

# 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](mailto: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

<b>Overview .....</b>	<b>4</b>
Introduction.....	4
Abbreviations.....	4
Preconditions.....	5
<b>AMC licenses.....</b>	<b>9</b>
Create ARID for MBG .....	10
<b>Customer Data.....</b>	<b>18</b>
<b>Prepare MiVoice Office 400 .....</b>	<b>21</b>
<b>MiVoice Border Gateway Installation / Configuration .....</b>	<b>30</b>
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
<b>Mitel SIP phone: Start-up.....</b>	<b>112</b>
Set config-server in phone GUI.....	113
Set config-server in the TUI .....	116
Login screen.....	119
<b>Maintenance .....</b>	<b>121</b>

# 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

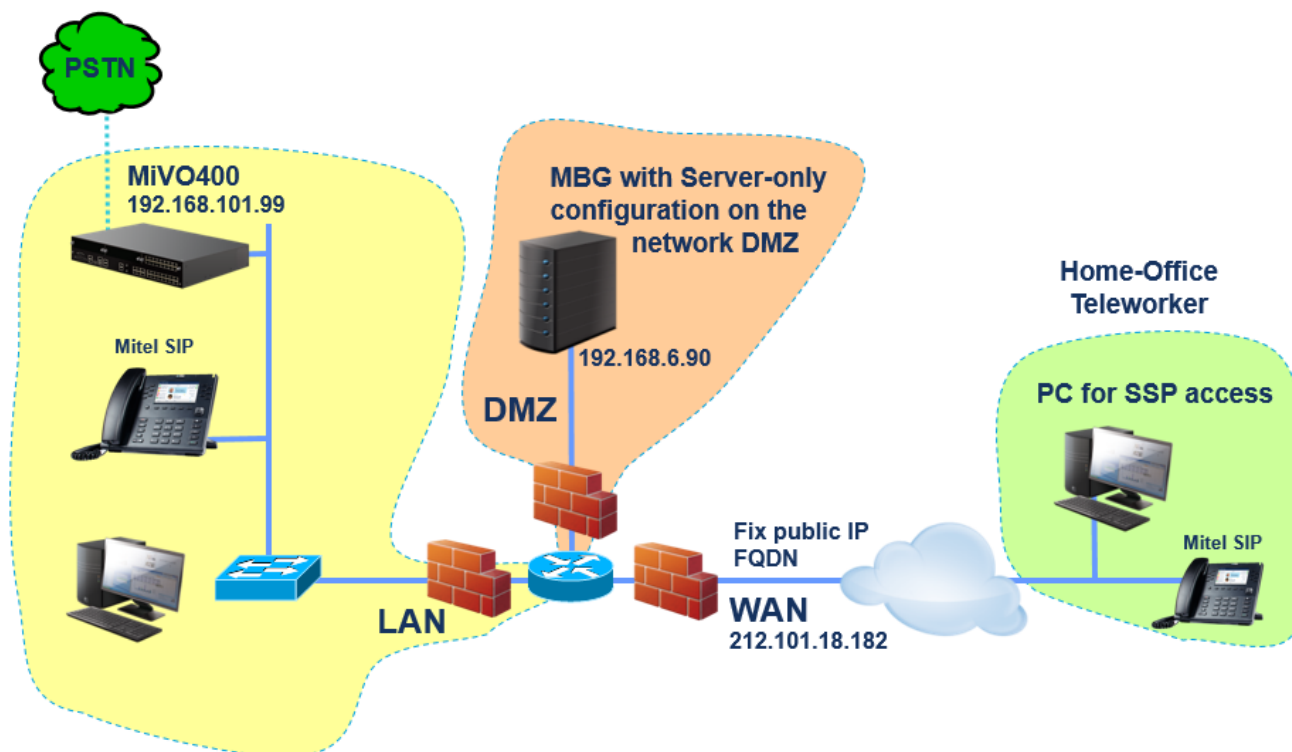
Abb.	Description
AMC	Applications Management Center (License server for MBG,...)
ARID	Application Record ID
CSR	Certificate Signing Request
GUI	Graphical user interface
ICP	IP Communication Platform (e.g. MiVoice Office 400)
MBG	MiVoice Border Gateway
RCS	Redirect and Configuration Server
SSP	MiVO400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

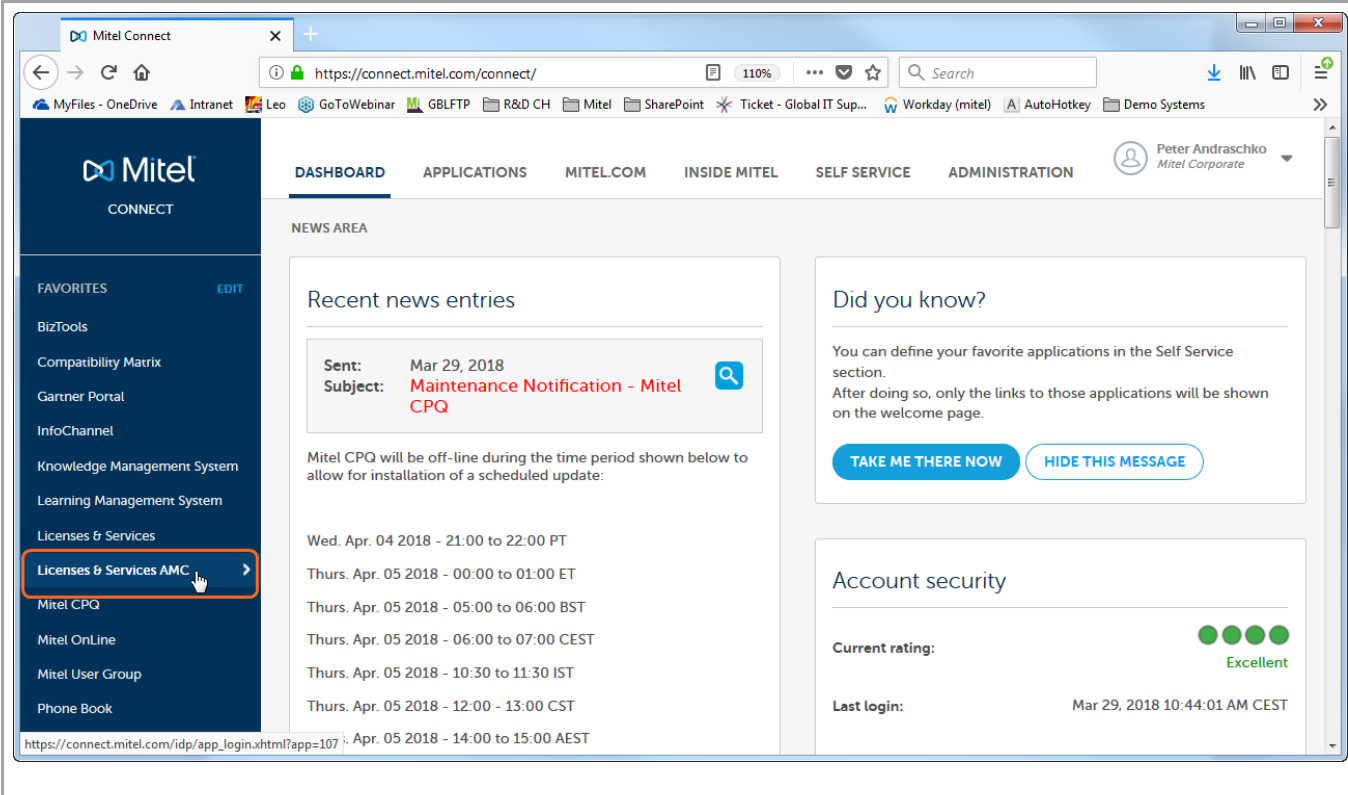
### MiVoice Border Gateway Products

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"

 <b>Licenses &amp; Services AMC</b>	
<div>Home   <b>Products &amp; Customers</b>   License Bank   Reports   Self Service   Administration</div> <div>Partner Accounts   <u>End Customers</u></div>	
<div>Create Customer</div> <div><b>Help</b> If you would like more information about Mitel's innovative solutions for small, medium and enterprise businesses, please follow this link <a href="http://www.mitel.com">http://www.mitel.com</a>. If you are experiencing problems with Licenses &amp; Services AMC please click the link below: <a href="#">Help</a> <a href="#">Contact</a> <a href="#">Update schedule</a></div>	<div><b>Select "Customer"</b></div> <div>and "Search" for your customer</div> <div>or</div> <div>create a new customer</div>
<div><b>Search Criteria</b></div> <div><b>Customer Criteria :</b> Customer name : <input type="text" value="Trainingchb110"/> Identification : <input type="text"/></div> <div><b>Application Record Criteria :</b> Identification : <input type="text"/> Description : <input type="text"/> Product Category : <input type="text" value="Select"/> Hardware ID : <input type="text"/> Status : <input type="text" value="All Records"/></div> <div><input type="button" value="Search"/> <input type="button" value="Clear"/></div>	

<div><h3>Search Results</h3><table><thead><tr><th></th><th>Customer ID</th><th>Customer Name</th><th>Application Records</th></tr></thead><tbody><tr><td>  </td><td>Unknown</td><td>Trainingchb11o</td><td>3</td></tr></tbody></table><div>   Page 1 / 1  </div></div>		Customer ID	Customer Name	Application Records	  	Unknown	Trainingchb11o	3	Click "Create App Record"
	Customer ID	Customer Name	Application Records						
  	Unknown	Trainingchb11o	3						
<div><h3>Create Application Record (TEST: Mitel Internal)</h3><h4>Application Record Details</h4><p><i>The application record description field is used to help identify an application at a given customers site. It allows the use of a more descriptive unique value in describing each installation instead of having to remember each application record ID.</i></p><p>Solution Provider : TEST: Mitel Internal</p><p>End Customer : Trainingchb11o</p><p>Application Record Description : <input type="text" value="MBG-9_b11o"/></p><p>Assign Product <input checked="" type="checkbox"/></p><p></p></div>	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 : *MBG-9\_b11o*

Description :

Assign : *Product or License after Commit*

Commit >>



## Assign - License Bank (TEST: Mitel Internal)

Successfully created new application record identifier 62822816.

PO # :

Sales Order # :

Part No :

Product Category :  ▼





Order Date From :

Order Date To :

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.

### Search Results

	PO	Sales Reference	Order Date	Available Products
 		Peter Andraschko	2016-Oct-06	171
 		Peter Andraschko	2016-Nov-14	6

Page 1 / 1

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

Available Licenses

Part NO	Description	Destination customer	Available	Assign
54005339	MiVoice Border Gateway Virtual		1	<input type="text" value="1"/>
54004572	MBG Teleworker Service User x1		5	<input type="text" value="5"/>

Assign >>

For the MBG server the ARID needs this licenses assigned.

Assign - Confirmation

Assign > partner Accounts ( TEST: Mitel Internal ) > License Bank > Confirmation

**Step Three :** Please confirm the products which are about to be assigned to application record 62822816(MBG-9\_b11o):

Customer: Trainingchb11o

Customer PO:

Application Type: Mitel Generic Application

Active Products:

From: TEST: Mitel Internal

Part NO	Description	Dest Customer	Available	Assign
54005339	MiVoice Border Gateway Virtual		1	1
54004572	MBG Teleworker Service User x1		5	5

Confirm >>

Cancel X

"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
<b>Transaction Audit Trail</b>		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.



<div><h3>Assign - Apply Point of Sale SWA Licenses ( TEST: Mitel Internal )</h3><p>Details for application record 62822816 (MBG-9_b11o)</p><p>Application Record Id : 62822816</p><p>Reseller : TEST: Mitel Internal</p><p>Customer : Trainingchb11o</p><p>Description : MBG-9_b11o</p><p>Purchased Support Level* : STANDARD - 8x5 SWA coverage ▼</p><p>Purchased years of SWA coverage* : 1 ▼</p><p><a href="#">Submit &gt;&gt;</a></p></div>	<p>Please note: Premium SWA is not supported for MBG together with MiVO 400. Hit "Submit"</p>
<p>Now the ARID for MBG is ready!</p>	

## Customer Data

Please use this data sheet for your customer project to collect and save 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

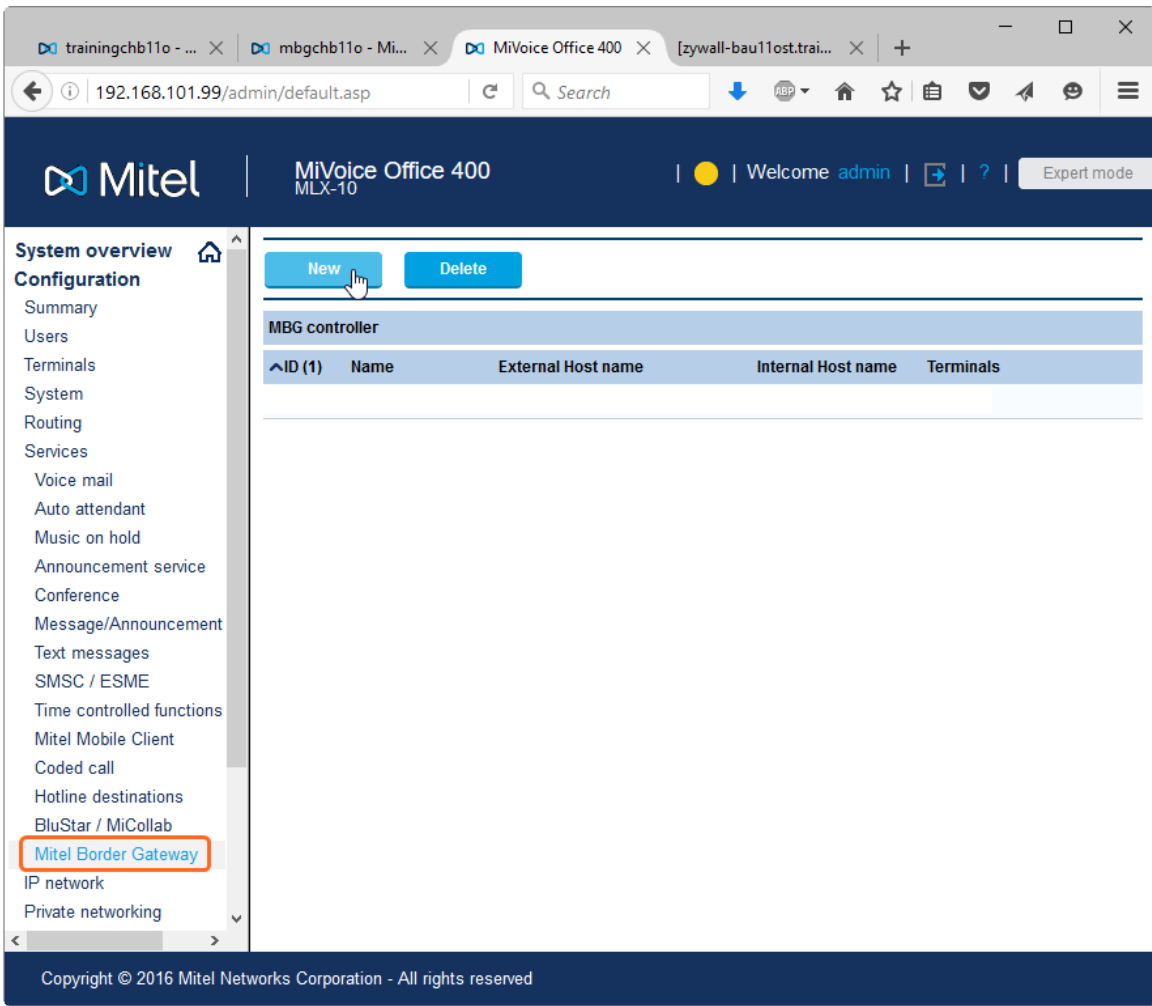
System type	vMiVO400		
EID:	49065AE28839FC3400DD20C753521E807ECF		
Sales channel:	CH-Freemarket		
Host name:	mlx-10		
Domain	micollabdemo.com		
IP address:	192.168.101.99		
DNS	192.168.1.5		
User name:	admin	password:	your password



ARIDs		remarks
MBG	12707414	
System size	users	
<input checked="" type="checkbox"/>	150	Small business (1 vCPUs / 1 GB RAM / 20 GB HDD)
<input type="checkbox"/>	500	Enterprise (3 vCPUs / 2 GB RAM / 40 GB HDD)
Host name (FQDN)	mbgchb11o.micollabdemo.com	
Certificate authority:		
<input type="checkbox"/>	self-signed certificate	
<input checked="" type="checkbox"/>	Let's Encrypt certificate authority	
<input type="checkbox"/>	Common Name:	mbgchb11o.micollabdemo.com
<input type="checkbox"/>	Alternate Name(s):	trainingchb11o.micollabdemo.com
<input type="checkbox"/>	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.



trainingchb11o - ... × mbgchb11o - Mi... × MiVoice Office 400 × [zywall-bau11ost.trai... × +

192.168.101.99/admin/default.asp Search

Mitel MiVoice Office 400 MLX-10 | Welcome admin | Expert mode

**System overview** Configuration Summary Users Terminals System Routing Services Voice mail Auto attendant Music on hold Announcement service Conference Message/Announcement Text messages SMSC / ESME Time controlled functions Mitel Mobile Client Coded call Hotline destinations BluStar / MiCollab **Mitel Border Gateway** IP network Private networking

New Delete

**MBG controller**

^ID (1)	Name	External Host name	Internal Host name	Terminals
---------	------	--------------------	--------------------	-----------

Copyright © 2016 Mitel Networks Corporation - All rights reserved

Add a new MBG

The screenshot shows the Mitel MiVoice Office 400 MLX-10 configuration interface. The left sidebar contains a 'System overview' menu with options like Summary, Users, Terminals, System, Routing, and Services. The 'Services' section is expanded, showing 'Voice mail', 'Auto attendant', 'Music on hold', 'Announcement service', 'Conference', 'Message/Announcement groups', 'Text messages', 'SMSC / ESME', 'Time controlled functions', 'Mitel Mobile Client', 'Coded call', 'Hotline destinations', 'BluStar / MiCollab', 'Mitel Border Gateway' (highlighted), 'Mitel CloudLink Gateway', and 'IP network'. The main content area displays the 'MBG controller' configuration for ID 1. Fields for 'External host name', 'Internal host name', 'Name', and 'XML listen port' are highlighted with orange boxes. Below these fields is a table with columns 'ID (0)', 'Interface', 'Terminal type', 'Description', 'Call number', and 'User name', which is currently empty.

**System overview**  
**Configuration**  
 Summary  
 Users  
 Terminals  
 System  
 Routing  
 Services  
 Voice mail  
 Auto attendant  
 Music on hold  
 Announcement service  
 Conference  
 Message/Announcement groups  
 Text messages  
 SMSC / ESME  
 Time controlled functions  
 Mitel Mobile Client  
 Coded call  
 Hotline destinations  
 BluStar / MiCollab  
 Mitel Border Gateway  
 Mitel CloudLink Gateway  
 IP network

**MBG controller**  
 ID 1  
 External host name mbgchb11o.micollab.com  
 Internal host name 192.168.6.90  
 Name mbgchb11o  
 XML listen port 4430

ID (0)	Interface	Terminal type	Description	Call number	User name
Empty list					

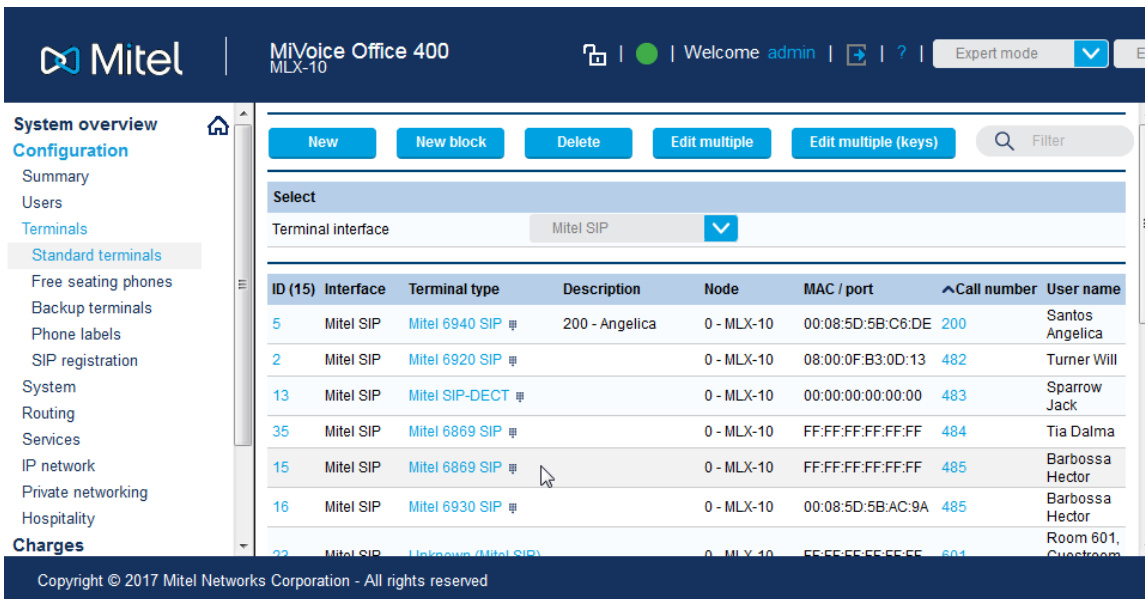
Copyright © 2017 Mitel Networks Corporation - All rights reserved

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)



**Mitel** | MiVoice Office 400 MLX-10 | Welcome admin | Expert mode

**System overview**

- Configuration
  - Summary
  - Users
  - Terminals
    - Standard terminals**
    - Free seating phones
    - Backup terminals
    - Phone labels
    - SIP registration
  - System
  - Routing
  - Services
  - IP network
  - Private networking
  - Hospitality
- Charges

**Select**

Terminal interface: Mitel SIP

ID (15)	Interface	Terminal type	Description	Node	MAC / port	Call number	User name
5	Mitel SIP	Mitel 6940 SIP	200 - Angelica	0 - MLX-10	00:08:5D:5B:C6:DE	200	Santos Angelica
2	Mitel SIP	Mitel 6920 SIP		0 - MLX-10	08:00:0F:B3:0D:13	482	Turner Will
13	Mitel SIP	Mitel SIP-DECT		0 - MLX-10	00:00:00:00:00:00	483	Sparrow Jack
35	Mitel SIP	Mitel 6869 SIP		0 - MLX-10	FF:FF:FF:FF:FF:FF	484	Tia Dalma
15	Mitel SIP	Mitel 6869 SIP		0 - MLX-10	FF:FF:FF:FF:FF:FF	485	Barbossa Hector
16	Mitel SIP	Mitel 6930 SIP		0 - MLX-10	00:08:5D:5B:AC:9A	485	Barbossa Hector
22	Mitel SIP	Unknown (Mitel SIP)		0 - MLX-10	FF:FF:FF:FF:FF:FF	601	Room 601, Cuckoo

Copyright © 2017 Mitel Networks Corporation - All rights reserved

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

**Mitel** | MiVoice Office 400 MLX-10 | Welcome admin | Expert mode

**System overview**  
**Configuration**  
 Summary  
 Users  
 Terminals  
 Standard terminals  
 Free seating phones  
 Backup terminals  
 Phone labels  
 SIP registration  
 System  
 Routing  
 Services  
 IP network  
 Private networking  
 Hospitality  
 Charges  
 Phone book  
 Maintenance  
 Setup wizard

**Select**  
 Mitel 6869 SIP, 485 - Barbossa Hector

**Connection settings**  
 State: Not registered  
 IP address: -  
 RTP Port: 3000  
 MAC address: FF:FF:FF:FF:FF:FF  
 MBG controller: 1 - mbgchb110  
 SIP user name: 485-QS  
 SIP password: 86bVK7AI3Uympj6aSpzx  
 MBG SIP user name:  
 MBG SIP password:  
 Transport protocol: TCP  
 Terminal is behind NAT:  
 Enable keep alive:  
 Relay RTP data via:

Copyright © 2017 Mitel Networks Corporation - All rights reserved

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 screenshot shows the Mitel MiVoice Office 400 configuration interface. The left sidebar contains navigation links: System overview, Configuration (Summary, Users, Terminals), Standard terminals, Free seating phones, Backup terminals, Phone labels, SIP registration, System, Routing, Services, IP network, Private networking, Hospitality, Charges, Phone book, Maintenance, and Setup wizard. The main content area displays the configuration for a specific terminal, 'Mitel 6869 SIP, 485 - Barbossa Hector'. The 'Connection settings' section is expanded, showing fields for State (Not registered), IP address, RTP Port (3000), MAC address (FF:FF:FF:FF:FF:FF), MBG controller (1 - mbgchb11o), SIP user name (485-QS), SIP password (86bVK7AI3Uympj6aSpzx), MBG SIP user name (485-ck), MBG SIP password (rVTgM0wKeG1fclWbDHlh), Transport protocol (TCP), Terminal is behind NAT, Enable keep alive, and Relay RTP data via communication server (indirect switching). The 'Transport protocol' dropdown is highlighted with a red box. At the bottom, there is a copyright notice: Copyright © 2017 Mitel Networks Corporation - All rights reserved.

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.

**Mitel** | MiVoice Office 400 MLX-10 | Welcome admin | Expert mode

**System overview**

- Configuration
  - Summary
  - Users
  - Terminals
  - System
  - Routing
  - Services
    - Voice mail
    - Auto attendant
    - Music on hold
    - Announcement service
    - Conference
    - Message/Announcement group
    - Text messages
    - SMSC / ESME
    - Time controlled functions
    - Mitel Mobile Client
    - Coded call
    - Hotline destinations
    - BluStar / MiCollab
    - Mitel Border Gateway
    - Mitel CloudLink Gateway
    - IP network
    - Private networking

**MBG controller**

ID 1

External host name mbgchb11o.micollabc

Internal host name 192.168.6.90

Name mbgchb11o

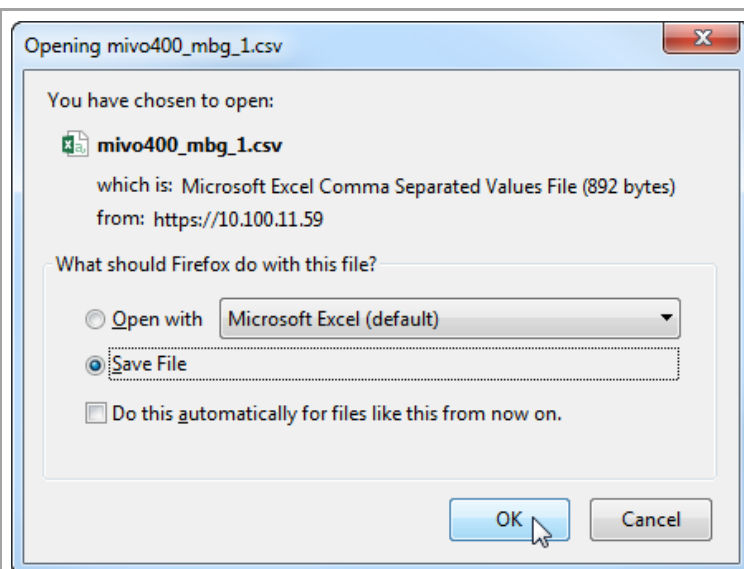
XML listen port 4430

ID (1)	Interface	Terminal type	Description	Call number	User name
15	Mitel SIP	Mitel 6869 SIP		485	Barbossa Hector

Copyright © 2017 Mitel Networks Corporation - All rights reserved

Go back to "Services -> MiVoice Border Gateway"

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



Save the file.

