BlackBerry UEM

Managing secure connections

Administration

12.23

Contents

Managing secure connections with BlackBerry UEM

The following table summarizes the administration tasks that are covered in this guide. Review to determine which tasks you should complete based on your organization's needs.

Task	Description
Create a Wi-Fi profile	You can create a Wi-Fi profile to specify how devices connect to a work Wi-Fi network.
Create a VPN profile	You can create a VPN profile to specify how devices connect to a work VPN.
Create a per-app VPN profile	You can specify which apps on devices must use a VPN for their data in transit.
Create a proxy profile	You can specify how devices use a proxy server to access web services on the Internet or on a work network.
Create an enterprise connectivity profile	You can specify how devices connect to your organization’s resources using enterprise connectivity and BlackBerry Secure Connect Plus to provide a secure IP tunnel between apps and your organization's network.
Create a BlackBerry 2FA profile	You can enable two-factor authentication for users and specify the configuration of preauthentication and self-rescue features.
Create a single sign-on extension profile or single sign-on profile	You can enable iOS and iPadOS devices to authenticate automatically with domains and web services in your organization's network.
Create a BlackBerry Dynamics connectivity profile	You can define the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps. For more information, see Setting up network connections for BlackBerry Dynamics apps in the Administration content.
Create a DNS profile	You can specify the DNS servers that you want iOS and macOS devices to use to access specified domains.
Create an email profile	You can specify how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler. For more information, see Creating email profiles in the Administration content.
Create an IMAP/POP3 email profile	You can specify how devices connect to an IMAP or POP3 mail server and synchronize email messages. For more information, see Create an IMAP/POP3 email profile in the Administration content.
Create a network usage profile	You can manage network mobile network usage for iOS and iPadOS apps.
Create a web content filter profile	You can limit the websites that a user can view in Safari or other browsers on a supervised iOS or iPadOS device.
Create an AirPrint profile	You can help users find printers.

Task	Description
Create an AirPlay profile	You can specify which AirPlay devices iOS and iPadOS users can connect to.
Create an Access Point Name profile	You can specify the information Android devices need to communicate with the carrier's network.
Connect the UEM to your organization's PKI software	You can extend the certificate-based authentication provided by your PKI services to the devices and apps that you manage with UEM. For example, you can • Connect BlackBerry UEM to your organization’s Entrust software • Connect BlackBerry UEM to your organization’s Entrust IdentityGuard server to use smart credentials • Connect BlackBerry UEM to your organization's OpenTrust software • Connect BlackBerry UEM to a BlackBerry Dynamics PKI connector • Connect BlackBerry UEM to your organization’s app-based PKI solution
Send certificates to devices and apps using profiles	You can send certificates to devices and apps using UEM profiles.
Manage 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.

Managing work connections using profiles

You can use profiles to set up and manage work connections for devices in your organization. Work connections define how devices connect to work resources in your organization's environment, such as mail servers, proxy servers, Wi-Fi networks, and VPNs. You can specify settings for iOS, macOS, Android, and Windows 10 devices in the same profile and then assign the profile to user accounts, user groups, or device groups.

Some work connection profiles can include one or more associated profiles. When you specify an associated profile, you link an existing profile to a work connection profile, and devices must use the associated profile when they use the work connection profile. For example, you can associate certificate profiles and proxy profiles with various work connection profiles. You should create profiles in the following order:

1. Certificate profiles
2. Proxy profiles
3. Work connection profiles such as email, VPN, and Wi-Fi

For example, if you create a Wi-Fi profile first, you cannot associate a proxy profile with the Wi-Fi profile when you create it. After you create a proxy profile, you must change the Wi-Fi profile to associate the proxy profile with it.

Setting up work Wi-Fi networks for devices

You can use a Wi-Fi profile to specify how devices connect to a work Wi-Fi network behind the firewall. You can assign a Wi-Fi profile to user accounts, user groups, or device groups.

By default, both work and personal apps can use Wi-Fi profiles to connect to your organization's network.

Create a Wi-Fi profile

The required profile settings vary for each device type and depend on the Wi-Fi security type and authentication protocol that you select. You can use a variable in any profile setting that is a text field to reference a value instead of specifying the actual value.

Before you begin:

- If devices use certificate-based authentication for work Wi-Fi connections, create a CA certificate profile and assign it to user accounts, user groups, or device groups. To send client certificates to devices, create a SCEP, shared certificate, or user credential profile to associate with the Wi-Fi profile.
- For iOS, iPadOS, macOS, and Android Enterprise devices that use a proxy server for work Wi-Fi connections, create a proxy profile to associate with the Wi-Fi profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > Wi-Fi**.
3. Click +.
4. Type a name and description for the Wi-Fi profile. This information is displayed on devices.
5. In the **SSID** field, type the network name of a Wi-Fi network.
6. If the Wi-Fi network does not broadcast the SSID, select the **Hidden network** check box.
7. Click the tab for a device type to configure the appropriate settings. For more information, see the Wi-Fi profile settings for iOS and macOS, Android, and Windows.

   If your organization requires that users provide a username and password to connect to the Wi-Fi network, in the **Username** field, type `%UserName%`.
8. Repeat step 7 for each device type.
9. Click **Add**.

After you finish: Assign the Wi-Fi profile to user accounts, user groups, or device groups.

iOS and macOS: Wi-Fi profile settings

iOS, iPadOS, and macOS: Wi-Fi profile setting	Description
Apply profile to	This setting specifies whether the Wi-Fi profile on a macOS device is applied to the user account or the device.
Automatically join network	This setting specifies whether a device can automatically join the Wi-Fi network.
Disable MAC randomization	This setting specifies whether devices can randomize their MAC addresses when they join the Wi-Fi network.
Associated proxy profile	This setting specifies the associated proxy profile that a device uses to connect to a proxy server when the device is connected to the Wi-Fi network.
Network type	This setting specifies a configuration for the Wi-Fi network. Hotspot configurations apply only to iOS, iPadOS, and macOS devices. If you select one of the hotspot options, do not use the same Wi-Fi profile to configure settings for other device types.
Displayed operator name	This setting specifies the friendly name of the hotspot operator. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0."
Domain name	This setting specifies the domain name of the hotspot operator. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0." The "SSID" setting is not required when you use this setting.
Roaming consortium OIs	This setting specifies the organization identifiers of roaming consortiums and service providers that are accessible through the hotspot. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0."
NAI realm names	This setting specifies the NAI realm names that can authenticate a device. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0."
MCC/MNCs	This setting specifies the MCC/MNC combinations that identify mobile network operators. Each value must contain exactly six digits. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0."
Allow connecting to roaming partner networks	This setting specifies whether a device can connect to roaming partners for the hotspot. This setting is valid only if the "Network type" setting is set to "Hotspot 2.0."

iOS, iPadOS, and macOS: Wi-Fi profile setting	Description
Security type	This setting specifies the type of security that the Wi-Fi network uses. If the "Network type" setting is set to "Hotspot 2.0," this setting is set to "WPA2-Enterprise."
WEP key	This setting specifies the WEP key for the Wi-Fi network. The WEP key must be 10 or 26 hexadecimal characters (0-9, A-F) or 5 or 13 alphanumeric characters (0-9, A-Z). Examples of hexadecimal key values are ABCDEF0123 or ABCDEF0123456789ABCDEF0123. Examples of alphanumeric key values are abCD5 or abCDefGHijKL1. This setting is valid only if the "Security type" setting is set to "WEP personal."
Preshared key	This setting specifies the preshared key for the Wi-Fi network. This setting is valid only if the "Security type" setting is set to "WPA-Personal," "WPA2-Personal" or "WPA3-Personal."
Protocols	
Authentication protocol	This setting specifies the EAP methods that the Wi-Fi network supports. You can select multiple EAP methods. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Inner authentication	This setting specifies the inner authentication method for use with TTLS. This setting is valid only if the "Authentication protocol" setting is set to "TTLS."
Use PAC	This setting specifies whether the EAP-FAST method uses a Protected Access Credential. This setting is valid only if the "Authentication protocol" setting is set to "EAP-FAST."
Provision PAC	This setting specifies whether the EAP-FAST method allows PAC provisioning. This setting is valid only if the "Authentication protocol" setting is set to "EAP-FAST" and the "Use PAC" setting is selected.
Provision PAC anonymously	This setting specifies whether the EAP-FAST method allows anonymous PAC provisioning. This setting is valid only if the "Authentication protocol" setting is set to "EAP-FAST," the "Use PAC" setting is selected, and the "Provision PAC" setting is selected.
Authentication	

iOS, iPadOS, and macOS: Wi-Fi profile setting	Description
Outer identity for TTLS, PEAP, and EAP-FAST	This setting specifies the outer identity for a user that is sent in clear text. You can specify an anonymous username to hide the user's real identity (for example, anonymous). The encrypted tunnel is used to send the real username to authenticate with the Wi-Fi network. If the outer identity includes the realm name to route the request, it must be the user's actual realm (for example, anonymous@example.com). This setting is valid only if the "Authentication protocol" setting is set to "TTLS," "PEAP," or "EAP-FAST."
Use password included in Wi-Fi profile	This setting specifies whether the Wi-Fi profile includes the password for authentication. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Password	This setting specifies the password that a device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Use password included in Wi-Fi profile" setting is selected.
Username	This setting specifies the username that a device uses to authenticate with the Wi-Fi network. If the profile is for multiple users, you can specify the %UserName% variable. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Authentication type	This setting specifies the type of authentication that a device uses to connect to the Wi-Fi network. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Type of certificate linking	This setting specifies the type of linking for the client certificate associated with the Wi-Fi profile. This setting is valid only if the "Authentication type" setting is set to "Shared certificate."
Shared certificate profile	This setting specifies the shared certificate profile with the client certificate that a device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Single reference."
Client certificate name	This setting specifies the name of the client certificate that a device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Variable injection."

iOS, iPadOS, and macOS: Wi-Fi profile setting	Description
Associated SCEP profile	This setting specifies the associated SCEP profile that a device uses to obtain a client certificate to authenticate with the Wi-Fi network. This setting is valid only if the "Authentication type" setting is set to "SCEP".
Associated ACME profile	This setting specifies the associated ACME profile that a device uses to obtain a client certificate to authenticate with the Wi-Fi network. This setting is valid only if the "Authentication type" setting is set to "ACME".
Associated user credential profile	This setting specifies the associated user credential profile that a device uses to obtain a client certificate to authenticate with the Wi-Fi network. This setting is valid only if the "Authentication type" setting is set to "User credential."
Trust	
Certificate common names expected from authentication server	This setting specifies the common names in the certificate that the authentication server sends to the device (for example, *.example.com). This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Type of certificate linking	This setting specifies the type of linking for the trusted certificates associated with the Wi-Fi profile. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
CA certificate profiles	This setting specifies the CA certificate profiles with the trusted certificates that a device uses to establish trust with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Single reference."
Trusted certificate names	This setting specifies the names of the trusted certificates that a device uses to establish trust with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Variable injection."
Trust user decisions	This setting specifies whether a device prompts the user to trust a server when the chain of trust can't be established. If this setting is not selected, only connections to trusted servers that you specify are allowed. This setting is valid only if the "Security type" setting is set to "WEP enterprise," "WPA-Enterprise," "WPA2-Enterprise" or "WPA3-Enterprise."
Bypass captive network	This setting specifies whether devices can bypass captive networks.
Enable QoS marking	This setting specifies whether you can enable L2 and L3 marking for traffic sent through the Wi-Fi network.

iOS, iPadOS, and macOS: Wi-Fi profile setting	Description
Use QoS for FaceTime calls	This setting specifies whether audio and video traffic for FaceTime calls can use L2 and L3 marking.
Use only L2 marking for QoS traffic	This setting specifies whether traffic sent through the Wi-Fi network uses only L2 marking.
Apply QoS marking to selected apps	This setting specifies the bundle IDs for apps that can use L2 and L3 marking.

Android: Wi-Fi profile settings

Android: Wi-Fi profile setting	Description
Associated proxy profile	This setting specifies the associated proxy profile that Android devices use to connect to a proxy server when the device is connected to the Wi-Fi network. Android devices with MDM controls or User privacy activations don't support Wi-Fi profiles with proxy settings.
BSSID	This setting specifies the MAC address of a wireless access point in the Wi-Fi network.
Primary DNS	This setting specifies the primary DNS server in dot-decimal notation (for example, 192.0.2.0). This setting applies only to devices that use Samsung Knox when the IP address is statically assigned by the organization's network.
Secondary DNS	This setting specifies the secondary DNS server in dot-decimal notation (for example, 192.0.2.0). This setting applies only to devices that use Samsung Knox when the IP address is statically assigned by the organization's network.
Security type	This setting specifies the type of security that the Wi-Fi network uses.
Personal security type	This setting specifies the type of personal security that the Wi-Fi network uses. This setting is valid only if the "Security type" setting is set to "Personal."
WEP key	This setting specifies the WEP key for the Wi-Fi network. The WEP key must be 10 or 26 hexadecimal characters (0-9, A-F) or 5 or 13 alphanumeric characters (0-9, A-Z). Examples of hexadecimal key values are ABCDEF0123 or ABCDEF0123456789ABCDEF0123. Examples of alphanumeric key values are abCD5 or abCDefGHijKL1. This setting is valid only if the "Personal security type" setting is set to "WEP personal."

