A MITEL
PRODUCT
GUIDE

MiCollab

Thrift Server – Client Certificate Update Guide

Document Version 2.0

July 2025

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), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Preface 1

This chapter contains the following sections:

1.1 Purpose

This document is intended to help MMP, MiVoice MX-ONE, MiVoice 5000, and MiCW partners manage and update their Thrift Certificates that are set to expire in December 2024 within their MiCollab deployments.

1.2 Intended Audience

This guide is intended for administrators and partners of MMP, MiVoice MX-ONE, MiVoice 5000, and MiCW.

1.3 Pre-Requisite

Anyone using this document is expected to have:

1. Basic hands-on using the MiCollab terminal
2. Access to MiCollab terminal
3. Understanding of the certificate generation process
4. Understand the MiCollab server backup-restore process
5. Taken a backup of the MiCollab server

For information on MiCollab processes, refer to the MiCollab Installation and Maintenance Guide.

The related documents for the applications (MMP, MiVoice MX-ONE, MiCW, and MiVoice 5000) are as follows:

- MMP
  - MiCloud Management Portal Installation and Administration Guide
  - MiCloud Management Portal Service Provider Portal Help
- MiCW
  - Mitel Integrated Configuration Wizard Online Help (Online help, hence cross-reference to the document is not available)

- MiVoice MX-ONE
  - Installing MX-ONE Provisioning Manager -Installation Instructions (9_1531-ANF90115)
- MiVoice 5000
  - Mitel 5000 Server Operating Manual

Thrift Certificate – An Overview 2

This chapter contains the following sections:

The Thrift SDK (Software Development Kit) is associated with Apache Thrift, a scalable cross-language services development framework. MiCollab SAS provides a Thrift SDK to application developers, enabling them to create and manage users and services within MiCollab SAS. This SDK is utilized by MMP, MiVoice MX-ONE, MiVoice 5000, and MiCW. Communication between the Thrift server and its clients is secured over SSL and authenticated using mutual TLS (mTLS).

The certificates used for mTLS are generated by MiCollab and are valid for five years.

To ensure seamless integration between MiCollab (which is the server in this scenario) and the client applications like MMP, MiVoice MX-ONE, MiVoice 5000, and MiCW, the certificate used for communication between the MiCollab server, and the application must remain valid. The certificates for the Thrift interface will expire at the end of 2024 and should be renewed.

The objective of this solution is to enable remote token management through a new command line interface.

MiCollab offers an SDK to application developers, enabling them to create and manage users within MiCollab. The SDK uses certificates for secure communication with MiCollab and is utilized by:

- MiClould Management Portal (MMP) (Formerly known as ORIA)
- MiVoice 5000 Web Admin (MiVoice 5000)
- MiVoice MX-ONE Provisioning Manager (MiVoice MX-ONE)
- MiConfiguration Wizard (MiCW)

Steps to manage Thrift Certificates:

1. Certificate Generation
2. Certificate Installation
3. Configuration
4. Renewal and Revocation

2.1 Limitations

- This script is supported with MiCollab version 9.x and higher (until version 10.0).
- The MiCollab server does not have a UI for generating Thrift server certificates.
- Server upgrades require manual steps.
- Updating the Thrift server and client certificates will impact service, so it should be performed during off-hours.
- Up until MiCollab Release 10.0, there is no alarm in MiCollab to notify the admins of an expiring certificate.

Getting Started 3

This chapter contains the following sections:

A new capability is developed for the MiCollab server to generate certificates at runtime and share them with client applications. This functionality is introduced as a side-loaded patch containing a script for MiCollab version 9.x onwards until version 10.0. Additionally, this capability will be integrated into the server manager in future MiCollab versions.

3.1 Solution

The objective of this solution is to be as simple and easy as possible while ensuring that:

- The solution is secure.
- The partner/customer can self-manage certificates on an ongoing basis.
- Remote token management through a new command line interface.

1. **Distribution of the solution**

   A patch script is shared at https://downloads.mitel.io/micollab/patches/genThriftCertificate.tar.gz. See the Generate Thrift Server Certificate on page 4 section in this document for more details.
2. **How to generate a new Thrift Certificate?**

   The administrator will run a script on the MiCollab server to generate a new certificate to upgrade their installed base.
3. **Distribution of the certificate**

   a. The certificates are generated on MiCollab server.
   b. The administrator will transfer the newly generated certificate on all MiVoice MX-ONE, MMP, MiCW, and MiVoice 5000 over SFTP or SCP.
   c. Customers can now use the new certificate on all the platforms mentioned.

3.2 Generate Thrift Server Certificate

Perform the following steps to generate the Thrift Server Certificate on MiCollab server using the script:

1. Download `genThriftCertificate.tar.gz` from:

   https://downloads.mitel.io/micollab/patches/genThriftCertificate.tar.gz
2. Copy `genThriftCertificate.tar.gz` to *usr/mas/bin* directory.

3. Navigate to the *usr/mas/bin* directory:

```
cd /usr/mas/bin/
```

4. Extract the tar.gz in the current directory using:

```
tar -xvzf genThriftCertificate.tar.gz
```

5. Run the python script to generate the certificate:

```
[root@vmas91 bin]# python genThriftCertificate.py
```

The Menu options that are displayed are defined below:

1. **List certificate details**: Displays the details of existing certificates.
   - Alias name: The unique identifier for the certificate.
   - Creation date: When the certificate was created.
   - Valid from: The start date and time from which the certificate is valid.
   - Valid until: The expiry date and time of the certificate.
   - Owner: The owner of the certificate, typically including email and other identifying information
2. **Generate server certificate**: Creates a new server certificate.
3. **Generate client certificate**: Creates a new client certificate.
4. **Revoke client certificate**: Revoke an existing client certificate.
5. **Renew server certificate**: Renews an existing server certificate.
6. **Restore previous certificate**: Restores a previously backed-up certificate.
7. **Exit**: Exits the script.

3.3 Usage of Menu

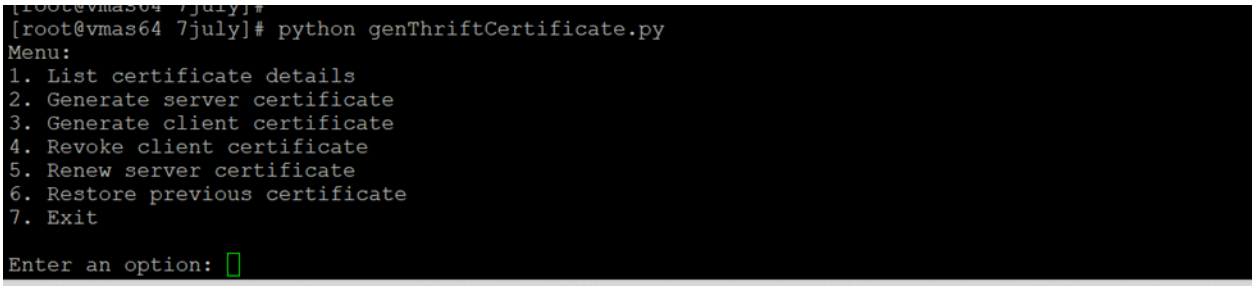
For servers with expiring certificates, administrators must run the menu option 2 (see section *Generate server certificate*) and menu option 3 (see section *Generate client certificate*) to update certificates on the MiCollab server and the client application platforms (MMP, MiVoice MX-ONE, MiCW, and MiVoice 5000). The other menu options help administrators manage the certificate lifecycle effectively.

During the certificate creation or update process, zip files containing the required data will be created in the */usr/mas/bin* directory for Thrift clients to download (utilizing a token per client, generated as part of the process). Once the Thrift client downloads the zip file, it is no longer required, and therefore a cron job is utilized to delete these zip files nightly.

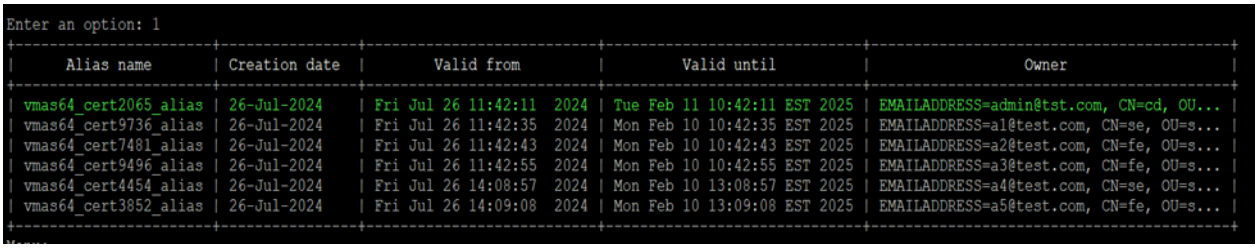
Warning:
After updating the Thrift server and client certificates, the script restarts the mom-server, causing a brief impact on MiCollab services (why we recommend doing this at off-hours). A cron job is scheduled to delete all existing ZIP files in the /usr/mas/thrift directory. It does not verify the validity of any certificates and will delete all certificates located in the /usr/mas/bin directory. This script runs nightly.

1. **Listing Certificates**: To view the list of server and client certificates installed on the MiCollab server and their details, perform the following.

   a. To list MiCollab Thrift Server Certificates installed on the server, run the script `genThriftCertificate.py` from the MiCollab terminal and select option 1.



   b. The terminal will display a list of server certificates. The list displays the certificate alias name, creation date, valid from, valid until, and *certificate owner information.*



   As seen or displayed in green in the above screenshot, the server-side certificate will be the first element in the list from the top. The list is sorted based on creation date, and the first created certificate is listed first.

2. **Generate server certificate:** If the existing MiCollab Thrift server/client certificates are about to expire or have already expired, the MiCollab admin needs to generate new certificates.

Note:
When generating a server certificate, the admin will specify how long the certificate will be valid. This ensures the certificate is up-to-date and prevents issues when it eventually expires.

Note:
If the server certificate's validity is less than 6 months, you cannot create a client certificate.

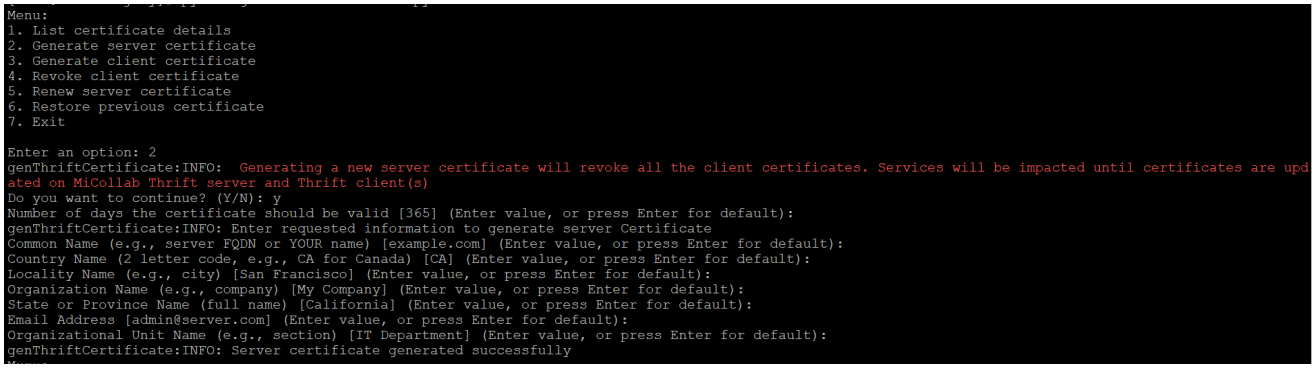
a. To generate a new MiCollab Server Thrift certificate, run the script `genThriftCertificate.py` from the MiCollab terminal and select option 2.

b. As an administrator, you will be prompted to enter the required information to generate the server certificate. The values to be entered are self-explanatory, and you can refer to the table below for additional details:

Field	Description	Example	Notes
Number of days the certificate should be valid (365)	Validity period of the Thrift Certificate.	365 days is the default value, or any number of days can be specified by the admin. Minimum validity period should be of 180 days.	The default value is 365 days, but the admin can modify it. If no value is provided, it defaults to 365 days for the Thrift server certificate expiry. At the end of the validity period, the admin must renew the certificate again.
Common Name (CN)	The server's domain name (FQDN) or your own name	example.com	The domain name of the server or system for which the certificate is being generated
Country Name (C)	A two-letter country code as per ISO 3166 standard, representing your country	US (for USA)	Only two letters are permitted, and they must follow the ISO 3166 standard (e.g., 'IN' for India)

Field	Description	Example	Notes
Locality Name (L)	The city or locality where your organization is located	San Francisco	Optional but helps specify your location for additional identification
Organization Name (O)	The legal name of your organization or company	Mitel	The full official name of your company or organization, if applicable
State or Province Name (ST)	The full name of the state or province where your organization is located	California	Must be the full name, not an abbreviation (e.g., 'California' instead of 'CA')
Email Address	The contact email address for the administrator responsible for the certificate	admin@example.com	Used for administrative purposes and contact.
Organizational Unit Name (OU)	The specific department or division within your organization	IT Department	IT Department

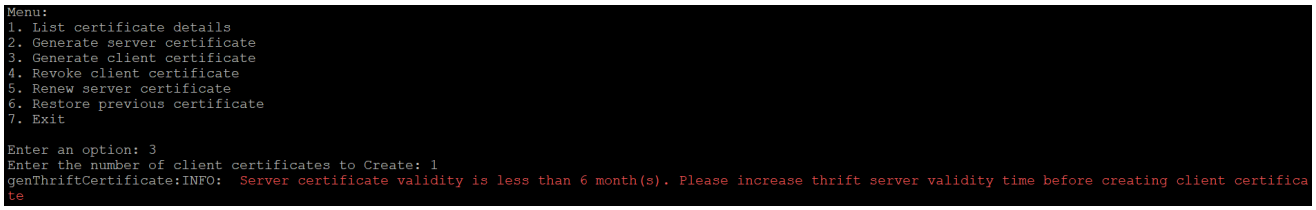
Note:
Ensure the server certificate CN is distinct from the CN of any client certificate to avoid validation errors during mutual authentication.



This process will replace all existing server and client thrift certificates installed on MiCollab server. Once the server certificate is generated, all actions from client are not possible until the client certificate is generated.

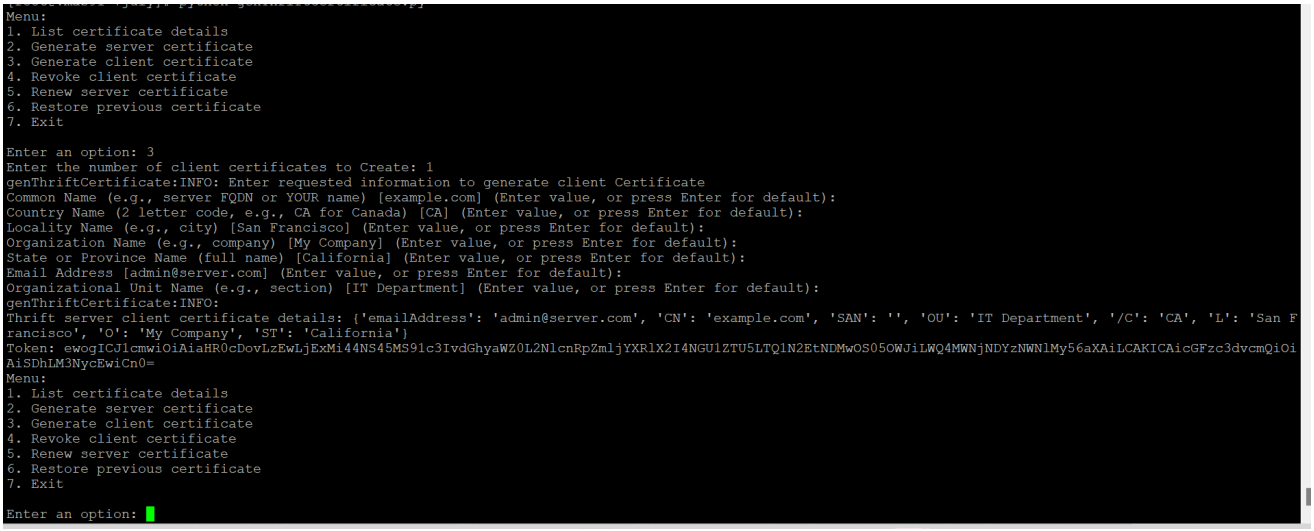
3. **Generate client certificate:** To generate a new Thrift client certificate corresponding to an existing Thrift server certificate, so that the MiCollab Thrift server and client can establish an SSL connection, perform the following:

Note:
If the server certificate's validity is less than 6 months, you cannot create a client certificate. To proceed, extend the server certificate's validity to at least 6 months by renewing or generating a new one first.



a. To generate a new client certificate which should be installed on Thrift server clients, run the script `genThriftCertificate.py` from the MiCollab terminal and select option 3.

b. As an administrator, you will be prompted to enter the required information to generate the client certificate. The values to be entered are self-explanatory, as shown in the screenshot below or refer to the table under *Generate server certificate* section for information on the values to be entered.



Note:
Ensure that client certificates have unique Common Names (CNs) to prevent conflicts.

The Common Name (CN) in a certificate is used to identify the entity, whether it's a server or client, during communication. If both the server and client certificates share the same CN, it can cause confusion during the SSL/TLS handshake, as the system may struggle to differentiate between the two entities, potentially leading to validation errors.

c. Once the script is executed successfully, it will generate a token as shown in the output below.

```
genThriftCertificate:INFO

ewogICJjZXJ0aWZpY2F0ZTEiOiB7CiAgICAidXJsIjogImh0dHA6Ly8xMC4xMTIuODUuMTMwL

3Vzci90aHJpZnQvY2VydGlmaWNhdGVfMS56aXAiLCAKICAgICJwYX

Nzd29yZCI6ICI/R1R8Wi9lbTVDOHwiCiAgfQp9
```

```
Menu:
1. List certificate details
2. Generate server certificate
3. Generate client certificate
4. Revoke client certificate
5. Renew server certificate
6. Restore previous certificate
7. Exit

Enter an option: 3
Enter the number of client certificates to Create: 2
genThriftCertificate:INFO: Enter requested information to generate client Certificate
Enter Common Name (CN): se
Enter Country (C): fe
Enter Locality (L): se
Enter Organization (O): fe
Enter State or Province Name (ST): se
Enter Email (emailAddress): wd@test.com
Enter Organizational Unit (OU): se
genThriftCertificate:INFO: Enter requested information to generate client Certificate
Enter Common Name (CN): fe
Enter Country (C): se
Enter Locality (L): fe
Enter Organization (O): se
Enter State or Province Name (ST): fe
Enter Email (emailAddress): de@test.com
Enter Organizational Unit (OU): se
genThriftCertificate:INFO:
Thrift server client certificate details: {'emailAddress': 'wd@test.com', 'CN': 'se', 'SAN': '', 'OU': 'se', '/C': 'fe', 'L': 'se', 'O': 'fe', 'ST': 'se'}
Token: ewogICJ1cmwiOiAiaHR0cDovLzEwLjExMi44NS45MS91c3IvdGhyaWZ0L2NlcnRpZmljYXRlXzBmM2EzOGQ5LWNiZWEtNDliMS04OTAwLWRmNGVlMWMwODlkOC56aXAiLCAKICAicGFzc3dvcmQiOiAiNG9OazRKRSIKfQ==
genThriftCertificate:INFO:
Thrift server client certificate details: {'emailAddress': 'de@test.com', 'CN': 'fe', 'SAN': '', 'OU': 'se', '/C': 'se', 'L': 'fe', 'O': 'se', 'ST': 'fe'}
Token: ewogICJ1cmwiOiAiaHR0cDovLzEwLjExMi44NS45MS91c3IvdGhyaWZ0L2NlcnRpZmljYXRlX2M5ZTAyMmY5LTAyYjQtNDMyMi04MmZlLTYwNTY3ZGYzMWIwNC56aXAiLCAKICAicGFzc3dvcmQiOiAiWU43RXJKSEkiCn0=
Menu:
```

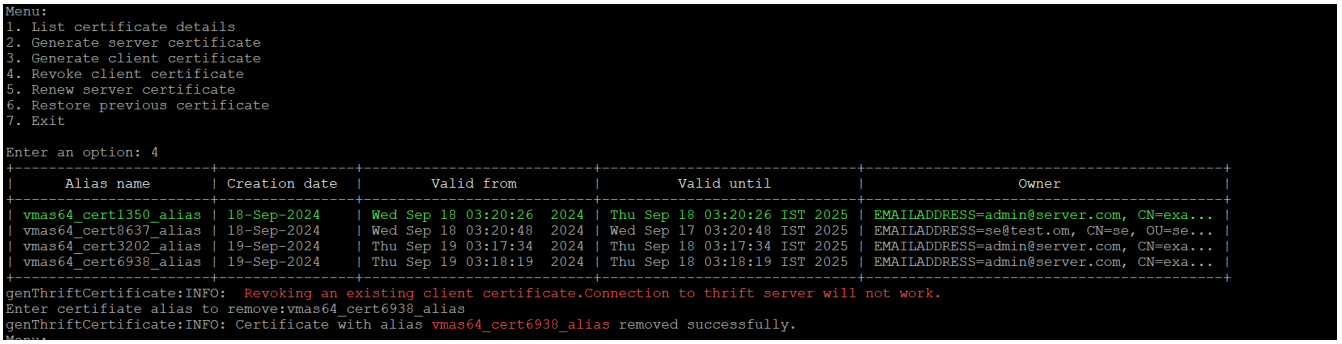
Note:
Make a note of the token(s) displayed, as these will need to be provided to the client applications (MiVoice 5000 Manager, MiVoice MX-ONE Provisioning Manager, MiCW, and MMP) to download certificates from the MiCollab server.

Note:
The admin can generate any number of client certificates.

4. **Revoke client certificate:** When an administrator needs to revoke a certificate issued to a Thrift server client, they do so to either issue a new certificate to the client or remove the client from the network. Only the certificate associated with the alias will be removed from the MiCollab Server; there will be no impact on other certificates. Server certificate CANNOT be revoked.

   a. To revoke a new certificate and install it on the MiCollab server, run the script `genThriftCertificate.py` from the MiCollab terminal and select option 4.

   This process will replace existing server and client thrift certificates installed on MiCollab server.



> **Note**:
> You can delete the client certificate using the alias name, but you cannot delete the server certificate.

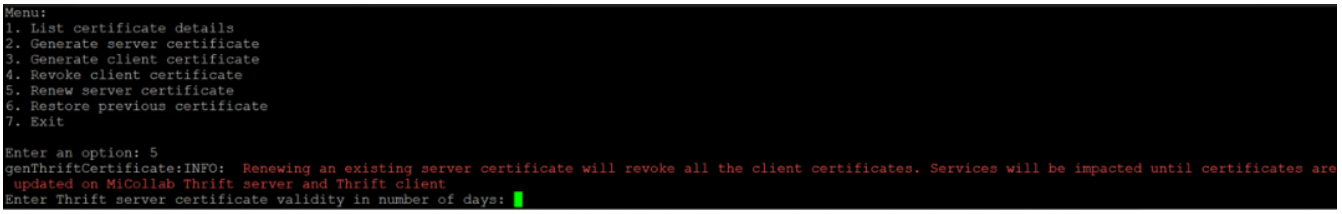
5. **Renew server certificate:** This is done to update the validity of an already existing server certificate. Admin will not be prompted to enter existing server details.

   In this scenario, all client certificates will be regenerated, and the associated tokens will be displayed. The only input required is the duration of the new certificates, which specifies how long they will remain valid.

Warning:
During this operation, client apps will cease communication with the server until the updated certificate is installed on them. Ensure you perform this task only when you can promptly install the new certificate on the client apps.

a. To renew a server certificate, run the script, `genThriftCertificate.py` from MiCollab terminal and select option 5.

b. When renewing the server certificate, the script will prompt you to "*Enter Thrift server certificate validity in number of days*."



The new tokens for the client certificates will be displayed. Use these to update the clients with their respective certificates, as per the sections below depending on the product type.

6. **Restore previous certificate:** This procedure is useful in situations where you need to restore your certificates to a previously known good state, such as after a failed update (attempt to generate thrift server or thrift client certificate) or when troubleshooting issues related to certificate renewals.

   a. To restore a previously installed client certificate on Thrift server clients, run the script `genThriftCertificate.py` from MiCollab terminal and select option 6.

```
[root@vmas64 7july]# python genThriftCertificate.py
Menu:
1. List certificate details
2. Generate server certificate
3. Generate client certificate
4. Revoke client certificate
5. Renew server certificate
6. Restore previous certificate
7. Exit

Enter an option:
```

```
Menu:
1. List certificate details
2. Generate server certificate
3. Generate client certificate
4. Revoke client certificate
5. Renew server certificate
6. Restore previous certificate
7. Exit

Enter an option: 6
genThriftCertificate:INFO: Certificate on MiCollab Server Restored Successfully!
```

   b. When you run the script to restore previous certificates, it reinstates all certificates created earlier, except for the currently running certificate.

      This process involves the following steps:

      i. **Identify Previous Certificates**: The script will first identify all certificates that have been created and stored in the system.
      ii. **Exclude Current Certificate**: The current running certificate, which is actively being used, will be excluded from the restoration process to ensure there is no interruption in service.
      iii. **Restore Certificates**: The script will then restore all other identified certificates to their previous states. This ensures that all previously-valid certificates, except the current one, are reinstated.

7. **Exit (Exiting the program)**

   The script includes an option to exit the program or exit from the script.

```
Menu:
1. List certificate details
2. Generate server certificate
3. Generate client certificate
4. Revoke client certificate
5. Renew server certificate
6. Restore previous certificate
7. Exit

Enter an option: 7
genThriftCertificate:INFO: Exiting program...
```

3.3.1 MiCollab Scripts used for Thrift Certificate Management

There are a total of four scripts used for the management of Thrift Certificates, but the administrator managing the certificates only needs to run the script: `genThriftCertificate.py`.

1. **`genThriftCertificate.py`**: When you generate the server certificate using `genThriftCertificate.py`, it will automatically create `/home/e-smith/thriftbackup` and store the current certificate there. This ensures that any MiCollab backup taken after this process will recover the existing certificate.
2. **`55MASThrift`**: This is used to create an entry in the Apache configuration; it is not used in the manual certificate management process.
3. **`removeZipFile.py`** :This script is run to remove files from the HTTP repository and is not used in the upgrade path.
4. **`restoreFromDbBackupOVAUpgrade.py`**: This script is used when the server is upgraded from an OVA file using a database backup-restore or upgraded from a running server.

Note:
Any errors encountered during script usage will be logged in `/var/log/genThriftCertificate.log`

Note:
The scripts are not backed up. Therefore, following a new OVA deployment, it is essential for the admin to download the patch from *Mitel.io* , and subsequently, transfer it to the MiCollab Server directory located at `/usr/mas/bin` folder, and run the `restoreFromDbBackupOVAUpgrade.py` script.

MiCollab Server Upgrades 4

This chapter contains the following sections:

When upgrading a server, it's important to restore all key settings, including certificates, to keep the system secure and stable. The admin should manually run the script `restoreFromDbBackupOVAUpgrade.py` to restore the new server certificates after the upgrade is done.

Following any re-deployment of MiCollab, whether for an upgrade, rebuild, or other reasons, it is essential for the administrator to re-download `genThriftCertificate.tar.gz`, even if the backup from the previous server contains the certificates. This process is crucial for reinstating the ability to manage certificates and obtaining the file `restoreFromDbBackupOVAUpgrade.py`, which is referenced in the subsequent steps. Failure to execute this re-download will result in the absence of this critical file.

4.1 Moving forward

- If your system includes an MMP client, refer to Chapter MiCollab Thrift Certificate Renewal and Update Information for MMP.
- If your system includes an MiCW client, refer to Chapter MiCollab Thrift Certificate Renewal and Update Information for MiCW.
- If your system includes an MiVoice MX-ONE client, refer to Chapter MiCollab Thrift Certificate Renewal and Update Information for MX-One.
- If your system includes a MiVoice 5000 client, refer to Chapter MiCollab Thrift Certificate Renewal and Update Information for MiVoice 5000.

MiCollab Thrift Certificate Renewal and Update Information for MMP

5

This chapter contains the following sections:

MMP interacts with MiCollab to fetch details using the Thrift Certificate for data synchronization. Starting from MMP Release 6.2 SP4, a new maintenance command has been introduced to update the renewed Thrift certificates in MMP from MiCollab.

When you run the new MMP maintenance command, MMP will fetch the newly generated certificate from MiCollab and store it in the MMP keystore path for accessing MiCollab.

5.1 Prerequisite

The new capability of certificate renewal requires the following:

- A Base64-encoded token generated from MiCollab.
- A client certificate, which can be obtained using a token. To generate a new token as part of the certificate renewal process, refer to the Generate Thrift Server Certificate on page 4 section.
- All existing MMP setups must be upgraded to version 6.2 SP4 or above before the current certificate expires.

5.2 Updating the Thrift Certificate for MMP

Note:
The same procedure should be followed before registering a new platform in MMP. The platform group hostname and the maintenance command **<IP/Hostname>** must match the configuration the customer will set up. First, run the maintenance command, then create the platform group using the IP/hostname provided in the command.

Perform the following procedure to update or renew the Thrift Certificate:

1. In a web browser, enter the URL *https://<IP or Host>/konos/commands.jsp* to access the MMP Maintenance Command page.

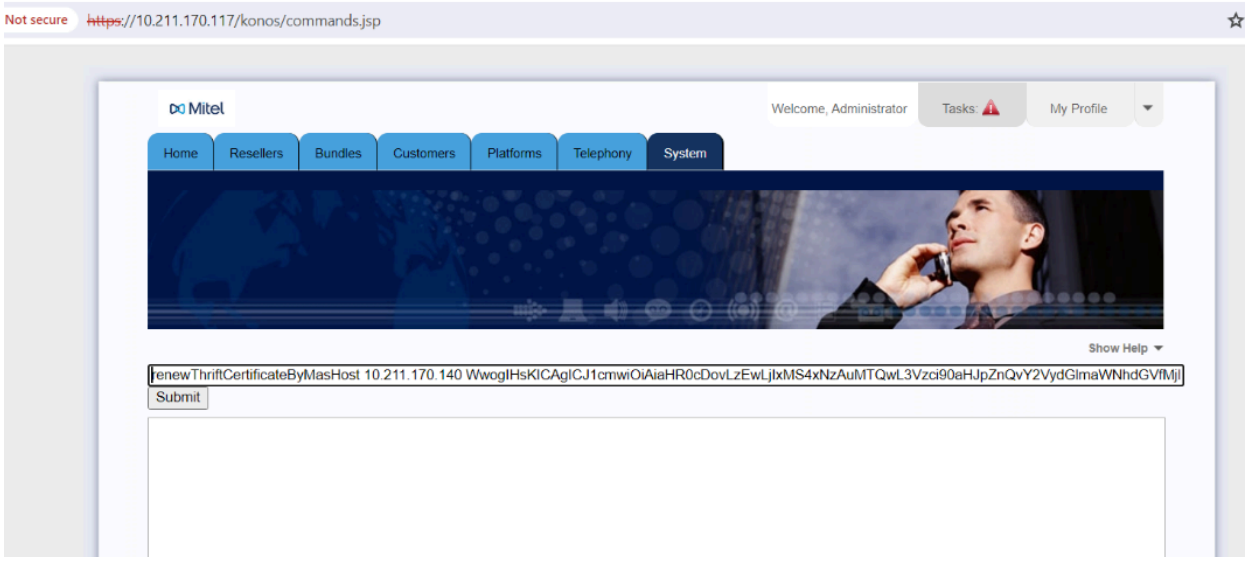
2. In the Maintenance Command page enter the details using the following syntax:

```
renewThriftCertificateByMasHost <MiCollab IP Address/Host name> <MiCollab
Thrift Token>
```

Example: **`renewThriftCertificateByMasHost`** `10.211.170.140`
`WwogIHsKICAgICJ1cmwiOiAiaHR0cDovLzEwLjIxMS4xNzAuMTQwL3Vzci90aHJpZnQvY2VydGlmaWNhdGV`

`GlmaWNhdGVfMjhhYWU1MDgtNTZkMC00NTA3LWIxMTQtNmM0NDVhMjg`

`4Y2Y5LnppcCIsIAogICAgInBhc3N3b3JkIjogImJDTHdIb1dOIgogIH0KXQ==`



3. Click **Submit** to proceed.

Once the Thrift certificate is successfully updated, a confirmation message will be displayed.

MiCollab Thrift Certificate Renewal and Update Information for MiCW

6

This chapter contains the following sections:

After December 2024, connections from MiCW to MiCollab will cease to operate with the existing Thrift certificate. If new certificates are not generated and used in MiCW from the respective MiCollab, both existing and new customers will be affected.

6.1 Prerequisites

The new capability of certificate renewal requires the following:

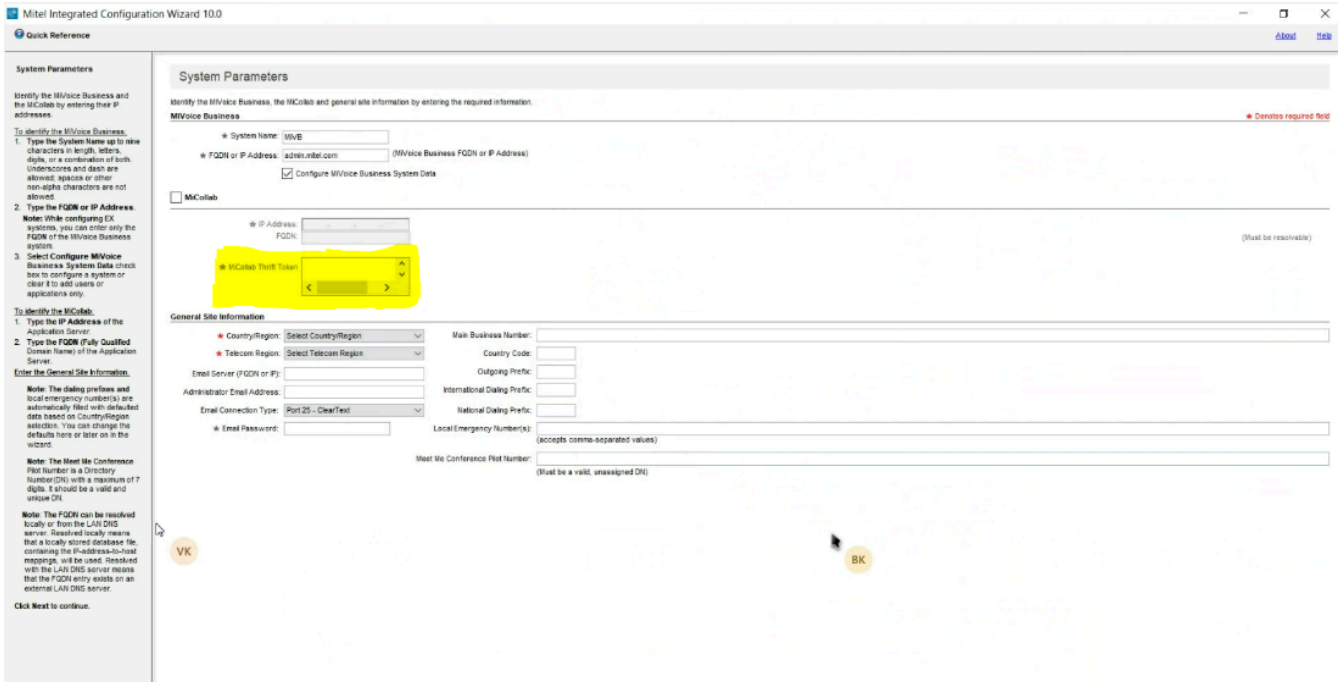
- MiCW version 10.1 SP2 and above.
- A client certificate, which can be obtained using a token. To generate a new token as part of the certificate renewal process, refer to the Generate Thrift Server Certificate on page 4 section.

6.2 Updating Thrift Certificate for MiCW

1. In the Mitel Integrated Configuration Wizard, navigate to the **System Parameters** page.
2. Enter the Thrift token details in the **MiCollab Thrift Token** field and click **Submit.**

Note:

This field is a mandatory (*) input field when the MiCollab checkbox is enabled for new and existing setups.



MiCW validates the token, downloads the certificate from MiCollab, and stores it in the MiCW keystore path location.

After successfully extracting and replacing the certificate, MiCW can now fetch and update information on MiCollab.

MiCollab Thrift Certificate Renewal and Update Information for MiVoice MX-ONE 7

This chapter contains the following sections:

Thrift certificates are used to authenticate and encrypt communications between various components within the MiVoice MX-ONE and MiCollab systems.

7.1 Prerequisites

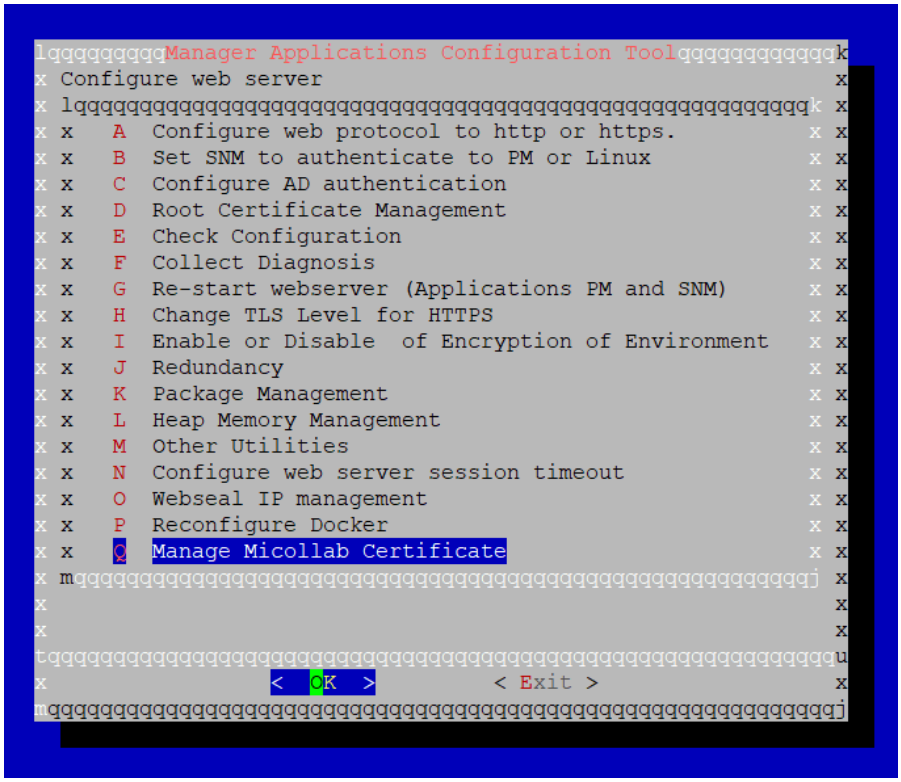
The new capability of certificate renewal requires the following:

- MiVoice MX-ONE version 7.7 SP1 onwards. For older versions, the solution will be provided as a patch along with the necessary Java binaries.
- A client certificate, which can be obtained using a token. To generate a new token as part of the certificate renewal process, refer to the Generate Thrift Server Certificate on page 4 section.

