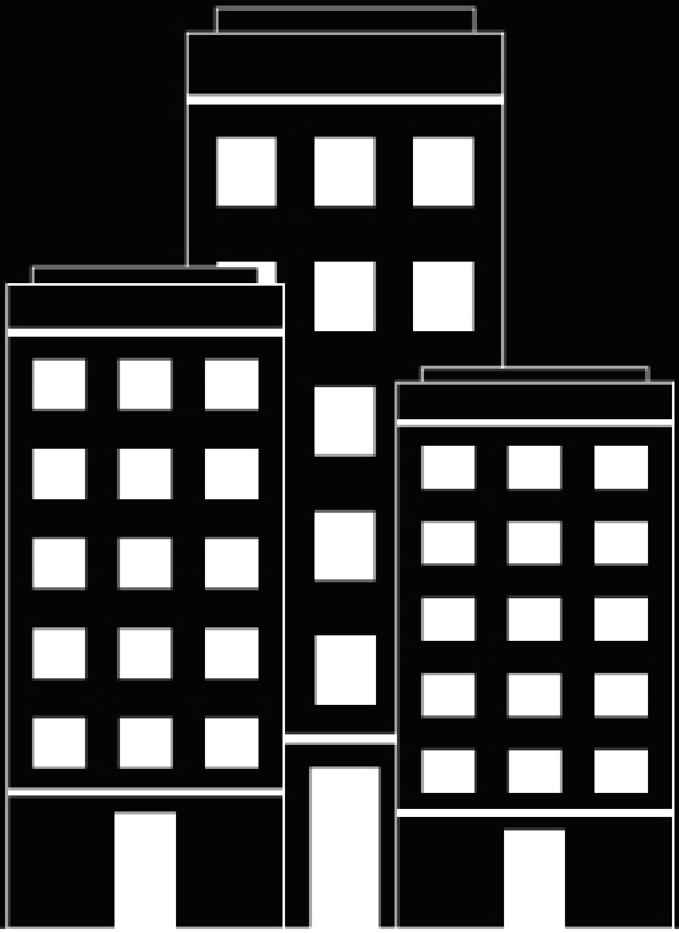

BlackBerry UEM

Securing connections using PKI

Administration

12.12

Contents

Certificates and PKI

A PKI certificate is a digital document issued by a CA that verifies the identity of a certificate subject and binds the identity to a public key. Each certificate has a corresponding private key that is stored separately. The public key and private key form an asymmetric key pair that can be used for data encryption and identity authentication. A CA signs the certificate to verify that entities that trust the CA can also trust the certificate.

Depending on the device capabilities and activation type, devices and apps can use certificates to:

- Authenticate using SSL/TLS when connecting to webpages that use HTTPS
- Authenticate with a work mail server
- Authenticate with a work Wi-Fi network or VPN
- Encrypt and sign email messages using S/MIME protection

Multiple certificates used for different purposes can be stored on a device.

Steps to use certificates

When you use PKI certificates with devices or apps, you perform the following actions:

Step	Action
1	If necessary, connect BlackBerry UEM to your organization’s PKI software.
2	Create one or more CA certificate profiles to send CA certificates to devices and apps.
3	Create SCEP, user credential, or shared certificate profiles or upload certificates for a specific user to send client certificates to devices and apps.
4	If necessary, associate certificate profiles with Wi-Fi, VPN, or email profiles.
5	If necessary, assign certificate profiles to user accounts, user groups, or device groups.
6	If using certificates with a BlackBerry Dynamics app, in the app settings, select "Allow BlackBerry Dynamics apps to use user certificates, SCEP profiles, and user credential profiles".

Integrating BlackBerry UEM with your organization's PKI software

If your organization uses a PKI solution to issue certificates, you can extend the certificate-based authentication provided by those PKI services to the devices and apps that you manage with BlackBerry UEM.

Entrust products (for example, Entrust IdentityGuard and Entrust Authority Administration Services) and OpenTrust products (for example, OpenTrust PKI and OpenTrust CMS) provide CAs that issue client certificates. You can configure a connection with your organization’s PKI software and use profiles to send the CA certificate and client certificates to devices.

For BlackBerry Dynamics enabled devices, you can also set up a PKI connector that creates a connection between BlackBerry UEM and a CA server to enroll certificates for BlackBerry Dynamics apps or use an app that supports app-based certificate enrollment such as Purebred.

Connect BlackBerry UEM to your organization’s Entrust software

To allow BlackBerry UEM to send certificates issued by your organization's Entrust software (for example, Entrust IdentityGuard or Entrust Authority Administration Services) to devices and BlackBerry Dynamics apps, you can add a connection to your organization's Entrust software to BlackBerry UEM.

Before you begin: Contact your organization’s Entrust administrator to obtain:

- the URL of the Entrust MDM Web Service
- the login information for an Entrust administrator account that you can use to connect BlackBerry UEM to the Entrust software
- the Entrust CA certificate that contains the public key (.der, .pem, or .cert); BlackBerry UEM uses this certificate to establish SSL connections to the Entrust server

1. On the menu bar, click **Settings**.
2. Click **External integration > Certificate authority**.
3. Click **Add an Entrust connection**.
4. In the **Connection name** field, type a name for the connection.
5. In the **URL** field, type the URL of the Entrust MDM Web Service.
6. In the **Username** field, type the username of the Entrust administrator account.
7. In the **Password** field, type the password of the Entrust administrator account.
8. To upload a CA certificate to allow BlackBerry UEM to establish SSL connections to the Entrust server, click **Browse**. Navigate to and select the CA certificate.
9. To test the connection, click **Test connection**.
10. Click **Save**.

After you finish:

- Create a user credential profile to send certificates from your PKI software to devices.

Connect BlackBerry UEM to your organization’s Entrust IdentityGuard server to use smart credentials

If your organization uses derived smart credentials managed by Entrust IdentityGuard, you can use derived smart credentials with Android devices and with BlackBerry Dynamics apps on iOS and Android devices.

Before you begin:

Contact your organization’s Entrust administrator to obtain the following information:

- URL of the Entrust IdentityGuard server
- Name of the smart credential to be activated on devices as specified in Entrust IdentityGuard
- Entrust CA certificate to send the certificate to devices

1. On the menu bar, click **Settings**.
2. Click **External integration > Certificate authority**.
3. Click **Add a connection for Entrust smart credentials**.
4. In the **Smart credential name** field, type the name of the smart credential specified in Entrust IdentityGuard.
5. In the **Entrust URL** field, type the URL of the Entrust IdentityGuard server.
6. Click **Add**.

After you finish:

- Create a CA certificate profile to send the Entrust CA certificate to devices and assign the profile to the same users or groups that the user credential profile will be assigned to.
- Create a user credential profile to use Entrust smart credentials on devices.

Connect BlackBerry UEM to your organization's OpenTrust software

To extend OpenTrust certificate-based authentication to devices, you must add a connection to your organization's OpenTrust software. BlackBerry UEM supports integration with OpenTrust PKI 4.8.0 and later and OpenTrust CMS 2.0.4 and later. This connection is not supported by BlackBerry Dynamics apps.

Before you begin: Contact your organization’s OpenTrust administrator to obtain the URL of the OpenTrust server, the client-side certificate that contains the private key (.pfx or .p12 format), and the certificate password.

1. On the menu bar, click **Settings**.
2. Click **External integration > Certificate authority**.
3. Click **Add an OpenTrust connection**.
4. In the **Connection name** field, type a name for the connection.
5. In the **URL** field, type the URL of the OpenTrust software.
6. Click **Browse**. Navigate to and select the client-side certificate that BlackBerry UEM can use to authenticate the connection to the OpenTrust server.
7. In the **Certificate password** field, type the password for the OpenTrust server certificate.
8. To test the connection, click **Test connection**.
9. Click **Save**.

After you finish:

- Create a user credential profile to send certificates from your PKI software to devices.

- When you use the BlackBerry UEM connection with OpenTrust software to distribute certificates to devices, there may be a short delay before the certificates are valid. This delay might cause issues with email authentication during the device activation process. To resolve this issue, in the OpenTrust software, configure the OpenTrust CA and set "Backdate Certificates (seconds)" to 180.

Connect BlackBerry UEM to a BlackBerry Dynamics PKI Connector

If you want to use your organization's PKI software to enroll certificates for BlackBerry Dynamics apps, and your PKI software isn't supported for a direct connection with BlackBerry UEM, you can set up a BlackBerry Dynamics PKI connector to communicate with your CA and link BlackBerry UEM to the PKI connector.

Before you begin: Set up a BlackBerry Dynamics PKI connector.

