



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

User Data Management Administrator's Guide

Certificates Management

11/4/2024

Contents

- 1 Requirements
 - 1.1 General Data Protection Regulation (GDPR) compliance
- 2 Importing an encryption certificate

Learn how to set up certificates to use UDM.

Requirements

UDM requires public/private keys for the encryption and decryption of data files and a valid X.509 RSA-compliant certificate in PEM format. Before you can export data, you must have a valid encryption certificate specified in your user preferences.

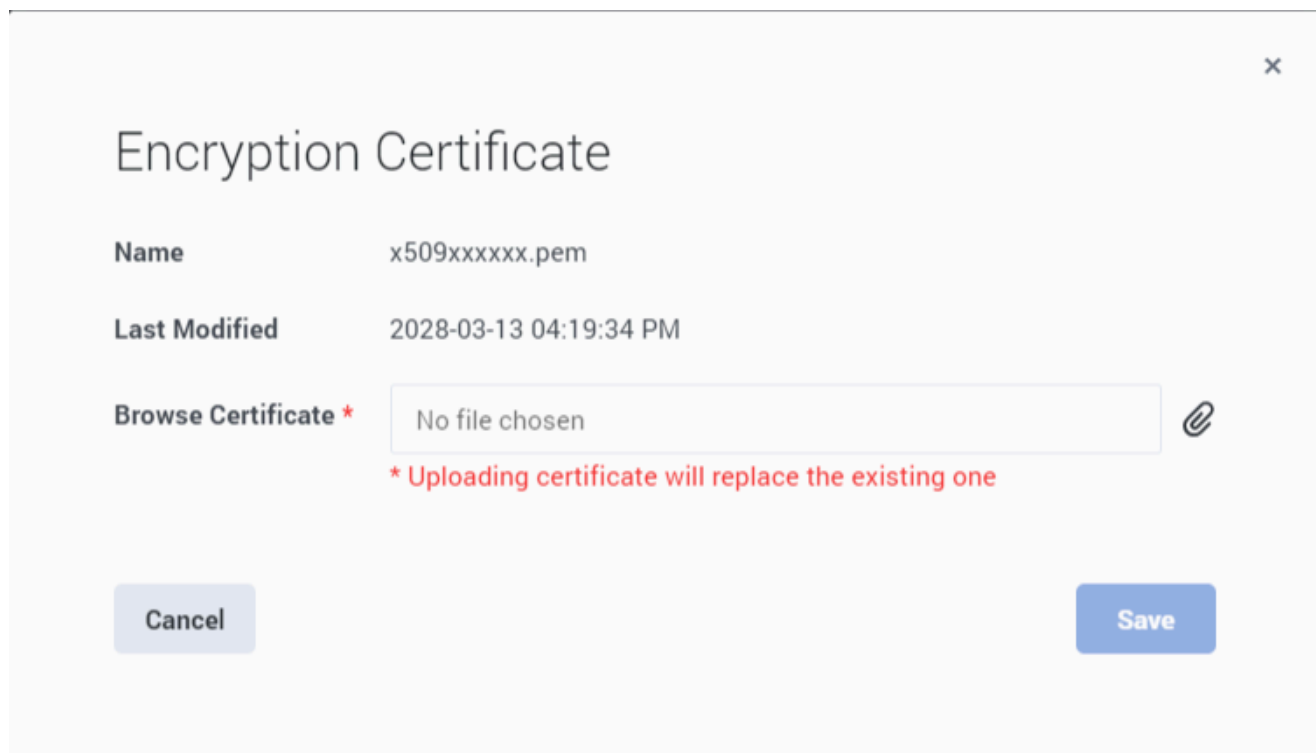
For an example of how to generate a self-signed certificate you can use with UDM, see [Certificate Requirements](#). You can then import the certificate into UDM.

General Data Protection Regulation (GDPR) compliance

In general, Genesys support for GDPR compliance is based on default configuration settings and typical application usage. User Data Management, like other underlying components within Genesys Multicloud CX, does not store sensitive information beyond 30 days. Users who download their data using this tool are responsible for GDPR compliance in regards to any data that they have downloaded.

For more information, see [Genesys Multicloud CX Support for GDPR](#).

Importing an encryption certificate



The screenshot shows a dialog box titled "Encryption Certificate" with a close button (X) in the top right corner. The dialog contains the following information:

- Name:** x509xxxxxx.pem
- Last Modified:** 2028-03-13 04:19:34 PM
- Browse Certificate ***: A text input field containing "No file chosen" and a gear icon (Settings) to its right.

Below the input field, a red asterisked note reads: *** Uploading certificate will replace the existing one**

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Save" on the right.

Before you can export data, a valid encryption certificate must be specified in your user preferences.

To add (or change) your encryption certificate, click on **Settings** (the gear icon) and select **Encryption Certificate**.

In the **Browse** field, choose the certificate file you want to use and save your changes.

Important

When you upload a certificate, it replaces the current certificate.