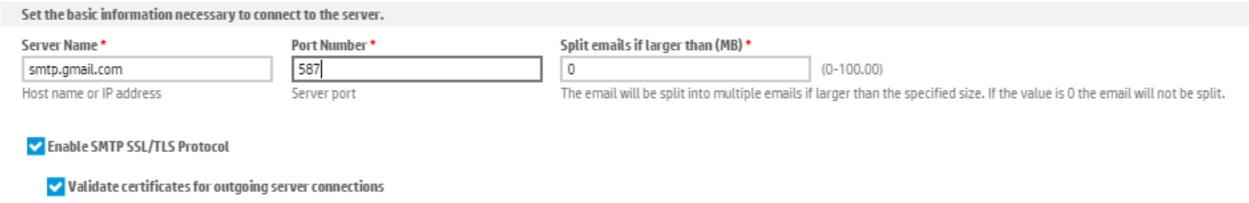
Scan to Email Setup with Cloud-Based SMTP Services

This document provides some tips and tricks for getting Scan to Email configured correctly when using Cloud-Based SMTP services. While this is generally a straightforward process when using an on-premise SMTP server, many customers are using SMTP services from Google or Microsoft. There are some unique setup options that may need to be enabled for these.

Using Gmail

Basic Settings-You will need a valid Google account since the Gmail server requires authentication. In the SMTP setup use the smtp server name “smtp.gmail.com”. The device will need to connect over TLS, so configure the device to use port 587 and make sure the “Enable SMTP SSL/TLS Protocol” box is checked. If you choose to leave the “Validate certificates for outgoing server connections” checked, you will need to install a valid certificate for Gmail on the MFP. See section “Validate Certificates” below.



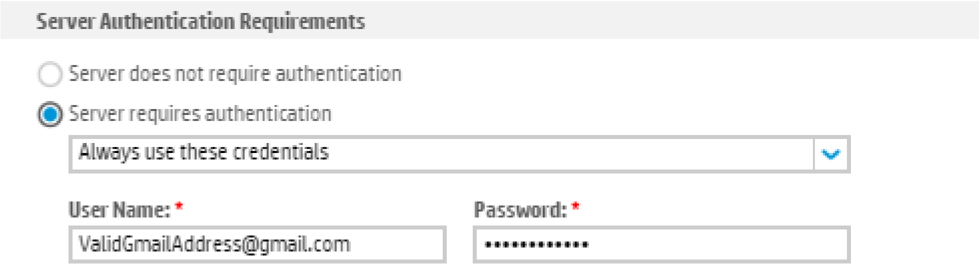
Set the basic information necessary to connect to the server.

Server Name *	Port Number *	Split emails if larger than (MB) *
smtp.gmail.com	587	0 (0-100.00)
Host name or IP address	Server port	The email will be split into multiple emails if larger than the specified size. If the value is 0 the email will not be split.

☑ Enable SMTP SSL/TLS Protocol

☑ Validate certificates for outgoing server connections

As mentioned, Gmail requires authentication, and you will want to always use the same Gmail credential



Server Authentication Requirements

○ Server does not require authentication

● Server requires authentication

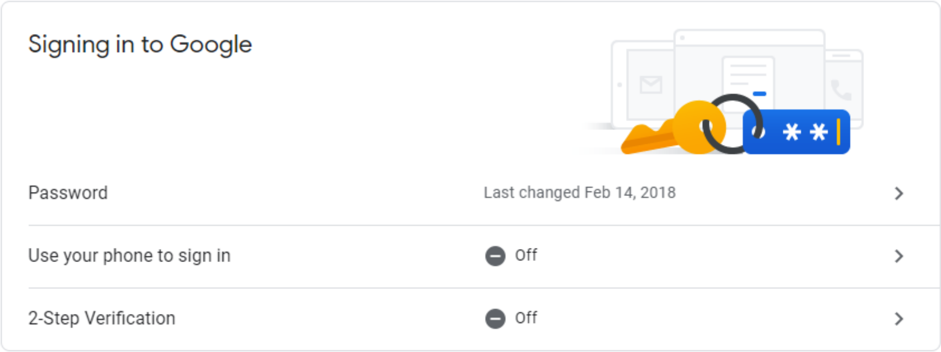
Always use these credentials

User Name: * ValidGmailAddress@gmail.com

Password: * •••••••••••••

Also note that while you will also need to configure a “Default From:” address on the MFP, the actual email address that will be used for sending is the account used to authenticate to Gmail.