Mitel | MiVoice Office 400 MLX-10 | Welcome admin | Expert mode | EN | Search

System overview | Configuration | Summary | Users | Terminals | Standard terminals | Free seating phones | Backup terminals | Phone labels | SIP registration | System | Routing

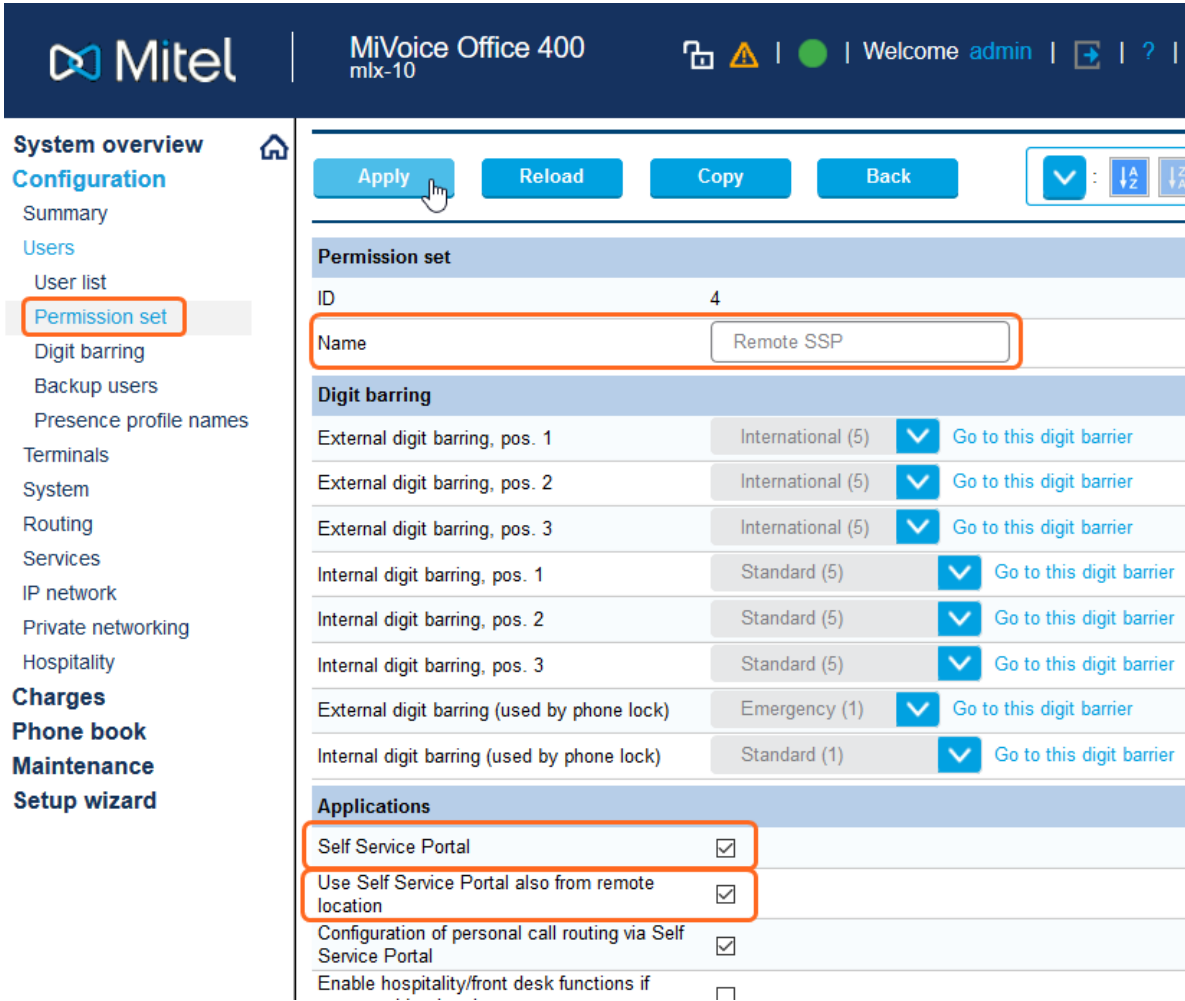
Filter | Filter | Print | Re-register phones

User (10)	Terminal type	Description	Registration user name	Registration password	E-mail address	Select all registration e-mails
Tia Dalma (484)	Mitel 6869 SIP	484*35	23773815	tia.dalma@trainingch.local	<input type="checkbox"/>	Send registration e-mail
Barbosa Hector (485)	Mitel 6869 SIP	485*15	11726772	hector.barbosa@trainingch.local	<input type="checkbox"/>	Send registration e-mail
Room 601, Guestroom 601 (601)	Unknown (Mitel SIP)	601*23	81987203			
Room 602, Guestroom 602 (602)	Unknown (Mitel SIP)	602*24	01991504			
Room 603, Guestroom 603 (603)	Mitel 6869 SIP	603*25	49001740			
Room 604, Guestroom 604 (604)	Mitel 6869 SIP	604*26	10557513			
Room 605, Room 605 (605)	Mitel 6865 SIP	605*17	78339220			

Copyright © 2017 Mitel Networks Corporation - All rights reserved

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:



The screenshot shows the Mitel MiVoice Office 400 web interface. The left sidebar contains a 'System overview' menu with options like Summary, Users, User list, Permission set (highlighted), Digit barring, Backup users, Presence profile names, Terminals, System, Routing, Services, IP network, Private networking, Hospitality, Charges, Phone book, Maintenance, and Setup wizard. The main content area shows the 'Permission set' configuration for ID 4. The 'Name' field is 'Remote SSP'. The 'Digit barring' section lists various barring options with dropdown menus and 'Go to this digit barrier' links. The 'Applications' section at the bottom has four checkboxes: 'Self Service Portal' (checked), 'Use Self Service Portal also from remote location' (checked and highlighted with an orange box), 'Configuration of personal call routing via Self Service Portal' (checked), and 'Enable hospitality/front desk functions if' (unchecked).

Create a permission set which authorizes:

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

"Apply" the settings

**Mitel** MiVoice Office 400  
mlx-10 | Welcome admin

**System overview**  
Configuration  
Summary  
Users  
**User list**  
Permission set  
Digit barring  
Backup users  
Presence profile names  
Terminals  
System  
Routing  
Services  
IP network  
Private networking  
Hospitality  
Charges  
Phone book  
Maintenance  
Setup wizard

**Apply** **Reload** **Back** **Expand all sections**

**Select**  
Sparrow Jack (400)

**User**  
Call number: 400  
Name: Sparrow Jack  
PIN:   
Confirm PIN:   
Windows user name: jsparrow  
Use PIN instead of password: ☐  
Password: ..... Password confirmation: .....  
E-mail address: 02.trainingchb11o@gmail.com  
User language: English

**Settings**  
Licence / Role: User 0 - None  
Go to MiCollab server ...  
Permission set: Remote SSP (4) Go to permission set  
Authorization profile: ---  
Route: 1 Go to route

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"

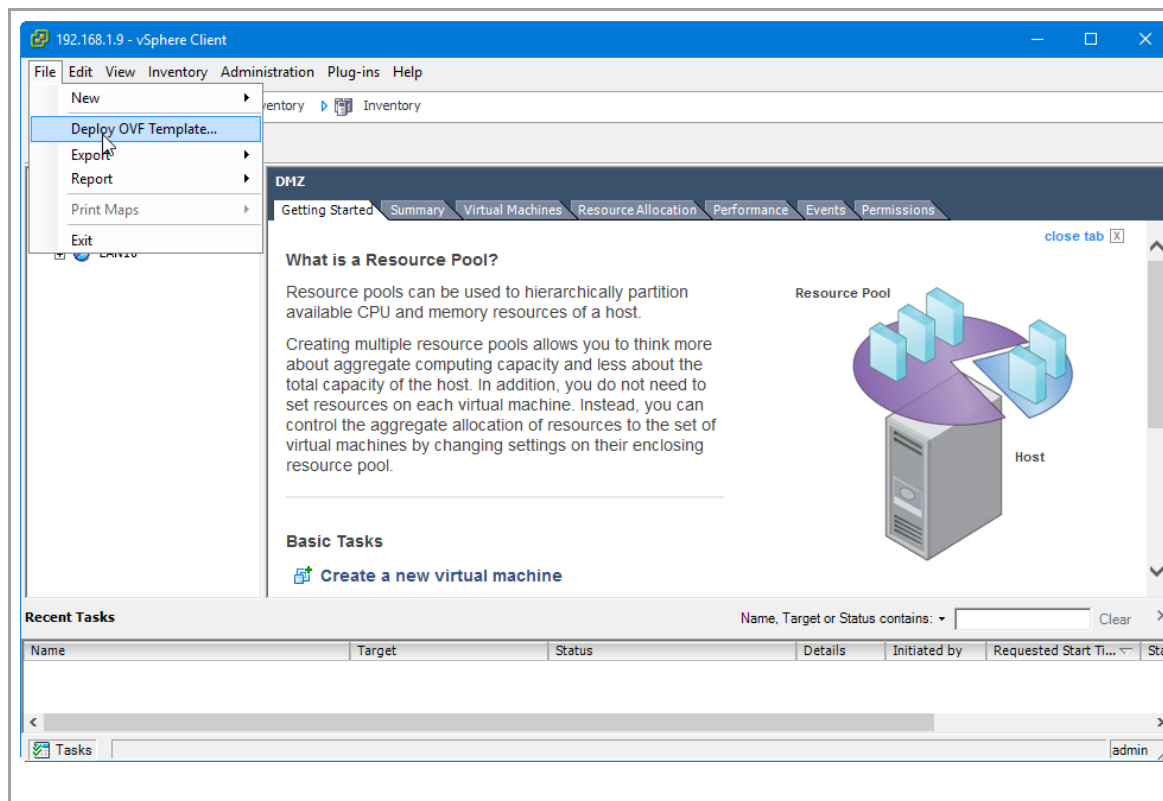
The user finally has to access to the SSP from remote by

- 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

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.

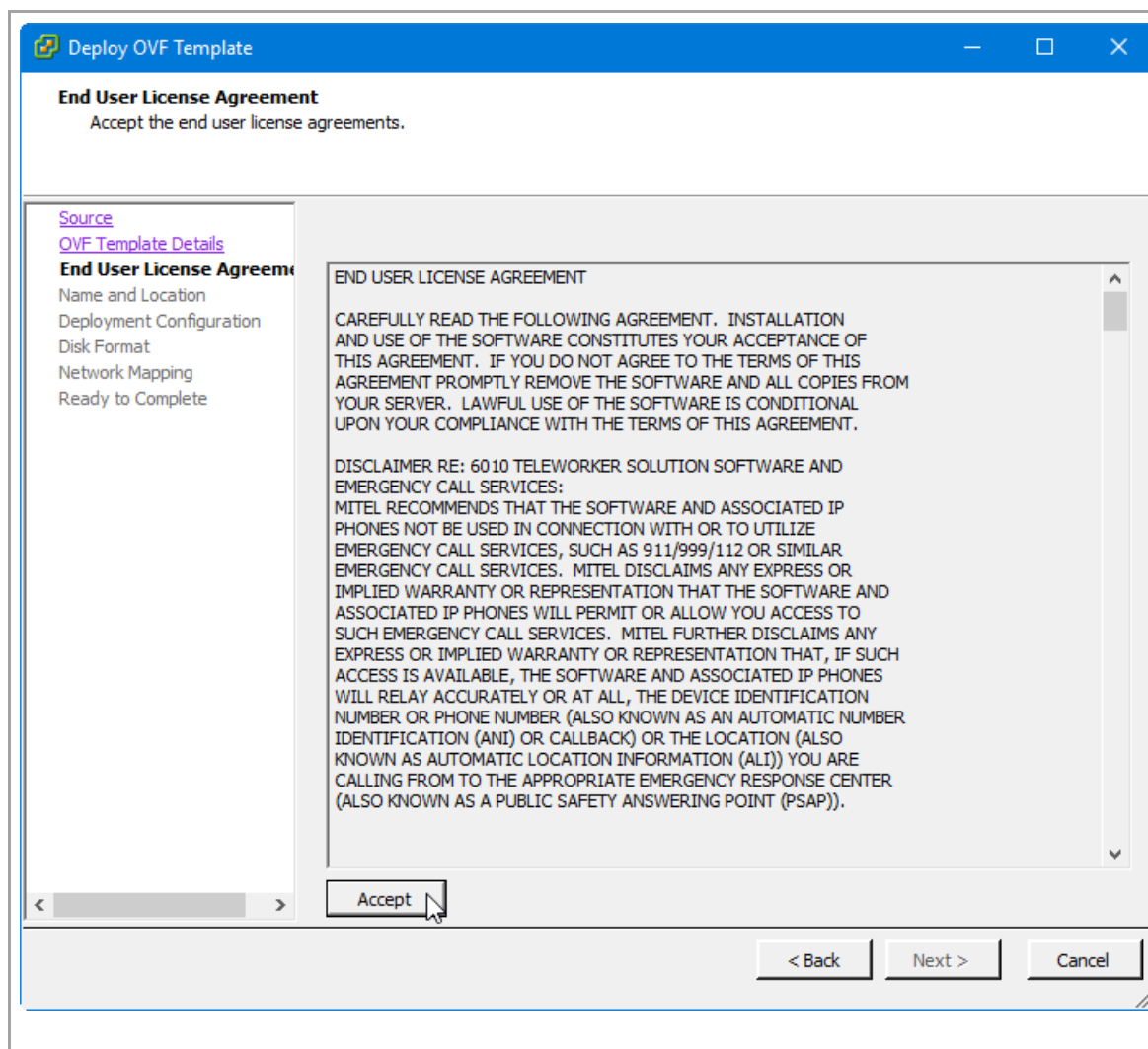
< Back   Next >   Cancel

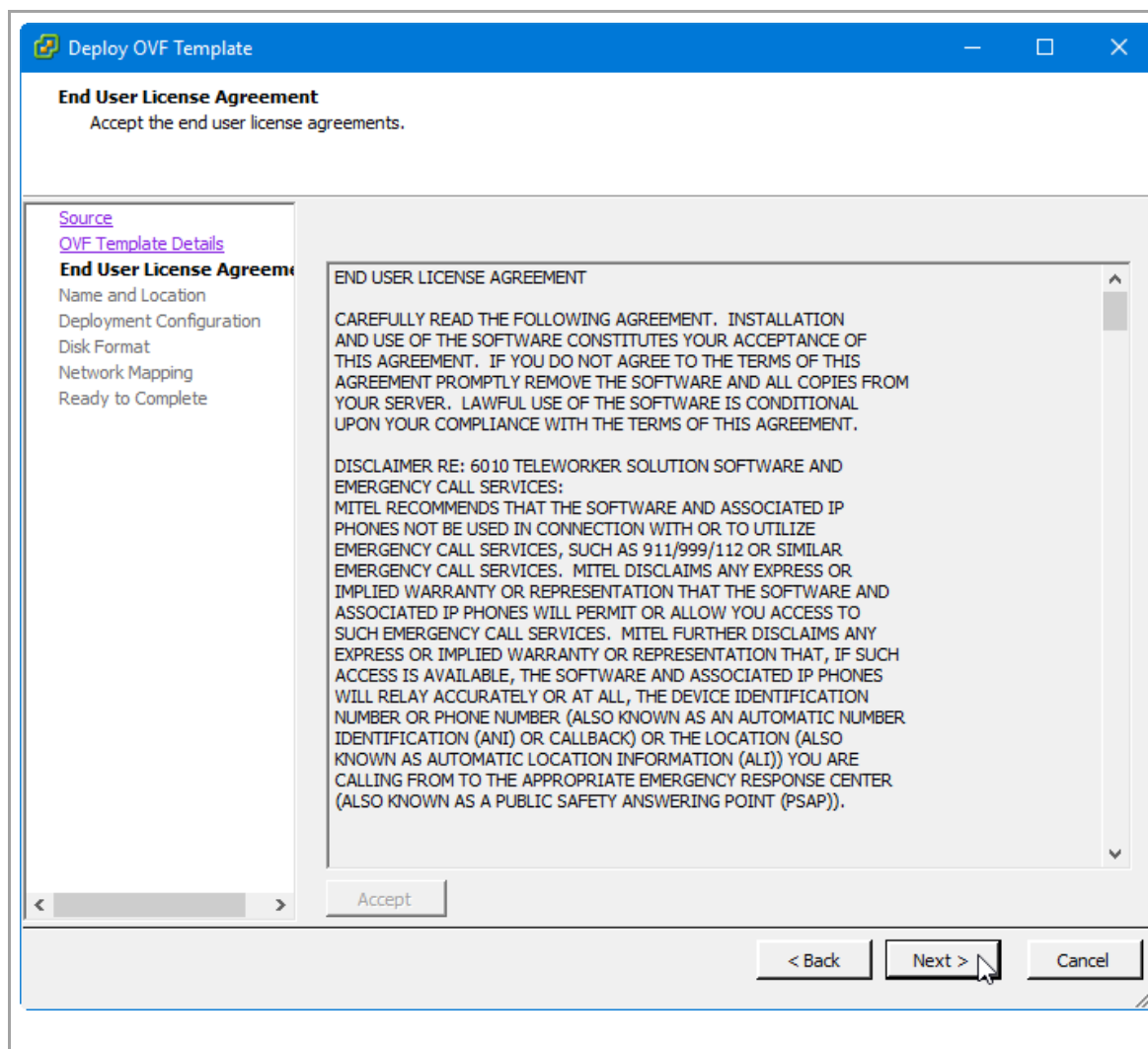
The screenshot shows a software window titled "Deploy OVF Template". Inside, the "OVF Template Details" section is active, displaying a list of steps on the left and a details table on the right. The steps include "Source", "OVF Template Details", "End User License Agreement", "Name and Location", "Deployment Configuration", "Disk Format", "Network Mapping", and "Ready to Complete". The details table lists information about the vMBG template, including its version (9.3.0.14), vendor (Mitel Networks Corporation), and size (1.1 GB download, 3.0 GB thin provisioned disk).

Property	Value
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

Navigation buttons at the bottom: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.







The screenshot shows a Windows-style window titled "Deploy OVF Template". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). Below the header, the main content area is divided into two sections. On the left is a vertical sidebar with a list of steps: "Source", "OVF Template Details", "End User License Agreement", "Name and Location" (which is bolded, indicating the current step), "Deployment Configuration", "Disk Format", "Network Mapping", and "Ready to Complete". The main area on the right is titled "Name and Location" with the instruction "Specify a name and location for the deployed template". It contains a "Name:" label, a text input field with the value "vMBG\_93014", and a note below it stating "The name can contain up to 80 characters and it must be unique within the inventory folder." At the bottom of the window, there are three buttons: "< Back", "Next >" (with a mouse cursor hovering over it), and "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

The screenshot shows a Windows-style window titled "Deploy OVF Template". Inside, the "Deployment Configuration" step is active, with the instruction "Select a deployment configuration." A left-hand pane lists the steps: "Source", "OVF Template Details", "End User License Agreement", "Name and Location", "Deployment Configuration" (highlighted), "Disk Format", "Network Mapping", and "Ready to Complete". The main area shows a "Configuration:" dropdown menu with "Small business" selected. Below it, text reads: "Small business configuration: Please refer to the Engineering Guidelines for full details." At the bottom right are three buttons: "< Back", "Next >" (with a mouse cursor over it), and "Cancel".

**Deploy OVF Template**

**Deployment Configuration**  
Select a deployment configuration.

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
**Deployment Configuration**  
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

The screenshot shows a Windows-style window titled "Deploy OVF Template". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). Below the header, the main content area is divided into a left sidebar and a main panel. The sidebar contains a list of steps: "Source", "OVF Template Details", "End User License Agreement", "Name and Location", "Deployment Configuration", "Disk Format" (which is highlighted), "Network Mapping", and "Ready to Complete". The main panel displays the "Disk Format" configuration. It includes a label "In which format do you want to store the virtual disks?". Below this, there are two input fields: "Datastore:" with the value "datastore 1" and "Available space (GB):" with the value "1040.4". There are three radio button options: "Thick Provision Lazy Zeroed" (which is selected), "Thick Provision Eager Zeroed", and "Thin Provision". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.

**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:

Available space (GB):

☒ 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

The screenshot shows the 'Deploy OVF Template' wizard in a window. The title bar says 'Deploy OVF Template'. The main area is titled 'Properties' with the subtitle 'Customize the software solution for this deployment.' On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Deployment Configuration', 'Host / Cluster' (selected), 'Storage', 'Disk Format', 'Network Mapping', and 'Properties' (Ready to Complete). The main content area is divided into three sections: 'Administration' with a 'Restore from backup' checkbox; 'Localization' with 'Timezone setting' (dropdown set to 'Europe/Zurich') and 'Keyboard' (dropdown set to 'sg'); and 'Application' with 'Initial Administrator Password' (two password fields, both masked with asterisks). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A red warning message at the bottom of the main area states: 'Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.'

**Deploy OVF Template**

**Properties**  
Customize the software solution for this deployment.

Source  
OVF Template Details  
End User License Agreement  
Name and Location  
Deployment Configuration  
Host / Cluster  
Storage  
Disk Format  
Network Mapping  
Properties  
Ready to Complete

**Administration**

**Restore from backup**  
Check this box to restore the VM from an existing backup via the server console. You must complete the mandatory fields.  
☐

**Localization**

**Timezone setting**  
Select the appropriate timezone.  
Europe/Zurich

**Keyboard**  
Select a keyboard  
sg

**Application**

**Initial Administrator Password**  
The initial password to use to when accessing this deployed virtual appliance. The password must be at least 7 characters long.  
Enter password: \*\*\*\*\*  
Confirm password: \*\*\*\*\*

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

< Back   Next >   Cancel

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

- Time zone
- Keyboard layout
- Admin password

**Deploy OVF Template**

**Properties**  
Customize the software solution for this deployment.

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
+ [Host / Cluster](#)  
[Storage](#)  
[Disk Format](#)  
[Network Mapping](#)  
**Properties**  
[Ready to Complete](#)

**Hostname**  
The hostname of the virtual appliance. You should select a unique hostname for each virtual appliance. The hostname must start with a letter and can be composed of letters, numbers and hyphens.

**Domain Name (Optional)**  
The domain name this virtual appliance should belong to.

**License Key (Optional)**  
The license key (ARID) to apply to this virtual appliance.

**DNS Server IP (Optional)**  
Please enter the IP address for the domain name server(s) for this VM (comma separated).

**Remote Network Address (Optional)**  
If you intend to manage the virtual appliance remotely from the Internet (WAN), enter the network address for the host(s) for which you want to allow access.

**Remote Network Netmask (Optional)**

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

< Back   Next >   Cancel

- Hostname
- Domain
- DNS server



The screenshot shows the 'Deploy OVF Template' wizard in the 'Properties' step. The left sidebar contains a tree view with the following items: Source, OVF Template Details, End User License Agreement, Name and Location, Deployment Configuration, Host / Cluster, Storage, Disk Format, Network Mapping, Properties (selected), and Ready to Complete. The main content area is titled 'Network Settings' and contains the following sections:

- LAN IP Address**  
The LAN IP address for this VM.  
192 . 168 . 6 . 90
- LAN Netmask**  
Please enter the netmask or prefix for the LAN interface.  
255 . 255 . 255 . 0
- WAN IP Address**  
For deployment in Server-Gateway mode, enter the WAN IP address.  
0 . 0 . 0 . 0
- WAN Netmask**  
Please enter the netmask or prefix for the WAN interface. Use default settings for Server-Only deployment.  
255 . 255 . 255 . 0
- Second WAN IP Address (Optional)**  
For deployment in Server-Gateway mode, enter an optional second WAN IP address.  
0 . 0 . 0 . 0
- Default Gateway Address**  
The default gateway. This typically points to the internet gateway for a Server-Gateway deployment or LAN router in a Server-Only configuration.  
192 . 168 . 6 . 1

At the bottom of the wizard are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

- 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**

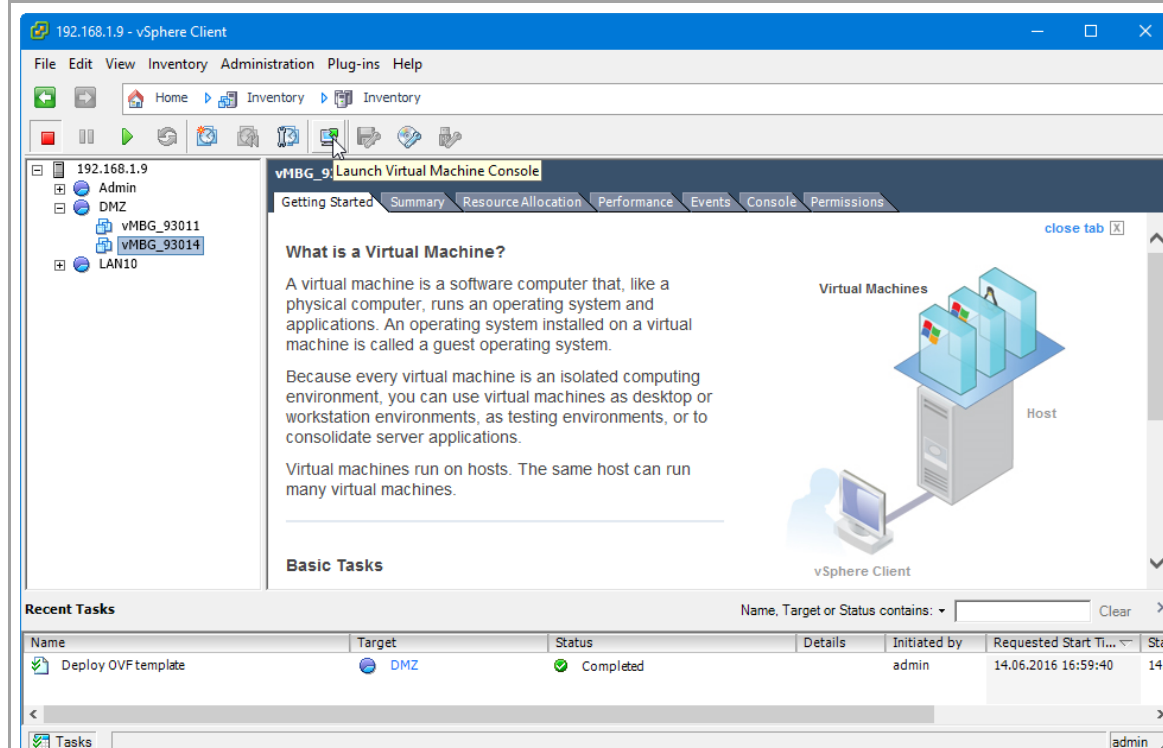
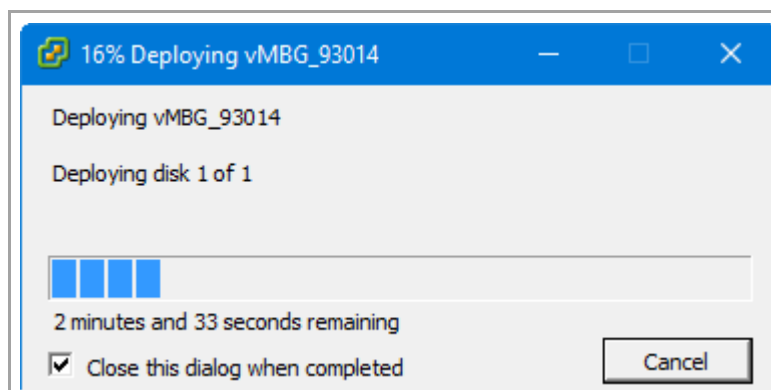
When you click Finish, the deployment task will be started.

