A MITEL
PRODUCT
GUIDE

MiCollab Client Deployment

Release 9.5
May 2022

Mitel
Powering connections

Notices

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

Trademarks

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

®,™ Trademark of Mitel Networks Corporation

© Copyright 2022, Mitel Networks Corporation

All rights reserved

Contents

MiCollab Client Deployment 1

This chapter contains the following sections:

1.1 Getting Started

1.1.1 About MiCollab Client Deployment

This blade supports the simplified deployment of MiCollab for Mobile Client. This solution is supported in integrated and co-located MiCollab Client deployments.

End users are no longer required to enter configuration settings such as server and SIP credentials. Administrators configure these settings and MiCollab for Mobile Clients are deployed Over the Air (OTA). The administrator portal enables administrators to:

- deploy large groups
- leverage profiles
- download multiple files to the clients
- update clients.

Note:

The **User Tab** elements in the “MiCollab Client Deployment” application should **NOT** be used to create or manage MiCollab Release 7.0 or later clients.

You use the MiCollab Client Deployment service to configure the deployment parameters, change the default deployment profile, or to run the diagnostics. After you have configured the MiCollab Client Deployment service when you create a user on the communication platform, the service automatically deploys the user's MiCollab for Mobile Client. The following is a summary of the behavior for each platform:

MiVoice Business (Integrated Mode)

You create and modify users from the Users and Services application. Only phones types “UC Endpoint” and “External Hot Desk” can be deployed. Whenever you select a deployment profile in the Users and Services application, the user gets deployed automatically. To send out a Deployment email again, Deploy the user from the Users and Services application.

MiVoice Business (Collocated Mode)

You create and modify users from the MiCollab Client Service. After a user is created, it is automatically added to the deployment and an email is send out. An email address must be configured for the user. You re-send a Deployment email from the “MiCollab Client Deployment” Users Tab.

If existing users (Pre-MiCollab Release 7.0) need to be deployed, they can be added using the Users > Import Users function. Note that this is an advanced task that should be performed by an experienced administrator.

MiVoice MX-ONE

You create and modify users in the **Users** > **User** > **Add** page of the MiVoice MX-ONE Provisioning Manager. Users are assigned with an “MiCollab role”. The Role is mapped on the MiCollab Server to the User Template, which determines the Deployment Profile. The users are then deployed automatically. There is no need to import users.

MiVoice 5000

You create and modify users in the **GUI Telephony service** > **Subscribers** > **Subscriptions** > **Characteristics** page of the MiVoice 5000 Provisioning Manager. Users are assigned with an “MiCollab role”. The Role is mapped on the MiCollab Server to the User Template, which determines the Deployment Profile. The users are then deployed automatically. There is no need to import users.

MiVoice Office 400

You create users in the **Users** > **User list** > **New** page of the MiVoice Office 400 Web Admin (Expert mode). Users are assigned with an “MiCollab role”. The Role is mapped on the MiCollab Server to the User Template, which determines the Deployment Profile. The users are then deployed automatically. There is no need to import users.

1.1.2 Deploy Client with MiVoice Business or MiVoice Business Express

The deployment procedure that you used depends on if MiCollab Client is configured in Integrated Mode or in Co-located Mode. Note that MiVoice Business Express only supports MiCollab Client in Integrated Mode.

1.1.2.1 MiCollab Client in Integrated Mode

To deploy MiCollab for Mobile Clients with MiVoice Business or MiVoice Business Express:

1. Define deployment configuration and configure MiCollab Client Deployment.
2. Purchase and install SSL Web Server Certificate.
3. Add connections to MBGs.
4. Add profiles.
5. Run the Diagnostic test to:
   - confirm the connection to the Redirect Server, and
   - validate that the MiCollab Clients on the public Internet can reach the MiCollab Client Deployment service.
6. Customize deployment email.
7. Add the MiCollab Client for Mobile softphone user through the Users and Services application:
   - Log into the MiCollab server manager.
   - Under **Applications**, click **Users and Services**.
   - Click **Quick Add**.
   - Select the default UCC (Vx.0) Premium role or create a custom role and template from the Premium template. The template must have a Teleworker license and the MiCollab Client Feature Profile must be licensed for Mobile SIP Softphone.

     When you add Teleworker service to a user's device, the system automatically configures a corresponding SIP service on the MiVoice Border Gateway. Note the following:

     - The system sets the **Set-side username** on the MiVoice Border Gateway to <username-DN> (for example smithj-7328).
     - You must set the password field in the template to "Use Random Password" or "Use This Value. If you select "Use This Value", the password value must be a strong password.

Note:

The user will be deployed with the default deployment profile. If you want to use a custom default profile, create a custom template from the Premium template and select the desired profile in the template.

- Enter the user's first and last name.
- Enter the user's primary e-mail address.
- Under **Other Phone**, enter the extension number.
- Click **Save**.
- The user downloads the client from the store and scans the code in the deployment e-mail with their cell phone to initiate activation. The MiCollab for Mobile Client deployment configuration is downloaded to the user's cell phone.

1.1.2.2 MiCollab Client in Co-located Mode

To deploy MiCollab for Mobile Clients with MiVoice Business (not applicable to MiVoice Business Express):

1. Define deployment configuration and configure MiCollab Client Deployment.
2. Add connections to MBGs.
3. Add profiles.
4. Run the diagnostic test to:
   - confirm the connection to the Redirect Server, and
   - validate that the MiCollab Clients on the public Internet can reach the MiCollab Client Deployment service.
5. Customize deployment email.
6. Program the user on the MiVoice Business with an Other Phone configured as a softphone (UC Endpoint):
   - Log into the MiVoice Business system administration.
   - Under **Users and Services**, click **Users and Services Configuration**.
   - Click **Add** > **by Role** and select a role that supports multiple phones.
   - Configure the user entry. Under **Service Profile**, set **Hot Desking User** to **No** and set the **Device Type** to **UC Endpoint**.
   - Click **Save Changes**.

7. Synchronize the MiCollab Client database with the MiVoice Business database to obtain the user entry:

   - Log into the MiCollab server manager.
   - Under **Applications**, click **MiCollab Client Service**, and then click **Configure MiCollab Client Service**.
   - Click **PBX Nodes**.
   - Select the box next to the MiVoice Business platform, click **[Synchronize]** and then click **OK**.

8. Add the UC Endpoint for the MiCollab Client for Mobile softphone to the user's account:

   - Log into the MiCollab server manager.
   - Under **Applications**, click **MiCollab Client Service**.
   - Click **Configure MiCollab Client Service**.
   - Click **Accounts**.
   - Use **Search accounts** to locate the user.
   - Configure the users account. Under **Licensed Features** assign the user with the Feature Profile "UCC Vx.0 Premium" or with a custom profile that provides Teleworker and UC Endpoint licenses.

     When you add Teleworker service to UC Endpoint devices the system automatically configures a corresponding SIP service on the MiVoice Border Gateway. Note the following:

     - The system sets the SIP username on the MiVoice Border Gateway to (username_DN) (for example smithj_7328).
     - You must set the password field in the template to "Use Random Password" or "User This Value. If you select "User This Value", the password value must be a strong password.
   - Click **Save**.
   - The user downloads the client from the store and scans the code in the deployment e-mail with their cell phone to initiate activation. The MiCollab for Mobile Client deployment configuration is downloaded to the user's cell phone.

1.1.3 Deploy Client with MV5000 or MV MX-ONE

1. Define deployment configuration and configure MiCollab Client Deployment
2. Purchase and install SSL Web Server Certificate
3. Add connections to MBGs.
4. Add profiles.
5. Customize deployment email.

6. Run the diagnostic test to:
   - confirm the connection to the Redirect Server, and
   - validate that the MiCollab Clients on the public Internet can reach the MiCollab Client Deployment service.
7. The user downloads the client from the store and scans the code in the deployment e-mail with their cell phone to initiate activation.
8. The MiCollab for Mobile Client deployment configuration is downloaded to the user's cell phone.

1.2 Users Tab (Pre-MiCollab 7.0 only)

1.2.1 Manage Users

The **Users** tab allows you to manage and deploy existing, pre-MiCollab Release 7.0 users.

Note:

If you change a user's ID, you need to factory reset and redeploy the MiCollab for Mobile application. A new deployment email needs to be sent to the user.

This tab displays a list of all users that have been manually added, synchronized from MiCollab Client Service,Users and Services Application, MBGs and other applications.

Note:
If this is the first time you have logged into MiCollab Client Deployment, you should connect MBGs for user import before importing user records. Go to Configuration, Connections to MBGs.

Setting	Description
Profile	Shows the deployment profile that is used for a user account. The deployment profile adds deployment settings which are necessary to set up the client software, but are NOT YET specified by the user account information. Go to the Deployment Profiles tab for more information.
Firstname	These pieces of information are most often imported from other applications (such as MBGs), or entered manually. Go to Configuration >> Connections to MBGs to set up these connections. Go to Users >> Import Users to import user account information from the set-up connections.
Lastname	
Number	
MBG SIP User name	The user name as it was imported from the MBG or entered manually.
MiCollab Client Service Account	MiCollab Client Service Account that is associated with the user.
Email address	The email address that will be used to send download links and authentication credentials to a user.
Deployed	Indicates the date and time when the deployment file was sent to a client.
Downloaded	Indicates the date and time when the deployment file was actually downloaded (and installed) for a client.

Sync data: Synchronizes the selected data sets with their source data sets, i.e. the data set residing on the application such as an MBG if a user was imported.

Auto deploy: This can be used to “set force config” for clients which have already been deployed (settings downloaded) and at the same time deploy to new users.

Deploy: Deploys the configuration (download link or QR-Code) to the clients, so that users can retrieve the new configuration (scheduled or user-initiated updates). Please note that the link or QR-Code will be cached by the Redirect Server. User data will never be cached for security reasons. To resend a deployment email to a user, click Deploy.

Set Force Config: This option forces the client to download its configuration from the Client Deployment Service automatically at the next possible opportunity.

Export (CSV): Exports the selected data set(s) into a CSV. The MiCollab Client password, PBX SIP password, Teleworker SIP password and Voicemail PIN will not be exported.

Delete: Deletes the selected user accounts from the Client Deployment.

1.2.2 Importing users

This page provides an integrated view of all user records found on all connected components (Users and Services Application, MBGs, MiCollab Client Service).

All records can be imported to **Users** > **Manage** with the options located at the bottom of the table (available if users have been selected):

1. Select the Deployment Profile you would like to use.
2. Select the header row check box to select all records across all pages, or select the check boxes to the left of every row to select individual records.
3. Select **Import**. If you would like to deploy to users immediately, click **Import and Deploy**.

When MiCollab Client is configured as a stand-alone deployment without MiCollab or an MBG, you must enter the PBX SIP fields manually. See Manually Create Users for more information.

Once the records have been imported, they will appear in the **Manage** view.

Note:

Imported records cannot be modified.

Setting	Description
Firstname	These pieces of information are most often imported from other applications (such as MBGs), or entered manually. Go to **Configuration** > **Connections to MBGs** to set up these connections. Go to **Users** > **Import Users** to import user account information from the set-up connections.
Lastname	
Directory Number	
PBX Number	PBX number or name.
MBG UserName	The user name as it is synced from the MBG or entered manually.
MiCollab Client Service Account	MiCollab Client Service Account that is associated with the user.
E-mail address	The email address that will be used to send download links and authentication credentials to a user.

Note:

To configure the e-mail subject and body, go to Mobile Client deployment e-mail. To use a centralized Deployment e-mail address, edit the deployment profile(s) by clicking **Deployment Profiles** > **Modify**.

Note:

The link or QR-Code will be cached by the Redirect Server. However, even if the default e-mail content residing on the Redirect Server is used, for security reasons, user data such as First name, Last name, Directory number, and e-mail address will never be cached.

Note:

irectory extension number with **#** cannot be synced with the DeployU if a remote MBG connection is used. Replace **#** with ***** or use a local MBG connection and Clustered MBGs for synchronizing the data set with their source data set. For example, use **1*001** in place of **1#001**.

1.2.3 Importing CSV files

This page allows you to:

- download a CSV template that you can use to import user records, or
- manually create new users.

Download CSV Template

You can download a CSV template file, add user records to the template file, and then import it into the MiCollab Client service. Consider the following when importing a CSV file:

- Select **Allow partial import** to ensure erroneous data sets are ignored and only valid data sets are imported. If this option is not selected, nothing will be imported if one data set is invalid.
- Select **Allow overwrite import** to avoid duplicates. This is helpful if you are importing an edited CSV that has been exported from this application.
- ID necessary for "Allow overwrite": This setting only works to prevent duplicate entries if it contains a row "ID", containing a value for each entry (user). Since different systems use different user IDs, this option will only work properly (and should only be used) if the data was (re-)exported from the same system.
- If the select box is set to "From CSV", there must be a column of the Name "Profile" within the CSV, containing a value for each entry (user).
- Only last name and email address are mandatory settings to add/import user-account information. If there are whole columns with without any values within the CSV, these

rows have to be DELETED to prevent existing data from being overwritten by the empty value (unless this is the desired effect).

- The order of the columns is not important for Import CSV to work.

Note:

You can set the same PIN for all users. After setting up all user accounts, select **Manage** under the **Users** menu. Select **Export CSV** at the bottom of the table. The MiCollab Client password, PBX SIP password, Teleworker SIP password and Voicemail PIN will not be exported. However, in the exported file, you can set the PIN to the same number sequence for all table rows and re-import the file using **Import CSV**.

Manually Create New Users

To manually add a pre-MiCollab Release 7.0 user, click **Manage** > **Create New User**. Enter the following fields and click **Save**.

Note:

Imported user data cannot be modified, and users created in this view are not synchronized with any other applications (Users and Services, PBX, MiCollab Client Service and so on).

WhenMiCollab Client is configured as a stand-alone deployment without MiCollab or an MBG, you must enter the PBX SIP fields manually.

Users can only self-deploy their MiCollab Clients if you create their services from the MiCollab Users and Services application or import the users from the MiCollab Client service. If you manually create a user from the **MiCollab Client Deployment** > **Manually create user new user page**, or import new users via a CSV file, self-deployment is not available.

Setting	Description
Profile	Select the deployment profile to use for the new user account. The deployment profile adds deployment settings which are necessary to set up the client software, but are not yet specified by the user account information. Go to Deployment Profiles Tabfor more information.
First name	The user's first name.
Last name	The user's last name. This is a required setting.
Directory Number	User name or device number of the PBX user account that this account uses.
Email address	The email address used to send download links and authentication credentials to a user. This is a required setting.
PBX SIP Host	IP address of the PBX this client uses for SIP.
PBX SIP user name/Device number	User name or device number of the PBX user account that this account uses.
PBX SIP password	Password that allows access to the PBX SIP user account.
MBG SIP host	Displays the FQDN or IP address of the Mitel Border Gateway (MBG) for this user's MiCollab Mobile client account. This value is fetched from the selected Deployment Profile.