1. On the menu bar, click **Settings > External integration > Certificate authority**.
2. Click **Add a BlackBerry Dynamics PKI connection**.
3. In the **Connection name** field, type a name for the connection.
4. In the **URL** field, type the URL of the PKI connector.
5. Select one of the following options:
   - **Authenticate with username and password**: Choose this option if BlackBerry UEM authenticates with the BlackBerry Dynamics PKI Connector using password-based authentication.
   - **Authenticate with client certificate**: Choose this option if BlackBerry UEM authenticates with the BlackBerry Dynamics PKI Connector using certificate-based authentication.
6. If you selected **Authenticate with username and password**, in the **Username** and **Password** fields, type the username and password for the BlackBerry Dynamics PKI connector.
7. If you selected **Authenticate with client certificate**, click **Browse** to select and upload a certificate that is trusted by the BlackBerry Dynamics PKI Connector. In the **Client certificate password** field, type the password for the certificate.
8. In the **Trusted certificate for the PKI connector** section you can specify the certificate that BlackBerry UEM uses to trust connections to the PKI connector, select one of the following options:
   - **CA certificate from BlackBerry Control TrustStore**
   - **CA certificate**: If you select this option you must click Browse to navigate to and select your organization's CA certificate.
   - **PKI connector server certificate**: If you select this option you must click Browse to navigate to and select your organization's PKI connector server certificate.
9. To test the connection, click **Test connection**.
10. Click **Save**.

After you finish:

- Create a user credential profile to send certificates from your PKI software to devices.

Configuring a PKI connector for BlackBerry Dynamics apps

A PKI connector is a set of Java programs and web services on a back-end server that allows BlackBerry UEM to send certificate requests and receive responses from the CA.

BlackBerry UEM uses the BlackBerry Dynamics user certificate management protocol to communicate with the PKI connector. This protocol runs over HTTPS and defines JSON-formatted messages.

The PKI connector implements the user certificate management protocol. For an example of an implementation of a PKI connector, visit the Good Control documentation to see the *PKI Cert Creation via Good Control: Reference Implementation* and PKI Connector reference implementation. The example to build and deploy the

PKI connector in this document also applies for BlackBerry UEM; however, you must configure the connection between BlackBerry UEM and the PKI connector in the BlackBerry UEM management console.

PKI connector interactions

BlackBerry UEM makes API calls to the PKI connector using the HTTP POST method. The PKI connector supports password authentication and certificate-based authentication.

GetInfo API

This API detects the commands that the PKI connector has implemented. This command is also used to verify the authentication credentials provided in BlackBerry UEM and to test the connection between BlackBerry UEM and the PKI connector.

If this command is not implemented, BlackBerry UEM will assume this is not a valid PKI connector.

The path component of the URI sent is as follows: `customerSpecifiedPrefix/pki?operation=getInfo`

The `customerSpecifiedPrefix` is optional. It specifies where the service is hosted on the server when it is not hosted in the default path.

The JSON formatted response expected in the HTTP body is as follows:

Element or Key	Type	Required	Response
operations	Array of strings	Y	Array listing all of the commands implemented by the PKI connector

Sample request/response

Assuming that in the BlackBerry UEM management console, the PKI connector URL is set as: https://cert.example.com

```
GET /pki?operation=getInfo HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: 0

Response

HTTP/1.0 200 OK Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ

{
      “operations” : [“getInfo”, “getUserKeyPair”]
}
```

Request Key Pair API

This API is used to fetch a user certificate when the key pair has been created. This request may be used for initial certificate requests.

The path component of the URI is sent as follows: `customerSpecifiedPrefix/pki?operation=getUserKeyPair`.

The `customerSpecifiedPrefix` is optional. It specifies where the service is hosted on the server when it is not hosted in the default path.

The JSON formatted input sent in the HTTP body is as follows:

Element or Key	Type	Required	Comment
mType	String	Y	{"initialCert"]
user	String	Y	User email address or some other identifier Subject for the certificate created by the issuer
authToken	String	N	OTP or password (for initialCert)
reqId	String	Y	To assist sender to match response

The JSON formatted response in the HTTP body, a PKCS #12 payload which may be encrypted, is as follows:

Element/Key	Type	Required	Comments
status	String	Y	{success, failure}
failureInfo	String	N	See *Failure reasons* below
payloadType	String	N	=pkcs12
payload	Base64 encoded	N	pkcs12 containing the user's private key and public certificate. It may or may not be encrypted.
decryptionPassword	Base64 encoded	N	If the encryption password is the same as the OTP provided by the user, there is no need to provide descryptionPassword. If pkcs12 was password encrypted and OTP was not used, the password may be returned in the decryptionPassword.
reqId	String	Y	reqID received in the request

Sample request/response

Assuming that in the BlackBerry UEM management console, the PKI connector URL is set as: https://cert.example.com

Request: Over the SSL connection to server cert.example.com the following payload will be sent:

```
POST /pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
{
      "mType": "initialCert",
      "user": "joe.foo@example.com",
      "authToken": "56ht12d0",
      "reqId": "12487"
}
```

If the server URL was set as https://cert.example.com/foo, the request will look like:

```
POST /foo/pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
```

Response:

```
HTTP/1.0 200 OK
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
 {
      "status":"success",
      "reqId": "12487",
      "payloadType":"pkcs12",
      "decryptionPassword":"NTZodDEyZDA=",
      "payload":"BASE64 Encoded PKCS#12"
}
```

Failure reasons

These errors may be returned by the CA:

Failure	Description
unknownUser	User does not exist or is not allowed
badRequest	Badly formatted request
unknownRequest	Requested action is not supported
authFailure	Expired or incorrect OTP or password
badAlg	Unsupported or unrecognized algorithm used
unknownCert	Certificate used or referenced in the operation not found
badMessageCheck	Signature or integrity check failed
badTime	Time in the signature was not close enough
unknown	Any other errors treated as unknown errors

Connect BlackBerry UEM to your organization’s app-based PKI solution

App-based PKI solutions such as Purebred include an app installed on a device that communicates with a CA to enroll certificates and add them to the device. You can use an app-based PKI solution to provide certificates for use by BlackBerry Dynamics apps.

To use an app-based PKI solution with iOS devices, you must add a connection between BlackBerry UEM and the PKI provider. This task is not required to use an app-based PKI solution with only Android devices.

If the PKI app that retrieves certificates from the CA is not a BlackBerry Dynamics app, the BlackBerry UEM Client communicates with the PKI app to get the certificates and provide them to BlackBerry Dynamics apps.

Before you begin: Verify that the app that retrieves certificates for use by BlackBerry Dynamics apps is in the app list in BlackBerry UEM.

1. On the menu bar, click **Settings > External integration > Certificate authority**.
2. Click **Add a connection for device based certificates**.
3. Select the app that retrieves certificates from the PKI app for use by BlackBerry Dynamics apps. To use Purebred, select the BlackBerry UEM Client.
4. Click **Add**.

After you finish:

- Creating user credential profiles for app-based certificates.
- Create a user credential profile to use app-based certificates on iOS devices.
- Create a user credential profile to use certificates from the native keystore on Android devices

Providing client certificates to devices and apps

You and users can send client certificates to devices and apps in several ways.

How the certificate is added	Description	Supported devices
During device activation	BlackBerry UEM sends certificates to devices during the activation process. Devices use these certificates to establish secure connections between the device and BlackBerry UEM.	All
SCEP profiles	You can create SCEP profiles that devices use to connect to, and obtain client certificates from, your organization's CA using a SCEP service. Devices and BlackBerry Dynamics apps can use these certificates for certificate-based authentication and to connect to your work Wi-Fi network, work VPN, and work mail server.	iOS macOS Android Windows 10 BlackBerry 10
Connection to your organization's PKI solution	If your organization uses a PKI solution, such as Entrust or OpenTrust software products, to issue and manage certificates, you can create user credential profiles that devices use to get client certificates from your organization's CA. BlackBerry Dynamics enabled devices use these certificates for certificate-based authentication from BlackBerry Dynamics apps. Other devices use these certificates for certificate-based authentication from the browser, and to connect to your work Wi-Fi network, work VPN, and work mail server.	iOS Android BlackBerry 10
Shared certificate profiles	A shared certificate profile specifies a client certificate that BlackBerry UEM sends to iOS, macOS, and Android devices. BlackBerry UEM sends the same client certificate to every user that the profile is assigned to. The administrator must have access to the certificate and private key to create a shared certificate profile.	iOS macOS Android
Sending client certificates to individual user accounts	You can add a client certificate to a user account. BlackBerry UEM can send the certificate to the user's iOS and Android devices. If the certificate is associated with a user credential profile, devices can use these certificates to connect to your work Wi-Fi network, work VPN, and work mail server. The administrator must have access to the certificate and private key to send the client certificate to the user.	iOS Android BlackBerry 10

