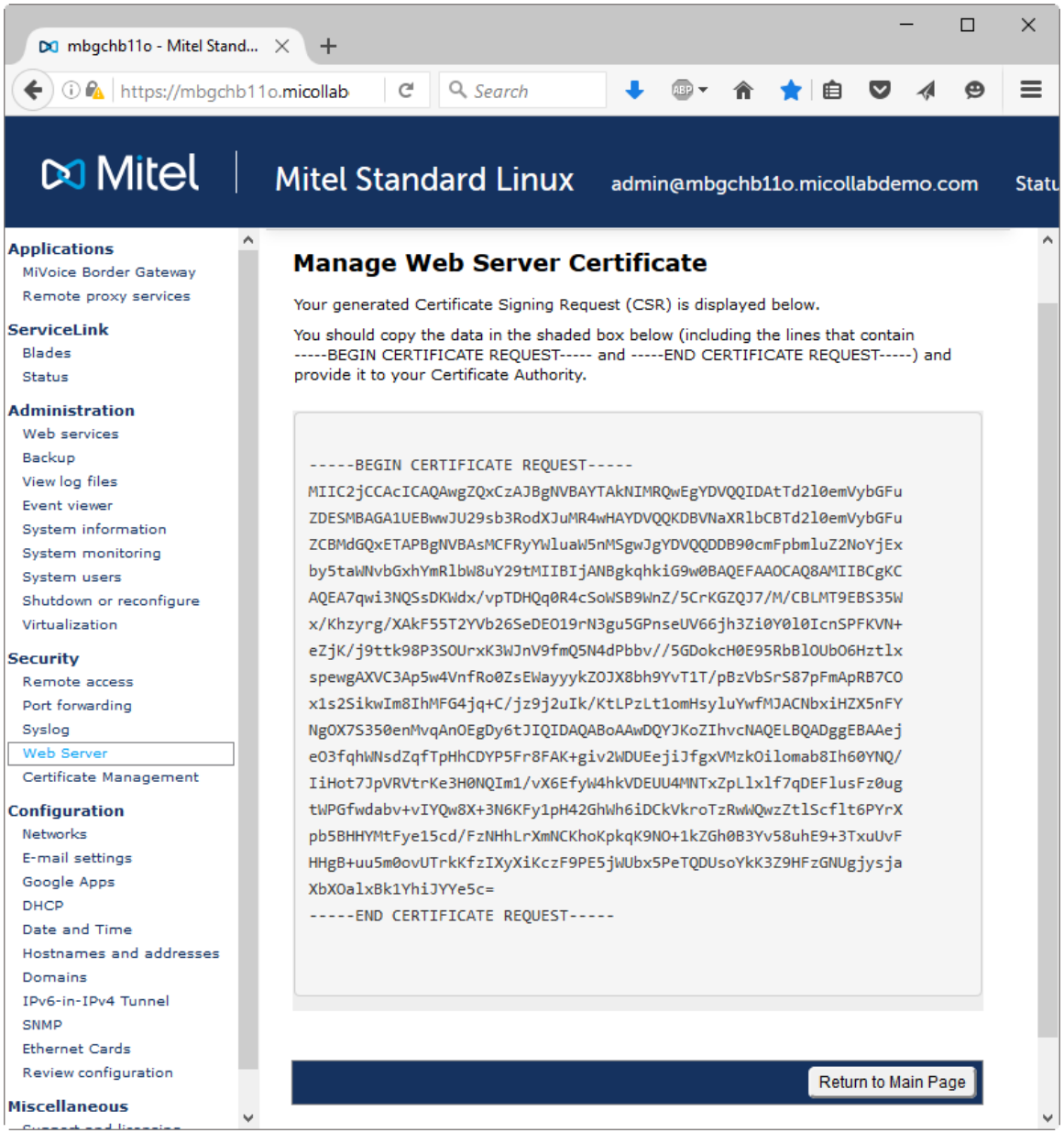
and click "Perform"



Enter the required information.

The common name has to be the FQDN, which is reachable from the Internet to your MBG in the DMZ.

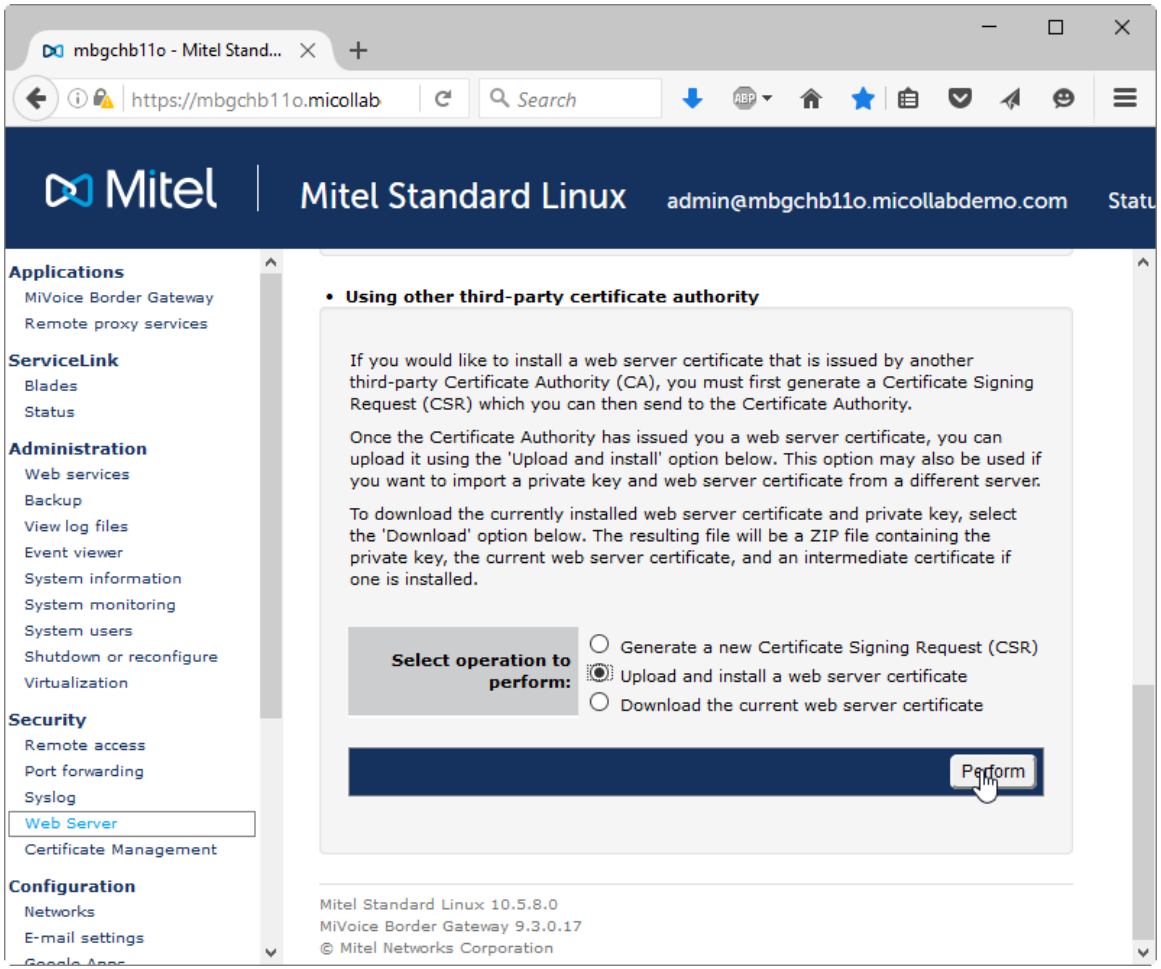
Click "Generate CSR"



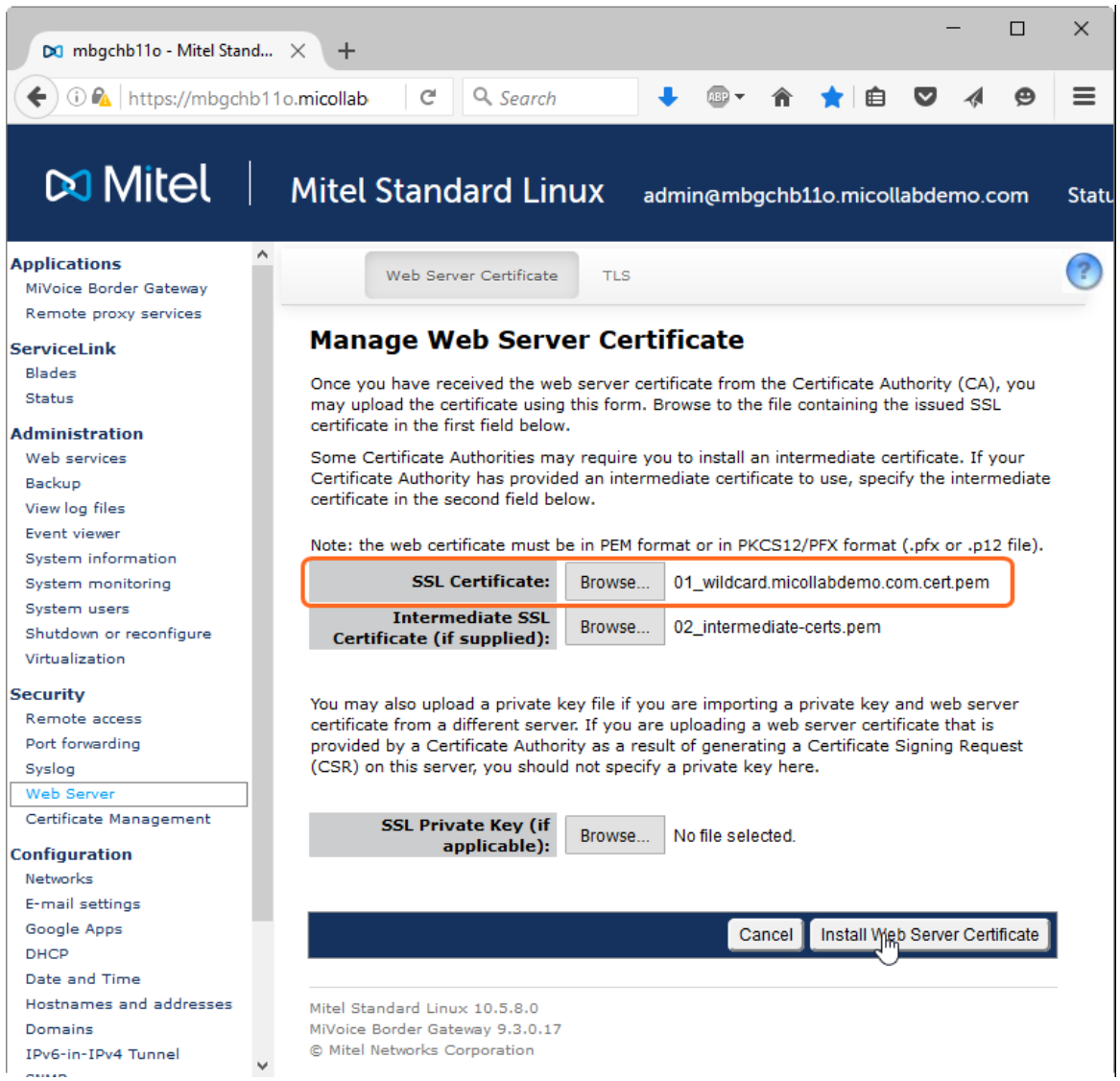
MSL has created a private key and the CSR.

Copy the CSR into a text file. You will need it to request the cert from your public CA.

Upload and install a Certificate



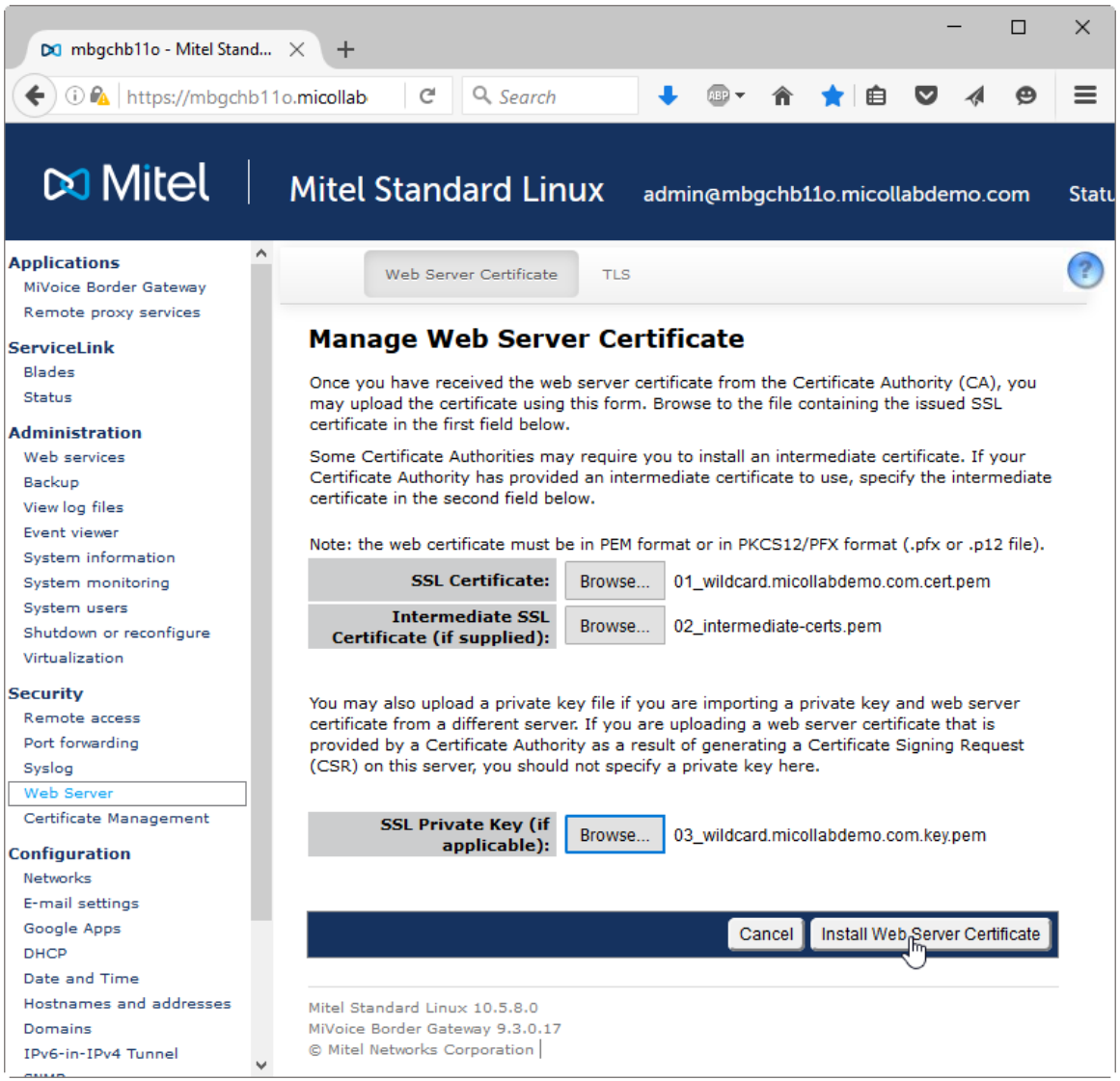
After you received the certificate from your public CA you can upload it here.



