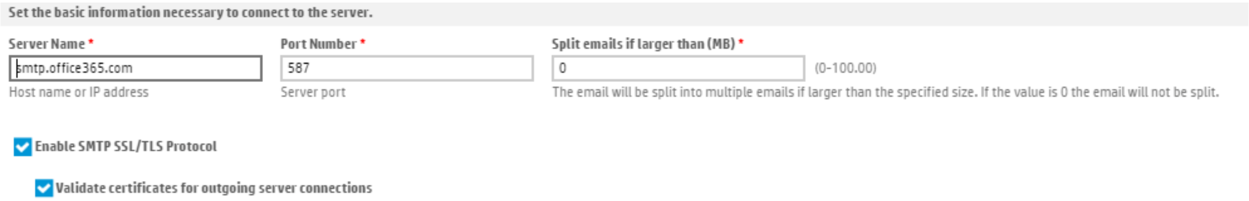
Using Office365

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

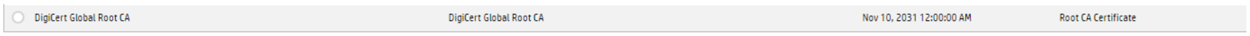
Port Number * 587
Server port

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

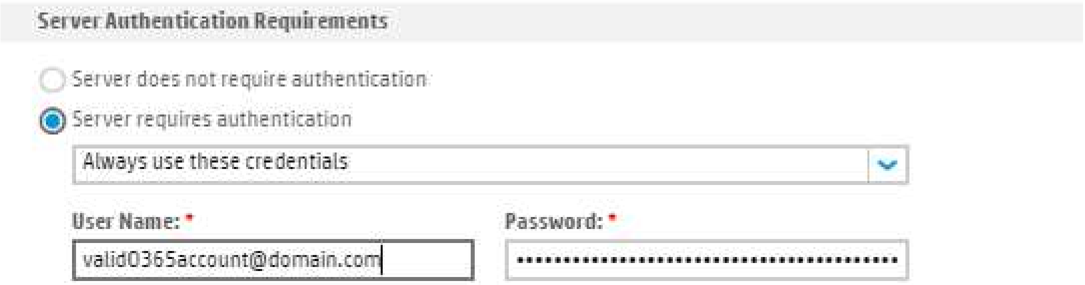
If you choose to enable the “Validate certificates for outgoing server connections” option, you will need to verify that the appropriate certificate is installed. As of the writing of this document, HP Enterprise devices come pre-loaded with the DigiCert Global Root CA, which is the required certificate. 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

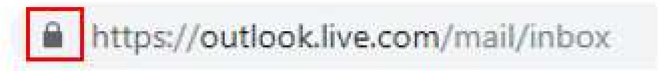
User Name: * validO365account@domain.com

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.

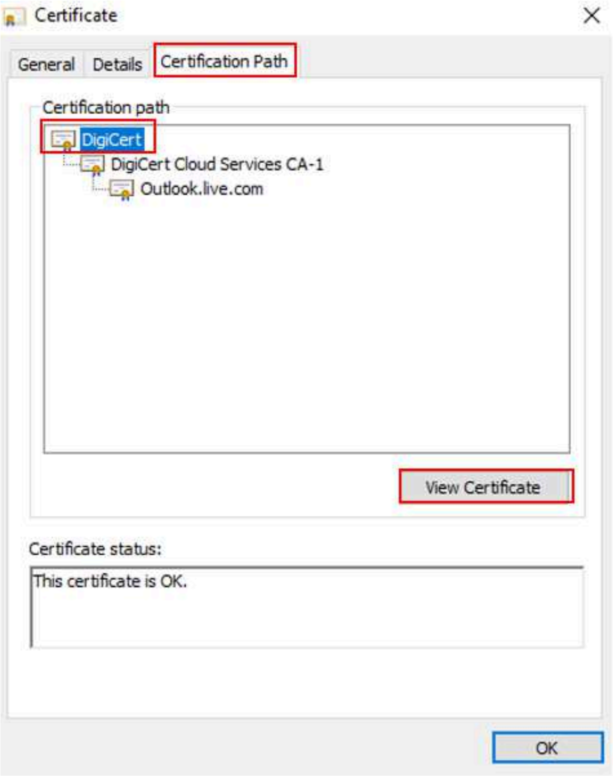
Validate Certificates-If this option is chosen when setting up the SMTP information, the MFP needs to have a root CA certificate to validate O365’s server certificate against. In HP Enterprise MFPs, this CA certificate is generally pre-loaded. If is the “DigiCert Global Root CA”. If this certificate 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



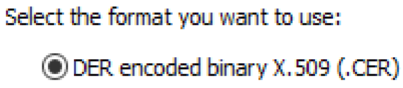
https://outlook.live.com/mail/inbox

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”.