How the certificate is added	Description	Supported devices
User upload to UEM Self-Service	If your organization has an on-premises BlackBerry UEM environment, users can upload certificates to BlackBerry UEM Self-Service. BlackBerry UEM then pushes the certificate to the users devices. If the certificate is associated with a user credential profile, devices and BlackBerry Dynamics apps can use these certificates for certificate-based authentication and to connect to your work Wi-Fi network, work VPN, and work mail server. This feature is not supported in BlackBerry UEM Cloud.	iOS Android BlackBerry 10
User import	On BlackBerry 10 devices, users can import client certificates into the device's certificate store in the "Security and Privacy" section of the "System Settings". Certificates intended for use by the work browser or for sending S/MIME-protected messages from the work email account can be imported from the file system on the device or from a network location that is accessible from the work space. On Android devices, users can add certificates to the device native keystore for use with BlackBerry Dynamics apps.	Android BlackBerry 10
Smart cards	Users can import S/MIME and SSL certificates to their devices from a smart card.	BlackBerry 10

Sending certificates to devices and apps using profiles

You can send certificates to devices and apps using the following profiles available in the Policies and Profiles library:

Profile	Description
CA certificate	CA certificate profiles specify a CA certificate that devices and BlackBerry Dynamics apps can use to trust the identity associated with any client or server certificate that has been signed by that CA.
User credential	User credential profiles send certificates to devices in the following ways: • They can specify a connection to your organization's PKI software to send client certificates to devices and BlackBerry Dynamics apps. • They can allow you to manually upload certificates in BlackBerry UEM and, in an on-premises environment, allow users to upload certificates using BlackBerry UEM Self-Service. • They can allow BlackBerry Dynamics apps on Android devices to use certificates from the device native keystore. • They can allow BlackBerry Dynamics apps to import certificates from other app-based PKI solutions such as Purebred.
SCEP	SCEP profiles specify how devices and BlackBerry Dynamics apps connect to, and obtain client certificates from, your organization's CA using a SCEP service.
Shared certificate	Shared certificate profiles specify a client certificate that BlackBerry UEM sends to iOS and Android devices. BlackBerry UEM sends the same client certificate to every user that the profile is assigned to.

For iOS and Android devices, you can also send a client certificate to a device by adding the certificate directly to a user account. For more information, see Add a client certificate to a user account.

For iOS, Android, and BlackBerry 10 devices, if your organization uses certificates for S/MIME, you can also use profiles to allow devices to get recipient public keys and check certificate status. For more information, see Extending email security using S/MIME.

For BlackBerry Dynamics apps to use certificates sent by profiles, you must select "Allow BlackBerry Dynamics apps to use user certificates, SCEP profiles, and user credential profiles" in the settings for the app.

Choosing profiles to send client certificates to devices and apps

You can use different types of profiles to send client certificates to devices and BlackBerry Dynamics apps. The type of profile that you choose depends on how your organization uses certificates and the types of devices that your organization supports. Consider the following guidelines:

- To use SCEP profiles, you must have a CA that supports SCEP.
- If you have set up a connection between BlackBerry UEM and your organization's PKI solution, use user credential profiles to send certificates to devices. You can connect directly to an Entrust CA or OpenTrust CA. You can also use a BlackBerry Dynamics PKI connector to connect to a CA server to enroll certificates for BlackBerry Dynamics enabled devices.

- To use certificates with BlackBerry Dynamics apps, you must use a user credential profile or add the certificates to individual user accounts.
- To allow users to upload certificates that they can use to connect to your work Wi-Fi network, work VPN, and work mail server, use a user credential profile.
- To use client certificates for Wi-Fi, VPN, and mail server authentication, you must associate the certificate profile with a Wi-Fi, VPN, or email profile.

  Note: Android Enterprise devices don't support using certificates sent to devices by BlackBerry UEM for Wi-Fi authentication.
- Shared certificate profiles and certificates that you add to user accounts do not keep the private key private because you must have access to the private key. Connecting to a CA using SCEP or user credential profiles is more secure because the private key is sent only to the device that the certificate was issued to.

Sending CA certificates to devices and apps

You might need to send CA certificates to devices if your organization uses S/MIME or if devices or BlackBerry Dynamics apps use certificate-based authentication to connect to a network or server in your organization’s environment.

When a CA certificate is stored on a device, the device and apps trust the identity associated with any client or server certificate signed by the CA. When the certificate for the CA that signed your organization's network and server certificates is stored on devices, device and apps can trust your networks and servers when they make secure connections. When the CA certificate that signed your organization's S/MIME certificates is stored on devices, the email client can trust the sender's certificate when a secure email message is received.

Multiple CA certificates that are used for different purposes can be stored on a device. You can use CA certificate profiles to send CA certificates to devices.

Create a CA certificate profile

Before you begin: Obtain the CA certificate file from your PKI administrator.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > CA certificate**.
3. Click +.
4. Type a name and description for the profile. Each CA certificate profile must have a unique name. Some names (for example, ca_1) are reserved.
5. In the **Certificate file** field, click **Browse** to locate the certificate file.
6. If the CA certificate is sent to BlackBerry 10 devices, on the BlackBerry tab, specify one or more of the following certificate stores to send the certificate to on the device:
   - Browser certificate store
   - VPN certificate store
   - Wi-Fi certificate store
   - Enterprise certificate store
7. If the CA certificate is sent to macOS devices, on the macOS tab, in the **Apply profile to** drop-down list, select **User** or **Device**.
8. Click **Add**.

CA certificate stores on BlackBerry 10 devices

CA certificates that are sent to BlackBerry 10 devices are saved to different certificate stores, depending on the purpose of the certificate.

Store	Description
Browser certificate store	The work browser on BlackBerry 10 devices uses the certificates in this store to establish SSL connections with servers in your organization's environment.
VPN certificate store	BlackBerry 10 devices use certificates in this store for VPN connections. You must set the "Trusted certificate source" setting in the VPN profile to "Trusted certificate store" to use the certificates in this store for work VPN connections.
Wi-Fi certificate store	BlackBerry 10 devices use certificates in this store for Wi-Fi connections. You must set the "Trusted certificate source" setting in the Wi-Fi profile to "Trusted certificate store" to use certificates in this store for work Wi-Fi connections.
Enterprise certificate store	BlackBerry 10 devices use certificates in this store to authenticate S/MIME-protected email messages that are received.

Sending client certificates to devices and apps using user credential profiles

User credential profiles allow devices to use client certificates obtained by the following methods:

- Manually uploading certificates to the BlackBerry UEM management console or, in an on-premises environment, to BlackBerry UEM Self-Service
- An established connection between BlackBerry UEM and your organization’s Entrust CA or OpenTrust CA
- For BlackBerry Dynamics apps on Android devices, certificates stored in the device native keystore
- For BlackBerry Dynamics apps, through an established BlackBerry Dynamics PKI connector connection
- For BlackBerry Dynamics apps, using an app-based PKI solution such as Purebred.

If users manually upload certificates in UEM Self-Service, you can see the certificate on the user page in the management console. You can also delete or replace the certificate. This feature is not supported in BlackBerry UEM Cloud.

User credential profiles are supported on iOS and Android devices, and on devices running BlackBerry 10 OS version 10.3.1 and later. App-based PKI solutions are supported for BlackBerry Dynamics apps on iOS and Android devices. Manually uploading certificates is supported for iOS, Android Enterprise, Samsung Knox Workspace, and BlackBerry 10 devices.

For more information about connecting BlackBerry UEM to your organization's PKI software, see Integrating BlackBerry UEM with your organization's PKI software.

Alternatively, you can use SCEP profiles to enroll client certificates to devices. You can also upload certificates directly to a user account. The type of profile you choose depends on how your organization uses the PKI software, the types of devices your organization supports, and how you want to manage certificates.

Create a user credential profile to manually upload certificates

User credential profiles can allow you or users to manually upload a certificate to be sent to the user's devices.

1. On the menu bar, click **Policies and Profiles**.

2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select **Manually uploaded certificate**.
6. If you are managing Android Enterprise devices and you want to prevent users from selecting the certificate to use for other purposes, on the **Android** tab, select **Hide certificate on Android Enterprise devices**. This option applies only to Android 9.0 and later devices.
7. Click **Add**.

After you finish:

- If devices use client certificates to authenticate with a Wi-Fi network, VPN, or mail server, associate the user credential profile with a Wi-Fi, VPN, or email profile.
- Assign the profile to user accounts and user groups.
- Add a client certificate to a user credential profile or instruct users to use BlackBerry UEM Self-Service to upload their own certificate.

Create a user credential profile to connect to your organization's PKI software

User credential profiles that connect to your organization's PKI software can enroll certificates for iOS, Android, and BlackBerry 10 OS version 10.3.1 and later devices. If the connection is to Entrust PKI software, the user credential profile can also enroll certificates for BlackBerry Dynamics apps.