Android: Wi-Fi profile setting	Description
Preshared key	This setting specifies the preshared key for the Wi-Fi network. This setting is valid only if the "Personal security type" setting is set to "WPA-Personal/WPA2-Personal."
Authentication protocol	This setting specifies the EAP method that the Wi-Fi network uses. This setting is valid only if the "Security type" setting is set to "Enterprise." LEAP is not supported by devices that use Samsung Knox.
Inner authentication	This setting specifies the inner authentication method for use with TTLS. This setting is valid only if the "Authentication protocol" setting is set to "TTLS." CHAP is not supported by devices that use Samsung Knox.
Outer identity for TTLS	This setting specifies the outer identity for a user that is sent in clear text. You can specify an anonymous username to hide the user's real identity (for example, anonymous). The encrypted tunnel is used to send the real username to authenticate with the Wi-Fi network. If the outer identity includes the realm name to route the request, it must be the user's actual realm (for example, anonymous@example.com). This setting is valid only if the "Authentication protocol" setting is set to "TTLS."
Outer identity for PEAP	This setting specifies the outer identity for a user that is sent in clear text. You can specify an anonymous username to hide the user's real identity (for example, anonymous). The encrypted tunnel is used to send the real username to authenticate with the Wi-Fi network. If the outer identity includes the realm name to route the request, it must be the user's actual realm (for example, anonymous@example.com). This setting is valid only if the "Authentication protocol" setting is set to "PEAP."
Username	This setting specifies the username that an Android device uses to authenticate with the Wi-Fi network. If the profile is for multiple users, you can specify the %UserName% variable. This setting is valid only if the "Security type" setting is set to "Enterprise."
Use password included in Wi-Fi profile	This setting specifies whether the Wi-Fi profile includes the password for authentication. This setting is valid only if the "Security type" setting is set to "Enterprise."
Password	This setting specifies the password that an Android device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Use password included in Wi-Fi profile" setting is selected.

Android: Wi-Fi profile setting	Description
Authentication type	This setting specifies the type of authentication that an Android device uses to connect to the Wi-Fi network. This setting is valid only if the "Security type" setting is set to "Enterprise."
Type of certificate linking	This setting specifies the type of linking for the client certificate associated with the Wi-Fi profile. This setting is valid only if the "Authentication type" setting is set to "Shared certificate."
Shared certificate profile	This setting specifies the shared certificate profile with the client certificate that an Android device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Single reference." The shared certificate profile name must be less than 36 characters for devices that use a Knox Workspace.
Associated SCEP profile	This setting specifies the associated SCEP profile that an Android device uses to obtain a client certificate to authenticate with the Wi-Fi network. This setting is valid only if the "Authentication type" setting is set to "SCEP." The SCEP profile name must be less than 36 characters for devices that use a Knox Workspace.
Associated user credential profile	This setting specifies the associated user credential profile that an Android device uses to obtain a client certificate to authenticate with the Wi-Fi network. This setting is valid only if the "Authentication type" setting is set to "User credential." The user credential profile name must be less than 36 characters for devices that use a Knox Workspace.
Client certificate name	This setting specifies the name of the client certificate that an Android device uses to authenticate with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Variable injection."
Certificate common names expected from authentication server	This setting specifies the common names in the certificate that the authentication server sends to the device (for example, *.example.com). This setting is valid only if the "Security type" setting is set to "Enterprise."
Type of certificate linking	This setting specifies the type of linking for the trusted certificates associated with the Wi-Fi profile. This setting is valid only if the "Security type" setting is set to "Enterprise."

Android: Wi-Fi profile setting	Description
CA certificate profile	This setting specifies the CA certificate profile with the trusted certificate that an Android device uses to establish trust with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Single reference."
Trusted certificate names	This setting specifies the names of the trusted certificates that an Android device uses to establish trust with the Wi-Fi network. This setting is valid only if the "Type of certificate linking" setting is set to "Variable injection."

Windows: Wi-Fi profile settings

Windows: Wi-Fi profile setting	Description
Connect automatically when this network is in range	This setting specifies whether devices can connect automatically to the Wi-Fi network.
Security type	This setting specifies the type of security that the Wi-Fi network uses.
Encryption type	This setting specifies the encryption method that the Wi-Fi network uses. The "Security type" setting determines which encryption types are supported and the default value for this setting.
WEP key	This setting specifies the WEP key for the Wi-Fi network. The WEP key must be 10 or 26 hexadecimal characters (0-9, A-F) or 5 or 13 alphanumeric characters (0-9, A-Z). Examples of hexadecimal key values are ABCDEF0123 or ABCDEF0123456789ABCDEF0123. Examples of alphanumeric key values are abCD5 or abCDefGHijKL1. This setting is valid only if the "Security type" setting is set to "Open" and the "Encryption type" is set to "WEP."
Key index	This setting specifies the position of the matching key stored on the wireless access point. This setting is valid only if the "Security type" setting is set to "Open" and the "Encryption type" is set to "WEP."
Preshared key	This setting specifies the preshared key for the Wi-Fi network. This setting is valid only if the "Security type" setting is set to "WPA-Personal."

Windows: Wi-Fi profile setting	Description
Enable single sign-on	This setting specifies whether the Wi-Fi network supports single sign-on authentication. This setting is valid only if the "Security type" setting is set to "WPA-Enterprise" or "WPA2-Enterprise."
Single sign-on type	This setting specifies when single sign-on authentication is performed. When set to “Perform immediately before user login”, single sign-on is performed before the user logs in to Active Directory. When set to “Perform immediately after user login”, single sign-on is performed immediately after the user logs in to Active Directory. This setting is valid only if the “Enable single sign-on" setting is selected.
Maximum delay for connectivity	This setting specifies, in seconds, the maximum delay before the single sign-on connection attempt fails. This setting is valid only if the “Enable single sign-on" setting is selected.
Allow additional dialogs to be displayed during single sign-on	This setting specifies whether a device can display dialog boxes beyond the login screen. For example, if an EAP authentication type requires a user to confirm the certificate sent from server during authentication, the device can display the dialog box. This setting is valid only if the “Enable single sign-on" setting is selected.
This network uses separate virtual LANs for machine and user authentication	This setting specifies whether the VLAN used by a device changes based on the user's login information. For example, if the device is placed on one VLAN when it starts, and then (based on user permissions) transitions to a different VLAN network after the user logs in. This setting is valid only if the “Enable single sign-on" setting is selected.
Validate server certificate	This setting specifies whether a device must validate the server certificate that verifies the identity of the wireless access point. This setting is valid only if the "Security type" setting is set to "WPA-Enterprise" or "WPA2-Enterprise."
Do not prompt user to authorize new servers or trusted certification authorities	This setting specifies whether a user is prompted to trust the server certificate. This setting is valid only if the “Validate server certificate" setting is selected.
CA certificate profiles	This setting specifies the CA certificate profile that provides the root of trust for the server certificate that the wireless access point uses. This setting limits the root CAs that devices trust to the selected CAs. If you do not select any trusted root CAs, devices trust all root CAs listed in their trusted root certification authority store. This setting is valid only if the “Validate server certificate" setting is selected.

Windows: Wi-Fi profile setting	Description
Enable fast reconnect	This setting specifies whether the Wi-Fi network supports fast reconnect for PEAP authentication across multiple wireless access points. This setting is valid only if the "Security type" setting is set to "WPA-Enterprise" or "WPA2-Enterprise."
Enforce NAP	This setting specifies whether the Wi-Fi network uses NAP to perform system health checks on devices to verify that they meet health requirements before connections to the network are permitted. This setting is valid only if the "Security type" setting is set to "WPA-Enterprise" or "WPA2-Enterprise."
Enable FIPS mode	This setting specifies whether the Wi-Fi network supports compliance with the FIPS 140-2 standard. This setting is valid only if the "Security type" setting is set to "WPA2-Enterprise" or "WPA2-Personal" and the "Encryption type" is set to "AES."
Enable PMK caching	This setting specifies whether a device can cache the PMK to turn on WPA2 fast roaming. Fast roaming skips 802.1X settings with a wireless access point that the device authenticated with previously. This setting is valid only if the "Security type" setting is set to "WPA2-Enterprise."
PMK time to live	This setting specifies the duration, in minutes, that a device can store the PMK in cache. This setting is valid only if the “Enable PMK caching" setting is selected.
Number of entries in PMK cache	This setting specifies the maximum number of PMK entries that a device can store in cache. This setting is valid only if the “Enable PMK caching" setting is selected.
This network uses preauthentication	This setting specifies whether the access point supports preauthentication for WPA2 fast roaming. Preauthentication allows devices that connect to one wireless access point to perform 802.1X settings with other wireless access points within its range. Preauthentication stores the PMK and its associated information in the PMK cache. When the device connects to a wireless access point with which it has preauthenticated, it uses the cached PMK information to reduce the time required to authenticate and connect. This setting is valid only if the “Enable PMK caching" setting is selected.
Maximum preauthentication attempts	This setting specifies the maximum number of allowed preauthentication attempts. This setting is valid only if the “This network uses preauthentication" setting is selected.

Windows: Wi-Fi profile setting	Description
Proxy type	This setting specifies the type of proxy configuration for the Wi-Fi profile. This setting applies only to Windows 10 Mobile devices.
PAC URL	This setting specifies the URL for the web server that hosts the PAC file and the PAC file name in the format http://<web_server_URL>/<filename>.pac. This setting is valid only if the "Proxy type" setting is set to "PAC configuration."
Address	This setting specifies the server name and port for the network proxy. Use the format host:port (for example, server01.example.com:123). The host must be one of the following: • A registered name, such as a server name, FQDN, or Single Label Name (for example, server01 instead of server01.example.com) • An IPv4 or IPv6 address This setting is valid only if the "Proxy type" setting is set to "Manual configuration."
Web Proxy Autodiscovery	This setting specifies whether to enable the Web Proxy Autodiscovery Protocol (WPAD) for proxy lookup. This setting is valid only if the "Proxy type" setting is set to "Web Proxy Autodiscovery."
Turn off Internet connectivity checks	This setting specifies whether to turn off Internet connectivity checks.
Associated SCEP profile	This setting specifies the associated SCEP profile that a device uses to obtain a client certificate to authenticate with the Wi-Fi network.

Setting up work VPNs for devices

You can use a VPN profile to specify how iOS, iPadOS, macOS, Samsung Knox, and Windows 10 devices connect to a work VPN. You can assign a VPN profile to user accounts, user groups, or device groups.

To connect to a work VPN for Android devices other than Samsung Knox, you can configure VPN settings using app configuration settings for a VPN app, or users can manually configure the VPN settings on their devices.

Device	Apps and network connections
iOS and iPadOS	Work and personal apps can use the VPN profiles stored on the device to connect to your organization's network. You can enable per-app VPN for a VPN profile to limit the profile to the work apps that you specify. You can enable VPN on demand to have devices connect automatically to a VPN in a particular domain. For example, you can specify your organization's domain to allow users access to your intranet content using VPN on demand.

Device	Apps and network connections
macOS	You can configure VPN profiles to allow apps to connect to your organization's network. You can enable VPN on demand to have devices connect automatically to a VPN in a particular domain. For example, you can specify your organization's domain to allow users access to your intranet content using VPN on demand.
Samsung Knox	On Samsung Knox devices with Android Enterprise or Samsung Knox Workspace activations, work apps can use the VPN profiles stored on the device to connect to your organization's network. You can enable per-app VPN to limit the profile to the work apps that you specify. You must install a supported VPN client app that uses KNOX SDK on the device.
Windows 10	You can configure VPN profiles to allow apps to connect to your organization's network. In the VPN profile, you can specify a list of apps that must use the VPN.

Create a VPN profile

The required profile settings vary for each device type and depend on the VPN connection type and authentication type that you select. You can use a variable in any profile setting that is a text field to reference a value instead of specifying the actual value.

Before you begin:

- If devices use certificate-based authentication for work VPN connections, create a CA certificate profile and assign it to user accounts, user groups, or device groups. To send client certificates to devices, create a SCEP, shared certificate, or user credential profile to associate with the VPN profile.
- For iOS, iPadOS, macOS, and Samsung Knox devices that use a proxy server, create a proxy profile to associate with the VPN profile.
- For Samsung Knox devices, add the appropriate VPN client app to the app list and assign it to user accounts, user groups, or device groups. The supported VPN client apps are Cisco AnyConnect, Juniper, and GlobalProtect.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > VPN**.
3. Click +.
4. Type a name and description for the VPN profile. This information is displayed on devices.
5. Click the tab for a device type to configure the appropriate settings. For more information, see the VPN profile settings for iOS and macOS, Android, and Windows.