Setting	Description
MBG-WebRTC SIP host	Displays the FQDN of the Mitel Border Gateway (MBG) for this user's WebRTC client account. This value is fetched from the selected Deployment Profile.
MBG SIP user name	User name of the MBG user account that this account uses. It is synched from the MBG or entered manually.
MBG SIP password	Password that allows access to the MBG SIP user account.
MiCollab Client Service host	FQDN of the MiCollab administration server.
MiCollab Client Service user name	User name for the MiCollab Client Service. **Note**: If the MiCollab Client Service user name changes, a factory reset has to be executed on the client and the configuration has to be redeployed with the option **Deploy** under **Action** dropdown list on the page **Users** > **Manage**.
MiCollab Client Service password	Password for MiCollab Client Service user account.

Setting	Description
Deployment PIN (**Generate PIN**) (Optional)	You can set a Deployment PIN for users to increase security for MiCollab Client deployment. Click **Generate PIN** to auto-generate a PIN for the user. The user has to enter this PIN after scanning the QR code or clicking on the deployment link. The Deployment PIN must be between 4 and 20 characters long and must contain only numbers. **Note**: For security reasons, this PIN is **not** included in the deployment e-mail. You must communicate the Deployment PIN to the end users separately.

Note:

You can set the same Deployment PIN for all users. After setting up all user accounts, select **Manage** under the **Users** menu. Select **Export CSV** at the bottom of the table. The MiCollab Client password, PBX SIP password, Teleworker SIP password and Voicemail PIN will not be exported. However, in the exported file, you can set the Deployment PIN to the same number sequence for all table rows and re-import the file using **Import CSV**. Ensure you communicate the Deployment PIN to end users.

Note:

Directory extension number with **#**cannot be synced with the DeployU if a remote MBG connection i used. Replace **#**with ***or use a local MBG connection and Clustered MBGs for synchronizing the data set with their source data set. For example, use **1*001**, in place of **1#001**.

1.3 Deployment Profiles

1.3.1 Deployment Profiles Tab

The Deployment Profiles tab allows you to view, manage and create Deployment Profiles.

The Deployment Profile defines further options which are not already set within the user accounts of User And Services, MiCollab Client Service, and MBGs. Additionally, the Deployment Profile will directly link to one MBG.

Note:

The deployment profile should use the default connection generated by the DeployU to the local MBG. A connection to the external MBG is required only when the local MBG and external MBG do not share their databases.

The page displays the Default Deployment Profile (delivered with this application) and any additional Deployment Profiles.

Setting	Description
Modify	Use this option to change the settings made by a Deployment Profile.
Copy	Copies the Deployment Profile to use it as a template to create a similar profile.

Note:

TCP as the SIP transport protocol is not supported by some Android devices. If you are using any of the devices listed below, set the protocol to TLS. UDP is also possible, but from a functionality perspective, TLS is preferable. The following phones have been tested and documented, but with new phones frequently entering the market this list may not be complete: HTC One M7, HTC One Mini 601n, HTC One M8, HTC One M9, HTC One X, SONY XPERIA Z, SONY XPERIA Z2, SONY XPERIA Z3, SONY XPERIA Z3 Compact, CAT B15Q, YotaPhone 2.

1.3.2 Managing Deployment Profiles

If you have multiple MBGs, you must configure multiple Deployment Profiles. You may wish to use the Copy Profile method.

Setting	Description
Profile Name	Descriptive name.
PBX Type	Select the PBX type. This can be either MiVoice Business, MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400.
Call Mode	This setting can be Audio or Video. When set to Audio, the user's outgoing calls use audio. When set to Video, outgoing calls support both audio and video. It is recommended that you use the default setting (Audio). Users have the ability to enable video from the client.
Softphone	Shows if the associated users use softphones instead of deskphones, for example, use their clients directly via their mobile phones.

Setting	Description
Teleworker	Forces the associated clients to connect to the PBX indirectly, for example, through an MBG. This setting mandatory in case the device is not in the campus network (that is, directly connected through VPN). It is also mandatory for iPhone and Windows Phone devices (which will switch the Teleworker Mode On automatically). **Note**: If the Call recording option is used along with the softphone, please ensure that the **teleworker** setting is enabled.

1.3.3 Adding or modifying a profile

To manually add a Deployment Profile:

1. Click **Create new profile**.
2. Enter the following parameters.

Setting	Description
General Settings	
Name	A descriptive name for the profile.

Setting	Description
Use Teleworker	Select the Teleworker setting for the user from the drop-down menu. • off to disable the Client to register via the MBG. • on to enable a client to register via the MBG instead of directly with the PBX. If the Client is deployed with this setting, the user has the option to manually change the setting, but this change will not be overwritten by force configuration updates from the DeployU. • on (locked) to enable a client to register via the MBG instead of directly with the PBX. If the Client is deployed with this setting, the user has the option to manually change the setting and this change will be overwritten by force configuration updates from the DeployU. This will always reset the setting to on. **Note**: If the setting is on or on (locked), then all the mandatory MBG SIP host options are displayed.

Setting	Description
Use Softphone	Select the Softphone setting for the user from the drop-down menu. • off to use deskphone for calls. • on to bypass the deskphone and have users handle calls directly on their smartphones. If the Client is deployed with this setting, the user has the option to manually change the setting, but this change will not be overwritten by force configuration updates from the DeployU. • on (locked) to bypass the deskphone and have users handle calls directly on their smartphones. If the Client is deployed with this setting, the user has the option to manually change the setting and this change will be overwritten by force configuration updates from the DeployU. This will always reset the setting to on.
MBG	Select the MBG connection to use. To connect MBGs, go to Configuration > Connections to MBGs.
Override user e-mail	Select this box if the Deployment e-mail address (see below) should be used as the recipient of all deployment e-mails.
Deployment e-mail address	Enter an e-mail address to be used as the recipient for the deployment file if a user account does not have an e-mail address connected to it. This is a mandatory setting.
Log level	Select the log level at which errors should be recorded. The collected logs are added to the server logs on the MiCollab where they can be downloaded with administrator privileges.

Setting	Description
Call Mode	Select Audio or Video. Audio enables outgoing audio-only calls.
Office Number	Enter the phone number used to route client calls through the system. For MiVoice Business, Office Number is matched to the Hot Desking Access Number. When a client makes a call to a telephone number shorter than the MiCollab Client PBX Node Extension length, and they select to make a 'Native Call', the client will first make a call to the Office Number, then it will dial the desired number through the PBX.
Office Number Pause	Specifies the number of seconds that should pass before dialing an extension.
Config download host	Specify where the configuration should be downloaded. Choose between the MiCollab Server FQDN and Custom. The Custom setting supports the use of an FQDN that is different from the MiCollab Server FQDN. The Custom setting should not be used with an IP address.

Setting	Description
MBG SIP host	This setting is only available if Use Teleworker is on or on (locked). The MBG SIP host provides the main features telephony, chat, presence, and so forth of the MiCollab Mobile Client. Specify the interface that should be used on the MBG: • MBG's FQDN: The FQDN of the connected MBG that is used for MiCollab Mobile Client connections • MBGs Public IP: The public IP visible to the Application Management Center (AMC) • MBGs External Interface: The public IP of the WAN interface of the MBG • Custom: Enter an FQDN or IP address • Custom DNS SRV: A DNS-name used for SRV requests only It is highly recommended to use an FQDN which only resolves to the outside WAN even from behind the company firewall. Custom and Custom DNS SRV allow you to enter an IP address or domain name, respectively.
MBG-WebRTC SIP host	This setting specifies the interface that should be used on the MBG for WebRTC client connections. This field must be set to **MBG's FQDN (default)**. The **Custom** setting is available for use with possible future deployment scenarios and should not be used.

Setting	Description
PBX SIP host	Choose between Default or Custom DNS SRV. If set to Default the value returned by the PBX is used. If Custom DNS SRV is used, a field to specify the host appears. Please note that the Softphone Setting (see below) SIP Port is disabled. **Note**: If the PBX IP address is changed, a manual sync for the users in MiCollab Client deployment is required to enable softphone for the users.
Conference Access Code	Enter the access code for initiating conferences (if available) on your PBX System.
Emergency Numbers	These numbers are exempt from any special routing and are dialed directly! Certain numbers are pre-configured but can be modified and more can be added. Multiple emergency numbers must be separated with commas and no spaces. Although it is not recommended, emergency numbers that are not applicable to the user's region can be deleted if the emergency number (for example, 119) conflicts with an existing dialing string (for example, extension 119). Before you delete an emergency number, you should be certain that the user will not be traveling to a region that uses it.
Softphone Settings	
PBX Type	Select the PBX. Options are MiVoice Business, MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400.

Setting	Description
SIP transport protocol	Select TLS or TCP. TLS is the recommended setting. **Note**: TCP as the SIP transport protocol is not supported by some Android devices. If you are using any of the devices listed below, set the protocol to TLS. UDP is also possible, but from a functionality perspective, TLS is preferable. The following phones have been tested and documented, but with new phones frequently entering the market this list may not be complete: HTC One M7, HTC One Mini 601n, HTC One M8, HTC One M9, HTC One X, SONY XPERIA Z, SONY XPERIA Z2, SONY XPERIA Z3, SONY XPERIA Z3 Compact, CAT B15Q, YotaPhone 2.
SRTP mode	Secure Real-time Transport Protocol mode (Off, Mandatory, or Optional). SRTP mode option is visible only when SIP transport protocol is set as TLS. **Note**: SRTP mode is supported for audio only.
SIP port	Specify the port that should be used for the selected protocol. This setting is only applicable if the PBX SIP host is set to Default.
SIP DTMF method	Select RFC 2833/RFC 4733 or SIP INFO. RFC 2833/RFC 4733 is the default.

Setting	Description
Default audio codec	Select G722, G722.1, G729, PCMA, or PCMU. This only sets the initially requested codec. The codec used will be negotiated according to codecs requested by other devices.
Max video TX rate (kbits/s)	Select the maximum video data-transmit rate allowed when in a call. The default value is 768. Valid values are: 1536, 1024, 768, 512, 384, 192, 128. If a non-matching value is set, it will be changed to nearest supported one e.g. 850 to 768 accordingly.
Max video RX rate (kbits/s)	Select the maximum video-receive rate that the client will indicate in AS line. The default value is 768. Valid values are 1536, 1024, 768, 512, 384, 192, 128. If a non-matching value is set, it will be changed to the nearest supported one e.g. 850 to 768 accordingly.
DSCP SIP	Specify the Types of Service (ToS) for SIP traffic. Valid values can be created in compliance with RFC 2474.
DSCP RTP audio	Specify Types of Service (ToS) for RTP traffic. Valid values can be created in compliance with RFC 2474.
DSCP RTP video	Specify Types of Service (ToS) for RTP Video traffic. Valid values can be created in compliance with RFC 2474.
Verify TLS-server-certificate	Select the checkbox to validate and verify the TLS server certificate for the SIP connection.

Setting	Description
TLS-server-certificate CA	Select the TLS-server-certificate type to validate the PBX or MBG identity on the SIP TLS connection. Types of certificates that are supported on the TLS connection (PBX or MBG): • **Public CA** (Trusted 3rd party certificate): The admin must apply a trusted certificate on the PBX or MBG. • **Mitel CA** (built-in Mitel certificates): These certificates are shipped along with MiVB and MBG. • **Custom**: In case the administrator, who has implemented their own Certification Authority (CA), the admin can upload the certificate to the Client Deployment Service and will be distributed to the client from there. With this setting, the clients will validate the MBG identity on the SIP TLS connection using the certificate provided. If the **Mitel CA** certificate is selected, set MBG SIP TLS certificate option (**MiVoice Border Gateway** > **System Configuration** > **Settings**) to **Mitel**. If the **Public CA** certificate is selected, set MBG SIP TLS certificate option to Web server. **Note**: MiCollab Client Deployment profile setting for TLS server certificate validation must match the above MBG setting. If the setting does not match, the MiCollab Client softphones will fail to register as validation will fail. For more information on MBG configuration settings, see **MiVoice Border Gateway** > **System Configuration** help section.

Setting	Description
TLS-server-certificate CA Upload	This option is available only if the Custom certificate is selected in TLS-server-certificate CA. Browse and select the Custom certificate issued by the admin.
Teleworker Type	If the account belongs to a teleworker, this option must be set to MBG. The only Teleworker type currently supported is MBG.
SIP transport protocol	Select TLS or TCP. TLS is the recommended setting. **Note**: TCP as the SIP transport protocol is not supported by some Android devices. If you are using any of the devices listed below, set the protocol to TLS. UDP is also possible, but from a functionality perspective, TLS is preferable. The following phones have been tested and documented, but with new phones frequently entering the market this list may not be complete: HTC One M7, HTC One Mini 601n, HTC One M8, HTC One M9, HTC One X, SONY XPERIA Z, SONY XPERIA Z2, SONY XPERIA Z3, SONY XPERIA Z3 Compact, CAT B15Q, YotaPhone 2.
SRTP mode	Secure Real-time Transport Protocol mode (Off, Mandatory, or Optional)
SIP Port	Specify the port that should be used for the selected protocol.

Setting	Description
SIP DTMF mode	Choose RFC 2833/RFC 4733, or SIP INFO. RFC 2833/RFC 4733 is used as the default mode.
Default audio codec	Select G722, G722.1, G729, PCMA, or PCMU. This only sets the initially requested codec. The codec used will be negotiated according to codecs requested by other devices.
Max video TX rate (kbits/s)	Select the maximum video data-transmit rate allowed when in a call. Default value is 768. Valid values are: 1536, 1024, 768, 512, 384, 192, 128. If a non-matching value is set, it will be changed to nearest supported one e.g. 850 to 768 accordingly.
Max video RX rate (kbits/s)	Select the maximum video-receive rate that the client will indicate in AS line. Default value is 768. Valid values are 1536, 1024, 768, 512, 384, 192, 128. If a non-matching value is set, it will be changed to nearest supported one e.g. 850 to 768 accordingly.
DSCP SIP	Specify the Types of Service (ToS) for SIP traffic. Valid values can be created in compliance with RFC 2474.
DSCP RTP audio	Specify Types of Service (ToS) for RTP traffic. Valid values can be created in compliance with RFC 2474.
DSCP RTP video	Specify Types of Service (ToS) for RTP Video traffic. Valid values can be created in compliance with RFC 2474.
Verify TLS-server-certificate	Select the checkbox to validate and verify the TLS server certificate for the SIP connection.

Setting	Description
TLS-server-certificate CA	Select the TLS-server-certificate type to validate the MBG identity on the SIP TLS connection. Types of certificates that are supported on the TLS connection (MBG): • **Public CA** (Trusted 3rd party certificate): The admin must apply a trusted certificate on the MBG. • **Mitel CA** (built-in Mitel certificates): These certificates are shipped along with MiVB and MBG. • **Custom**: In case the admin who has implemented their own Certification Authority (CA), the admin can upload the certificate to the Client Deployment Service and will be distributed to the client from there. With this setting, the clients will validate the MBG identity on the SIP TLS connection using the certificate provided. If **Mitel CA** certificate is selected, set MBG SIP TLS certificate option (**MiVoice Border Gateway** > **System Configuration** > **Settings**) to **Mitel**. If **Public CA** certificate is selected, set MBG SIP TLS certificate option to Web server. **Note**: MiCollab Client Deployment profile setting for TLS server certificate validation must match the above MBG setting. If the setting does not match, the MiCollab Client softphones will fail to register as validation will fail. For more information on MBG configuration settings, see **MiVoice Border Gateway** > **System Configuration** help section.

Note:
TCP as the SIP transport protocol is not supported by some Android devices. If you are using any of the devices listed below, set the protocol to TLS. UDP is also possible, but from a functionality perspective, TLS is preferable. The following phones have been tested and documented, but with new phones frequently entering the market this list may not be complete: HTC One M7, HTC One Mini 601n, HTC One M8, HTC One M9, HTC One X, SONY XPERIA Z, SONY XPERIA Z2, SONY XPERIA Z3, SONY XPERIA Z3 Compact, CAT B15Q, YotaPhone 2.

3. Click **Validate configuration** and **save** (recommended) to run the diagnostic tests and save the profile settings.

   or Click **Save** to save the profile settings only.

1.4 Configuration Tab

1.4.1 Configuration Overview

The Configuration tab allows you to perform the following tasks:

- Define Deployment Configuration
- Purchase and Install Web Server Certificate
- Add or Modify Connections to MBG
- Customize Deployment Email

1.4.2 Define Deployment Configurations

The MiCollab server can be deployed in a variety of ways, depending on which services and applications you wish to provide, where your users are located, and whether you are using a physical or virtual system.

Note:
User configuration data can be downloaded three times, before it expires. Deployment data is deleted after six weeks.

MiCollab is deployed with MiCollab Client Deployment, however, the following basic configuration scenarios are recommended:

- MiCollab in LAN Mode Clustered with MBG(s) in the DMZ
- MiCollab in LAN Mode Clustered with MBG(s) on the Network Edge
- MiCollab with MBG on the Network Edge (Server Gateway Mode)

Note:
A trusted third party SSL certificate is required for MiCollab Client Deployment. Install the certificate on the MBG in the DMZ and on the MiCollab on the LAN.

Use these scenarios to obtain an overview of the conditions and settings that you need to employ. For detailed instructions, refer to the documents provided with MiCollab, MBG, and MiCollab Client Deployment. For other deployment configuration examples, see the*MiCollab Engineering Guidelines*.

Note:
The MBG Web Proxy is not supported directly on a MiCollab server in either LAN mode or Network Edge mode.

Note:
For sites using Integrated Directory Services, users may need to manually enter their Active Directory credentials on their phone after deployment.

1.4.2.1 MiCollab in LAN Mode Clustered with MBG(s) in the DMZ

This solution consists of MiCollab on the corporate LAN and one or more MBGs providing Teleworker and Web Proxy services in the DMZ. The Teleworker service is employed on both the MiCollab and MBG systems while the Web Proxy Service is provided only by the MBGs. The Teleworker service in MiCollab is only used to remotely manage the Teleworker phones that are configured on the MBGs.

To support this configuration, install the MiCollab server with the MBG application in the LAN and install one or more standalone MBG servers in the DMZ. Then create a cluster that ties the MBGs together.

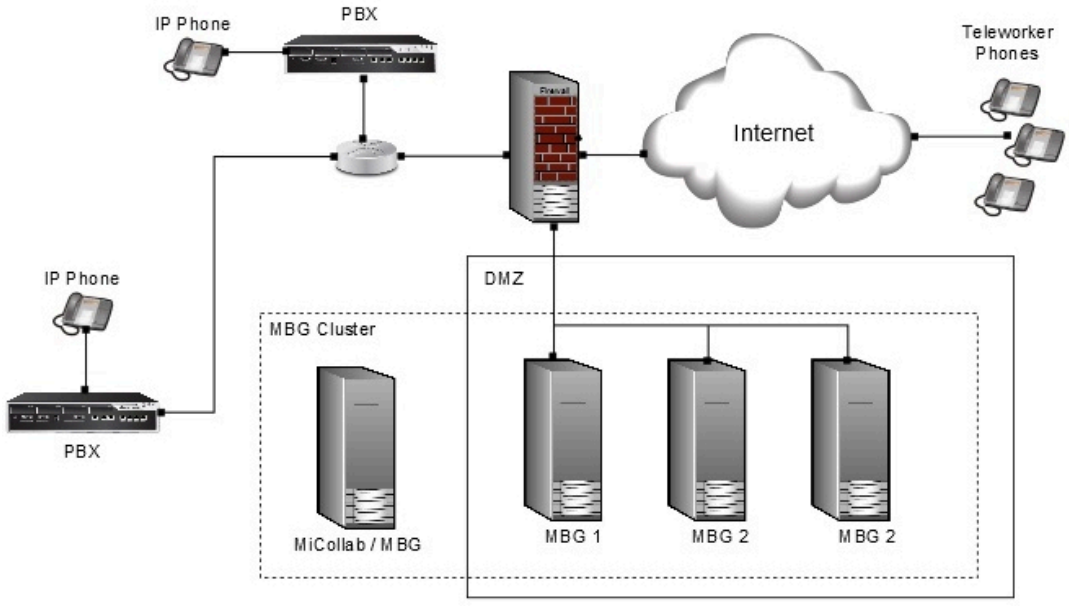
Conditions

- The MiCollab server on the LAN must be configured in "Server-only on LAN" mode and the MBG(s) in the DMZ must be configured in "Server-only on DMZ" mode. (Note

that MBG clustering is only supported for MiCollab systems that are configured in "Server-only on LAN" mode.)

- The MBGs in the DMZ must be routable to the MiCollab server on the LAN.
- All MBGs must have the same software version. This ensures support for the full range of MBG features and services.
- The MBG on MiCollab and the MBG(s) in the DMZ must be added to a cluster. Clustering provides the following benefits:
  - Allows data (including Teleworker services) to be managed from the MiCollab application.
  - Enables licence pooling. Note that, although licences are pooled, it is recommended that you purchase all Teleworker service licenses for the MBG(s) located in the DMZ in order to avoid licensing issues.
- The MiCollab and MBG nodes must reside in separate logical zones. Use the default zone for the node located on the LAN (which you may rename) and create a new zone for the nodes located in the DMZ.

MiCollab in LAN Mode Clustered with MBGs in the DMZ



Key Settings

The following table lists the key settings required to successfully program the systems (MiCollab, MBGs, firewall) in conjunction MiCollab Client Deployment. For a complete programming instructions, refer to the appropriate product documentation.

Feature	System	Configuration
Installing the Systems	MiCollab	Install MiCollab on the LAN: 1. Install and configure the MSL operating system software, configuring only the "Local" (internal) adapter. 2. Enter the ARID and install the application software.

Feature	System	Configuration
	MBGs	Install MBG(s) in the DMZ: 1. Install and configure the MSL operating system software, configuring only the "Local" (internal) adapter. 2. Enter the ARID. 3. Configure the network profile: a. Under **Applications**, select **MiVoice Border Gateway**. b. Select **System Configuration** > **Network Profiles**. c. Select **Server-only on network DMZ**. d. Click **Apply**. 4. Configure the SIP options: a. Under **System Configuration**, select **Settings**. b. For **SIP support** the recommended setting is **TLS**. To support SIP resiliency, select TLS or TCP. Configure matching values in the MiCollab Mobile Client deployment profiles (below). c. For **Allowed URI names**, enter the addresses that MBG should accept in SIP requests, in addition to its own. For example, if DNS is being used to resolve the MiCollab server on the LAN, enter its server name in FQDN format (mycompany.com). Configure matching values in the MiCollab Mobile Client deployment profiles (below). 5. Configure the LAN server web proxy: a. Under **Applications**, select **Remote proxy services**. b. Select **Add new LAN server proxy**. c. Enter the **WAN-side FQDN** of MiCollab Client Deployment. d. Select **MiCollab** as the server type and **Deployment Unit** as the user interface. e. Enable the new server and click **Save**. **Note**: To share MBG configuration data (but not IP addresses or network profiles) amongst the systems, create a cluster. See below for instructions.

Feature	System	Configuration
Configuring the Firewall	Firewall	1. Program firewall rules to allow the Client Deployment Service – which resides on your MiCollab Server – to reach the Redirect Servers (mcdepl01.easydeploy.net and mcdepl02.easydeploy.net) on port 443/tcp. This is required to send data to the Redirect Servers which help the clients to find the respective MiCollab server and which will also send the deployment emails to the end user's email address. 2. If you are using MBG Teleworker service in the DMZ, consult the MiCollab Engineering Guidelines for a description of the port usage and firewall settings.

Feature	System	Configuration
Clustering the MBGs	MiCollab and MBGs	Create a cluster: 1. Access the MiCollab MBG and create a new cluster: a. Designate the MiCollab MBG as a master by clicking **Create a cluster**. b. Enter the IP address of the server you have selected to be the slave as the **IP Address of peer node**. c. Click **Save**. 2. Access the slave MBG and add it to the cluster: a. Designate the MBG as a slave by clicking **Join**. b. Enter the IP address of the master server as the **IP Address of peer node**. c. Click **Save**. 3. Synchronize the master/slave databases. 4. Set the weight of both the master and slave to 100. 5. If there are any other MBGs in the DMZ, add them as slaves and adjust their weight value to 100. Subdivide the cluster into two logical zones: 1. Access the MiCollab MBG and add a new cluster zone called "DMZ". Rename the "Default" zone as "LAN" zone, add the current node to it, and set "DMZ" as the backup zone. (You can use other names if you wish.) 2. Access the MBGs in the DMZ, add them to the "DMZ" zone, and set the "LAN" as the backup zone. 3. Direct LAN-based devices to the a "LAN" zone and Internet-based devices to the "DMZ" zone.

Feature	System	Configuration
Configuring MiCollab Client Deployment	MiCollab	Connect to the MBG(s): 1. Access MiCollab Client Deployment and create a connection to an MBG in the DMZ. First enter configuration details and then generate an authentication request. 2. Access the MBG in the DMZ, open Web Services, approve the authentication request and copy the verifier. 3. Access MiCollab Client Deployment and paste the verifier into the newly created MBG connection. The connection is validated with a token. 4. If there are any other MBGs in the DMZ, connect to them to the MiCollab Client Deployment as described above. Create deployment profiles for the MBG(s): 1. Access the MiCollab Client Deployment and either modify the default profile (which is currently associated with the local MBG) or add a new profile. 2. Configure the profile, ensuring that the following settings are correct: • **Use Teleworker**- Select to enable Teleworker clients to register via the MBG instead of directly to the PBX. • **MBG**- Select the MBG connection in the DMZ that this profile will employ. • **Config download host**- Specify where clients can download the configuration. To have clients connect using DNS, select MiCollab Server FQDN or Custom. In most cases, you will need to set this to Custom and enter the FQDN of the MBG configured in external DNS. If multiple MBGs are providing SIP device resiliency, a single FQDN can be used to resolve to them. For example, use mycompany.com to resolve to mbg1.mycompany.com and mbg2.mycompany.com. • **MBG SIP host**- Specify on which interface that Teleworker clients must use to register via the MBG.To have clients connect using DNS, select MBG's FQDN or Custom DNS SRV and enter the FQDN of the MBG configured in external DNS. If multiple MBGs are providing SIP device resiliency, a single FQDN can be used to resolve to them. For example, use mycompany.com to resolve to mbg1.mycompany.com and mbg2.mycompany.com.
		Note:

Feature	System	Configuration
Add Web Server Certificate	MBGs and MiCollab	You are required to purchase a Third-Party SSL Certificate and install it on the MBG(s) in the DMZ and the MiCollab on the LAN. SeeMiCollab in LAN Mode with MBGs in DMZ on page 54.

1.4.2.2 MiCollab in LAN Mode Clustered with MBG(s) on the Network Edge

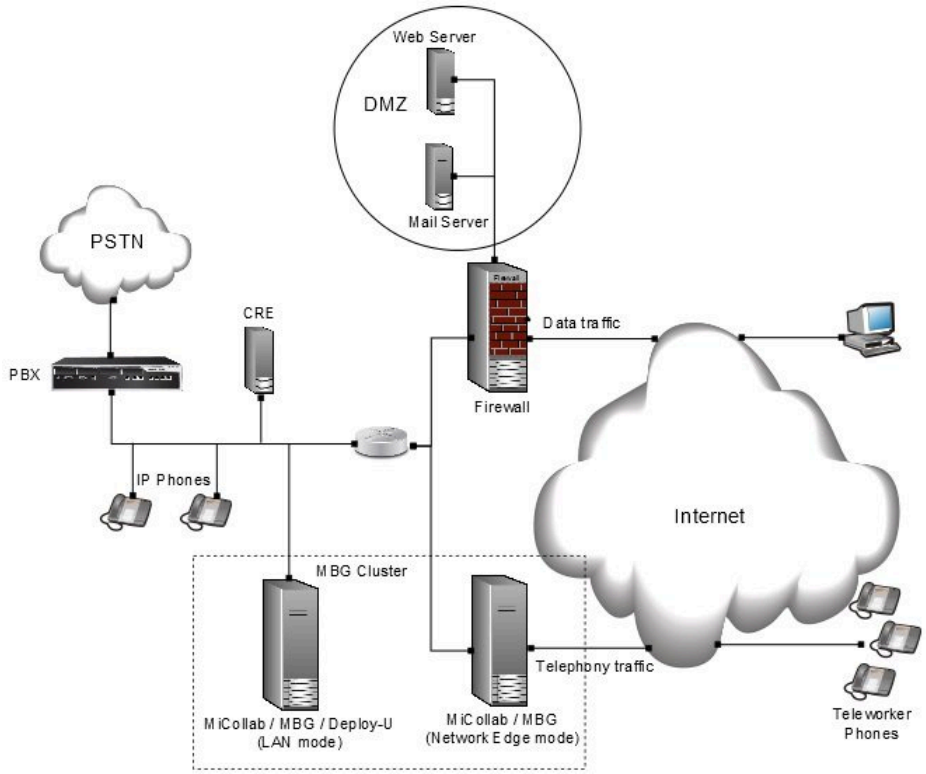
This solution consists of MiCollab on the corporate LAN and one or more MBGs providing Teleworker and Web Proxy services on the network edge. The Teleworker service is employed on both the MiCollab and MBG systems while the Web Proxy Service is provided only by the MBGs. The Teleworker service in MiCollab is only used to remotely manage the Teleworker phones that are configured on the MBGs.

To support this configuration, install the MiCollab server with the MBG application in the LAN and install one or more standalone MBG servers on the network edge. Then create a cluster that ties the MBGs together.

Conditions

- The MiCollab server on the LAN must be configured in "Server-only on LAN" mode and the MBG(s) on the network edge must be configured in "Server-only on network edge" mode. (Note that MBG clustering is only supported for MiCollab systems that are configured in "Server-only on LAN" mode.)
- The MBGs on the network edge must be routable to the MiCollab server on the LAN.
- All MBGs must have the same software version. This ensures support for the full range of MBG features and services.
- The MBG on MiCollab and the MBG(s) on the network edge must be added to a cluster. Clustering provides the following benefits:
  - Allows data (including Teleworker services) to be managed from the MiCollab application.
  - Enables licence pooling. Note that, although licences are pooled, it is recommended that you purchase all Teleworker service licenses for the MBG(s) located in the DMZ in order to avoid licensing issues.
- The MiCollab and MBG nodes must reside in separate logical zones. Use the default zone for the node located on the LAN (which you may rename) and create a new zone for the nodes located on the network edge.

MiCollab in LAN Mode Clustered with MBG on Network Edge



Key Settings

The following table lists the key settings required to successfully program the systems (MiCollab, MBGs, firewall) in conjunction with MiCollab Client Deployment. For a complete programming instructions, refer to the appropriate product documentation.

Feature	System	Configuration
Installing the Systems	MiCollab	Install MiCollab on the network edge: 1. Install and configure the MSL operating system software, configuring only the "Local" (internal) adapter. 2. Enter the ARID and install the application software.

Feature	System	Configuration
	MBGs	Install MBG(s) on the network edge: 1. Install and configure the MSL operating system software, configuring the "Local" (internal) and "WAN" (external) adapters. 2. Enter the ARID. 3. Configure the network profile: a. Under **Applications**, select **MiVoice Border Gateway**. b. Select **System Configuration** > **Network Profiles**. c. Select **Server-gateway on network edge**. d. Click **Apply**. 4. Configure the SIP options: a. Under **System Configuration**, select **Settings**. b. For **SIP support** the recommended setting is **TLS**. To support SIP resiliency, select TLS or TCP. Configure matching values in the MiCollab Mobile Client deployment profiles (below). c. For **Allowed URI names**, enter the addresses that MBG should accept in SIP requests, in addition to its own. For example, if DNS is being used to resolve the MiCollab server on the LAN, enter its server name in FQDN format (mycompany.com). Configure matching values in the MiCollab Mobile Client deployment profiles (below). 5. Configure the LAN server web proxy: a. Under **Applications**, select **Remote proxy services**. b. Select **Add new LAN server proxy**. c. Enter the **WAN-side FQDN** of the MiCollab Client Deployment. d. Select **MiCollab** as the server type and **Deployment Unit** as the user interface. e. Enable the new server and click**Save**. 6. Enable MiCollab Client connector: a. Under **Service configuration**, select **Application integration**. b. Under **Mobile Client**, select **Mobile Client**

Feature	System	Configuration
Configuring the Firewall	Firewall	If you are using MBG Teleworker service on the network edge, consult the MiCollab Engineering Guidelines for a description of the port usage and firewall settings.
Clustering the MBGs	MiCollab and MBGs	

Feature	System	Configuration
Configuring MiCollab Client Deployment	MiCollab	Create a cluster: 1. Access the MiCollab MBG and create a new cluster: a. Designate the MiCollab MBG as a master by clicking **Create a cluster**. b. Enter the IP address of the server you have selected to be the slave as the **IP Address of peer node**. c. Click **Save**. 2. Access the slave MBG and add it to the cluster: a. Designate the MBG as a slave by clicking **Join**. b. Enter the IP address of the master server as the **IP Address of peer node**. c. Click **Save**. 3. Synchronize the master/slave databases. 4. Set the weight of both the master and slave to 100. 5. If there are any other MBGs on the network edge, add them as slaves and adjust their weight value to 100. Subdivide the cluster into two logical zones: 1. Access the MiCollab MBG and add a new cluster zone called "Edge". Rename the "Default" zone as "LAN" zone, add the current node to it, and set "Edge" as the backup zone.(You can use other names if you wish.) 2. Access the MBGs on the Edge, add them to the "Edge" zone, and set the "LAN" as the backup zone. 3. Direct LAN-based devices to the a "LAN" zone and Internet-based devices to the "Edge" zone.
Add Web Server Certificate	MBGs and MiCollab	You are required to purchase a Third-Party SSL Certificate and install it on the MBG(s) on the network edge and the MiCollab on the LAN. SeeMiCollab Server in LAN Mode on page 68.

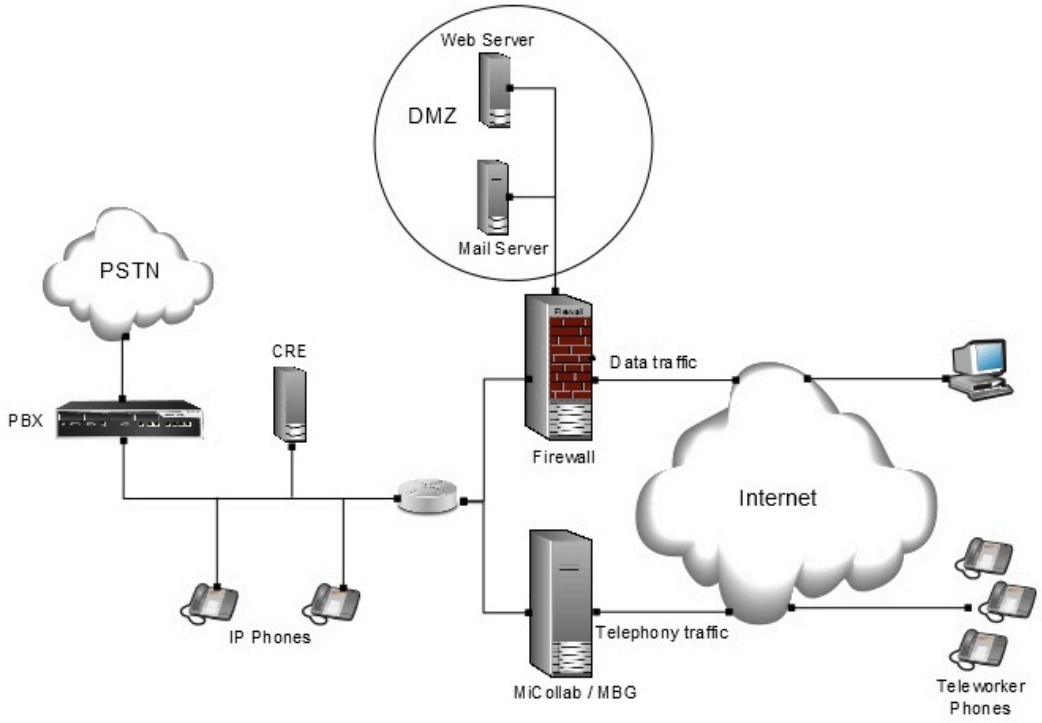
1.4.2.3 MiCollab Server with MBG on the Network Edge (Server Gateway Mode)

Network Edge (Server-Gateway) mode can be used to deploy any of the MiCollab applications. In this configuration, MiCollab must have direct Internet access, which is required by the MBG Teleworker and MiCollab Client applications.

Conditions

- The MiCollab server requires two Ethernet adaptors. One adapter is configured as "Local" for connection to the LAN, and the other is configured as "WAN" for connection to the Internet. The WAN network adapter requires a publicly routable IP address that is accessible to both the Internet and the LAN (in other words, the server should not reside behind a NAT device).
- Preferably, MiCollab should be used in conjunction with the corporate firewall. The MiCollab system acts as a firewall/gateway for MiCollab applications while the corporate firewall controls data traffic for the enterprise. If your voice/telephony network and your data network are separate, connect the MiCollab's local network adapter to the voice/telephony network in order to support the MiCollab's telephony applications.
- Network Edge (Server-Gateway) mode involves a number of security considerations:
  - Most application traffic is encrypted, because the system supports Secure Real-time Transport Protocol (SRTP) for SIP traffic on both the ICP side as well as the set side of the network edge. However, calls between SIP endpoints and some older Mitel MiNET devices may be unencrypted because the MiNET devices only support RTP. This issue does not arise when newer Mitel MiNET devices are in use.
  - When using Teleworker in conjunction with LAN-facing applications, you must ensure that they review the configuration in relation to your corporate security policy. You may choose to deploy Teleworker on a separate server in a DMZ.

MiCollab with MBG on Network Edge (Server Gateway) with Corporate Firewall



Key Settings

The following table lists the key settings required to successfully program the systems (MiCollab, MBGs, firewall) in conjunction with MiCollab Client Deployment. For a complete programming instructions, refer to the appropriate product documentation.

Feature	System	Configuration
Installing the Systems	MiCollab / MBG	Install MiCollab on the network edge (server-gateway): 1. Install and configure the MSL operating system software, configuring the "Local" (internal) and "WAN" (external) adapters. Program firewall rules to send deployment tokens and configuration download URLs to the Mitel redirect deployment

Feature	System	Configuration
		servers (default port 443). 2. Enter the ARID and install the application software. 3. Configure the network profile: a. Under **Applications**, select **MiVoice Border Gateway**. b. Select **System Configuration** > **Network Profiles**. c. Select **Server-gateway on network edge**. d. Click **Apply**. 4. Configure the SIP options: a. Under **System Configuration**, select **Settings**. b. For **SIP support**, the recommended setting is**TLS**. To support SIP resiliency, select TCP or TLS. To support iPhones you MUST set to TCP. Most Android devices require TLS. Configure matching values in the MiCollab Mobile Client deployment profiles (below). c. For**Allowed URI names**, enter the addresses that MBG

Feature	System	Configuration
		should accept in SIP requests, in addition to its own. For example, if DNS is being used to resolve the MiCollab server on the LAN, enter its server name in FQDN format (mycompany.com). Configure matching values in the MiCollab Mobile Client deployment profile (below). 5. Configure the LAN server web proxy: a. Under**Applications**, select**Remote proxy services**. b. Select**Add new LAN server proxy**. c. Enter the**WAN-side FQDN**of MiCollab Client Deployment. d. Select**MiCollab**as the server type and**Deployment Unit**as the user interface. e. Enable the new server and click**Save**. 6. Enable MiCollab Client connector: a. Under**Service configuration**, select**Application integration**. b. Under**Mobile Client**, select**Mobile**

Feature	System	Configuration
		Client connector enabledand enter the Mobile Client hostname or server IP address.
Configuring the Firewall	Firewall	If you are using MBG Teleworker service in the DMZ, consult the MiCollab Engineering Guidelines for a description of the port usage and firewall settings. Since these settings are provided automatically and cannot be changed, the information is provided for reference only.
Configuring MiCollab Client Deployment	MiCollab	Create a deployment profile for the MBG: 1. Access MiCollab Client Deployment and modify the default profile (which is currently associated with the local MBG). 2. Configure the profile, ensuring that the following settings are correct: • **Use Teleworker**- Select to enable Teleworker clients to register via the MBG instead of directly to the PBX. • **MBG**- Select the local MBG connection. • **Config download host**- Specify where

Feature	System	Configuration
		clients can download the configuration. To have clients connect using DNS, select **MiCollab Server FQDN** or **Custom**. In most cases, you will need to set this to **Custom** and enter the FQDN of the MBG configured in external DNS. If multiple MBGs are providing SIP device resiliency, a single FQDN can be used to resolve to them. For example, use mycompany.com to resolve to mbg1.mycompany.com and mbg2.mycompany.com. • **MBG SIP host**- Specify on which interface that Teleworker clients must use to register via the MBG. To have clients connect using DNS, select **MBG's FQDN** or **Custom DNS SRV** and enter the FQDN of the MBG configured in external DNS. • SIP transport protocol - Recommended setting is TLS. To support SIP resiliency, select TLS or TCP. This setting must match the SIP support setting on the MBG. Assign deployment profiles to users:

Feature	System	Configuration
		1. Access **MiCollab Client Deployment** and either modify an existing user or add a new user. 2. Select the deployment profile that this user account will employ. **Note**: It is also possible to assign deployment profiles using templates in the Users and Services application. For conditions and configuration instructions, refer to the MiCollab documentation.
Add Web Server Certificate	MiCollab / MBG	You are required to purchase a Third-Party SSL Certificate and install it on the MiCollab server. SeeMiCollab Server in Network Edge Mode on page 61.

1.4.3 Purchase and Install Web Server Certificate

1.4.3.1 About SSL Web Certificates

Secure Sockets Layer (SSL) is an encryption technology that creates a secure connection between a web server and a client's web browser. Information that is transmitted must be encrypted to prevent security issues such as eavesdropping or data tampering. An SSL web certificate is purchased from a Certificate Authority and installed on the web server to enable encryption.

The SSL web certificate authenticates the identity of a web site and encrypts information passed between the web server and the web client using Secure Sockets Layer (SSL) technology. The use of an SSL web certificate on a website is usually indicated by a padlock icon in web browsers, but it can also be indicated by a green address bar. After an SSL web certificate is installed on a website, users can be sure that the information that they enter such as contact or credit card information, is secured and only seen by the organization that owns the website.

SSL encryption is required between the MiCollab servers and MiCollab for Mobile phone users because sensitive user information and configuration data is transmitted during the deployment of the clients. The SSL web certificate ensures that the MiCollab for Mobile clients establish secure connections during deployment.

To support the MiCollab Client deployment, you must purchase a signed SSL web certificate from a third-party Certificate Authority (CA) such as Entrust or GoDaddy. This involves generating a certificate signing request (CSR) on the MiCollab or MBG server and submitting it to the CA. The CA will then return a package containing your web server certificate, plus any intermediate certificates that are required to maintain the certificate key chain. You then import the certificate and any required intermediate certificates onto the MiCollab and MBG servers. The third-party SSL web certificate allows MiCollab for Mobile Client users to establish connections and receive their deployment configurations.

Note:

Information about different certificate chains must be obtained from the issuer. You must read and understand the certificate installation instructions from your certificate vendor. Normally they should be e-mailed to you whenever you receive the signed certificate from them.

Using Third-Party SSL Web Certificates

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

- **PEM** certificates typically have extensions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format. Apache and similar servers use PEM format certificates. Several PEM certificates, including the private key, can be included in a single file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files.
- **PKCS#12** or **PFX** format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually

have extensions such as .pfx and .p12. PFX files are typically used on Windows machines to import and export certificates and private keys.

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

About TLS

MiCollab and MBG might require multiple hostnames, especially if the services are running on multiple servers. For most deployment scenariosa certificate that is valid for multiple names is required. One SSL key plus the certificate must be used on multiple MSL servers (for example, MBG and MiCollab).

In most of the deployments, the MBG must host multiple domain names, so it is mandatory to have a certificate which includes all the required DNS names.

SSL Web Certificate Options

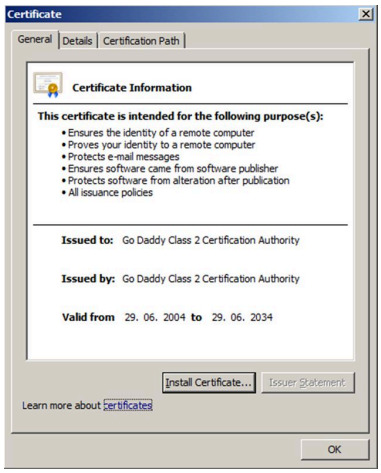
The following options are recommended:

Wildcard Certificate	Extended Attributes
This is probably the easiest way, especially if there is already a certificate available, e.g *.example.com. **Advantage:** Other hosts and nodes can be added later without reissuing the certificate. **Disadvantage:** Slightly more expensive than a single certificate.	Use of the x509 v3 Extended attributes (as described below). Multiple DNS names can be included in the certificate request. Many CAs allow up to 15 names. **Advantage:** Sometimes a second name makes only a little or no price difference. **Disadvantage:** Adding another DNS name requires reissuing the certificate.

1.4.3.2 Certificate Examples

Certificate	Description
Root Certificate Example	Below is and example of a root certificate. A root certificate can be identified as a root certificate if “issued to:” and “issued by:” contain the same name. Installing this certificate on the server is typically notrequired. The root certificate is normally pre-installed in the operating system of the phone or the web browser. 

Certificate	Description
Secure Intermediate Certificate Example	This is the "not pre-installed certificate" issued to “Go Daddy Secure Certificate Authority - G2”. You must install this file as an Intermediate CA. **Note**: You might need more than one Intermediate CA if the Intermediate CA was not signed by a root CA known by the phone or by the web browser. In the following example the “Issued by:” does point to the Root CA, and no second intermediate CA is needed. If the “Go Daddy Secure Certificate Authority - G2” root CA from 2009 is unknown to the phone (because it is relatively new), another (alternative) certificate chain can be installed. 

Certificate	Description
Alternative Certificate Example	This Alternative Certificate contains the “Go Daddy Secure Certificate Authority - G2”, plus another intermediate certificate “Go Daddy Root Certificate Authority - G2”. In this case, the “Go Daddy Root Certificate Authority - G2” is not a root certificate, because it is issued by a different root CA: “Go Daddy Class 2 Certification Authority”. 
	The ”Go Daddy Class 2 Certification Authority” is much older and it is more likely to be installed in all web browsers and phones. Downloading the root CA certificate (not required) will show its validly (from 2004, as shown in the example below: 

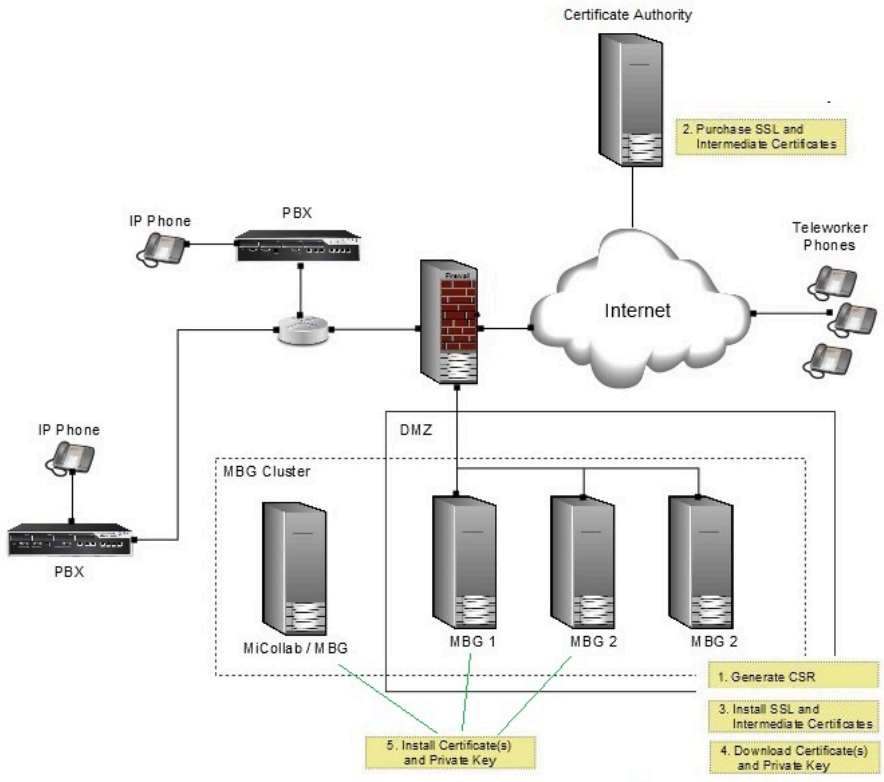
1.4.3.3 Certificate Installation

1.4.3.3.1 MiCollab in LAN Mode with MBGs in DMZ

This topic describes the installation of the SSL web server certificate on a MiCollab server clustered with MiVoice Border Gateways in the DMZ.

Certificate Installation Overview

1. Generate the certificate signing request (CSR) on an MBG node in the DMZ. Ensure that you include “Subject Alternate Names” for each additional server (MiCollab and MBGs) in the DMZ that will use the certificate.
2. Submit the CSR to the Certificate Authority, complete the online registration forms and purchase your web server certificate and intermediate certificates.
3. Install the SSL web server certificate and intermediate certificates on the MBG server from which you generated the CSR.
4. Download the certificates and private key from the MBG server.
5. Upload the certificates and private key onto the MiCollab server and the other MBG servers in the DMZ.
6. Restart the MiCollab and MBG servers.



Generate a Certificate Signing Request (CSR) on MBG Cluster Manager Server

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

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

Note:

When completing the fields, use first capital letters only (for example Ontario, not ONTARIO).

Field Name	Description
Country Name (two letter code)	Enter the two-letter International Organization for Standardization- (ISO-) format country codefor the country in which your organization is legally registered. Examples are, CA for Canada and US for United States.
State or Province Name	Enter the full name of state or province where your organization is located. Do not abbreviate. The first letter of the name entered must be a **capital with remaining letters lower case**. For example, you would enter "Ontario" for Mitel Corporation.
Locality Name	The Locality Name is the city, town, route used in the mail address of the organization that is submitting the CSR. Enter the full name of the city in which your organization is located. Do not abbreviate.

Field Name	Description
Organization Name	The Organization Name is the name used in the mail address of the organization / business submitting the CSR. Enter the name under which your organization / business is legally registered. The listed organization must be the legal registrant of the domain name in the trusted certificate request. If you are enrolling as an individual, please enter the certificate requestor's name in the Organization field, and the DBA (doing business as) name in the Organizational Unit field.
Organizational Unit Name	Enter the organization unit or department name. Use this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, you may enter the DBA (doing business as) name in this field.
Common Name	The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com). The common name is the fully-qualified domain name (FQDN) to which you plan to apply your certificate. A web browser checks this field. It is required. In addition to entering a FQDN, you can also enter a domain name with a wild card character (e.g. *.example.com) in order to generate a wild card certificate request.

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

8. Copy the text of the CSR file.

Submit the CSR to the Certificate Authority and Purchase the SSL Certificate

1. Access the web site of a Certificate Authority and purchase a certificate for multiple domains or a wildcard domain. You will be prompted to do the following:

> **Note**:
>
> Each Certificate Authority has unique requirements. Accordingly, you may not be prompted for all of the steps listed below, and some of the field names may vary.

a. Select the number of domains you wish to protect:

i. **Single domain**: Select this option if your implementation has one MSL server on a single domain (for example, www.domain.com and domain.com).
ii. **Multi-domain**: Select this option if your implementation has multiple MSL servers on a specific number of domains (for example, www.domain.com and domain.com, plus three sub-domains).
iii. **Multi-domain and wildcard**: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (for example, www.domain.com and domain.com, plus an unlimited number of sub-domains).

b. Enter your account and contact details in the CA web form:

- **Login Name** and **Password**.
- **Name**, **Email Address**, and **Telephone Number**.
- **Organization Name** and **Address**.
- **Domain Name**.

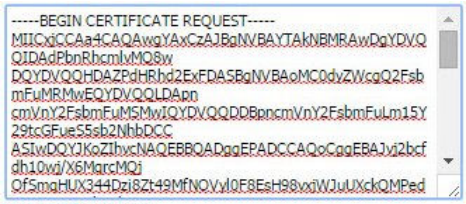
> **Note**:
>
> Some CAs may prompt you to enter the Subject Alternate Names (SANs) or wildcard domain in this step. For more information on these entries, see below.

- **Web Server Software**.

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

- **Hashing Algorithm**.

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



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

- **Subject Alternate Name (SAN)**: Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied.Note: You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.
- **Wildcard**: To consolidate your domain and unlimited sub-domains into a single SSL certificate, enter a wildcard domain name. For example, if your deployment includes numerous MSL application servers on the LAN (eg. MiCollab, MiVoice Business, MiCollab Client, MiCollab Unified Messaging, generic MSL, and Oria), you can include them all by entering an FQDN such as *.mitel.com.

2. Complete the purchase transaction. The Certificate Authority will do the following:

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

Note:

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

- Contact the administrator for the domain used in a CSR. The administrator is identified using information supplied when your organization originally registered its internet FQDN.

3. Upload the certificate files to a location that is accessible to the MSL server.

Install the SSL Certificate Files on the MBG Server

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

To install the SSL certificate files on the MSL server:

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

Note:

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

7. Click **Install WebServer Certificate**.
8. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.

Download the Certificate and Private Key from the MBG Server

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

Note:

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

Upload the certificates and private key onto the MiCollab and other MBG servers in the DMZ

1. Log into each of the server managers.
2. Under **Security**, click **Web Server**.

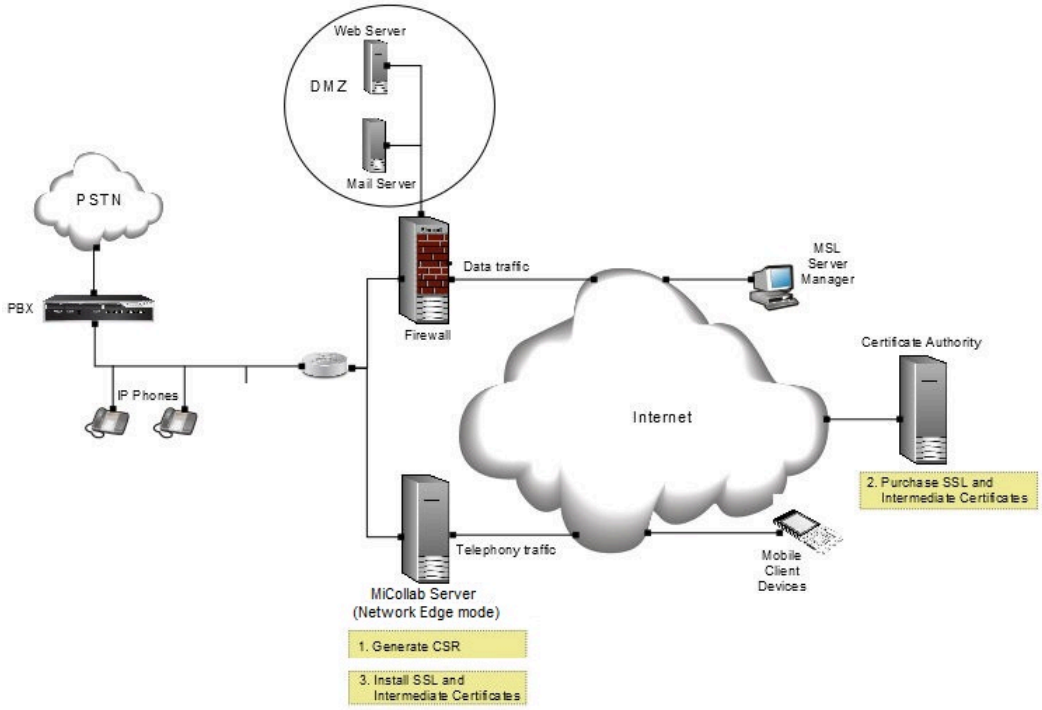
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.
5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the **SSL certificate**, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the **Intermediate SSL certificate**, select it and click **Open**.
7. Import the private key pair created on the other MSL server:
   - Beside the **SSL Private Key** field, click **Browse**.
   - Navigate to the **SSL Private Key** file, select it and click **Open**.
8. Click **Install WebServer Certificate**.
9. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.
10. To prevent fraudulent use of your certificates, delete the certificate and private key files from any media they are stored on.

1.4.3.3.2 MiCollab Server in Network Edge Mode

This topic describes the installation of the SSL web server certificate on a MiCollab server in network edge mode.

Certificate Installation Overview

1. Generate the certificate signing request (CSR) on the MiCollab server.
2. Submit the CSR to the Certificate Authority, complete the online registration forms and purchase your web server certificate and intermediate certificates.
3. Install the certificates on the MiCollab server.
4. Restart the MiCollab server.



Generate a Certificate Signing Request (CSR)

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

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

Note:

When completing the fields, use first capital letters only (for example Ontario, not ONTARIO).

Field Name	Description
Country Name (two letter code)	Enter thetwo-letter International Organization for Standardization- (ISO-) format country codefor the country in which your organization is legally registered. Examples are, CA for Canada and US for United States.
State or Province Name	Enter the full name of state or province where your organization is located. Do not abbreviate. The first letter of the name entered must be a **capital with remaining letters lower case**. For example, you would enter "Ontario" for Mitel Corporation.
Locality Name	The Locality Name is the city, town, route used in the mail address of the organization that is submitting the CSR. Enter the full name of the city in which your organization is located. Do not abbreviate.

Field Name	Description
Organization Name	The Organization Name is the name used in the mail address of the organization / business submitting the CSR. Enter the name under which your organization / business is legally registered. The listed organization must be the legal registrant of the domain name in the trusted certificate request. If you are enrolling as an individual, please enter the certificate requestor's name in the Organization field, and the DBA (doing business as) name in the Organizational Unit field.
Organizational Unit Name	Enter the organization unit or department name. Use this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, you may enter the DBA (doing business as) name in this field.
Common Name	The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com). The common name is the fully-qualified domain name (FQDN) to which you plan to apply your certificate. A web browser checks this field. It is required. In addition to entering a FQDN, you can also enter a domain name with a wild card character (e.g. *.example.com) in order to generate a wild card certificate request.

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

8. Copy the text of the CSR file.

Submit the CSR to the Certificate Authority and Purchase the SSL Certificate

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

Note:

Each Certificate Authority has unique requirements. Accordingly, you may not be prompted for all of the steps listed below, and some of the field names may vary.

a. Select the number of domains you wish to protect:

- **Single domain**: Select this option if your implementation has one MSL server on a single domain (for example, www.domain.com and domain.com).
- **Multi-domain**: Select this option if your implementation has multiple MSL servers on a specific number of domains (for example,www.domain.com and domain.com, plus three sub-domains).
- **Multi-domain and wildcard**: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (for example, www.domain.com and domain.com, plus an unlimited number of sub-domains).

b. Enter your account and contact details in the CA web form:

- **Login Name** and **Password**.
- **Name**, **Email Address**, and **Telephone Number**.
- **Organization Name** and **Address**.
- **Domain Name**.

Note:

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

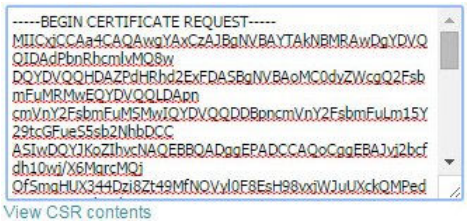
- **Web Server Software**.

Note:

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

- **Hashing Algorithm**.

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



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

- **Subject Alternate Name (SAN)**: Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied.

Note:

You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.

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

2. Complete the purchase transaction. The Certificate Authority will do the following:

- Send you the certificate files. These include your SSL server certificate and, if required, intermediate certificates. An intermediate certificate is a subordinate certificate issued to establish a certificate chain that begins at the CA's trusted root certificate, carries through the intermediate and ends with your own SSL

server certificate. Some CAs provide a single intermediate certificate while others provide multiple intermediate certificates. There should be no need to open and inspect the files, provided that they are in the correct format and that the intermediate certificates have been bundled into a single file by the CA. Consult the documentation provided by your Certificate Authority for instructions to obtain, unzip and identify exactly which files you need to use.

Note:

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

- Contact the administrator for the domain used in a CSR. The administrator is identified using information supplied when your organization originally registered its internet FQDN.

3. Upload the certificate files to a location that is accessible to the MSL server.

Install the SSL Certificate Files on the MiCollab Server

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

To install the SSL certificate files on the MSL server:

1. Log into the MiCollab Server Manager for the system that was used to generate the CSR.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.
5. Select the SSL certificate:

   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the**SSL certificate**, select it and click **Open**.

6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the **Intermediate SSL certificate**, select it and click **Open**.

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

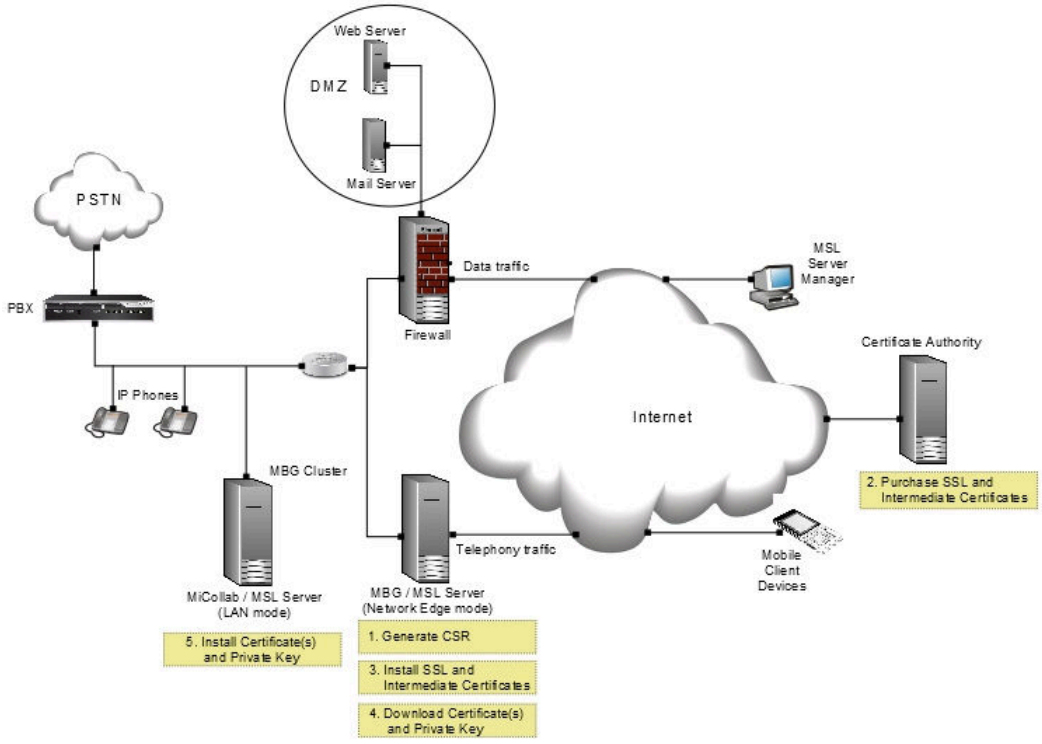
7. Click **Install WebServer Certificate**.
8. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.

1.4.3.3.3 MiCollab Server in LAN Mode

This topic describes the installation of the SSL web server certificate on a MiCollab server in LAN mode with a MiVoice Border Gateway on the network edge.

Certificate Installation Overview

1. Generate the certificate signing request (CSR) on the MBG server.Ensure that you include “Subject Alternate Names” for each additional server (MiCollab and MBGs) in the DMZ that will use the certificate.
2. Submit the CSR to the Certificate Authority, complete the online registration forms and purchase your web server certificate and intermediate certificates.
3. Install the SSL and intermediate certificates on the MBG server
4. Download the certificates and private key from the MBG server
5. Upload the certificates and private key onto the MiCollab server on the LAN.
6. Restart the MiCollab and MBG servers.



Generate a Certificate Signing Request (CSR) on MBG Server

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

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

Note:

When completing the fields, use first capital letters only (for example Ontario, not ONTARIO).

Field Name	Description
Country Name (two letter code)	Enter thetwo-letter International Organization for Standardization- (ISO-) format country codefor the country in which your organization is legally registered. Examples are, CA for Canada and US for United States.
State or Province Name	Enter the full name of state or province where your organization is located. Do not abbreviate. The first letter of the name entered must be a **capital with remaining letters lower case**. For example, you would enter "Ontario" for Mitel Corporation.
Locality Name	The Locality Name is the city, town, route used in the mail address of the organization that is submitting the CSR. Enter the full name of the city in which your organization is located. Do not abbreviate.

Field Name	Description
Organization Name	The Organization Name is the name used in the mail address of the organization / business submitting the CSR. Enter the name under which your organization / business is legally registered. The listed organization must be the legal registrant of the domain name in the trusted certificate request. If you are enrolling as an individual, please enter the certificate requestor's name in the Organization field, and the DBA (doing business as) name in the Organizational Unit field.
Organizational Unit Name	Enter the organization unit or department name. Use this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, you may enter the DBA (doing business as) name in this field.
Common Name	The default value presented in this field is the FQDN of the server including the domain name (for example, mbg.example.com). The common name is the fully-qualified domain name (FQDN) to which you plan to apply your certificate. A web browser checks this field. It is required. In addition to entering a FQDN, you can also enter a domain name with a wild card character (for example, *.example.com) in order to generate a wild card certificate request.

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

8. Copy the text of the CSR file.

Submit the CSR to the Certificate Authority and Purchase the SSL Certificate

1. Access the web site of a Certificate Authority and purchase a certificate for multiple domains or a wildcard domain. You will be prompted to do the following:

> **Note**:
>
> Each Certificate Authority has unique requirements. Accordingly, you may not be prompted for all of the steps listed below, and some of the field names may vary.

a. Select the number of domains you wish to protect:

- **Single domain**: Select this option if your implementation has one MSL server on a single domain (for example, www.domain.com and domain.com).
- **Multi-domain**: Select this option if your implementation has multiple MSL servers on a specific number of domains (for example,www.domain.com and domain.com, plus three sub-domains).
- **Multi-domain and wildcard**: Select this option if your implementation has multiple MSL servers with a large number of sub-domains (for example,www.domain.com and domain.com, plus an unlimited number of sub-domains).

b. Enter your account and contact details in the CA web form:

- **Login Name** and **Password**.
- **Name**, **Email Address**, and **Telephone Number**.
- **Organization Name** and **Address**.
- **Domain Name**.

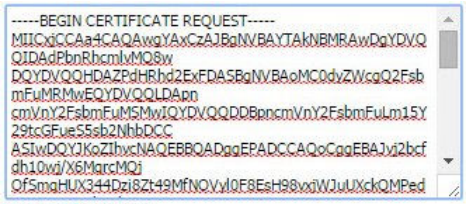
> **Note**:
>
> Some CAs may prompt you to enter the Subject Alternate Names (SANs) or wildcard domain in this step. For more information on these entries, see below.

- **Web Server Software**.

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

- **Hashing Algorithm**.

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



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

- **Subject Alternate Name (SAN)**: Enter the domain name for each service (or "virtual host") in the LAN that you want to include in this certificate. For example, if your deployment includes a number of MSL application servers on the LAN, you would enter the FQDN of each server such as micollab.mitel.com, mivb.mitel.com, and micollabclient.mitel.com. If these addresses are not configured correctly, remote client access to the LAN-based services will be denied.

Note:
You can also enter an IP address as a SAN if your users are accessing an MSL application server from the internal network rather than through the MBG / Web Proxy. Typically, you would do this for testing purposes or to enable direct access from the LAN.

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

2. Complete the purchase transaction. The Certificate Authority will do the following:

- Send you the certificate files. These include your SSL server certificate and, if required, intermediate certificates. An intermediate certificate is a subordinate certificate issued to establish a certificate chain that begins at the CA's trusted root certificate, carries through the intermediate and ends with your own SSL server certificate. Some CAs provide a single intermediate certificate while others provide multiple intermediate certificates. There should be no need to open and inspect the files, provided that they are in the correct format and that the

intermediate certificates have been bundled into a single file by the CA. Consult the documentation provided by your Certificate Authority for instructions to obtain, unzip and identify exactly which files you need to use.

Note:

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

- Contact the administrator for the domain used in a CSR. The administrator is identified using information supplied when your organization originally registered its internet FQDN.

3. Upload the certificate files to a location that is accessible to the MSL server.

Install the SSL Certificate Files on the MBG Server

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

To install the SSL certificate files on the MSL server:

1. Log into the MiCollab Server Manager for the system that was used to generate the CSR.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Select **Upload and install a web server certificate**, and then click **Perform**.
5. Select the SSL certificate:

   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the **SSL certificate**, select it and click **Open**.

6. If you also received an Intermediate SSL certificate, select it as well:

   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the **Intermediate SSL certificate**, select it and click **Open**.

Note:

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

7. Click **Install WebServer Certificate**.
8. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.

Download the Certificate and Private Key from the MBG Server

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

Note:

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

Upload the certificates and private key onto the MiCollab server on the LAN

1. Log into the MiCollab Server Manager for a LAN-based MSL server.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.

4. Select **Upload and install a web server certificate**, and then click **Perform**.
5. Select the SSL certificate:
   - Beside the **SSL Certificate** field, click **Browse**.
   - Navigate to the **SSL certificate**, select it and click **Open**.
6. If you also received an Intermediate SSL certificate, select it as well:
   - Beside the **Intermediate SSL Certificate** field, click **Browse**.
   - Navigate to the **Intermediate SSL certificate**, select it and click **Open**.
7. Import the private key pair created on the other MSL server:
   - Beside the **SSL Private Key** field, click **Browse**.
   - Navigate to the **SSL Private Key**file, select it and click **Open**.
8. Click **Install WebServer Certificate**.
9. Restart the server to ensure all components and services that require the certificate are informed of the certificate's presence.
10. To prevent fraudulent use of your certificates, delete the certificate and private key files from any media they are stored on.

1.4.3.4 Verify Certificate Installation

Verify the Installed Certificate

To verify that the certificate is installed:

1. Log into the server manager.
2. Under **Security**, click **Web Server**.
3. Click the **Web Server Certificate** tab.
4. Verify that the certificate name and issuer are displayed on the page.

Currently Installed Web Server Certificate

If a web server certificate is currently installed on the server, the details are listed on the Web Server Certificate page in the server manager:

Field Name	Details
Issuer	Lists the following information for the certificate authorization company that issued the certificate:

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

Field Name	Details
	CN: MBG Web Proxy server hostname
Not before	Date and time when the certificate takes effect.
Not after	Date and time when the certificate expires.

1.4.3.5 Testing Server Certificates

You need to upload the signed certificate to the server. In most of the cases, uploading an “Intermediate SSL Certificate” is also required. This topic describes how to test your certificates after installation to ensure that they are fully trusted.

Background Information

The easiest way to test if your installed server certificate is fully trusted, is to use a test tool. If the web server certificate is not valid or unknown to the mobile phone, no connection can be made and the configuration deployment will fail.

During the TLS handshake the client will check if the certificate offered by the MiCollab or MBG server can be verified. In some cases, the authenticity for the server cannot be verified because the signing Certificate Authority (CA) is unknown to the phone. This is an issue which may not occur on a web browser, because Firefox - for example - uses its own CA certificate pool and does not use the same certificate store as the operating system.

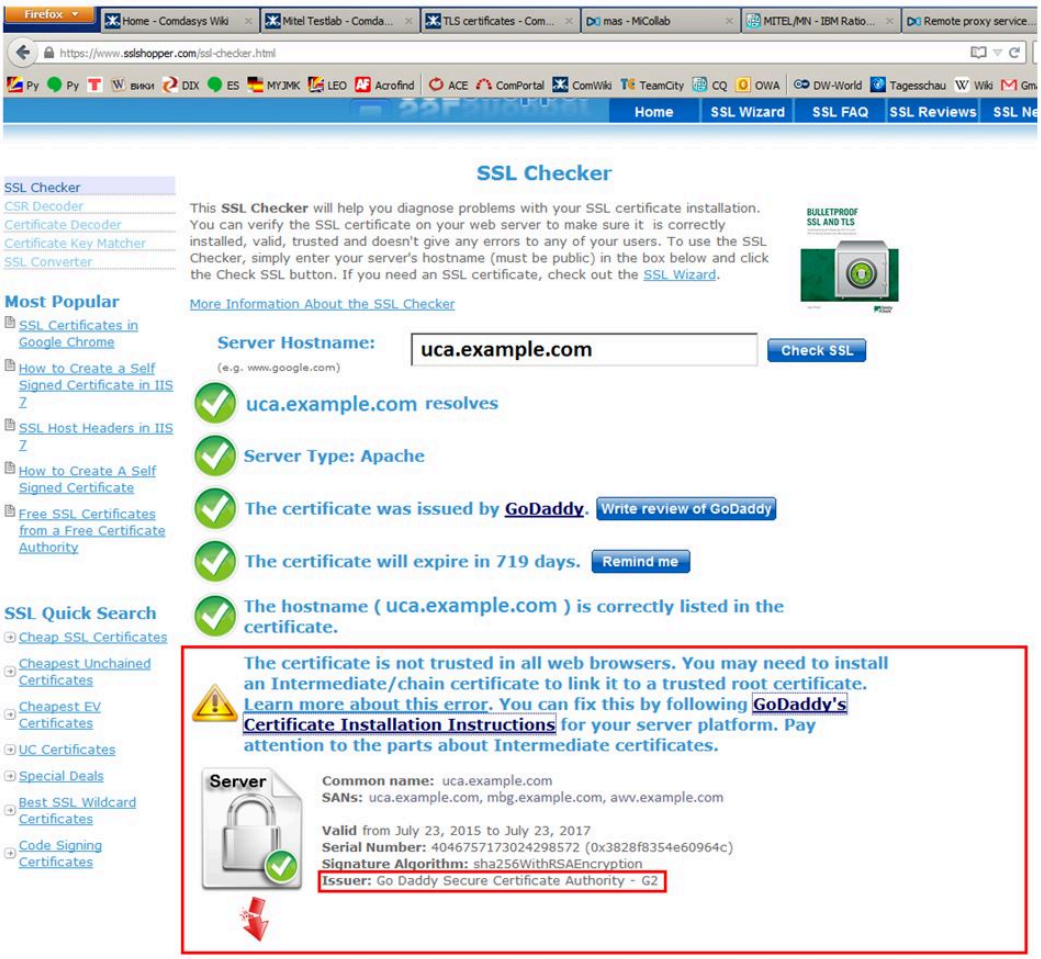
The MiCollab server allows you to specify and upload an “Intermediate SSL Certificate file”. This file can contain one or more intermediate certificates which are transferred to the client once it connects to the server. The certificate path can be validated, even if the phone does not have all Intermediate CAs installed.

Note:

Certificates must be in a BASE64 encoded format (*.pem or *.crt) and the file must use the UNIX file format.

SSL Checker

1. Go to https://www.sslshopper.com/ssl-checker.html .
2. Enter the hostname of your UCA server:



Note:

If an error occurs as shown in the above example, most likely all the required intermediate certificates are not installed.

Note:

Information about different certificate chains must be obtained from the issuer. You must read and understand the certificate installation instructions from your certificate vendor. Normally they should be e-mailed to you whenever you receive the signed certificate from them.

Alternative Method for Checking Certificate: Open SSL

Instead of the using the sslshopper test site, you can use the following openssl command:

```
openssl s_client -CAfile /etc/pki/tls/certs/ca-bundle.crt -
connect uca.example.com:443 < /dev/null
```

The UCA websocket connection for the client should also be verified:

```
openssl s_client -CAfile /etc/pki/tls/certs/ca-bundle.crt -
connect uca.example.com:36008 < /dev/null
```

Both commands must return:

```
Verify return code: 0 (ok)
```

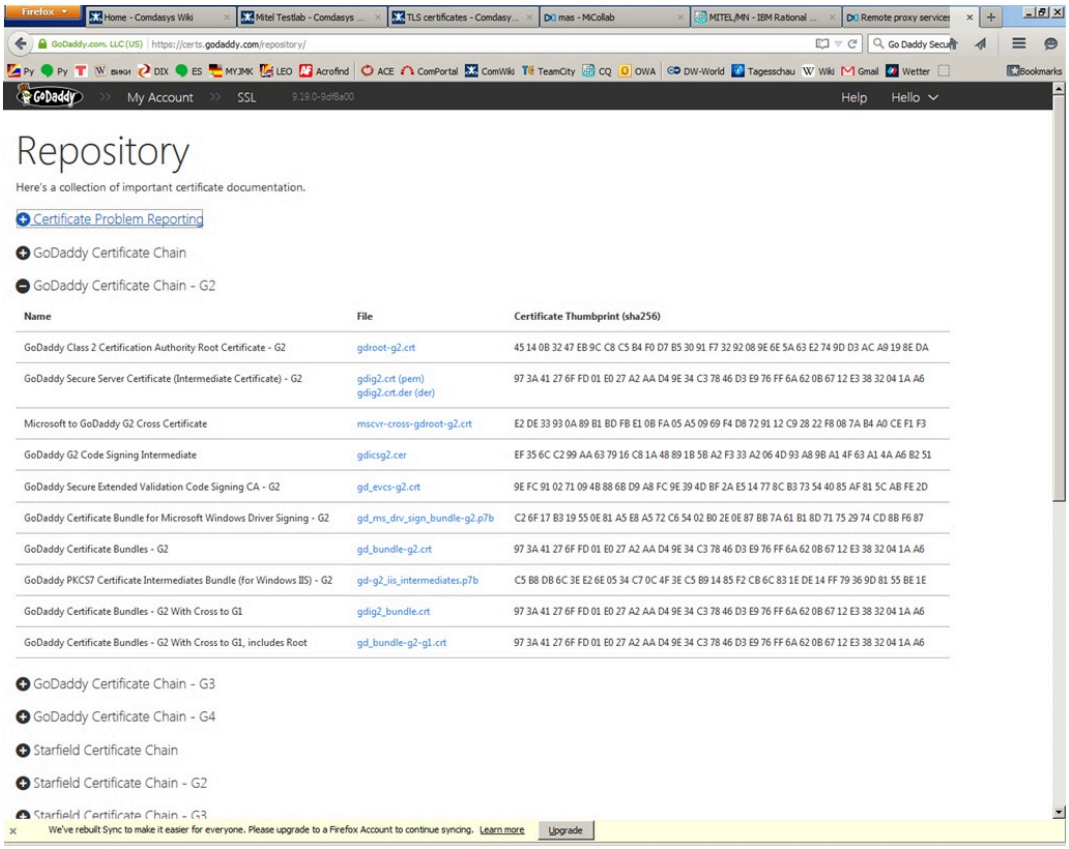
Identifying the Correct Intermediate Certificates

The information about the installed certificates can be contained by connecting via web browser to the MiCollab or MBG server. Click on

the  symbol in order to find information about the installed certificate:

The “Issued by:” field of your certificate, that is “Go Daddy Secure Certificate Authority - G2”, helps you to identify which CA was used to sign your MiCollab certificate.

Locate the website of the certificate authority and check the instructions: https://certs.godaddy.com/repository/



Certificates can be downloaded to this repository. If the filename extension is .crt, you can open and display the certificate with Windows .

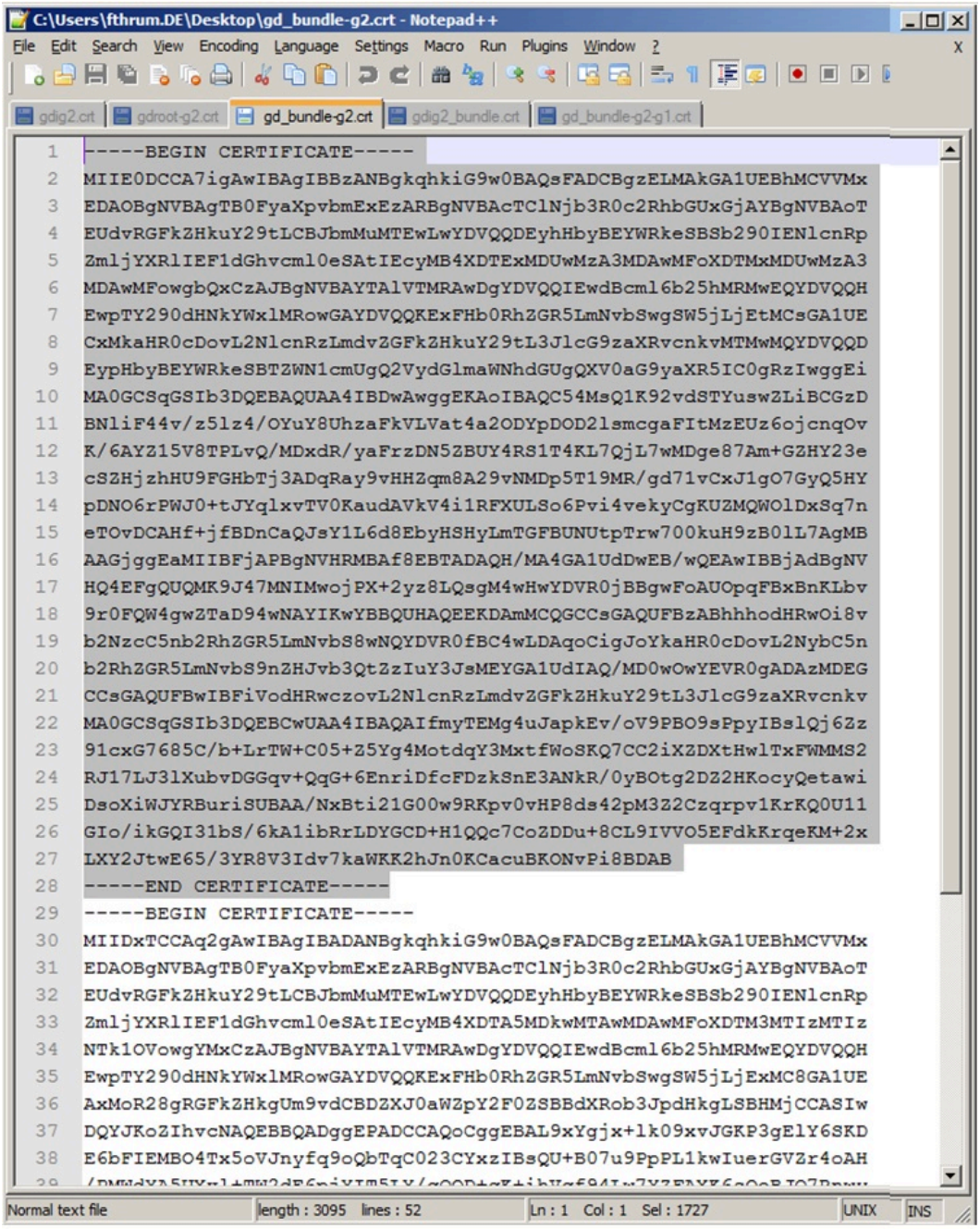
Separating Multiple Certificates

Text Editor Example

Windows will only display the first certificate included in the file. If the file contains more than one certificate, you can display them using a text editor. Separate both certificate sections and save them to different files.

Note:

Do not use Notepad because it does not understand the UNIX line formatting.


C:\Users\fthrum.DE\Desktop\gd_bundle-g2.crt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
gdig2.crt
gdroot-g2.crt
gd_bundle-g2.crt
gdig2_bundle.crt
gd_bundle-g2-g1.crt
-----BEGIN CERTIFICATE-----
MIIE0DCCA7igAwIBAgIBBzANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoT
EUdvRGFkZHkuY29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRp
ZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTExMDUwMzA3MDAwMFoXDTMxMDUwMzA3
MDAwMFowgbQxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQH
EwpTY290dHNkYWxlMRowGAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UE
CxMkaHR0cDovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQD
EypHbyBEYWRkeSBTZWN1cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC54MsQ1K92vdSTYuswZLiBCGzD
BNliF44v/z5lz4/OYuY8UhzaFkVLVat4a2ODYpDOD2lsmcgaFItMzEUz6ojcnqOv
K/6AYZ15V8TPLvQ/MDxdR/yaFrzDN5ZBUY4RS1T4KL7QjL7wMDge87Am+GZHY23e
cSZHjzhHU9FGHbTj3ADqRay9vHHZqm8A29vNMDp5T19MR/gd71vCxJ1gO7GyQ5HY
pDNO6rPWJ0+tJYqlxvTV0KaudAVkV4i1RFXULSo6Pvi4vekyCgKUZMQWOlDxSq7n
eTOvDCAHf+jfBDnCaQJsY1L6d8EbyHSHyLmTGFBUNUtpTrw700kuH9zB0lL7AgMB
AAGjggEaMIIBFjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNV
HQ4EFgQUQMK9J47MNIMwojPX+2yz8LQsgM4wHwYDVR0jBBgwFoAUOpqFBxBnKLbv
9r0FQW4gwZTaD94wNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8v
b2NzcC5nb2RhZGR5LmNvbS8wNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL2NybC5n
b2RhZGR5LmNvbS9nZHJvb3QtZzIuY3JsMEYGA1UdIAQ/MD0wOwYEVR0gADAzMDEG
CCsGAQUFBwIBFiVodHRwczovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkv
MA0GCSqGSIb3DQEBCwUAA4IBAQAIfmyTEMg4uJapkEv/oV9PBO9sPpyIBslQj6Zz
91cxG7685C/b+LrTW+C05+Z5Yg4MotdqY3MxtfWoSKQ7CC2iXZDXtHwlTxFWMMS2
RJ17LJ3lXubvDGGqv+QqG+6EnriDfcFDzkSnE3ANkR/0yBOtg2DZ2HKocyQetawi
DsoXiWJYRBuriSUBAA/NxBti21G00w9RKpv0vHP8ds42pM3Z2Czqrpv1KrKQ0U11
GIo/ikGQI31bS/6kA1ibRrLDYGCD+H1QQc7CoZDDu+8CL9IVVO5EFdkKrqeKM+2x
LXY2JtwE65/3YR8V3Idv7kaWKK2hJn0KCacuBKONvPi8BDAB
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIBADANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoT
EUdvRGFkZHkuY29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRp
ZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTA5MDkwMTAwMDAwMFoXDTM3MTIzMTIz
NTk1OVowgYMxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQH
EwpTY290dHNkYWxlMRowGAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjExMC8GA1UE
AxMoR28gRGFkZHkgUm9vdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgLSBHMjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL9xYgjx+lk09xvJGKP3gElY6SKD
E6bFIEMBO4Tx5oVJnyfq9oQbTqC023CYxzIBsQU+B07u9PpPL1kwIuerGVZr4oAH

1.4.3.6 Troubleshooting Certificate Installation

Symptom	Probable Cause	Corrective Action
Self signed certificate is distributed on port TCP 36008 instead of port TCP 443	MBG does not automatically pick up certificate changes. You must restart the server after uploading a new web certificate. Otherwise, it distributes the self-signed certificate on port TCP 36008.	Restart the MBG/MiCollab server after installing a new web server certificate.
You installed the root certificate, but MiCollab for Mobile Clients are still unable to connect.	Intermediate certificate missing from certificate chain. You need to install the correct intermediate certificate bundles.	See Testing Server Certificates for additional information. Contact your Certificate Authority supplier for assistance with installing the intermediate certificates.

Viewing MSL Server Certificates

The certificates available on a given MSL system are determined by the content of the ca-certificates rpm. On MSL 10.4 the current version is ca-certificates-2015.2.4-65.0.1.el6_6.noarch. That rpm contains file /etc/ssl/certs/ca-bundle.crt which contains the CA certificates of the primary Certificate Authorities. You can look at them using the following openssl commands:

```
awk -v cmd='openssl x509 -noout -subject' '/BEGIN/{close(cmd)};
{print | cmd}' < /etc/ssl/certs/ca-bundle.crt
```

Below is an openssl command that can be used to show the certs being used by a particular server connection:

```
openssl s_client -showcerts -connect 10.35.29.49:443
```

1.4.4 Adding or Modifying Connections to MBG

The **Connections to MBG** page initiates connections to MBGs. Typically, a connection to the local MBG is created automatically.

Note:

You must verify the connection to the MBG to guarantee security.

You can only connect an MBG if its Web Service has been activated in the MBG server manager. While MiCollab is running in the browser, you can open the MBG Web Services in a second browser tab.

To add and verify a new MBG connection:

1. Click **Create new connection** and enter the following information:

Setting	Description
Name	Descriptive name for the MBG.
Host	Hostname or IP address.

2. Click**Save and send AuthRequest**. The connection is populated with a Token key and a popup window appears.
3. Click **OK** in the popup window to allow the connection to the MBG.
4. Click **Authorize**. The MiCollab Login page is displayed.
5. Enter the MiCollab server manager Username and Password and click **Login**.

   After you enter the credentials, the popup-window closes and the connection to the MBG is updated with the credentials.

Note:

Creating or re-authenticating an MBG connection is limited to primary administrator account.

6. If you accidentally close the popup-window or if it does not open (for example, due to a browser issue) click Authenticate on the Connection page to open the pop-up window. This button is only present if the connection to the MBG has not been verified.

7. Click Connections to MBGs. The table on the **Connections to MBGs** page will have been updated with the following information:

Setting	Description
ID	This is the local identifier number for an MBG. It also indicates the order in which MBGs were added.
Name	Descriptive name for the MBG.
Hostname	Hostname or IP address. Required to enable Client Deployment to request the connection.
Token ID	This string is needed to verify the connection between the Client Deployment application and the MBG.
Verified	This field indicates if the verification process has been completed for the connection to this MBG.
Expires in Days	This field displays the number of days before the Token ID expires at which time the connection must be re-authenticated.

Note:

The authentication is valid for one year. After its expiry date, the connection has to be re-authenticated.

Note:

Events are raised before and on the date of expiry. Make sure to regularly check the Event viewer or configure e-mail alerts.

- At expiration date: Major (orange)
- Two weeks before expiration date: Minor (yellow)
- Four weeks before expiration date: Warning (blue)

1.4.5 Customize Mobile Client deployment email

You can to customize the deployment e-mail that is sent to MiCollab for Mobile users. If left blank, the default content (which resides on the Redirect Server) is used.

Add your e-mail subject line and body text. If no e-mail subject and body text are saved here, the default content, which resides on the Redirect Server, will be used. You also have the option to load the default content here.

Note:

Ensure you include the placeholder links to the configuration, the Authentication Token (Authtoken), and the QR-Code to the e-mail body.

All placeholders will be personalized according to user records when e-mails are sent out.

Setting	Description
E-mail Subject Line	When you click in the email subject line, the following buttons appear: • First name ([####firstname####]) • Last name ([####lastname####]) • Device number ([####dn####]) All three placeholders are contained in the subject line by default and will be personalized according to user records when e-mails are sent out.

Setting	Description
E-mail Body	App Store links for MiCollab Mobile Client: **[####appstore####]** **[####playstore####]** **[####microsoftstore####]** **[####bbworld####]** Links to the application store for download and installation of client. NextGen MiCollab Client for Mac and Windows download links: **[####appstore_mac####]** **[####winpc####]** For MiCollab Servers that are upgraded from an older version to 8.0 or higher, the administrator must load the default text or add the link manually. **Link:[####link####]** Links to the configuration (via the Redirect Server). When the end user clicks it on the mobile phone, it initiates the download of the settings. **Authtoken: [####authtoken####]** If a client is started for the very first time, this authentication token can be used as an alternative method to download the configuration. **QR-Code: [####qrcode####]** This method can be used to generate a QR-Code that can be scanned with a QR-Code scanning application from a computer monitor or a tablet. The process following the scan is identical to clicking the download link. **Load default text** Click to load the default e-mail body text from the Redirect Server.

Note:

The Deployment Profile can be used to overwrite the e-mail address of the connected users with a general Deployment e-mail address.

Note:

The link or QR-Code will be cached by the Redirect Server. However, even if the default e-mail content residing on the Redirect Server is used, for security reasons, user data such as First name, Last name, Directory number, and e-mail address will never be cached.

Note:

MiCollab for PC Client and MiCollab for Mac Client can be deployed by clicking the direct link provided in the deployment e-mail.

1.5 Diagnostics Tab

1.5.1 Run Diagnostics

To verify if Internet connectivity is available to support MiCollab Client Deployment, it is recommended that you run the diagnostic test provided on this page against a deployment profile. This diagnostic test performs three functions:

- **Verifies that the MiCollab Client Deployment service can connect to the Redirect Server.** The MiCollab Client Deployment service must be able to reach the Redirect Server (https://mcdiagnostics.easydeploy.net:443) on the Internet.

Note:

MiCollab Server needs to verify the identity of the Redirection Server. Therefore Proxy Server is not supported for MiCollab Client Deployment.

- **Validates that the MiCollab Clients on the public Internet can reach the MiCollab Client Deployment service.** This diagnostic test validates that the MiCollab Clients can reach the MiCollab Client Deployment service to download their configuration. During the test, the Redirect Server attempts to open an https connection to the MiCollab Client Deployment service residing on the MiCollab Server. Note that the Redirect Server only initiates a connection to the MiCollab Client Deployment service when you run this test. It does not deploy the client. However, after you have completed MiCollab Client Deployment configuration, MiCollab Clients will be able to connect to the MiCollab Server to update their configurations whenever required.

  The test uses the "Config download host" configuration from the selected MiCollab Client Deployment profile; all other MiCollab Client Deployment parameters are not relevant to this test. The test relies on the MBG Remote proxy services configuration.

  The following limitations apply:

  - Configuration issues with the local Wi-Fi, the local split-DNS or with local firewalls can cause the deployment process to fail on the mobile client even though this test validates the connection between the MiCollab Clients on the internet and the MiCollab Client Deployment service.
  - It is possible that the connection between MiCollab Clients on the internet and the MiCollab Client Deployment service fails validation while deployment to the Mobile Clients is successful. This can occur if the MiCollab server has no public IP address or if an MBG is not included in the deployment configuration. Typically, this type of deployment configuration would only be found in a lab environment during testing.

Note:

Geofencing (a software that helps define geographical boundaries) can cause deployments to fail. When geofencing is enabled, traffic to and from the Redirect servers (mcdepl01.easydeploy.net, mcdepl02.easydeploy.net and mcdiagnostics.easydeploy.net) should be allowed on port 443.

- **Validates that the MiCollab Clients on the public Internet can reach the MiCollab Client Service.**This diagnostic test validates that the MiCollab Clients can reach the MiCollab Client Service for successful login and operation. During the test, the Redirect Server attempts to open a connection to the Fully Qualified Domain Name

(FQDN) of the MiCollab server, using TCP port 36008. The server FQDN must be resolvable from the Internet for this test to pass.

The test relies on the MiCollab connector being enabled within the MBG's Application Integration area.

To run the Diagnostic test:

1. Select the Deployment Profile that you want to test.
2. Click **Run test**. The results are presented on the screen.

- If the tests are successful, you can proceed with client deployment.
- If one or both tests fail, refer to the following tables to interpret the results. The tables list possible error messages and provide tips on how to troubleshoot a particular network issue. In most of the cases, a network trace containing DNS traffic port 53 and tcp port 443 will help identify the problem.

To run the Diagnostic test with MiCloud deployments:

For MiCloud deployments, users belong to different customer sites. Therefore, you must set the 'ConfigDownloadHost' field in the deployment profile to the configuration download hostname of the user's site in order for the Diagnostic test to function correctly. To run the Diagnostic test for a user on a specific customer site:

1. Access the **Deployment Profiles** tab.
2. Create a copy the default deployment profile.
3. Access the **User** tab.
4. Open (Modify) the user that you want to test.
5. Copy the hostname from the "MiCollab Client Service host" field.
6. Access the **Deployment Profiles** tab.
7. Edit the newly created profile and copy the hostname into the "ConfigurationloadHost" field.
8. Access the **Diagnostics** tab.
9. Select the newly created Deployment Profile.
10. Click **Run test**. The results are presented on the screen.

Table 1: Connection test to Redirect Server

Error Message	Meaning
ConnectionError: [Errno -2] Name or service not known	The DNS server of the MiCollab Server cannot resolve the name mcdiagnostics.easydeploy.net Note: Changing the DNS server might require a restart of the server.
ConnectionError: [Errno -3] Temporary failure in name resolution	The DNS server configured on your MiCollab Server is not reachable.
ConnectionError: [Errno 110] Connection timed out	The MiCollab Client Deployment service cannot reach the server tcp:mcdiagnostics.easydeploy.net:443. Packets are being dropped, most likely because of a firewall.
ConnectionError: [Errno 111] Connection refused	The MiCollab Client Deployment service cannot reach the server.
ConnectionError: [Errno 113] No route to host	There is no route to the Redirect Server. Check the IP configuration and the routing (that is, the default route).
SSLError: hostname 'mcdiagnostics.easydeploy.net' doesn't match either of '*.somehostname.com', 'somehostname.com'	There is transparent TLS-proxy or another device (can also be a MITM) between the MiCollab Client Deployment service and the Redirect Server which intercepts the TLS traffic.
SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed	There is transparent TLS-proxy or another device (can also be a MITM) between the MiCollab Client Deployment service and the Redirect Server which intercepts the TLS traffic.

Table 2: MiCollab Client Deployment test from public internet

Error Message	Meaning/Corrective Action
ERROR: query A ENOTFOUND	The “Config download host” DNS entry configured in the "Deployment Profile" cannot be resolved.
ERROR: ETIMEDOUT (400 Bad Request) from host 12.12.12.12	The "Config download host" does not reply. Most likely, the incoming packets are dropped by a firewall before reaching the MBG.
	The MBG cannot reach the MiCollab-Server due to dropped packets or no route to host (DMZ-firewall, routing between MiCollab and MBG)
	The MBG cannot send the request to the MiCollab server. Check DNS and configuration on the MBG.
Cannot reach MiCollab Client Deployment service (503 Service Unavailable) from host 12.12.12.12	The MBG cannot reach the MiCollab-server (DMZ-firewall).
ERROR: connect ECONNREFUSED (400 Bad Request) from host 12.12.12.13	Packets are rejected by a firewall.
ERROR: connect EHOSTUNREACH (400 Bad Request) from host 12.12.12.14	“Config download host” configured in the MiCollab Client Deployment service’s deployment profile may point to the wrong machine.
ERROR: SELF_SIGNED_CERT_IN_CHAIN (400 Bad Request) from host 12.12.12.15	The configured "Config download host" in the MiCollab Client Deployment service’s deployment profile may point to the wrong machine and/or the certificate is not correctly installed on the MBG.

Error Message	Meaning/Corrective Action
ERROR: UNABLE_TO_VERIFY_LEAF_SIGNATURE	TLS Certificate issue. The certificate chain is missing or not properly installed. Verify that the right intermediate certificates are installed on the internet facing Web Proxy Server (MBG).
Cannot reach MiCollab Client Deployment service (404 Not Found) from host 12.12.12.13	The configured "Config download host" in the MiCollab Client Deployment service points to the wrong machine.
	Check that the IP address 12.12.12.13 belongs to the MBG which serves your MiCollab Server. Check the MBG configuration.
	Check that the "Config download host" resolves internally to the IP address of the MiCollab Server and not the MBG IP address.
Cannot reach MiCollab Client Deployment service (401 Unauthorized) from host 12.12.12.12	The MBG does not forward the request to a MiCollab Server but to another machine or web server.
Invalid MiCollab Client Deployment Config download host configured (host: 12.12.12.12)	The Remote Proxy Services does not allow access to the MiCollab Client Deployment Service. Check the MBG Remote Proxy Services configuration.
	Incorrect “Configuration download host” configured in the deployment profile of the MiCollab Client Deployment service.

Table 3: Connection test from public internet to MiCollab Client Service

Error Message	Meaning
ERROR: queryA ENOTFOUND	The DNS name of the MiCollab Client Service cannot be resolved from the internet.
Error: connect ECONNREFUSED	The MiCollab Client Service is not started or not reachable. UCA websocket requests for the TCP port 36008 are blocked by a firewall. The MiCollab Client connector on the MBG is not enabled or is configured incorrectly.
Error: connect ETIMEDOUT	The MiCollab Client Service is not reachable or requests for the TCP port 36008 are blocked by a firewall.
Error: socket hang up	The MiCollab Client Service does not respond. Most likely a connection issue between MBG and MiCollab Server.
Error: read ECONNRESET	The MiCollab Client Service does not respond. Most likely a connection issue between MBG and MiCollab Server.
Error: DEPTH_ZERO_SELF_SIGNED_CERT	TLS certificate issue. The certificate of the MiCollab Client Service is self-signed. Make sure that the certificate is correctly installed on both MBG and MiCollab Server. Run the following command from any other host on the internet in order get more details: `openssl s_client -CAfile / etc/pki/tls/certs/ca-bundle.crt -connect mas.yourmashostname.com:36008 < /dev/null.`

Error Message	Meaning
Error: SELF_SIGNED_CERT_IN_CHAIN	TLS certificate issue. Run the following command from any other host on the internet in order get more details: `openssl s_client -CAfile / etc/pki/tls/certs/ca-bundle.crt -connect mas.yourmashostname.com:36008 < /dev/null`
Error: UNABLE_TO_VERIFY_LEAF_SIGNATURE	TLS Certificate issue. The certificate chain is missing or not properly installed. Verify that the right intermediate certificates are installed on the internet facing MBG. The MBG might require a reboot after certificate installation to activate them.
Error: Hostname/IP doesn't match certificate's altnames	TLS certificate issue. The name of the certificate does not match to the name used by the MiCollab Client server. Run the following command from any other host on the internet in order get more details: `openssl s_client -CAfile / etc/pki/tls/certs/ca-bundle.crt -connect mas.yourmashostname.com:36008 < /dev/null`
Error: Server responded with a non-101 status: 200 Response Headers Follow: content-type: text/html	The connection test gets a reply for the TCP port 36008, but the connection could not be identified as a websocket connection. For some reason a different service or server responds to the request, but not the MiCollab Client service.

Mitel
Powering connections
mitel.com

Copyright 2022, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.