Note: BlackBerry UEM doesn't support key history for certificates issued to BlackBerry Dynamics apps.

Before you begin:

- Configure a connection to your organization's Entrust or OpenTrust software.
- Contact your organization’s Entrust or OpenTrust administrator to confirm which PKI profile you should select. BlackBerry UEM obtains a list of profiles from the PKI software.
- Ask the Entrust or OpenTrust administrator for the profile values that you must provide. For example, the values for device type (devicetype), Entrust IdentityGuard group (iggroup), and Entrust IdentityGuard username (igusername).
- If your organization’s OpenTrust system is configured to return Escrowed Keys only, the OpenTrust administrator must verify that certificates are present for each user in the OpenTrust system. Assigning a user credential profile to users in BlackBerry UEM does not automatically create certificates for users in OpenTrust. In this scenario, a user credential profile can only distribute certificates to users who have an existing certificate in the OpenTrust system.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select the Entrust or OpenTrust connection that you configured.
6. In the **Profile** drop-down list, click the appropriate profile.
7. Specify the values for the profile.
8. If necessary, you can specify a SAN type and value for an Entrust client certificate.
   a) In the SAN table, click +.
   b) In the **SAN type** drop-down list, click the appropriate type.
   c) In the **SAN value** field, type the SAN value.

If the SAN type is set to "RFC822 name," the value must be a valid email address. If it is set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If it is set to "NT principal name," the value must be a valid principal name. If it is set to "DNS name," the value must be a valid FQDN.

9. Specify the **Renewal period** for the certificate. The period can be between 1 and 120 days.
10. If BlackBerry 10 devices use the client certificate to encrypt email messages using S/MIME, and you want devices to retain access to expired certificates so that users can open older email messages, select the **Include certificate history** check box.
11. Click **Add**.

After you finish:

- If devices use client certificates to authenticate with a Wi-Fi network, VPN, or mail server, associate the user credential profile with a Wi-Fi, VPN, or email profile.
- Assign the profile to user accounts and user groups. Android users are prompted to enter a password when they receive the profile (the password is displayed on the screen).

Create a user credential profile to use Entrust smart credentials on devices

Entrust derived smart credentials are supported by the following apps:

- BlackBerry Dynamics apps on iOS devices
- BlackBerry Dynamics apps on Android devices other than Samsung Knox Workspace devices
- Apps on Android Enterprise devices that use certificates for signing, encryption, and identity authentication, such as BlackBerry Hub and supported web browsers
- Apps on Samsung Knox Workspace devices that use certificates for signing, encryption, and identity authentication, such as the Samsung native email client and supported web browsers

Note: BlackBerry UEM doesn't support key history for derived smart credentials.

Before you begin:

- Connect BlackBerry UEM to your organization’s Entrust IdentityGuard server to use smart credentials.
- Create a CA certificate profile to send the Entrust CA certificate to devices and assign the profile to the same users or groups that this user credential profile will be assigned to.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select the Entrust smart credential connection that you configured.
6. In the **Certificate type** drop-down list, specify whether the smart credential will be used for identity authentication, signing, or encryption.

   If you want to send smart credentials to apps for more than one purpose, create additional user credential profiles.
7. If the smart credential will be sent to Samsung Knox Workspace devices or apps other than BlackBerry Dynamics apps on Android Enterprise devices, click the **Android** tab and select **Deliver to native key chain**.

   If this setting is not selected, the smart credential can be used only by BlackBerry Dynamics apps.
8. If the smart credential will be sent to BlackBerry Dynamics apps, click the **BlackBerry Dynamics** tab and perform the following actions:
   a) If you want the device to delete duplicate credentials, select **Delete duplicate certificates**. The device deletes the credential that has the earliest start date.
   b) If you want the device to delete expired credentials, select **Delete expired certificates**.

c) To allow all BlackBerry Dynamics apps to use the smart credentials, select **Allow all apps to use certificates**.

d) To specify the BlackBerry Dynamics apps to use the smart credentials, select **Allow specified apps to use certificates** and click + to specify the apps. You must include BlackBerry UEM Client in the list of apps.

9. Click **Add**.

After you finish:

- Assign the profile to user accounts and user groups.
- After a device receives the profile, users must log in to the Entrust IdentityGuard Self-Service Module to activate their smart credential and use the BlackBerry UEM Client to scan the QR code presented by the Entrust IdentityGuard Self-Service Module to add the smart credential to the device.
- To remove an Entrust smart credential from a device, the user should deactivate the smart credential in the BlackBerry UEM Client before you unassign the profile or remove the certificate.

Create a user credential profile to use certificates from the native keystore on Android devices

You can configure the user certificate profile to allow BlackBerry Dynamics apps to use a certificate from the native keystore on Android devices. You can allow BlackBerry Dynamics apps to use any certificate that had been added to the keystore or you can define restrictions on which certificate the app can choose. For example, if you are using an app-based PKI solution such as Purebred that adds certificates to the native keystore, you can force the app to select a certificate issued by your Purebred PKI solution and require that the app use certificates with specified capabilities.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select **Native keystore**.
6. To specify which certificate the BlackBerry Dynamics app will use, perform the following actions:

    a) Beside **Issuers**, click + and type the issuer name.

    BlackBerry Dynamics apps will only use a certificate if the specified issuer matches the OpenSSL short-form OID in the certificate. You can copy this value from the issuer's certificate. Do not put spaces before or after equal sign (=). For example:

    ```
    CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                              CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                              CN=Acme_cert TLS
    ```

    b) In the **Key usage** section, select the operations that the certificate supports.

    BlackBerry Dynamics apps will only use certificates that have at least the specified key usage value set. For example, an encryption certificate may have a key usage value of **Key encipherment**. An authentication certificate may have a key usage value of **Digital signature**. A signing certificate may have a key usage value of both **Digital signature** and **Nonrepudiation**.

    c) In the **Extended key usage** section, select the functions that the certificate was issued for.

    BlackBerry Dynamics apps will only use certificates if all selected extended key usage values are present in the certificate. Certificates can have additional extended key usage values.

    d) If the certificate was issued for purposes other than email, client authentication, or smart card login, select **Additional Object ID usage**, click + and specify the OID for the key usage. For example, if the certificate will be used for server authentication, it may have the OID 1.3.6.1.5.5.7.3.1

7. If you want the device to delete expired certificates, select **Delete expired certificates**.

Expired encryption certificates used for S/MIME should be retained on the device to allow users to read messages that were encrypted before the certificate expired.

8. If you want the device to delete duplicate certificates, select **Remove duplicate certificates**. The device deletes the certificate that has the earliest start date.
9. Click **Add**.

After you finish:

- Allow BlackBerry Dynamics apps to use certificates.
- Assign the profile to user accounts and user groups.

Create a user credential profile to connect to your BlackBerry Dynamics PKI connector

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select the BlackBerry Dynamics PKI connection that you configured.
6. If the user must provide a password to request a certificate, select **Require user-entered password or OTP**.
7. If you want to allow the device to automatically request a new certificate before the current certificate expires, select **Enable certificate renewal** and specify the number of days prior to expiry that devices request a new certificate.
8. If you want the device to delete expired certificates, select **Delete expired certificates**.
9. If you want the device to delete duplicate certificates, select **Remove duplicate certificates**. The device deletes the certificate that has the earliest start date.
10. Click **Add**.

After you finish:

- Allow BlackBerry Dynamics apps to use certificates.
- Assign the profile to user accounts and user groups.
- If you update the PKI connector, click **Refresh PKI capabilities** to update the supported PKI features for the profile.

Renew certificates that are enrolled through the BlackBerry Dynamics PKI connector

If you need to update user certificates for all BlackBerry Dynamics users, you can send a command to request certificate renewal to all devices that are assigned the user credential profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click the name of the profile that you want to change.
4. Click **Refresh PKI capabilities** to ensure that BlackBerry UEM has the most recent details for the PKI connector.
5. Click **Renew** to command all BlackBerry Dynamics enabled devices that are assigned the profile to request certificate renewal.

Creating user credential profiles for app-based certificates

App-based PKI solutions such as Purebred include an app installed on a device that communicates with a CA to enroll certificates and add them to the device. You can use an app-based PKI solution to provide certificates for use by BlackBerry Dynamics apps.

To use an app-based PKI solution with iOS devices, you must add a connection between BlackBerry UEM and the PKI provider. This task is not required to use an app-based PKI solution with only Android devices.

If the PKI app that retrieves certificates from the CA is not a BlackBerry Dynamics app, the BlackBerry UEM Client communicates with the PKI app to get the certificates and provide them to BlackBerry Dynamics apps.