   If your organization requires that users provide a username and password to connect to the VPN network, in the **Username** field, type `%UserName%`.
6. Click **Add**.

After you finish: Assign the Wi-Fi profile to user accounts, user groups, or device groups.

iOS and macOS: VPN profile settings

iOS, iPadOS, and macOS: VPN profile setting	Description
Apply profile to	This setting specifies whether the VPN profile on a macOS device is applied to the user account or the device.
Connection type	This setting specifies the connection type that a device uses for a VPN gateway. Some connection types also require users to install the appropriate VPN app on the device. If you select "IKEv2 Always On," many settings have separate values for cellular and Wi-Fi connections.
VPN bundle ID	This setting specifies the bundle ID of the VPN app for a custom SSL VPN. The bundle ID is in reverse-DNS format (for example, com.example.VPNapp). This setting is valid only if the "Connection type" setting is set to "Custom."
Server	This setting specifies the FQDN or IP address of a VPN server.
Username	This setting specifies the username that a device uses to authenticate with the VPN gateway. If the profile is for multiple users, you can specify the %UserName % variable.
Custom key-value pairs	This setting specifies the keys and associated values for the custom SSL VPN. The configuration information is specific to the vendor's VPN app. This setting is valid only if the "Connection type" setting is set to "Custom."
Login group or Domain	This setting specifies the login group or domain that the VPN gateway uses to authenticate a device. This setting is valid only if the "Connection type" setting is set to "SonicWALL Mobile Connect."
Realm	This setting specifies the name of the authentication realm that the VPN gateway uses to authenticate a device. This setting is valid only if the "Connection type" setting is set to "Juniper" or "Pulse Secure."
Role	This setting specifies the name of the user role that the VPN gateway uses to verify the network resources that a device can access. This setting is valid only if the "Connection type" setting is set to "Juniper" or Pulse Secure."
Authentication type	This setting specifies the authentication type for the VPN gateway. The "Connection type" setting determines which authentication types are supported and the default value for this setting.

iOS, iPadOS, and macOS: VPN profile setting	Description
EAP plug-ins	This setting specifies authentication plugins for the VPN. This setting is valid only if the "Connection type" setting is set to "L2TP" or "PPTP" and the "Authentication type" setting is set to "RSA SecurID."
Authentication protocol	This setting specifies authentication protocols for the VPN. This setting is valid only if the "Connection type" setting is set to "L2TP" or "PPTP" and the "Authentication type" setting is set to "RSA SecurID."
Password	This setting specifies the password that a device uses to authenticate with the VPN gateway. This setting is valid only if the "Authentication type" setting is set to "Password."
Group name	This setting specifies the group name for the VPN gateway. This setting is valid only in the following conditions: • The "Connection type" setting is set to "Cisco AnyConnect." • The "Connection type" setting is set to "IPsec" and the "Authentication type" setting is set to "Shared secret/Group name."
Shared secret	This setting specifies the shared secret to use for VPN authentication. This setting is valid only in the following conditions: • The "Connection type" setting is set to "L2TP." • The "Connection type" setting is set to "IPsec" and the "Authentication type" setting is set to "Shared secret/Group name." • The "Connection type" setting is set to "IKEv2" or "IKEv2 Always On" and the "Authentication type" setting is set to "Shared secret."
Shared certificate profile	This setting specifies the shared certificate profile with the client certificate that a device uses to authenticate with the VPN gateway. This setting is valid only if the "Authentication type" setting is set to "Shared certificate."
Associated SCEP profile	This setting specifies the associated SCEP profile that a device uses to obtain a client certificate to authenticate with the VPN. This setting is valid only if the "Authentication type" setting is set to "SCEP."
Associated ACME profile	This setting specifies the associated ACME profile that a device uses to obtain a client certificate to authenticate with the VPN. This setting is valid only if the "Authentication type" setting is set to "ACME."
Associated user credential profile	This setting specifies the associated user credential profile that a device uses to obtain a client certificate to authenticate with the VPN. This setting is valid only if the "Authentication type" setting is set to "User credential."

iOS, iPadOS, and macOS: VPN profile setting	Description
Encryption level	This setting specifies the level of data encryption for the VPN connection. If this setting is set to "Automatic," all available encryption strengths are allowed. If this setting is set to "Maximum," only the maximum encryption strength is allowed. This setting is valid only if the "Connection type" setting is set to "PPTP."
Route network traffic through VPN	This setting specifies whether to send all network traffic through the VPN connection. This setting is valid only if the "Connection type" setting is set to "L2TP" or "PPTP."
Use hybrid authentication	This setting specifies whether to use a server-side certificate for authentication. This setting is valid only if the "Connection type" setting is set to "IPsec" and "Authentication type" is set to "Shared secret/Group name"
Prompt for password	This setting specifies whether a device prompts the user for a password. This setting is valid only if the "Connection type" setting is set to "IPsec" and "Authentication type" is set to "Shared secret/Group name"
Prompt for user PIN	This setting specifies whether the device prompts the user for a PIN. This setting is valid only if the "Connection type" setting is set to "IPsec" and the "Authentication type" setting is set to "Shared Certificate," "SCEP," or "User credential."
Remote address	This setting specifies the IP address or hostname of the VPN server. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Local ID	This setting specifies the identity of the IKEv2 client in one of the following formats: FQDN, UserFQDN, Address, and ASN1DN. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Remote ID	This setting specifies the remote identifier of the IKEv2 client using one of the following formats: FQDN, user FQND, Address, or ASN1DN. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."

iOS, iPadOS, and macOS: VPN profile setting	Description
Enable VPN on demand	This setting specifies whether a device can start a VPN connection automatically when it accesses certain domains. For iOS and iPadOS devices, this setting applies to work apps. This setting is valid only in the following conditions: • The "Connection type" setting is set to "IPsec," "Cisco AnyConnect," "Juniper," "Pulse Secure," "F5," "SonicWALL Mobile Connect," "Aruba VIA," "Check Point Mobile," "OpenVPN," or "Custom" and the "Authentication type" is set to "Shared certificate," "SCEP," or "User credential." • The "Connection type" is set to IKEv2 and the "Authentication type" is set to Shared certificate, SCEP, or User credential.
Domain or host names that can use VPN on demand	This setting specifies the domains and the associated actions for VPN on demand. This setting is valid only if the "Enable VPN on demand" setting is selected.
VPN on demand rules for iOS 7.0 and later	This setting specifies the connection requirements for VPN on demand. You must use one or more keys from the payload format example. This setting overrides the "Domain or host names that can use VPN on demand" setting. This setting is valid only if the "Enable VPN on demand" setting is selected.
Disconnect on idle	This setting specifies whether the VPN connection disconnects if it idle for a specified period of time. This setting is valid only if the "Enable VPN on demand" setting is selected.
Disconnect on idle timer	This setting specifies the idle time in seconds after which the VPN disconnects. This setting is valid only if the "Disconnect on idle" setting is selected.
Do not allow user to disable VPN on demand	This setting specifies whether the user can disable VPN on demand. This setting is valid only if the "Connection type" setting is set to "IPsec," "Cisco AnyConnect," "Juniper," "Pulse Secure," "F5," "SonicWALL Mobile Connect," "Aruba VIA," "Check Point Mobile," "OpenVPN," or "Custom."
Exclude local network	This setting specifies whether to exclude local network traffic from using the VPN connection. If the “Include all networks” setting is also selected, no local network traffic is routed through the VPN.
All non-default routes take precedence over any locally defined routes	This setting specifies whether the non-default routes for the VPN take precedence over any locally defined routes. If the “Include all networks” setting is also selected, this setting is ignored. This setting is valid only if the "Connection type" setting is set to "Cisco AnyConnect," "Juniper," "Pulse Secure," "F5," "SonicWALL Mobile Connect," "Aruba VIA," "Check Point Mobile," "OpenVPN," or "Custom."

iOS, iPadOS, and macOS: VPN profile setting	Description
Include all networks	This setting specifies whether to route all traffic through the VPN. If "Exclude local network" is also selected, local network traffic in not routed through the VPN. This setting applies only to devices running iOS and iPadOS 13 and later.
Provider designated requirement	This setting specifies a designated VPN provider. If the VPN provider is implemented as a system extension, this setting is required. This setting is valid only if the "Connection type" setting is set to "IPsec," "Cisco AnyConnect," "Juniper," "Pulse Secure," "F5," "SonicWALL Mobile Connect," "Aruba VIA," "Check Point Mobile," "OpenVPN," or "Custom."
Allow user to disable automatic connection	This setting specifies whether users can disable the VPN connection. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On."
Use same tunnel configuration for cellular and Wi-Fi	This setting specifies whether you want to set separate VPN settings for the device depending on whether the device is sending data over a cellular network or a Wi-Fi network. If this setting is not selected, you can set different cellular and Wi-Fi settings in the same profile. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On."
Enable xAuth	This setting specifies whether the VPN supports extended authentication. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Minimum TLS version	This setting specifies the minimum TLS version that devices use for EAP-TLS authentication. This setting is valid only if the "Enable xAuth" setting is selected and the Authentication type is “Certificate.”
Maximum TLS version	This setting specifies the maximum TLS version that devices use for EAP-TLS authentication. This setting is valid only if the "Enable xAuth" setting is selected and the Authentication type is “Certificate.”
Certificate type	This setting specifies the type of certificate used for IKEv2 machine authentication. This setting is valid only if the "Enable xAuth" setting is selected and the Authentication type is “Certificate.”
Common name of the server certificate issuer	This setting specifies the common name of the CA that issued the server certificate that the IKE server sends to the device. If you enable xAuth using a certificate, this setting is required. This setting is valid only if the "Enable xAuth" setting is selected and the Authentication type is “Certificate.”

iOS, iPadOS, and macOS: VPN profile setting	Description
Common name of the server certificate	This setting specifies the common name of the server certificate that the IKE server sends to the device. This setting is valid only if the "Enable xAuth" setting is selected and the Authentication type is “Certificate.”
Keepalive interval	This setting specifies how often a device sends a keepalive packet. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Disable MOBIKE	This setting specifies whether MOBIKE is disabled. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Disable IKEv2 redirect	This setting specifies whether IKEv2 redirect is disabled. If this setting is not selected, the IKEv2 connection is redirected if a redirect request is received from the server. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Enable perfect forward secrecy	This setting specifies whether the VPN supports PFS. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Enable NAT keepalive	This setting specifies whether the VPN supports NAT keepalive packets. Keepalive packets are used to maintain NAT mappings for IKEv2 connections. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
NAT keepalive interval	This setting specifies how often a device sends a NAT keepalive packet (in seconds). This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On" and the "Enable NAT keepalive" setting is selected.
Use IPv4 and IPv6 IKEv2 internal subnets	This setting specifies whether the VPN can use the IKEv2 configuration attribute INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Common name of the server certificate	This setting specifies the common name in the certificate that the IKE server sends to the device. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."

iOS, iPadOS, and macOS: VPN profile setting	Description
Common name of the server certificate issuer	This setting specifies the common name of the certificate issuer in the certificate that the IKE server sends to the device. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Enable certificate revocation check	This setting specifies whether a certificate revocation check is attempted for the server certificate. The check does not fail if there is no response. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Enable fallback	This setting specifies whether the device can establish a VPN tunnel over the mobile network when Wi-Fi Assist is enabled. This setting applies only to devices running iOS and iPadOS 13 and later and requires that the server support multiple tunnels for individual users. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Apply Child Security Association parameters	This setting specifies whether to apply child security association parameters. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
Apply IKE Security Association parameters	This setting specifies whether to apply IKE security association parameters. This setting is valid only if the "Connection type" setting is set to "IKEv2" or "IKEv2 Always On."
MTU	This setting specifies the Maximum Transmission Unit in bytes. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On."
VoiceMail	This setting specifies whether connections to the voice mail service are sent through the VPN tunnel, sent outside of the VPN tunnel, or are blocked. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.
AirPrint	This setting specifies whether AirPrint connections are sent through the VPN tunnel, sent outside of the VPN tunnel, or are blocked. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.
Allow traffic from captive web sheet outside the VPN tunnel	This setting specifies whether traffic from captive web sheets can be sent outside of the VPN tunnel. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.