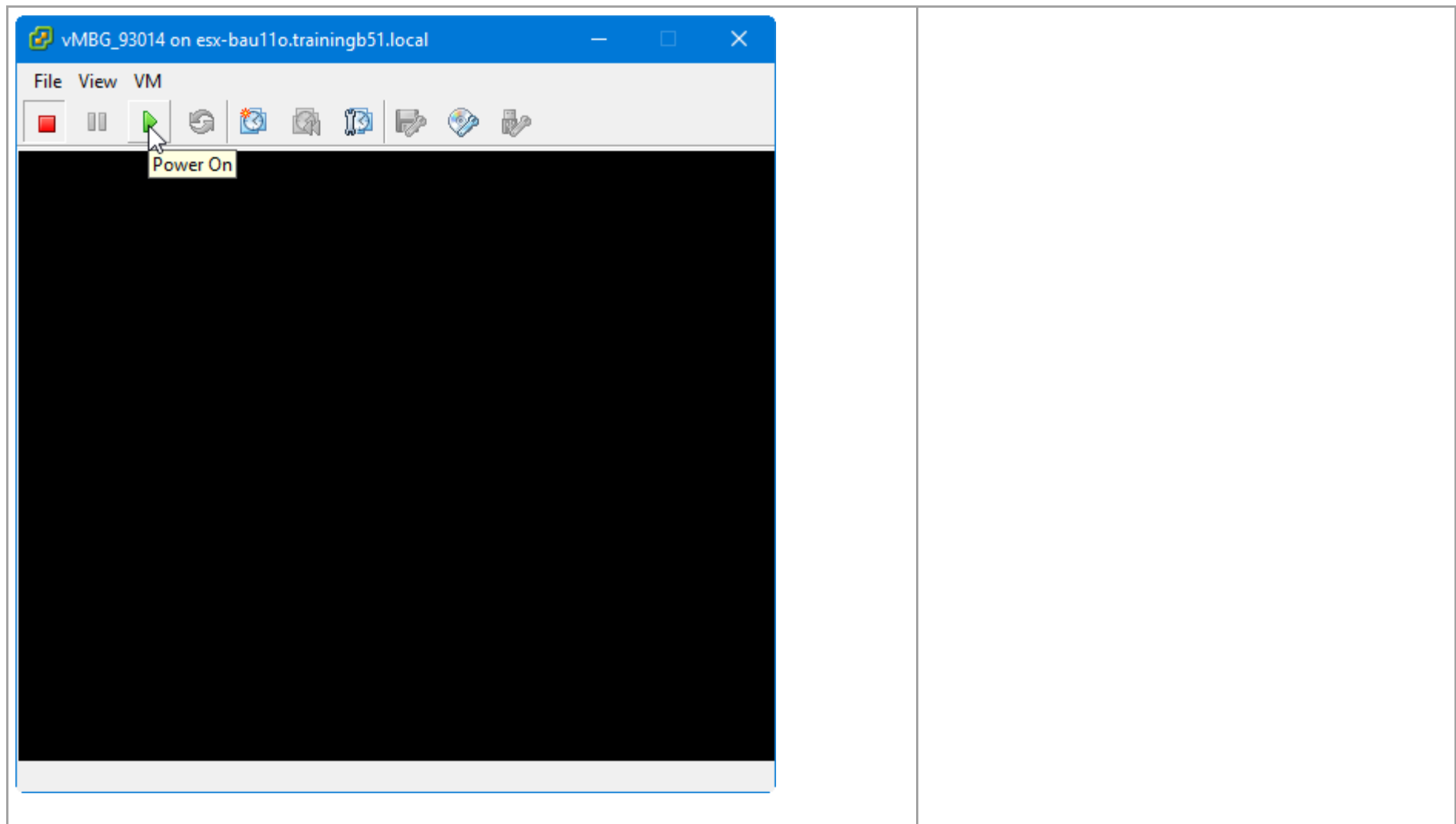
Deployment settings:

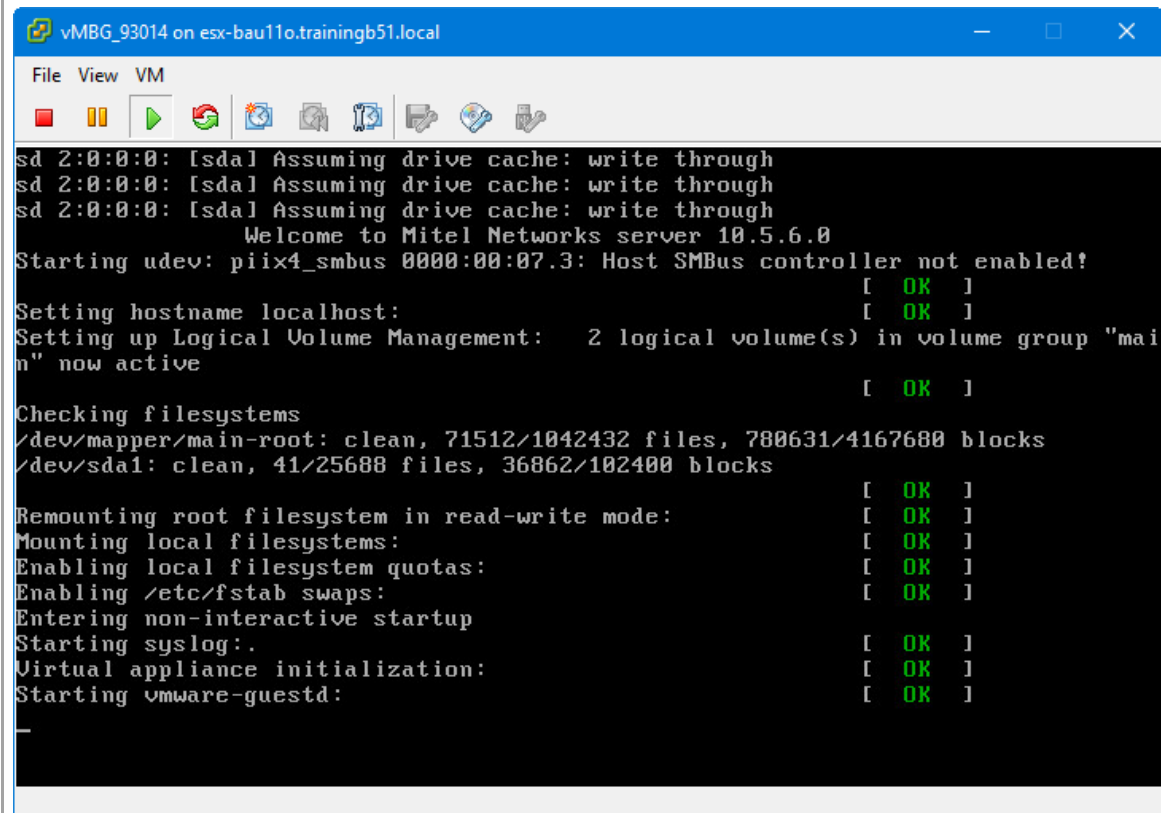
OVF file:	E:\Mitel Software\MBG\vmBG_9.3.0.14.ova
Download size:	1.1 GB
Size on disk:	20.0 GB
Name:	vmBG_93014
Deployment Configuration:	Small business
Host/Cluster:	esx-bau11o.trainingb51.local
Resource Pool:	DMZ
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"LAN" 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

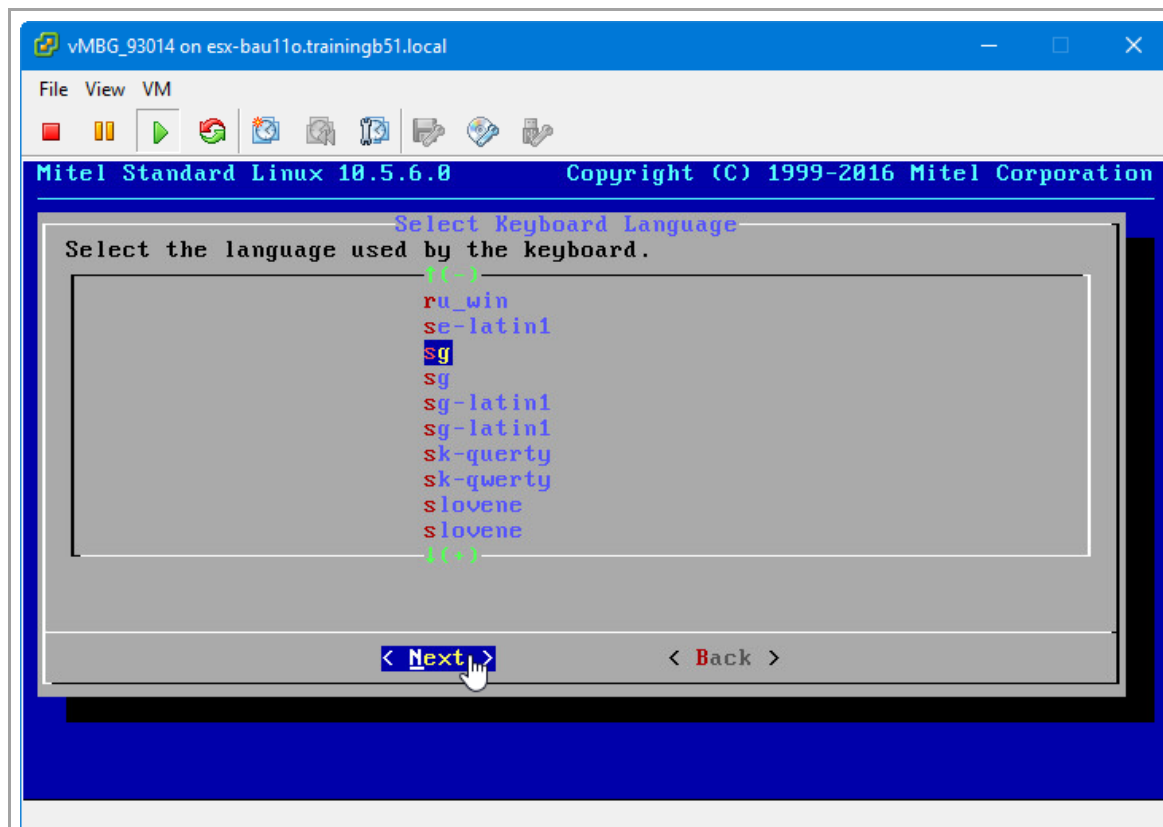






```
vMBG_93014 on esx-bau11o.trainingb51.local
File View VM

sd 2:0:0:0: [sdal] Assuming drive cache: write through
sd 2:0:0:0: [sdal] Assuming drive cache: write through
sd 2:0:0:0: [sdal] 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 "main" 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 ]
-
```

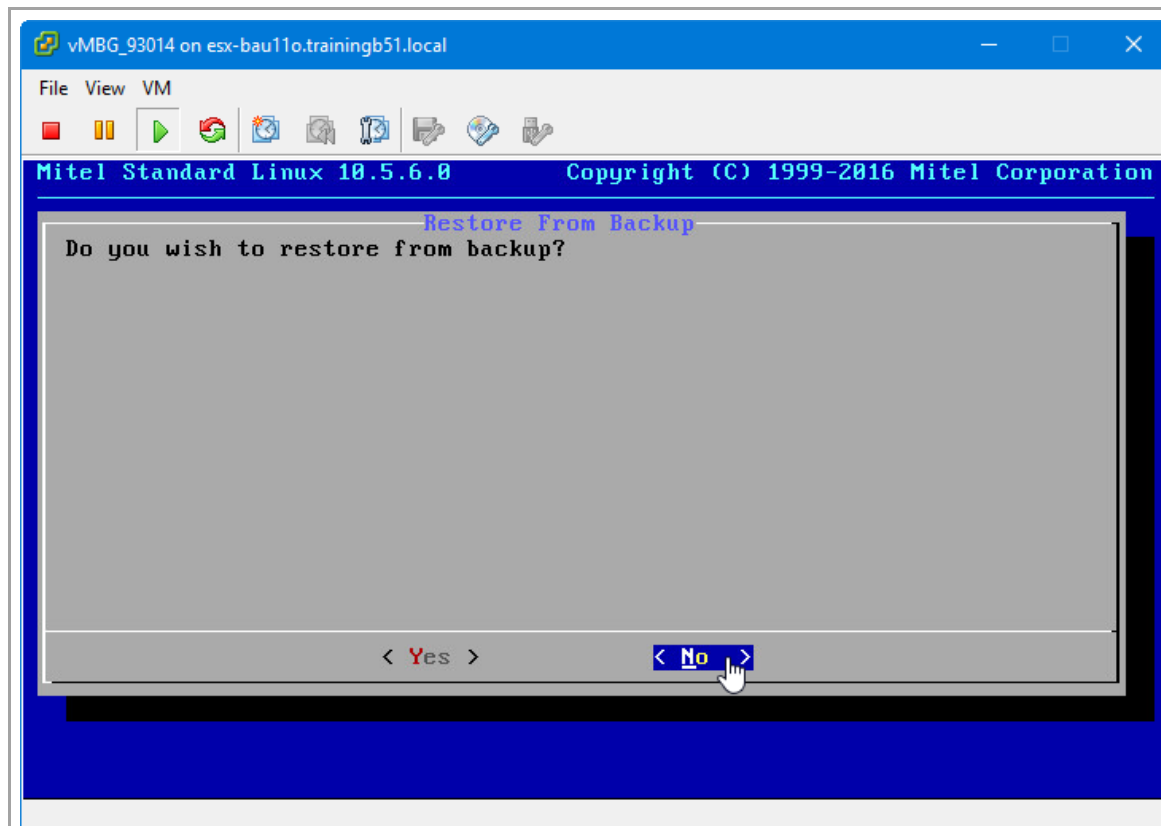


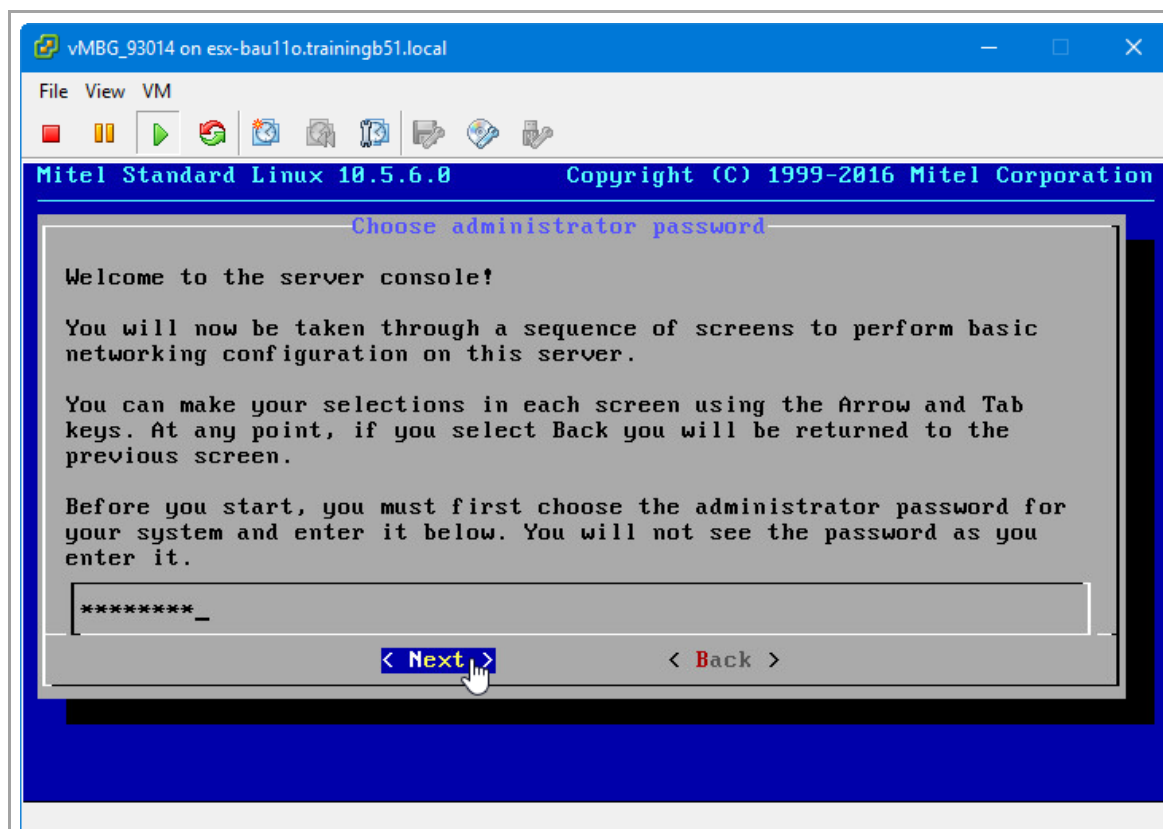
If you do not have the vCenter licenses you have to do the initial settings here in the console:

Select your keyboard layout:

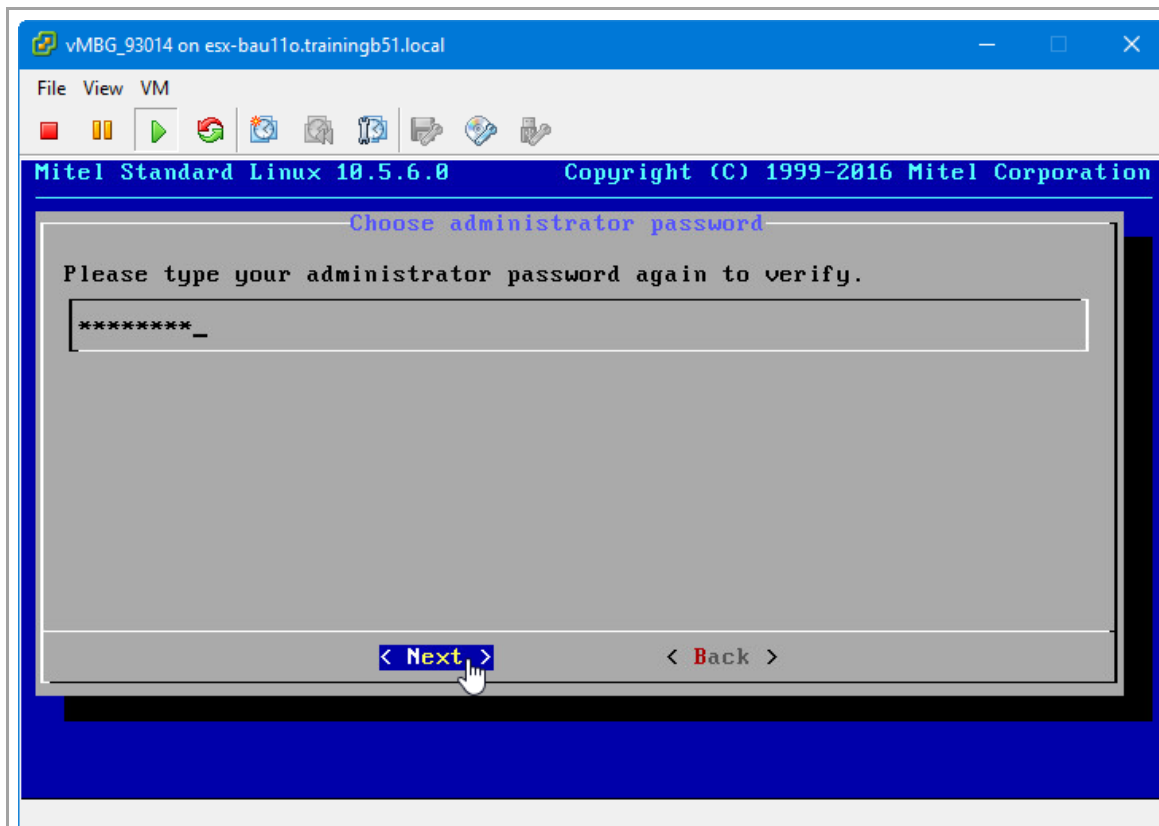
e.g.