If you send more than one certificate to devices using this method, it is recommended that you set up multiple user credential profiles with each profile using a different type of certificate. If you use a single profile instance for multiple certificates, there is no indication if any certificates are missing. For example, if a profile includes separate encryption, signing, and authentication certificates and only the signing and authentication certificates are imported, it appears on the device that the that the import was successful even though the encryption certificate is missing. However, if you set up three separate user credential profiles and the encryption certificate is missing, the issue is apparent.

Steps to use app-based certificates

Some of the steps required to use your organization's app-based PKI solution are necessary only if you use the solution with iOS devices.

Step	Action
1	To use an app-based PKI solution with iOS devices, in the BlackBerry Dynamics profile, select, **Enable UEM Client to enroll in BlackBerry Dynamics** and designate BlackBerry UEM Client for **App authentication delegation**.
2	To use an app-based PKI solution with iOS devices, connect BlackBerry UEM to your organization’s app-based PKI solution.
3	To use an app-based PKI solution with iOS devices, if the PKI app is not a BlackBerry Dynamics app, configure the BlackBerry UEM Client to support app-based certificates.
4	Configure BlackBerry Dynamics apps to use app-based certificates.
5	Ensure that the PKI app (for example, Purebred) is installed on users' devices.
6	To use the app-based PKI solution with iOS devices, create a user credential profile to use app-based certificates.
7	To use the app-based PKI solution with Android devices, create a user credential profile to use certificates from the native keystore.

Configure the BlackBerry UEM Client to support app-based certificates

This task is required only if you use your organization's app-based PKI solution with iOS devices and the PKI app is not a BlackBerry Dynamics app.

1. In the BlackBerry UEM management console, on the menu bar click **Apps**.
2. In the app list, select BlackBerry UEM Client.
3. In the App configuration section, click +.
4. In the **App name** field, type a name for the app.
5. In the **UTI schemes** field, specify the UTI schemes for your organization's app-based PKI solution. For example, if you are using the Purebred app use the following schemes: purebred.zip.all, purebred.zip.no_filter.
6. Click **Save**.
7. Assign the BlackBerry UEM Client with the app configuration that you created to the users and devices you want to use the app-based PKI solution.

Configure BlackBerry Dynamics apps to use app-based certificates

BlackBerry Dynamics apps automatically select which certificate to use for S/MIME and for authentication over TLS connections based on the key usage and extended key usage properties in the certificates. If two or more certificates have same set of properties, apps may not be able to resolve which certificate to use for TLS authentication. You can help apps determine which certificate to use by following the steps below.

1. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
2. In the app list, select the app (for example, BlackBerry Work or BlackBerry Access).
3. Select the **Allow BlackBerry Dynamics apps to use user certificates and user credential profiles** option.
4. If you are configuring BlackBerry Work, in the App configuration section, click + and perform one of the following tasks:

Task	Steps
Configure BlackBerry Work when your organization is using BEMS	**a.** On the Configuration Settings tab, select **Clients must have individual login certificates (SSL) uploaded in the GC**. **b.** To enable automatic discovery of the Microsoft Exchange server that the users are on, select **Use BEMS to perform Autodiscover of the EAS/EWS endpoint for the user**. **c.** On the **Exchange Settings** tab, in the **User Credential Profile Name** field, type the name of the user credential profile.
Configure BlackBerry Work when your organization is not using BEMS	**a.** Select the **Exchange Settings** tab. **b.** If your server uses the *domain name\user* login format, in the **Default Domain** field, specify the default Windows NT Domain that BlackBerry Work connects to when users log in. **c.** In the **Active Sync Server** field, specify the default Exchange ActiveSync server that BlackBerry Work connects to when users log in to BlackBerry Work (for example, cas.mydomain.com). **d.** In the **Auto Discover URL** field, specify the auto discover URL if known. This speeds up the autodiscover setup process (for example, https://autodiscover.mydomain.com). **e.** In the **Auto Discover Connection Timeout in Seconds (iOS only)** field, specify the autodiscover connection timeout in seconds. **f.** In the **User Credential Profile Name** field, type the name of the user credential profile.

5. Click **Save**.

Create a user credential profile to use app-based certificates on iOS devices

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > User credential**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, select the name of the app you specified when you connected BlackBerry UEM to your PKI solution. If you are using Purebred, select the BlackBerry UEM Client
6. To specify which certificate the BlackBerry Dynamics app will use, perform the following actions:
   a) In the **Key usage** section, select the operations that the certificate supports.

      BlackBerry Dynamics apps will only use certificates that have at least the specified key usage value set. For example, an encryption certificate may have a key usage value of **Key encipherment**. An authentication certificate may have a key usage value of **Digital signature**. A signing certificate may have a key usage value of both **Digital signature** and **Nonrepudiation**.

   b) In the **Extended key usage** section, select the functions that the certificate was issued for.

      BlackBerry Dynamics apps will only use certificates if all selected extended key usage values are present in the certificate. Certificates can have additional extended key usage values.

   c) If the certificate was issued for purposes other than email, client authentication, or smart card login, select **Additional Object ID usage**, click + and specify the OID for the key usage. For example, if the certificate will be used for server authentication, it may have the OID 1.3.6.1.5.5.7.3.1

   d) Beside **Issuers**, click + and type the issuer name.

      BlackBerry Dynamics apps will only use a certificate if the specified issuer matches the OpenSSL short-form OID in the certificate. You can copy this value from the issuer's certificate. Do not put spaces before or after the equal sign (=). For example:

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                            CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                            CN=Acme_cert TLS
      ```

7. If you want the device to delete expired certificates, select **Delete expired certificates**.

   Expired encryption certificates used for S/MIME should be retained on the device to allow users to read messages that were encrypted before the certificate expired.

8. If you want the device to delete duplicate certificates, select **Remove duplicate certificates**. The device deletes the certificate that has the earliest start date.
9. Click **Add**.

After you finish:

- Allow BlackBerry Dynamics apps to use certificates.
- Assign the profile to user accounts and user groups.

Sending client certificates to devices and apps using SCEP

You can use SCEP profiles to specify how devices and BlackBerry Dynamics apps obtain client certificates from your organization's CA through a SCEP service. SCEP is an IETF protocol that simplifies the process of enrolling client certificates to a large number of devices or apps without any administrator input or approval required to issue each certificate. Devices and BlackBerry Dynamics apps can use SCEP to request and obtain client certificates from a SCEP-compliant CA that is used by your organization.

The CA that you use must support challenge passwords. The CA uses challenge passwords to verify that the device or app is authorized to submit a certificate request.

To use SCEP in a BlackBerry UEM Cloud environment, you must install the most recent version of the BlackBerry Connectivity Node to allow BlackBerry UEM Cloud to access your company directory.

If your organization uses an Entrust CA or OpenTrust CA, SCEP profiles are not supported for Windows 10 devices.

Create a SCEP profile

The required profile settings depend on the SCEP service configuration in your organization's environment and vary depending on whether the certificate is used by a BlackBerry Dynamics app or by a specified device type.

You can use a variable in any text field to reference a value instead of specifying the actual value.

Note: If you want to use a SCEP profile to distribute OpenTrust client certificates to devices, you must apply a hotfix to your OpenTrust software. For more information, contact your OpenTrust support representative and reference support case SUPPORT-798.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > SCEP**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **Certificate authority connection** drop-down list, perform one of the following actions:
    - To use an Entrust connection that you configured, click the appropriate connection. In the **Profile** drop-down list, click a profile. Specify the values for the profile.
    - To use an OpenTrust connection that you configured, click the appropriate connection. In the **Profile** drop-down list, click a profile. Specify the values for the profile.
        - The following settings in the SCEP profile do not apply to OpenTrust client certificates: Key usage, Extended key usage, Subject, and SAN.
    - To use another CA, click **Generic**. In the **SCEP challenge type** drop-down list, select **Static** or **Dynamic** and specify the required settings for the challenge type.

    Note: For Windows devices, only static passwords are supported.
6. In the **URL** field, type the URL for the SCEP service. The URL should include the protocol, FQDN, port number, and SCEP path.
7. In the **Instance name** field, type the instance name for the CA.
8. Optionally, clear the check box for any device type that you do not want to configure the profile for.
9. Perform the following actions:
    a) Click the tab for a device type.
    b) Configure the appropriate values for each profile setting to match the SCEP service configuration in your organization's environment.
10. Repeat step 8 for each device type in your organization.
11. Click **Add**.

After you finish: If devices use the client certificate to authenticate with a work Wi-Fi network, work VPN, or work mail server, associate the SCEP profile with a Wi-Fi, VPN, or email profile.