iOS, iPadOS, and macOS: VPN profile setting	Description
Allow traffic from all captive networking apps outside VPN tunnel	This setting specifies whether traffic from all captive networking apps can be sent outside of the VPN tunnel. If this setting is not selected, you can specify individual apps for which traffic can be sent outside the tunnel. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.
Traffic from these apps is allowed outside VPN tunnel	This setting specifies individual captive networking apps for which traffic can be sent outside the tunnel. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.
Allow app traffic outside the VPN tunnel	This setting specifies apps whose traffic can be sent outside the tunnel. This setting is valid only if the "Connection type" setting is set to "IKEv2 Always On." It applies only to Wi-Fi connections.
DH group	This setting specifies the DH group that a device uses to generate key material. This setting is valid only if the "Apply Child Security Association parameters" or "Apply IKE Security Association parameters" setting is selected.
Encryption algorithm	This setting specifies the IKE encryption algorithm. This setting is valid only if the "Apply Child Security Association parameters" or "Apply IKE Security Association parameters" setting is selected.
Integrity algorithm	This setting specifies the IKE integrity algorithm. This setting is valid only if the "Apply Child Security Association parameters" or "Apply IKE Security Association parameters" setting is selected.
Rekey interval	This setting specifies the lifetime of the IKE connection. This setting is valid only if the "Apply Child Security Association parameters" or "Apply IKE Security Association parameters" setting is selected.
Enable per-app VPN	This setting specifies whether the VPN gateway supports per-app VPN. This feature helps decrease the load on an organization's VPN. For example, you can enable only certain work traffic to use the VPN, such as accessing application servers or webpages behind the firewall. This setting is valid only if the "Connection type" setting is set to "Cisco AnyConnect," "Juniper," "Pulse Secure," "F5," "SonicWALL Mobile Connect," "Aruba VIA," "Check Point Mobile," "OpenVPN," "Custom," or "IKEv2".
Allow apps to connect automatically	This setting whether apps associated with per-app VPN can start the VPN connection automatically. This setting is valid only if the "Enable per-app VPN" setting is selected.

iOS, iPadOS, and macOS: VPN profile setting	Description
Safari domains	This setting specifies the domains that can start the VPN connection in Safari. This setting is valid only if the "Enable per-app VPN" setting is selected.
Calendar domains	This setting specifies the domains that can start the VPN connection in Calendar. This setting is valid only if the "Enable per-app VPN" setting is selected.
Contacts domains	This setting specifies the domains that can start the VPN connection in Contacts. This setting is valid only if the "Enable per-app VPN" setting is selected.
Mail domains	This setting specifies the domains that can start the VPN connection in Mail. This setting is valid only if the "Enable per-app VPN" setting is selected.
Associated domains	This setting specifies domains that can start the VPN connection on the device. The domains must also be included in the apple-app-site-association file. This setting is valid only if the "Enable per-app VPN" setting is selected.
Excluded domains	This setting specifies domains that are blocked from starting the VPN connection on the device. This setting is valid only if the "Enable per-app VPN" setting is selected.
Traffic tunneling	This setting specifies whether the VPN tunnels traffic at the application layer or the IP layer. This setting is valid only if the "Enable per-app VPN" setting is selected.
Associated proxy profile	This setting specifies the associated proxy profile that a device uses to connect to a proxy server when the device is connected to the VPN.

Android: VPN profile settings

The following VPN profile settings are supported only on Samsung Knox devices.

Android: VPN profile setting	Description
Server address	This setting specifies the FQDN or IP address of a VPN server.
VPN type	This setting specifies whether a device uses IPsec or SSL to connect to the VPN server. The Juniper VPN app supports "SSL" only.
User authentication required	This setting specifies whether a device user must provide a username and password to connect to the VPN server.

Android: VPN profile setting	Description
Username	This setting specifies the username that a device uses to authenticate with the VPN gateway. If the profile is for multiple users, you can use the %UserName% variable. This setting is valid only if the “User authentication required” setting is selected.
Password	This setting specifies the password that a device uses to authenticate with the VPN gateway. This setting is valid only if the “User authentication required” setting is selected.
Split tunnel type	This setting specifies whether a device can use split tunneling to bypass the VPN gateway, if the VPN gateway supports it. If the "VPN type" setting is set to "IPsec," this setting must be set to “Disabled."
Forward routes	This setting specifies the route or routes that bypass the VPN gateway. You can specify one or more IP addresses. This setting is valid only if the "VPN type" setting is set to "SSL" and the “Split tunnel type” setting is set to “Manual.”
DPD	This setting specifies whether DPD is enabled. This setting is valid only if the "VPN type" setting is set to "IPsec."
IKE version	This setting specifies the version of IKE protocol to use with the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec authentication type	This setting specifies the authentication type for the IPsec VPN connection. The "IKE version" setting determines which IPsec authentication types are supported and the default value for this setting. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec group ID type	This setting specifies the IPsec group ID type for the VPN connection. The "IPsec authentication type" setting determines which IPsec group ID types are supported and the default value for this setting. If the setting for “IPsec authentication type” is “Certificate," then this setting is automatically set to “Default." This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec group ID	This setting specifies the IPsec group ID for the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec."
IKE phase 1 key exchange mode	This setting specifies the exchange mode for the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec."

Android: VPN profile setting	Description
IKE lifetime	This setting specifies the lifetime, in seconds, of the IKE connection. If you set an unsupported value or a null value, the device default value is used. This setting is valid only if the "VPN type" setting is set to "IPsec."
IKE encryption algorithm	This setting specifies the encryption algorithm used for the IKE connection. This setting is valid only if the "VPN type" setting is set to "IPsec."
IKE integrity algorithm	This setting specifies the integrity algorithm used for the IKE connection. This setting is valid only if the "VPN type" setting is set to "IPsec and the "IKE version" is set to "IKEv2."
IPsec DH group	This setting specifies the DH group that a device uses to generate key material. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec parameter	This setting specifies the IPsec parameter used for the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec."
Perfect forward secrecy	This setting specifies whether the VPN gateway supports PFS. This setting is valid only if the "VPN type" setting is set to "IPsec."
Enable MOBIKE	This setting specifies whether the VPN gateway supports MOBIKE. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec lifetime	This setting specifies the lifetime, in seconds, of the IPsec connection. If you set an unsupported value or a null value, the device default value is used. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec encryption algorithm	This setting specifies the IPsec encryption algorithm used for the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec."
IPsec integrity algorithm	This setting specifies the IPsec integrity algorithm used for the VPN connection. This setting is valid only if the "VPN type" setting is set to "IPsec" and the and the "IKE version" is set to "IKEv2."
Authentication type	This setting specifies the authentication type for the VPN gateway. This setting is valid only if the "VPN type" setting is set to "SSL."
SSL algorithm	This setting specifies the encryption algorithm required for an SSL VPN connection. This setting is valid only if the "VPN type" setting is set to "SSL."

Android: VPN profile setting	Description
Append UID/PID information	This setting specifies whether UID and PID information is appended to packets that are sent to the VPN client app. This setting must be selected for the Cisco AnyConnect VPN app.
Support chaining	This setting specifies how VPN chaining is supported.
Vendor string input type	This setting specifies the key-value pairs or JSON string for the VPN. The configuration information is specific to the vendor's VPN app.
Vendor key-value pairs	This setting specifies the keys and associated values for the VPN. The configuration information is specific to the vendor's VPN app. This setting is valid only if the "Vendor string input type" setting is set to "Vendor key-value pairs."
Vendor JSON value	This setting specifies the configuration information specific to the vendor's VPN app, in .json format. This setting is valid only if the "Vendor string input type" setting is set to "Vendor JSON value."
VPN client package ID	This setting specifies the package ID of the VPN app.
Automatically retry connection after error	This setting specifies whether the VPN connection should be automatically restarted after the connection is lost.
Enable FIPS mode	This setting specifies whether FIPS mode is enabled. Enabling FIPS mode makes sure that only FIPS-validated cryptographic algorithms are used for the VPN connection.
Enterprise connectivity for Android devices with a work space	This setting specifies whether Samsung Knox devices use a VPN connection for all apps in the work space or only for specified apps. • "Container wide VPN" uses a VPN connection for all apps in the work space on the device. • "Per-app VPN" uses a VPN connection only for specified apps.
Apps allowed to use the VPN connection	This setting specifies the apps in the work space that can use a VPN connection. You can select apps from a list of available apps or specify the app package ID. This setting is valid only if the "Enterprise connectivity for Android devices with a work space" setting is set to "Per-app VPN."
Associated proxy profile	This setting specifies the associated proxy profile that a device uses to connect to a proxy server when the device is connected to the VPN.

Windows 10: VPN profile settings

Windows: VPN profile setting	Description
Connection type	This setting specifies the connection type that a Windows 10 device uses for a VPN.
Server	This setting specifies the public or routable IP address or DNS name for the VPN. This setting can point to the external IP of a VPN, or a virtual IP for a server farm. This setting is valid only if the "Connection type" is set to "Microsoft."
Server URL list	This setting specifies a comma-separated list of servers in URL, host name, or IP format. This setting is valid only if the "Connection type" is not set to "Microsoft".
Routing policy type	This setting specifies the type of routing policy. This setting is valid only if the "Connection type" is set to "Microsoft."
Built-in protocol type	This setting specifies the type of routing policy used by the VPN. This setting is valid only if the "Connection type" is set to "Microsoft."
Authentication	This setting specifies the method of authentication used for the native VPN. The "Built-in protocol type" setting determines which authentication methods are supported and the default value for this setting.
EAP configuration	This setting specifies the XML of the EAP configuration. This setting is valid only if the "Authentication " setting is set to "EAP."
User method	This setting specifies the type of user method authentication to use. This setting is valid only if the "Authentication " setting is set to "User method."
Machine method	This setting specifies the type of machine method authentication to use. This setting is valid only if the "Authentication " setting is set to "Machine method."
Custom configuration	This setting specifies the HTML encoded XML blob for an SSL-VPN plug-in specific configuration, including authentication information, that is sent to the device to make it available for SSL-VPN plug-ins. This setting is valid only if the "Connection type" is not set to "Microsoft."
Plugin package family name	This setting specifies the package family name of the custom SSL VPN. This setting is valid only if the "Connection type" is set to "Manual connection definition."
L2TP preshared key	This setting specifies the preshared key used for an L2TP connection.
App trigger list	This setting specifies a list of apps that start the VPN connection.

Windows: VPN profile setting	Description
App trigger list > App ID	This setting identifies an app for a per-app VPN. Possible values: • Package family name. To find the package family name, install the app and run the Windows PowerShell command, `Get-AppxPackage`. • Installation location of the app. For example, C:\Windows\System \Notepad.exe.
Route list	This setting specifies a list of routes that the VPN can use. If the VPN uses split tunneling, a route list is required.
Subnet address	This setting specifies the IP address of the destination prefix using the IPv4 or IPv6 address format.
Subnet prefix	This setting specifies the subnet prefix of the destination prefix.
Exclusion	This setting specifies whether the route that is added must point to the VPN interface as the gateway or a physical interface. If you select the check box, traffic is directed over the physical interface. If you leave the box unchecked, traffic is directed over the VPN.
Domain name list	This setting specifies the Name Resolution Policy Table (NRPT) rules for the VPN.
Domain name	This setting specifies the FQDN or suffix of the domain.
DNS servers	This setting specifies the list of IP addresses of the DNS servers, separated by commas.
Web proxy server	This setting specifies the IP address of the web proxy server.
Trigger VPN	This setting specifies whether this domain name rule triggers the VPN.
Persistent	This setting specifies whether the domain name rule is applied when the VPN is not connected.
Traffic filter list	This setting specifies the rules that allow traffic over the VPN.
Traffic filter list > App ID	This setting identifies an app for an app-based traffic filter. Possible values: • Package family name. To find the package family name, install the app and run the Windows PowerShell command, `Get-AppxPackage`. • Installation location of the app. For example, `C:\Windows\System \Notepad.exe`. • Type "SYSTEM" to enable Kernel Drivers to send traffic through the VPN (for example, PING or SMB).
Protocol	This setting specifies the protocol that the VPN uses.

Windows: VPN profile setting	Description
Local port ranges	This setting specifies the list of allowed local port ranges separated by commas. For example, 100-120, 200, 300-320.
Remote port ranges	This setting specifies the list of allowed remote port ranges separated by commas. For example, 100-120, 200, 300-320.
Local address ranges	This setting specifies the list of allowed local IP address ranges, separated by commas.
Remote address ranges	This setting specifies the list of allowed remote IP address ranges, separated by commas.
Routing policy type	This setting specifies the routing policy that the traffic filter uses. If set to "Force tunnel," all traffic goes through the VPN. If set to "Split tunnel," traffic can go through the VPN or the Internet.
Remember credentials	This setting specifies whether the credentials are cached whenever possible.
Always on	This setting specifies whether devices automatically connect to the VPN at sign-in and stay connected until the user manually disconnects the VPN.
Lock down	This setting specifies whether this VPN connection must be used when the device connects to a network. When this setting is enabled, the following applies: • The device stays connected to the VPN. It cannot be disconnected. • The device must be connected to this VPN to have any network connection. • The device cannot connect to, or modify, other VPN profiles.
DNS suffix	This setting specifies one or more DNS suffixes separated by commas. The first DNS suffix in the list is also used as the primary connection for the VPN. The list is added to the SuffixSearchList.
Trusted network detection	This setting specifies a comma-separated string to identify the trusted network. The VPN does not connect automatically when users are on their organization's wireless network.
IP Security properties	
Authentication transform constants	This setting specifies the authentication level of a VPN. This setting must match the setting on the VPN server.
Cipher transform constants	This setting specifies the encryptions level of a VPN. This setting must match the setting on the VPN server.
Encryption method	This setting specifies the phase 1 encryption level of a VPN. This setting must match the setting on the VPN server.
Integrity check method	This setting specifies the phase 1 authentication level of a VPN. This setting must match the setting on the VPN server.