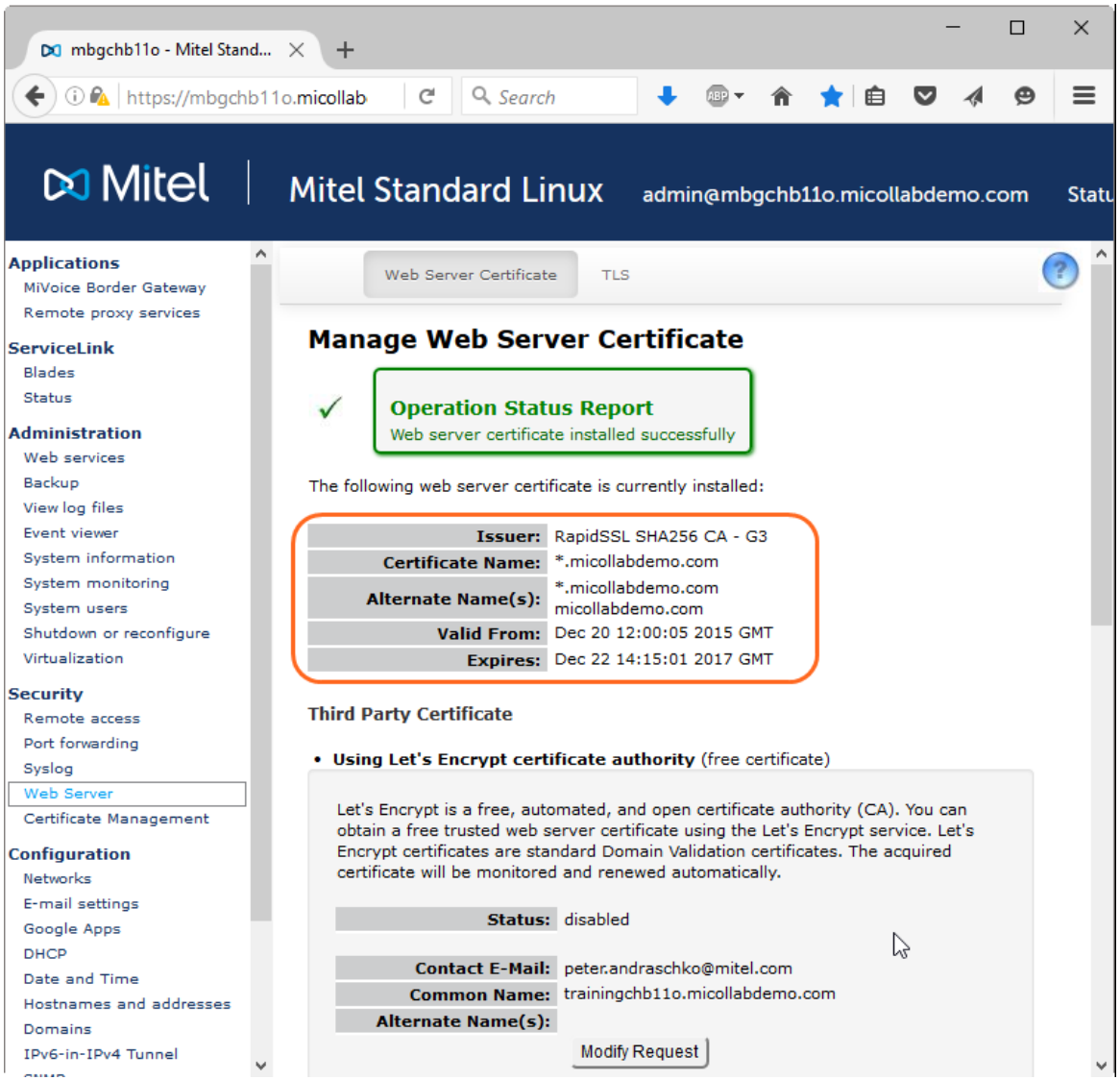
Enter the SSL certificate

(and if provided by your CA enter also the intermediate SSL certificate)

This is enough if the CSR was done on this MBG.

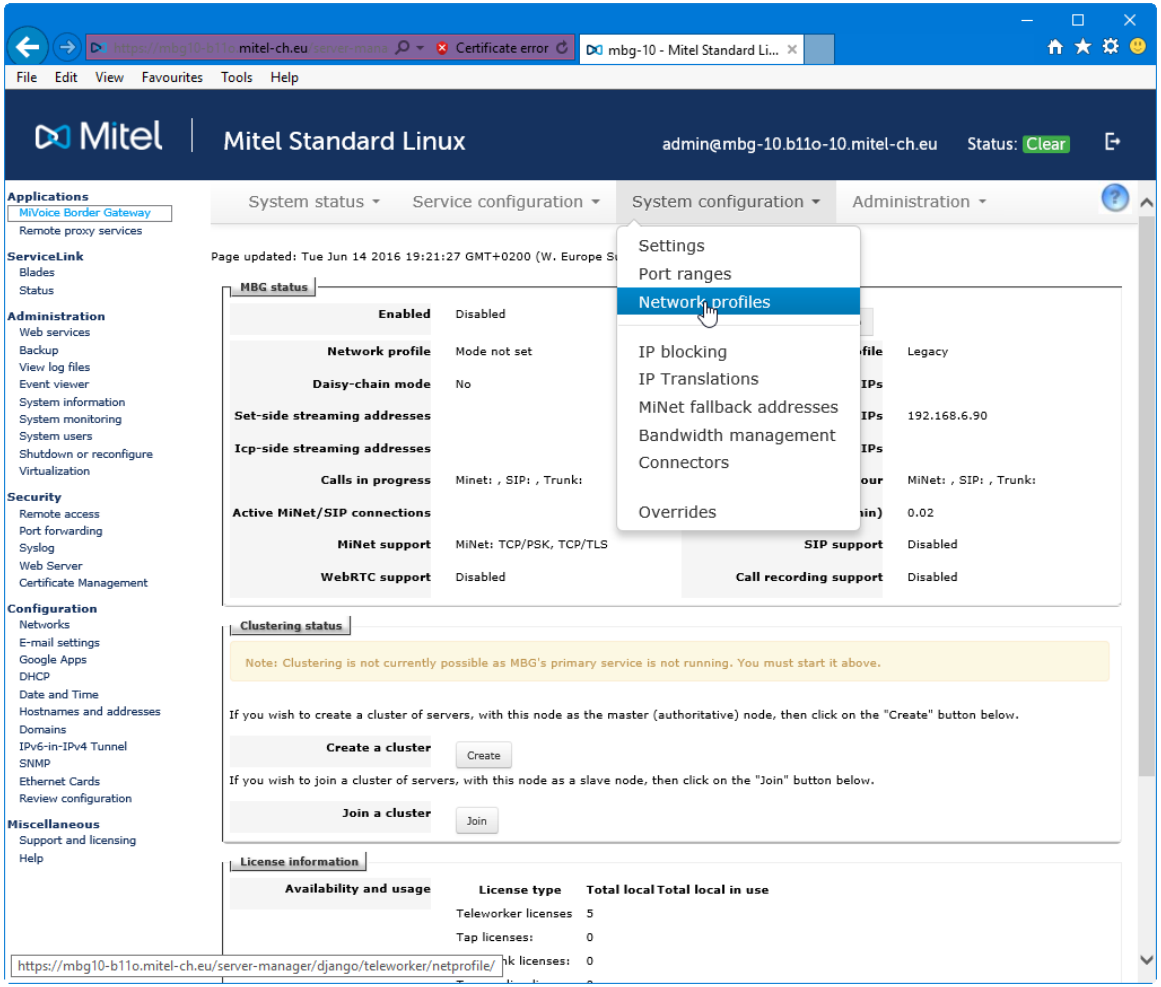


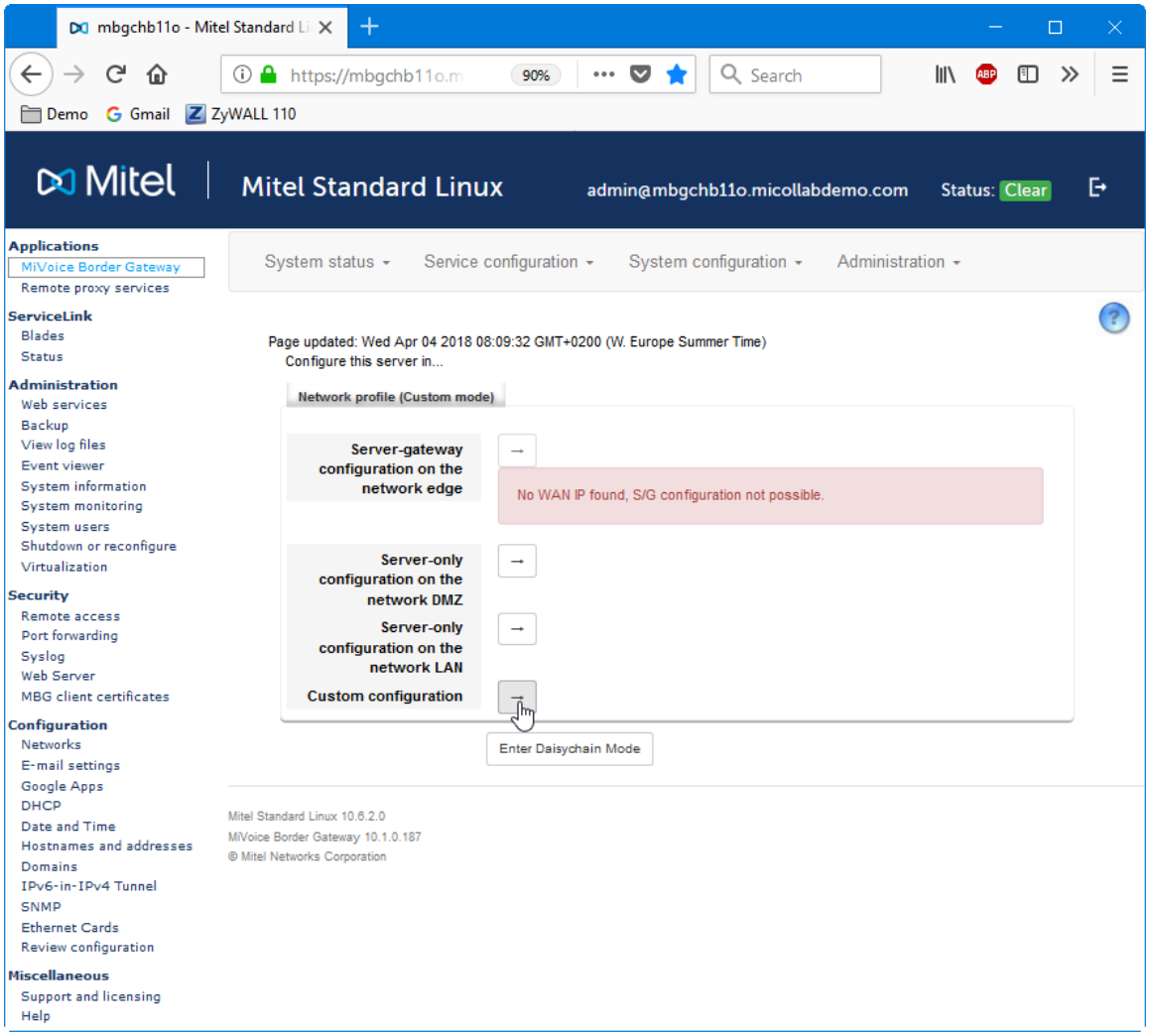
If the CSR was not done on this MBG, you have to install the private key for this certificate as well.



