DigiCert® PKI Platform

Import tool for Intune S/MIME Certificate

March 14, 2023

digicert®

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

Introduction

This document details the steps required to bulk recover S/MIME keys/certificates in PKCS12 format with associated passwords and upload them onto an Intune tenant account, on a single operation, using a script that can be run as a scheduled task on the same machine where the Microsoft PFXConnector is installed

Once the script is run, S/MIME certificates can be provisioned by Intune to user's registered devices.

Client distributable consists of a Java jar file which needs to be executed on the same Windows Server 2019 machine where the Microsoft PFXConnector is installed.

Pre-requisites

⚠ Software pre-requisites:

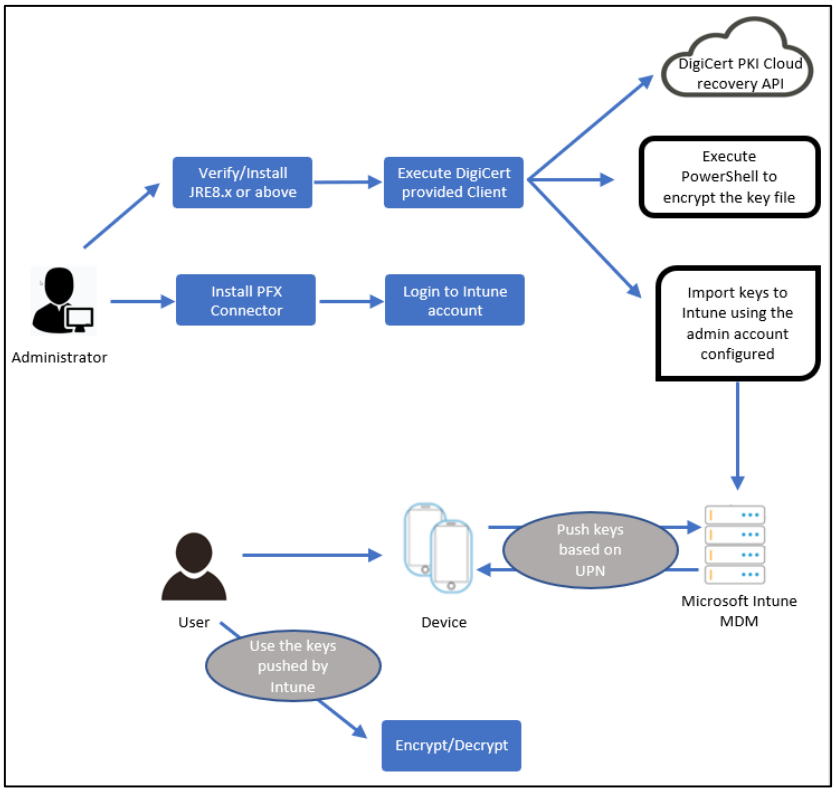
1. Java JRE version 8 supported
2. PowerShell version 5.1 supported
3. Windows Server 2019/2022 supported
4. Run the tool on the same Windows server where the PFXConnector tool is running.

Other pre-requisites:

1. Azure admin should be an Intune administrator.
2. User certificates being imported should have assigned Intune license.

Process Overview

The below diagram shows the high-level flow for the Intune S/MIME solution. Note that S/MIME certificates must have been issued via a standard flow, configured as a certificate profile within the PKI Manager portal (e.g. via a browser or PKI Client enrollment flow), which enables the encryption private keys to be escrowed and secured by the DigiCert PKI Platform solution. Once S/MIME certificates have been issued to users, they can be recovered by running the bulk recovery script, uploaded onto your Intune account and provisioned/pushed onto the user's registered devices.



How to use the client provided by DigiCert

1. Logon onto your Windows Server 2019 machine.
2. Ensure that JRE_HOME is configured to point to your JRE installation folder.
3. Create a directory in the drive of your choice – for example (D:) by the name PFXConnector.
4. Download DigiCertIntuneRecoveryClientForIntune.zip and extract into the above created directory.