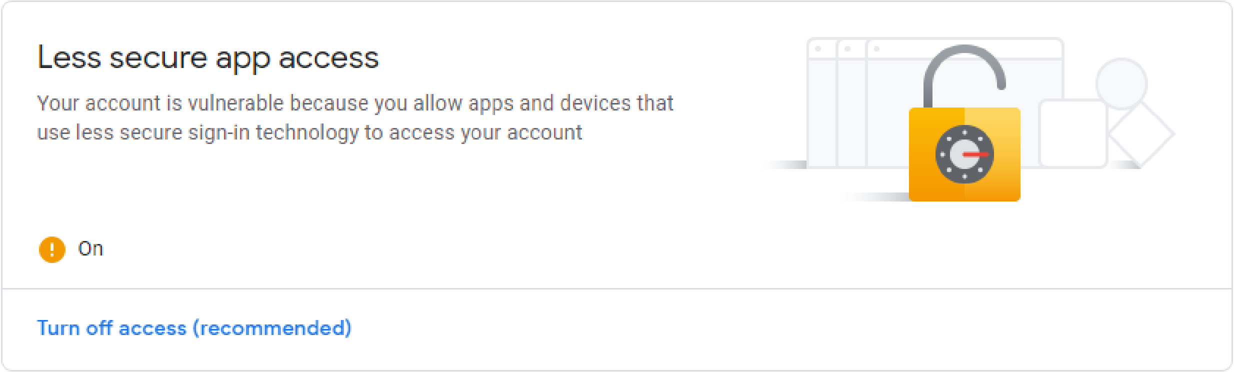
Turn off 2-Step Verification-while 2-step verification is often a good security practice, if this is enabled, it will block the MFP from being able to authenticate to Gmail. This should be turned off for the Gmail account being used to authenticate. Go to the Google Account, and you can disable this under Security>Signing in to Google



Signing in to Google

Password	Last changed Feb 14, 2018	›
Use your phone to sign in	⊖ Off	›
2-Step Verification	⊖ Off	›

Allow Less Secure App Access-Google will consider this a security risk, but without turning this on, the authentication from the MFP will fail. Go to the Google Account being used to authenticate, and enable it under Security>Less Secure App Access



Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account

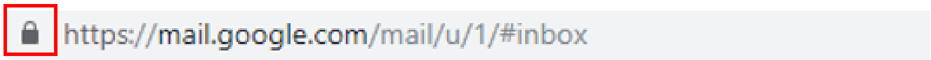
! On

Turn off access (recommended)

Validate Certificates-when setting up the SMTP information you can choose to validate certificates for outgoing server connections.   If you leave this option checked, the MFP will need a root CA certificate to validate the Gmail server certificate against. By default, it doesn't have the matching CA certificate needed, so connection to the server will fail. You can either uncheck the box so that the MFP doesn't validate the server's certificate, or you can install a proper CA certificate for it to validate against. To get the certificate and install it, take the following steps.

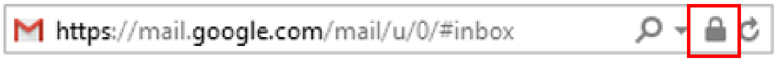
Browse to Gmail in an internet browser and log in with a valid account. Near where the URL is displayed, click on the padlock icon

Google Chrome



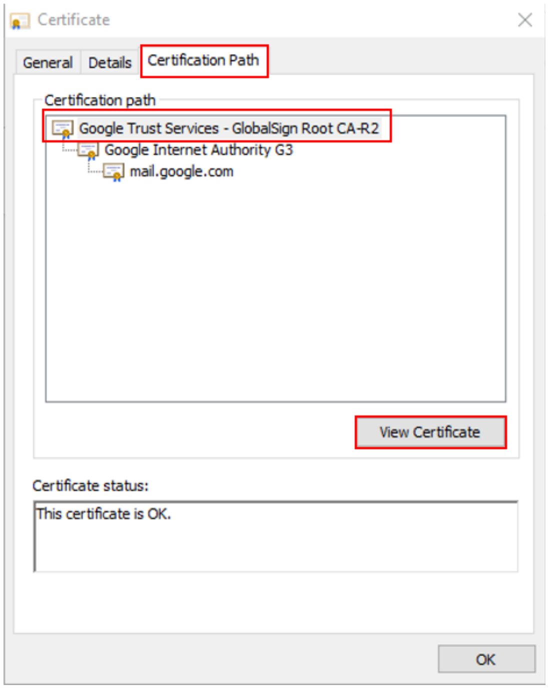
https://mail.google.com/mail/u/1/#inbox

Internet Explorer



https://mail.google.com/mail/u/0/#inbox

Click on “Certificate (Valid)” in Google Chrome or “View Certificates” in IE. Click on the “Certification Path” tab, and then click on “Google Trust Services -GlobalSign Root CA-R2” and click “View Certificate”.



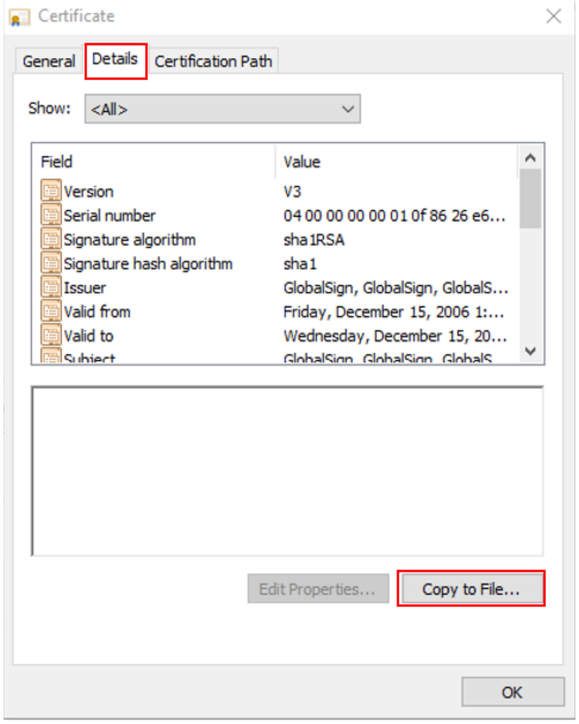
Certification path

- Google Trust Services - GlobalSign Root CA-R2
  - Google Internet Authority G3
    - mail.google.com

Certificate status:

This certificate is OK.

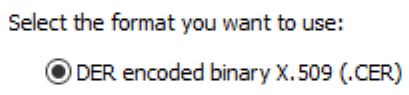
In the new window that opens, click on the “Details” tab and then click “Copy to File…” This will export the GlobalSign Root CA certificate to your computer.



Show: <All>

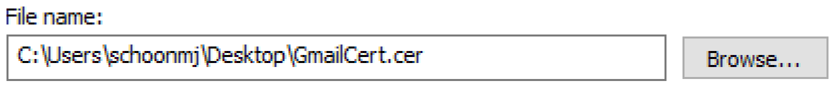
Field	Value
Version	V3
Serial number	04 00 00 00 00 01 0f 86 26 e6...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	GlobalSign, GlobalSign, GlobalS...
Valid from	Friday, December 15, 2006 1:...
Valid to	Wednesday, December 15, 20...
Subject	GlobalSign, GlobalSign, GlobalS

The Certificate Export Wizard will open, click “Next” on the first page. Next, choose the format “DER encoded binary X.509 (.CER)” and click “Next”


Select the format you want to use:

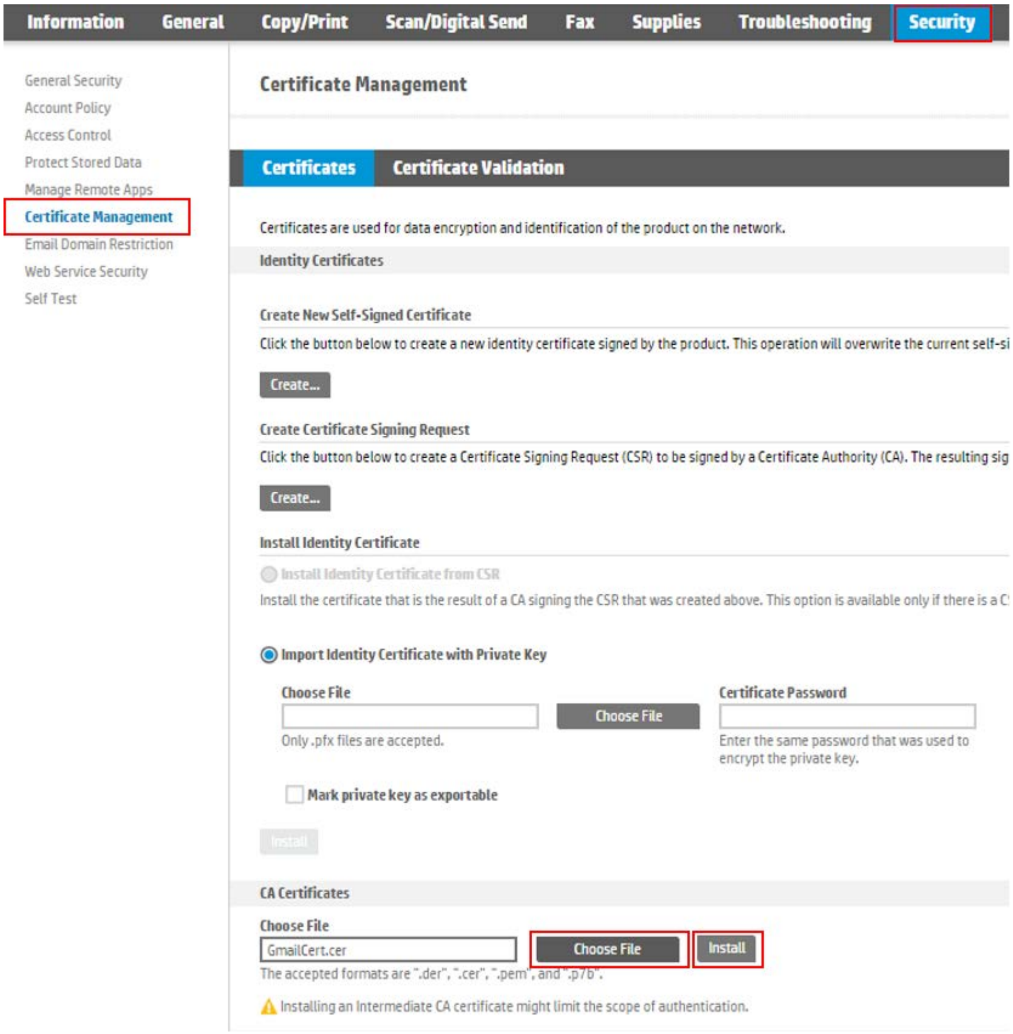
● DER encoded binary X.509 (.CER)

On the next page, select the path you want to save the certificate to:


File name:

C:\Users\schoonmj\Desktop\GmailCert.cer

Then click “Next” and “Finish”. You now need to upload the certificate to the MFP. Browse to the device’s web server, sign in as the administrator, then click over the Security Tab and on the left hand side, select “Certificate Management”. Scroll down until you see a label for “CA Certificates”. Use the “Choose File” button to browse to your certificate, and then click “Install”.



Certificate Management

Certificates are used for data encryption and identification of the product on the network.

Identity Certificates

Create New Self-Signed Certificate

Click the button below to create a new identity certificate signed by the product. This operation will overwrite the current self-si

Create Certificate Signing Request

Click the button below to create a Certificate Signing Request (CSR) to be signed by a Certificate Authority (CA). The resulting sig

Install Identity Certificate

○ Install Identity Certificate from CSR

Install the certificate that is the result of a CA signing the CSR that was created above. This option is available only if there is a C

● Import Identity Certificate with Private Key

Choose File

Only .pfx files are accepted.

Certificate Password

Enter the same password that was used to encrypt the private key.

□ Mark private key as exportable

CA Certificates

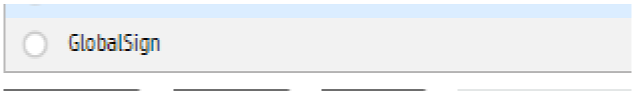
Choose File

GmailCert.cer

The accepted formats are ".der", ".cer", ".pem", and ".p7b".

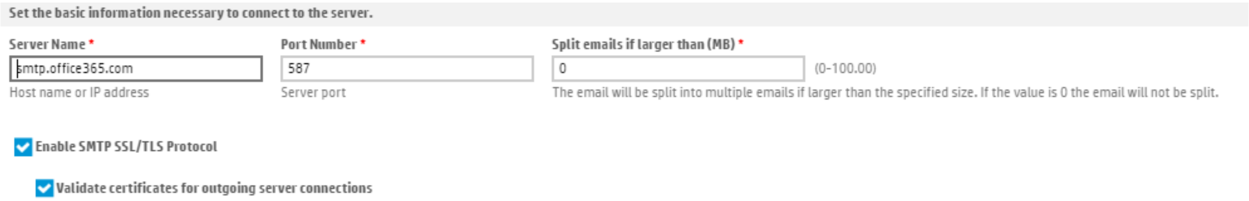
⚠ Installing an Intermediate CA certificate might limit the scope of authentication.

You should now see a new GlobalSign CA certificate in the Certificates list at the bottom of the screen, and the MFP will now be able to properly validate Gmail’s certificate.


○ GlobalSign

Using Office365

Basic Settings-A valid O365, Hotmail.com or Outlook.com email address will be required to authenticate to the server. In the SMTP setup, use the SMTP server name “smtp.office365.com”. The device will need to connect over TLS 1.2, so configure the device to use port 587 and make sure the “Enable SMTP SSL/TLS Protocol” box is checked.



Set the basic information necessary to connect to the server.

Server Name * smtp.office365.com
Host name or IP address

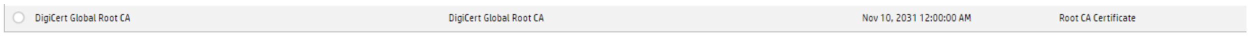
Port Number * 587
Server port

Split emails if larger than (MB) * 0 (0-100.00)
The email will be split into multiple emails if larger than the specified size. If the value is 0 the email will not be split.

☑ Enable SMTP SSL/TLS Protocol

☑ Validate certificates for outgoing server connections

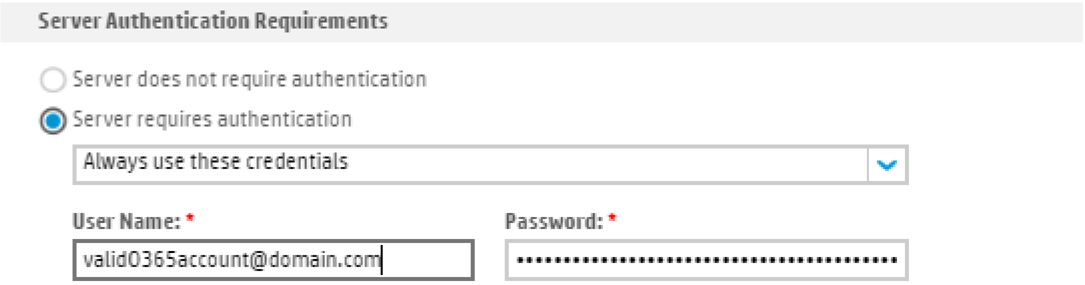
If you choose to enable the “Validate certificates for outgoing server connections” option, you will need to verify that the appropriate certificate is installed. As of the writing of this document, HP Enterprise devices come pre-loaded with the DigiCert Global Root CA, which is the required certificate. You can validate the presence of this certificate in the EWS by browsing to Security>Certificate Management, and then viewing it in the Installed Certificates area:



○ DigiCert Global Root CA   DigiCert Global Root CA   Nov 10, 2031 12:00:00 AM   Root CA Certificate

If the certificate is not installed, you will need to install it. See section “Validate Certificates” below.

As mentioned above, O365 requires authentication, you will want to always use the same O365 credentials. This can be an O365 account, a Hotmail.com account, or an Outlook.com account-all are serviced by the same Office 365 SMTP servers.



Server Authentication Requirements

○ Server does not require authentication

● Server requires authentication

Always use these credentials

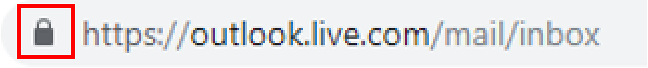
User Name: * valid0365account@domain.com

Password: * ••

Default From-A Default From address must always be included to complete a valid setup of Scan to Email. When using O365, there is an additional requirement that the Default From address be a valid O365 email address and must be the same address that is used for authentication to the server. If these two do not match, sending emails from the device will fail.

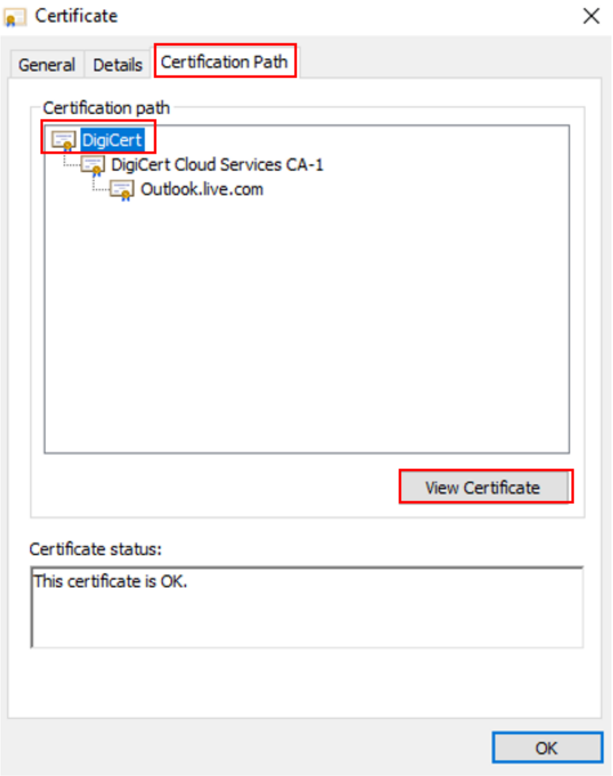
Validate Certificates-If this option is chosen when setting up the SMTP information, the MFP needs to have a root CA certificate to validate O365’s server certificate against. In HP Enterprise MFPs, this CA certificate is generally pre-loaded. If is the “DigiCert Global Root CA”. If this certificate is not present, then the connection to the SMTP server will fail. The option to validate server certificates can either be disabled, or a valid CA can be added. To get the certificate and install it, take the following steps:

Browse to O365 in an internet browser and log in with a valid account. Near where the URL is displayed, click on the padlock icon



https://outlook.live.com/mail/inbox

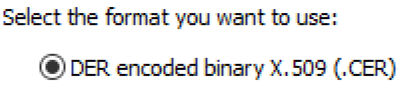
Click on "Certificate (Valid)" in Google Chrome or "View Certificates" in IE. Click on the "Certification Path" tab, and then click on "DigiCert" and click "View Certificate".



DigiCert
DigiCert Cloud Services CA-1
Outlook.live.com

Certificate status:
This certificate is OK.

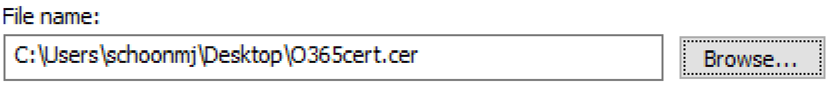
In the new window that opens, click on the "Details" tab and then click "Copy to File…" This will export the DigiCert certificate to your computer. The Certificate Export Wizard will open, click "Next" on the first page. Next, choose the format "DER encoded binary X.509 (.CER)" and click "Next"



Select the format you want to use:

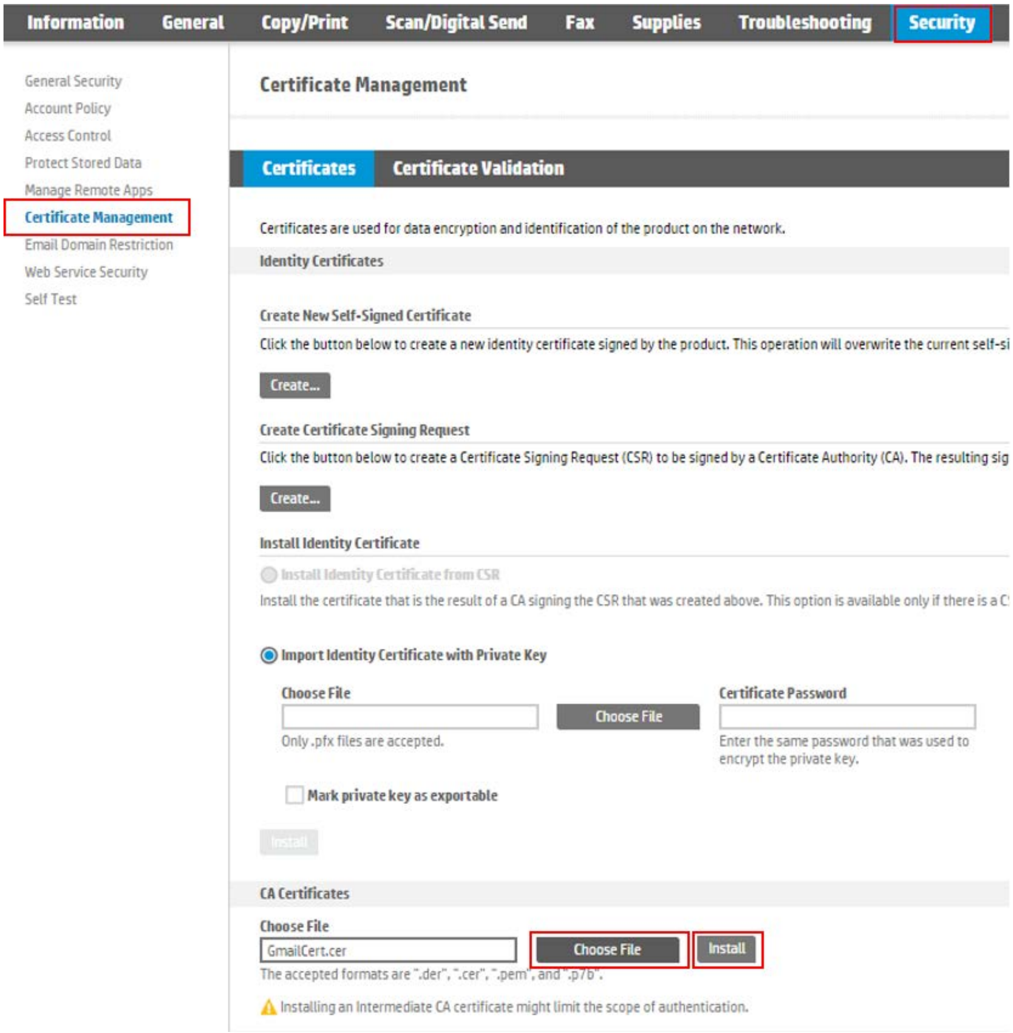
● DER encoded binary X.509 (.CER)

On the next page, select the path you want to save the certificate to:



File name: C:\Users\schoonmj\Desktop\O365cert.cer

Then click "Next" and "Finish". You now need to upload the certificate to the MFP. Browse to the device's web server, sign in as the administrator, then click over the Security Tab and on the left hand side, select “Certificate Management”. Scroll down until you see a label for “CA Certificates”. Use the “Choose File” button to browse to your certificate, and then click “Install”.



Certificate Management

Certificates | Certificate Validation

Certificates are used for data encryption and identification of the product on the network.

Identity Certificates

Create New Self-Signed Certificate

Click the button below to create a new identity certificate signed by the product. This operation will overwrite the current self-si

Create...

Create Certificate Signing Request

Click the button below to create a Certificate Signing Request (CSR) to be signed by a Certificate Authority (CA). The resulting sig

Create...

Install Identity Certificate

○ Install Identity Certificate from CSR

Install the certificate that is the result of a CA signing the CSR that was created above. This option is available only if there is a C

● Import Identity Certificate with Private Key

Choose File [ ] Choose File

Only .pfx files are accepted.

Certificate Password [ ]

Enter the same password that was used to encrypt the private key.

□ Mark private key as exportable

Install

CA Certificates

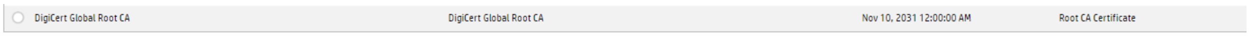
Choose File

GmailCert.cer | Choose File | Install

The accepted formats are ".der", ".cer", ".pem", and ".p7b".

⚠ Installing an Intermediate CA certificate might limit the scope of authentication.

You should now see the DigiCert Global Root CA loaded on the device and can now properly scan using the O365 SMTP server.



○ DigiCert Global Root CA	DigiCert Global Root CA	Nov 10, 2031 12:00:00 AM	Root CA Certificate