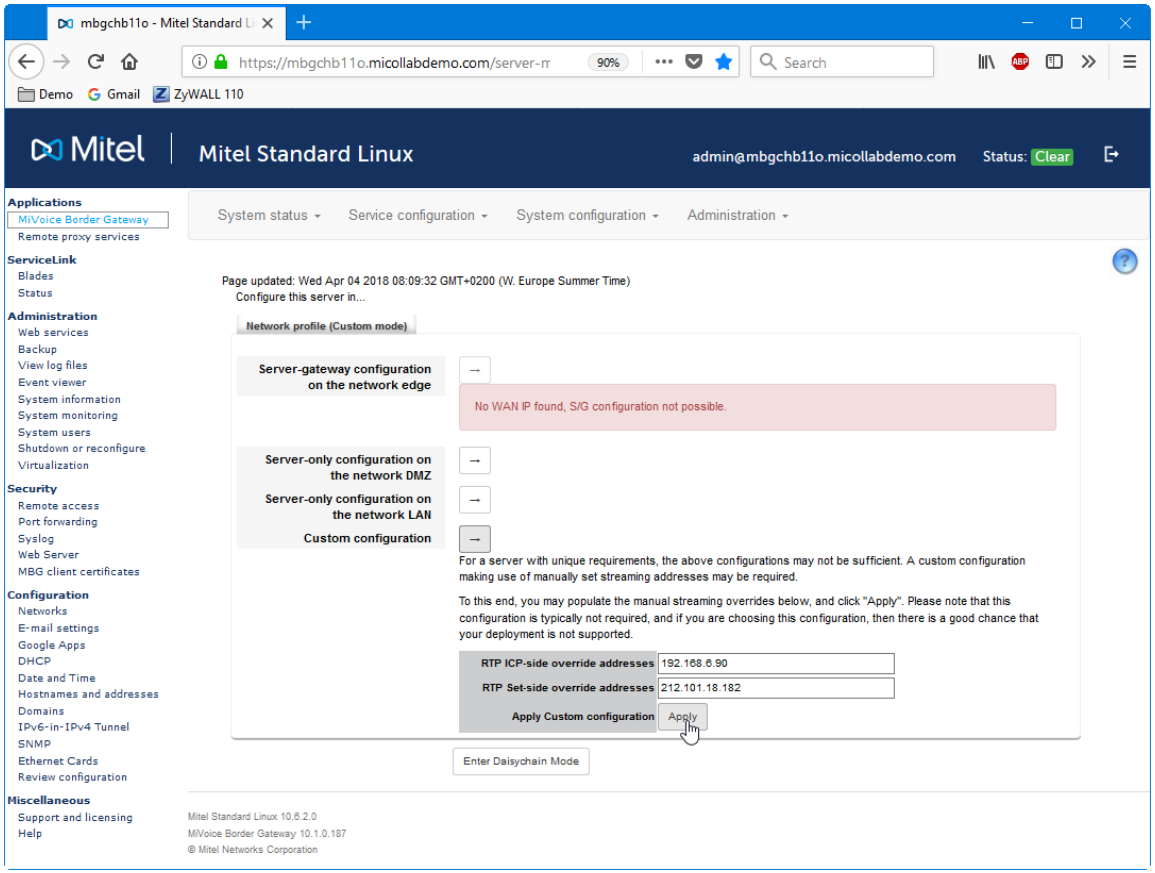
The installed certificate is directly visible.

MBG: System configuration: Network profile





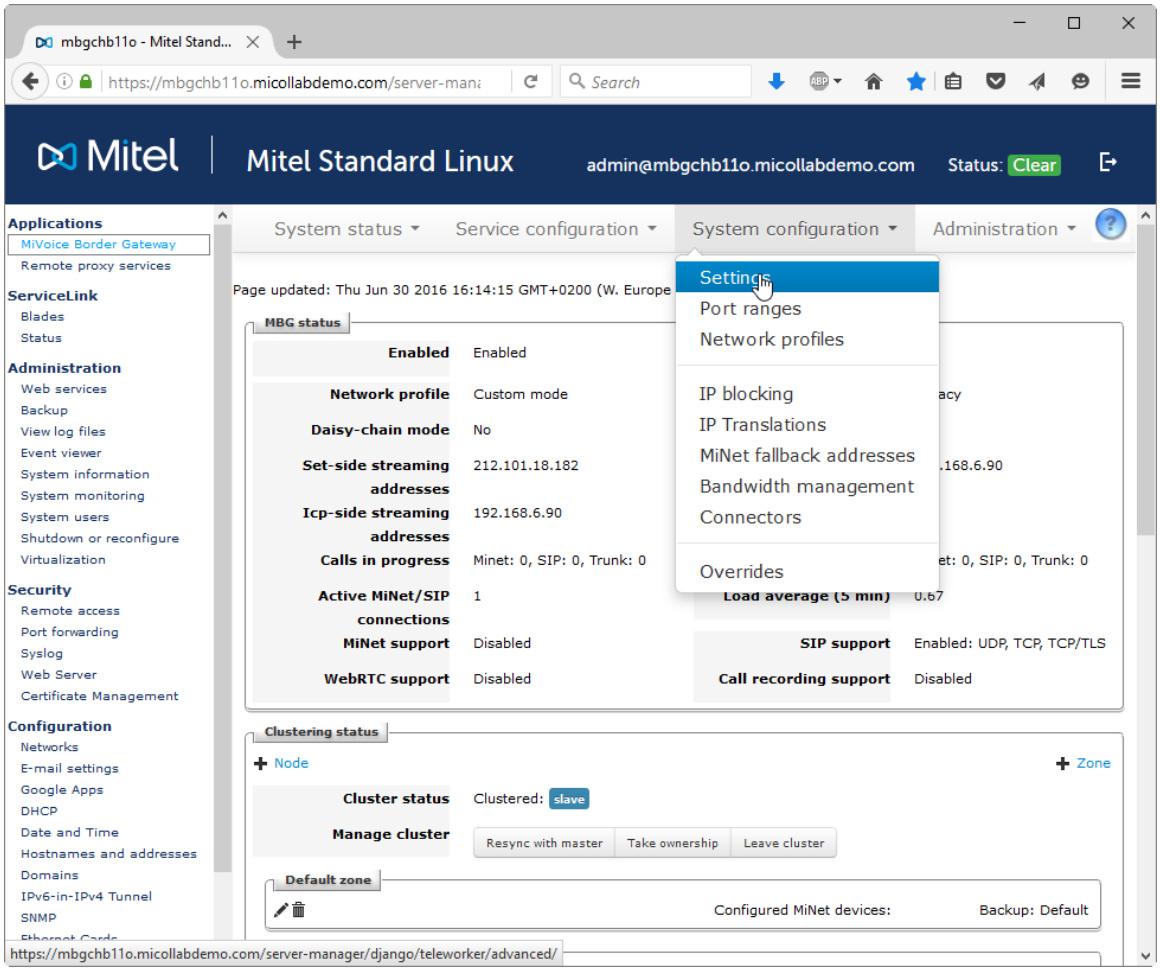
Chose Custom configuration

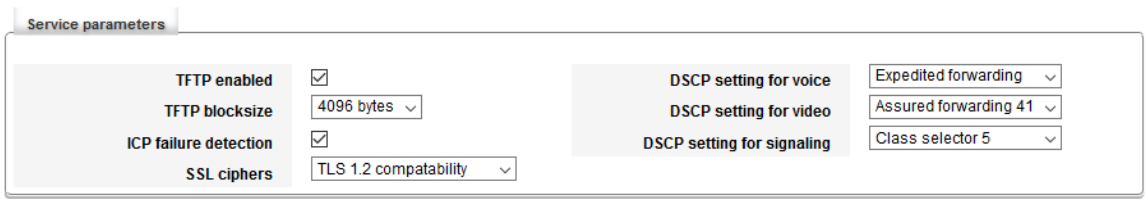
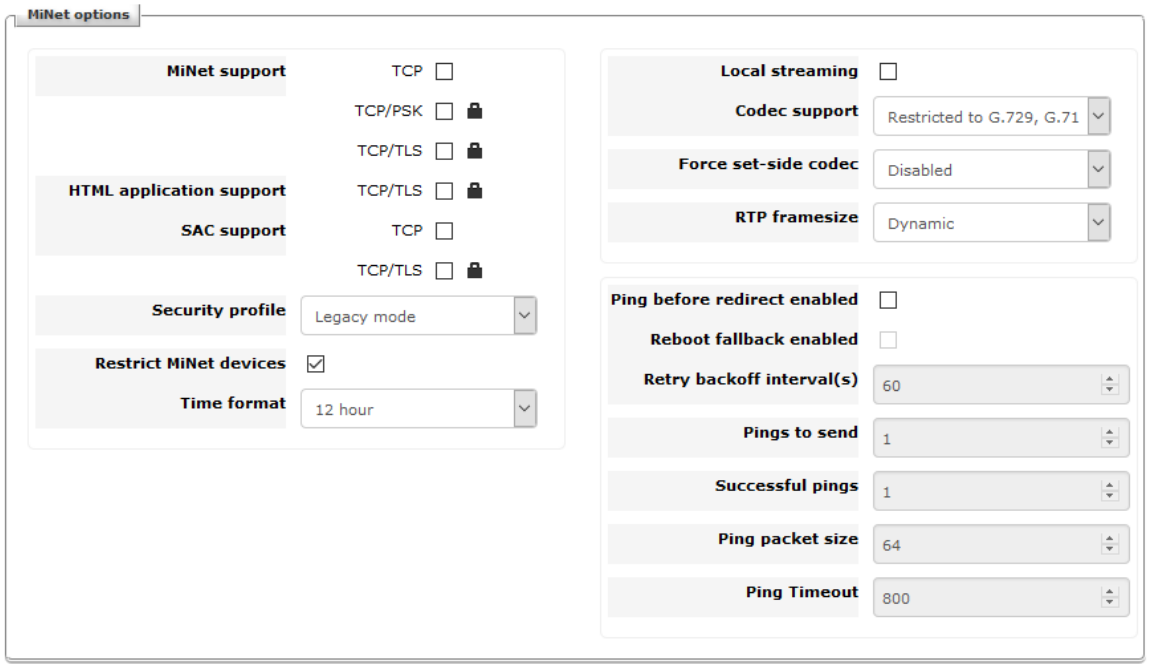


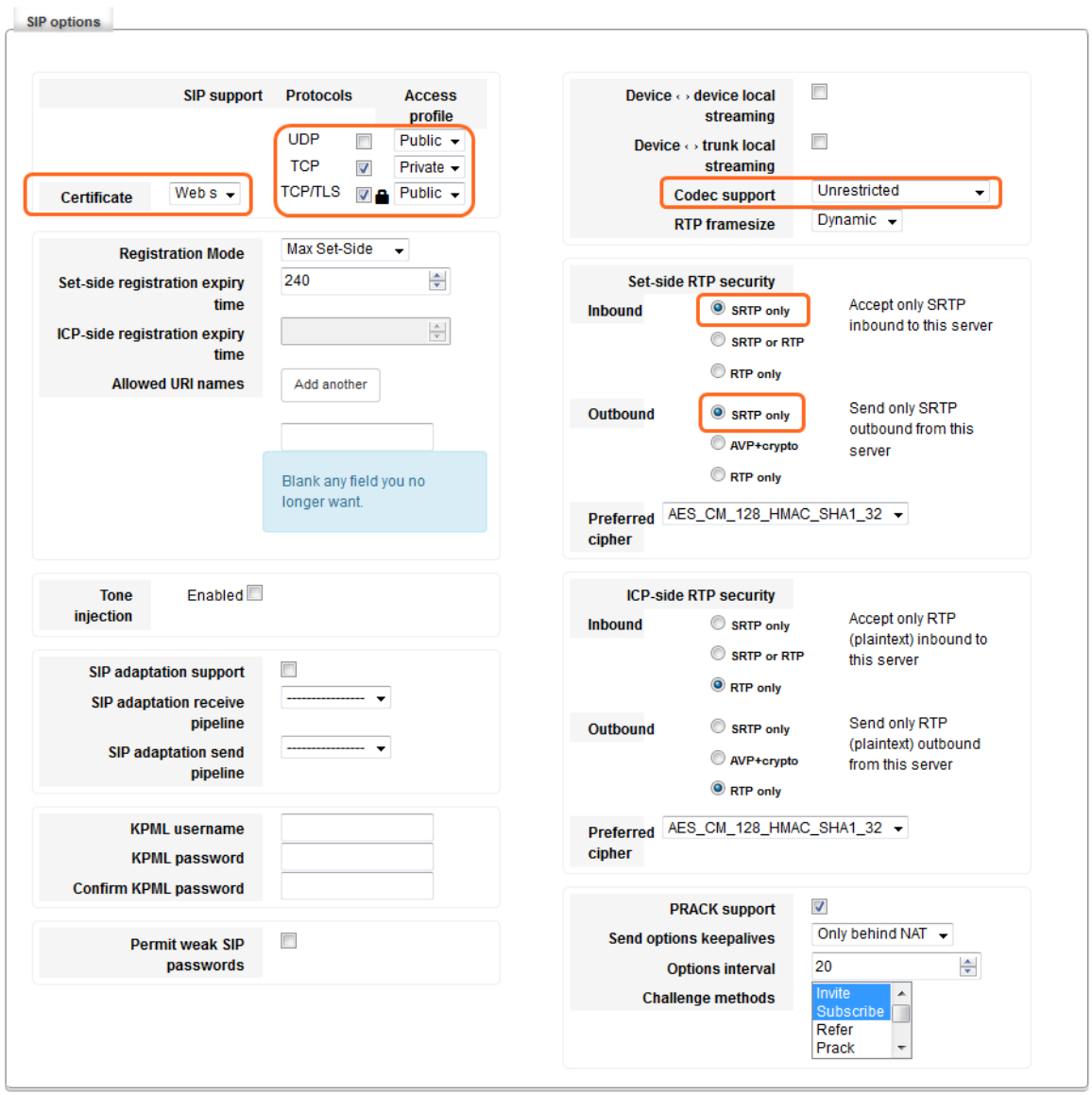
Enter your "ICP-side" and "Set-side" IP address.

ICP-side = internal IP of MBG
Set-side = public IP of MBG

MBG: System configuration: Settings



	SSL cipher: TLS 1.2 DSCP values: You can keep default values or change like shown here to match with the settings of MiVO400.
	Remove all ticks. No MiNet phones will be used.



Configure the SIP options as shown.

SIP support:
TCP with private profile
TCP/TLS with public profile

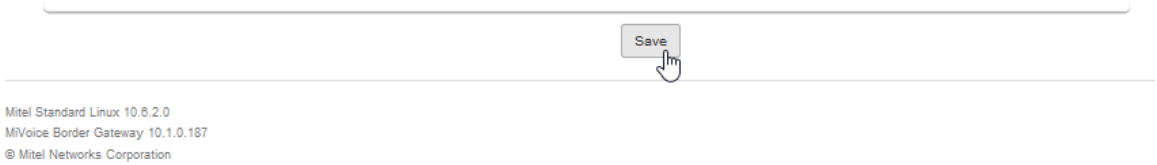
Certificate: **Web server**

Local streaming: does not work with SRTP so keep it unticked

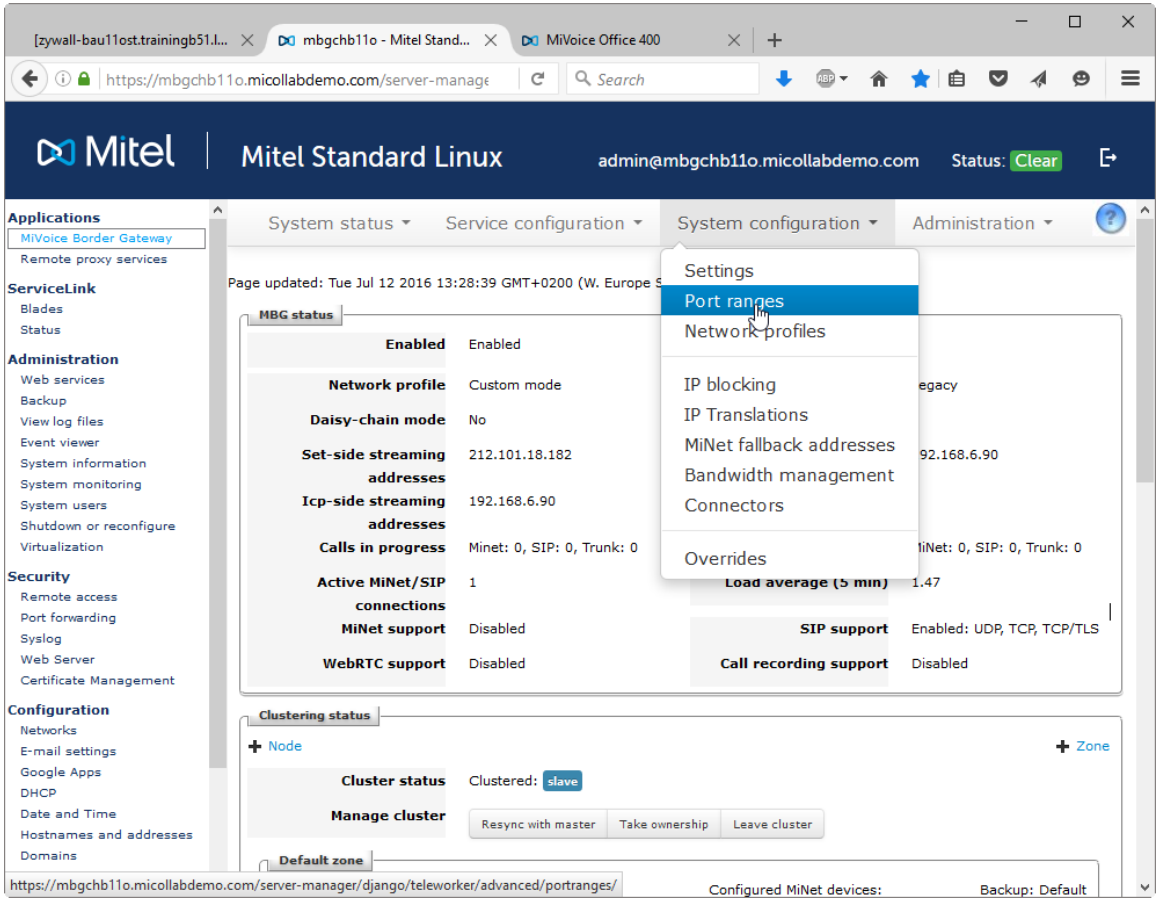
Set-side RTP security:
Inbound: **SRTP only**
Outbound: **SRTP only**

ICP-side RTP security:
Set to match MiVO400 configured capabilities. If no encryption is required in the company LAN keep the default value "RTP only".

All other parameter:
Keep default values

	Don't forget to "Save"

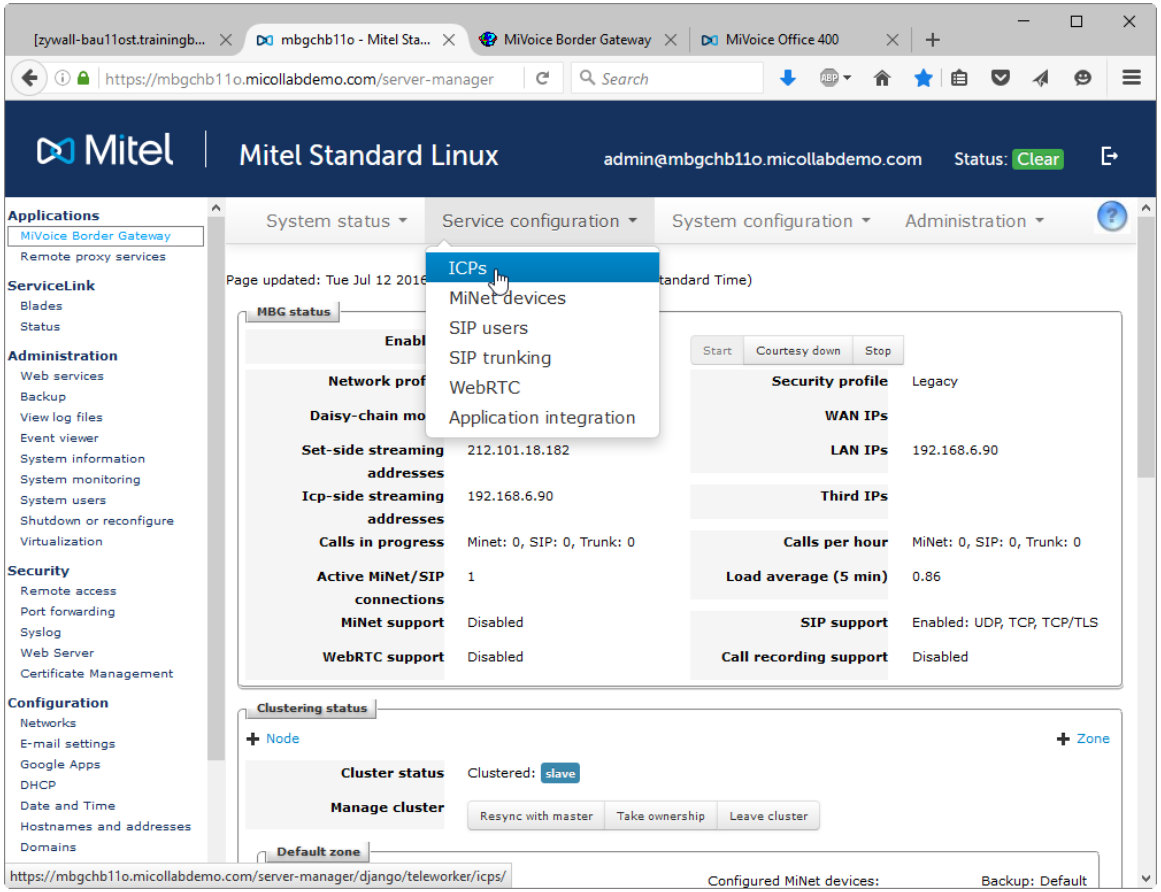
MBG: System configuration: Port ranges

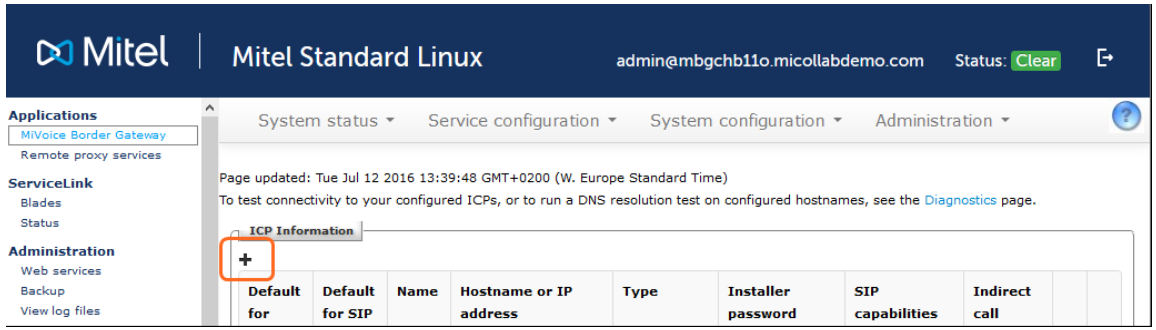


Take care that the port range which is entered here also matches with the corresponding firewall settings.

MiNet and SIP port ranges SRTP starting port: 20000 Video starting port: 21950 SRTP/Video ending port: 21999 **Number of supported calls** 487 pure audio and 12 with video	Note: • At least half of the total number of ports must be allocated to audio. • The Video starting port must be greater than the SRTP starting port and less than or equal to the SRTP/Video ending port. • The SRTP/Video ending port must be less than the WebRTC public starting port.
Save	"Save"

MBG: Service configuration: ICPs





Add a new ICP (PBX)

Name: Enter a name for you call server. The name should match with the name of your MiVO400 system (see next screenshot).

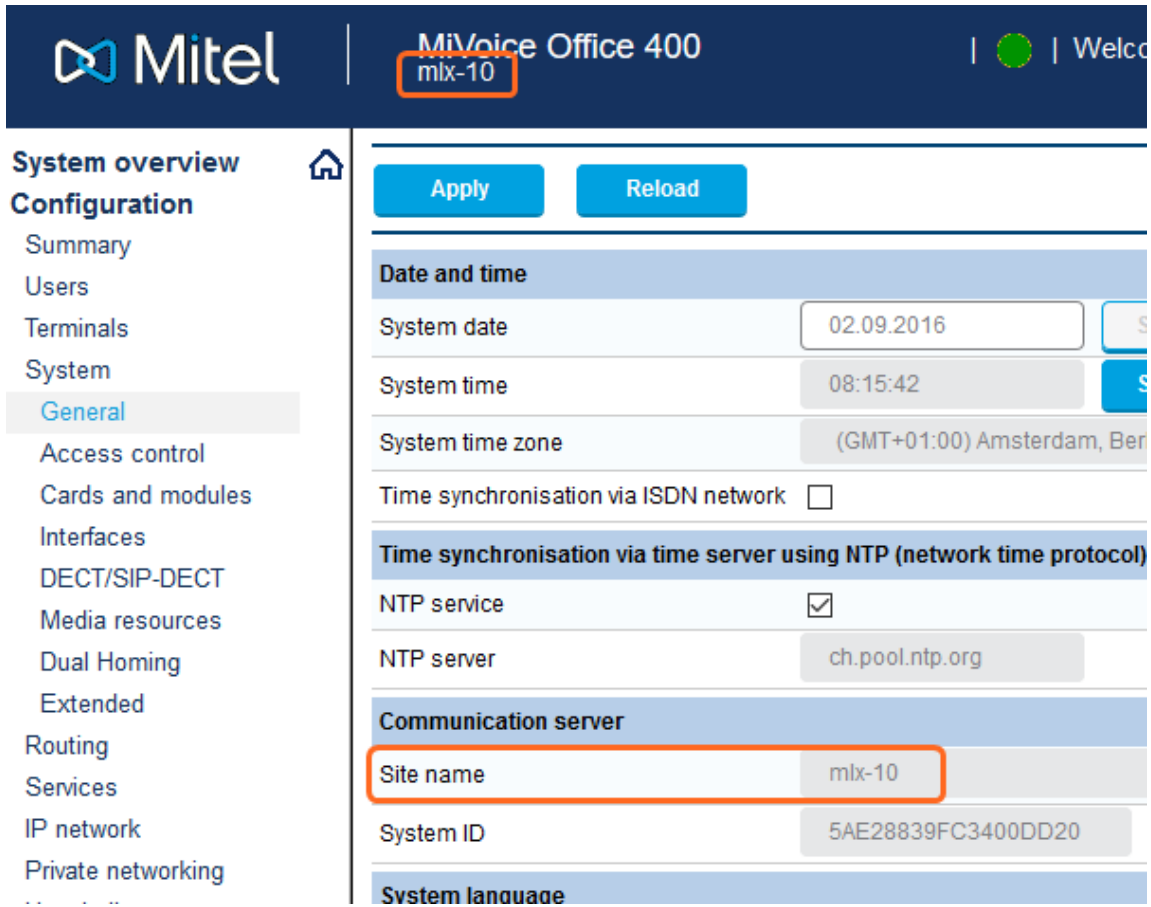
Type: **MiVoice Office 400**

SIP capabilities: **UDP, TCP**
(if the traffic between MBG and PBX is not encrypted).
Otherwise chose "UPD, TCP, TLS"