SCEP profile settings

SCEP profiles are supported on the following device types:

- iOS

- macOS
- Android
- Windows 10
- BlackBerry 10

Common: SCEP profile settings

Common: SCEP profile setting	Description
Certificate authority connection	This setting specifies whether the CA is Entrust, OpenTrust, or another CA. If you configured one or more connections to your organization's Entrust software or OpenTrust software, you can select one of the connections in the drop-down list. Select Generic if you are using any other CA. If you select an Entrust or OpenTrust connection, you must then select the appropriate PKI profile and specify the necessary values. The available profiles vary based on what the Entrust or OpenTrust administrator has configured in the PKI software. The default value is Generic.
URL	This setting specifies the URL of the SCEP service. The URL should include the protocol, FQDN, port number, and SCEP path (CGI path that is defined in the SCEP specification). You must set a value for this setting to activate a device successfully. SCEP HTTPS URLs are supported by iOS devices and BlackBerry 10 OS version 10.3.0 and later.
Instance name	This setting specifies the name of the CA instance. The value can be any string that is understood by the SCEP service. For example, it could be a domain name like example.org. If a CA has multiple CA certificates, this field can be used to distinguish which one is required.
Verify SCEP server connection trust chain	This setting specifies whether BlackBerry UEM verifies that the root CA of the SCEP server is stored in the BlackBerry UEM certificate store to allow BlackBerry UEM to trust the SCEP server when testing connections, retrieving challenge passwords, and acting as a proxy for SCEP requests from devices.
SCEP challenge type	This setting specifies whether the SCEP challenge password is dynamically generated or provided as a static password. If this setting is set to "Static," every device uses the same challenge password. If this setting is set to "Dynamic," every device receives a unique challenge password. Possible values: • Static • Dynamic The default value is Dynamic. For Windows devices, only "Static" passwords are supported.

Common: SCEP profile setting	Description
Challenge password generation URL	This setting specifies the URL that devices use to obtain a dynamically generated challenge password from the SCEP service. The URL should include the protocol, domain, port, and SCEP path (CGI path that is defined in the SCEP specification). If you use a dynamic challenge password, you must set a value to activate BlackBerry 10 devices successfully. This setting is valid only if the "SCEP challenge type" setting is set to "Dynamic."
Authentication type	This setting specifies the authentication type devices use to connect to the SCEP service and obtain a challenge password. This setting is valid only if the "SCEP challenge type" setting is set to "Dynamic." Possible values: • Basic • NTLM The default value is Basic.
Domain	This setting specifies the domain used for NTLM authentication when devices connect to the SCEP service to obtain a challenge password. This setting is valid only if the "Authentication type" setting is set to "NTLM."
Username	This setting specifies the username required to obtain a challenge password from the SCEP service. This setting is valid only if the "SCEP challenge type" setting is set to "Dynamic."
Password	This setting specifies the password required to obtain the challenge password from the SCEP service. This setting is valid only if the "SCEP challenge type" setting is set to "Dynamic."
Challenge password	This setting specifies the challenge password that a device uses for certificate enrollment. If you use a static challenge password, you must set a value for this setting to activate BlackBerry 10 devices successfully. This setting is valid only if the "SCEP challenge type" setting is set to "Static."

iOS: SCEP profile settings

iOS: SCEP profile setting	Description
Use BlackBerry UEM as a proxy for SCEP requests	This setting specifies whether all SCEP requests from devices are sent through BlackBerry UEM. If the CA is behind your firewall, this setting allows you to enroll client certificates to devices without exposing the CA outside of the firewall.
Use BlackBerry Connectivity Node for CA connectivity	This setting specifies whether SCEP requests should be routed through the BlackBerry Connectivity Node. This setting displays only in BlackBerry UEM Cloud.

iOS: SCEP profile setting	Description
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*/O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.
Retries	This setting specifies how many times to retry connecting to the SCEP service if the connection attempt fails. The possible values are from 1 to 999. The default value is "3."
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service. The possible values are from 1 to 999. The default value is "10" seconds.
Key size	This setting specifies the key size for the certificate. Possible values: • 1024 • 2048 The default value is 1024.
Fingerprint	This setting specifies the fingerprint for enrolling a SCEP certificate. If your CA uses HTTP instead of HTTPS, devices use the fingerprint to confirm the identity of the CA during the enrollment process. The fingerprint can't contain spaces.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • None • RFC822 name • DNS name • Uniform Resource Identifier The default value is "None."
SAN value	This setting specifies the alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, or the fully qualified URL of the server. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.

iOS: SCEP profile setting	Description
NT principal name	This setting specifies the NT principal name for certificate generation. This setting is valid only if the "SAN type" setting is set to something other than "None."
Profile expiration	Specify the number of days after a certificate is issued that the device requests a new certificate from the CA. The value should be less than the certificate validity period defined by the CA. The maximum value is 1825 days.

macOS: SCEP profile settings

macOS applies profiles to user accounts or devices. You can configure SCEP profiles to apply to one or the other.

macOS: SCEP profile setting	Description
Use BlackBerry UEM as a proxy for SCEP requests	This setting specifies whether all SCEP requests from devices are sent through BlackBerry UEM. If the CA is behind your firewall, this setting allows you to enroll client certificates to devices without exposing the CA outside of the firewall.
Use BlackBerry Connectivity Node for CA connectivity	This setting specifies whether SCEP requests should be routed through the BlackBerry Connectivity Node. This setting displays only in BlackBerry UEM Cloud.
Apply profile to	This setting specifies whether the SCEP profile is applied to the user account or the device. Possible values: • User • Device
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*/O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.
Retries	This setting specifies how many times to retry connecting to the SCEP service if the connection attempt fails. The possible values are from 1 to 999. The default value is "3."
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service. The possible values are from 1 to 999. The default value is "10" seconds.

macOS: SCEP profile setting	Description
Key size	This setting specifies the key size for the certificate. Possible values: - 1024 - 2048 The default value is "1024."
Fingerprint	This setting specifies the fingerprint for enrolling a SCEP certificate. If your CA uses HTTP instead of HTTPS, devices use the fingerprint to confirm the identity of the CA during the enrollment process. The fingerprint can't contain spaces.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: - None - RFC822 name - DNS name - Uniform Resource Identifier The default value is "None."
SAN value	This setting specifies the alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, or the fully qualified URL of the server. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.
NT principal name	This setting specifies the NT principal name for certificate generation. This setting is valid only if the "SAN type" setting is set to something other than "None."

Android: SCEP profile settings

To see an example of a SCEP profile for Android devices, visit support.blackberry.com/community to read article 38248.

Android: SCEP profile setting	Description
Use BlackBerry UEM as a proxy for SCEP requests	This setting specifies whether all SCEP requests from devices are sent through BlackBerry UEM. If the CA is behind your firewall, this setting allows you to enroll client certificates to devices without exposing the CA outside of the firewall.

Android: SCEP profile setting	**Description**
Hide certificate on Android Enterprise devices	This setting specifies whether the certificate is visible to users on Android 9.0 and later Android Enterprise. If the certificate is hidden, users can't select the certificate to use it for additional purposes.
Use BlackBerry Connectivity Node for CA connectivity	This setting specifies whether SCEP requests should be routed through the BlackBerry Connectivity Node. This setting displays only in BlackBerry UEM Cloud.
Encryption algorithm	This setting specifies the encryption algorithm that Android devices use for the certificate enrollment request. Possible values: • None • Triple DES • AES (128-bit) • AES (196-bit) • AES (256-bit) The default value is "Triple DES."
Hash function	This setting specifies the hash function that Android devices use for the certificate enrollment request. Possible values: • None • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 The default value is "SHA-1."
Certificate thumbprint	This setting specifies the hexadecimal-encoded hash of the root certificate for the CA. You can use the following algorithms to specify the thumbprint: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. You must set a value for this setting to activate Android Enterprise or Samsung Knox devices.
Automatic renewal	This setting specifies how many days before a certificate expires that automatic certificate renewal occurs. The possible values are 1 to 365. The default value is "30."
Android Enterprise / Samsung KNOX	

Android: SCEP profile setting	Description
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*/O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • RFC 822 name • Uniform resource identifier • NT principal name • DNS name The default value is "RFC 822 name."
SAN value	This setting specifies the subject alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, the fully qualified URL of the server, or principal name. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.
Key algorithm	This setting specifies the algorithm that Android Enterprise and Samsung Knox devices use to generate the client key pair. You must select an algorithm that is supported by your CA. Possible values: • None • RSA • ECC The default value is "RSA."
RSA strength	This setting specifies the RSA strength that Android Enterprise and Samsung Knox devices use to generate the client key pair. You must enter a key strength that is supported by your CA. This setting is valid only if the "Key algorithm" setting is set to "RSA.". Possible values: • 1024 • 2048 • 4096 • 8192 • 16384 The default value is "1024."