Windows: VPN profile setting	Description
Diffie-Hellman Group	This setting species the key group of a VPN. This setting must match the setting on the VPN server.
PFS Group	This setting specifies the Perfect Forward Secrecy encryption protocol used for the VPN. This setting must match the setting on the VPN server.
Proxy type	This setting specifies the type of proxy configuration for the VPN.
PAC URL	This setting specifies the URL for the web server that hosts the PAC file, including the PAC file name. For example, http://www.example.com/PACfile.pac. This setting is valid only if the "Proxy type" setting is set to "PAC configuration."
Address	This setting specifies the FQDN or IP address for the proxy server. This setting is valid only if the "Proxy type" setting is set to "Manual configuration."
Associated SCEP profile	This setting specifies the associated SCEP profile that a device uses to obtain a client certificate to authenticate with the VPN.

Enabling and assigning per-app VPN settings

You can set up per-app VPN for iOS, iPadOS, Samsung Knox, and Windows devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization's VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or web pages behind the firewall). In on-premises environments, this feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN.

Devices	App settings
iOS and iPadOS	Apps are associated with a VPN profile when you assign the app or app group to a user, user group, or device group.
Samsung Knox devices with Android Enterprise and Samsung Knox Workspace activations	Apps are added to the "Apps allowed to use the VPN connection" setting in the VPN profile.
Windows 10	Apps are added to the "App trigger list" setting in the VPN profile.

Only one VPN profile can be assigned to an app or app group.

BlackBerry UEM uses the following rules to determine which per-app VPN settings to assign to an app on iOS and iPadOS devices:

Per-app VPN settings	Precedence
If associated with an app directly	Takes precedence over per-app VPN settings associated indirectly by an app group.
If associated with a user directly	Take precedence over per-app VPN settings associated indirectly by a user group.
If assigned to a required app	Takes precedence over per-app VPN settings assigned to an optional instance of the same app.
If associated with the user group name that appears earlier in the alphabetical list	Takes precedence if the following conditions are met: • An app is assigned to multiple user groups • The same app appears in the user groups • The app is assigned in the same way, either as a single app or an app group • The app has the same disposition in all assignments, either required or optional For example, you assign Cisco WebEx Meetings as an optional app to the user groups Development and Marketing. When a user is in both groups, the per-app VPN settings for the Development group is applied to the WebEx Meetings app for that user.

If a per-app VPN profile is assigned to a device group, it takes precedence over the per-app VPN profile that is assigned to the user account for any devices that belong to the device group.

Setting up proxy profiles for devices

You can specify how devices use a proxy server to access web services on the Internet or a work network. For, iOS, iPadOS, macOS, and Android devices, you create a proxy profile. For Windows 10 devices, you add the proxy settings in the Wi-Fi or VPN profile.

Unless otherwise noted, proxy profiles support proxy servers that use basic or no authentication.

Device	Proxy configuration
iOS and iPadOS	Create a proxy profile and associate it with a Wi-Fior VPN profile. You can assign a proxy profile to user accounts, user groups, or device groups. A proxy profile that is assigned to user accounts, user groups, or device groups is a global proxy for supervised devices only and takes precedence over a proxy profile that is associated with a Wi-Fi or VPN profile. Supervised devices use the global proxy settings for all HTTP connections.
macOS	Create a proxy profile and associate it with a Wi-Fi or VPN profile. macOS applies profiles to user accounts or devices. Proxy profiles are applied to devices.

Device	Proxy configuration
Android	For Android Enterprise devices, create a proxy profile and associate it with a Wi-Fi profile. Android devices with MDM controls or User privacy activations don't support Wi-Fi profiles with proxy settings.
Samsung Knox	Create a proxy profile and associate it with a Wi-Fi, VPN, or enterprise connectivity profile. The following conditions apply: • For Wi-Fi profiles, only proxy profiles with manual configuration are supported on Knox devices. Proxy profiles that you associate with Wi-Fi profiles support proxy servers that use basic, NTLM, or no authentication. • For VPN and enterprise connectivity profiles, proxy profiles with manual configuration are supported on Samsung Knox devices with Android Enterprise activations and Samsung Knox Workspace devices that use Knox 2.5 and later. Proxy profiles with PAC configuration are supported on Samsung Knox devices with Android Enterprise activations and Knox Workspace devices that use a version of Knox that is later than 2.5. You can assign a proxy profile to user accounts, user groups, or device groups. The following conditions apply: • On Knox Workspace devices and Samsung Knox devices with Android Enterprise activations, the profile configures the browser proxy settings in the work space. • On Samsung Knox MDM devices, the profile configures the browser proxy settings on the device. • PAC configuration is not supported on Knox Workspace devices that use Knox 2.5 and earlier and Knox MDM devices.
Windows 10	Create a Wi-Fi or VPN profile and specify the proxy server information in the profile settings. The following conditions apply: • Wi-Fi proxy supports only manual configuration and is supported only on Windows 10 Mobile devices. • VPN proxy supports PAC or manual configuration.

Create a proxy profile

1. On the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > Proxy**.
3. Click +.
4. Type a name and description for the proxy profile.
5. Click the tab for a device type.
6. Perform one of the following tasks:

Task	Steps
Specify PAC configuration settings	**a.** In the **Type** drop-down list, click **PAC configuration**. **b.** In the **PAC URL** field, type the URL for the web server that hosts the PAC file and include the PAC file name (for example, http://www.example.com/PACfile.pac). The PAC file should not be hosted on a server that hosts UEM or any of its components.
Specify manual configuration settings	**a.** In the **Type** drop-down list, click **Manual configuration**. **b.** In the **Host** field, type the FQDN or IP address of the proxy server. **c.** In the **Port** field, type the port number of the proxy server. **d.** If your organization requires that users provide a username and password to connect to the proxy server and the profile is for multiple users, in the **Username** field, type `%UserName%`. If the proxy server requires the domain name for authentication, use the format *<domain>**<username>*.

7. Repeat steps 4 to 6 for each device type.
8. Click **Add**.

After you finish:

- Associate the proxy profile with a Wi-Fi, VPN, or enterprise connectivity profile.
- If you create more than one proxy profile, rank the profiles as necessary. The ranking that you specify applies only if you assign a proxy profile to user groups or device groups. Select a profile and click ⇅ to move the profile up or down the ranking. Click **Save**.

Using BlackBerry Secure Connect Plus for connections to work resources

BlackBerry Secure Connect Plus is a BlackBerry UEM component that provides a secure IP tunnel between apps and your organization's network:

- For Android Enterprise and Android Management devices, all work apps use the secure tunnel.
- For Samsung Knox Workspace devices and Samsung Knox devices with Android Enterprise activations, you can allow all work space apps to use the tunnel or specify apps using per-app VPN.
- For iOS and iPadOS devices, you can allow all apps to use the tunnel or specify apps using per-app VPN.

The secure IP tunnel gives users access to work resources behind your organization’s firewall while ensuring the security of data using standard protocols and end-to-end encryption.

Note: If BlackBerry Secure Connect Plus is not available in your region, you must manually disable it for Android devices in the Enterprise connectivity profile.

BlackBerry Secure Connect Plus and a supported device establish a secure IP tunnel when it is the best available option for connecting to the organization’s network. If a device is assigned a Wi-Fi profile or VPN profile, and the device can access the work Wi-Fi network or VPN, the device uses those methods to connect to the network. If those options are not available (for example, if the user is not in range of the work Wi-Fi network), then BlackBerry Secure Connect Plus and the device establish a secure IP tunnel.

Supported devices communicate with UEM to establish the secure tunnel through the BlackBerry Infrastructure. One tunnel is established for each device. The tunnel supports standard IPv4 protocols (TCP and UDP) and the IP

traffic that is sent between devices and UEM is encrypted end-to-end using AES256. As long as the tunnel is open, apps can access network resources. When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), it is terminated.

When you enable BlackBerry Secure Connect Plus, you perform the following actions:

Step	Action
1	Verify that your organization's BlackBerry UEM domain meets the requirements to use BlackBerry Secure Connect Plus.
2	Enable BlackBerry Secure Connect Plus in the Default enterprise connectivity profile or in a custom enterprise connectivity profile that you create.
3	Optionally, specify the DNS settings for the BlackBerry Connectivity app.
4	If you have an on-premises environment that includes Android Enterprise devices and Samsung Knox Workspace devices that are BlackBerry Dynamics enabled, optimize secure tunnel connections.
5	Assign the enterprise connectivity profile to user accounts and groups. If you assign an enterprise connectivity profile as the per-app VPN directly to an Android app, the enterprise connectivity profile does not take effect. Assigning an enterprise connectivity profile directly to an app as the per-app VPN is supported for iOS apps only. For Android devices, assign the enterprise connectivity profile to user groups or to user accounts.

If you configure per-app VPN for BlackBerry Secure Connect Plus for iOS and iPadOS devices, the configured apps always use a secure tunnel connection through BlackBerry Secure Connect Plus, even if the app can connect to the work Wi-Fi network or the VPN specified in a VPN profile.

You can associate an enterprise connectivity profile with an email, IMAP/POP3, CardDAV, and CalDAV profiles to enable iOS devices to use BlackBerry Secure Connect Plus as the per-account VPN for email, calendar, and contact data that is managed by these profiles. This is an alternative to associating per-account VPN profiles and provides the added benefit of leveraging BlackBerry's secure connectivity infrastructure. This option is turned off by default in email, IMAP/POP3, CardDAV, and CalDAV profiles. When enabled, the device will use the configuration of its assigned enterprise connectivity profile for the relevant secure connections.

Server and device requirements for BlackBerry Secure Connect Plus

To use BlackBerry Secure Connect Plus, your organization's environment must meet the following requirements.

For the BlackBerry UEM domain:

Environment	Requirements
All UEM environments	• Your organization's firewall must allow outbound connections over port 3101 to <*region*>.turnb.bbsecure.com and <*region*>.bbsecure.com. If you configure UEM to use a proxy server, verify that the proxy server allows connections over port 3101 to these subdomains. • In each UEM instance, the BlackBerry Secure Connect Plus component must be running. • By default, Android Enterprise and Android Management devices are restricted from using BlackBerry Secure Connect Plus to connect to Google Play and underlying services (com.android.providers.media, com.android.vending, and com.google.android.apps.gcs). Google Play does not have proxy support. Android Enterprise and Android Management devices use a direct connection over the Internet to Google Play. These restrictions are configured in the Default enterprise connectivity profile and in any new enterprise connectivity profiles that you create. It is recommended to keep these restrictions in place. If you remove these restrictions, you must contact Google Play support for the firewall configuration required to allow connections to Google Play using BlackBerry Secure Connect Plus. • If you use an email profile to enable the BlackBerry Secure Gateway for iOS devices, it is a best practice to configure per-app VPN for BlackBerry Secure Connect Plus.
UEM on-premises	• If your environment includes Knox Workspace, Android Enterprise devices with BlackBerry Dynamics apps, or Android Management devices with BlackBerry Dynamics apps, see Optimize secure tunnel connections for Android devices that use BlackBerry Dynamics apps. • Optionally, you can install additional BlackBerry Secure Connect Plus instances by installing more than one BlackBerry Connectivity Node. • Optionally, you can create a server group to direct BlackBerry Secure Connect Plus traffic to a specific regional path to the BlackBerry Infrastructure.
UEM Cloud	• You must install the BlackBerry Connectivity Node or upgrade to the latest version. When you install or upgrade the BlackBerry Connectivity Node, BlackBerry Secure Connect Plus is also installed or upgraded. You must make sure that you activate the BlackBerry Connectivity Node before you enable BlackBerry Secure Connect Plus. • If you route the data that travels between BlackBerry Secure Connect Plus and the BlackBerry Infrastructure through a TCP proxy server (transparent or SOCKS v5), you can configure the proxy settings using the BlackBerry Connectivity Node management console (General settings > Proxy).

For supported devices:

Profile	Description
iOS and iPadOS	• MDM controls activation type • DEP and non-DEP devices require the BlackBerry UEM Client to support BlackBerry Secure Connect Plus. Shared iPad devices are the exception to this requirement; shared iPad devices use DEP activation and do not require the UEM Client to support BlackBerry Secure Connect Plus.

Profile	Description
Android Enterprise	Any of the following activation types: • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - user privacy (Premium)
Android Management	Any of the following activation types: • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - user privacy (Premium)

Samsung Knox Workspace	• A supported version of Samsung Knox.
	• Any of the following activation types:
	  • Work and personal - full control (Samsung Knox)
	  • Work and personal - user privacy (Samsung Knox)

Enable BlackBerry Secure Connect Plus

To allow devices to use BlackBerry Secure Connect Plus, you must enable BlackBerry Secure Connect Plus in an enterprise connectivity profile and assign the profile to users and groups.

When the enterprise connectivity profile is applied to the device after activation, BlackBerry UEM installs the BlackBerry Connectivity app on the device (for Android Enterprise or Android Management devices, the app is installed automatically from Google Play; for iOS and iPadOS devices, the app is installed automatically from the App Store).

Before you begin: Verify that your organization's UEM domain meets the requirements to use BlackBerry Secure Connect Plus.

1. In the management console, on the menu bar, click **Policies and Profiles > Networks and connections > Enterprise connectivity**.
2. Edit an existing enterprise connectivity profile or create a new one.
3. If you created and configured one or more server groups to direct BlackBerry Secure Connect Plus traffic to a specific regional path to the BlackBerry Infrastructure, in the **BlackBerry Secure Connect Plus server group** drop-down list, click the appropriate server group.
4. Configure the appropriate values for the profile settings for each device type. For more information about each profile setting, see the Enterprise connectivity profile settings.
5. Click **Add**.
6. Assign the profile to groups or user accounts.

   Note: If you assign an enterprise connectivity profile as the per-app VPN directly to an Android app, the enterprise connectivity profile does not take effect. Assigning an enterprise connectivity profile directly to an app as the per-app VPN is supported for iOS apps only. For Android devices, assign the enterprise connectivity profile to user groups or to user accounts.

After you finish:

- On Android Enterprise, Android Management, and Samsung Knox Workspace devices, the BlackBerry Connectivity app prompts users to allow it to run as a VPN and to allow access to private keys on the device. Instruct users to accept the requests. Device users can open the app to view the status of the connection. No further action is required from users.

- If you created more than one enterprise connectivity profile, rank the profiles.
- If you want to enable iOS devices to use BlackBerry Secure Connect Plus as the per-account VPN for email, calendar, and contact data, enable this option in the appropriate email, IMAP/POP3, CardDAV, and CalDAV profiles. When enabled, the device will use its assigned enterprise connectivity profile for secure connections.
- If you are troubleshooting a connection issue, the app allows the user to send the device logs to an administrator's email address (the user enters an email address that you must provide). Note that the logs are not viewable with Winzip. It is recommended to use another utility such as 7-Zip.
- Optionally, specify the DNS settings for the BlackBerry Connectivity app.

Updating the BlackBerry Connectivity app

The latest BlackBerry Connectivity app is available in Google Play and from BlackBerry myAccount Software Downloads.

- **Android users:** Instruct device users to update to the latest versions of the BlackBerry UEM Client and the BlackBerry Connectivity app available in Google Play. For devices that don't have access to Google Play, follow the instructions in Update the BlackBerry Connectivity app for Samsung Knox Workspace, Android Enterprise, and Android Management devices that don't have access to Google Play.
- **Samsung Knox Workspace users:**
  - For Knox devices that have Google Play app management enabled, instruct device users to update to the latest versions of the BlackBerry UEM Client and the BlackBerry Connectivity app available in Google Play. In the UEM management console, make sure that you set the BlackBerry Connectivity app to be sent to “All Android devices” and assign it to the appropriate users and groups.
  - For Knox devices that don’t have Google Play app management enabled, follow the instructions in Update the BlackBerry Connectivity app for Samsung Knox Workspace, Android Enterprise, and Android Management devices that don't have access to Google Play.

Note: If you use CA certificate profiles to distribute CA certificates to Android or Knox Workspace devices, verify that the certificates that you uploaded are DER-encoded with a .der file extension, or PEM-encoded with a .pem file extension. CA certificates that do not meet these requirements might cause connection issues for the BlackBerry Connectivity app.

Update the BlackBerry Connectivity app for Samsung Knox Workspace, Android Enterprise, and Android Management devices that don't have access to Google Play

Follow the instructions below to update the BlackBerry Connectivity app on users' devices to the latest version.

To benefit from the latest server updates, it is a best practice to upgrade to the latest version of BlackBerry UEM.

Before you begin:

- Visit BlackBerry myAccount Software Downloads to download the latest version of the BlackBerry Connectivity app. Save the files on each computer that hosts a UEM instance.
- Instruct Knox Workspace device users to update the BlackBerry UEM Client to the latest version available in Google Play.
- For Knox Workspace activations, since the latest release of the BlackBerry Connectivity app is available in Google Play, users can update the app themselves. You must still complete the following steps to configure UEM to support the app.
- For Android Enterprise and Android Management activations, users can update to the latest release of the BlackBerry Connectivity app from Google Play themselves if Google Play is enabled in the workspace. You must still complete the following steps to configure UEM to support the app.
- To configure UEM to support the BlackBerry Connectivity app for devices that need BlackBerry Secure Connect Plus:

1. In the UEM management console, on the menu bar, click **Apps**.

2. Click > **Internal apps**.
3. Click **Browse** and select the .apk file for the latest BlackBerry Connectivity app for Android.
4. Click **Add**.
5. In the **Send to** field, select **All Android devices**.
6. Deselect **Publish app in Google domain**.
7. Click **Add**.
8. Assign the app that you added in the previous step to devices that don't have access to Google Play. The app disposition must be set to **Required**.

After you finish: UEM sends a policy update notification to the UEM Client on Knox Workspace devices. The UEM Client updates the BlackBerry Connectivity app when the app is assigned as a required app.

Enterprise connectivity profile settings

Enterprise connectivity profiles are supported on the following device types:

- iOS
- iPadOS
- Android

Common: Enterprise connectivity profile settings

Common: Compliance profile setting	Description
BlackBerry Secure Connect Plus server group	This setting specifies the server group that BlackBerry Secure Connect Plus uses to direct traffic to a specific regional path.

iOS: Enterprise connectivity profile settings

Settings for iOS also apply to iPadOS devices.

Setting	Description
Enable BlackBerry Secure Connect Plus	This setting specifies whether work apps use BlackBerry Secure Connect Plus for sending work data between devices and your network.
Enable VPN on demand	Select this setting to allow only specific apps to use BlackBerry Secure Connect Plus. **Note:** If you select this option, users must manually turn on the VPN connection on their device to use BlackBerry Secure Connect Plus. As long as the VPN connection is on, the device uses BlackBerry Secure Connect Plus to connect to the work network. The user must turn the VPN connection off to use another connection, such as the work Wi-Fi network. Instruct users when it is appropriate to turn on and turn off the VPN connection (for example, you can instruct users to turn on the VPN connection when they are not in range of the work Wi-Fi network).

Setting	Description
VPN on demand rules for iOS 9 and later	This setting specifies the connection requirements for VPN on demand using BlackBerry Secure Connect Plus. You must use one or more keys from the payload format example. This setting is valid only if the "Enable VPN on demand" setting is selected.
Enable per-app VPN	This setting specifies whether work apps can automatically start a VPN connection using BlackBerry Secure Connect Plus when it accesses work resources. Select this setting to specify rules for BlackBerry Secure Connect Plus connections.
Safari domains	Specify the domains that are allowed to start a VPN connection in Safari.
Associated domains	Specify the associated domains.
Allow apps to connect automatically	Specify whether apps can start the VPN connection automatically.
Proxy profile	This setting specifies the associated proxy profile if you want to route secure tunnel traffic from devices to the work network through a proxy server. The proxy profile must use a manual configuration with an IP address. PAC configuration is not supported. For more information, see Setting up proxy profiles for devices.

Android: Enterprise connectivity profile settings

Setting	Description
Enable BlackBerry Secure Connect Plus	This setting specifies whether work apps use BlackBerry Secure Connect Plus for sending work data between devices and your network.
Enterprise connectivity for Android devices with a work space	This setting specifies whether Android Enterprise, Android Management, and Samsung Knox Workspace devices use BlackBerry Secure Connect Plus for all apps in the work space, or only for specified apps. • "Container wide VPN" uses a VPN connection for all apps in the work space on the device. • "Per-app VPN" uses a VPN connection only for specified apps.

Setting	Description
Apps restricted from using BlackBerry Secure Connect Plus	This setting specifies apps in the work space on Android Enterprise and Android Management devices that are not allowed to use BlackBerry Secure Connect Plus. This setting is valid only if the "Enterprise connectivity for Android devices with a work space" setting is set to "Container wide VPN." If the “Force work apps to only use VPN” IT policy rule is applied to the device, this setting is ignored and no work apps, including the BlackBerry UEM Client and Google Play, are restricted from using BlackBerry Secure Connect Plus. In this case you will have to open ports in the firewall to allow the UEM Client to communicate with the BlackBerry Infrastructure through UEM. For more information about opening ports in the firewall when work apps use BlackBerry Secure Connect Plus, see KB 48330. If your organization uses BlackBerry Dynamics apps, it is recommended that you restrict the apps from using BlackBerry Secure Connect Plus. If you don't, you must open additional ports in your organization’s firewall to allow the apps to send data to the BlackBerry Dynamics NOC, and network activity from the apps might be delayed because data is routed to both the BlackBerry Infrastructure and BlackBerry Dynamics NOC. See Optimize secure tunnel connections for Android devices that use BlackBerry Dynamics apps. As of UEM Client version 12.45.0.158273, if a user is assigned an Intercede user credential profile and an enterprise connectivity profile with "Container wide VPN" enabled, by default the UEM Client will route container wide VPN traffic through BlackBerry Secure Connect Plus to UEM. If you do not want the UEM Client to route traffic through BlackBerry Secure Connect Plus, add the package ID of the UEM Client to the restricted apps list.
Apps allowed to use Enterprise Connectivity	This setting specifies apps in the work space on Android Enterprise, Android Management, and Samsung Knox Workspace devices that are allowed to use BlackBerry Secure Connect Plus. You can select apps from a list of available apps or specify the app package ID. This setting is valid only if the "Enterprise connectivity for Android devices with a work space" setting is set to "Per-app VPN."
Proxy profile	You can select a proxy profile that you configured to route secure tunnel traffic through a proxy server. This option is supported for devices with Android Enterprise and Android Management activation types. BlackBerry Secure Connect Plus supports both PAC configuration and manual configuration of the proxy server in the proxy profile, but take note of the limitations detailed under setHttpProxy from developer.android.com. Web proxy support for BlackBerry Secure Connect Plus requires the BlackBerry Connectivity app version 1.0.25.x or later and UEM Client 12.44.x or later.

Specify the DNS settings for the BlackBerry Connectivity app

You can specify the DNS servers that you want the BlackBerry Connectivity app to use for secure tunnel connections. If you do not specify DNS settings, the app obtains DNS addresses from the computer that hosts the BlackBerry Secure Connect Plus component, and the default search suffix is the DNS domain of that computer.

1. Perform one of the following actions:

- In an on-premises environment, in the UEM management console, on the menu bar click **Settings > Infrastructure > BlackBerry Secure Connect Plus**.
- In a cloud environment, in the BlackBerry Connectivity Node console (http://localhost:8088), in the left pane, click **General settings > BlackBerry Secure Connect Plus**.

2. Select the **Manually configure DNS servers** check box and click +.
3. Type the DNS server address in dot-decimal notation (for example, 192.0.2.0). Click **Add**.
4. If necessary, repeat steps 2 and 3 to add more DNS servers. In the **DNS servers** table, click the arrows in the **Ranking** column to set the priority for the DNS servers.
5. If you want to specify DNS search suffixes, complete the following steps:
   a) Select the **Manage DNS search suffixes manually** check box and click +.
   b) Type the DNS search suffix (for example, domain.com). Click **Add**.
6. If necessary, repeat step 5 to add more DNS search suffixes. In the **DNS search suffix** table, click the arrows in the **Ranking** column to set the priority for the DNS servers.
7. Click **Save**.

Optimize secure tunnel connections for Android devices that use BlackBerry Dynamics apps

If you enable BlackBerry Secure Connect Plus and you have an on-premises environment that includes BlackBerry Dynamics apps installed on Android Enterprise or Android Management devices, or Samsung Knox Workspace devices, it is recommended that you configure the BlackBerry Dynamics connectivity profile assigned to these devices to disable BlackBerry Proxy. Using both BlackBerry Proxy and BlackBerry Secure Connect Plus might delay network activity from the apps because the data is routed to both network components.

1. In the management console, on the menu bar, click **Policies and Profiles > Networks and connections > BlackBerry Dynamics connectivity**.
2. Edit the profile that is assigned to devices.
3. Clear the **Route all traffic** check box.
4. In the **Default allowed domain route type** section, select **Direct** to route traffic directly from the app to the domain without going through BlackBerry Proxy.
5. Click **Save**.

Troubleshooting BlackBerry Secure Connect Plus

Consider the following issues if you are having trouble setting up BlackBerry Secure Connect Plus.

BlackBerry Secure Connect Plus does not start

Possible cause

The TCP/IPv4 settings for the BlackBerry Secure Connect Plus Adapter might not be correct.

Possible solution

In **Network Connections > BlackBerry Secure Connect Plus Adapter > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties**, verify that **Use the following IP address** is selected, with the following default values:

- IP address: 172.16.0.1
- Subnet mask: 255.255.0.0

If necessary, correct these settings and restart the server.

