

Title	MiVoice Business Security Certificate Update
Summary	Mitel has released its latest security certificate update for all MiVoice Business customers on Releases 5.0 through 9.0. A patch will need to be installed for MiVoice Business Release 5.0 to 8.0 customers. MiVoice Business Release 9.0 customers should upgrade to Release 9.0 SP3 to ensure continuity of service
Posted Date	1 st September 2019
Effective Date	1 st September 2019
Bulletin Number	PB2019Sept1E
Bulletin Type	Product Announcement
Product Family	MiVoice Business
Audience	All MiVoice Business partners globally
Revision version	2
Revision reason	Release of Manual Patch for R9 MiVB systems

Bulletin Details

MiVoice Business Security Certificate Update

Mitel has released its latest security certificate update for all MiVoice Business customers on Releases 5.0 through 9.0. MiVoice Business Release 5.0 to 8.0 customers will need to upgrade to MiVoice Business R9.0 SP3 or install the relevant Security patch. For MiVoice Business Release 9.0 systems Mitel highly recommends upgrading to Release 9.0 SP3 to ensure continuity of service, but where this is not convenient a Security Certificate Update patch has now been released.

If the patch or R9.0 SP3 is not installed, then on or after August 21, 2020 the MiVoice Business system will issue a License Violation alarm. Three weeks later the customer's MiVoice Business system will then enter license violation and regular lines will be barred from normal operations.

Security Certificate Update installation options

MiVoice Business Release 5.0 to 8.0 customers

For MiVoice Business Release 5.0 to 8.0 customers Mitel has developed a Security Certificate Update (SCU) patch which can be installed manually, or via a simple to use Software Installer tool.

Update patches have been developed depending on the type of MiVoice Business system that the customer has, for example:

- 3300 Controllers (e.g. AX, CX, CX I, LX, MXe)
- Virtual, MiVoice Business Express, ISS, MXe Server and Stratus
- MiCD

If the Security Certificate Update patch is installed manually a reboot of the MiVoice Business system will not be required, however a reboot will be required if the Software Installer tool is used to install the patch.

Installation of the patch can be conducted remotely and typically will take less than 5 minutes. A five minute step by step patch installation video can be viewed at the following location;

<https://www.mitel.com/articles/mivoice-business-security-certificate-requirement>:











The Software Installer tool additionally automatically applies the patch on a full install, online and offline upgrades for 3300 controllers, online upgrades of MXE servers and MiCD instances. For ISS, vMCD, Stratus, MiVB Express Software Installer tool installations and patch installation using the manual process the patch will need to be re-applied if the MiVoice Business system is upgraded to a later release.

Download the relevant patch from the **Software Download Center** within [MiAccess](#).

1. Log into your MiAccess Account and select "Software Download Center"
2. Once you are in Software Download Center, Click "Navigate by categories"

3. Select “MiVoice Business” and then “Root Certificate Update (RCU) for pre-MiVB9.0”

MiVoice Business > Root Certificate Update(RCU) for Pre-MiVB9.0

 	Patch for ISS, VMCD, MXe Server	rootCert2040_linux.zip	Hotfix
 	Patch for MiCD Software Inventory	RCUForMICDInventory.zip	Hotfix
 	Patch for MiCD tenants	rootCert2040_x86	Hotfix
 	Patch for Mxe, CX, AX, LX, MX	rootCert2040_ppc	Hotfix
 	Software Installer to support RCU update (latest update 14.0.0.22 with bug fixes)	MiVBSoftwareInstallerSetup_14.0.0.22.exe	Software

MiVoice Business Release 9.0 customers

Mitel recommends MiVoice Business Release 9.0 customers update to Release 9.0 SP3 or later using the standard Service Pack installation process (Release 9.0 SP3 includes the Security Certificate Update as part of the Service Pack).

Manual update patches have been developed depending on the type of MiVoice Business R9.0 system that the customer has:





- 3300 Controllers (e.g. CX II and MXe)
- Virtual, ISS, and EX controllers

If the Security Certificate Update patch is installed manually, rather than part of a Service Pack install, a reboot of the MiVoice Business system will not be required.

Download the relevant patch from the **Software Download Center** within [MiAccess](#).

1. Log into your MiAccess Account and select “Software Download Center”
2. Once you are in Software Download Center, Click “Navigate by categories”
3. Select “MiVoice Business” and then “Root Certificate Update (RCU) for MiVB9.0~9.0SP2”

MiVoice Business > Root Certificate Update(RCU) for MiVB9.0~9.0SP2

 	Patch for CX II and MXe III	rootCert2040-9.0_ppc.tar	Hotfix
 	Patch for ISS, VMCD, EX	rootCert2040-9.0_x86.tar	Hotfix

Questions & Answers

Q: Where can I find the Technical Documents relating the Security Certificate Update?

A: You can find the Technical Documents relating to the MiVoice Business Security Certificate Update within the Mitel Knowledge Management System.

1. To access the Mitel Knowledge System, login to MiAccess and click on the link for it on

[mitel.com](#)



- the left-hand side.
2. Type in “Root Certificate Update” into the search bar (as below).



Search Tips

Case is not sensitive e.g. VoiceMail == voicemail. Use double quotes for exact string matching e.g. "Number is not known". When searching by document ID, include the prefix together with the number e.g. HO1234 (no spaces).

Q: Is a software upgrade required to implement the SCU

A: By upgrading to the latest release of MiVoice Business (9.0 SP3 or later) it will resolve the SCU issue. For Release 5.0 to 8.0 customers who choose not to upgrade to Release 9.0 SP3, a patch is available.

Q: How long does it take to install the patch?

A: Assuming the MiVoice Business system has an internet connection to Mitel’s AMC, initially it should take between 10 – 15 minutes for someone that is familiar with MiVoice Business. Once familiar with the process, the actual patch application can be done in less than 5 minutes.

Q: Is there any charge for the Patch?

A: No. Mitel is providing the Security Certificate Update patch and the associated Software Installer free of charge to all MiVoice Business partners via a software download.

Q: Will the MiVoice Business system need to be rebooted after the installation of the patch?

A: If the installer of the patch uses the Software Installer, then a MiVoice Business reboot will be part of the process. If the patch is installed manually then a reboot is not required.

Q: What will happen after the Security certificate expires?

A: After the certificate expiry date in August 2020 a MiVoice Business system will go into a **Critical license violation** when the MiVoice Business system validates the certificate embedded in the license key files. This will result in a critical system alarm. The displays of idle IP phones will indicate “License Violation”, and administrators will be notified accordingly.

After 3 weeks the customer’s MiVoice Business system **Critical license violation** is escalated to **System Lock**. Regular lines will be barred from making calls, other than outbound emergency calls and calls to the Attendant Console. Attendant Consoles retain full service, and internal calls from the Attendant Console will

be accepted. Incoming external calls will also be accepted.

Q: Does the Mitel Partner need to install the patch?

A: Mitel recommends the partner installs the patch as the person installing the patch should be knowledgeable and trained on the MiVoice Business solution.

The information conveyed in this document is confidential and proprietary to Mitel® and is intended solely for Mitel employees and members of Mitel's reseller channel who specifically have a need to know this information. If you are not a Mitel employee or a Mitel authorized PARTNER, you are not the intended recipient of this information. Please delete or return any related material. Mitel will enforce its right to protect its confidential and proprietary information and failure to comply with the foregoing may result in legal action against you or your company.