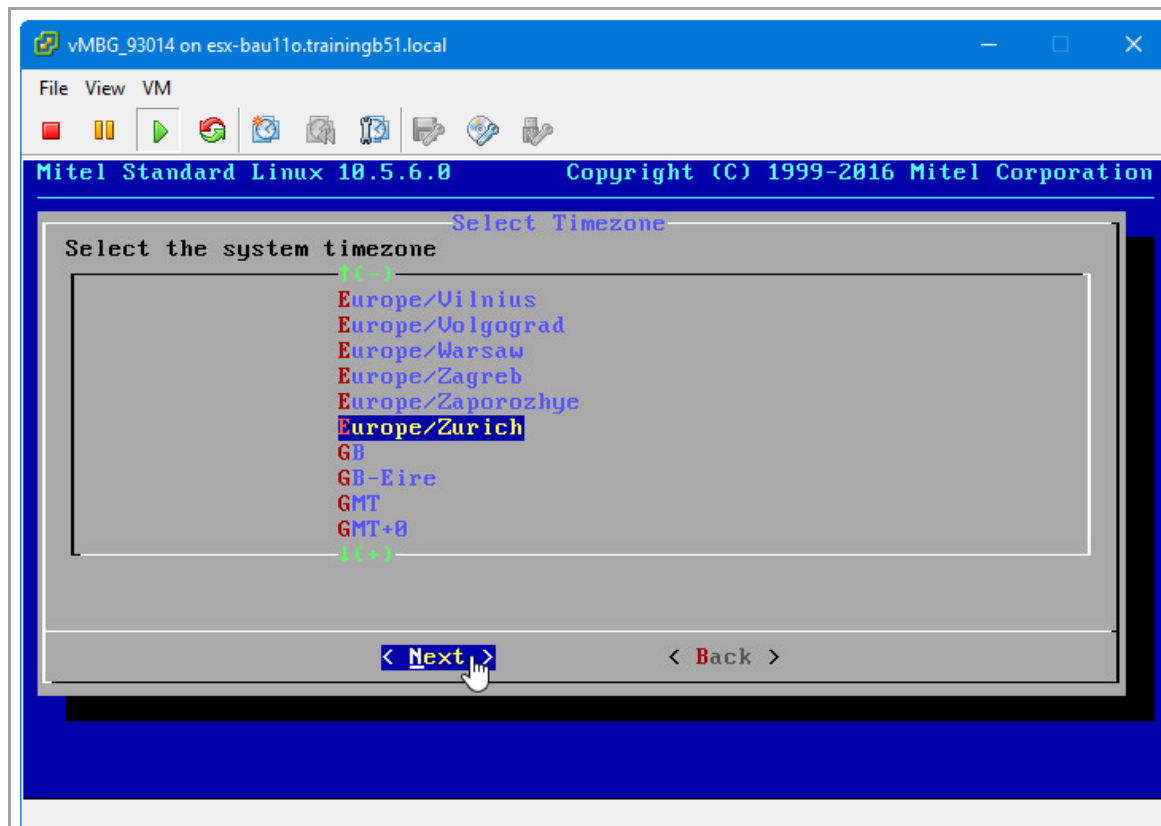
sg = SwissGerman

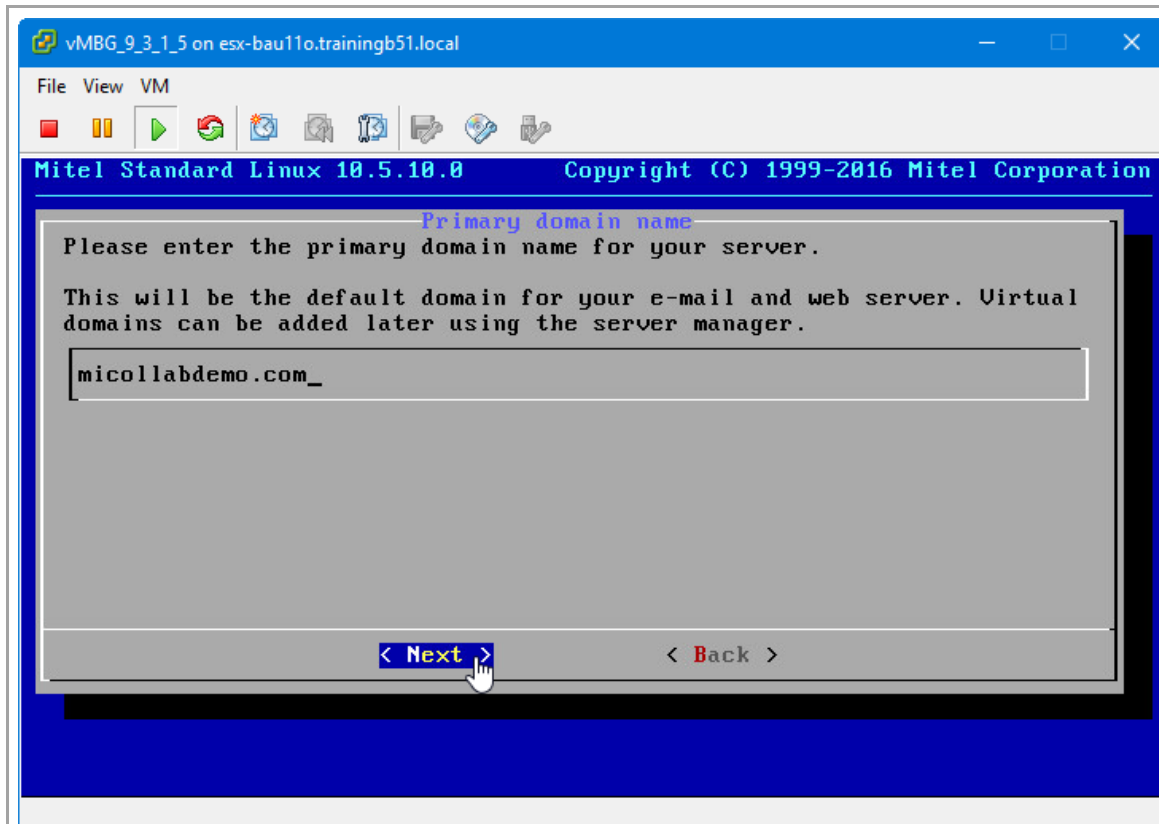


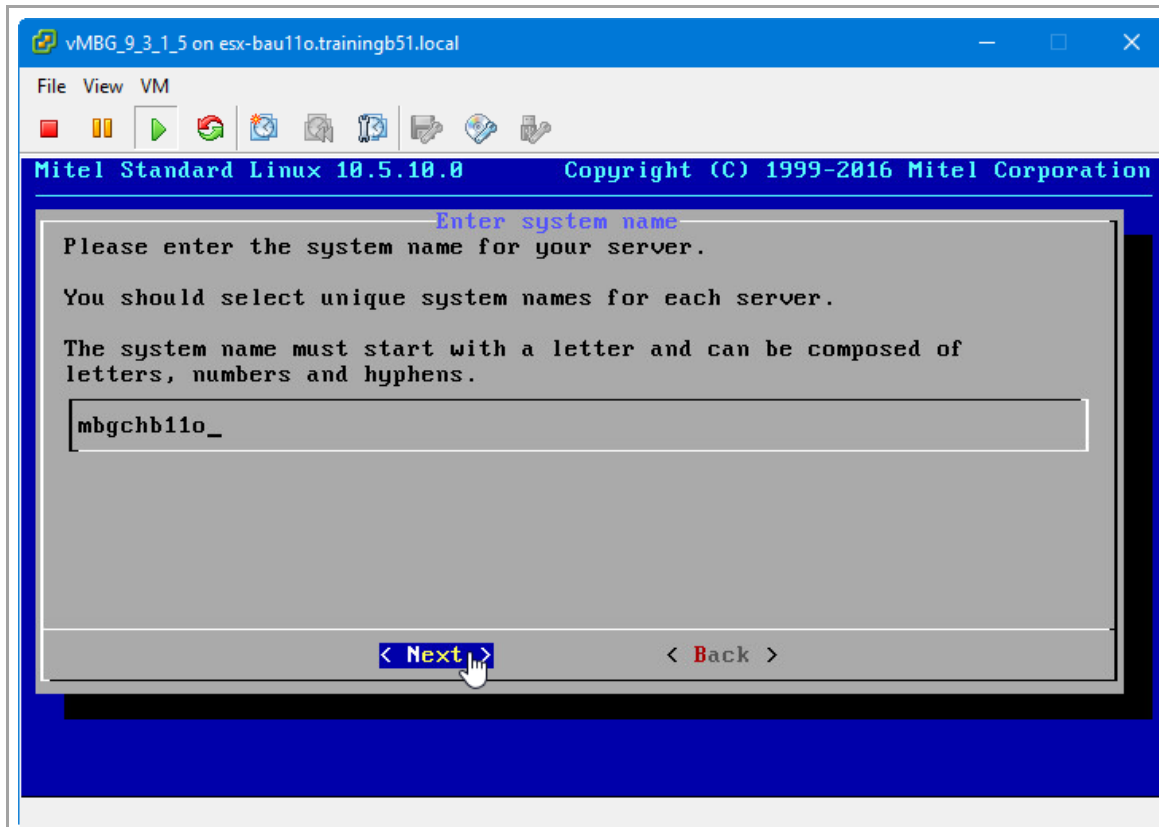


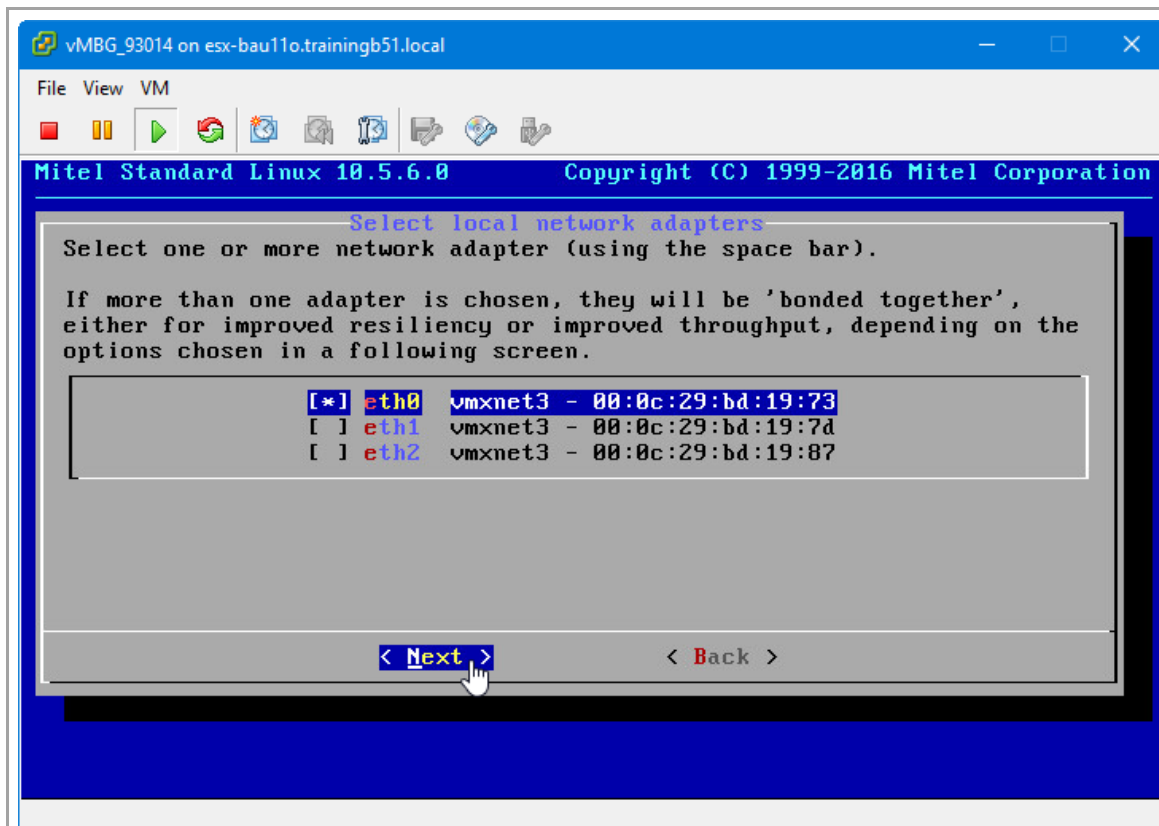


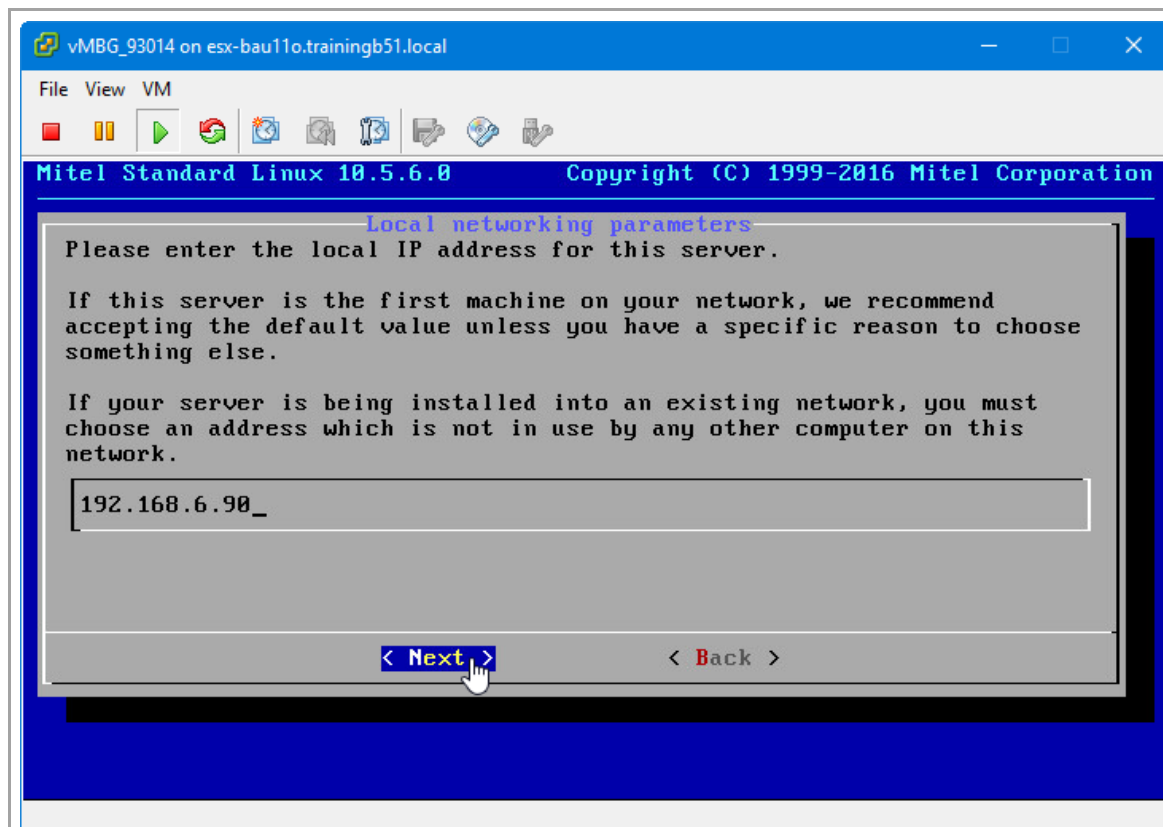


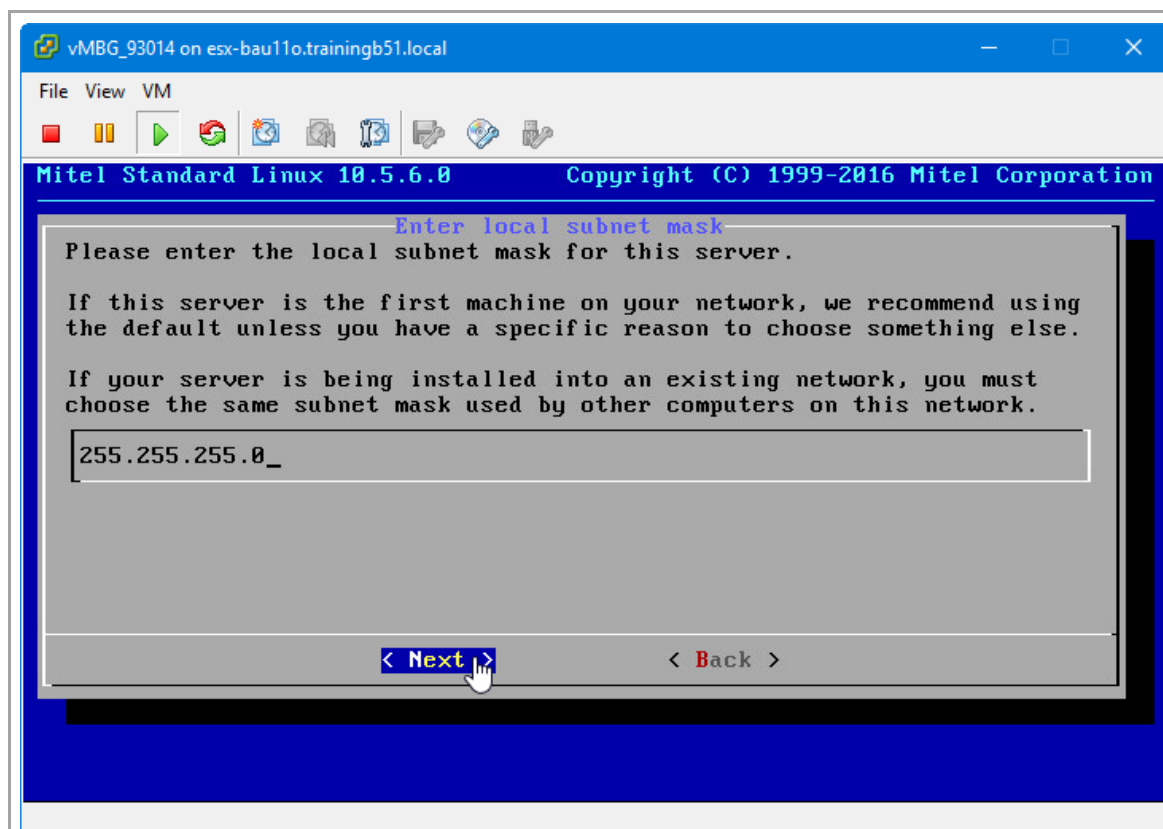


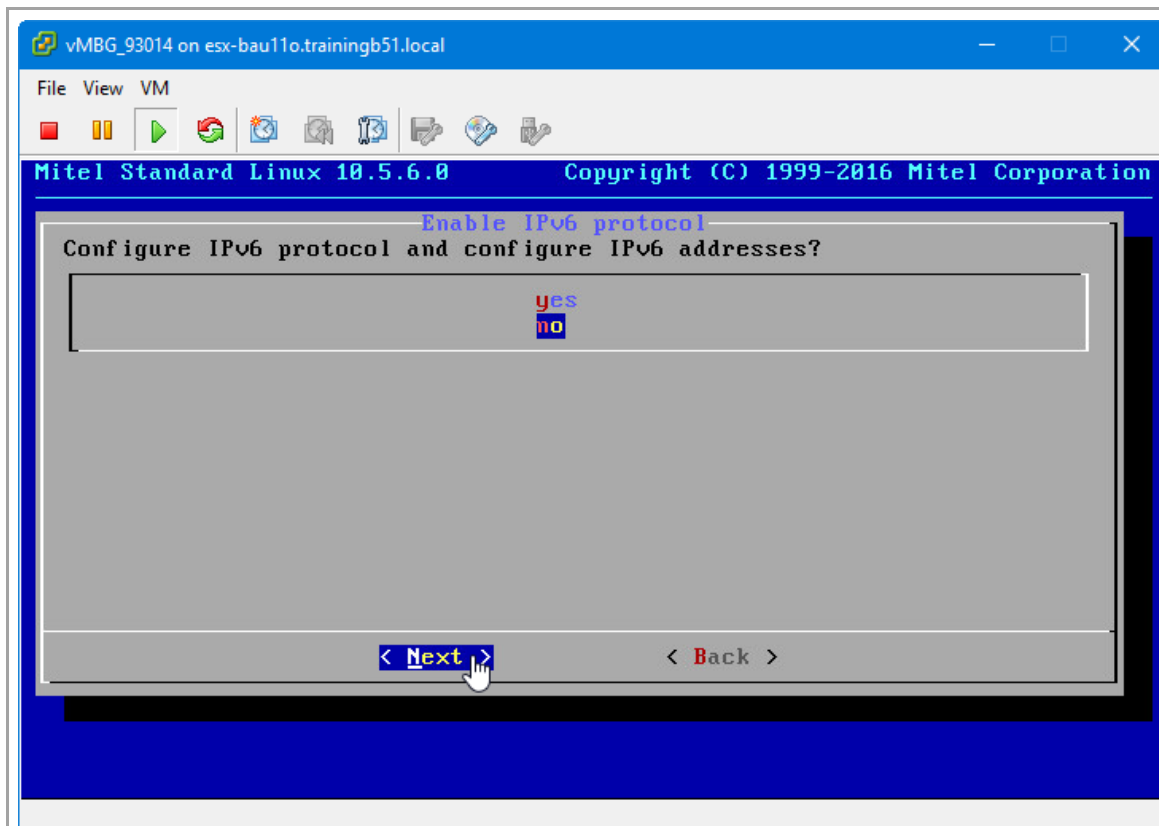




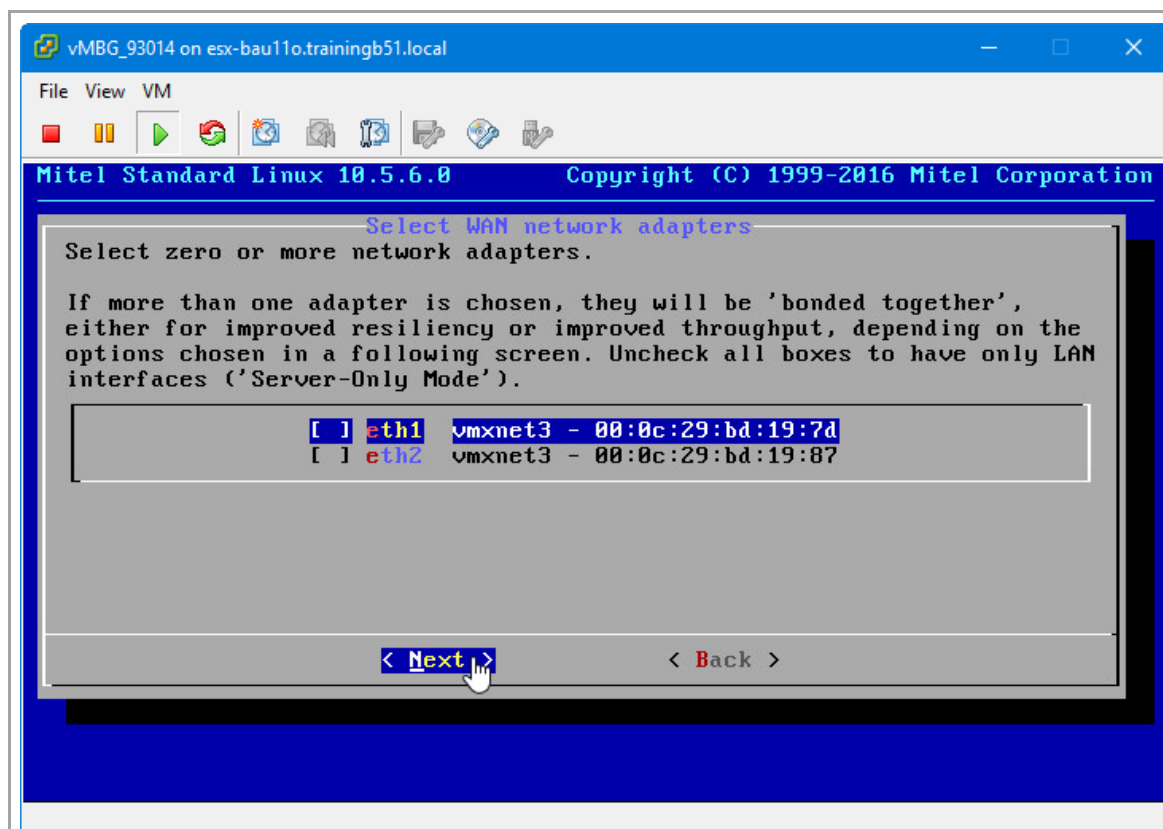




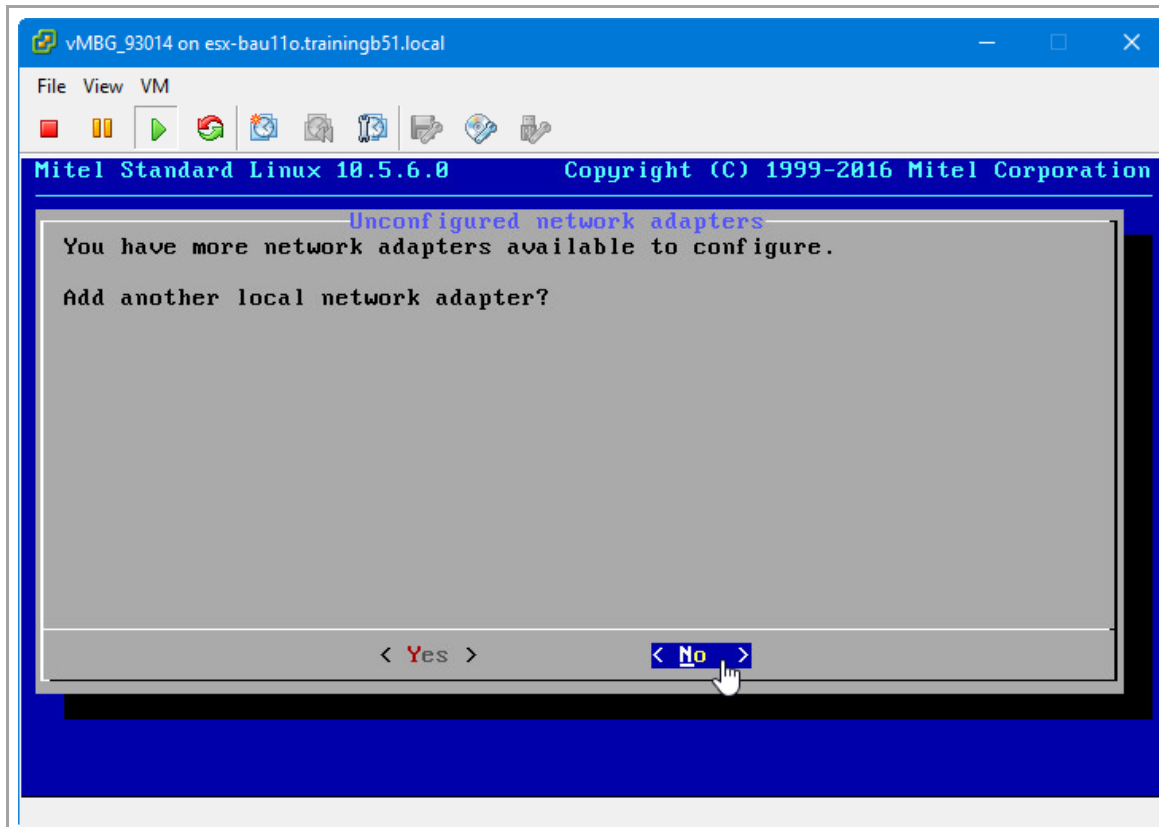


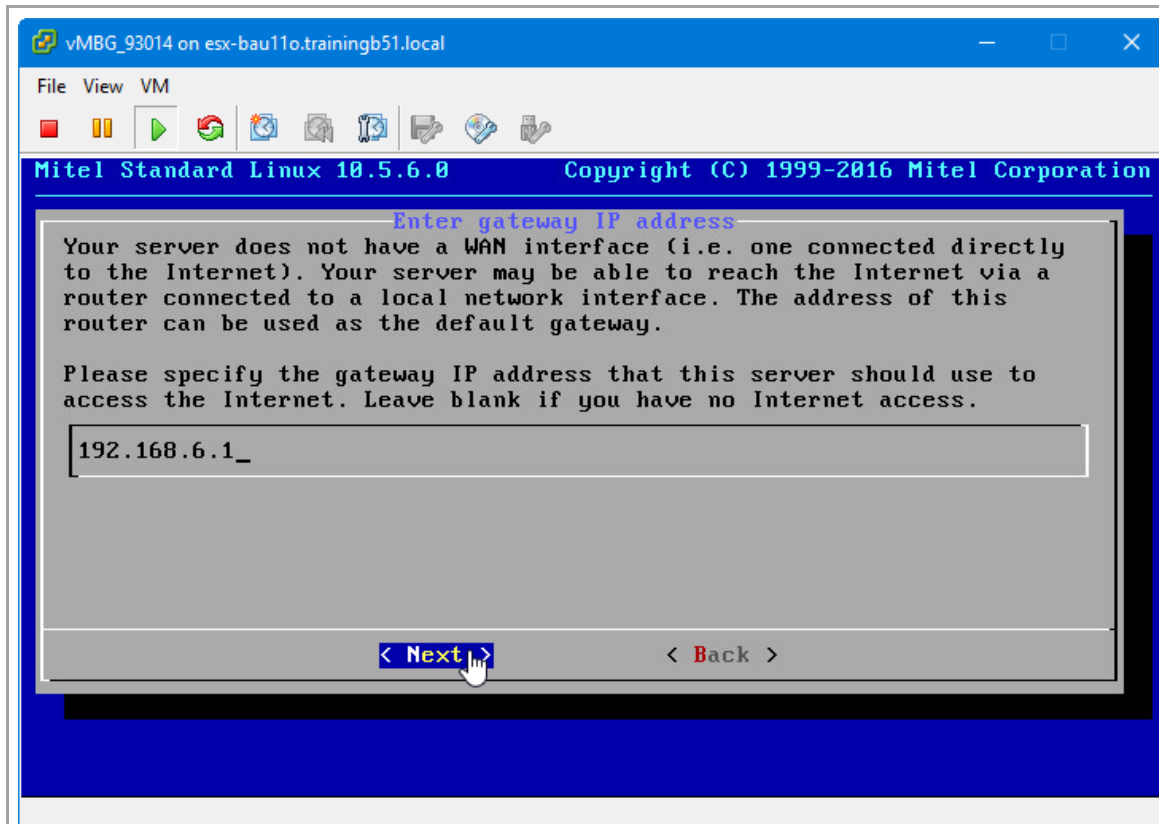


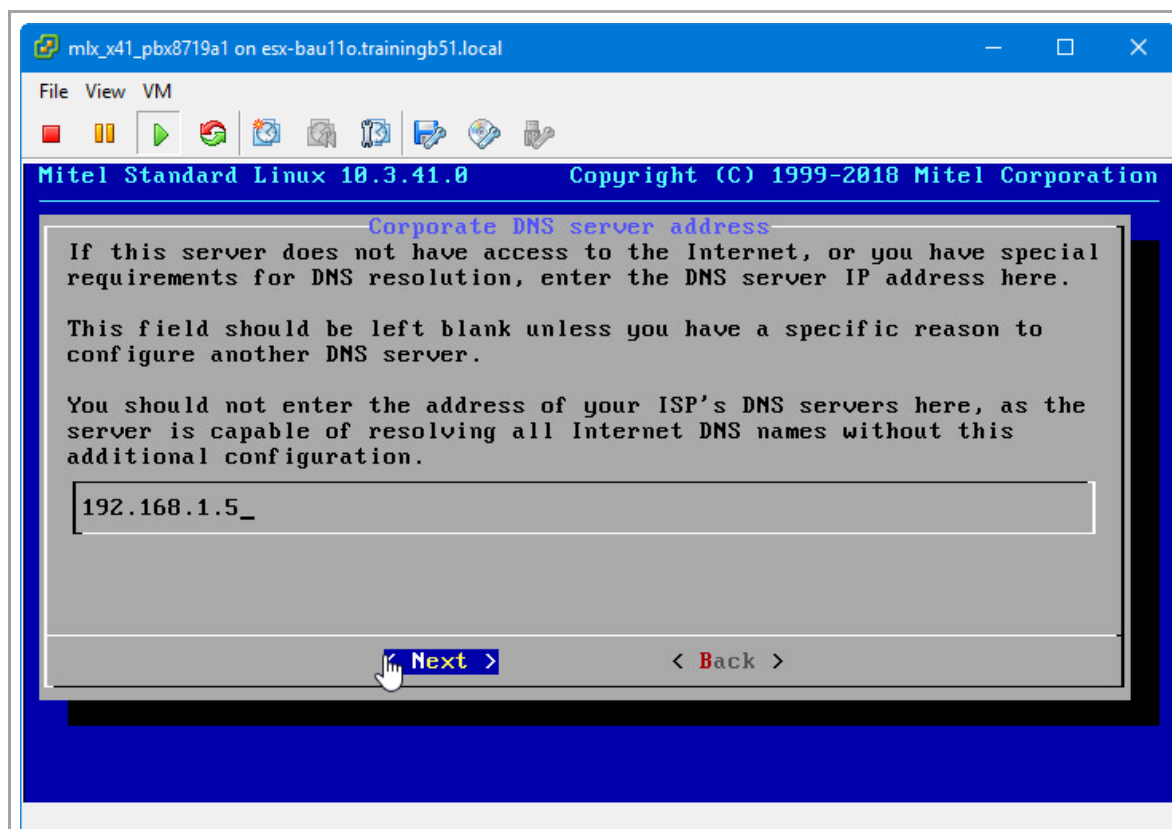




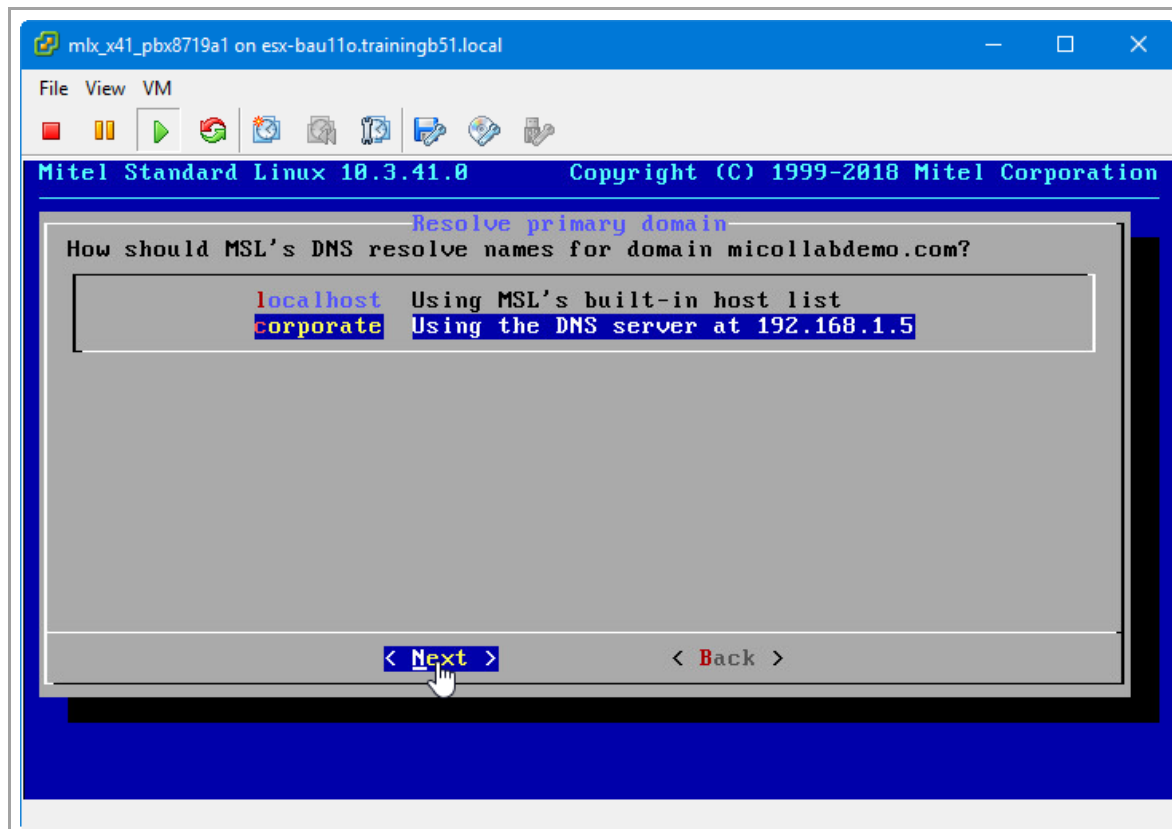
No other network adapter is used.  
So just hit "Next".