BlackBerry Secure Connect Plus stops working after a BlackBerry UEM installation or upgrade

Cause

This issue might occur if the server wasn't restarted during an RRAS update before BlackBerry UEM is upgraded in an on-premises environment, which causes NAT/routing setup to fail during the upgrade. This issue might also occur after a new installation of UEM.

Solution

1. Restart the server.
2. In the Windows Services, stop the **BlackBerry UEM – BlackBerry Secure Connect Plus** service.
3. As an administrator, start Windows PowerShell (64-bit) or open a command prompt.
4. Navigate to `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` and Run **configureRRAS.bat**
5. Navigate to `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\` and Run **configure-network-interface.cmd**
6. In the Windows Services, start the **BlackBerry UEM – BlackBerry Secure Connect Plus** service.

View the log files for BlackBerry Secure Connect Plus

Two log files record data about BlackBerry Secure Connect Plus:

- BSCP: log data about the BlackBerry Secure Connect Plus server component
- BSCP-TS: log data for connections with the BlackBerry Connectivity app

In an on-premises environment, the files are located by default at *<drive>*:\Program Files\BlackBerry\UEM\Logs*<yyyymmdd>*. On each computer that hosts a BlackBerry Connectivity Node instance, the log files for BlackBerry Secure Connect Plus are located at *<drive>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs*<yyyymmdd>*.

In a cloud environment, on each computer that hosts a BlackBerry Connectivity Node instance, the log files are located by default at *<drive>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs*<yyyymmdd>*.

Purpose	Log file	Example
Verify that BlackBerry Secure Connect Plus is connected to the BlackBerry Infrastructure	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]
Verify that BlackBerry Secure Connect Plus is ready to receive calls from the BlackBerry Connectivity app on devices	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created

Purpose	Log file	Example
Verify that devices are using the secure tunnel	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249

Using BlackBerry 2FA for secure connections to critical resources

BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. BlackBerry 2FA uses a password that users enter and a secure prompt on their mobile device each time they attempt to access resources.

You manage BlackBerry 2FA from the BlackBerry UEM management console, where you use a BlackBerry 2FA profile to enable two-factor authentication for your users. To use the latest version of BlackBerry 2FA and its associated features, such as preauthentication and self-rescue, your users must have the BlackBerry 2FA profile assigned to them. For more information, see the BlackBerry 2FA content.

Setting up up automatic authentication for iOS devices

You can enable iOS devices to authenticate automatically with hosts or domains and web services in your organization's network. You configure this single sign-on authentication using either of the following profiles:

- Single sign-on extension profile: You can specify settings for a custom extension or use the Kerberos extension provided by Apple. This profile is an updated version of the basic single sign-on profile and offers advanced configuration options.
- Single sign-on profile: The legacy profile that offers basic configuration for single sign-on authentication using Kerberos.

After you assign the profile, the user is prompted for a username and password the first time they try to access a secure host or domain that you specified. The login information is saved on the user's device and used automatically when the user tries to access any of the secure hosts or domains specified in the profile. When the user changes the password, the user is prompted the next time they try to access a secure host or domain.

Enable automatic authentication for iOS devices using a single sign-on extension profile

Before you begin:

- Single sign-on extension profiles are supported for devices with the MDM controls activation type, or with the User privacy activation type with management of all profiles enabled. For more information, see Activation types: iOS devices.
- If you want to use certificate-based authentication, you must first create a shared certificate profile, SCEP profile, or user credential profile.

1. In the management console, on the menu bar, click **Policies and profiles > Networks and connections > Single sign-on extension**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Single sign-on extension type** drop-down list, click **Custom extension** or **Kerberos built-in extension**.

Task	Steps
If you selected **Custom extenstion**	**a.** In the **Extension identifier** field, type the identifier for the app that performs the single sign-on. **b.** Select the appropriate sign-on type. **c.** If you selected **Credential** as the sign-on type, perform the following steps: **1.** In the **Realm** field, type the realm name for the credential. **2.** In the **Domains** section, click + to add a host or domain. **3.** In the **Name** field, type the host or domain for which the app extension performs single sign-on. **4.** Add additional hosts or domains as required. **d.** If you selected **Redirect** as the sign-on type, perform the following steps: **1.** In the **URLs** section, click + to add a URL. **2.** In the **Name** field, type the URL prefix for the identity provider for which the app extension performs single sign-on. Add additional URLs as required. **e.** In the **Custom payload code** field, enter the custom payload code for the app extension.
If you selected **Kerberos built-in extension**	**a.** In the **Domains** section, click + to add a host or domain. **b.** In the **Realm name** field, type the realm name for the credential. **c.** Select the appropriate **Apple Kerberos SSO extension data** for your environment. By default, automatic login and Active Directory autodiscovery are allowed. You can also specify the default realm, allow only managed apps to use single sign-on, and require users to confirm access. **d.** Set the **Principal name** for the connection. **e.** If you want to use a certificate profile to provide the PKINIT certificate for authentication, select the profile type from the **Select the PKINIT certificate for authentication** drop-down list and then select the appropriate profile. **f.** If you're using the Generic Security Service API, specify the **GSS name of the Kerberos cache**. **g.** In the **App bundle identifiers** section, click + to specify the bundle IDs that are allowed to access the ticket-granting ticket. **h.** In the **Preferred key distribution centers** section, click + to specify preferred servers if they are not discoverable using DNS. Specify each server in the same format used in a krb5.conf file. The specified servers are used for connectivity checks and tried first for Kerberos traffic. If the servers do not respond, the device uses DNS discovery. **i.** In the **Custom domain-realm mapping** field, enter any required custom mapping of domains to realm names in payload format, for example `<key>sample-realm1</key><array><string>org</string></array>`. **j.** In the **Login hint** field, specify text to display at bottom of the Kerberos login window.

5. Click **Save**.

After you finish: Assign the profile to user accounts and groups.

Enable automatic authentication for iOS devices using a single sign-on profile

The single sign-on profile is a legacy profile with basic configuration options. If you want to use the more advanced single sign-on extension profile, see Enable automatic authentication for iOS devices using a single sign-on extension profile.

Before you begin: If you want to use certificate-based authentication, you must first create a shared certificate profile, SCEP profile, or user credential profile.

1. In the management console, on the menu bar, click **Policies and profiles > Networks and connections > Single sign-on**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Kerberos** section, click +.
5. In the **Name** field, type a name for the configuration.
6. In the **Principal name** field, type the name of the Kerberos Principal, using the format *<primary>/<instance>@<realm>* (for example, user/admin@blackberry.example.com).
7. In the **Realm** field, type the Kerberos realm in uppercase letters (for example, EXAMPLE.COM).
8. In the **URL prefixes** field, type the URL prefix for the sites that you want devices to authenticate with. The prefix must begin with http:// or https://, and can include wildcard values (*) (for example, https://www.blackberry.example.com/*).

   If necessary, click + to add additional URL prefixes.
9. If you want to limit the configuration to specific apps, click + beside **App identifiers** and specify the app bundle ID. You can use a wildcard value (*) to match the ID to multiple apps (for example, com.company.*).

   If necessary, click + to add additional URL prefixes.
10. If you want iOS devices to use certificate-based authentication, in the **Credentials** drop-down list, click **Certificate**, **SCEP**, or **User credential**. In the drop-down list, click the certificate profile that you want to use.
11. Click **Add**.
12. Click **Add** again.

After you finish:

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

Specify DNS servers for iOS and macOS devices

You can specify the DNS servers that you want to use to access specific domains. This setting can help provide a faster and safer web browsing experience.

1. In the management console, on the menu bar, click **Policies and profiles > Networks and connections > DNS**.
2. Click +.
3. Type a name and description for the profile.
4. Click the tab for a device type.
5. Select the DNS protocol used to communicate with the DNS server.
6. Do one of the following:
   a) If you selected **HTTPS**, type the URI template of the DNS-over-HTTPS server using the https:// scheme.
   b) If you selected **TLS**, type the hostname of the DNS-over-TLS server.

7. To prevent users from disabling the settings, select the **Do not allow user to disable DNS settings** check box. This option affects supervised devices only.
8. In the **DNS addresses** field, specify the list of IP addresses for any DNS servers that you want to use. These can be a mixture of IPv4 and IPv6 addresses.
9. In the **Domains** field, specify the list of domain strings that will be used to determine which DNS queries will use the DNS servers.
10. In the **DNS on demand rules** field, specify the DNS on demand rules using the sample payload format.
11. Repeat steps 5 to 10 for each device type.
12. Click **Save**.

Specify email and web domains for iOS devices

You can use a managed domains profile to define certain email domains and web domains as "managed domains" that are internal to your organization. Managed domains profiles apply only to iOS and iPadOS devices with the MDM controls activation type.

After you assign a managed domains profile:

- When a user creates an email message and adds a recipient email address with a domain that is not specified in the managed domains profile, the device displays the address in red to warn the user that the recipient is external to the organization. The device does not prevent the user from sending email to external recipients.
- A user must use an app that is managed by BlackBerry UEM to view documents from a managed web domain or documents downloaded from a managed web domain. The device does not prevent the user from visiting or viewing documents from other web domains. The managed domains profile applies to the Safari browser only.

1. On the menu bar, click **Policies and profiles > Networks and connections > Managed domains**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Description** field, type a description for the profile.
5. In the **Managed domains** section, click +.
6. In the **Email domains** field, type a top-level domain name (for example, `example.com` instead of `example.com/canada`).
7. Click **Add**.
8. In the **Managed web domains** section, click +. For examples of web domain formats, see Managed Safari Web Domains in the iOS Developer Library.
9. In the **Web domains** field, type a domain name.
10. If you want to allow password autofill for the web domains that you specified, select the **Allow password autofill** check box. This option is supported only for supervised devices.
11. Click **Add**, then click **Add** again.

After you finish: Assign the managed domains to user accounts, user groups, or device groups.

Control network usage for apps on iOS devices

You can use a network usage profile to control how apps on iOS and iPadOS devices use the mobile network. To help manage network usage, you can prevent specified apps from transferring data when devices are connected to the mobile network or when devices are roaming. A network usage profile can contain rules for one app or multiple apps.

The rules in a network usage profile apply to work apps only. If you have not assigned apps to users or groups, the network usage profile does not have any effect.

Before you begin: Add apps to the app list and assign them to users and groups.

1. In the management console, on the menu bar, click **Policies and Profiles > Networks and connections > Network usage**.
2. Click +.
3. Type a name and description for the profile.
4. Click +.
5. Perform one of the following actions:
   - Click **Add an app** and click on an app in the list.
   - Select the **Specify the app package ID** option and type the ID. The app package ID is also known as the bundle ID. You can find the App package ID by clicking the app in the app list. Use a wildcard value (*) to match the ID to multiple apps. (For example, **com.company.***).
6. To prevent the app or apps from using data when the device is roaming, clear the **Allow data roaming** check box.
7. To prevent the app or apps from using data when the device is connected to the mobile network, clear the **Allow cellular data** check box.
8. Click **Add**.
9. Repeat steps 5 to 9 for each app that you want to add to the list.

After you finish: If you created more than one network usage profile, rank profiles. Select a profile and click ↓↑ to move the profile up or down the ranking. Click **Save**

Assign the network usage profile to user accounts, user groups, or device groups.

Create a web content filter profile on iOS devices

You can use web content filter profiles to limit the websites that a user can view in Safari or other browser apps on a supervised iOS or iPadOS device. You can assign web content filter profiles to user accounts, user groups, or device groups. When you create a web content filter profile, each URL that you specify must begin with http:// or https://. If necessary, you should add separate entries for http:// and https:// versions of the same URL. DNS resolution does not occur, so restricted websites could still be accessible (for example, if you specify http://www.example.com, users might be able to access the website using the IP address).

When you create a web content filter profile, you can choose the allowed websites option that supports your organization's standards for the use of mobile devices.

Allowed websites	Description
Specific websites only	This option allows access to only the websites that you specify. A bookmark is created in Safari for each allowed website. If you allow access only to specific websites, you must ensure that all websites that the device needs to access are specified in the list of allowed websites. For example, if you configure Microsoft Office 365 modern authentication for BlackBerry Dynamics apps, the device must be able to reach the Active Directory Federation Services website.

Allowed websites	Description
Limit adult content	This option enables automatic filtering to identify and block inappropriate content. You can also include specific websites using the following settings: • Permitted URLs: You can add one or more URLs to allow access to specific websites. Users can view websites in this list regardless of whether automatic filtering blocks access. • Blacklisted URLs: You can add one or more URLs to deny access to specific websites. Users cannot view websites in this list regardless of whether automatic filtering allows access.

