IAG Mirth Extension Deployment Guide

VERSION 1.0

CitiusTech

Copyright

Revision History

Document Version #	Revision Date	Prepared By	Approved By	Approval Date	Summary of Changes
1.0	01-07-2020	Akshaya Subramanian	Gaurav Chonkar	26-08-2020	First Version

Contents

1 Purpose

This document provides guidelines to import the GIT Plugin for Mirth Connect.

2 Deployment Requirements

The following sections enlists the pre-requisites for the deployment:

2.1 Server Requirements

The GIT Mirth Extension is primarily a zip file that will get imported using the Mirth UI for Extensions.

The process to install the extension is similar to the other commercial extensions made available by Mirth Connect. Mirth User Guide can be referred for installation/uninstallation of the extension.

<Screenshot for Mirth Extensions Page>

2.2 Installation Pre-requisites

This section refers to the pre-requisites that would be required for the installation of the extension:

- Ensure GIT repository is available to connect to
- Ensure users have commit and push permissions to the GIT repository
- Ensure user has Mirth administration rights to be able to restart Mirth service, post import of the ZIP file
- The trusted certificate needs to be installed in the system's trust store

2.3 Client Environment Requirements

There is no specific requirements as this would reside in the Mirth Connect set up.

2.4 Deployment User Requirements

- The user needs to be a Mirth system administrator for installation and import of the ZIP file
- The user needs to import the certificate shared along with the ZIP file

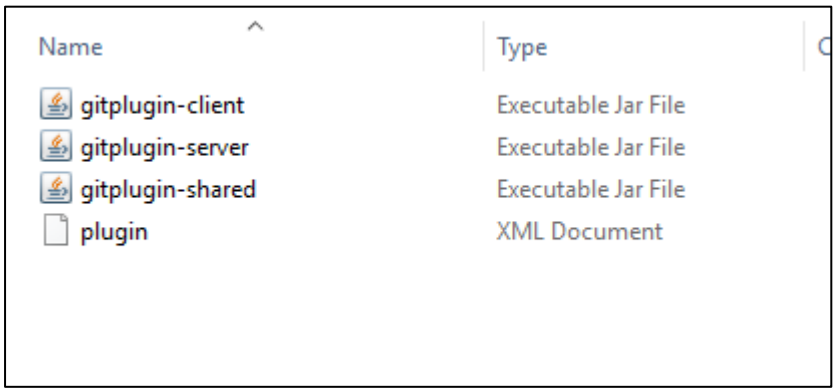
3 Deployment Steps

Download the Mirth Extension zip from

https://github.com/SalmanCitiustech/Mirth-Connect-Extension---GIT/tree/GitPluginZip

3.1 Verifying the Contents of the ZIP File

The GIT plugin ZIP file would consist of the following:



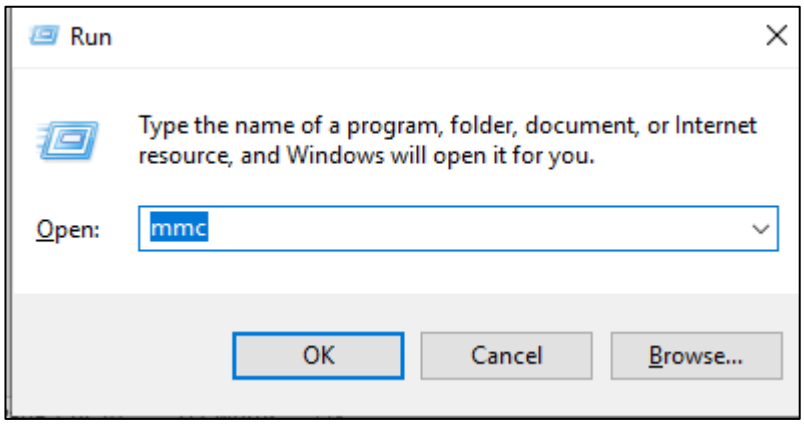
3.2 Importing the Certificates

Download the certificate shared along with the ZIP file and copy to some location on the Mirth server.

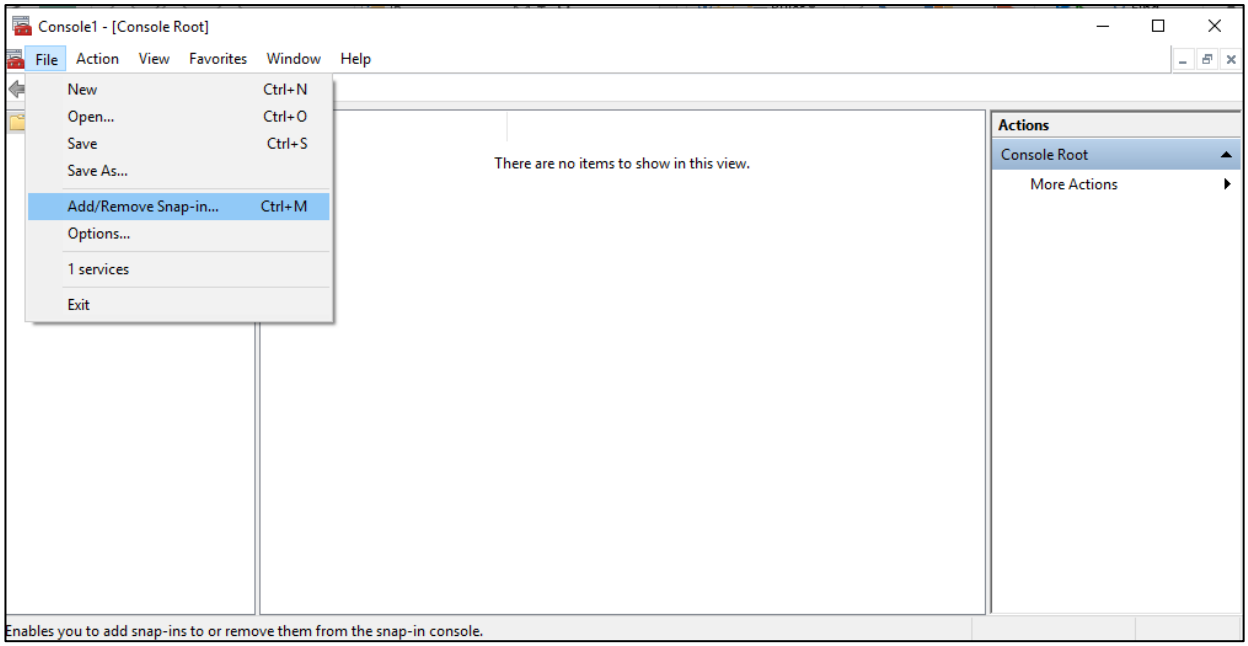
3.2.1 For Windows

Start the MMC and perform the following steps:

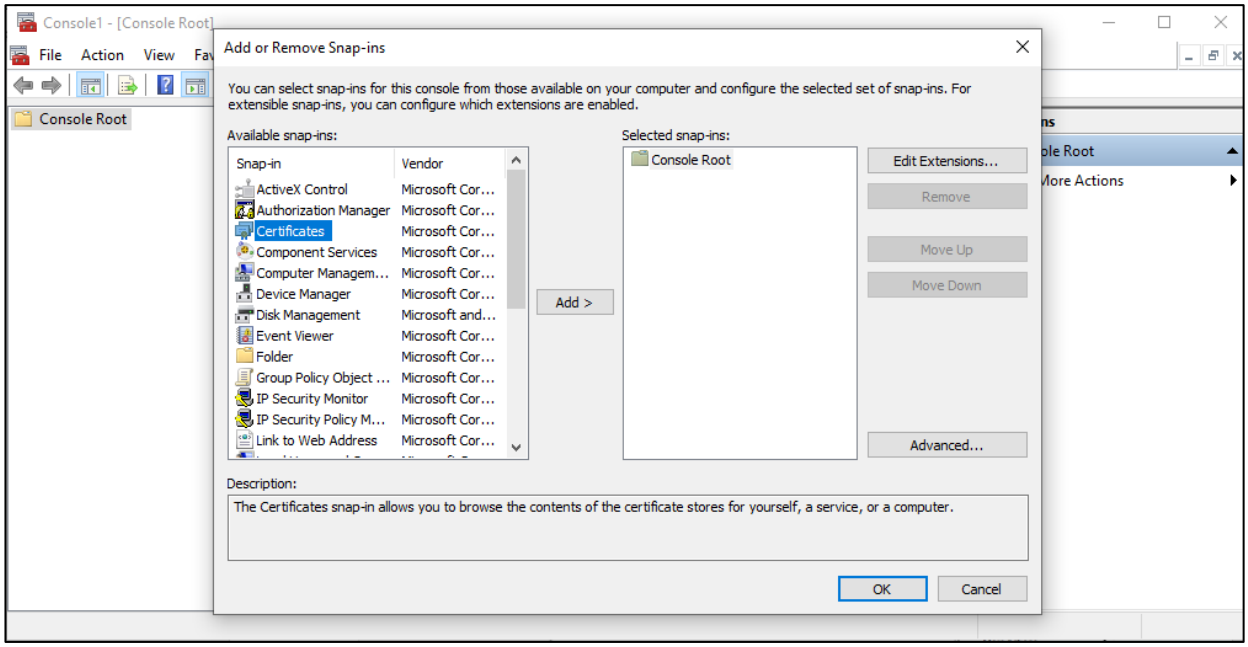
1. Go to Windows, open the Run application and type **mmc**:



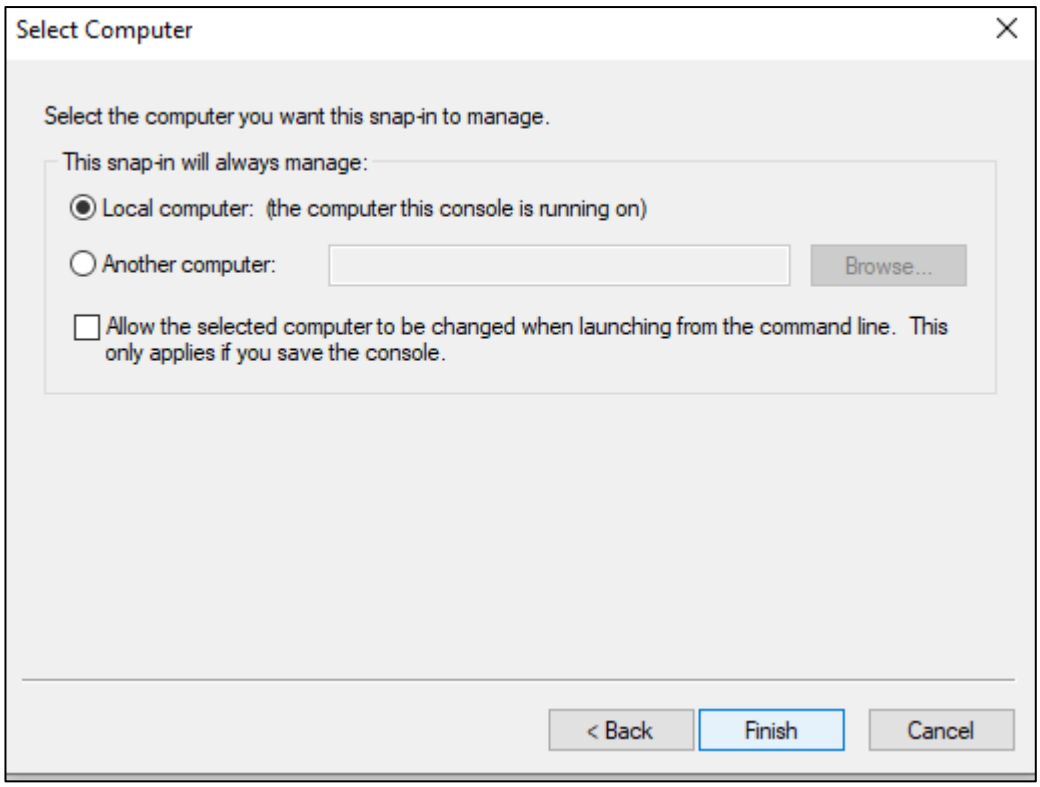
2. On the Console, click **File** | **Add/Remove Snap-in**:



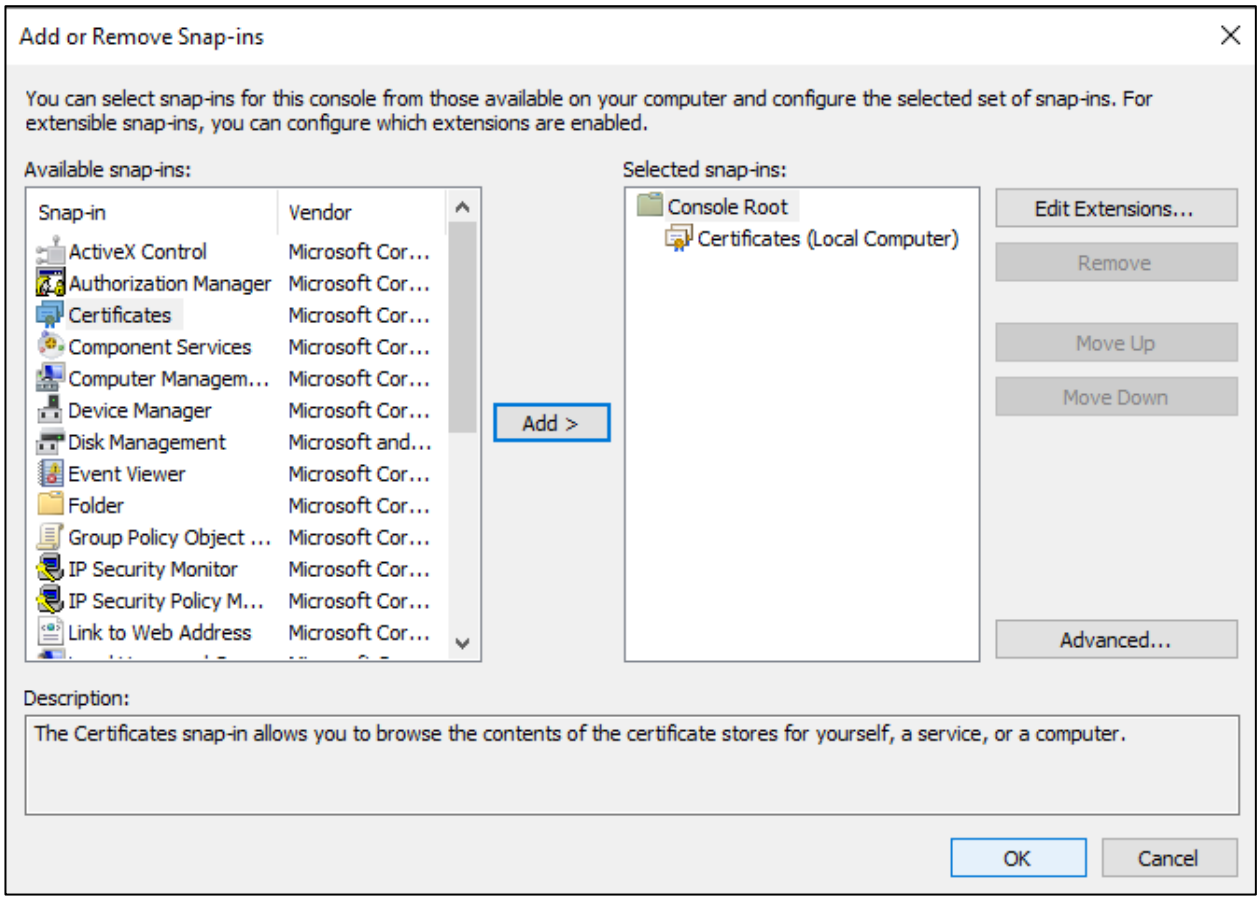
3. Select **Certificates** and click **Add**:



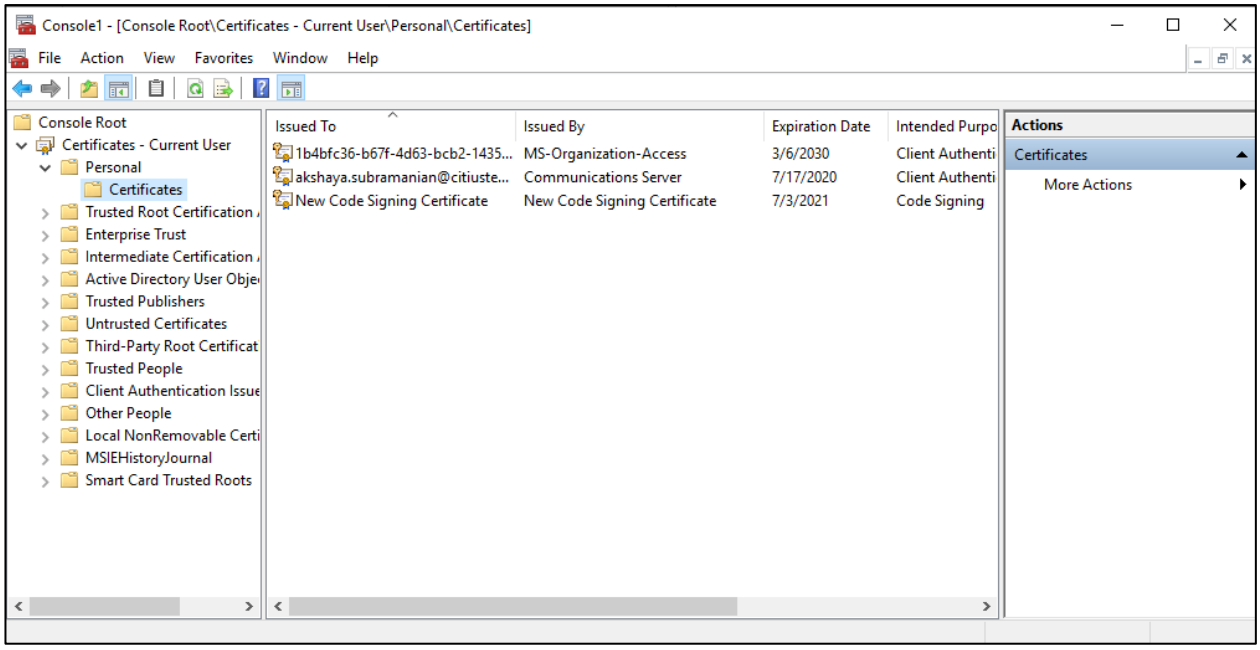
4. Select the **Service Account** or the **Computer Account**:



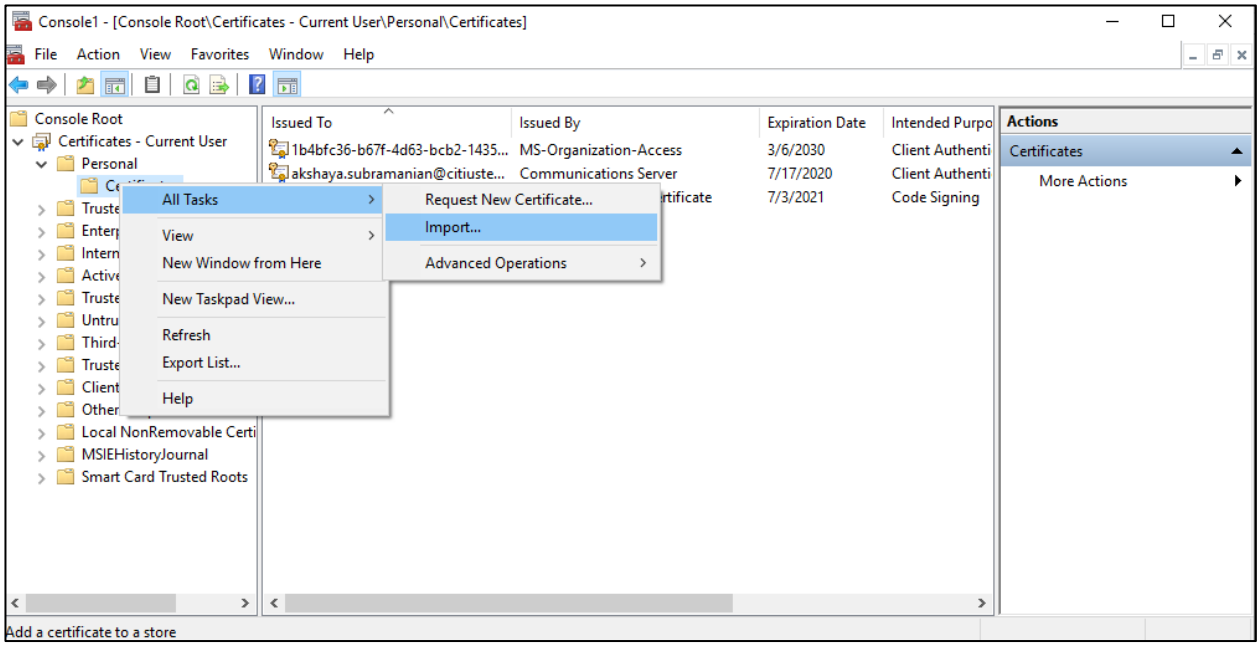
5. Click **OK**:



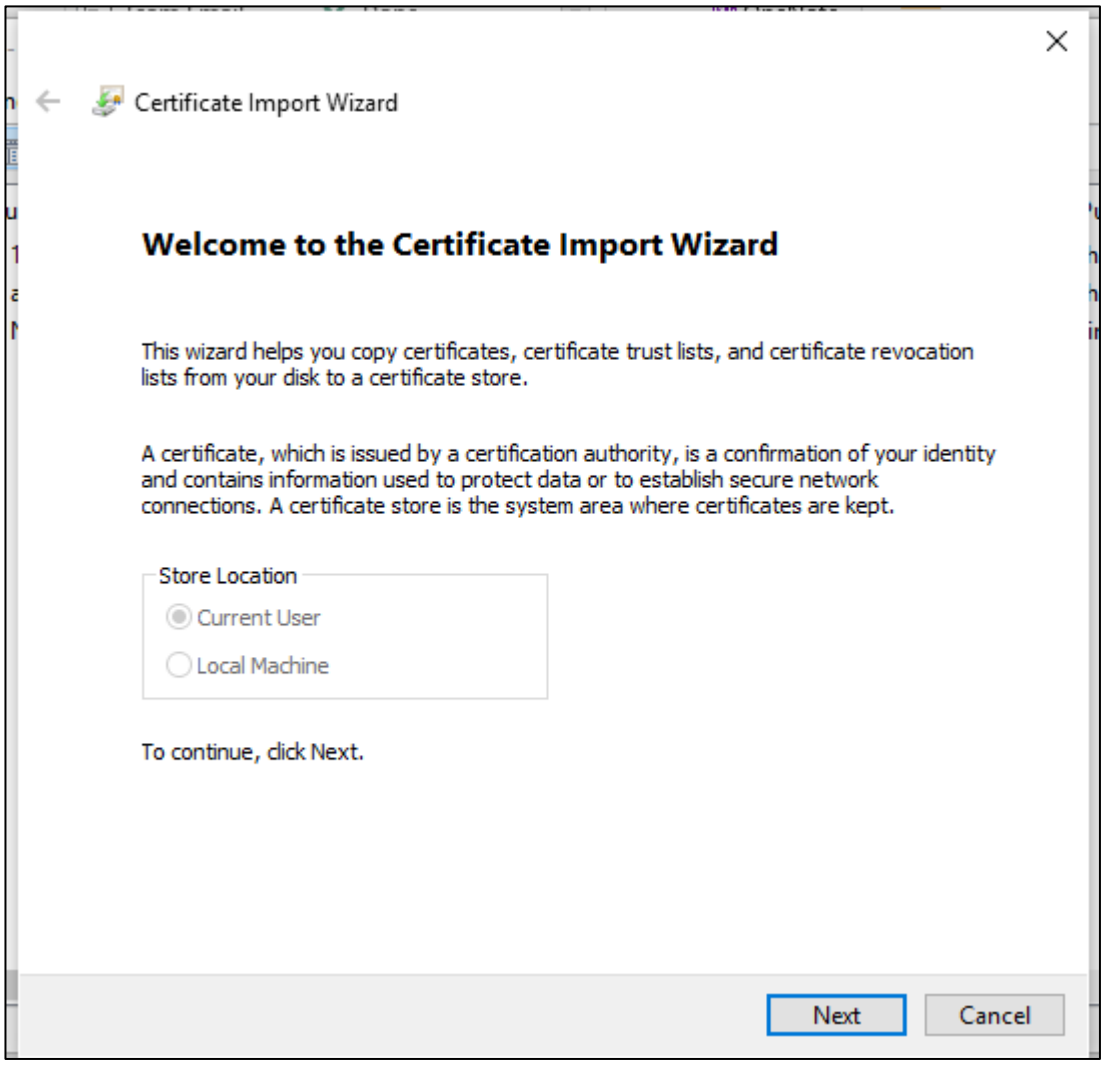
6. Select **Certificates** -> **Personal** -> **Certificates**:



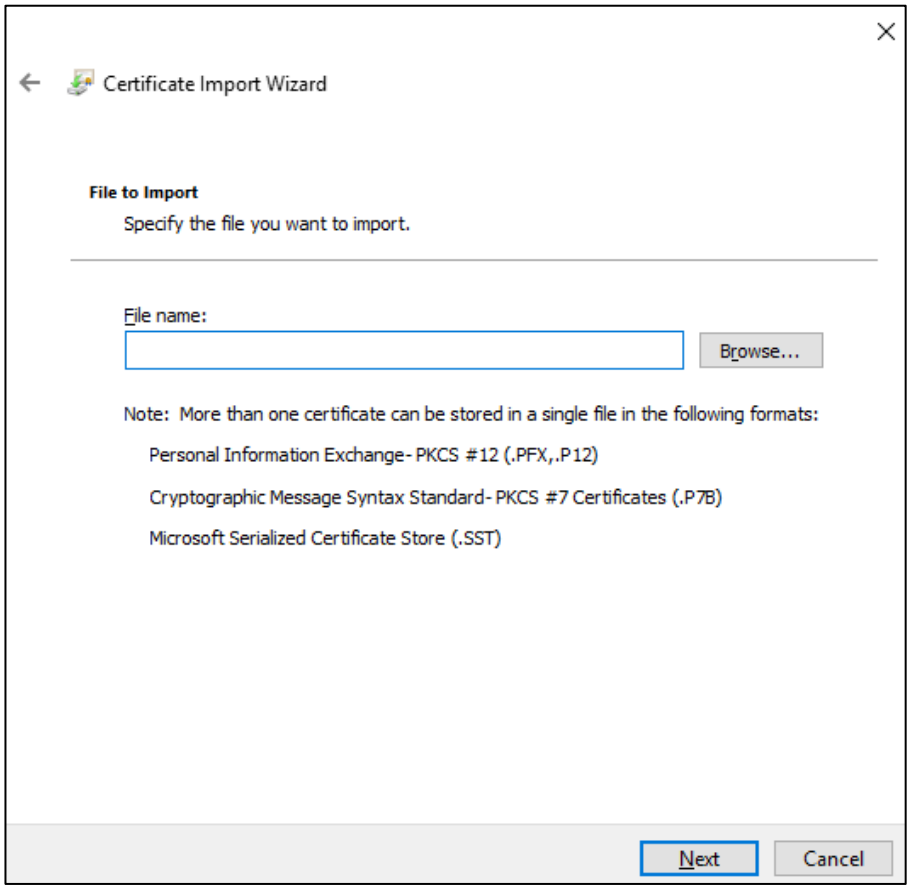
7. Right-click **Certificates,** select **All Tasks, and click Import**:



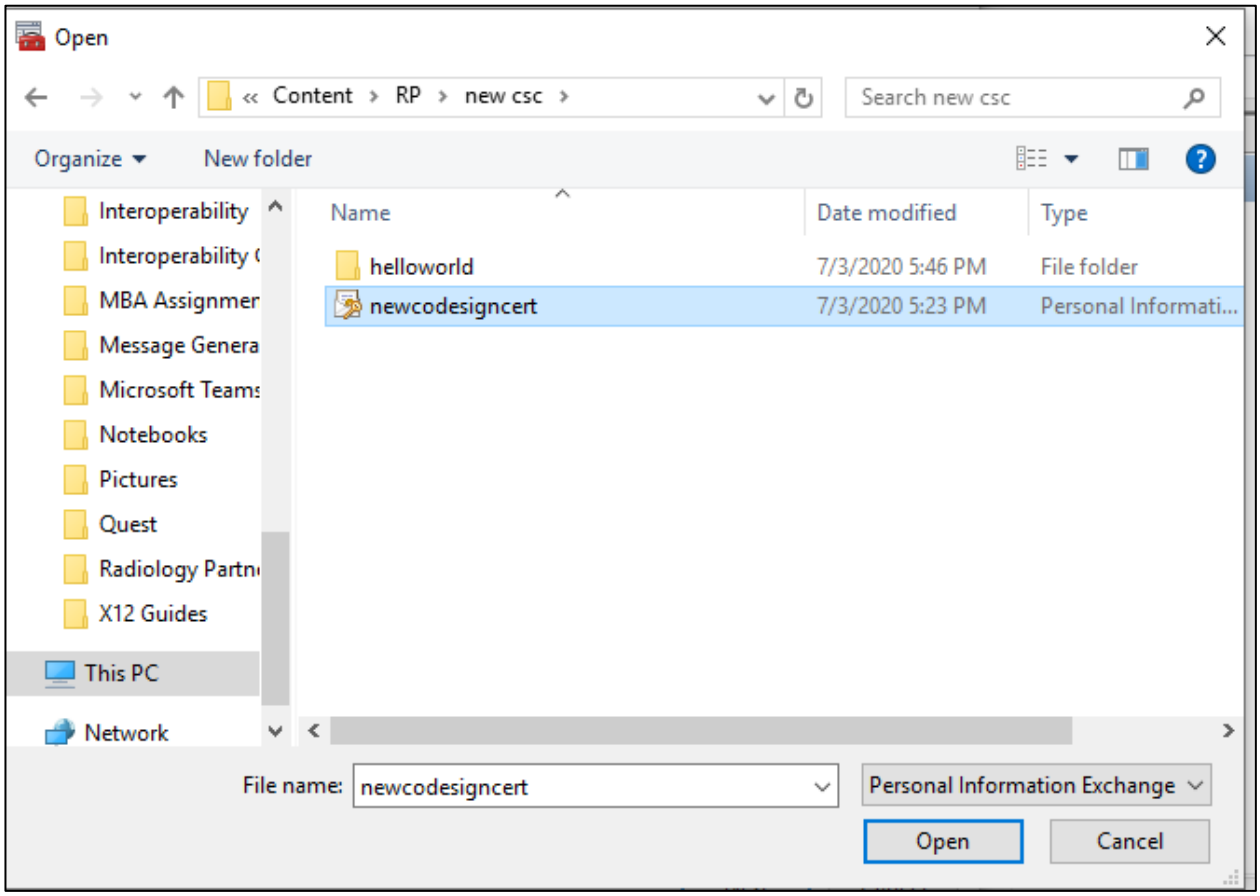
8. A Certificate Import Wizard gets launched, click **Next**.



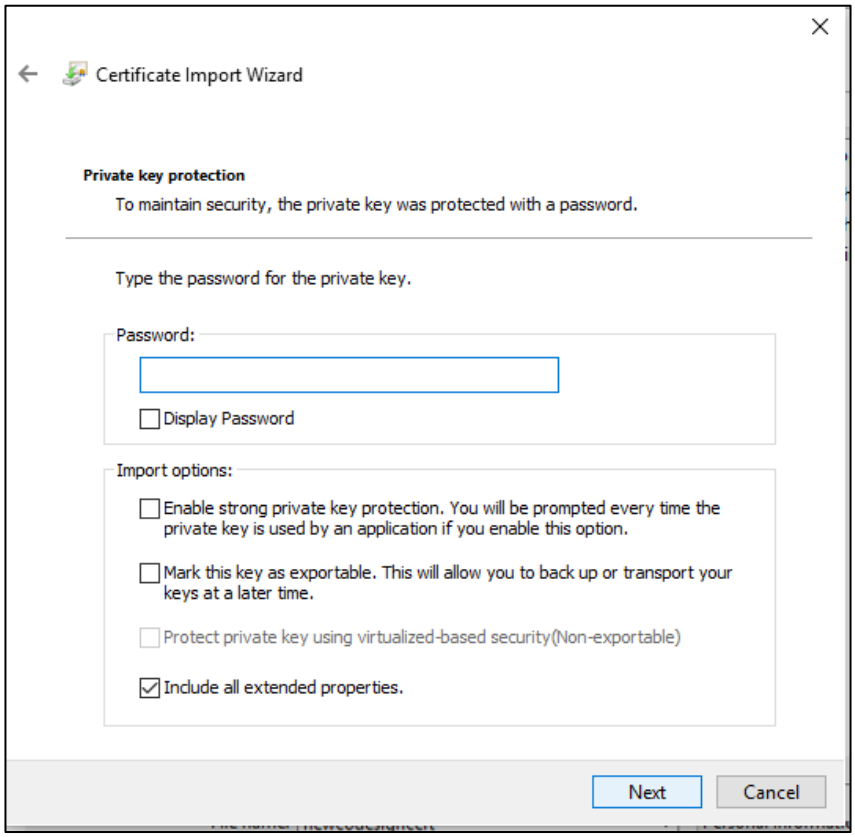
9. Choose the certificate that is part of the deployment package:



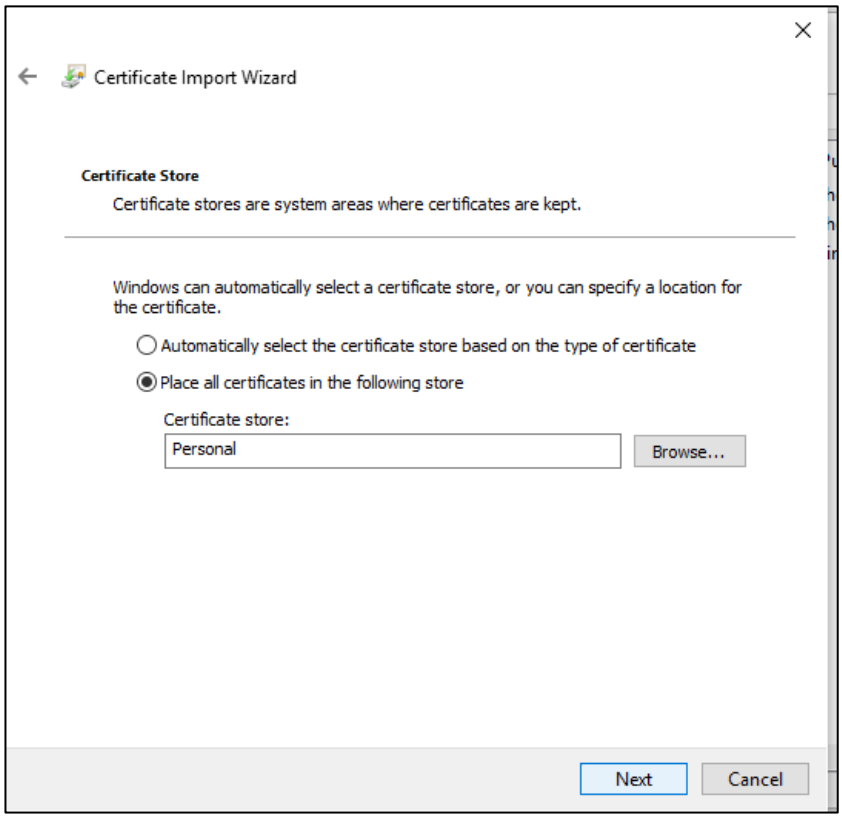
10. Browse to the location where the certificate file is saved and click **Open**:



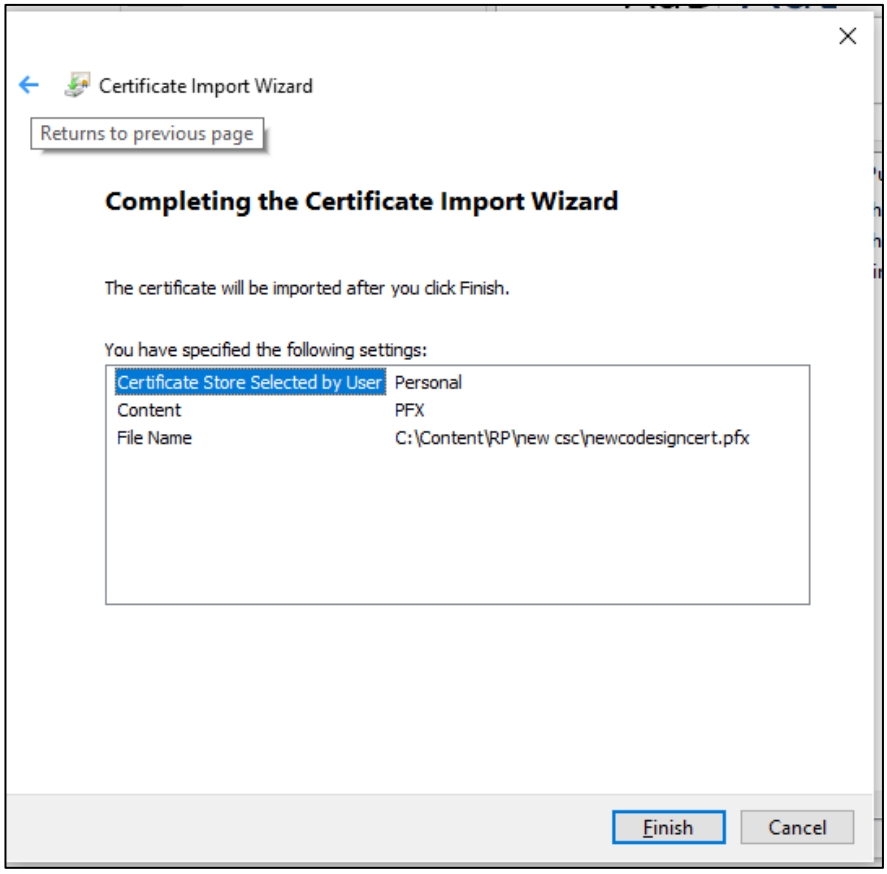
11. Click **Next** and type the private password that will be shared separately:



12. Click **Next** and choose the **Personal** Certificate store:

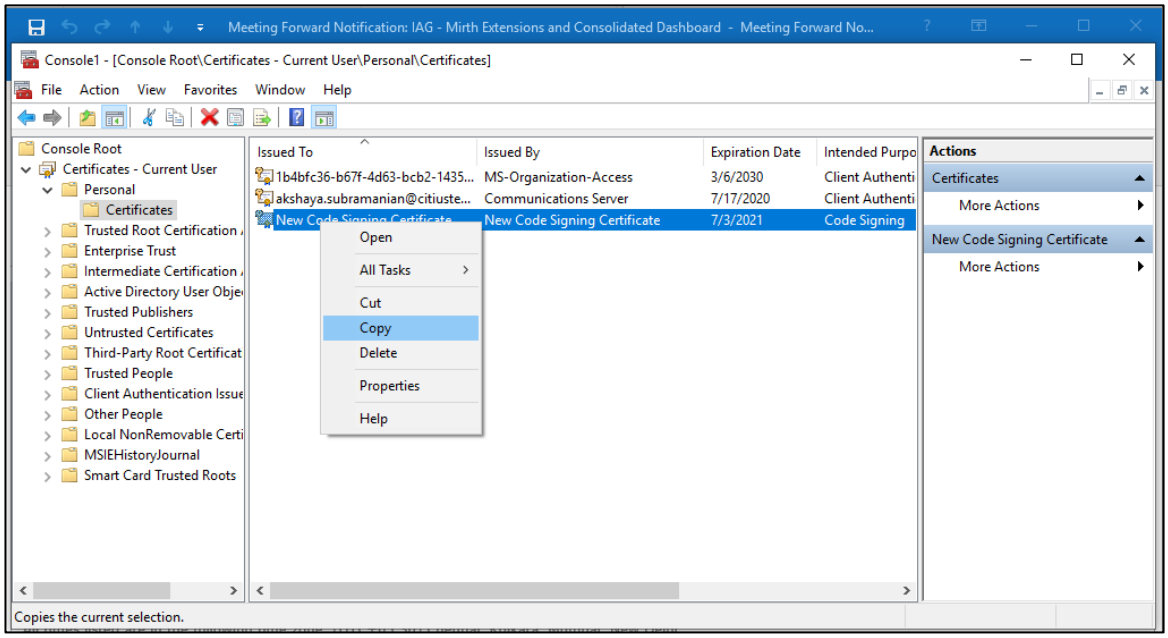


13. Click **Next** and then click **Finish**:

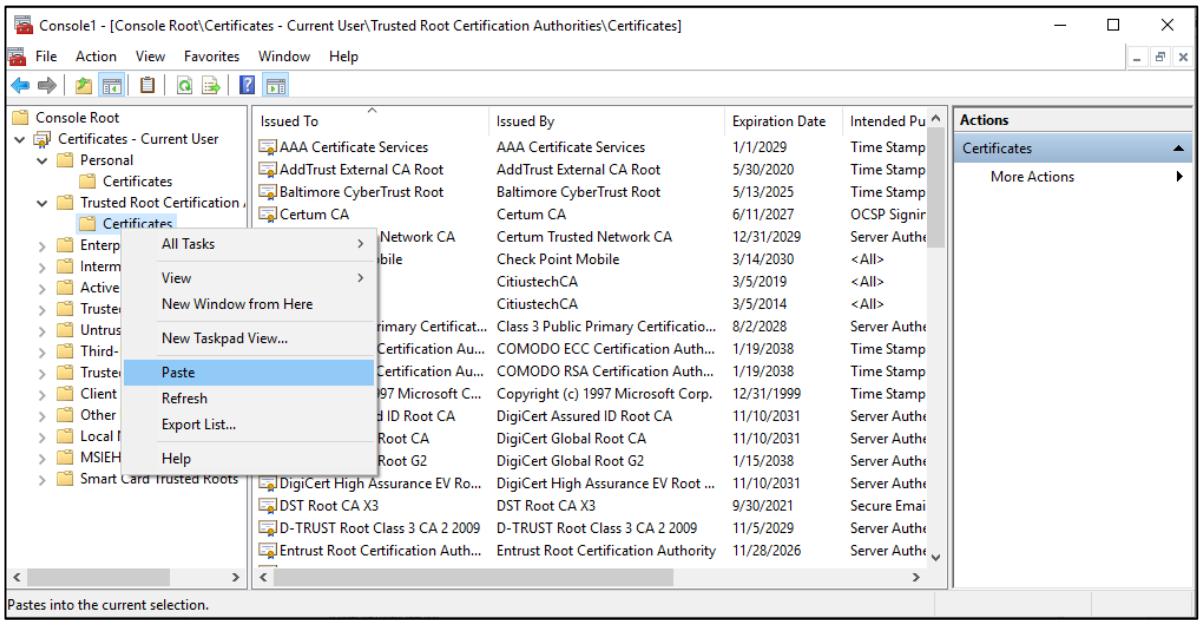


You should see the certificate installed in the Personal store.

14. Right-click the certificate and click **Copy**, as shown in the following screenshot:



15. Click **Trusted Root Certification Authorities** -> **Certificates**.
16. Right-click and select **Paste**:



The certificate would get copied in this location.

3.2.2 For Linux

Steps to add certificate to Linux: -

1. Copy the Code signing certificate .pfx and .jks files to Linux.

#Generate crt and key from pfx file
2. openssl pkcs12 -in newcodesigncert.pfx -nokeys -out Certificate.crt -nodes
3. openssl pkcs12 -in newcodesigncert.pfx -nocerts -out Key.pem -nodes

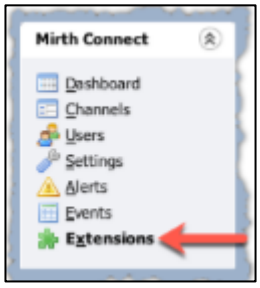
#Verifying
4. openssl x509 -text -noout -in Certificate.crt
 or
 openssl x509 -noout -modulus -in Certificate.crt | openssl md5

#Importing crt file to keystore jks file --- keep your own alies in below command
5. keytool -import -trustcacerts -alias mycert -file Certificate.crt -keystore newcodesign.jks -- added to keystore

#View list of keystore certificates
6. keytool -list -keystore newcodesign.jks -storepass <password>

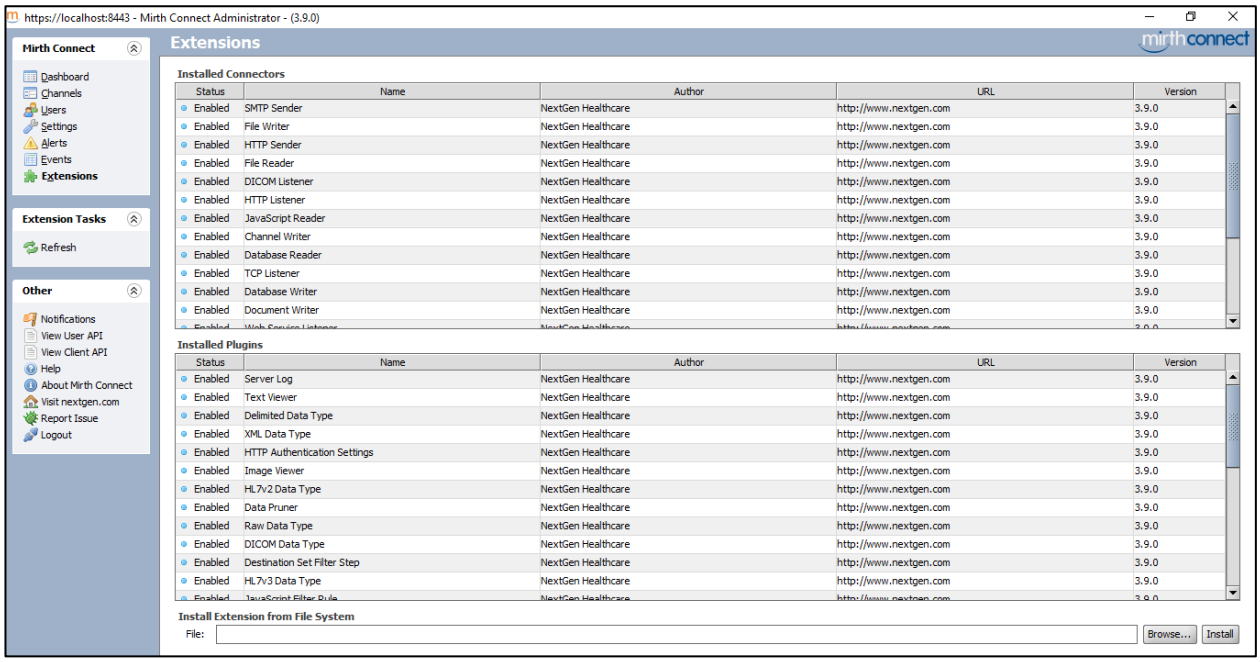
3.3 Installing the Extension

1. Launch the Mirth Connect administrator and login to the Mirth UI.
2. Click **Extensions** on the task pane at the upper left:

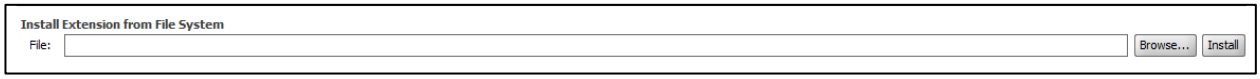


Extensions section is separated into the following categories:

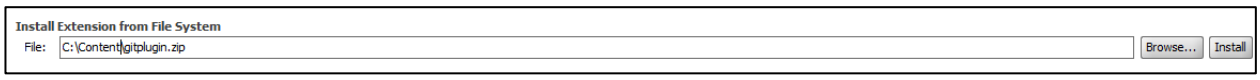
- **Installed Connectors**
- **Installed Plugins**
- **Installing Extensions from file system**
- **Extension Tasks**



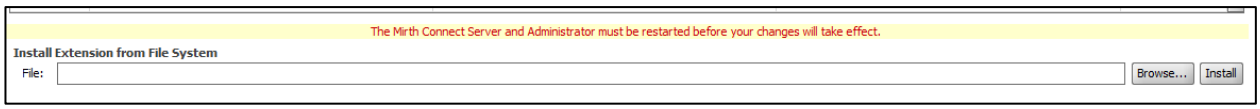
3. Navigate to the **Install Extension from File System** at the bottom of the screen:



4. Click **Browse** and select the **GITPlugin.zip** file from the respective folder:



5. Click **Install**. The user gets a notification to restart the server:



6. Restart the NextGen Connect Integration Engine server and launch the Mirth Connect Administrator. The user will be able to see the new extension listed in the Installed Plugins table.

3.4

Appendix

Licenses

The Software may contain third party software which requires notices and/or additional terms, conditions and licenses. Such required third party software notices and/or additional terms, conditions and licenses can be located here.

3.5 Annexure

Deployment Checklist:

This section provides the template for maintaining the details for each environment mentioned in section 2.1 (Separate row to be created for each environment).

Sr No	Client Name	Environment	Machine Name (IP Address)	Processor	# of Cores	Operating System	RAM	Total Hard Disk Space	Third Party Software Deployed	Solution Component Deployed