Android: SCEP profile setting	Description
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate. Possible selections: • Digital signature • Non-repudiation • Key encipherment • Data encipherment • Key agreement • Key certificate signing • CRL signing • Encipher only • Decipher only The default selections are "Digital signature," "Key encipherment," and "Key agreement."
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate. Possible selections: • Server authentication • Client authentication • Code signing • Email protection • Time stamping • OCSP signing • Secure shell client • Secure shell server The default selection is "Client authentication."

Windows 10: SCEP profile settings

Windows 10: SCEP profile setting	Description
User certificate store	This setting specifies whether the certificate is stored in the user certificates location on the device.
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*/O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.

Windows 10: SCEP profile setting	Description
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • None • RFC 822 name • DNS name • Uniform resource identifier The default value is "None."
SAN value	This setting specifies the alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, or the fully qualified URL of the server. The appropriate value for this setting depends on the value selected for the "SAN type" setting.
Retries	This setting specifies how many times to retry connecting to the SCEP service if the connection attempt fails. The possible values are 1 to 999. The default value is "3."
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service. The possible values are 1 to 999. The default value is "10" seconds.
Key size	This setting specifies the key size for the certificate. Possible values: • 1024 • 2048 • 4096 • 8192 • 16384 The default value is "1024."

Windows 10: SCEP profile setting	Description
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate. • Digital signature • Non-repudiation • Key encipherment • Data encipherment • Key agreement • Key certificate signing • CRL signing • Encipher only The default selections are "Key certificate signing" and "Encipher only."
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate. • Server authentication • Client authentication • Code signing • Email protection • Time stamping • OCSP signing • Secure shell client • Secure shell server The default selection is "Client authentication."
SCEP key storage	This setting specifies the storage location for the private key. Possible values: • TPM • TPM if supported • KSP The default value is "KSP."
Hash function	This setting specifies the hash function that a Windows 10 device uses for the certificate enrollment request. Possible values: • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 The default value is "SHA-1."

Windows 10: SCEP profile setting	Description
Certificate thumbprint	This setting specifies the hexadecimal-encoded hash of the root certificate for the CA. You can use the following algorithms to specify the thumbprint: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.
Automatic renewal	This setting specifies how many days before a certificate expires that automatic certificate renewal occurs. The possible values are 1 to 365. The default value is "30."

BlackBerry 10: SCEP profile settings

BlackBerry 10: SCEP profile setting	Description
Use device default subject and SAN	This setting specifies whether a BlackBerry 10 device generates the subject and subject alternative name for a certificate request. If this setting is not selected, you must specify the subject and subject alternative name type and value.
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*/O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%. This setting is valid only if the "Use device default subject and SAN" setting is not selected. The minimum requirement is BlackBerry 10 OS version 10.3.1.
SAN	This setting specifies the subject alternative name type and value for a certificate. This setting is valid only if the "Use device default subject and SAN" setting is not selected. The minimum requirement is BlackBerry 10 OS version 10.3.1.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • RFC 822 name • URI • NT principal name • DNS name The default value is "RFC 822 name."

BlackBerry 10: SCEP profile setting	Description
SAN value	This setting specifies the subject alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, the fully qualified URL of the server, or principal name. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.
Key algorithm	This setting specifies the algorithm that a BlackBerry 10 device uses to generate the client key pair. You must select an algorithm that is supported by your CA. Possible values: • None • RSA • ECC The default value is "RSA."
RSA strength	This setting specifies the RSA strength that a BlackBerry 10 device uses to generate the client key pair. You must enter a key strength that is supported by your CA. This setting is valid only if the "Key algorithm" setting is set to "RSA." Possible values: • 1024 • 2048 • 4096 • 8192 • 16384 The default value is "1024."
ECC strength	This setting specifies the elliptic curve that a BlackBerry 10 device uses to generate a client key pair. The elliptic curve defines the strength of the client key pair. You must select an elliptic curve that is supported by your CA. This setting is valid only if the "Key algorithm" setting is set to "ECC." Possible values: • sect163k1 • sect283k1 • secp192r1 • secp256r1 • secp384r1 • secp521r1 The default value is "secp521r1."

BlackBerry 10: SCEP profile setting	Description
Encryption algorithm	This setting specifies the encryption algorithm that a BlackBerry 10 device uses for the certificate enrollment request. Possible values: • None • Triple DES • AES (128-bit) • AES (196-bit) • AES (256-bit) The default value is "Triple DES."
Hash function	This setting specifies the hash function that a BlackBerry 10 device uses for the certificate enrollment request. Possible values: • None • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 The default value is "SHA-1."
Certificate thumbprint	This setting specifies the hexadecimal-encoded hash of the root certificate for the CA. You can use the following algorithms to specify the thumbprint: MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. You must set a value for this setting to activate a BlackBerry 10 device successfully.
Automatic renewal	This setting specifies how many days before a certificate expires that automatic certificate renewal occurs. The possible values are from 1 to 999,999,999 days. The default value is "30."

BlackBerry 10: SCEP profile setting	Description
Key usage	This setting specifies the cryptographic operations that can be performed using the public key contained in the certificate. Possible selections: • Digital signature • Non-repudiation • Key encipherment • Data encipherment • Key agreement • Key certificate signing • CRL signing • Encipher only • Decipher only The default selections are "Digital signature," "Key encipherment," and "Key agreement." The minimum requirement is BlackBerry 10 OS version 10.3.1.
Extended key usage	This setting specifies the purpose of the key contained in the certificate. Possible selections: • Server authentication • Client authentication • Code signing • Email protection • Time stamping • OCSP signing • Secure shell client • Secure shell server The default selection is "Client authentication." The minimum requirement is BlackBerry 10 OS version 10.3.1.

BlackBerry Dynamics: SCEP profile settings

These settings apply to SCEP certificates used with BlackBerry Dynamics apps on iOS and Android devices.

BlackBerry Dynamics: SCEP profile setting	Description
Subject	This setting specifies the subject for the certificate, if required for your organization's SCEP configuration. Type the subject in the format "/CN=*<common_name>*,O=*<domain_name>*" If the profile is for multiple users, you can use a variable, for example: %UserDistinguishedName%.

BlackBerry Dynamics: SCEP profile setting	**Description**
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required. Possible values: • RFC 822 name • Uniform resource identifier • NT principal name • DNS name The default value is "RFC 822 name."
SAN value	This setting specifies the subject alternative representation of the certificate subject. The value must be an email address, the DNS name of the CA server, the fully qualified URL of the server, or principal name. The "SAN type" setting determines the appropriate value to specify. If set to "RFC822 name," the value must be a valid email address. If set to "URI," the value must be a valid URL that includes the protocol and FQDN or IP address. If set to "NT principal name," the value must be a valid principal name. If set to "DNS name," the value must be a valid FQDN.
Key algorithm	This setting specifies the algorithm used to generate the client key pair. You must select an algorithm that is supported by your CA. Possible values: • RSA
RSA strength	This setting specifies the RSA strength used to generate the client key pair. You must enter a key strength that is supported by your CA. This setting is valid only if the "Key algorithm" setting is set to "RSA.". Possible values: • 2048 • 4096 The default value is "2048."
Encryption algorithm	This setting specifies the encryption algorithm used for the certificate enrollment request. Possible values: • Triple DES • AES (128-bit) • AES (196-bit) • AES (256-bit) The default value is "Triple DES."

BlackBerry Dynamics: SCEP profile setting	Description
Hash function	This setting specifies the hash function used for the certificate enrollment request. Possible values: • SHA-256 • SHA-384 • SHA-512 The default value is "SHA-256."
Certificate thumbprint	This setting specifies the hexadecimal-encoded hash of the root certificate for the CA. You can use one of the following algorithms to specify the thumbprint: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. MD5 is supported only if "Enable FIPS" is not selected in the BlackBerry Dynamics profile.
Automatic renewal	This setting specifies how many days before a certificate expires that automatic certificate renewal occurs. The possible values are 1 to 365. The default value is "30."
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate. Possible selections: • Digital signature • Non-repudiation • Key encipherment • Data encipherment • Key agreement • Key certificate signing • CRL signing • Encipher only • Decipher only The default selections are "Digital signature," "Key encipherment," and "Key agreement."

BlackBerry Dynamics: SCEP profile setting	Description
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate. Possible selections: • Server authentication • Client authentication • Code signing • Email protection • Time stamping • OCSP signing • Secure shell client • Secure shell server The default selection is "Client authentication."
App restrictions	This setting specifies which BlackBerry Dynamics apps can use the certificate. Possible values: • Allow all apps to use certificates • Allow specified apps to use certificates The default selection is "Allow all apps to use certificates."
Apps allowed to use SCEP	This setting specifies the BlackBerry Dynamics apps that are allowed to use SCEP certificates. This setting is valid only if the "App restrictions" setting is set to "Allow specified apps to use certificates."
Delete expired certificates	This setting specifies whether the device deletes expired certificates.
Remove duplicate certificates	This setting specifies whether the device deletes duplicate certificates. The device deletes the certificate that has the earliest start date.