IP address: **<IP of MiVO400>**

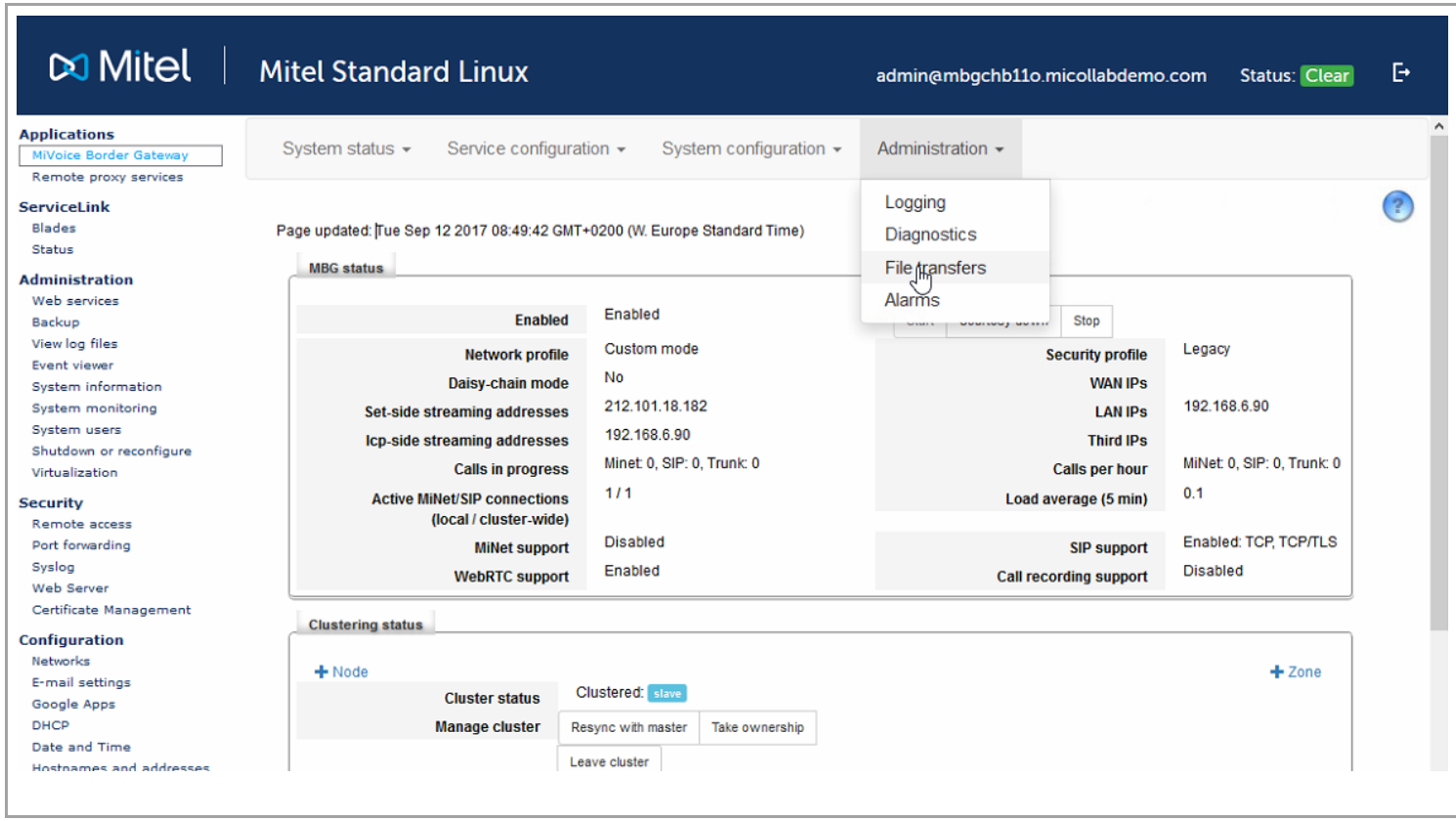
XML settings as shown on the screenshot.

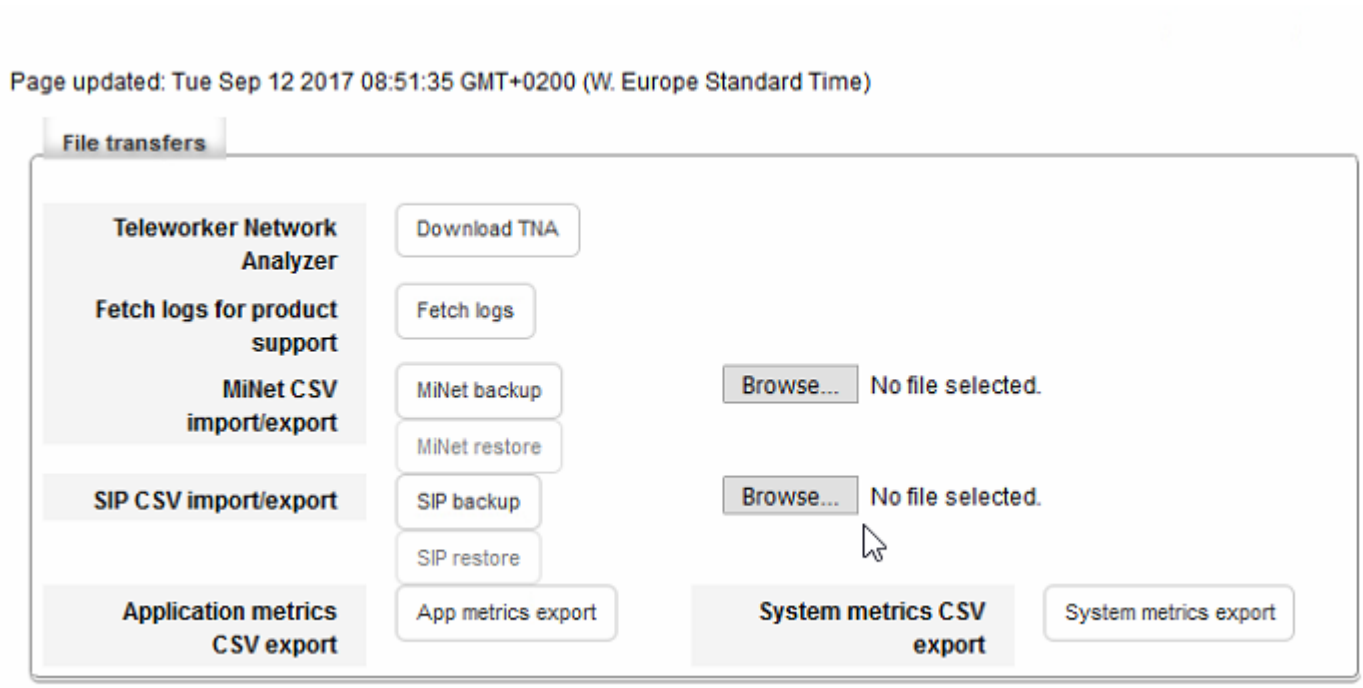
Don't forget to "Save"



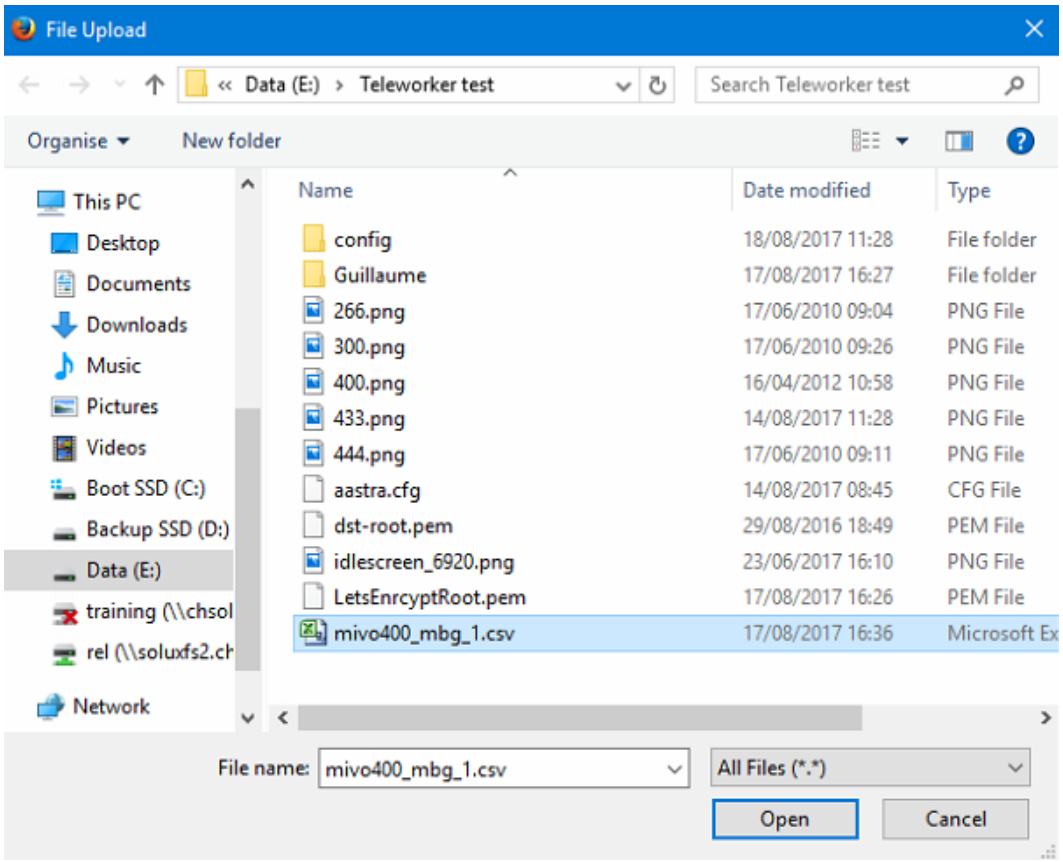
The site name of MiVO400 should be the same as the name given in the ICP configuration of the MBG

MBG: Administration: File transfer

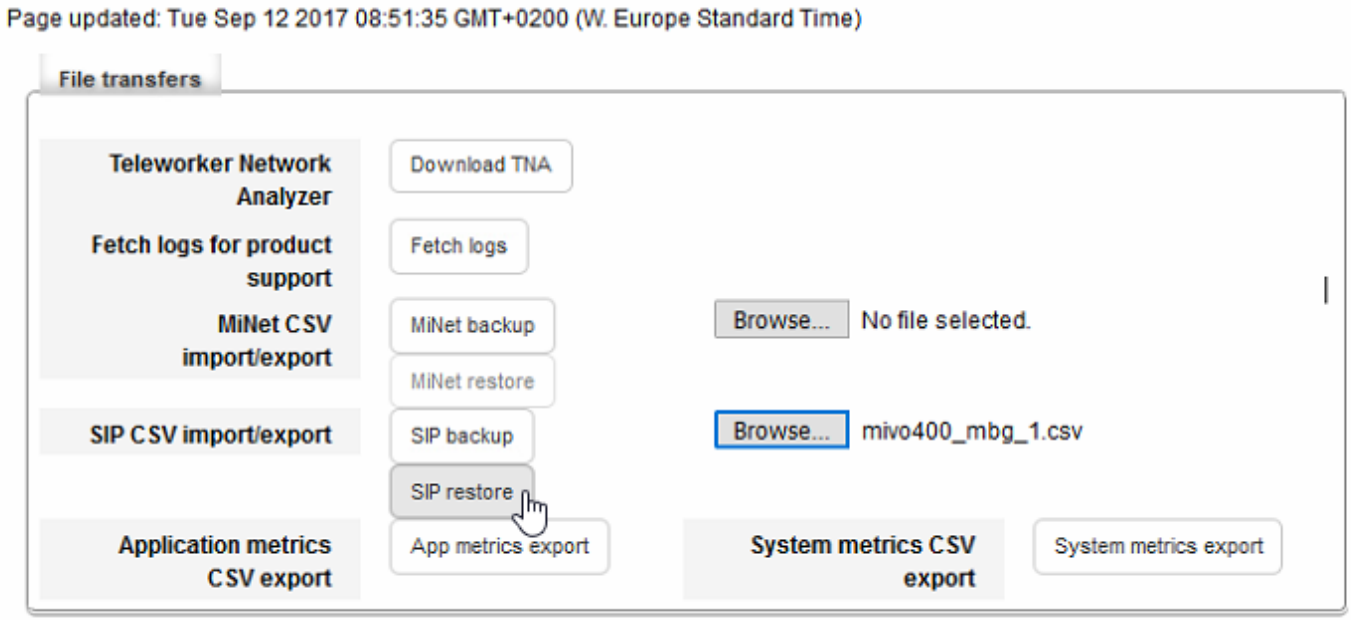


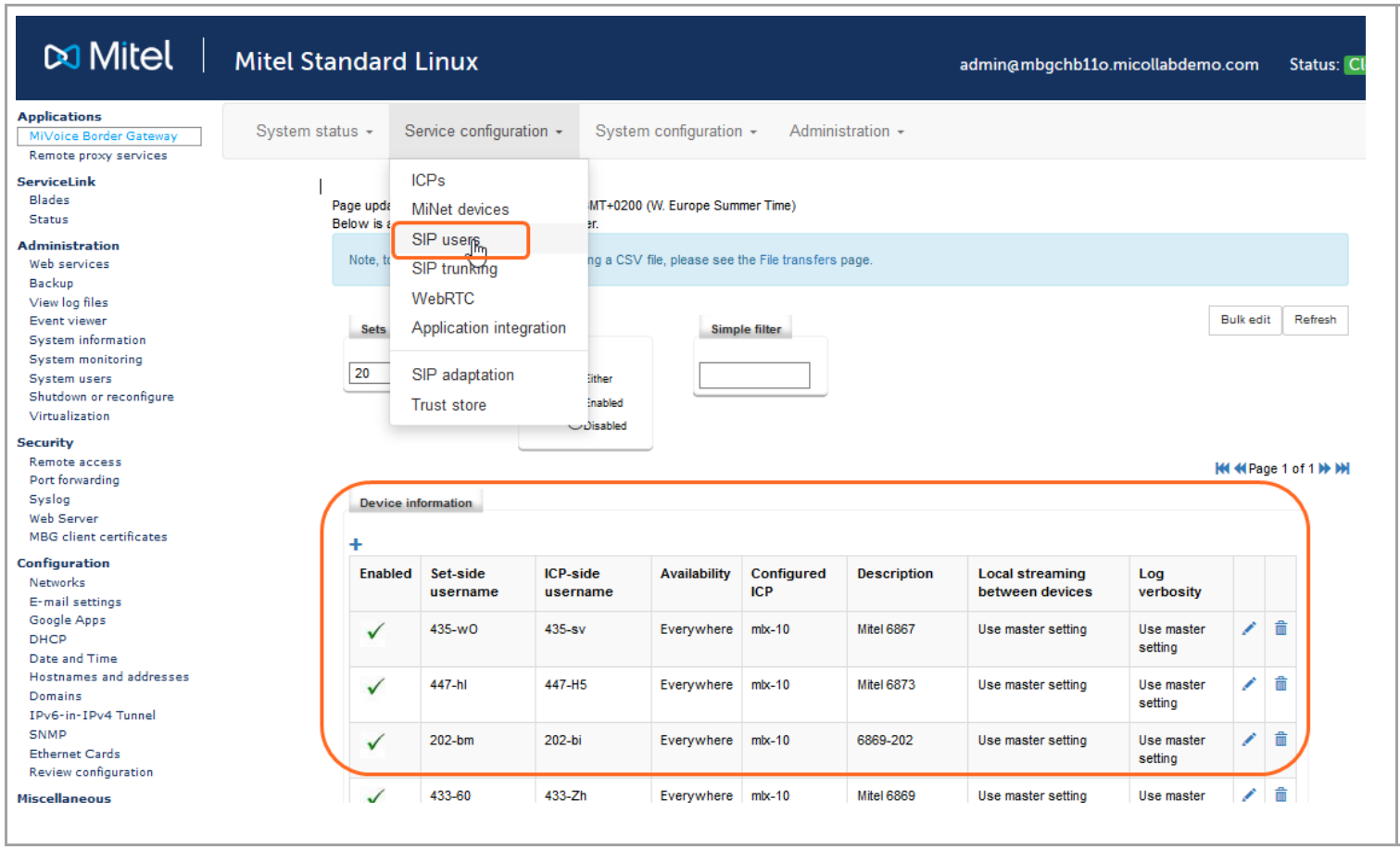


Click "Browse…" for SIP CSV import.



Select the file "mivo400_mbg_1.csv"

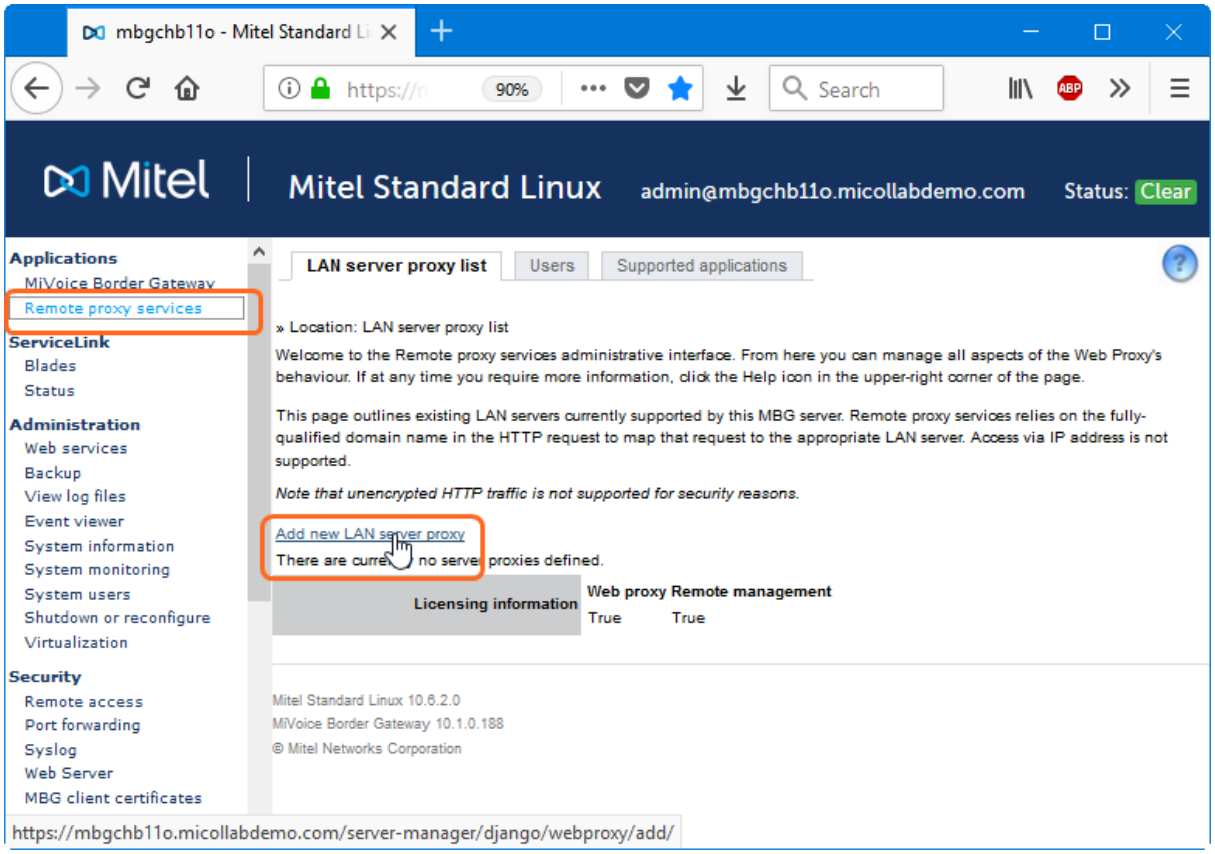
	click "SIP restore"



The imported user can be seen here.

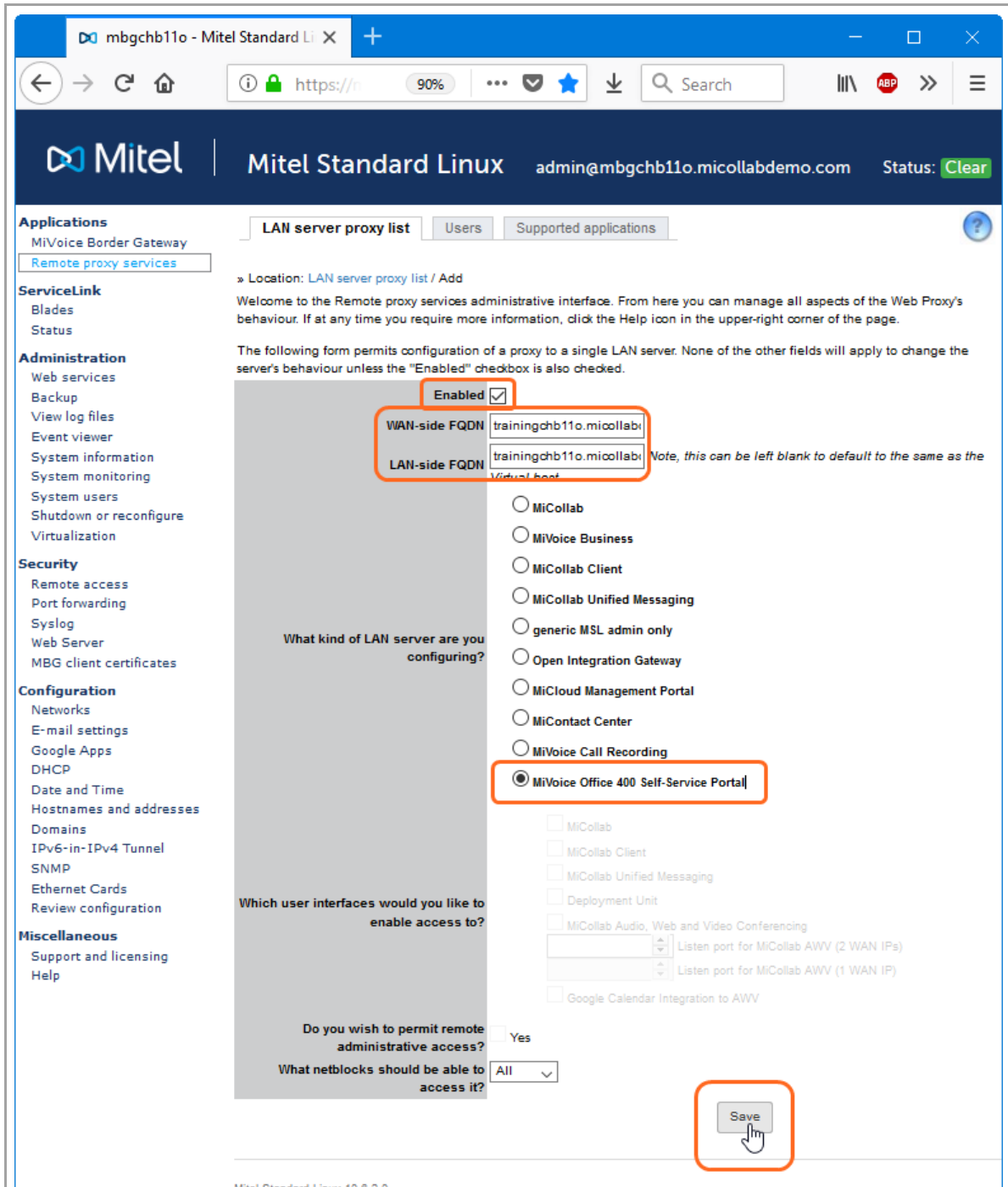
Web proxy for SSP access

To access the MiVO400 SSP from the teleworker side, a web proxy has to be configured on MBG.



Select "Remote proxy services"

Click "Add new LAN server proxy"



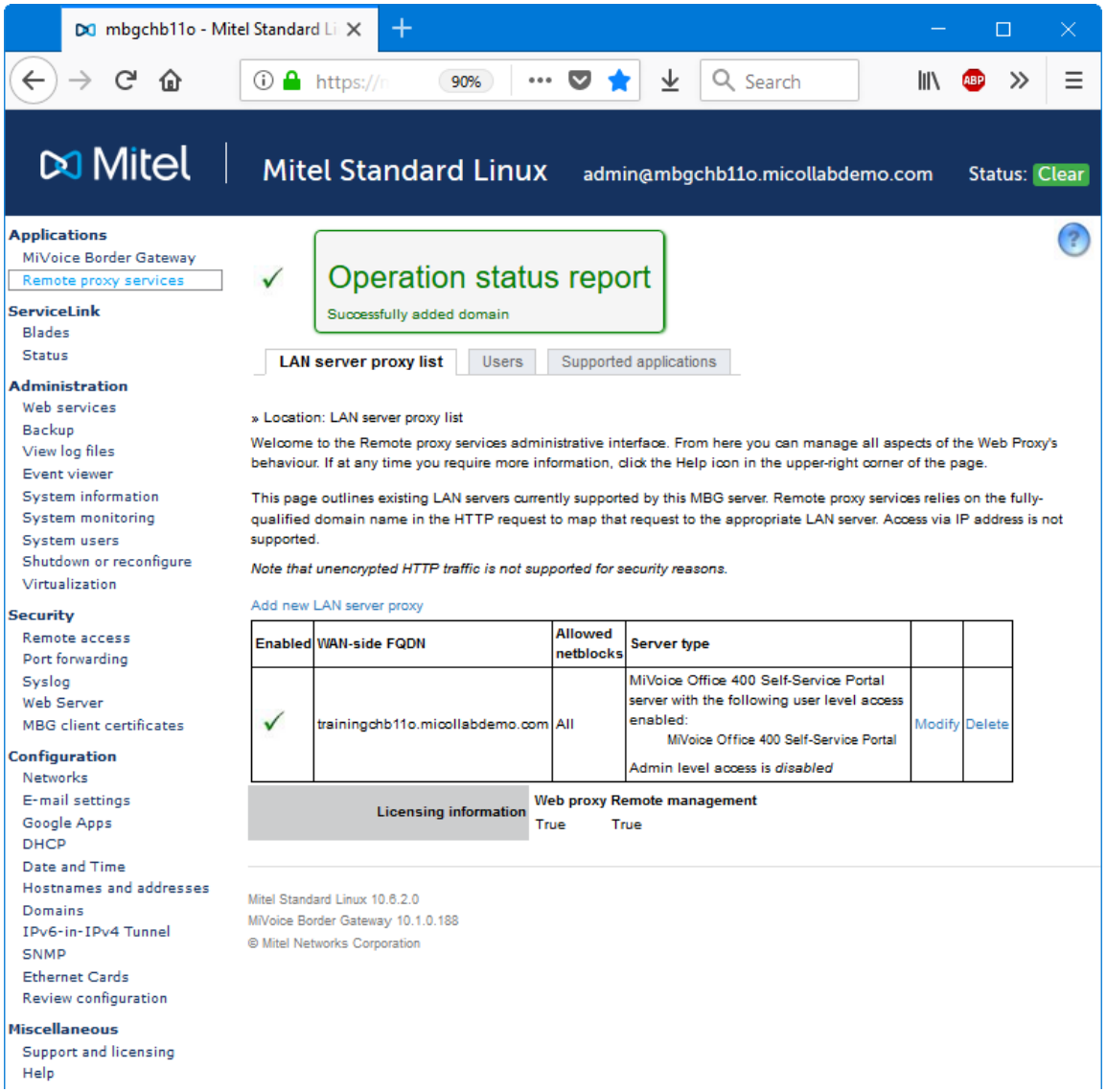
Enable the service

Enter WAN-side FQDN: **<FQDN for SSP>**
Note: This is another FQDN (not the MBG-FQDN).
This SSP-FQDN has to be resolvable:

- externally in the Internet to the public IP address of the MBG and
- internally in the LAN to the IP of MiVO400.

Tick **MiVoice Office 400 Self-Service Portal**

Don't forget to "Save"



The web-proxy is now available.

The self-service portal can be reached via URL:

https: // <FQDN for SSP>

Please note, that on MiVO400 the appropriate permissions has to be set and the login credentials are entered.

Mitel SIP phone: Start-up

The Mitel SIP phone has to be started with "Factory default" settings.

During the Start-up the phone needs to know where its configuration files can be downloaded (a configuration server information has to be set). Several possibilities to provide such an information are available:

- Possibility 1: The DHCP server of the Teleworker-LAN sends an option 66 or vendor specific option 43 with the corresponding config-server information. (This possibility is normally not used on the teleworker side)

- Possibility 2: If the DHCP server does not offer config-server information, the phone contact the RCS to get its corresponding config-server information. An admin has to enter on the RCS the configuration server information and the MAC address of the phone in advance.

- Possibility 3: If the RCS cannot provide the config-server information (i.e. they are not entered there), the configuration server information can be set manually in the terminal's GUI (Web page of the phone) or TUI (Setting menu on the phone)

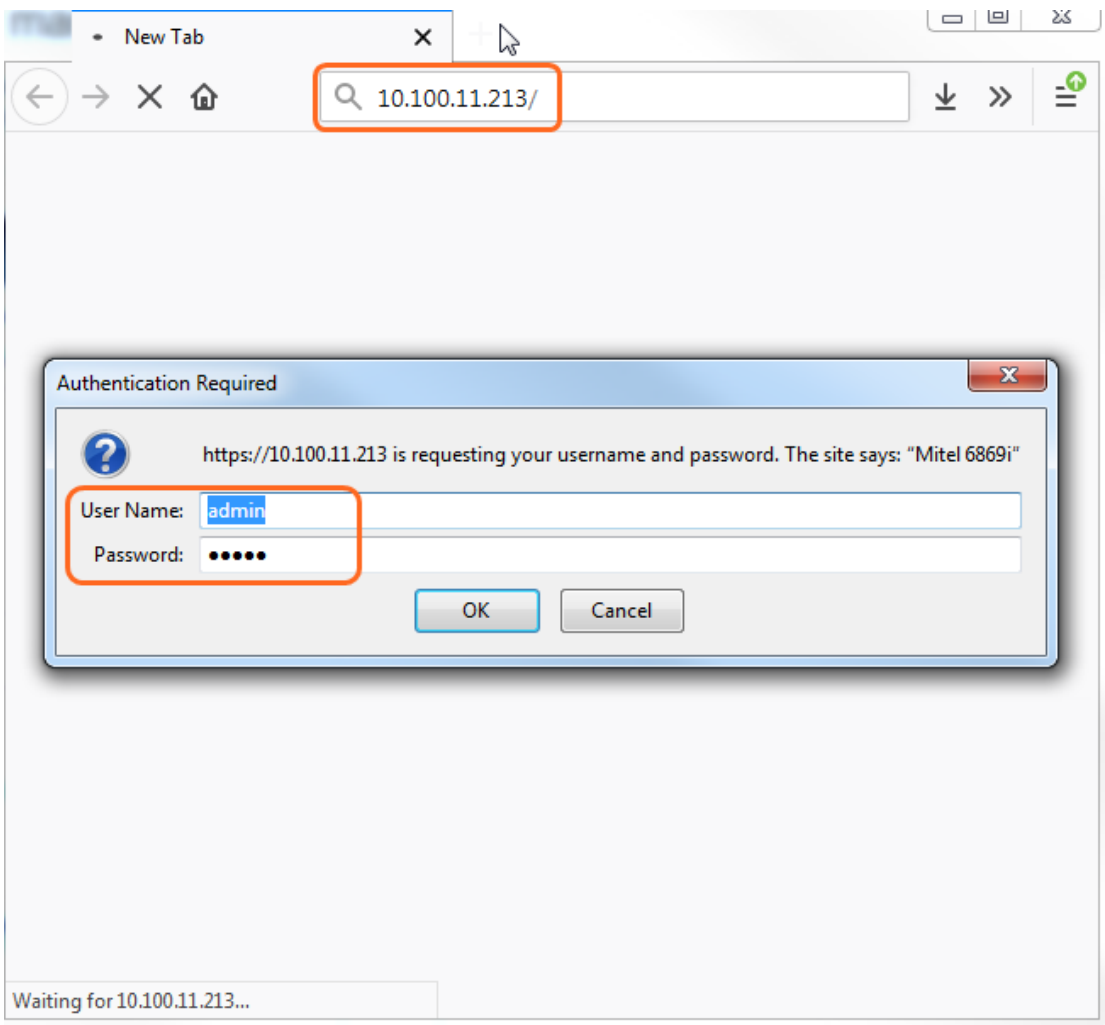
The configuration server address for teleworker always looks like:
http: // <public IP of MBG>/<internal IP of MiVO400> or
http: // <FQDN of MBG>/<internal IP of MiVO400> or
tftp: // <public IP of MBG>/<internal IP of MiVO400> or
tftp: // <FQDN of MBG>/<internal IP of MiVO400>

The Mitel SIP phone downloads new firmware, unless it already has it, and will reboot several times.

Eventually the set displays a key in the lower left on the screen labelled "Log In". Use this key to enter the registration username and registration password (found in that terminal's settings on the A400).

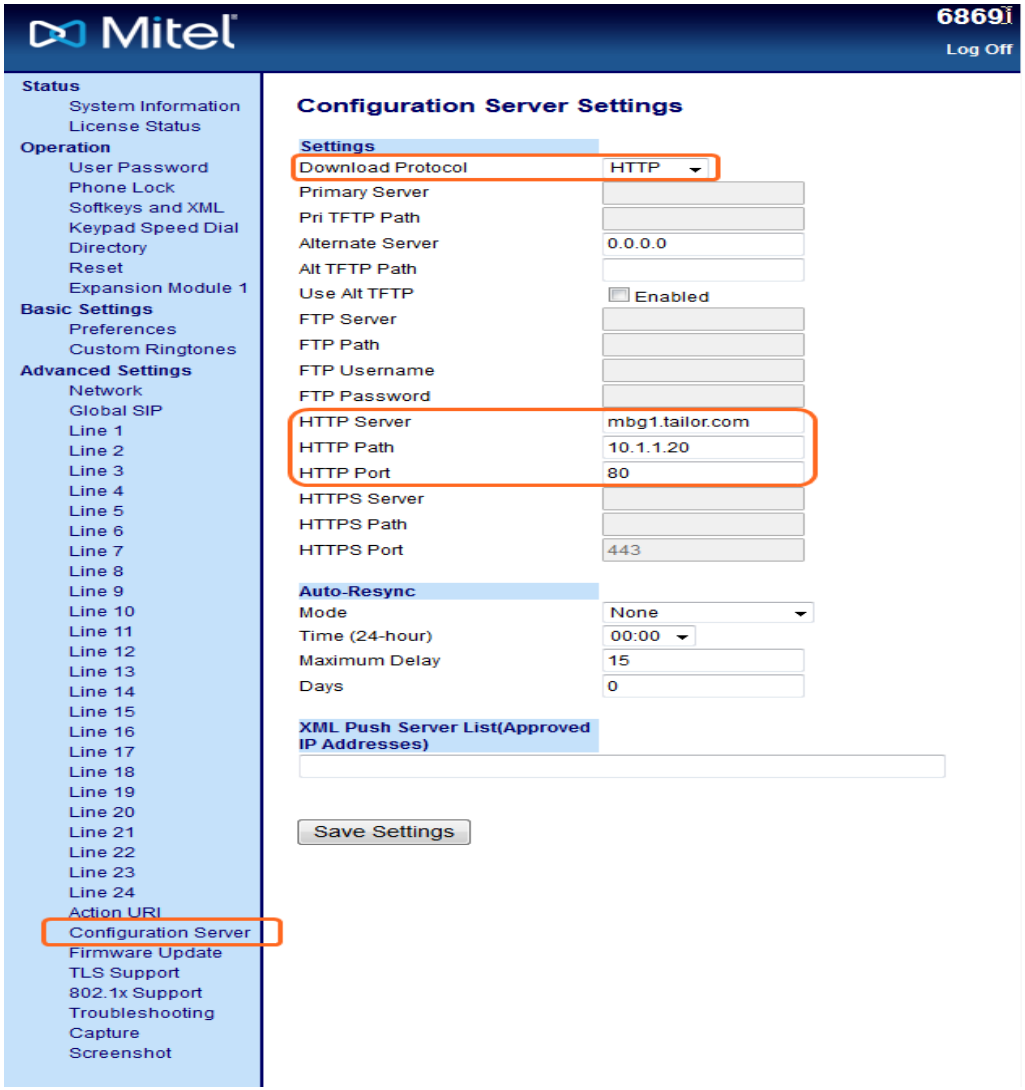
Set config-server in phone GUI

If the configuration server information is not provided during DHCP or from RCS, it can be entered manually in the phone.



Open a browser and enter the IP address of the Mitel SIP phone.

Login with
user name: admin
password: 22222



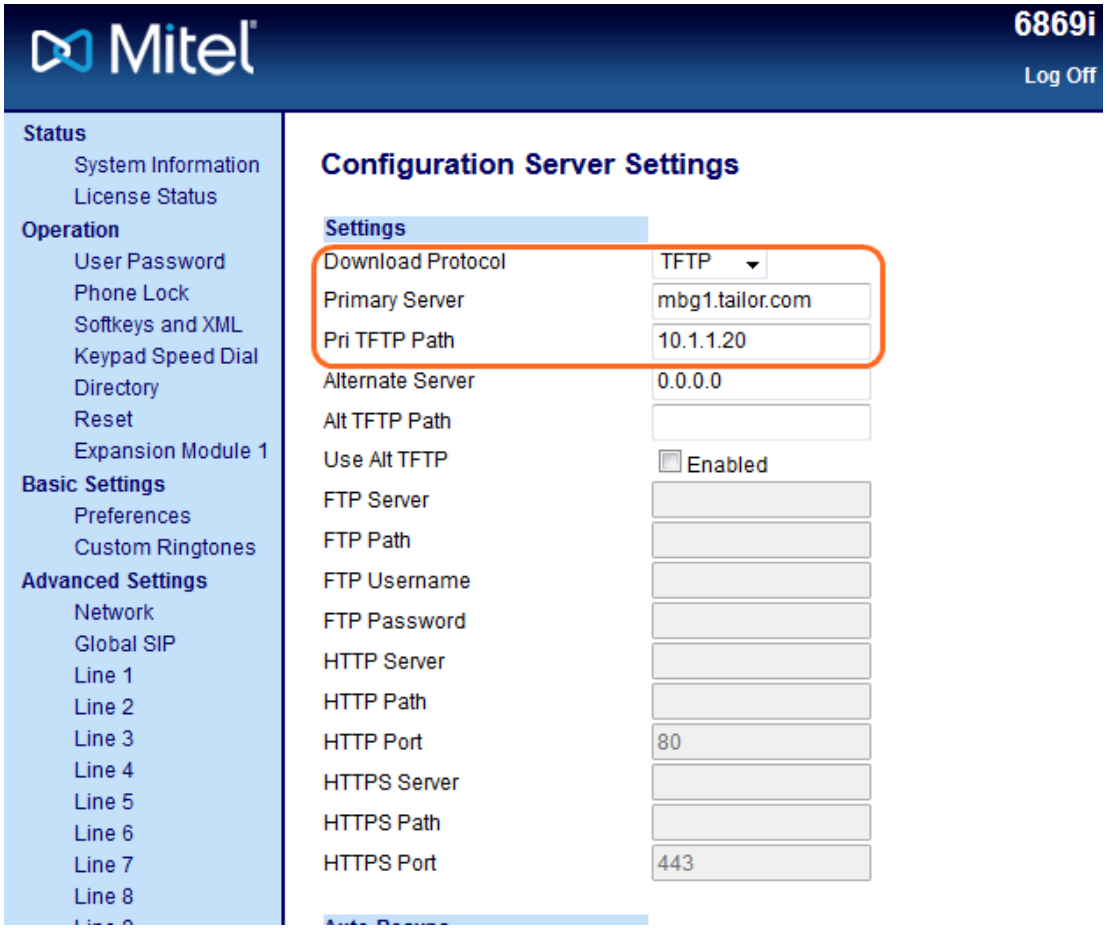
Go to "Configuration Server"

Select Download protocol: **HTTP**

Enter HTTP Server:
<FQDN of MBG>
(here e.g.: mbg1.tailor.com)

Enter HTTP Path:
<internal IP of MiVO400>
(here e.g.: 10.1.1.20)

Save settings and reboot the phone.



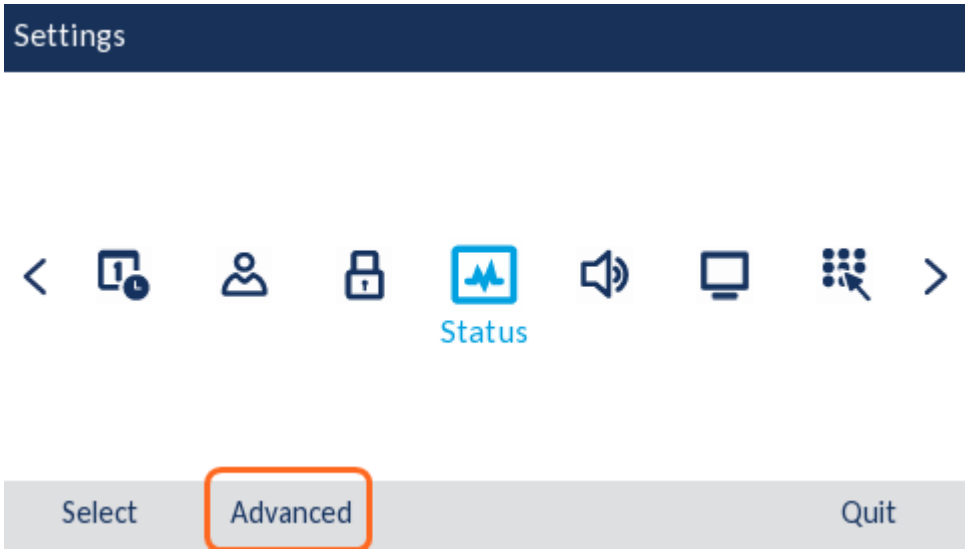
Alternatively (if http access is not available) the configuration server can be reached via TFTP with the settings shown here.

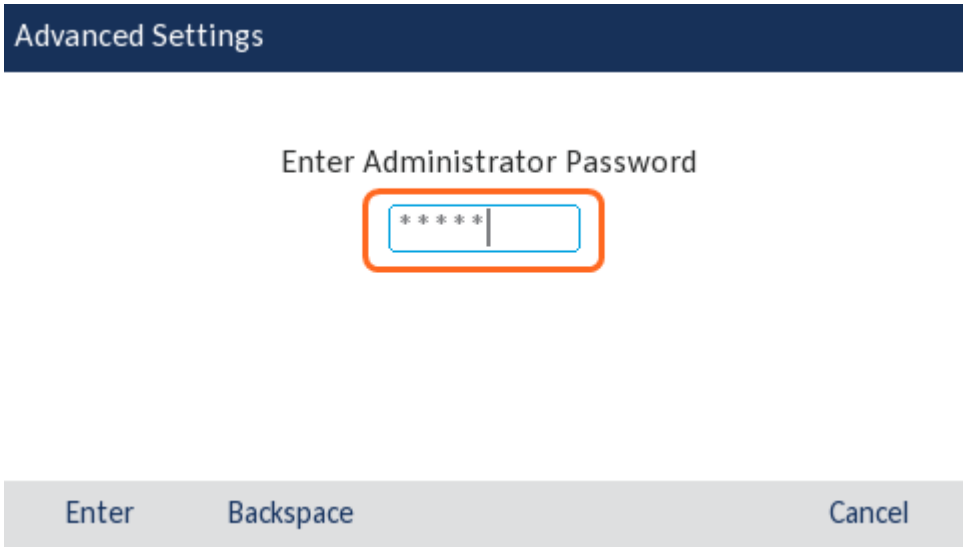
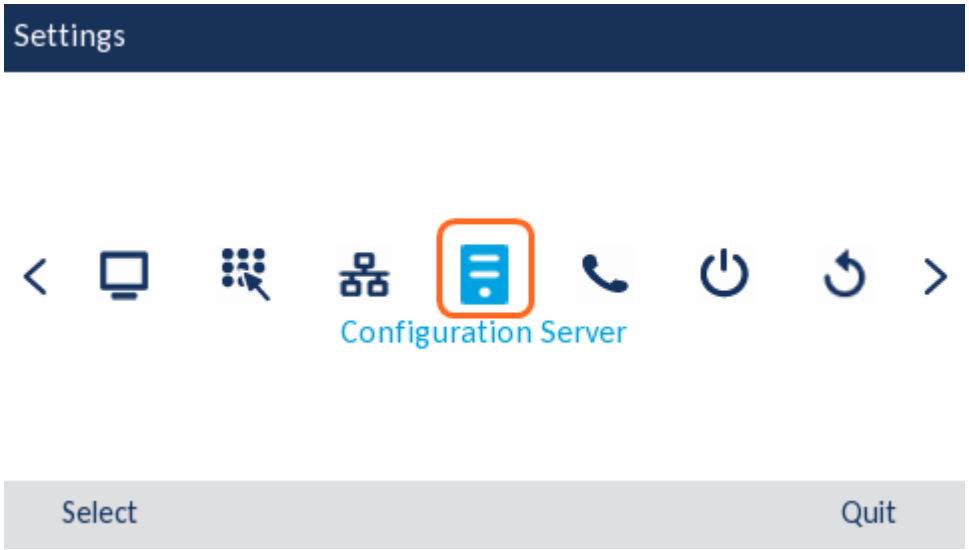
Select Download protocol: **TFTP**

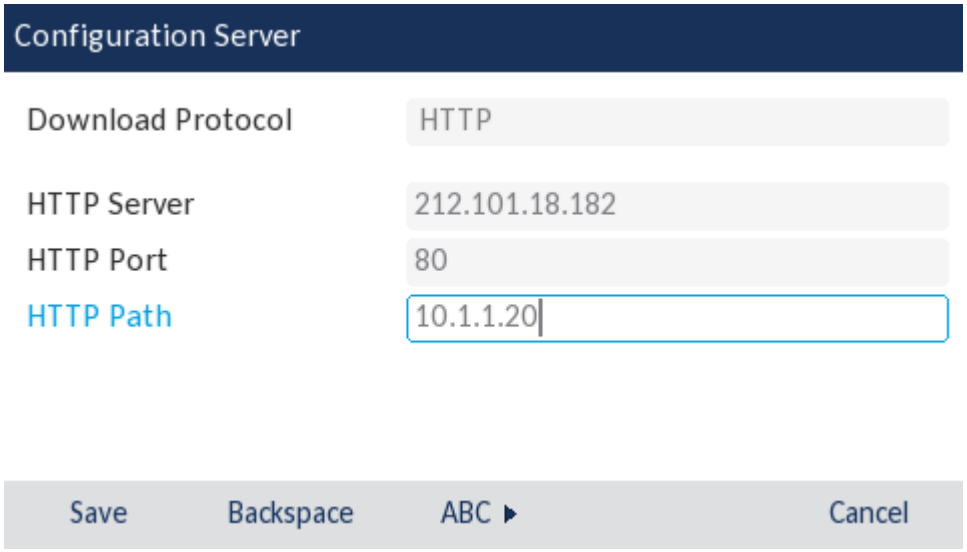
Enter Primary Server:
<FQDN of MBG>
(here e.g.: mbg1.tailor.com)

Enter Pri TFTP Path:
<internal IP of MiVO400>
(here e.g.: 10.1.1.20)

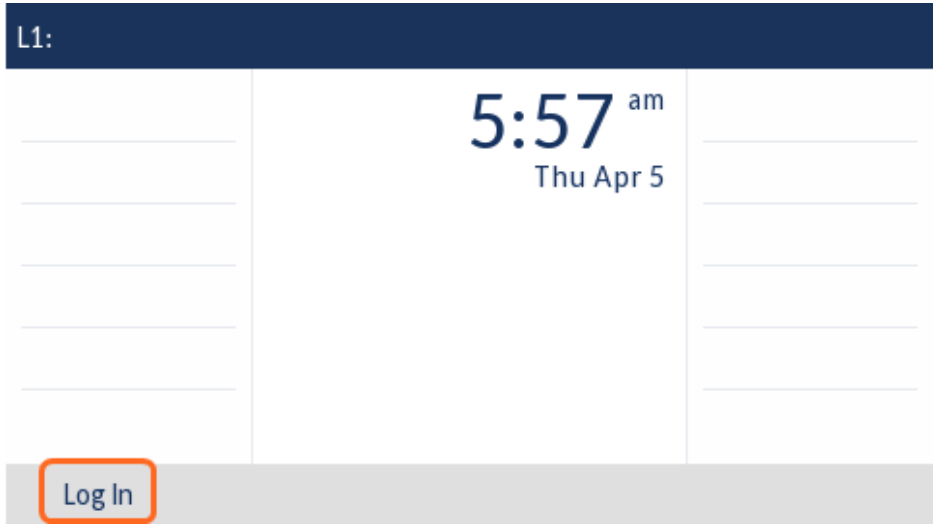
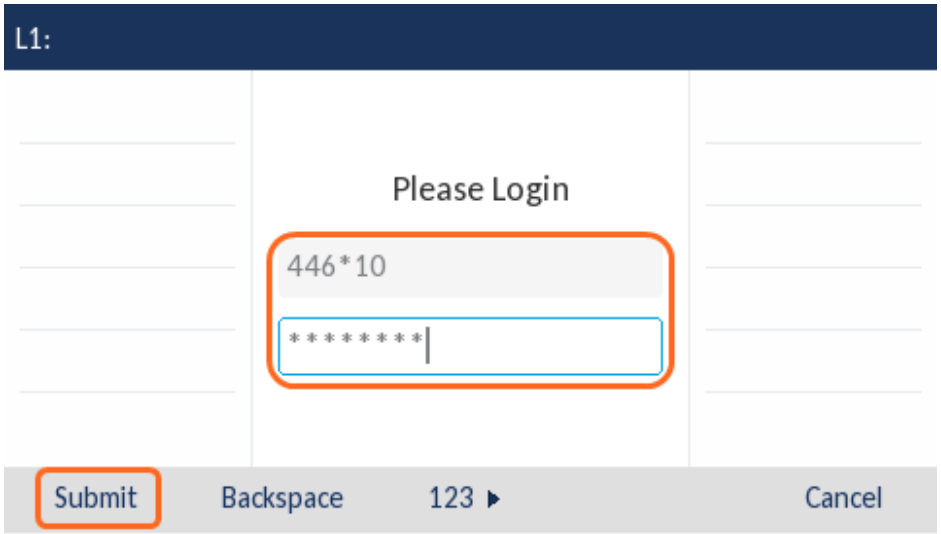
Set config-server in the TUI

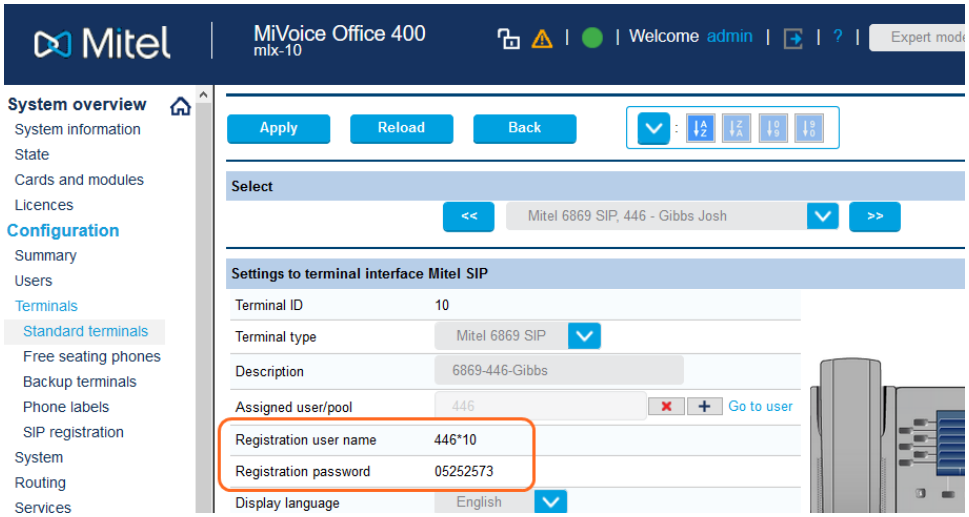
	Click on "Gear" key
	Select "Advanced"

	Enter password: **22222**
	Selected Configuration Server

	Set Download Protocol: **HTTP** HTTP Server: **<public IP of MBG>** HTTP Path: **<internal IP of MiVO400>** Save and reboot the phone

Login screen

	After some reboots the phone eventually come up with this login screen.
	The user has to enter the • Registration user name • Registration password



Registration user name and Registration password are visible here. They are only available if no MAC address is entered for this terminal in MiVO400.

They can be send via email to the user.

Maintenance

Test your installation:

- Test external access to MBG's public IP using the Teleworker Analyzer Tool (download windows executable from MBG's Administration - File Transfer).
- Contact IT if required external ports are reported as CLOSED.
- Test internal access to MiVo400 from Diagnostics - Connectivity test. Contact IT if required internal ports are reported as CLOSED.
- Under MSL server-manager, navigate to Administration - Event Viewer and check the event logs to make sure the configuration proceeded with no errors.

Powering connections

© Copyright 2018, Mitel Networks Corporation. All Rights Reserved.
The Mitel word and logo are trademarks of Mitel Networks Corporation.
Any reference to third party trademarks are for reference only and Mitel makes no representation of the ownership of these marks.