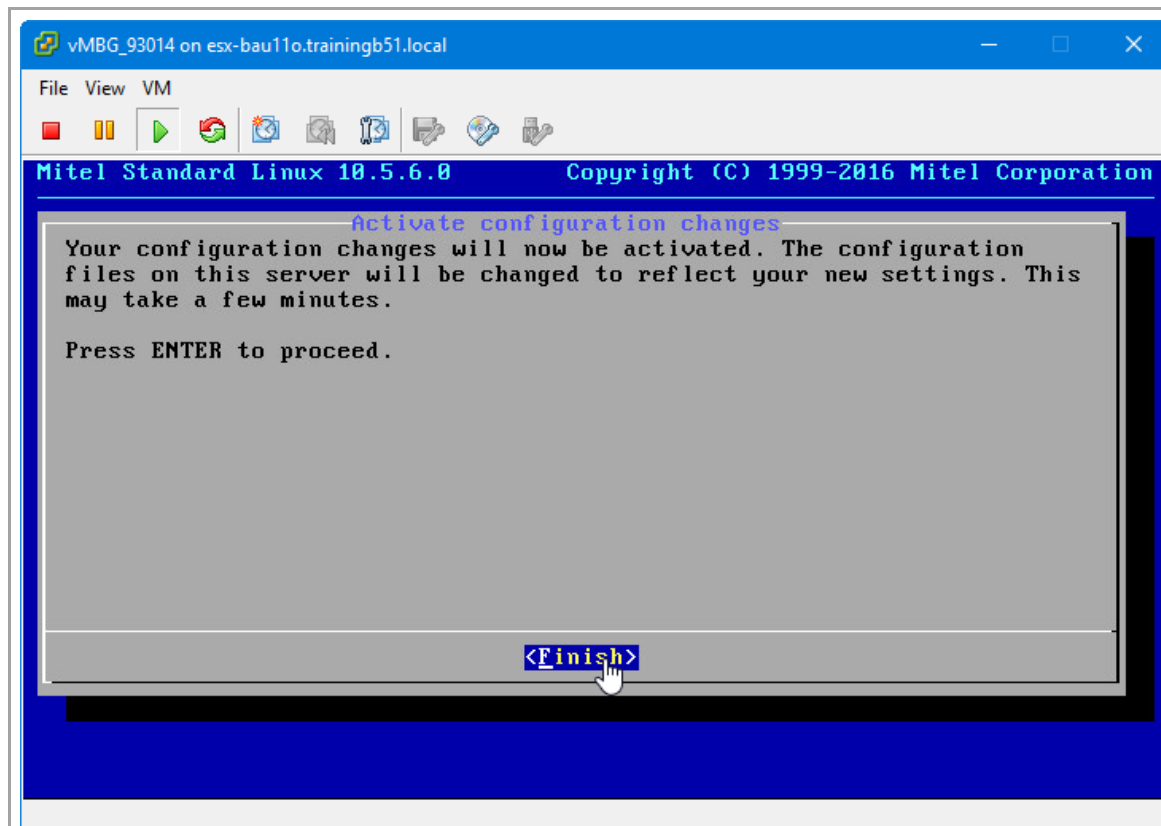


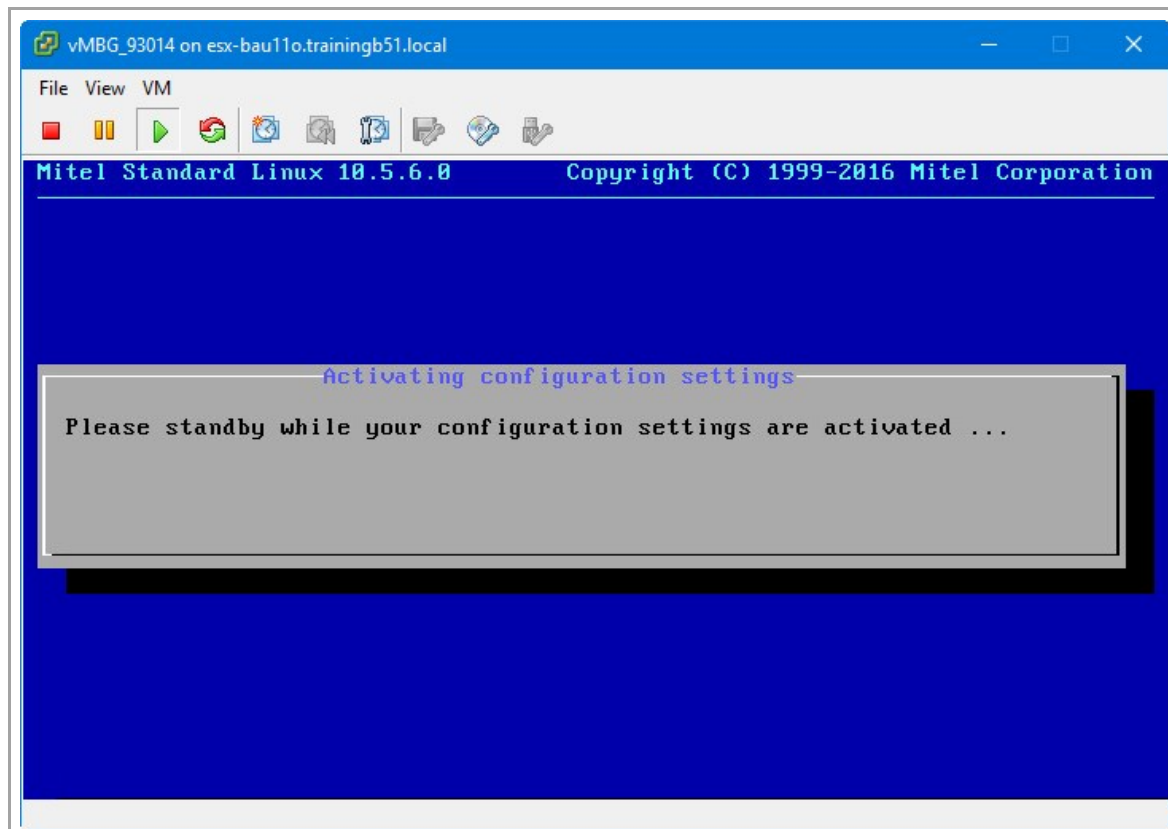


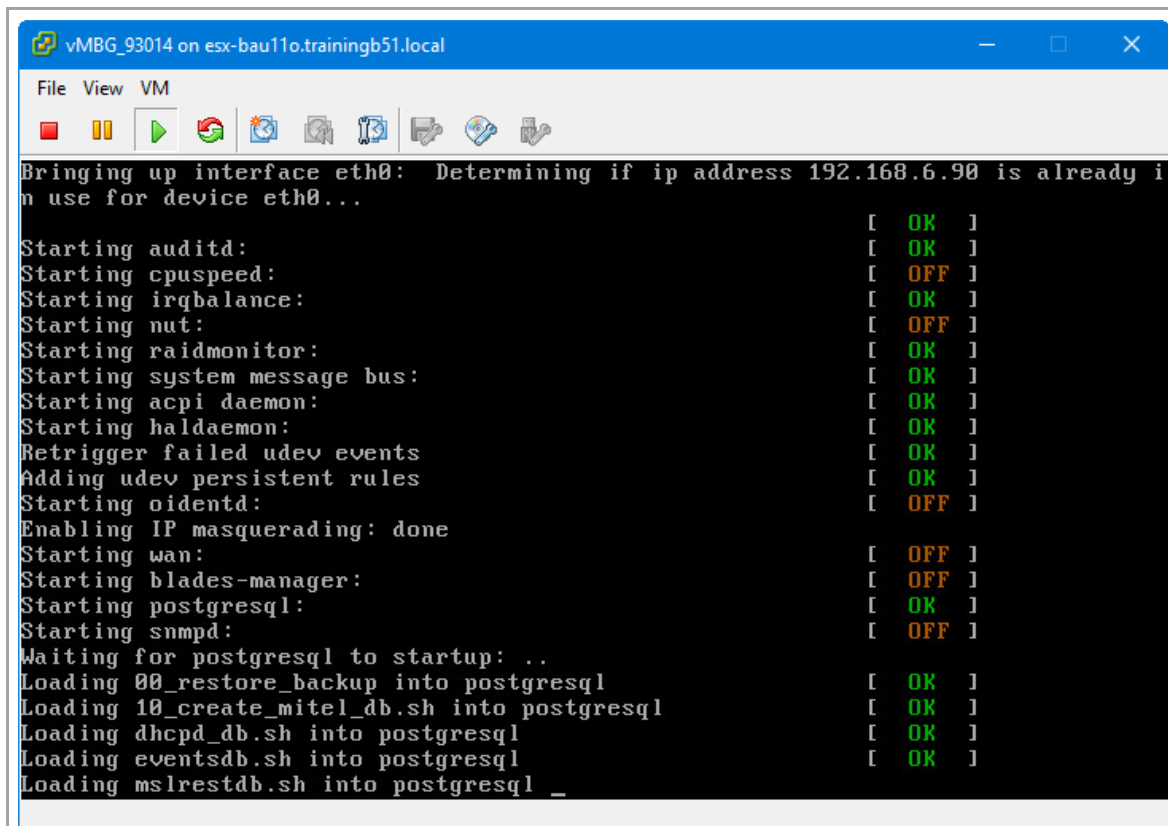


Enter your corporate DNS server here.



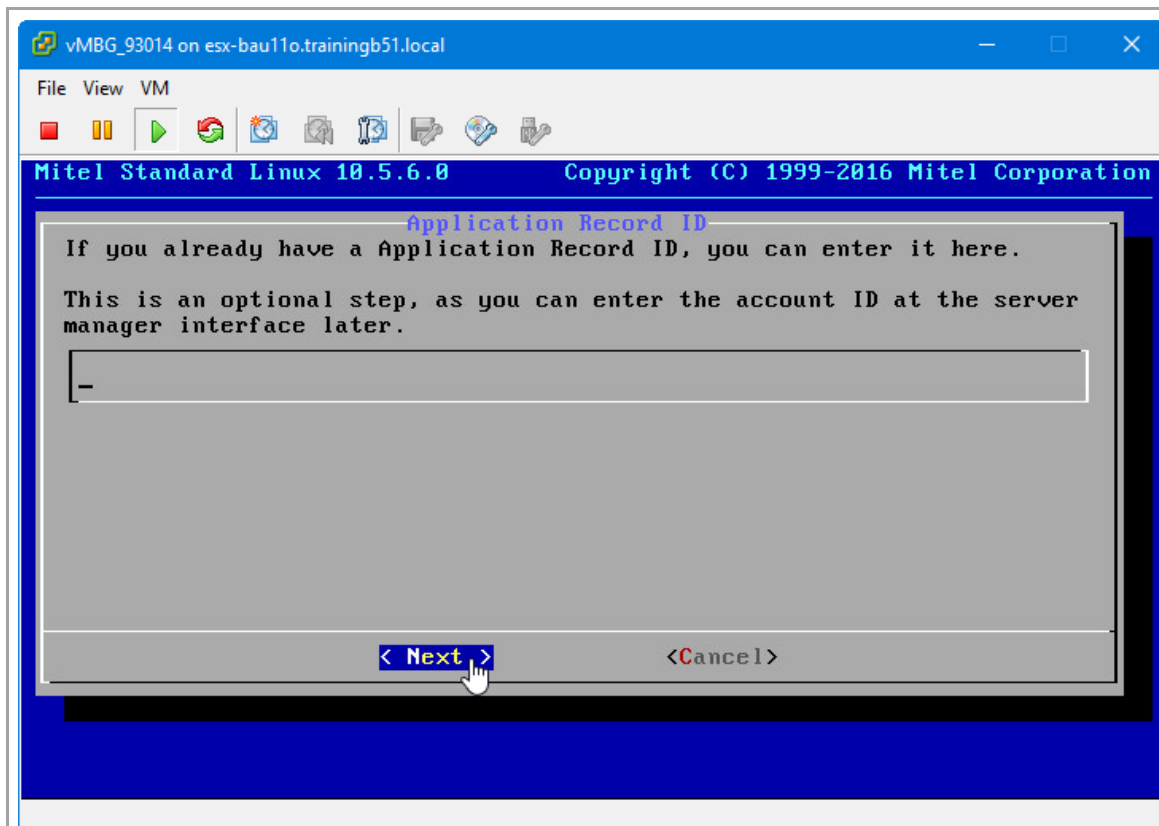




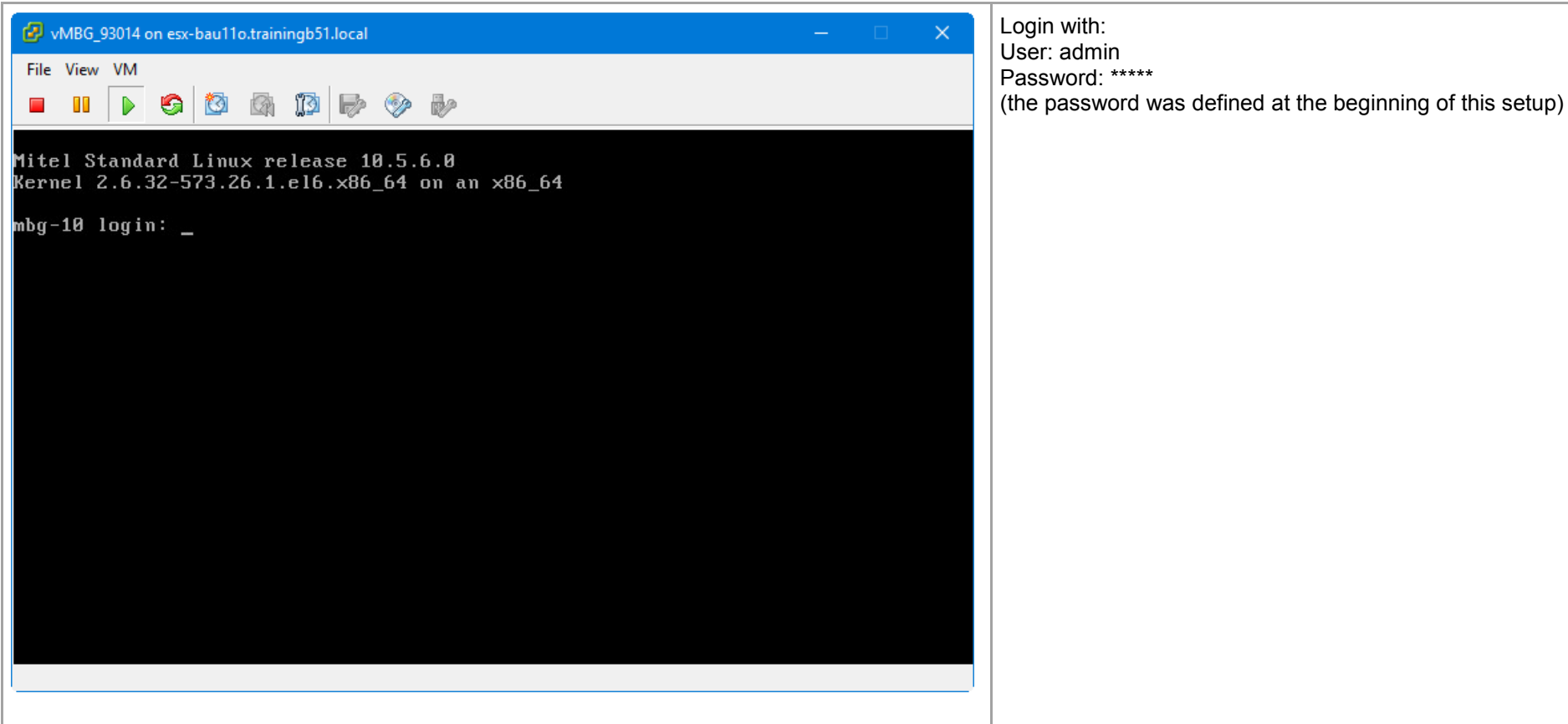


```
vMBG_93014 on esx-bau11o.trainingb51.local
File View VM
Bringing up interface eth0: Determining if ip address 192.168.6.90 is already in use for device eth0...
Starting auditd: [ OK ]
Starting cpuspeed: [ OFF ]
Starting irqbalance: [ OK ]
Starting nut: [ OFF ]
Starting raidmonitor: [ OK ]
Starting 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 _
```



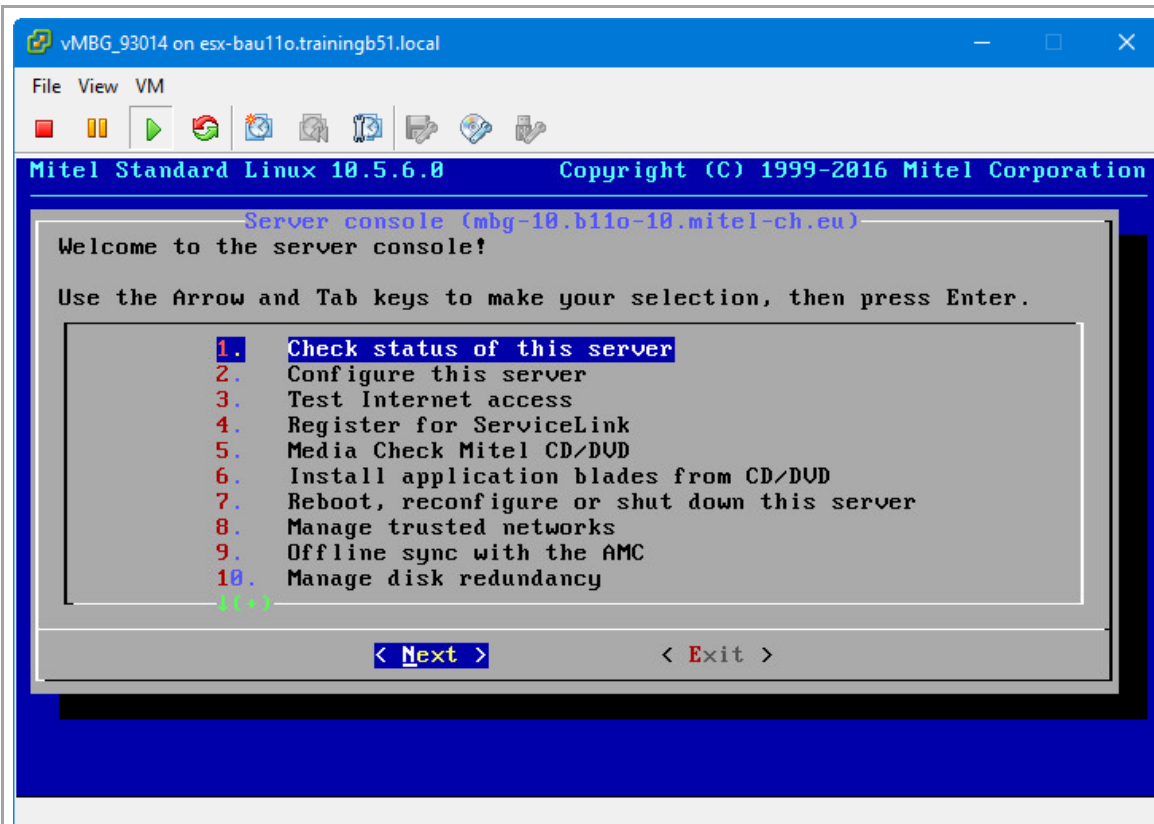


The ARID can be entered later in the Web-GUI.  
So just hit "Next"

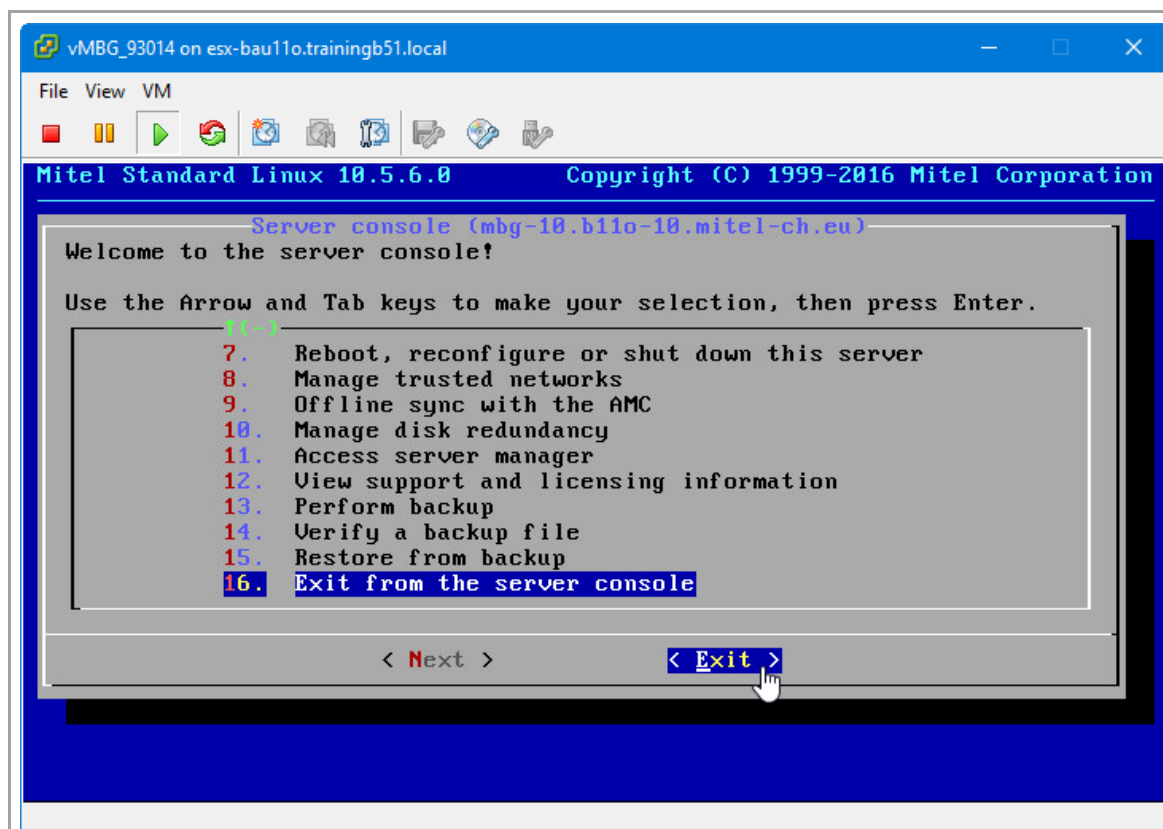


The screenshot shows a VMware Workstation window titled "vMBG\_93014 on esx-bau11o.trainingb51.local". The window contains a terminal window for a Mitel Standard Linux release 10.5.6.0. The terminal output shows the kernel version and architecture, followed by the login prompt "mbg-10 login: \_".

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.



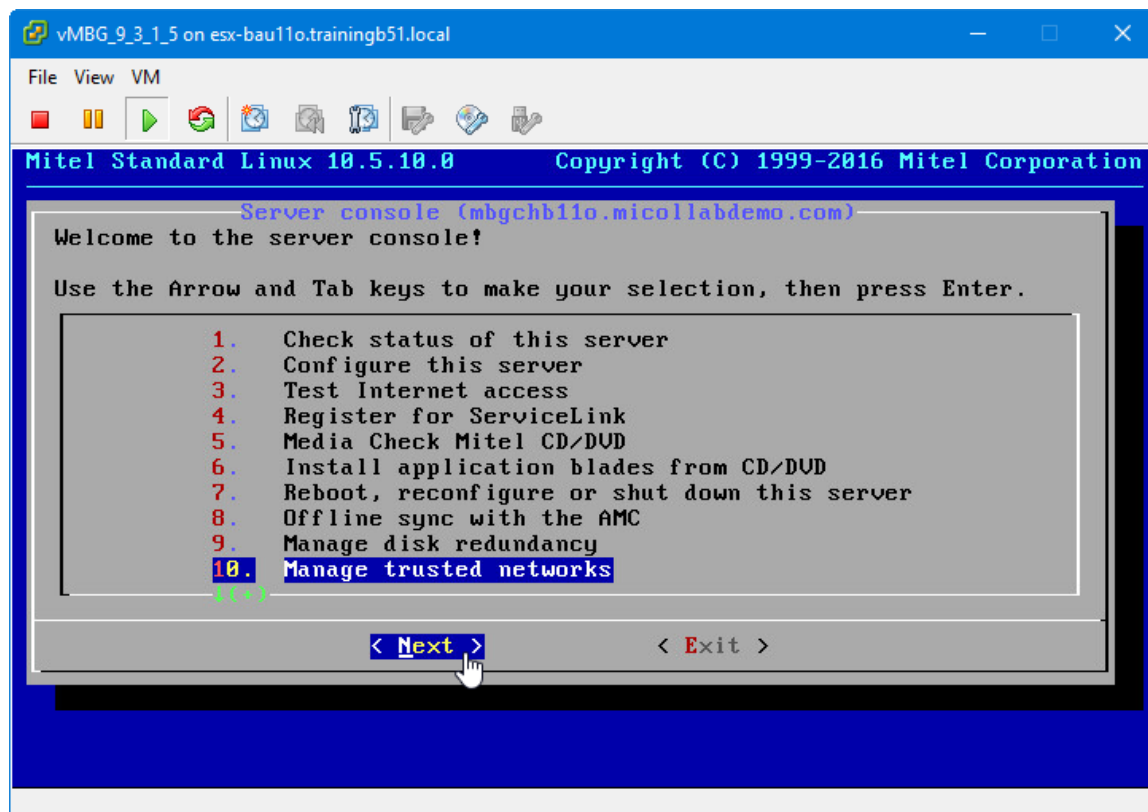
The system is successfully installed :-)

## 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	<b>sync.mitel-amc.com</b>	Default FQDN of AMC for synchronisation of the purchased licenses
TCP port to use for AMC connection	<b>22</b>	Default port

The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbg10-b11o-mitel-ch.eu` with a 'Certificate error' warning. The page title is 'Mitel Standard Linux' and the user is logged in as 'admin@mbg-10.b11o-10.mitel-ch.eu' with a 'Status: Clear' indicator.

The left sidebar contains the following navigation links:

- 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

The main content area is titled 'ServiceLink Activation'. It contains the following text:

In addition to the standard features of this server software, you can now take advantage of ServiceLink, an integrated suite of network-delivered services that enhance the security, reliability and functionality of your server. ServiceLink delivers critical system-management services including 24 x 7 monitoring and status reports, virus protection with automatic updates, point-and-click IPSEC Virtual Private Networks, guaranteed e-mail delivery and DNS services.

To read more about the benefits of ServiceLink, please visit <http://www.mitel.com/>.

To activate ServiceLink, you will require a service account ID which can be obtained from your authorized reseller. If you have already obtained a service account ID, please enter that ID now.

If this server does not have Internet connectivity to the Mitel Application Management Center (AMC), you must use the offline license generation process. To do this, select the *Enable offline license generation* checkbox below and press the *Activate* button.

The activation form includes the following fields:

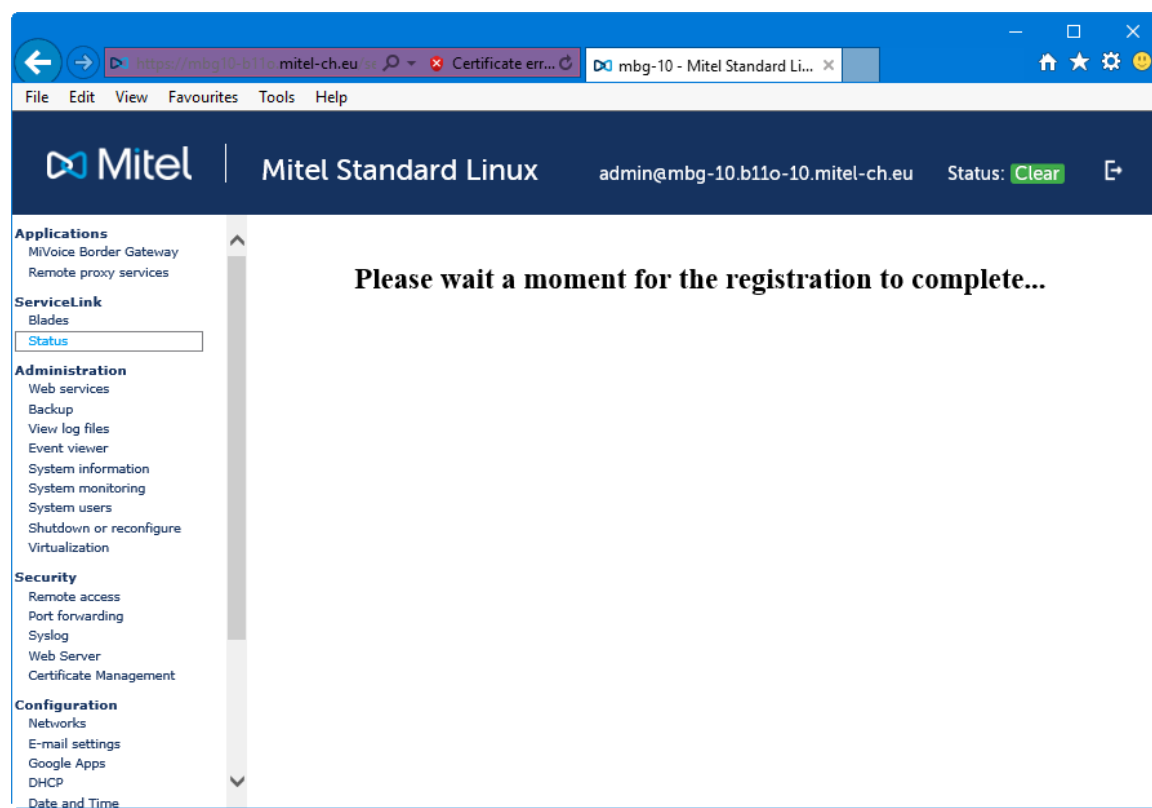
- Service account ID:** 12707414
- Address of Mitel AMC or proxy (optional):** (empty field)
- TCP port to use for AMC connection (optional):** (empty field)
- Enable offline license generation:** ☐

An 'Activate' button is located at the bottom right of the form.

At the bottom of the page, the following text is displayed:

Mitel Standard Linux 10.5.6.0  
MiVoice Border Gateway 9.3.0.14  
© Mitel Networks Corporation

The browser address bar at the bottom shows the URL: `https://mbg10-b11o.mitel-ch.eu/server-manager/cgi-bin/service_status`.



The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbg10-b11o-mitel-ch.eu` with a 'Certificate error' warning. The page title is 'Mitel Standard Linux' and the user is logged in as `admin@mbg-10.b11o-10.mitel-ch.eu` with a 'Status: Clear' indicator.

The left sidebar contains the following navigation menu:

- 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

The main content area is titled 'Operation status report' and contains the following information:

**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

At the bottom of the main content area, there is a 'Sync' button and the following version information:

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.

The screenshot shows the Mitel Standard Linux web interface. The left sidebar contains a menu with categories: Applications, ServiceLink, Administration, Security, and Configuration. Under 'Applications', 'Remote proxy services' is highlighted with a red box. The main content area is titled 'Configure Web Proxy & Remote Management Service'. It includes tabs for 'LAN server proxy list', 'Users', and 'Supported applications'. The 'LAN server proxy list' tab is active, showing a table with the following data:

Enabled	WAN-side FQDN	Allowed netblocks	Server type		
✓	trainingchb11o.micollabdemo.com	All	MiCollab server with the following user level access enabled: MiCollab Client MiCollab MiCollab Audio, Web and Video Conferencing Deployment Unit Admin level access is disabled	Modify	Delete

The 'Modify' link in the table is highlighted with a red box and a mouse cursor. The URL at the bottom of the browser window is <https://mbgchb11o.micollabdemo.com/server-manager/django/webproxy/modify/1/>.

Go to "Remote proxy services".

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

click "Modify"

The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbgchb11o.micollabdemo.com/serve`. The page title is "Configure Web Proxy & Remote Management Service". The left sidebar contains navigation links for Applications, ServiceLink, Administration, Security, and Configuration. The main content area shows the "LAN server proxy list" tab. The "Enabled" checkbox is checked and highlighted with an orange box. Below it, the "WAN side FQDN" is set to `trainingchb11o.micollabdemo.com`. The "What kind of LAN server are you configuring?" section has "MiCollab" selected. The "Which user interfaces would you like to enable access to?" section has "MiCollab", "MiCollab Client", "MiCollab Unified Messaging", and "Deployment Unit" checked. At the bottom, the "Save" button is highlighted with an orange box.

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

### Configure Web Proxy & Remote Management Service

LAN server proxy list Users Supported applications

» Location: LAN server proxy list / Modify

Welcome to the Remote proxy services administrative interface. From here you can manage all aspects of the Web Proxy's behaviour. If at any time you require more information, click the Help icon in the upper-right corner of the page.

The following form permits configuration of a proxy to a single LAN server. None of the other fields will apply to change the server's behaviour unless the "Enabled" checkbox is also checked.

Enabled ☒

WAN side FQDN trainingchb11o.micollabdemo.com

What kind of LAN server are you configuring?

- ☒ MiCollab
- ☐ MiVoice Business
- ☐ MiCollab Client
- ☐ MiCollab Unified Messaging
- ☐ generic MSL admin only
- ☐ Open Integration Gateway
- ☐ Oria
- ☐ MiContact Center
- ☐ MiVoice Call Recording

Which user interfaces would you like to enable access to?

- ☒ MiCollab
- ☒ MiCollab Client
- ☐ MiCollab Unified Messaging
- ☒ Deployment Unit

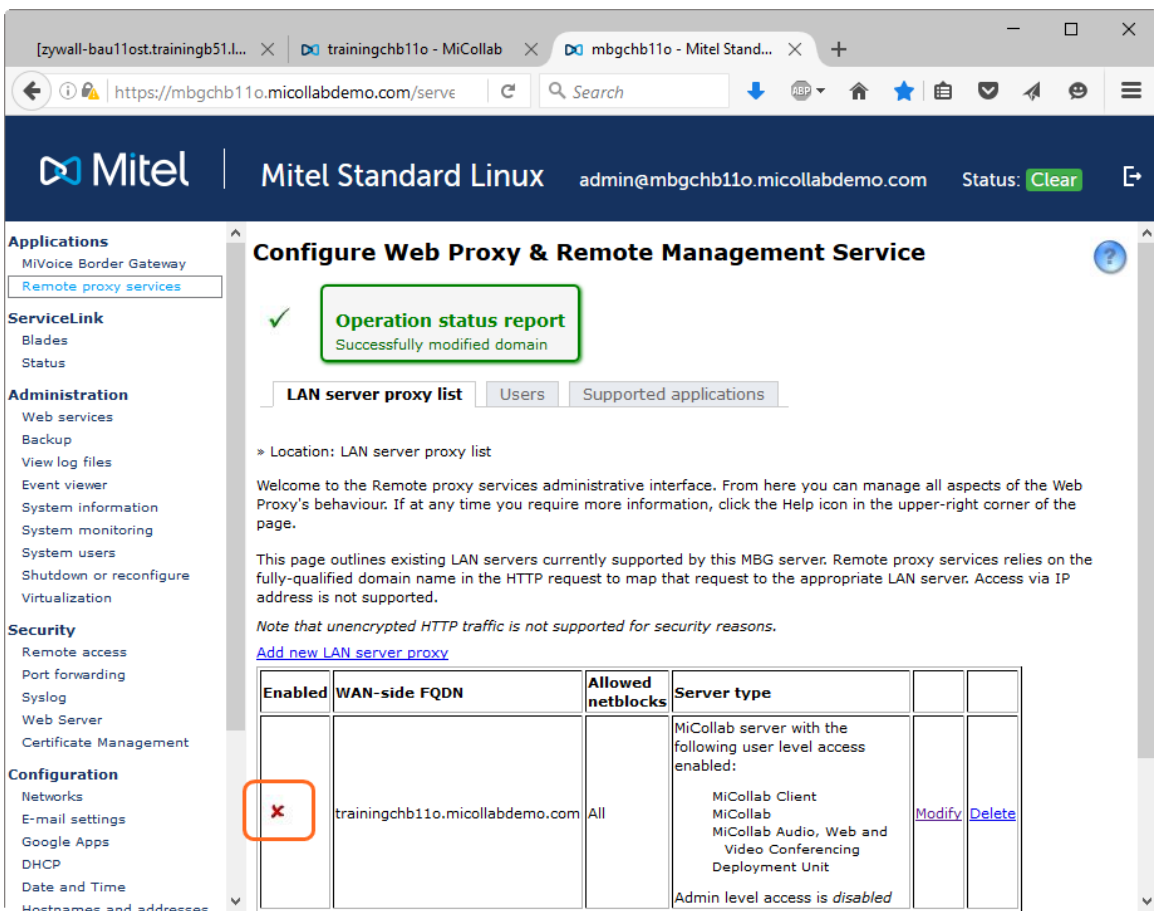
What networks should be able to access it? All

Save

Mitel Standard Linux 10.5.9.0  
MiVoice Border Gateway 9.3.0.17  
© Mitel Networks Corporation

Remove the "Enabled" tick.

Save



**Configure Web Proxy & Remote Management Service**

✓ **Operation status report**  
Successfully modified domain

**LAN server proxy list** | Users | Supported applications

» Location: LAN server proxy list

Welcome to the Remote proxy services administrative interface. From here you can manage all aspects of the Web Proxy's behaviour. If at any time you require more information, click the Help icon in the upper-right corner of the page.

This page outlines existing LAN servers currently supported by this MBG server. Remote proxy services relies on the fully-qualified domain name in the HTTP request to map that request to the appropriate LAN server. Access via IP address is not supported.

*Note that unencrypted HTTP traffic is not supported for security reasons.*

[Add new LAN server proxy](#)

Enabled	WAN-side FQDN	Allowed netblocks	Server type		
<input checked="" type="checkbox"/>	trainingchb11o.micollabdemo.com	All	MiCollab server with the following user level access enabled: MiCollab Client MiCollab MiCollab Audio, Web and Video Conferencing Deployment Unit Admin level access is disabled	<a href="#">Modify</a>	<a href="#">Delete</a>

**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	<p>Enter the common name to which you plan to apply your certificate. A web browser checks this field. It is required.</p> <p>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.</p>
Alternate Name(s)	<p>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.</p> <p><b>Note:</b> You may specify subject alternate names, separated by space. Currently Let's Encrypt does not accept IP addresses and wildcard names.</p>

The screenshot shows the Mitel Standard Linux web interface for managing a Web Server Certificate. The left sidebar contains navigation links for Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled 'Manage Web Server Certificate' and includes a 'Let's Encrypt Certificate Authority' section. The 'Status' is 'enabled'. The 'Contact E-Mail' field is 'peter.andraschko@mitel.com'. The 'Common Name' field is 'trainingchb11o.micollabdemo.com'. The 'Alternate Name(s)' field contains 'mbgchb11o.micollabdemo.com' and 'sspchb11o.micollabdemo.com'. A 'Get Certificate' button is highlighted with a red box, and a 'Return to Main Page' button is also visible.

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.

The screenshot shows a web browser window with the URL `https://mbgchb11o.micollabdemo.com/server-manager/`. The page title is "Mitel Standard Linux" and the user is logged in as `admin@mbgchb11o.micollabdemo.com`. The status is "Clear".

The left sidebar contains the following menu items:

- 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

The main content area is titled "Manage Web Server Certificate" and shows the "Web Server Certificate" tab selected. A green box highlights the "Operation Status Report" which states: "Let's Encrypt is processing the request." Below this, the "Let's Encrypt Certificate Authority" section explains that Let's Encrypt is a free, automated, and open certificate authority (CA). The status is "enabled". The "Contact E-Mail" is `peter.andraschko@mitel.com` and the "Common Name" is `trainingchb11o.micollabdemo.com`. The "Alternate Name(s)" field contains `mbgchb11o.micollabdemo.com`. At the bottom, there are buttons for "Get Certificate" and "Return to Main Page".



The screenshot shows the Mitel Standard Linux web interface for managing certificates. The left sidebar lists various system functions. The main panel is titled 'Manage Web Server Certificate' and shows details for a Let's Encrypt certificate. The certificate information is as follows:

Field	Value
Issuer	Let's Encrypt Authority X3
Certificate Name	trainingchb11o.micollabdemo.com
Alternate Name(s)	mbgchb11o.micollabdemo.com, trainingchb11o.micollabdemo.com
Valid From	Jul 11 12:44:00 2016 GMT
Expires	Oct 9 12:44:00 2016 GMT

Below this, the 'Third Party Certificate' section shows 'Using Let's Encrypt certificate authority' is selected. The status is 'enabled' with a 'last transaction: complete'. The contact email is 'peter.andraschko@mitel.com'. The common name is 'trainingchb11o.micollabdemo.com' and the alternate name is 'mbgchb11o.micollabdemo.com'. A 'Modify Request' button is present. At the bottom, there are 'Get Certificate' and 'Remove Certificate' buttons.

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.

The screenshot displays the Mitel Standard Linux web interface for managing the web server certificate. The browser address bar shows the URL `https://mbgchb11o.micollabdemo.com/server-manager/`. The page header includes the Mitel logo, the text "Mitel Standard Linux", the user email `admin@mbgchb11o.micollabdemo.com`, and a status indicator "Clear".

The left sidebar contains a navigation menu with categories: Applications, ServiceLink, Administration, Security, and Configuration. The "Web Server" option under "Configuration" is selected.

The main content area is titled "Manage Web Server Certificate". It states: "The following web server certificate is currently installed:". Below this, a table lists the certificate details:

<b>Issuer:</b>	Let's Encrypt Authority X3
<b>Certificate Name:</b>	trainingchb11o.micollabdemo.com
<b>Alternate Name(s):</b>	mbgchb11o.micollabdemo.com trainingchb11o.micollabdemo.com
<b>Valid From:</b>	Jul 11 12:44:00 2016 GMT
<b>Expires:</b>	Oct 9 12:44:00 2016 GMT

Below the table, the "Third Party Certificate" section is visible, which is currently empty. At the bottom of the page, there are two buttons: "Get Certificate" and "Remove Certificate".

## 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**.

The screenshot shows the Mitel Standard Linux web interface. The left sidebar contains a navigation menu with sections: 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), and a top status bar showing 'Mitel Standard Linux', 'admin@mbgchb11o.micollabdemo.com', and 'Status: Clear'.

The main content area is titled 'Manage Web Server Certificate' and shows the details of the currently installed Let's Encrypt certificate:

Issuer:	Let's Encrypt Authority X3
Certificate Name:	trainingchb11o.micollabdemo.com
Alternate Name(s):	mbgchb11o.micollabdemo.com trainingchb11o.micollabdemo.com
Valid From:	Jul 11 12:44:00 2016 GMT
Expires:	Oct 9 12:44:00 2016 GMT

Below this, the 'Third Party Certificate' section indicates 'Using Let's Encrypt certificate authority (free certificate)'. A text block explains that Let's Encrypt is a free, automated, and open certificate authority (CA) and that certificates are standard Domain Validation certificates monitored and renewed automatically.

At the bottom, there are two buttons: 'Get Certificate' and 'Remove Certificate'. The 'Remove Certificate' button is highlighted with an orange rectangle and a mouse cursor, indicating the action to be taken.

## 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

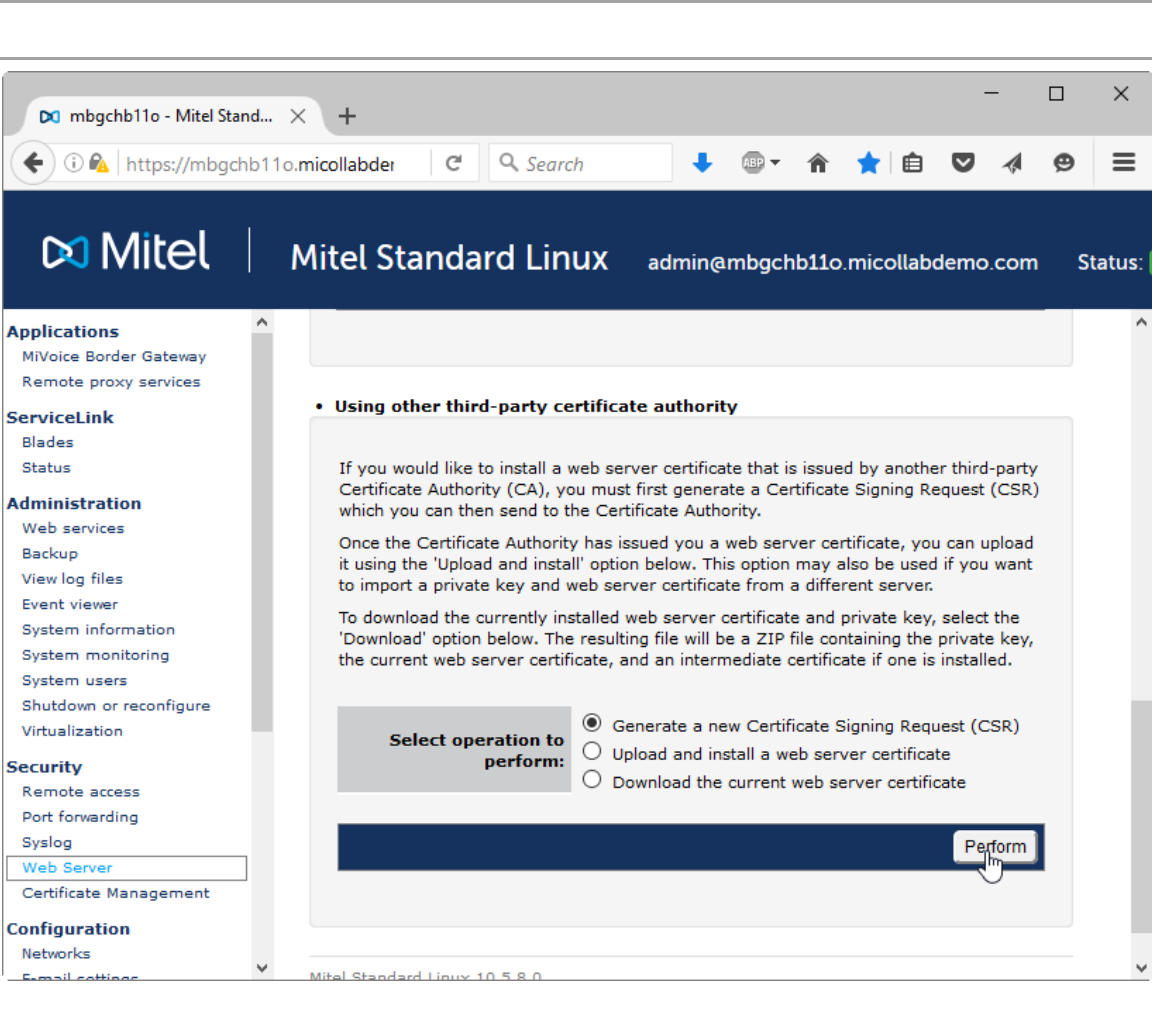
The screenshot shows the Mitel Standard Linux web interface. The left sidebar contains a navigation menu with sections: Applications, ServiceLink, Administration, Security, and Configuration. The 'Web Server' option under the 'Security' section is highlighted with a red box. The main content area is titled 'Manage Web Server Certificate' and shows the details of the currently installed self-signed certificate. The details are as follows:

<b>Issuer:</b>	mbgchb11o.micollabdemo.com
<b>Certificate Name:</b>	mbgchb11o.micollabdemo.com
<b>Alternate Name(s):</b>	*.micollabdemo.com 192.168.6.90 mbgchb11o mbgchb11o.micollabdemo.com micollabdemo.com
<b>Valid From:</b>	Jun 22 09:22:09 2016 GMT
<b>Expires:</b>	Jun 20 09:22:09 2026 GMT

Below the certificate details, there is a section for 'Third Party Certificate' with a bullet point: 'Using Let's Encrypt certificate authority (free certificate)'. The status of the certificate is shown as 'disabled'.

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

Scroll down



The screenshot shows the Mitel Standard Linux web interface. The left sidebar contains a navigation menu with sections: Applications, ServiceLink, Administration, Security, and Configuration. The 'Web Server' option under 'Administration' is highlighted. The main content area is titled 'Using other third-party certificate authority' and contains instructions on how to generate a CSR. Below the instructions, there are three radio button options: 'Generate a new Certificate Signing Request (CSR)' (which is selected), 'Upload and install a web server certificate', and 'Download the current web server certificate'. At the bottom right of this section is a 'Perform' button, which is being clicked by a hand cursor.

Select "Generate a new CSR"

and click "Perform"

The screenshot shows a web browser window with the URL `https://mbgchb11o.micollabdemo.com/server-manager/`. The page title is "Mitel Standard Linux" and the user is logged in as `admin@mbgchb11o.micollabdemo.com`. The status is "Clear".

The left sidebar contains the following menu items:

- 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

The main content area is titled "Manage Web Server Certificate" and has tabs for "Web Server Certificate" and "TLS".

The instructions state: "To generate a Certificate Signing Request, supply the information requested in the form below. This information is supplied to the Certificate Authority and will be validated by them before your certificate is issued. Be careful to ensure the accuracy of the information supplied as it can not be changed once it has been submitted to the Certificate Authority. If you have previously generated a Certificate Signing Request, the values previously entered will be displayed below."

The form fields are as follows:

- Country Name (2 letter code): CH
- State or Province Name (full name): Switzerland
- Locality Name (eg, city): Solothurn
- Organization Name (eg, company): Mitel Switzerland Ltd
- Organizational Unit Name (eg, section): Training
- Common Name (eg, your server's hostname): trainingchb11o.micollabdemo.com

At the bottom of the form, there are two buttons: "Cancel" and "Generate Certificate Signing Request". A mouse cursor is pointing at the "Generate Certificate Signing Request" button.

The footer of the page indicates "Mitel Standard Linux 10.5.8.0".

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"

mbgchb11o - Mitel Stand... X +

https://mbgchb11o.micollab Search

Mitel Mitel Standard Linux admin@mbgchb11o.micollabdemo.com Statu

**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**  
Support and licensing

### Manage Web Server Certificate

Your generated Certificate Signing Request (CSR) is displayed below.

You should copy the data in the shaded box below (including the lines that contain -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----) and provide it to your Certificate Authority.