Sending the same client certificate to multiple devices

You can use shared certificate profiles to send client certificates to iOS, macOS, and Android devices.

Shared certificate profiles send the same key pair to every user who is assigned the profile. You should use shared certificate profiles only if you want to allow more than one user to share a client certificate.

macOS applies profiles to user accounts or devices. You can configure a shared certificate profile to apply to one or the other.

Create a shared certificate profile

Before you begin: You must obtain the client certificate file that you want to send to devices. The certificate file must have a .pfx or .p12 file name extension.

1. On the menu bar, click **Policies and Profiles**.

2. Click **Certificates > Shared certificate**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name. Some names (for example, ca_1) are reserved.
5. In the **Password** field, type a password for the shared certificate profile.
6. In the **Certificate file** field, click **Browse** to locate the certificate file.
7. If you are managing Android Enterprise devices and you want to prevent users from selecting the certificate to use for other purposes, on the **Android** tab, select **Hide certificate on Android Enterprise devices**. This option applies only to Android 9.0 and later.
8. If you are managing macOS devices, on the **macOS** tab, in the **Apply profile to** drop-down list, select **User** or **Device**.
9. Click **Add**.

Specify the certificate used by an app

For Android devices, you can use a certificate mapping profile to specify the client certificates that apps use. The certificate mapping profile is not supported for BlackBerry Dynamics apps.

Certificate mapping profiles allow you to specify the certificates that Android apps use. You can require an app to use a certificate sent to the device by a SCEP, user credential, or shared certificate profile. You can use a certificate with one or more specified apps or all managed apps. You can also specify whether an app uses a certificate any time that one is required, or only for connections to a specific URI.

Multiple certificate mappings can be specified in a single profile. Only one certificate mapping profile can be assigned to a user.

Create a certificate mapping profile

Before you begin: Create any SCEP, user credential, or shared certificate profiles required to send certificates to devices and assign the profiles to users or groups.

1. On the menu bar, click **Policies and Profiles**.
2. Click Certificates > Certificate mapping.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the mapping table, click +.
6. Under **Destination URI**, select one of the following options:
   - Select **None** if the app won't use the certificate to authenticate a connection with a resource.
   - Select **Any** if the app can use the certificate to authenticate a connection with any resource.
   - Select **Specified host:port** and type the host and port if the app can use the certificate to authenticate with a specific resource.
7. Under **App certificate**, perform one of the following actions:
   - To specify that the app must use a certificate sent to the device by another profile, select **Selected certificate** and select the profile name from the drop-down list.
   - To specify that the app must use a certificate sent to the device by a third-party source, select **Certificate alias** and type the alias for the certificate. If you do not know the alias, consult the documentation or administrator for the certificate provider.

- To specify that the app must use a certificate sent to the device by another profile, select **Selected certificate** and select the profile name from the drop-down list.

8. Under **Allowed apps for destination URI**, perform one of the following actions:
    - To allow any managed app to request the specified certificate, select **Any apps in workspace**.
    - To allow only specified apps to request the certificate, select **Specified apps** and click + to specify one or more apps.
9. If necessary, repeat steps 5 to 8 to add to additional mappings to the profile.
10. Click **Add**.

After you finish:

- Assign the profile to user accounts and user groups.
- If necessary, rank profiles.

Managing client certificates for user accounts

You can add client certificates directly to individual user accounts or to a user credential profile assigned to the user account. Adding certificates directly to a user account is supported for BlackBerry Dynamics enabled devices or other managed iOS and Android devices. Uploading certificates to user credential profiles is supported for devices running BlackBerry 10 OS version 10.3.1 and later, iOS devices, and Android Enterprise devices.

To allow users to upload certificates that they can use to connect to your work Wi-Fi network, work VPN, and work mail server, use a user credential profile, which can be associated with a Wi-Fi, VPN, or email profile

If you have an on-premises environment and you upload certificates for BlackBerry Dynamics apps to user accounts, you should configure a time to live for user certificates. When the time to live ends, the certificates are deleted from the server.

Add a client certificate to a user account

You can add a client certificate to an individual user account and send the certificate to BlackBerry Dynamics enabled devices or other managed iOS and Android devices.

Add client certificates to user accounts when users devices need certificates for S/MIME or client authentication and the certificate can't be sent to devices via a user credential profile or SCEP profile.

The client certificate must have a .pfx or .p12 file name extension. You can send more than one client certificate to devices.

You can also use user credential profiles to upload certificates for individual users. User credential profiles can be associated with a Wi-Fi, VPN, or email profile.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **IT policy and profiles** section, click +.
5. Click **User certificate**.
6. Type a description for the certificate.
7. In the **Apply certificate to** section, select one of the following:
    - **Other managed devices**: Choose this option to send the certificate to iOS and Android devices for all supported uses other than for BlackBerry Dynamics apps.
    - **BlackBerry Dynamics enabled devices**: Choose this option to send the certificate to devices to use with BlackBerry Dynamics apps.
8. In the **Certificate file** field, click **Browse** to locate the certificate file.
9. If you selected **Other managed devices**, in the **Password** field, type a password for the certificate. For iOS devices, a password is required. For Android devices, you do not have to provide a password in BlackBerry UEM if the device is running the latest version of BlackBerry UEM Client. If you don't set a password, the user must enter the device password.
10. Click **Add**. The certificate is listed in the **User certificates** table on the user summary page.

After you finish:

- For BlackBerry Dynamics enabled devices, configure the length of time uploaded certificates remain on the BlackBerry UEM server before they are automatically deleted from the server. The default setting is 24 hours.

Change a client certificate for a user account

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **IT policy and profiles** section, click the user certificate that you want to change.
5. Click ✎.
6. Make the necessary changes. You can't change which devices the certificate applies to.
7. Click **Save**.

After you finish: If you change a BlackBerry Dynamics user certificate that you or a user has removed from a device, the certificate is resent to the device.

Renew or remove a BlackBerry Dynamics certificate for a user account

You can send a command to a user's device to request certificate renewal from the CA. You can also remove a BlackBerry Dynamics certificate from a user's device. If you remove a certificate, the BlackBerry Dynamics PKI connector sends a notification to the CA that the certificate is no longer in use, but the certificate is not automatically revoked.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **User certificates** section, perform one of the following actions:

    - Click ⟳ to request certificate renewal from the CA.
    - Click ✕ to remove the certificate from the user's devices.

    Note: To remove an Entrust smart credential from a device, the user must also deactivate the smart credential in the BlackBerry UEM Client.

Add a client certificate to a user credential profile

You can upload certificates for individual users to a user credential profile. Users can also upload their certificate to the user credential profile using BlackBerry UEM Self-Service. Uploading certificates to user credential profiles is supported for devices running BlackBerry 10 OS version 10.3.1 and later, iOS devices, and for Android Enterprise devices.

The client certificate must have a .pfx or .p12 file name extension. If you or a user uploads a new certificate to the user credential profile, it replaces the existing certificate on the users devices.

Before you begin:

- Create a user credential profile to manually upload certificates.
- Assign the user credential profile to users.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.

3. In the search results, click the name of a user account.
4. In the **IT policy and profiles** section, beside the user credential profile, click **Add a certificate**.
5. Click **Browse** to locate the certificate file.
6. Type the password for the certificate. For iOS devices, the password is required. For Android devices, you do not have to provide the password in BlackBerry UEM if the device is running the latest version of BlackBerry UEM Client. If you don't specify the password, the user must enter the device password.
7. Click **Add**.

Change a client certificate for a user credential profile

You can change the certificate that you or a user has added to a user credential profile. The new certificate replaces the existing certificate on the device.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **IT policy and profiles** section, in the row for the user credential profile, click **Update**.
5. Click **Browse** to locate the certificate file.
6. Type a password for the certificate. For iOS devices, a password is required. For Android devices, you do not have to provide the password in BlackBerry UEM if the device is running the latest version of BlackBerry UEM Client. If you don't specify the password, the user must enter the device password.
7. Click **Save**.

Configure a time to live for client certificates

If you upload certificates to individual user accounts for BlackBerry Dynamics apps, you should configure a time to live for client certificates. When the time to live ends, the certificates are deleted from the server. This prevents a client certificate from remaining on the server for a long time after it has been pushed to the device. The default time to live is 24 hours.

This feature is not supported in BlackBerry UEM Cloud.

1. On the menu bar, click **Settings > General settings > Certificates**.
2. Specify the time to live for PKCS#12 certificates on the server.

After you finish: If you have not already done so, add client certificates to user accounts.

Legal notice

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada