Mitel MiVoice Business

SECURITY CERTIFICATE UPDATE PROCEDURES FOR PRE-MIVB 9.0

NOTICE

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.

Trademarks

Mitel, and MiVoice Business are trademarks of Mitel Networks Corporation.

Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Root Certificate Update Procedures
V1

July 2019

Table of Contents

Purpose of this Document

On August 21, 2020 15:52:50, the MiVB's AMC root certificate will expire. As a result, all MiVB systems running release MCD 5.0 to MIVB 9.0 SP2 must be updated with a new AMC root certificate prior to the expiry date to prevent the system from going into critical license violation.

To update the AMC root certificate on the MiVB, refer to Table 1 for the summary of upgrade options.

Table1: AMC root certificate upgrade options

MCD/MIVB version	AMC root certificate Upgrade options	Remarks
MiVB 9.0 ~ MiVB 9.0 SP2	Upgrade to MiVB 9.0 SP3 or later	MiVB 9.0 SP3 includes the new AMC root certificate
MCD 5.0~MIVB 8.0 SP3 PR3	Manually apply the AMC root certificate for online licensing only; OR	Manual process does not require to reboot.
	Use Software Installer (S.I) 14.0.0.15 to apply the root certificate. For offline licensing option, S.I is required.	S.I Tool activates the patch by rebooting MIVB automatically
For pre-MCD 5.0	Not applicable	

This document describes procedures to update the AMC root certificate on systems running pre-9.0 software:

- S.I Update Procedure for all platforms

  Troubleshooting
- For Manual Update procedure, please download these patches for each associated platform from Software Download Center > MiVoice Business > AMCRootCertExpiryPatch for Pre-MiVB9.0

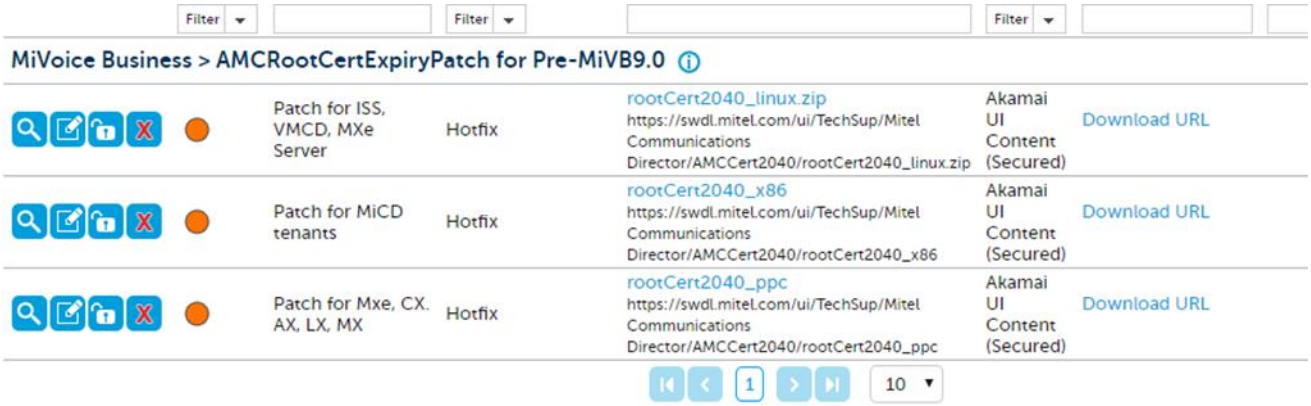


Table 2: Tools and patch deliverables required to manually update AMC root certificate

Platform Type	AMC root Patch deliverables	Tools required
AX CX, CXi (II) LX, MX MXe	rootCert2040_ppc	Tool= FTP for transferring patch RTC shell access (serial port or equivalent)
MiCD tenant(s)	rootCert2040_x86	Tool = FTP for transferring patch Putty (SSH) to access RTC shell
ISS,vMiVB, MIVBx Stratus, MXe Server	rootCert2040_linux.zip	Tool = WinSCP or sFTP for transferring patch Putty (SSH) to access RTC shell

- Manual Update Procedure for AX, CX, CXi, LX, MX, or MXe Systems
- Manual Manual Update Procedure for MICD Systems
- Manual Manual Update Procedure for ISS, vMiVB, MIVBx, MXe Server, Stratus Systems
- S.I Update Procedure for all platforms
- Troubleshooting

For Manual Update procedure, please download these patches for each associated platform from Software Download Center > MiVoice Business > AMCRootCertExpiryPatch for Pre-MiVB9.0

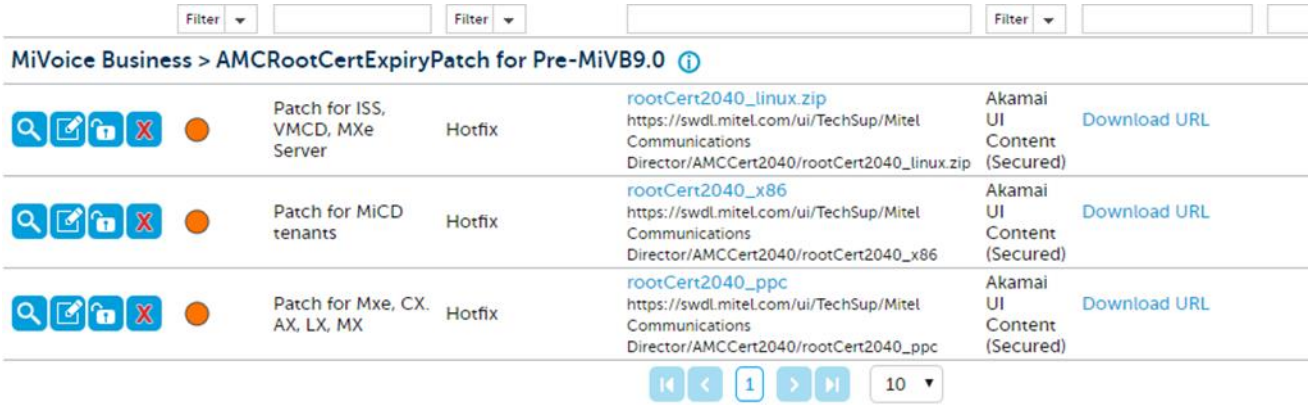


Table 2: Tools and patch deliverables required to manually update AMC root certificate

Platform Type	AMC root Patch deliverables	Tools required
AX CX, CXi (II) LX, MX MXe	rootCert2040_ppc	Tool= FTP for transferring patch RTC shell access (serial port or equivalent)
MiCD tenant(s)	rootCert2040_x86	Tool = FTP for transferring patch Putty (SSH) to access RTC shell
ISS,vMiVB, MIVBx Stratus, MXe Server	rootCert2040_linux.zip	Tool = WinSCP or sFTP for transferring patch Putty (SSH) to access RTC shell

Manual Update Procedure for AX, CX, CXi, LX, MX, or MXe Systems

Preparation:

a. Download the rootCer2040_ppc update (see page 4)
b. RTC shell access (serial port of the controller or Putty to system IP with port 2002 in raw mode)
c. FTP from DOS prompt or FTP application for transferring patch in BINARY mode.

Step 1	FTP rootCert2040_ppc to the /sysro folder of 3300 ICP system in Binary mode
	You can use your preferred FTP client. If you are not familiar with FTP, you can use the instructions below to FTP from the windows operation system To access DOS prompt: • To open the Windows command line, click Start > **Run**… • In the Run dialog, type: **cmd** and then click **OK**. A new DOS window opens, displaying the current path of C:/ < >. • Type: cd / to change the directory to where rootCert2040_ppc is To start FTP session in DOS: • Type: ftp <IP address of controller> and log in with ESM credentials. • Type: bin #for binary mode • Type: put rootCer2040_ppc • Type: bye #To terminate
Step 2	To install rootCert2040_ppc

	On RTC shell, type: ld </sysro/rootCert2040_ppc
	`-> ld </sysro/rootCert2040_ppc`
	`Wrote new certificate to /sysro/certificate/LM_AMC_root.pem`
	`New root certificate activated.value = 484762168 = 0x1ce4e238`

Step 3	To perform AMC sync to update ARID and/or GARID with the newly installed certificate
	3a> Launch ESM > License and Options Selection Form, click **Change**, click **Retrieve License** to perform AMC sync, then click **SAVE** 3b> For GARIID if applicable, access the Application Group Licensing form, click **Change**, click **Save** **Note: For offline licensing sync, S.I 14.0.0.15 or higher is required.**
Step 4	To validate if the new certificate is in use after AMC sync.
	4a> View ESM maintenance logs and verify that the software version would have ".9" appended to the current system's software version. "xx.9" confirms that new certificate is in use after AMC sync. Maintenance 1528 Warning 2019/Jun/05 08:44:00 Licensing AMC sync 3300-14.0.9=software 4b> (optional) View the ARID/GRID record in AMC to confirm that ".9" is appended to software version. Software Version : Software Version 3300 ICP / MCD MiVB 8.0.9

Manual Update Procedure for MICD Systems

Preparation:

a. Download the **rootCer2040_x86** update from software download center (see page 4)
b. RTC shell access (Require Putty or similar application to establish SSH session to MiCD server)
c. FTP from DOS prompt or FTP application for transferring patch in BINARY mode

Step 1	FTP **rootCert2040_x86** to the /sysro folder of 3300 ICP system in Binary mode
	You can use your preferred FTP client. If you are not familiar with FTP, you can use the instructions below to FTP in the windows operation system To access DOS prompt: • To open the Windows command line, click Start > **Run**… • In the Run dialog, type: **cmd** and then click **OK**. A new DOS window opens, displaying the current path of C:/ < >. • Type: cd / to change the directory to where rootCert2040_ppc is To start FTP session in DOS: • Type: ftp <IP address of controller> and log in with ESM credentials. • Type: bin #for binary mode • Type: put rootCer2040_x86 • Type: bye #To terminate
Step 2	To establish RTC shell of a tenant

	To identify the tenant ID in which patch will be applied,
	Launch I.E browser and access MICD sever-manager (https://<x.x.x.x>/server-manager) -> Applications > MiVoice Business Mulit-instance, identify the ID for RTC shell access.
	
	To establish RTC shell of a specific tenant,
	Launch Putty to establish SSH session to MiCD server and login as root user
	Type: mcd-debug-console N where N (e.g. 17) is the tenant ID to be entered.
	`login as: root`
	`root@10.37.54.2's password:`
	`Last login: Fri May 31 14:29:38 2019 from 10.35.27.23`
	`[root@micdlsupport ~]# mcd-debug-console 17`

Step 3	To install rootCert2040_x86

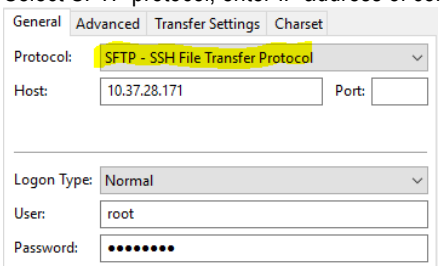
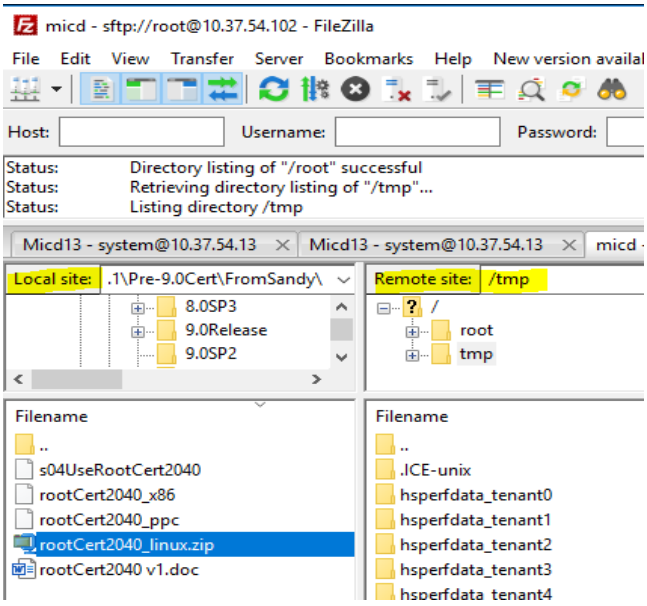
	On RTC shell (with ->prompt), type: ld </sysro/rootCert2040_x86
	Tip: If you do not see -> prompt, press Enter.
	`-> ld </sysro/rootCert2040_x86`
	`Wrote new certificate to /sysro/certificate/LM_AMC_root.pem`
	`New root certificate activated.value = 982517236 = 0x3a9005f4`
	`->`

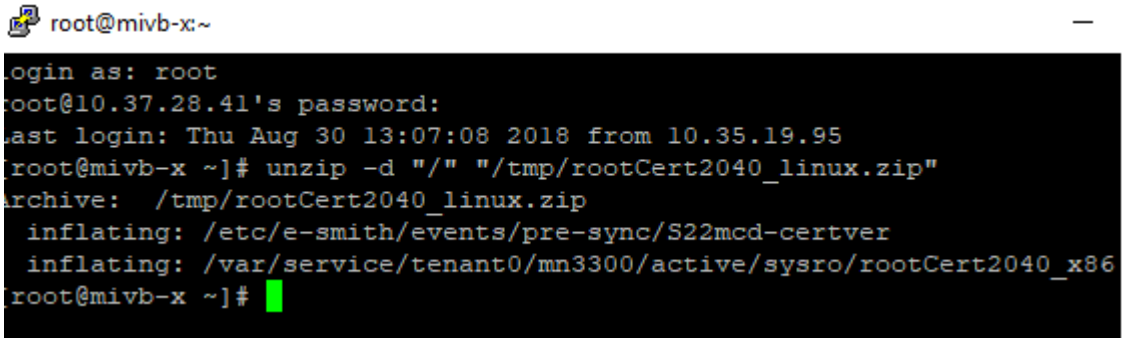
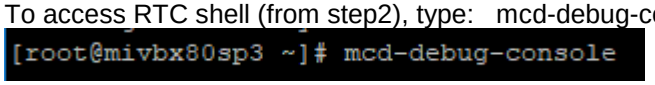
Step 4	To perform AMC sync to update ARID and/or GARID with the newly installed certificate
	4a> Launch ESM > License and Options Selection Form, click **Change**, click **Retrieve License** to perform AMC sync, then click **SAVE;** and/or 4b> For GRAID if applicable, access the Application Group Licensing form, click **Change**, click **Save**
Step 5	To validate if the new certificate is in use after AMC sync.
	5a> View ESM maintenance logs and verify that the software version would have ".9" appended to the current system's software version. "xx.9" confirms that new certificate is in use after AMC sync. Maintenance 1528 Warning 2019/Jun/05 08:44:00 Licensing AMC sync 3300-14.0.9=software 5b> (optional) View the ARID/GARID record in AMC to confirm that ".9" is appended to software version. Software Version : Software Version 3300 ICP / MCD MiVB 8.0.9

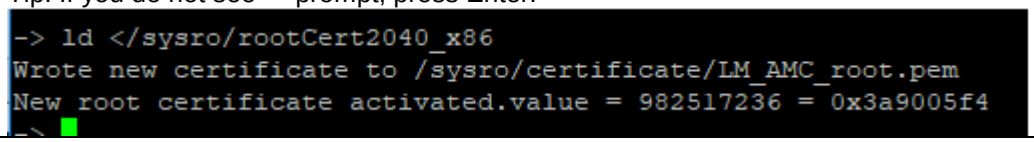
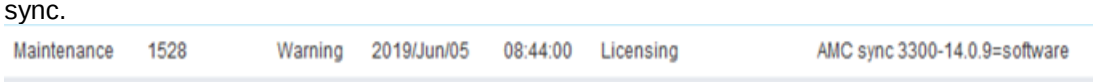
Manual Update Procedure for ISS, vMiVB, MIVBx, MXe Server, Stratus Systems

Preparation:

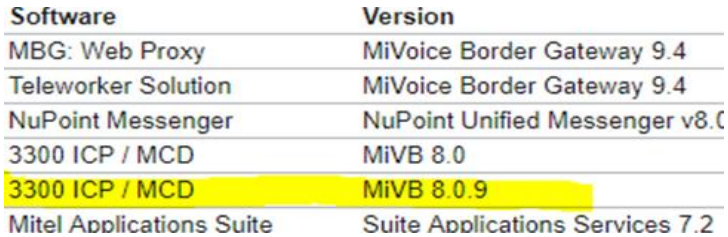
a. Download the **rootCer2040_linux.zip** update from software download center (see page 4)
b. RTC shell access (Require Putty or similar application to establish SSH session to MSL based server.
c. WinSCP or SFTP application for transferring rootCer2040_linux.zip in BINARY mode

Step 1	WinSCP or SFTP **rootCert2040_linux.zip** to the /tmp folder of MSL based server in Binary mode
	You can use your preferred SFTP application such as WinSCP. If you are not familiar, you can use the instructions using FileZilla application **To establish SFTP session to the controller:** Launch FileZilla application > File > Site Manager Select SFTP protocol, enter IP address of controller and log in as root user  **To transfer rootCert2040_linux.zip to the /tmp folder** On the local site (left), navigate to the folder in which rootCert2040_linux.zip is located On the remote site(controller), change to /tmp folder Select **rootCert2040_linux.zip**, right-click and select **Upload** to /tmp folder Note: Make sure the transfer option is in binary mode 
Step 2	To establish SSH session to MSL based server and then unzip rootCer2040_linux.zip
	Launch Putty to establish SSH session to MSL based server and login as root user

<table>
<tr><td></td><td>Type: unzip -d "/" "/tmp/rootCert2040_linux.zip"
 
</td></tr>
<tr><td>Step 3</td><td>To install the new certificate on RTC shell</td></tr>
<tr><td></td><td>To access RTC shell (from step2), type: mcd-debug-console
 

On RTC shell (with ->prompt), type: ld </sysro/rootCert2040_x86
Tip: If you do not see -> prompt, press Enter.
 
</td></tr>
<tr><td>Step 4</td><td>To perform AMC sync to update ARID and/or GARID with the newly installed certificate</td></tr>
<tr><td></td><td>4a> Launch ESM > License and Options Selection Form, click Change, click Retrieve License to perform AMC sync, then click SAVE; and/or
4b> For GRAID if applicable, access the Application Group Licensing form, click Change, click Save</td></tr>
<tr><td>Step 5</td><td>To validate if the new certificate is in use after AMC sync.</td></tr>
<tr><td></td><td>5a> View ESM maintenance logs and verify that the software version would have “.9” appended to the current system’s software version. “xx.9” confirms that new certificate is in use after AMC sync.
 

5b> (optional) View the ARID/GRID record in AMC to confirm that “.9” is appended to software version.
 

For ULM record, AMC displays .9 version as follows:
 
</td></tr>
</table>

Software Installer (S.I) update procedure for all platforms

To use S.I to update AMC Root Certificate, please download S.I version 14.0.0.15 or higher from Software download center.

S.I provides a new “Update Root Certificate” option to apply on the current 3300 controllers running MCD 5.0~MiVB 8.0 SP3 PR3. To prevent the loss of AMC root certificate, S.I automatically applies the new AMC root certificate on MiVB software upgrade.

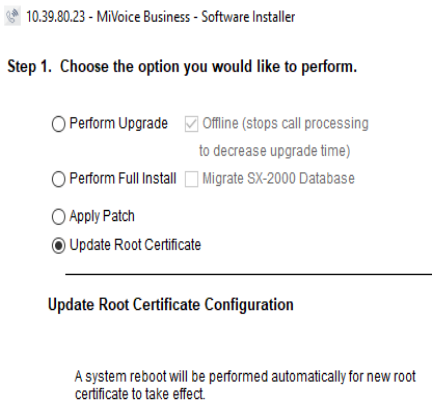
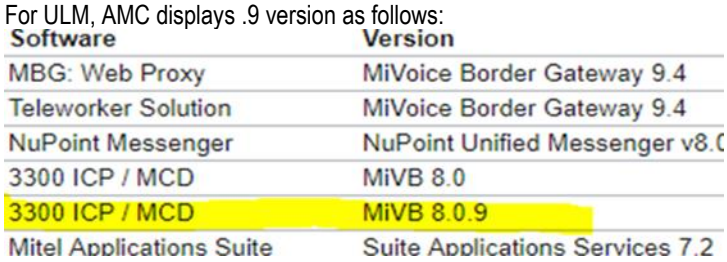


Table 3: S.I Option to update root certificate with or without MIVB Software upgrade

Platform Type	No MiVB software upgrade involved	MiVB Software upgrade involved
AX CX, CXi (II) LX, MX MXe	Use S.I option to “Update Root Certificate”	Launch S.I to perform MiVB upgrade. i.e. S.I automatically applies Root Certificate on MiVB upgrade.
MiCD tenant(s)	Use S.I option to “Update Root Certificate”	Launch S.I to perform MiVB upgrade. Note: If the MiVB upgrade is via MiCD server manager, no new Root Certificate is installed. Use S.I option to “Update Root Certificate”.
ISS, vMiVB, MIVBx Stratus	Use S.I option to “Update Root Certificate”	S.I does not support MiVB upgrade on these platforms. After MiVB software is upgraded, use S.I option to “Update Root Certificate”,
MXe Server	Use S.I option to “Update Root Certificate”	Launch S.I to perform MiVB upgrade. If MXe Server is re-installed via recovery iso image, choose one of following options: Launch S.I to upgrade MiVB software; or Use S.I option to “Update Root Certificate”.

S.I online licensing Procedure to "Update Root Certificate"

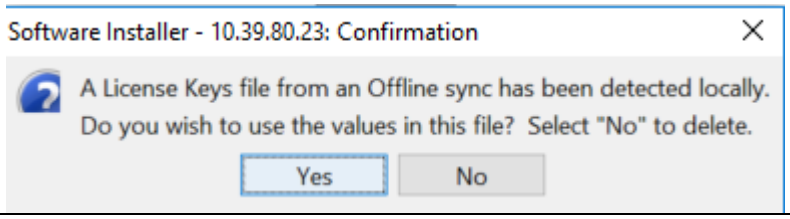
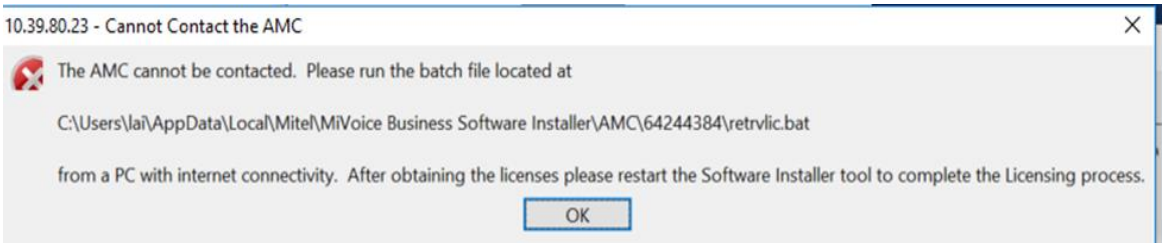
Step 1	Launch S.I 14.0.0.15 or higher to select "Update Root Certificate"
	• Connect to 3300 system, click Configure • Select "Update Root Certificate" option, click Next
Step 2	Retrieve ARID and/or GRID if applicable from AMC
	• In Step 3a. License and Option Selection, click **Retrieve Licenses** for ARID, click **Next**, Note: Please do not alter any license options as it may require database backup and restore. • In Step 3b, click Next • Click Start to update root certificate and to reboot. Wait until S.I confirms Update is successful.
Step 3	To validate if the new certificate is in use after AMC sync.
	View the ARID/GARID record in AMC to confirm that ".9" is appended to the corresponding software version  For GARID, dlm-1.0=software" would be updated to "dlm-1.0.9=software". For ULM, AMC displays .9 version as follows: 

Software	Version
MBG: Web Proxy	MiVoice Border Gateway 9.4
Teleworker Solution	MiVoice Border Gateway 9.4
NuPoint Messenger	NuPoint Unified Messenger v8.(
3300 ICP / MCD	MiVB 8.0
3300 ICP / MCD	MiVB 8.0.9
Mitel Applications Suite	Suite Applications Services 7.2

S.I offline licensing Procedure to "Update Root Certificate"

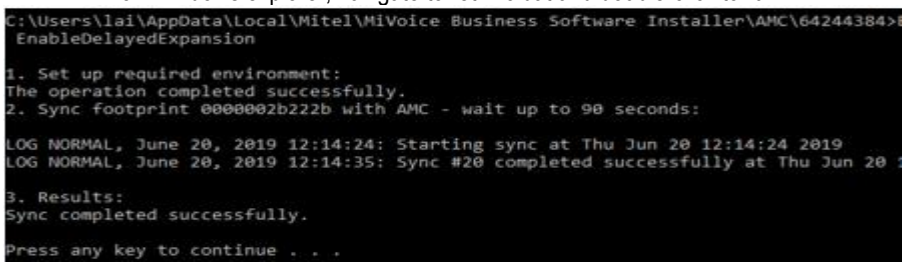
Conditions:

- 3300 system and PC running S.I does not have internet access in the customer's network

Step 1	**Launch S.I 14.0.0.15 or higher to select "Update Root Certificate"**
	• Connect to 3300 system, click Configure • Select "Update Root Certificate" option, click Next
Step 2	**Retrieve ARID and/or GRID if applicable from AMC**
	• In Step 3a. License and Option Selection, click **Retrieve Licenses** for ARID, click **Next**, Note: Please do not alter any license options as it may require database backup and restore.
Step 3	**(optional). S.I may present confirmation dialog. Press No to continue**
	The confirmation dialog(optional) is likely that license key was previously retrieved and/or saved to the local P.C. This is to confirm if you want to use the previous key saved to P.C. It is required to retrieve new key based on the new root certificate. 
Step 4	**Due to no AMC access, S.I prompts to license the system "OFFLINE"**
	S.I dialog - "**Cannot Contact AMC**" is presented when S.I is unable to connect to the AMC via the internet. The location of the batch file – retrvlic.bat is showed in the dialog. If you have GARID as well, S.I dialog displays 2 location of retrvlic.bat for both ARID and GARID. **Make a note of this location for Step 5 and then close the current S.I session.** For reference, the location of the batch file may vary depending on Windows as follows: For Windows 10, C:\Users\<user id>\AppData\Local\Mitel\MiVoice Business Software Installer\AMC\<ARID or GARID> For Windows XP, C:\Documents and Settings\<user id>\Application Data\Mitel\MiVoice Business Software Installer\AMC\<ARID or GARID> Note: The folder for the location of batch file is hidden by default in Windows. To unhide, open **File Explorer** from taskbar, select **View > Options>** Change Folder and search options. select **View** tab and, in **Advanced settings**, select "**Show hidden files, folders and drives**" 

<table>
<tr><td>Step 5</td><td>To perform AMC sync by running retrvlic.bat for ARID and/or GARID(if applicable)</td></tr>
<tr><td></td><td>

Connect the PC running S.I to the network with internet connectivity
From windows explorer, navigate to retrvlic.bat and double-click to run

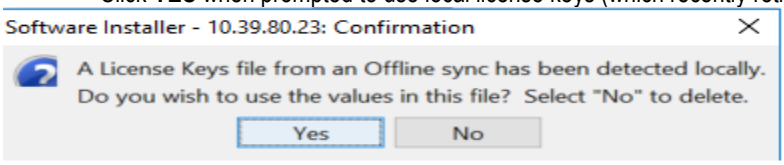


This confirms that the new license key is available

For GARID, navigate to retrvlic.bat (2nd location for GARID) and double-click to run to complete.

</td></tr>
<tr><td>Step 6</td><td>To license 3300 with the new license key</td></tr>
<tr><td></td><td>

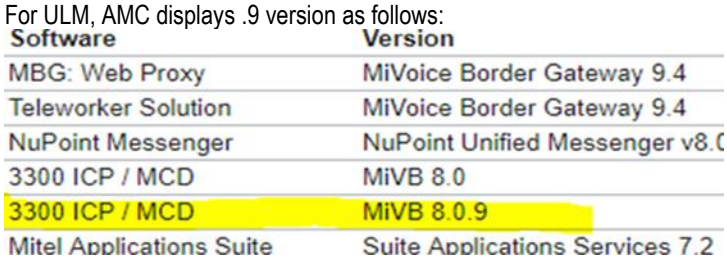
Reconnect PC running S.I to the local network in which 3300 is located (no internet connectivity)
Repeat Step 1 and 2 to launch S.I to retrieve license from 3300 controller
Click YES when prompted to use local license keys (which recently retrieved from step 5)



Complete the rest for S.I prompts and click Start to complete
Note: 3300 will reboot upon successful licenses

Wait until S.I confirms the Update is successful.
</td></tr>
<tr><td>Step 7</td><td>To validate if the new certificate is in use after AMC sync</td></tr>
<tr><td></td><td>
View the ARID/GARID record in AMC to confirm that ".9" is appended to the corresponding software version


For GARID, dlm-1.0=software" would be updated to "dlm-1.0.9=software".