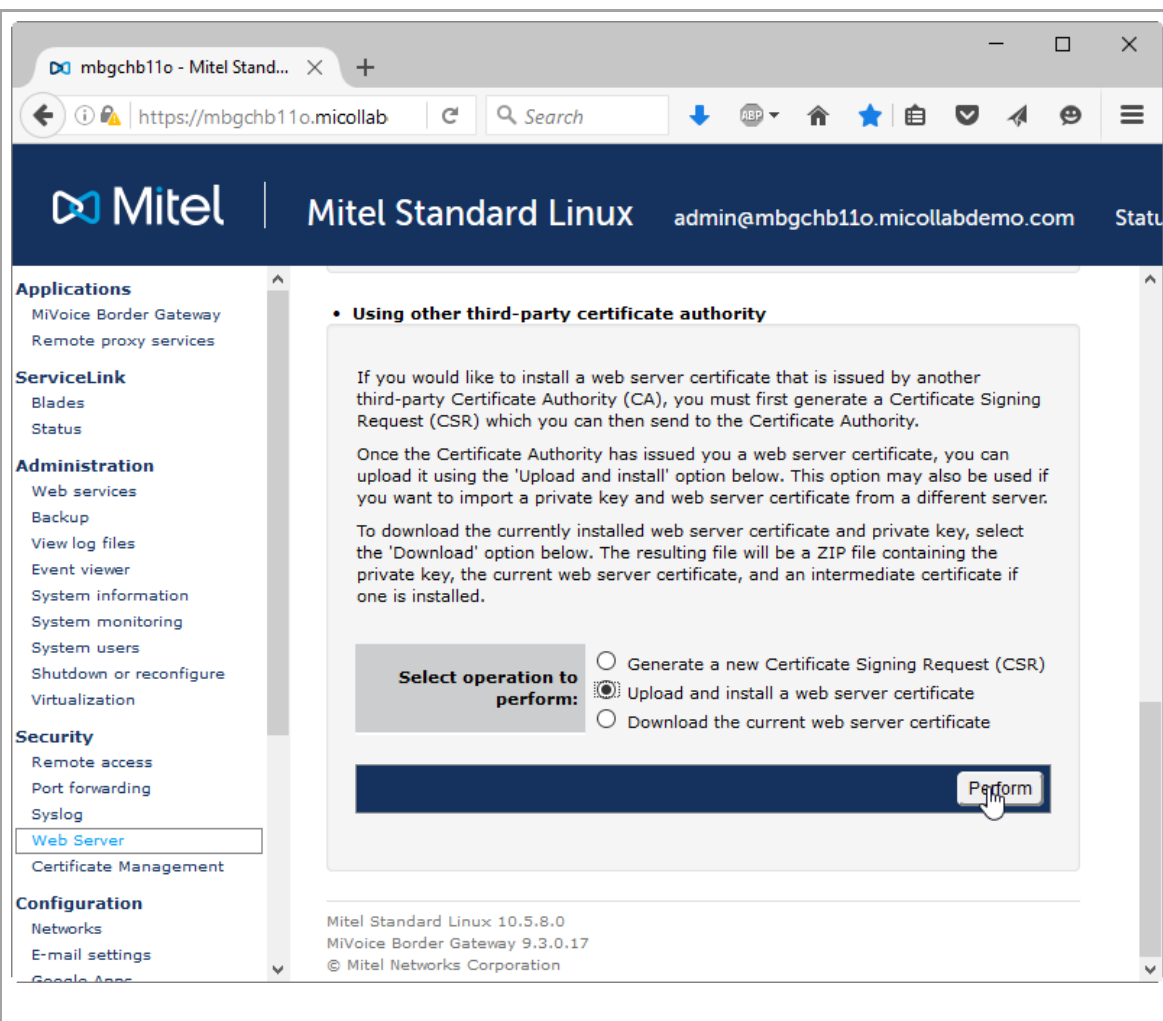
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC2jCCAcICAQAwZQxCzAJBgNVBAYTAkNIMRQwEgYDVQQIDAtTd2l0emVyYb6Fu
ZDESMBAGA1UEBwwJU29sb3RodXJuMR4wHAYDVQQKDBVNaXRlbCBTd2l0emVyYb6Fu
ZCBMdGQxETAPBgNVBAsMCFRyYmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
by5tawNvbGxhYmRlbW8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA7qwi3NQsDKWdx/vpTDHqQ0R4cSoWSB9WnZ/5CrKGZQJ7/M/CBLMT9EBS35W
x/Khzyrg/XAKF55T2YVb26SeDE019rN3gu56PnseUV66jh3Zi0Y0l0IcnSPFKVN+
eZjK/j9ttk98P3S0UrxK3WJnV9fmQ5N4dPbbv//5GDokcH0E95RbB10Ub06HztLx
spewgAXVC3Ap5w4VnfRo0ZsEWayyykZ0JX8bh9YvT1T/pBzVbSrS87pFmApRB7CO
x1s2SikwIm8IhMFG4jq+C/jz9j2uIk/KtLPzLt1omHsy1uYwfMJACNbxihZX5nFY
NgOX7S350enMvqAn0EgDy6tJIQIDAQABAAwDQYJKoZIhvcNAQELBQADggEBAAej
eO3fqhWnsdZqfTpHhCDYP5Fr8FAK+g1v2WdUEEjiJfgxVMzk0ilomab8Ih60YNQ/
IiHot7JpVRVtrKe3H0NQIm1/vX6EfyW4hkVDEUU4MNTxZpLl1f7qDEF1usFz0ug
tWP6Gfdabv+vIYQw8X+3N6Kfy1pH42GhWh6iDCkVkr0TzRwWQwzZt1Scfl6PYrX
pb5BHHYmtFye15cd/FzNHhLrXmNCKhoKpkqK9NO+1kZGh0B3Yv58uhE9+3TxuUvF
HHgB+uu5m0ovUTrkKfzIXyXIKczF9PE5jWUbX5PeTQDUsoYkK3Z9HFzGnUgjysja
XbX0alxBk1YhiJYYe5c=
-----END CERTIFICATE REQUEST-----
```

Return to Main Page

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



The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbgchb11o.micollab`. The page header includes the Mitel logo, the title "Mitel Standard Linux", the email address `admin@mbgchb11o.micollabdemo.com`, and a "Status" link. The left sidebar contains a navigation menu with sections: 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), and Configuration (Networks, E-mail settings, Google Apps). The main content area is titled "Using other third-party certificate authority" and contains the following text:

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

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

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

**Select operation to perform:**

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

A "Perform" button is located at the bottom right of the form.

At the bottom of the page, the version information is displayed: Mitel Standard Linux 10.5.8.0, MiVoice Border Gateway 9.3.0.17, and © Mitel Networks Corporation.

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



The screenshot shows a web browser window with the URL `https://mbgchb11o.micollab`. The page title is "Mitel Standard Linux" and the user is logged in as `admin@mbgchb11o.micollabdemo.com`. The left sidebar contains a navigation menu with sections: 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), and Configuration (Networks, E-mail settings, Google Apps, DHCP, Date and Time, Hostnames and addresses, Domains, IPv6-in-IPv4 Tunnel). The main content area is titled "Manage Web Server Certificate" and has tabs for "Web Server Certificate" and "TLS". The "Web Server Certificate" tab is active. The page contains the following text and form fields:

Once you have received the web server certificate from the Certificate Authority (CA), you may upload the certificate using this form. Browse to the file containing the issued SSL certificate in the first field below.

Some Certificate Authorities may require you to install an intermediate certificate. If your Certificate Authority has provided an intermediate certificate to use, specify the intermediate certificate in the second field below.

Note: the web certificate must be in PEM format or in PKCS12/PFX format (.pfx or .p12 file).

**SSL Certificate:**  01\_wildcard.micollabdemo.com.cert.pem

**Intermediate SSL Certificate (if supplied):**  02\_intermediate-certs.pem

You may also upload a private key file if you are importing a private key and web server certificate from a different server. If you are uploading a web server certificate that is provided by a Certificate Authority as a result of generating a Certificate Signing Request (CSR) on this server, you should not specify a private key here.

**SSL Private Key (if applicable):**  No file selected.

At the bottom of the form are two buttons: "Cancel" and "Install Web Server Certificate". A mouse cursor is pointing at the "Install Web Server Certificate" button.

At the very bottom of the page, the following text is displayed:

Mitel Standard Linux 10.5.8.0  
MiVoice Border Gateway 9.3.0.17  
© Mitel Networks Corporation

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.

The screenshot shows a web browser window with the URL `https://mbgchb11o.micollab`. The page title is "Mitel Standard Linux" and the user is logged in as `admin@mbgchb11o.micollabdemo.com`. The left sidebar contains a navigation menu with sections: Applications, ServiceLink, Administration, Security, and Configuration. The "Web Server" option under the Security section is selected. The main content area is titled "Manage Web Server Certificate" and contains the following text:

Once you have received the web server certificate from the Certificate Authority (CA), you may upload the certificate using this form. Browse to the file containing the issued SSL certificate in the first field below.

Some Certificate Authorities may require you to install an intermediate certificate. If your Certificate Authority has provided an intermediate certificate to use, specify the intermediate certificate in the second field below.

Note: the web certificate must be in PEM format or in PKCS12/PFX format (.pfx or .p12 file).

The form has three fields:

- SSL Certificate:** Browse... 01\_wildcard.micollabdemo.com.cert.pem
- Intermediate SSL Certificate (if supplied):** Browse... 02\_intermediate-certs.pem
- SSL Private Key (if applicable):** Browse... 03\_wildcard.micollabdemo.com.key.pem

Below the fields, there is a paragraph explaining that a private key file should be uploaded if it is imported from a different server, but not if it was generated on this server as part of a CSR.

At the bottom of the form, there are two buttons: "Cancel" and "Install Web Server Certificate". The "Install Web Server Certificate" button is highlighted with a mouse cursor.

At the very bottom of the page, the following version information is displayed:

Mitel Standard Linux 10.5.8.0  
MiVoice Border Gateway 9.3.0.17  
© Mitel Networks Corporation

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

The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbgchb11o.micollab`. The page header includes the Mitel logo and the text "Mitel Standard Linux" with the user email `admin@mbgchb11o.micollabdemo.com`. The left sidebar contains a navigation menu with sections: Applications, ServiceLink, Administration, Security, and Configuration. The "Web Server" option under the "Configuration" section is highlighted. The main content area is titled "Manage Web Server Certificate" and shows a green checkmark and a box labeled "Operation Status Report" with the text "Web server certificate installed successfully". Below this, it states "The following web server certificate is currently installed:" and displays a table of certificate details. The table is outlined with an orange border. The details include: Issuer: RapidSSL SHA256 CA - G3, Certificate Name: \*.micollabdemo.com, Alternate Name(s): \*.micollabdemo.com, micollabdemo.com, Valid From: Dec 20 12:00:05 2015 GMT, and Expires: Dec 22 14:15:01 2017 GMT. Below the table, there is a section for "Third Party Certificate" with a bullet point for "Using Let's Encrypt certificate authority (free certificate)". This section contains a paragraph about Let's Encrypt and a "Status" field set to "disabled". Other fields include "Contact E-Mail" (peter.andraschko@mitel.com), "Common Name" (trainingchb11o.micollabdemo.com), and "Alternate Name(s)". A "Modify Request" button is at the bottom.

<b>Issuer:</b>	RapidSSL SHA256 CA - G3
<b>Certificate Name:</b>	*.micollabdemo.com
<b>Alternate Name(s):</b>	*.micollabdemo.com micollabdemo.com
<b>Valid From:</b>	Dec 20 12:00:05 2015 GMT
<b>Expires:</b>	Dec 22 14:15:01 2017 GMT

The installed certificate is directly visible.

## MBG: System configuration: Network profile

The screenshot displays the Mitel Standard Linux web interface. The browser address bar shows the URL `https://mbg10-b11o.mitel-ch.eu/server-manager/` with a 'Certificate error' warning. The page title is 'Mitel Standard Linux' and the user is logged in as 'admin@mbg-10.b11o-10.mitel-ch.eu' with a 'Clear' status button.

The left sidebar contains a navigation menu with categories: Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The 'System configuration' tab is selected, and a dropdown menu is open, highlighting 'Network profiles'. Other options in the dropdown include Settings, Port ranges, IP blocking, IP Translations, MiNet fallback addresses, Bandwidth management, Connectors, and Overrides.

The main content area shows the 'MBG status' section with a table of system settings:

Enabled	Disabled
<b>Network profile</b>	Mode not set
<b>Daisy-chain mode</b>	No
<b>Set-side streaming addresses</b>	
<b>Icp-side streaming addresses</b>	
<b>Calls in progress</b>	Minet: , SIP: , Trunk:
<b>Active MiNet/SIP connections</b>	
<b>MiNet support</b>	Minet: TCP/PSK, TCP/TLS
<b>WebRTC support</b>	Disabled
<b>SIP support</b>	Disabled
<b>Call recording support</b>	Disabled

Below the status table is the 'Clustering status' section, which includes a note: 'Note: Clustering is not currently possible as MBG's primary service is not running. You must start it above.' It also provides instructions for creating or joining a cluster, with 'Create a cluster' and 'Join a cluster' buttons.

The 'License information' section at the bottom shows a table of license details:

Availability and usage	License type	Total local	Total local in use
Teleworker licenses		5	
Tap licenses:		0	
hk licenses:		0	

The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbgchb11o.m`. The page title is "Mitel Standard Linux" with the user `admin@mbgchb11o.micollabdemo.com` and a "Status: Clear" indicator. The left sidebar contains the following navigation categories:

- 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
  - MBG client certificates
- 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**
  - Support and licensing
  - Help

The main content area shows the "Network profile (Custom mode)" configuration page. It includes a status bar indicating the page was updated on Wed Apr 04 2018 08:09:32 GMT+0200 (W. Europe Summer Time) and a prompt to "Configure this server in...". The configuration options are:

- Server-gateway configuration on the network edge (disabled)
- Server-only configuration on the network DMZ (disabled)
- Server-only configuration on the network LAN (disabled)
- Custom configuration (selected)

A red error message states: "No WAN IP found, S/G configuration not possible." Below the configuration options, there is a button labeled "Enter Daisychain Mode".

Chose Custom configuration

The screenshot shows the Mitel Standard Linux web interface. The browser address bar displays `https://mbgchb11o.micollabdemo.com/server-nt`. The page title is "Mitel Standard Linux" with the user `admin@mbgchb11o.micollabdemo.com` and a "Status: Clear" indicator. The left sidebar contains navigation menus for Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled "Network profile (Custom mode)" and includes a "Server-gateway configuration on the network edge" section with a red error message: "No WAN IP found, S/G configuration not possible." Below this are sections for "Server-only configuration on the network DMZ" and "Server-only configuration on the network LAN". The "Custom configuration" section contains text explaining that manual streaming addresses may be required and provides two input fields: "RTP ICP-side override addresses" (192.168.6.90) and "RTP Set-side override addresses" (212.101.18.182). An "Apply Custom configuration" button is highlighted with a mouse cursor. At the bottom, there is an "Enter Daisychain Mode" button and version information: "Mitel Standard Linux 10.6.2.0", "MiVoice Border Gateway 10.1.0.187", and "© Mitel Networks Corporation".

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

The screenshot displays the Mitel Standard Linux web interface. The browser address bar shows the URL `https://mbgchb11o.micollabdemo.com/server-man...`. The page header includes the Mitel logo, the text "Mitel Standard Linux", the user email `admin@mbgchb11o.micollabdemo.com`, and a "Status: Clear" button.

The left sidebar contains a navigation menu with the following sections:

- 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
  - Phonnet Code

The main content area shows the "System configuration" tab selected. A dropdown menu is open under "System configuration", listing the following options:

- Settings (highlighted)
- Port ranges
- Network profiles
- IP blocking
- IP Translations
- MiNet fallback addresses
- Bandwidth management
- Connectors
- Overrides

The "MBG status" section displays the following configuration:

Parameter	Value
Enabled	Enabled
Network profile	Custom mode
Daisy-chain mode	No
Set-side streaming addresses	212.101.18.182
Icp-side streaming addresses	192.168.6.90
Calls in progress	Minet: 0, SIP: 0, Trunk: 0
Active MiNet/SIP connections	1
MiNet support	Disabled
WebRTC support	Disabled

The "Clustering status" section shows:

- Cluster status: Clustered: **slave**
- Manage cluster buttons: Resync with master, Take ownership, Leave cluster
- Default zone: Configured MiNet devices: Backup: Default

The bottom of the page shows the URL `https://mbgchb11o.micollabdemo.com/server-manager/django/teleworker/advanced/`.

<div> <div>Service parameters</div> <div> <div>TFTP enabled <input checked="" type="checkbox"/></div> <div>TFTP blocksize 4096 bytes</div> <div>ICP failure detection <input checked="" type="checkbox"/></div> <div>SSL ciphers TLS 1.2 compatability</div> <div>DSCP setting for voice Expedited forwarding</div> <div>DSCP setting for video Assured forwarding 41</div> <div>DSCP setting for signaling Class selector 5</div> </div> </div>	<p>SSL cipher: TLS 1.2</p> <p>DSCP values: You can keep default values or change like shown here to match with the settings of MiVO400.</p>
<div> <div>MiNet options</div> <div> <div> <div>MiNet support</div> <div>TCP <input type="checkbox"/></div> <div>TCP/PSK <input type="checkbox"/></div> <div>TCP/TLS <input type="checkbox"/></div> <div>HTML application support</div> <div>TCP/TLS <input type="checkbox"/></div> <div>SAC support</div> <div>TCP <input type="checkbox"/></div> <div>TCP/TLS <input type="checkbox"/></div> <div>Security profile Legacy mode</div> <div>Restrict MiNet devices <input checked="" type="checkbox"/></div> <div>Time format 12 hour</div> </div> <div> <div>Local streaming <input type="checkbox"/></div> <div>Codec support Restricted to G.729, G.71</div> <div>Force set-side codec Disabled</div> <div>RTP framesize Dynamic</div> <div>Ping before redirect enabled <input type="checkbox"/></div> <div>Reboot fallback enabled <input type="checkbox"/></div> <div>Retry backoff interval(s) 60</div> <div>Pings to send 1</div> <div>Successful pings 1</div> <div>Ping packet size 64</div> <div>Ping Timeout 800</div> </div> </div> </div>	<p>Remove all ticks. No MiNet phones will be used.</p>



**SIP options**

SIP support	Protocols	Access profile
Certificate: <b>Web s</b>	UDP <input type="checkbox"/> Public TCP <input checked="" type="checkbox"/> Private TCP/TLS <input checked="" type="checkbox"/> Public	

Registration Mode: Max Set-Side

Set-side registration expiry time: 240

ICP-side registration expiry time: [ ]

Allowed URI names: Add another

Blank any field you no longer want.

Tone injection: Enabled ☐

SIP adaptation support: ☐

SIP adaptation receive pipeline: [ ]

SIP adaptation send pipeline: [ ]

KPML username: [ ]

KPML password: [ ]

Confirm KPML password: [ ]

Permit weak SIP passwords: ☐

Device: device local streaming

Device: trunk local streaming

Codec support: **Unrestricted**

RTP framesize: Dynamic

**Set-side RTP security**

Inbound: **SRTP only** (Accept only SRTP inbound to this server)

Outbound: **SRTP only** (Send only SRTP outbound from this server)

Preferred cipher: AES\_CM\_128\_HMAC\_SHA1\_32

**ICP-side RTP security**

Inbound: ☐ SRTP only (Accept only RTP (plaintext) inbound to this server)

☐ SRTP or RTP

☒ RTP only

Outbound: ☐ SRTP only (Send only RTP (plaintext) outbound from this server)

☐ AVP+crypto

☒ RTP only

Preferred cipher: AES\_CM\_128\_HMAC\_SHA1\_32

**PRACK support** ☒

Send options keepalives: Only behind NAT

Options interval: 20

Challenge methods: Invite, Subscribe, Refer, Prack

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

<div data-bbox="813 228 875 285"><p>Save</p></div> <div data-bbox="190 303 412 371"><p>Mitel Standard Linux 10.6.2.0 MiVoice Border Gateway 10.1.0.187 © Mitel Networks Corporation</p></div>	<p>Don't forget to "Save"</p>
---	-------------------------------

## MBG: System configuration: Port ranges

The screenshot shows the Mitel Standard Linux web interface. The top navigation bar includes the Mitel logo, 'Mitel Standard Linux', the user 'admin@mbgchb11o.micollabdemo.com', and a 'Status: Clear' indicator. The left sidebar contains a menu with categories: 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), and Configuration (Networks, E-mail settings, Google Apps, DHCP, Date and Time, Hostnames and addresses, Domains). The main content area shows the 'System configuration' menu with a dropdown open, highlighting 'Port ranges'. Other options in the dropdown include Settings, Network profiles, IP blocking, IP Translations, MiNet fallback addresses, Bandwidth management, Connectors, and Overrides. The background configuration page shows various settings like MBG status (Enabled), Network profile (Custom mode), Daisy-chain mode (No), Set-side streaming addresses (212.101.18.182), Icp-side streaming addresses (192.168.6.90), Calls in progress (Minet: 0, SIP: 0, Trunk: 0), Active MiNet/SIP connections (1), MiNet support (Disabled), WebRTC support (Disabled), Load average (5 min) (1.47), SIP support (Enabled: UDP, TCP, TCP/TLS), and Call recording support (Disabled). At the bottom, there is a 'Clustering status' section with a '+ Node' button and a 'Cluster status' section with 'Clustered: slave' and buttons for 'Resync with master', 'Take ownership', and 'Leave cluster'. The footer shows the URL 'https://mbgchb11o.micollabdemo.com/server-manager/django/teleworker/advanced/portranges/' and 'Configured MiNet devices: Backup: Default'.

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

<div><b>MiNet and SIP port ranges</b></div> <div><div>SRTP starting port 20000</div><div>Video starting port 21950</div><div>SRTP/Video ending port 21999</div></div> <div><div>Number of supported calls</div><div>487 pure audio and 12 with video</div></div>	<p>Note:</p> <ul style="list-style-type: none"><li>• At least half of the total number of ports must be allocated to audio.</li><li>• The Video starting port must be greater than the SRTP starting port and less than or equal to the SRTP/Video ending port.</li><li>• The SRTP/Video ending port must be less than the WebRTC public starting port.</li></ul>
<div>Save</div>	"Save"

## MBG: Service configuration: ICPs

The screenshot displays the Mitel Standard Linux web interface. The browser tabs include 'zywall-bau110st.training...', 'mbgchb11o - Mitel Sta...', 'MiVoice Border Gateway', and 'MiVoice Office 400'. The address bar shows 'https://mbgchb11o.micollabdemo.com/server-manager'. The page header includes the Mitel logo, 'Mitel Standard Linux', the user 'admin@mbgchb11o.micollabdemo.com', and a 'Status: Clear' button.

The left sidebar contains the following navigation categories:

- 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

The main content area shows the 'Service configuration' tab selected. A dropdown menu is open, listing the following options: ICPs, MiNet devices, SIP users, SIP trunking, WebRTC, and Application integration. The 'ICPs' option is highlighted. Below the dropdown, the 'MBG status' section is visible, showing 'Enabled' and 'Network profile'. The 'Set-side streaming addresses' and 'Icp-side streaming addresses' are listed. The 'Calls in progress' section shows 'Minet: 0, SIP: 0, Trunk: 0'. The 'Active MiNet/SIP connections' section shows '1'. The 'MiNet support' and 'WebRTC support' are both 'Disabled'. The 'Security profile' is 'Legacy'. The 'WAN IPs' and 'LAN IPs' are listed. The 'Third IPs' section is empty. The 'Calls per hour' section shows 'MiNet: 0, SIP: 0, Trunk: 0'. The 'Load average (5 min)' is '0.86'. The 'SIP support' is 'Enabled: UDP, TCP, TCP/TLS'. The 'Call recording support' is 'Disabled'. The 'Clustering status' section shows 'Cluster status' as 'Clustered: slave' and 'Manage cluster' buttons: 'Resync with master', 'Take ownership', and 'Leave cluster'. The 'Default zone' is 'Default'. The footer shows the URL 'https://mbgchb11o.micollabdemo.com/server-manager/django/teleworker/icps/' and the text 'Configured MiNet devices: Backup: Default'.

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

System status Service configuration System configuration Administration

Page updated: Tue Jul 12 2016 13:39:48 GMT+0200 (W. Europe Standard Time)

To test connectivity to your configured ICPs, or to run a DNS resolution test on configured hostnames, see the [Diagnostics](#) page.

ICP Information

Default for	Default for SIP	Name	Hostname or IP address	Type	Installer password	SIP capabilities	Indirect call

Add a new ICP (PBX)

Manage ICP

Name:

Type:

SIP capabilities:

Hostname or IP address:

MiNet installer password:

Indirect call recording capable: ☐

MiVoice Office 400 support

Link to this ICP? ☒ Enable ☒

XML listen port:  TLS? ☒

XML destination port:  TLS? ☒

Save

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"



MiVoice Office 400

mlx-10

Welco

System overview

Configuration

Summary

Users

Terminals

System

General

Access control

Cards and modules

Interfaces

DECT/SIP-DECT

Media resources

Dual Homing

Extended

Routing

Services

IP network

Private networking

Apply

Reload

Date and time

System date02.09.2016

System time08:15:42

System time zone(GMT+01:00) Amsterdam, Ber

Time synchronisation via ISDN network

Time synchronisation via time server using NTP (network time protocol)

NTP service

NTP serverch.pool.ntp.org

Communication server

Site namemlx-10

System ID5AE28839FC3400DD20

System language

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

## MBG: Administration: File transfer

The screenshot displays the Mitel Standard Linux Administration web interface. The top navigation bar includes the Mitel logo, the text "Mitel Standard Linux", the user email "admin@mbgchb11o.micollabdemo.com", and a "Status: Clear" indicator. The left sidebar contains a menu with categories: 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), and Configuration (Networks, E-mail settings, Google Apps, DHCP, Date and Time, Hostnames and addresses).

The main content area shows the "Administration" tab selected, with a dropdown menu open displaying "Logging", "Diagnostics", "File transfers" (highlighted by a mouse cursor), and "Alarms". Below the menu, the "MBG status" section is visible, showing various system parameters and their status. The "Clustering status" section is also partially visible at the bottom.

Page updated: Tue Sep 12 2017 08:49:42 GMT+0200 (W. Europe Standard Time)

MBG status	
<b>Enabled</b>	Enabled
<b>Network profile</b>	Custom mode
<b>Daisy-chain mode</b>	No
<b>Set-side streaming addresses</b>	212.101.18.182
<b>Icp-side streaming addresses</b>	192.168.6.90
<b>Calls in progress</b>	Minet: 0, SIP: 0, Trunk: 0
<b>Active MiNet/SIP connections (local / cluster-wide)</b>	1 / 1
<b>MI Net support</b>	Disabled
<b>WebRTC support</b>	Enabled

Security profile	
<b>Legacy</b>	
<b>WAN IPs</b>	192.168.6.90
<b>LAN IPs</b>	192.168.6.90
<b>Third IPs</b>	Minet: 0, SIP: 0, Trunk: 0
<b>Calls per hour</b>	0.1
<b>Load average (5 min)</b>	0.1

SIP support	
<b>SIP support</b>	Enabled: TCP, TCP/TLS
<b>Call recording support</b>	Disabled

**Clustering status**

+ Node

Cluster status	
<b>Cluster status</b>	Clustered: slave
<b>Manage cluster</b>	Resync with master Take ownership
	Leave cluster

+ Zone



Page updated: Tue Sep 12 2017 08:51:35 GMT+0200 (W. Europe Standard Time)

**File transfers**

**Teleworker Network Analyzer**

Download TNA

**Fetch logs for product support**

Fetch logs

**MiNet CSV import/export**

MiNet backup

Browse... No file selected.

MiNet restore

**SIP CSV import/export**

SIP backup

Browse... No file selected.

SIP restore

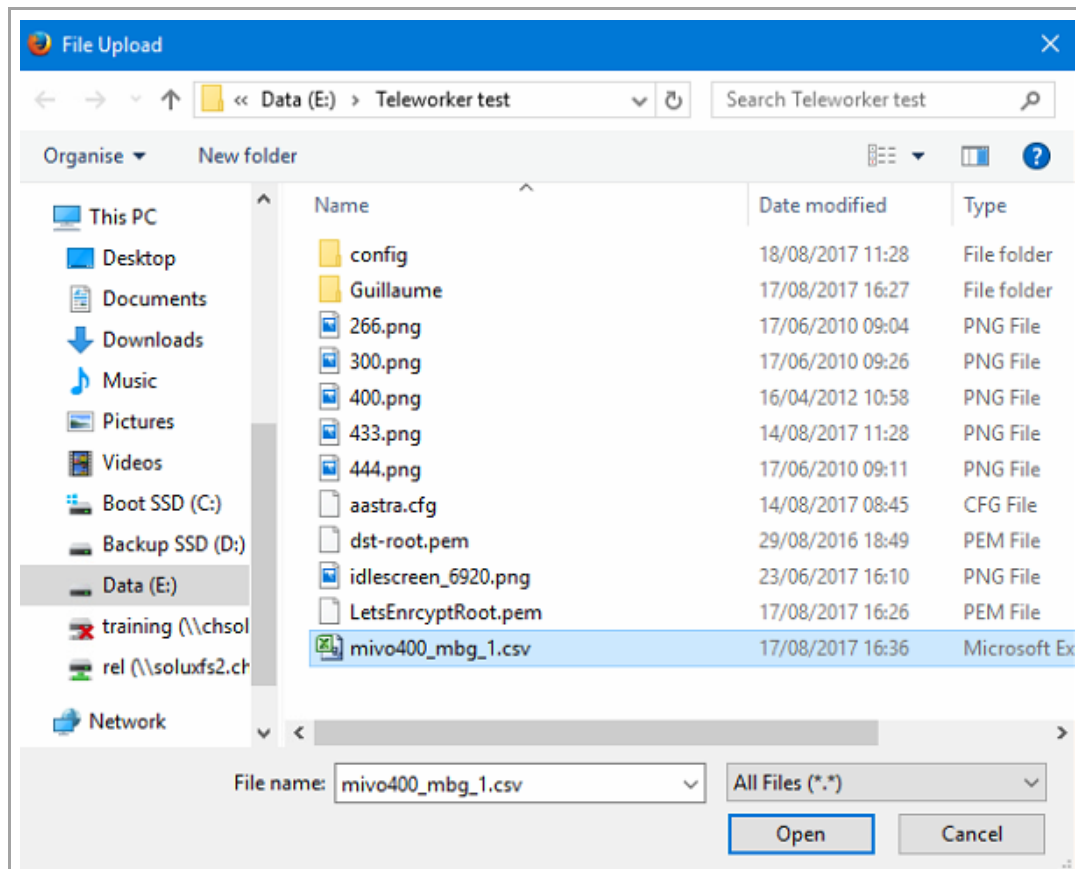
**Application metrics CSV export**

App metrics export

**System metrics CSV export**

System metrics export

Click "Browse..." for SIP CSV import.



Select the file  
"mivo400\_mbg\_1.csv"

Page updated: Tue Sep 12 2017 08:51:35 GMT+0200 (W. Europe Standard Time)

**File transfers**

<b>Teleworker Network Analyzer</b>	Download TNA	
<b>Fetch logs for product support</b>	Fetch logs	
<b>MiNet CSV import/export</b>	MiNet backup	Browse... No file selected.
	MiNet restore	
<b>SIP CSV import/export</b>	SIP backup	Browse... mivo400_mbg_1.csv
	SIP restore	
<b>Application metrics CSV export</b>	App metrics export	
	<b>System metrics CSV export</b>	System metrics export

click "SIP restore"

Mitel | Mitel Standard Linux

admin@mbgchb11o.micollabdemo.com Status: CL

**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

MBG client certificates

**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**

System status ▾

Service configuration ▾

System configuration ▾

Administration ▾

ICPs

MiNet devices

**SIP users**

SIP trunking

WebRTC

Application integration

SIP adaptation

Trust store

Page updated  
Below is the list of SIP users.

Note, to import a CSV file, please see the File transfers page.

20

Simple filter

Bulk edit Refresh

Page 1 of 1

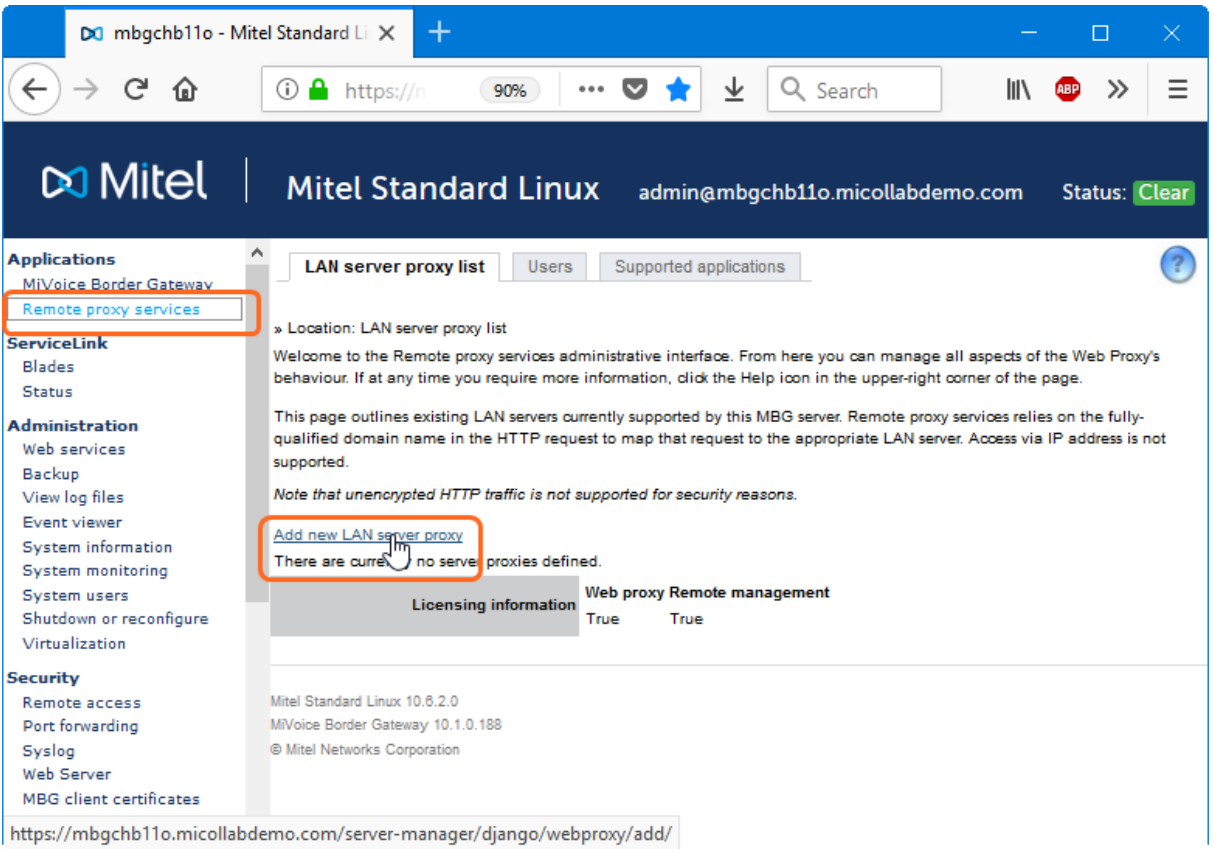
**Device information**

Enabled	Set-side username	ICP-side username	Availability	Configured ICP	Description	Local streaming between devices	Log verbosity		
✓	435-w0	435-sv	Everywhere	mx-10	Mitel 6867	Use master setting	Use master setting		
✓	447-hl	447-H5	Everywhere	mx-10	Mitel 6873	Use master setting	Use master setting		
✓	202-bm	202-bi	Everywhere	mx-10	6869-202	Use master setting	Use master setting		
✓	433-60	433-Zh	Everywhere	mx-10	Mitel 6869	Use master setting	Use master		

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.



The screenshot displays the Mitel Standard Linux administrative interface. The left sidebar contains a tree view with categories: Applications, ServiceLink, Administration, and Security. Under 'Applications', 'Remote proxy services' is highlighted with a red box. The main content area is titled 'LAN server proxy list' and includes a 'Users' tab and a 'Supported applications' tab. The text on the page states: '» Location: LAN server proxy list', 'Welcome to the Remote proxy services administrative interface. From here you can manage all aspects of the Web Proxy's behaviour. If at any time you require more information, click the Help icon in the upper-right corner of the page.', 'This page outlines existing LAN servers currently supported by this MBG server. Remote proxy services relies on the fully-qualified domain name in the HTTP request to map that request to the appropriate LAN server. Access via IP address is not supported.', and 'Note that unencrypted HTTP traffic is not supported for security reasons.' A link 'Add new LAN server proxy' is highlighted with a red box, and a mouse cursor is pointing at it. Below this link, it says 'There are currently no server proxies defined.' At the bottom, there is a 'Licensing information' section and a 'Web proxy Remote management' section with 'True' values. The URL bar at the bottom shows 'https://mbgchb11o.micollabdemo.com/server-manager/django/webproxy/add/'.

Select "Remote proxy services"

Click "Add new LAN server proxy"

mbgchb11o - Mitel Standard Linux

https://... 90%

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  
MBG client certificates

**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**  
Support and licensing  
Help

**LAN server proxy list** Users Supported applications

» Location: LAN server proxy list / Add

Welcome to the Remote proxy services administrative interface. From here you can manage all aspects of the Web Proxy's behaviour. If at any time you require more information, click the Help icon in the upper-right corner of the page.

The following form permits configuration of a proxy to a single LAN server. None of the other fields will apply to change the server's behaviour unless the "Enabled" checkbox is also checked.

**Enabled** ☒

WAN-side FQDN trainingchb11o.micollab

LAN-side FQDN trainingchb11o.micollab Note, this can be left blank to default to the same as the Virtual host

What kind of LAN server are you configuring?

☐ MiCollab  
☐ MiVoice Business  
☐ MiCollab Client  
☐ MiCollab Unified Messaging  
☐ generic MSL admin only  
☐ Open Integration Gateway  
☐ MiCloud Management Portal  
☐ MiContact Center  
☐ MiVoice Call Recording  
☒ **MiVoice Office 400 Self-Service Portal**

☐ MiCollab  
☐ MiCollab Client  
☐ MiCollab Unified Messaging  
☐ Deployment Unit  
☐ MiCollab Audio, Web and Video Conferencing  
☐ Listen port for MiCollab AWW (2 WAN IPs)  
☐ Listen port for MiCollab AWW (1 WAN IP)  
☐ Google Calendar Integration to AWW

Which user interfaces would you like to enable access to?

Do you wish to permit remote administrative access? ☐ Yes

What netblocks should be able to access it? All

Save

## 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 screenshot shows the Mitel Standard Linux web interface. The browser address bar displays 'https://trainingchb11o.micollabdemo.com'. The page title is 'Mitel Standard Linux' with the user 'admin@mbgchb11o.micollabdemo.com' and a 'Status: Clear' indicator. The left sidebar contains navigation links for Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled 'Remote proxy services' and features a green 'Operation status report' box stating 'Successfully added domain'. Below this, there is a 'LAN server proxy list' table. The table has four columns: 'Enabled', 'WAN-side FQDN', 'Allowed netblocks', and 'Server type'. The first row shows a checked 'Enabled' checkbox, the FQDN 'trainingchb11o.micollabdemo.com', 'All' for allowed netblocks, and 'MiVoice Office 400 Self-Service Portal' as the server type. The 'Server type' column also includes the text 'MiVoice Office 400 Self-Service Portal' and 'Admin level access is disabled'. At the bottom, there is a 'Licensing information' section showing 'Mitel Standard Linux 10.8.2.0' and 'MiVoice Border Gateway 10.1.0.188'.

Enabled	WAN-side FQDN	Allowed netblocks	Server type
<input checked="" type="checkbox"/>	trainingchb11o.micollabdemo.com	All	MiVoice Office 400 Self-Service Portal server with the following user level access enabled: MiVoice Office 400 Self-Service Portal Admin level access is disabled

**Licensing information**

Mitel Standard Linux 10.8.2.0  
MiVoice Border Gateway 10.1.0.188  
© Mitel Networks Corporation

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>

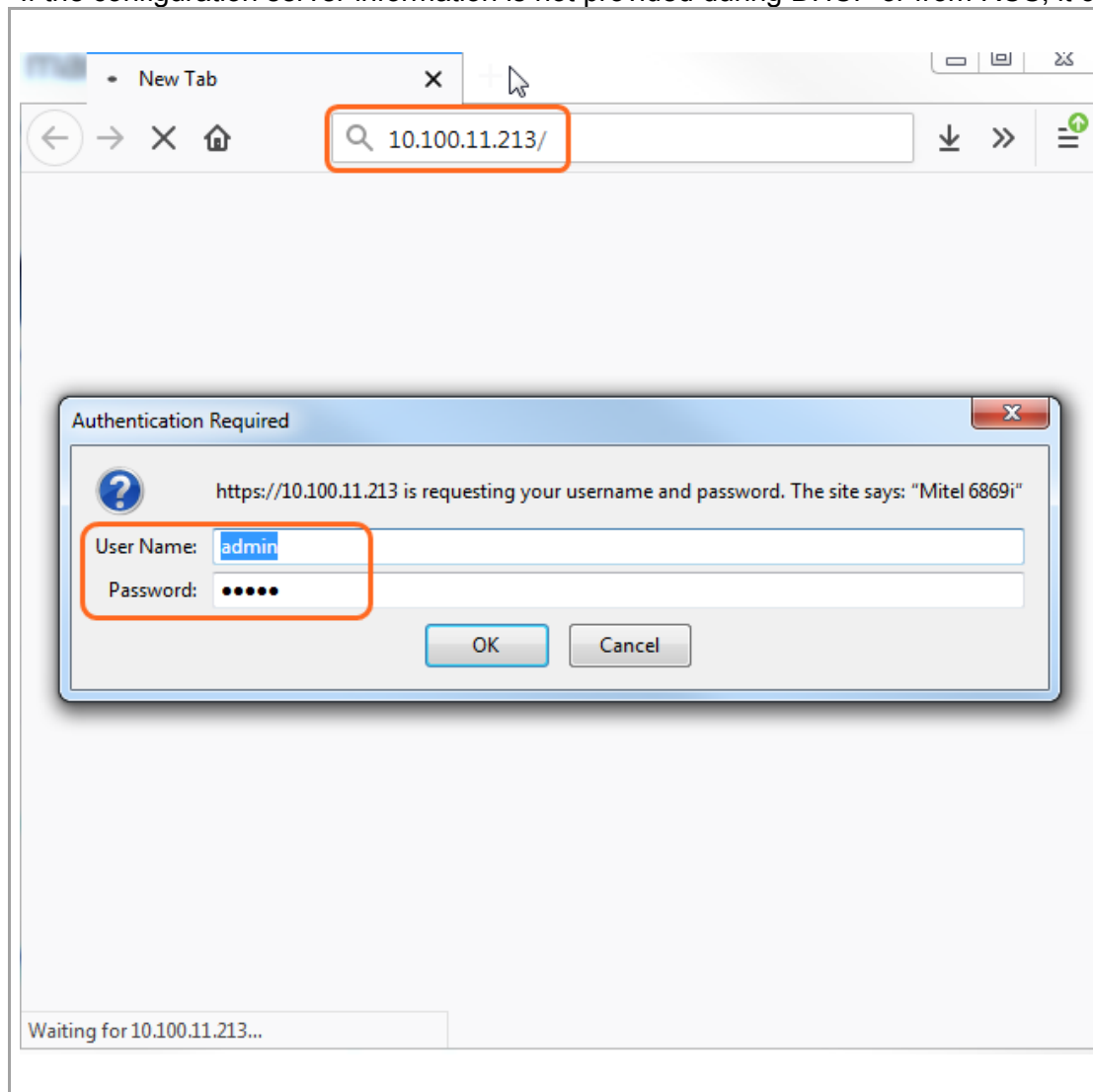
The Mitel SIP phone downloads new firmware, unless it already has it, and will reboot several times.

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

**Mitel** 6869i Log Off

**Status**  
System Information  
License Status

**Operation**  
User Password  
Phone Lock  
Softkeys and XML  
Keypad Speed Dial  
Directory  
Reset  
Expansion Module 1

**Basic Settings**  
Preferences  
Custom Ringtones

**Advanced Settings**  
Network  
Global SIP  
Line 1  
Line 2  
Line 3  
Line 4  
Line 5  
Line 6  
Line 7  
Line 8  
Line 9  
Line 10  
Line 11  
Line 12  
Line 13  
Line 14  
Line 15  
Line 16  
Line 17  
Line 18  
Line 19  
Line 20  
Line 21  
Line 22  
Line 23  
Line 24  
Action URI  
**Configuration Server**  
Firmware Update  
TLS Support  
802.1x Support  
Troubleshooting  
Capture  
Screenshot

### Configuration Server Settings

**Settings**

Download Protocol: HTTP

Primary Server:

Pri TFTP Path:

Alternate Server: 0.0.0.0

Alt TFTP Path:

Use Alt TFTP: ☐ Enabled

FTP Server:

FTP Path:

FTP Username:

FTP Password:

HTTP Server: mbg1.tailor.com

HTTP Path: 10.1.1.20

HTTP Port: 80

HTTPS Server:

HTTPS Path:

HTTPS Port: 443

**Auto-Resync**

Mode: None

Time (24-hour): 00:00

Maximum Delay: 15

Days: 0

**XML Push Server List(Approved IP Addresses)**

Save Settings

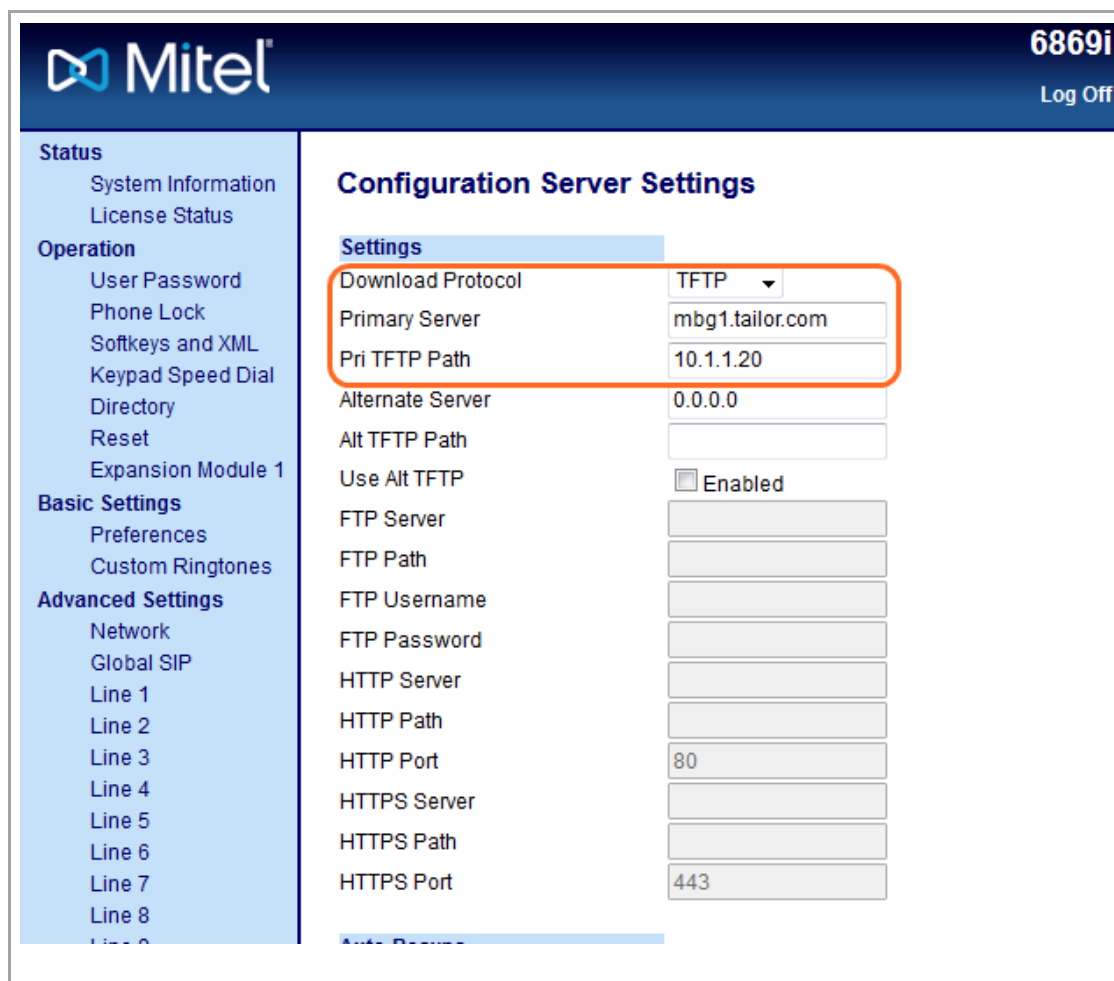
Go to "Configuration Server"

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.



**Mitel** 6869i  
Log Off

**Status**  
System Information  
License Status

**Operation**  
User Password  
Phone Lock  
Softkeys and XML  
Keypad Speed Dial  
Directory  
Reset  
Expansion Module 1

**Basic Settings**  
Preferences  
Custom Ringtones

**Advanced Settings**  
Network  
Global SIP  
Line 1  
Line 2  
Line 3  
Line 4  
Line 5  
Line 6  
Line 7  
Line 8  
Line 9

### Configuration Server Settings

**Settings**

Download Protocol	TFTP
Primary Server	mbg1.tailor.com
Pri TFTP Path	10.1.1.20
Alternate Server	0.0.0.0
Alt TFTP Path	
Use Alt TFTP	<input type="checkbox"/> Enabled
FTP Server	
FTP Path	
FTP Username	
FTP Password	
HTTP Server	
HTTP Path	
HTTP Port	80
HTTPS Server	
HTTPS Path	
HTTPS Port	443


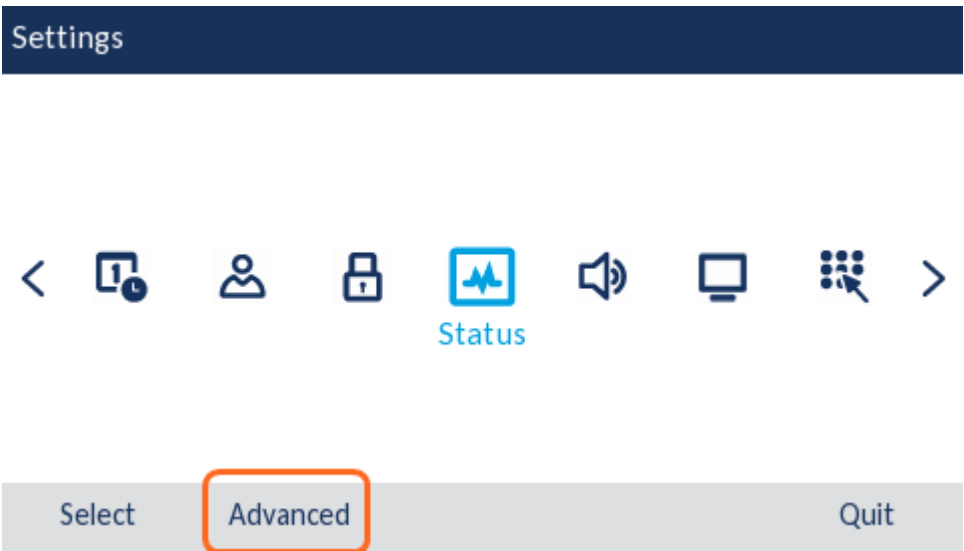
Alternatively (if http access is not available) the configuration server can be reached via TFTP with the settings shown here.

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"

<div data-bbox="188 204 1149 272" data-label="Section-Header"> <h2>Advanced Settings</h2> </div> <div data-bbox="452 343 889 383" data-label="Text"> <p>Enter Administrator Password</p> </div> <div data-bbox="542 389 788 474" data-label="Form"> <input type="password" value="*****"/> </div> <div data-bbox="237 694 331 734" data-label="Text"> <p>Enter</p> </div> <div data-bbox="400 694 546 737" data-label="Text"> <p>Backspace</p> </div> <div data-bbox="999 694 1102 734" data-label="Text"> <p>Cancel</p> </div>	<div data-bbox="1167 204 1494 244" data-label="Text"> <p>Enter password: <b>22222</b></p> </div>
<div data-bbox="188 810 1149 879" data-label="Section-Header"> <h2>Settings</h2> </div> <div data-bbox="201 1021 1133 1158" data-label="Image"> <p>The settings menu bar contains the following icons from left to right: a left arrow, a monitor icon, a grid icon, a server rack icon, a blue square icon with a white document symbol (highlighted with an orange box), a telephone handset icon, a power button icon, a refresh icon, and a right arrow. Below the blue square icon is the text 'Configuration Server'.</p> </div> <div data-bbox="232 1295 333 1335" data-label="Text"> <p>Select</p> </div> <div data-bbox="1012 1295 1090 1337" data-label="Text"> <p>Quit</p> </div>	<div data-bbox="1167 805 1583 847" data-label="Text"> <p>Selected Configuration Server</p> </div>

Configuration Server	
Download Protocol	HTTP
HTTP Server	212.101.18.182
HTTP Port	80
HTTP Path	10.1.1.20
<div>Save    Backspace    ABC ►    Cancel</div>	

Set

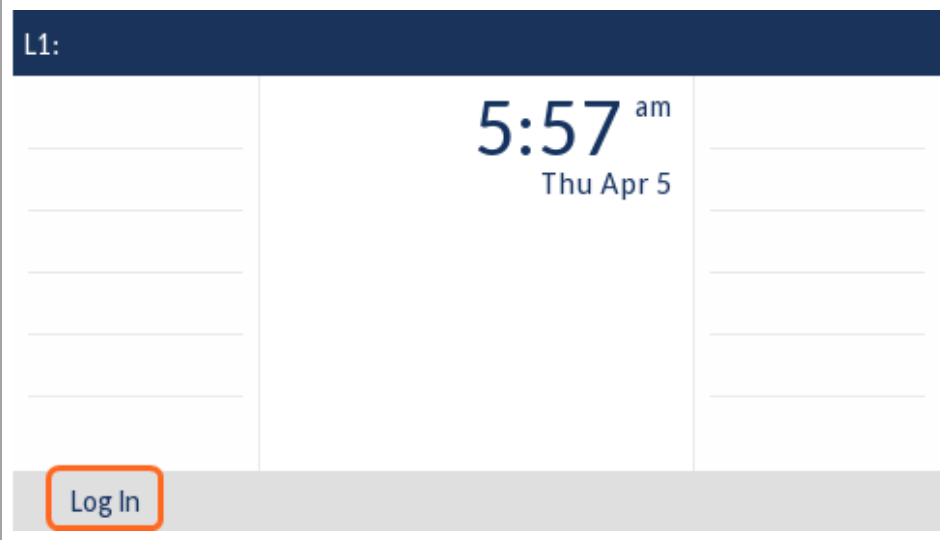
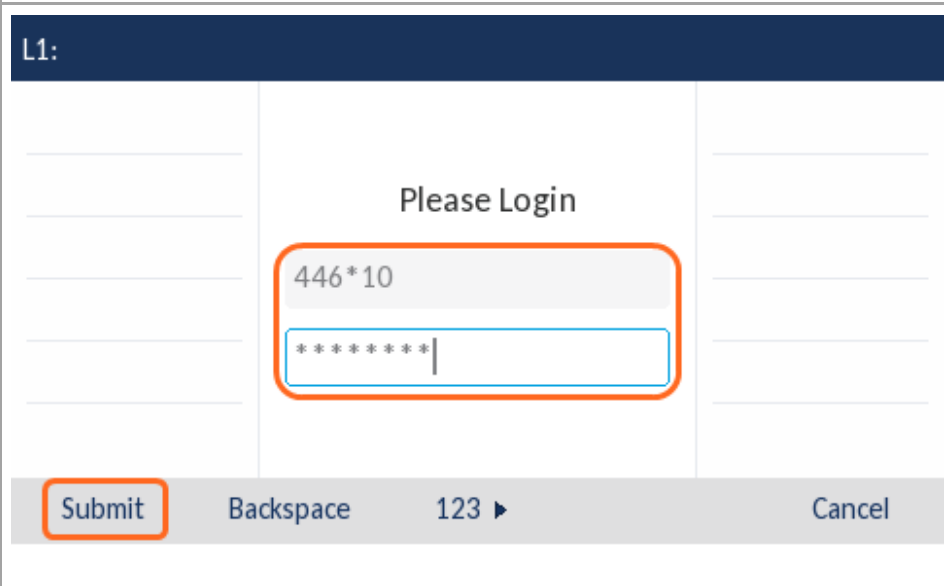
Download Protocol: **HTTP**

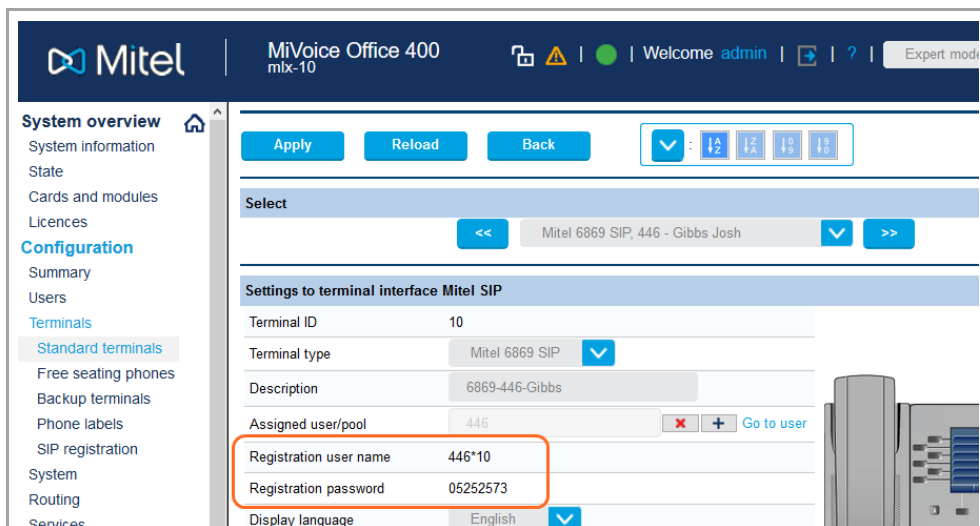
HTTP Server: **<public IP of MBG>**

HTTP Path: **<internal IP of MiVO400>**

Save and reboot the phone

## Login screen

	<p>After some reboots the phone eventually come up with this login screen.</p>
	<p>The user has to enter the</p> <ul style="list-style-type: none"><li>• Registration user name</li><li>• Registration password</li></ul>



The screenshot shows the Mitel MiVoice Office 400 configuration interface. The left sidebar contains a navigation menu with sections: System overview, Configuration, and Terminals. Under Configuration, there are links for Summary, Users, and Terminals. Under Terminals, there are links for Standard terminals, Free seating phones, Backup terminals, Phone labels, SIP registration, System, Routing, and Services. The main content area is titled 'Settings to terminal interface Mitel SIP'. It includes a 'Select' dropdown menu showing 'Mitel 6869 SIP, 446 - Gibbs Josh'. Below this, there are fields for Terminal ID (10), Terminal type (Mitel 6869 SIP), Description (6869-446-Gibbs), Assigned user/pool (446), Registration user name (446\*10), Registration password (05252573), and Display language (English). The Registration user name and Registration password fields are highlighted with a red rectangle.

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.