7.2 MiVoice MX-ONE Thrift Certificate Management: Updates and Renewals

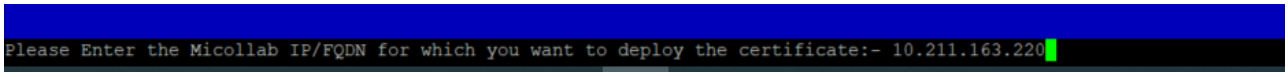
This section is applicable for MiVoice MX-ONE version 7.7 SP1 and higher.

1. Navigate to the new `Manage MiCollab Certificate` option in **`webserver_config`**

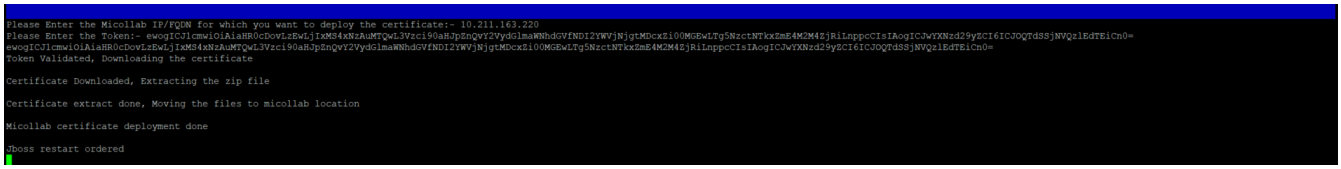


2. Enter the IP address or FQDN of the MiCollab server where the certificate should be deployed in PM/ SNM.

> **Note**:
> The IP or FQDN of the MiCollab server must match with what is configured in the PM subsystem.



3. Enter the token received from MiCollab Server (refer to prerequisites for token generation).



If the token is valid, it will fetch the certificate and deploy it to the PM server, initiating a restart of JBoss. If the token is invalid, an error message will be displayed on the console.

7.3 Deployment Steps for Java libraries/binaries

This section is applicable for MiVoice MX-ONE versions lower than 7.7 SP1 and java binaries are available for the following versions:

- 7.5 SP1
- 7.6 SP0
- 7.6 SP1
- 7.7 SP0

Download the java binary and patch from:

https://mitel.custhelp.com/app/answers/answer_view/a_id/1020747/loc/en_US

Copy the binaries to /local/home/mxone_admin folder of the MiVoice MX-ONE Server(PM Server in case of Standalone setup).

Note:
Use the java binary that matches the installed PM version.

Java libraries deployment

- Take a backup of the `mp.ear` file from `/opt/jboss/standalone/deployments` and save it to an alternative location.
- Copy the provided binaries to this location:

  `/opt/jboss/standalone/deployments`
- Navigate to `/opt/jboss/standalone/deployments` and run the command: `chmod 775 mp.ear`
- In the same directory, execute the command:

  `chown jboss:jboss mp.ear`
- Restart the JBoss web server from the `webserver_config` by selecting **Restart webserver.**

Patch deployment

1. Navigate to */local/home/mxone_admin* folder and execute the below command to change the permissions of the script file to make it executable:

   `chmod +x deploymicollabthriftcertificate.sh`
2. In the same directory, execute the command:

   `./deploymicollabthriftcertificate.sh`
3. When prompted, provide the MiCollab token. The token is needed to authenticate the deployment process. Refer to the specific instructions under the Generate Thrift Server Certificate on page 4 section to obtain this token.

MiCollab Thrift Certificate Renewal and Update Information for MiVoice 5000

8

This chapter contains the following sections:

8.1 Prerequisite

The new capability of certificate renewal requires the following:

- MiV5000 version R8.2 SP1, R8.1 SP3, R7.2 SP7 onwards.
- A client certificate, which can be obtained using a token. To generate a new token as part of the certificate renewal process, refer to the Generate Thrift Server Certificate on page 4 section.
- Ensure that TCP port 80 is open for incoming connections on the MiVoice 5000 system. This port is required for MiCollab Provisioning to perform an HTTP request to download certificates during initial setup.

Note:
When a new server certificate is generated, it affects all systems that were using the previous common certificate. As a result, MV5000 provisioning will not function properly on any system until new client certificates are generated and applied to each MV5000.

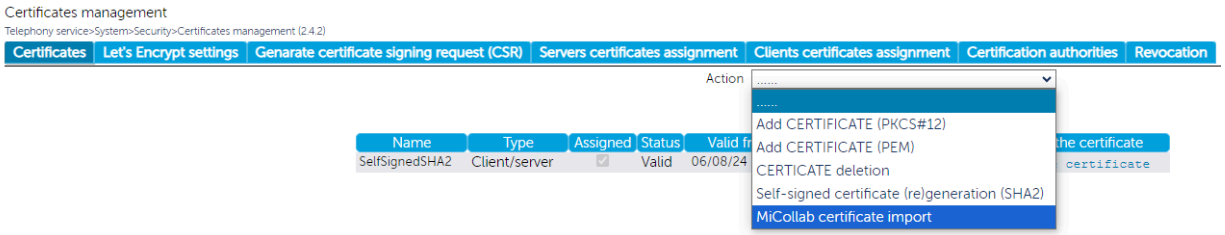
8.2 Updating Thrift Certificate for MiV5000

1. In the MiVoice 5000 Web Admin, navigate to **System > Security > Certificates management.**

Note:
This menu is used to manage the certificates installed and/or to be installed depending on the intended use. This action allows you to manually import the MiCollab Thrift Certificate.

2. From the **Actions** field dropdown menu select the option *MiCollab Certificate Import*.

   A Code field appears when the action is selected.



3. In the **Code** field enter the code generated by MiCollab during certificate generation.

   The Validation button then appears.

4. Click **Validation** to prompt the Call Server to retrieve the MiCollab Thrift certificate.

   The certificate is now:

   - visible on the list of certificates
   - can be assigned to a client in the Clients certificate assignment tab.