This certificate is OK.

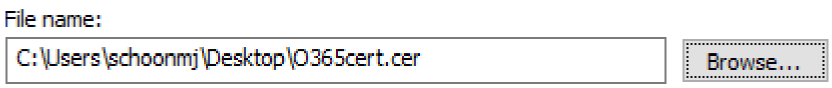
In the new window that opens, click on the “Details” tab and then click “Copy to File…” This will export the DigiCert certificate to your computer. The Certificate Export Wizard will open, click “Next” on the first page. Next, choose the format “DER encoded binary X.509 (.CER)” and click “Next”



Select the format you want to use:

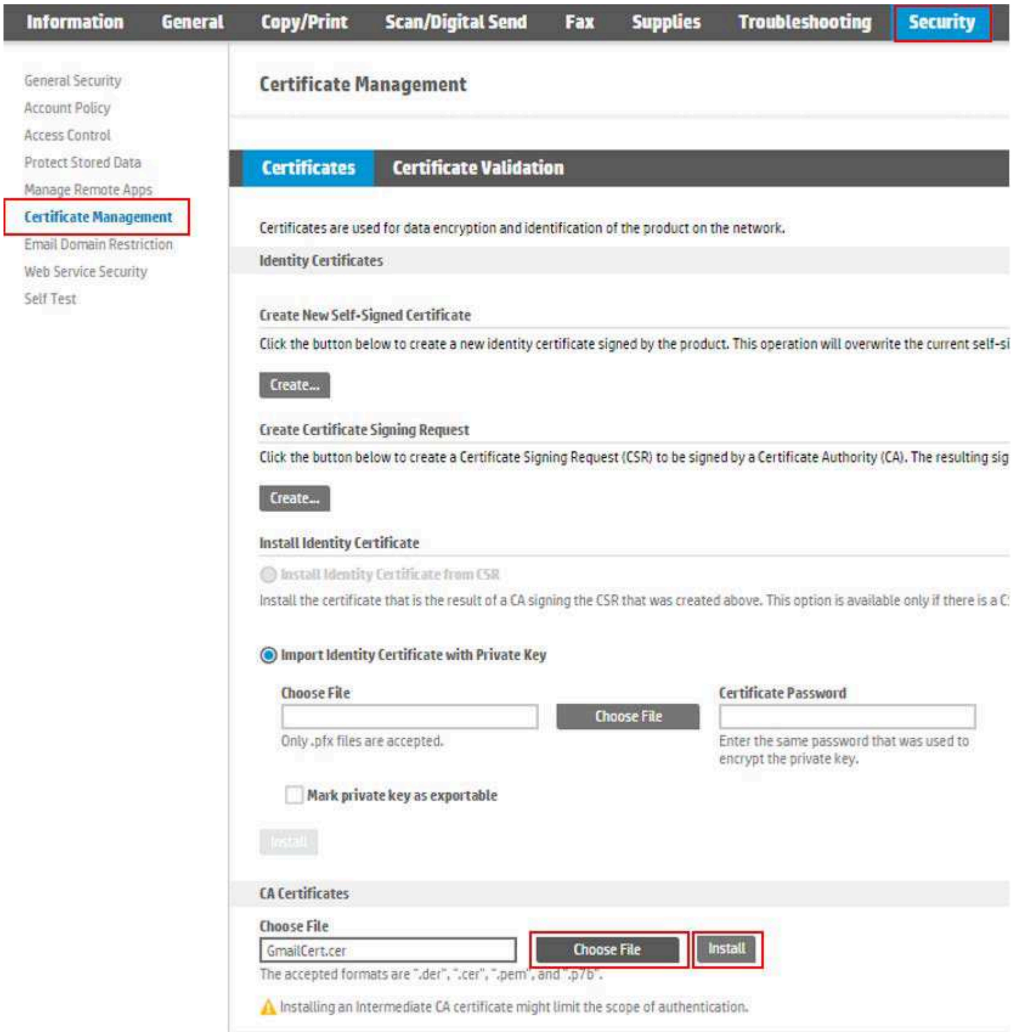
● DER encoded binary X.509 (.CER)

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 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

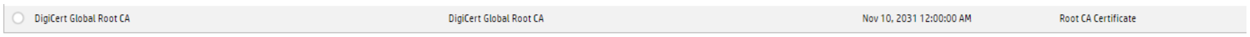
CA Certificates

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 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