For ULM, AMC displays .9 version as follows:


</td></tr>
</table>

Troubleshooting for manual update

Symptom when issuing ld command	**Solution**
When issuing ld </sysro/rootCert2040_ppc; OR ld </sysro/rootCert2040_x86, it fails as if the file does not exit	Make sure that rootCert2040_ppc or rootCert2040_x86 is in /sysro directory If so, make sure that the file was transferred in binary mode
If the returned error is Incorrect ELF header size: 13312 ld error: error loading file (errno = 0x3d0001).	Please make sure the patch is installed for the associated platform type: rootCert2040_ppc for MXe, etc., rootCert2040_x86 for MiCD rootCert2040_linux.zip for vMCD, MiVBX etc.
If the returned error is Unable to update AMC licensing client to request new licensekeys!! Unable to update validate to use the new root certificate!! New root certificate activated	This is the resulting of issuing ld command twice or more i.e. the first installed cert is still in effect. On RTC shell, issue moduleShow to confirm if there are more than one rootCert2040_ppc or rootCert2040_x86 loaded. If so, make sure if AMC sync can show .9 appended to software version, then reboot to clear the multiple ld issues.
Symptom on failing with AMC sync	
MiVB maintenance logs does not show AMC sync 3300 xx.09	On AMC, check if ARID has MiVB x.0.9 option If not so, please contact AMC Or Clear Hw ID from AMC and the re-sync.
In the unlikely event, you must remove the patch for any reason to revert to old Certificate. Note: Mitel does not recommend doing so as the old certificate will expire in 2020.	For MXe, CX, AX In RTC, Type: unld "rootCert2040_ppc" For MiCD In RTC shell, Type: unld "rootCert2040_x86" For ISS, Vmcd, MiVBX, Mxe Server, Stratus 1. SSH to the server as root and type: rm /etc/e-smith/events/pre-sync/S22mcd-certver 2. In RTC shell, Type: unld "rootCert2040_x86" For all platforms, then delete LM_AMC_root.pem and certVersion from /sysro/certificate To complete, perform AMC sync
License violation occurs after upgrade to MiVB 8.0 SP3 PR3	It is required to re-apply the patch for any manual software upgrade and/or see Table 3. If the upgrade is via S.I, S.I 14.0.0.15 or higher would re-apply the new root certificate automatically.

Troubleshooting for S.I update

In the event of S.I failing to update Root Certificate, S.I would have to rolled back to restore the original license key and remove patch files. No manual intervention should be required.

S.I error: Unable to upload files required for the new root certificate	Suggested action(s)
Potential reasons: SI fails to upload rootCert2040_ppc or sysro/rootCert2040_x86 or s04UseRootCert2040	Verify if the patch files exit in S.I PC as follows: C:\Users\<username>\AppData\Local\Mitel\MiVoice Business Software Installer\AMC\NewRC\<platform>\ If patch files are missing in S.I PC, re-install S.I 14.0.0.15 or higher or use Manual Update procedure to apply. If patch files exit, verify if you can ftp file to /sysro and /sysro/script/startup, then relaunch S.I or use Manual Update procedure to apply
Potential reason(s) SI fails to upload the new license keys (ARID or GARID)	Verify if you can ftp file to /db/temp/amc/<ARID>/sync/inbox. To ensure that the original license key is restored, log in ESM and retrieve the licenses from License and Option Selection for ARID; and/or update Application Group Licensing for GARID. Relaunch S.I or use Manual update procedure to apply
S.I error: Failed to rename the license key files Note: S.I renames the existing key to licensekeys_oldRC and then upload the new key	Verify if you can ftp /db/temp/amc/<ARID>/sync/inbox. Verify if you can rename licensekeys to licensekeys_oldRC. To ensure that the original license key is restored, log in ESM and retrieve the licenses from License and Option Selection for ARID; and/or update Application Group Licensing for GARID. Relaunch S.I or use Manual update procedure to apply.
S.I error: Failed to reboot the system after uploading new root certificate	Manual reboot 3300 and confirm if the ".9" is appended to software version in AMC.
S.I error: Failed to activate the new root certificate Reason: S.I may fail to log in to verify the new root certificate is installed at /sysro/certificate.	Verify if the LM_AMC_root.pem is located at /sysro/certificate On RTC, issue moduleShow to confirm if either rootCert2040_ppc or rootCert2040_x86 is loaded. If so, verify if the ".9" is appended to software version in AMC.