User Data Management Administrator's Guide

Certificates Management

11/4/2024

Contents

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.

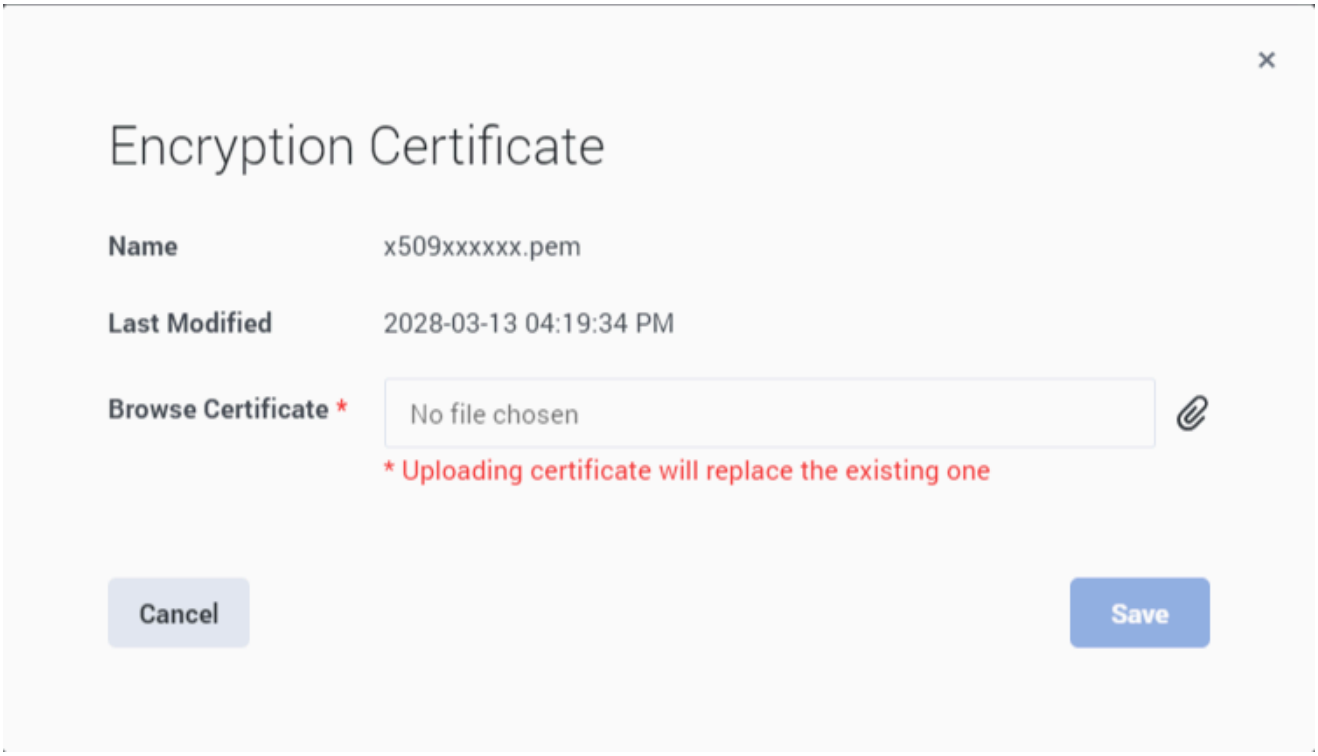
For an example of how to generate a self-signed certificate you can use with UDM, see Certificate Requirements. You can then import the certificate into UDM.

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



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.