   Please contact your DigiCert Representative to avail the script.

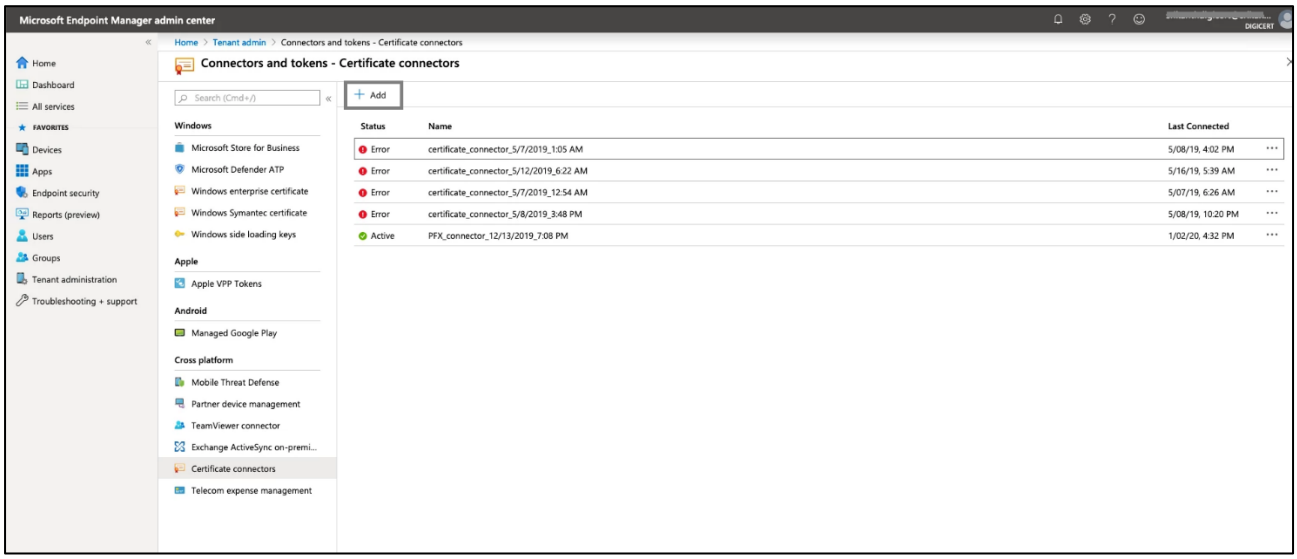
NOTE: Any CA vendor could download the script and reverse engineer it and implement a similar (if not identical) solution.

---

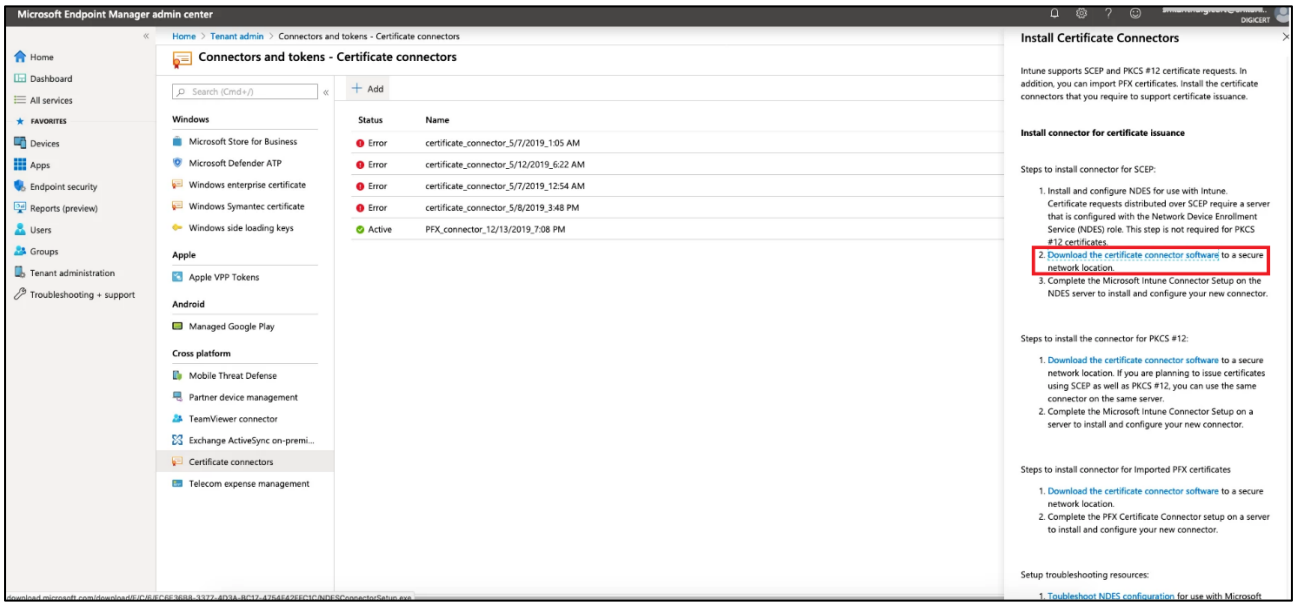
5. Before proceeding further, login to your Azure account at https://portal.azure.com using your administrator credential and navigate to https://devicemanagement.microsoft.com/#home

    a. Click on **Tenant Administration → Connectors and Tokens → Certificate Connectors**.

    b. Click on **Add.**



    c. Click on **Download the certificate connector software** from the section "**Steps to install connector for Imported PFX certificates**".



    d. Download and install the connector. Once the connector is installed - login using the Azure portal admin account and ensure the account is connected.

6. Login to the Windows Server 2019 machine where the PFXConnector is installed.

7. Launch PowerShell as an administrator and navigate to the directory where the **DigiCertIntuneRecoveryClientForIntune.zip** is extracted.

8. Now, in the extracted zip client, please find the DigiCertRecoveryClient.jar and execute it using the following command:

   ```
   java -jar DigicertRecoveryClient.jar -config recovery-config.properties
   ```

   See Appendix-A for details of the various parameters within the configuration file.

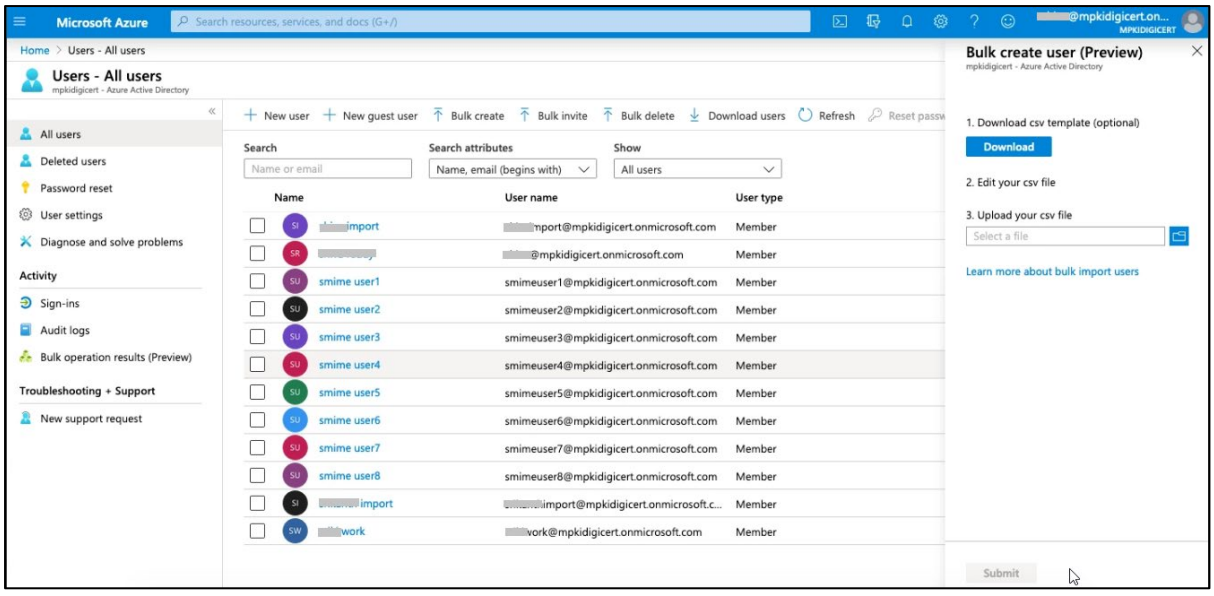
NOTE: The tool will recover and import certificates only if the users are already registered on Azure portal for an Intune tenant. If the user UPN does not match, then the import for that UPN fails.

Usually, the user (Device) creation/registration happens when the user installs the Company portal app on the end user device and logs in with the credentials provided by the admin.

Bulk import of users into Intune portal

If "for any reason" the admin wants to create users in bulk on Azure portal, the same can be achieved by uploading a CSV (in the template downloaded from Azure portal).

For this, navigate to https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/AllUsers



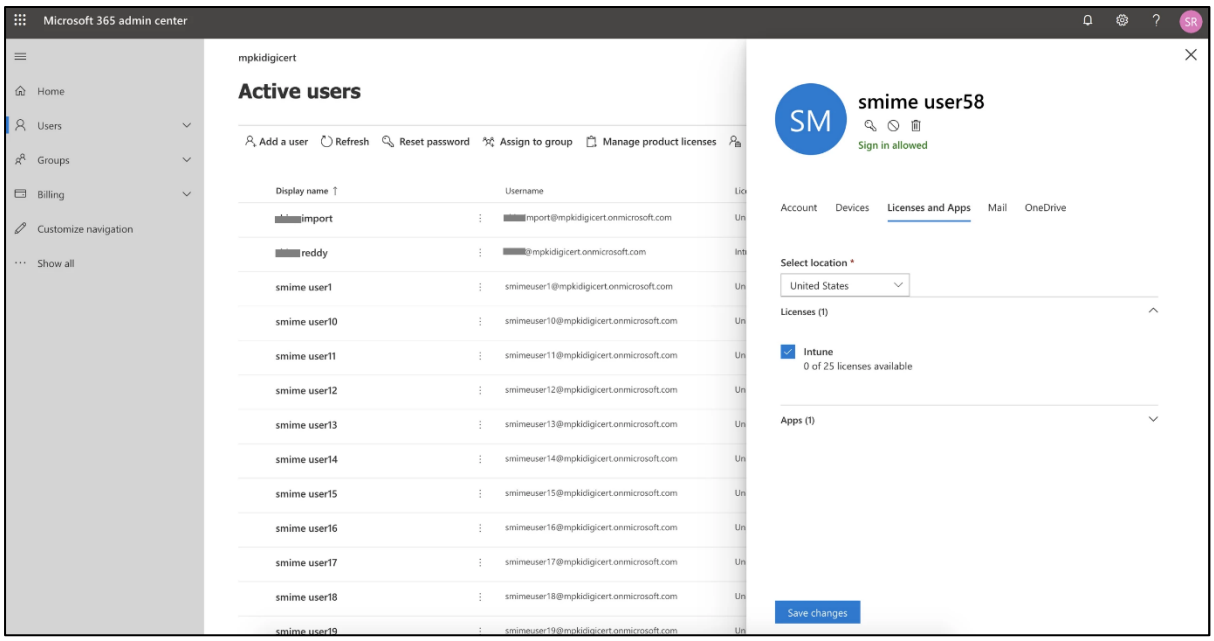
Once the users are created/uploaded, assign the Intune license for the bulk recovery script to import the users successfully.

Assign a License to the user

After you have created a user, you must use the Microsoft 365 admin center to assign an Intune license to the user. If you do not assign the user a license, they will be unable to enroll their device into Intune.

To assign an Intune license to a user:

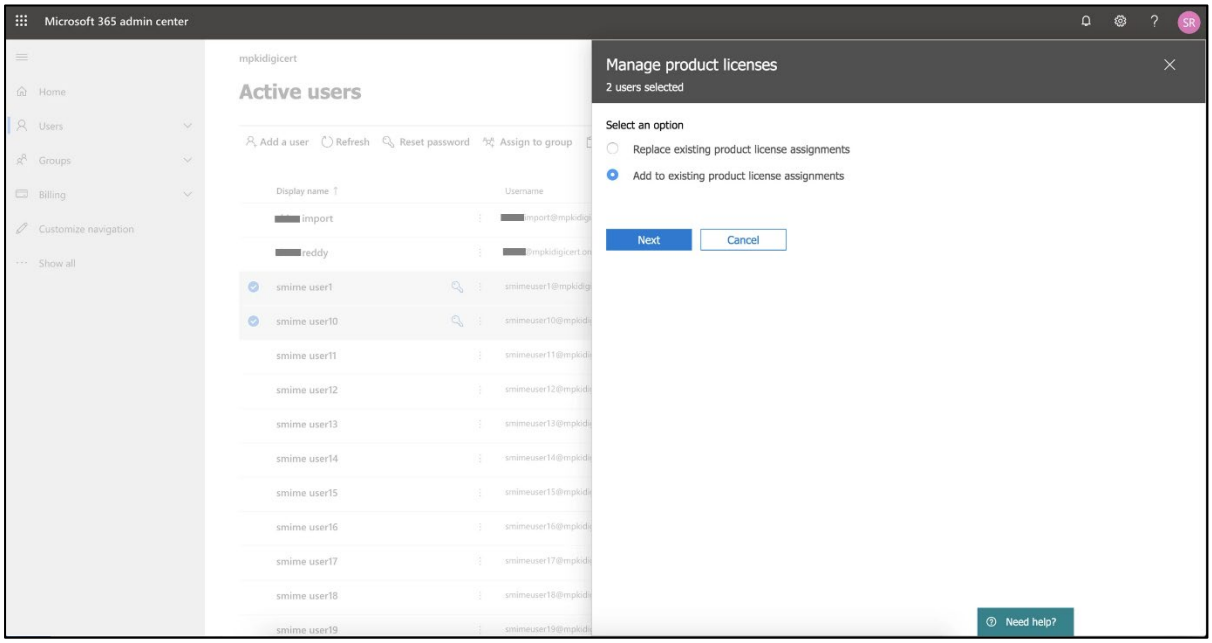
1. Login to the Microsoft 365 admin center with the same credentials you used to sign into Intune.
2. Select **Users** > **Active Users**, and then select the user you just imported or created.
3. Select the **Licenses and Apps** tab.
4. Under **Select location**, select a location for the user, if it is not already set.
5. Select the **Intune** check box in the **Licenses** section.



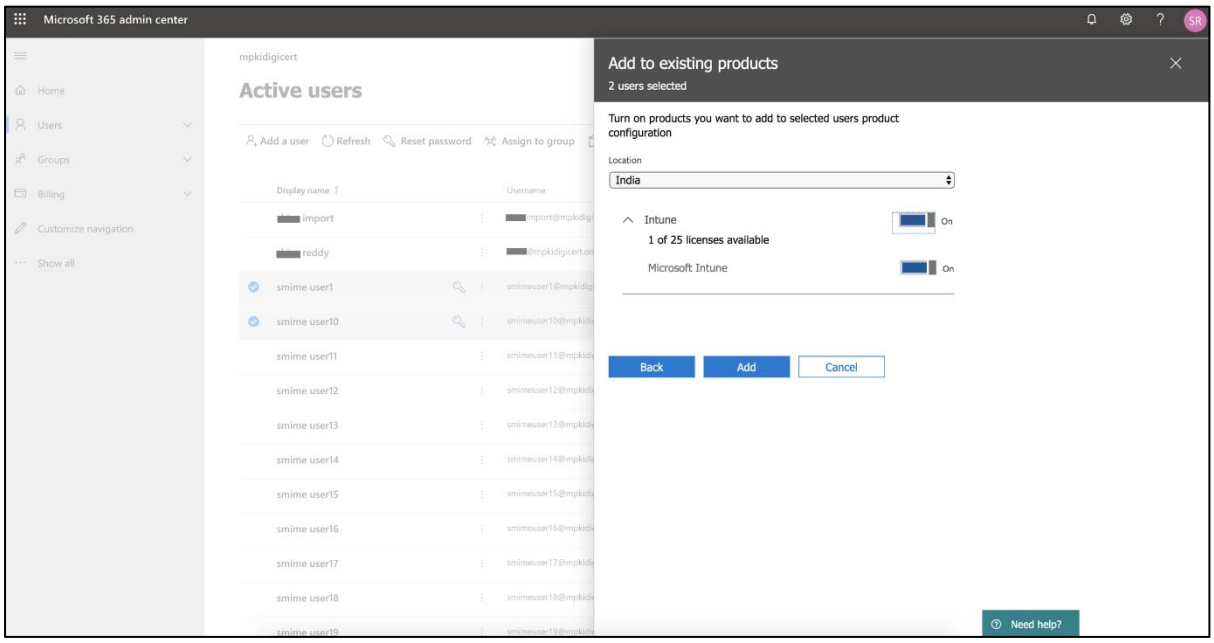
NOTE: This setting uses one of your licenses for the user. If you are using a trial environment, you will later reassign this license to a real user in a production environment.

6. Select **Save changes**.

If multiple users are selected to assign the license then click on **Manage product licenses link** at the top menu options, select **Add to existing product license assignments** option and click **Next** button.



Now select the **Location**, select the bar icon before **On** as shown below and click on **Add** button.



The new active Intune user(s) will now show that they are using an **Intune** license.

Once this is done, the application will be able to import certificates to these users.

Appendix-A – DigiCert Recovery Tool

The configuration file contains properties required to communicate with the DigiCert PKI Web Service to recover the escrowed S/MIME keys and then upload them onto an Intune tenant for onward distribution to registered devices.

Field	Description
host	DigiCert PKI Platform Host (environment on which PKI-WS is being executed. For example: https://pki-ws.symauth.com
log4jconfig	Configuration file for logging service log4j.properties location (usually same directory)
ssl.keystore	ra keystore path for the corresponding environment and account (jks)
ssl.keystorepass	password for the above ra keystore
ssl.truststore	trust store path for the ca being trusted
adminUserName	Intune admin username
adminUserPassword	Intune admin password
certmgmt.uri_context	/pki-ws/certificateManagementService (do not change)
certmgmt.version	1.0 (do not change)
certmgmt.operation_type	search (do not change)
certmgmt.account_id	account id from which to recover certs. You can get the Account id by login to **PKI Manager** and navigating to **Manage Accounts and sub-accounts**.
certmgmt.valid_from	start date (format: YYYY-MM-DD)
certmgmt.valid_to	end date (format: YYYY-MM-DD)
certmgmt.status	search by status. Possible status values include: • VALID • EXPIRED • REVOKED • SUSPENDED **NOTE:** Values are case-sensitive

Field	Description
certmgmt.serial_number	search by certificate serial number
certmgmt.seat_id	search by seat id
certmgmt.email_address	search by email address