Installing certificates to import MDM messages

1 Overview
2 Installer Utility
  2.1 System Administrators
3 Manual configuration
  3.1 Certificates
  3.2 Installation

Overview

This guide is to assist customers with MDM messages that fail to import due to certificate validity issues. It provides an overview for installing the Medicare Sha2 certificate chain so Medical Director will import MDM messages instead of rejecting them. **This is not necessary if Medical Director 4.1 and above is in use at the site.**

Installer Utility

Download the utility here.

The MD5 of the file should be 6494f7e2d2bca33304df32e2805ab186 if you want to validate your download has not been tampered with.

Medical Objects has packaged the required certificates into a single executable for easy installation. The certificates will be installed into the required locations once the application is run. Note that the application must be run by the user on the machine that they are performing their Medical Director message import on. This is because the certificates must be installed into the users certificate store not the local machine store for them to be available to Medical Director.

Once downloaded run the application CertificateChainInstaller.exe and press the install button when you are ready. If the certificates have not been installed for the user before, a dialog will appear asking if you want to trust the root certificate from Medicare. You will need to select Yes for the certificate to be installed (Note that this does mean any certificate authored by Medicare may now be found to be valid).

System Administrators

The application can be run with a switch "-silent". This will supress the GUI and install the certificates immediately on running the application. This means the application can be referenced in a user login script for automatic install. Note however that the user will still be asked by a secondary dialog if they want to trust the root certificate which is expected as it will then allow that user to utilise other Medicare certificates if they come into contact with them. Note also that once installed subsequent executions of the application will not cause the dialog to be raised as the root will be detected as already installed.

Manual configuration

Certificates

The required Sha2 certificates can be downloaded here: https://www.certificates-australia.com.au/

The files downloaded from the links in the left hand pane "Root CA Certificate" and "OCA Certificate" are what is required.

Installation

1. Download the **Root CA Certificate** above and open file that just downloaded; it should end in .cer
2. Click the 'Install Certificate' button.
3. Select 'Current User' and click 'Next'.
4. Select the 'Place Certificates in the following stores' option and click 'Browse'.
5. Select 'Trusted Root Certification Authorities' and then click the 'OK' button.
6. Click the 'Next' and then 'Finish' buttons.
7. If this certificate has never been installed a dialog will display asking if you trust the certificate. You will have to choose Yes if you agree that any Medicare certificates the user interacts with may be validated by the certificate you are installing.
8. Repeat the above steps but for the **OCA Certificate** link. **Except** this certificate must be placed in the 'Intermediate Certification Authorities' store.