1. On the menu bar, click **Policies and Profiles > Networks and connections > Web content filter**.
2. Click +.
3. Type a name and description for the web content filter profile.
4. Perform one of the following tasks:

Task	Steps
Allow access to specific websites only	**a.** In the **Allowed websites** drop-down list, verify that **Specific websites only** is selected. **b.** In the **Specific website bookmarks** section, click +. **c.** Perform the following actions: **1.** In the **URL** field, type a web address that you want to allow access to. **2.** Optionally, in the **Bookmark path** field, type the name of a bookmark folder (for example, /Work/). **3.** In the **Title** field, type a name for the website. **4.** Click **Add**. **d.** Repeat steps b and c for each allowed website.
Limit adult content	**a.** In the **Allowed websites** drop-down list, click **Limit adult content** to enable automatic filtering. **b.** Optionally, perform the following actions: **1.** Click + beside **Permitted URLs**. **2.** Type a web address that you want to allow access to. **3.** Repeat as necessary to add additional websites. **c.** Optionally, perform the following actions: **1.** Click + beside **Blacklisted URLs**. **2.** Type a web address that you want to deny access to. **3.** Repeat as necessary to add additional websites.

5. Click **Add**.

After you finish: Assign the web content filter profile to user accounts, user groups, or device groups.

Create an AirPrint profile for iOS devices

AirPrint profiles can help users find printers that support AirPrint, are accessible to them, and for which they have the required permissions. In situations where protocols such as Bonjour can't discover AirPrint enabled printers on another subnetwork, AirPrint profiles specify where resources are located. You can configure and assign AirPrint profiles to iOS andiPadOS devices so that users don’t have to configure printers manually.

1. On the menu bar, click **Policies and Profiles > Networks and connections > AirPrint**.
2. Click +.
3. Type a name and description for the profile.
4. In the **AirPrint configuration** section, click +.
5. In the **IP Address** field, type the IP address of the printer or AirPrint server.
6. In the **Resource Path** field, type the resource path of the printer.
   The printer's resource path corresponds to the `rp` parameter of the `_ipps.tcp` Bonjour record. For example:
   - printers/<*printer series*>
   - printers/<*printer model*>
   - ipp/print
   - IPP_Printer
7. Optionally, if AirPrint connections are secured by TLS, select the **Force TLS** checkbox.
8. Optionally, if the port differs from the default for the Internet Printing Protocol, type the port number in the **Port** field.
9. Click **Add**, then click **Add** again.

After you finish: Assign the AirPrint profile to user accounts, user groups, or device groups.

Create an AirPlay profile for iOS devices

AirPlay is a feature that lets you display photos or stream music and video to compatible AirPlay devices such as AppleTV, AirPort Express, or AirPlay enabled speakers.

With an AirPlay profile you can specify which AirPlay devices iOS and iPadOS users can connect to. The AirPlay profile has two options:

- If your organization's AirPlay devices are password protected, you can specify device passwords for allowed destination devices so that iOS and iPadOS device users are able to connect without knowing the password.
- For supervised devices, you can restrict which AirPlay devices users can connect to by specifying a list of allowed AirPlay devices for supervised devices. Supervised devices can connect only to the AirPlay devices specified in the list. If you don't create a list, supervised devices can connect to any AirPlay device.

1. On the menu bar, click **Policies and Profiles > Networks and connections > AirPlay**.
2. Click +.
3. Type a name and description for the AirPlay profile.
4. Click + in the **Allowed destination devices** section.
5. In the **Device name** field, type the name of the AirPlay device you want to provide the password for. You can find the name of the AirPlay device in the device settings or you can look up the name of the device by tapping **AirPlay** in the Control Center of an iOS or iPadOS device to see a list of available AirPlay devices near you.
6. In the **Password** field, type a password.
7. Click **Add**.

8. Click + in the **Allowed destination devices for supervised devices** section.
9. In the **Device ID** field, type the device ID of the AirPlay device you want to allow supervised devices to connect to. You can find the device ID of the AirPlay device in the device settings. Supervised devices can connect only to AirPlay devices in the list.
10. Click **Add**.

After you finish: Assign the AirPlay profile to user accounts, user groups, or device groups.

Create an Access Point Name profile for Android devices

An APN specifies the information a mobile device needs to connect to a carrier's network. You can use one or more Access Point Name profiles to send APNs for carriers to your users' Android devices. Access Point Name profiles are supported by devices with Work space only activations or with Work and personal - full control activations.

Devices usually have APNs preset for common carriers. Users can also add new APNs to a device. If you want to force a device to use an APN sent to it by an Access Point Name profile, select the "Force device to use Access Point Name profile settings" check box in the IT policy rule.

Before you begin: Obtain all of the necessary APN settings from your carrier.

1. On the menu bar, click **Policies and Profiles > Networks and connections > Access Point Name**.
2. Click +.
3. Type a name and description for the profile. This information is displayed on devices.
4. In the **Access Point Name** field, type the access point name.
5. Specify the values that match the carrier's specifications for each profile setting.
   For more information, see Access Point Name profile settings.
6. Click **Save**.

After you finish: Assign the Access Point Name profile to user accounts, user groups, or device groups.

Access Point Name profile settings

Access Point Name profile setting	Description
Access Point Name	This setting specifies the Access Point Name (APN) that your device should use when it communicates with the carrier. The APN is a short string of text.
APN type bitmask	This setting specifies the types of data communication that use this APN configuration. Different types of communications may use different configurations.
Proxy address	This setting specifies the HTTP proxy to use for all web traffic over the connection. This setting is not required for most carriers.
Proxy port	This setting specifies the HTTP proxy port to use for all web traffic over the connection. This setting is not required for most carriers.
MMSC	This setting specifies the Multimedia Messaging Service Center (MMSC) to use for sending and receiving MMS messages.

Access Point Name profile setting	Description
MMS proxy address	This setting specifies the HTTP proxy for communicating with the MMSC to send and receive MMS messages.
MMS proxy port	This setting specifies the HTTP proxy port for communicating with the MMSC to send and receive MMS messages.
Authentication type	This setting specifies the authentication type used for communications.
Username	If the "Authentication type" setting is set to something other than NONE, specify a username if it is required for authentication.
Password	If the "Authentication type" setting is set to something other than NONE, specify a password if it is required for authentication.
Mobile country code (MCC)	This setting specifies the Mobile Country Code for the carrier network that the APN configuration should be used for.
Mobile network code (MNC)	This setting specifies the Mobile Network Code for the carrier network that the APN configuration should be used for.
Protocol	This setting specifies whether to enable IPv4, IPv6, or both on the home network for devices that support IPv6 networking.
Roaming protocol	This setting specifies whether to enable IPv4, IPv6, or both while roaming for devices that support IPv6 networking.
Carrier enabled	This setting specifies whether the APN is enabled for the carrier.
MVNO type	This setting specifies whether to restrict use of this APN to certain MVNOs (mobile network resellers) or subscriber accounts.

Using PKI certificates with devices or apps

A PKI certificate is a digital document issued by a Certificate Authority (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 securely and 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. The CA can later revoke trust of the certificate, in case of a breach.

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

- Authenticate using SSL/TLS when connecting to web servers that support mutual TLS, including 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. BlackBerry UEM provides a number of profiles to help manage the PKI certificates on the device. For example:

- CA server trust can be assigned to devices and apps using a CA certificate profile.
- Automatic enrollment of certificates can be assigned to devices and apps using SCEP, ACME, and user credential profiles.
- Retrieval of public encryption certificates can be assigned to devices and apps using a certificate retrieval profile.
- Checking the certificate revocation status can be assigned to devices and apps using OCSP and CRL profiles.

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

Step	Action
1	If necessary, integrate UEM with your organization's PKI software.
2	Create one or more CA certificate profiles to send CA certificates to devices and apps.
3	Create SCEP, ACME, 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 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 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 UEM to the Entrust software.
- the Entrust CA certificate that contains the public key (.der, .pem, or .cert); UEM uses this certificate to establish SSL connections to the Entrust server.

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

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. In the management console, on the menu bar, click **Settings > External integration > Certificate authority**.
2. Click **Add a connection for Entrust smart credentials**.
3. In the **Smart credential name** field, type the name of the smart credential specified in Entrust IdentityGuard.

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

After you finish:

- Create a user credential profile to send certificates from your PKI software to devices.
- When you use the 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.
- If you make changes to your organization's OpenTrust software, verify that you update the URL for the OpenTrust connection in the management console. User credential profiles cannot be used to deliver certificates from OpenTrust if the URL is not valid.

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 UEM to the PKI connector. In a BlackBerry UEM Cloud environment, you must have a BlackBerry Connectivity Node installed to allow UEM to communicate with the PKI connector through the BlackBerry Cloud Connector.

For more information about setting up a BlackBerry Dynamics PKI connector, see the User Certificate Management Protocol and PKI Connector documentation.

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

1. In the management console, 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 UEM authenticates with the BlackBerry Dynamics PKI Connector using password-based authentication.
   - **Authenticate with client certificate**: Choose this option if 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 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, click **Browse** to navigate to and select your organization's CA certificate.
   - **PKI connector server certificate**: If you select this option, 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.

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 UEM.

1. In the management console, 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 UEM Client.
4. Click **Add**.

After you finish: Do any of the following:

- Create 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.

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 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
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 macOS (for BlackBerry Access only) Android Windows 10 (for BlackBerry Access only)
Shared certificate profiles	A shared certificate profile specifies a client certificate that UEM sends to iOS, macOS, and Android devices. 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. 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

How the certificate is added	Description	Supported devices
User upload to UEM Self-Service	Users can upload certificates to BlackBerry UEM Self-Service. 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.	iOS Android
User import	Users can add certificates to the device native keystore for use with BlackBerry Dynamics apps.	Android

Sending certificates to devices and apps using profiles

You can send certificates to devices and apps using the following profiles:

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: • Specify a connection to your organization's PKI software to send client certificates to devices and BlackBerry Dynamics apps. • Manually upload certificates in BlackBerry UEM and, in an on-premises environment, allow users to upload certificates using BlackBerry UEM Self-Service. • Allow BlackBerry Dynamics apps on Android devices and the BlackBerry Access app on macOS and Windows 10 devices to use certificates from the device native keystore. • Allow BlackBerry Dynamics apps to import certificates from other app-based PKI solutions such as Purebred.
User credential Intercede	User credential Intercede profiles can be configured and assigned to enable a user to use the UEM Client to activate their device with Intercede MyID and download derived credentials certificates from MyID to the BlackBerry Dynamics keystore, or to the BlackBerry Dynamics keystore and the device's native key chain. See Use Intercede MyID to provide derived credentials certificates to devices.
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.

Profile	Description
ACME	ACME profiles specify how devices obtain client certificates from your organization's CA using an ACME solution. Note that BlackBerry Dynamics apps do not currently support the use of ACME to obtain and manage client certificates.
Shared certificate	Shared certificate profiles specify a client certificate that UEM sends to iOS and Android devices. 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 and manage a client certificate for a user account.

For iOS and Android 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" for the specific app on the **App** screen, **Settings > BlackBerry Dynamics** tab.

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:

- If you have set up a connection between 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.
- Android Enterprise devices don't support using certificates sent to devices by 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, ACME, 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. In the management console, on the menu bar, click **Policies and Profiles > Certificates > CA certificate**.
2. Click +.
3. 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.
4. In the **Certificate file** field, click **Browse** to locate the certificate file.
5. 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**.
6. Click **Add**.

After you finish: Assign the CA certificate profile to user accounts, user groups, or device groups.

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 UEM.
- An established connection between 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.

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

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 > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile. Each certificate profile must have a unique name.
4. In the **Certificate authority connection** drop-down list, select **Manually uploaded certificate**.
5. 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 the **Hide certificate on Android Enterprise devices** check box.
6. 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 and Android devices. If the connection is to Entrust PKI software, the user credential profile can also enroll certificates for BlackBerry Dynamics apps.

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.
- Ask the Entrust or OpenTrust administrator for the profile values that you must provide.
- 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 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 > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile. Each certificate profile must have a unique name.
4. In the **Certificate authority connection** drop-down list, select the Entrust or OpenTrust connection that you configured.
5. In the **Profile** drop-down list, click the appropriate profile.
6. Specify the values for the profile.

   You can use variables to populate specific values. You can view the list of default variables in Settings > General settings > Default variables.
7. 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.

      You can use variables for the SAN values. For example, you can use `%UserEmailAddress%` for "RFC822 name", `%UserPrincipalName%` for "NT principal name", or `tag:microsoft.com,2022-09-14:sid:%UserAdSid%` for "URI"). Some variables require UEM to be synchronized with your organization's company directory.
8. Specify the **Renewal period** for the certificate. The period can be between 1 and 120 days.
9. 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**.
10. 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 the password that 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.

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 > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Certificate authority connection** drop-down list, select the Entrust smart credential connection that you configured.
5. 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.
6. If the smart credential will be sent to Samsung Knox Workspace devices or apps other than BlackBerry Dynamics apps on Android Enterprise devices, on the **Android** tab, select the **Deliver to built-in key chain** check box.

   If this setting is not selected, the smart credential can be used only by BlackBerry Dynamics apps.
7. If the smart credential will be sent to BlackBerry Dynamics apps, on the **BlackBerry Dynamics** tab, do the following:
   a) If you want to allow users to dismiss certificate enrollment and complete it later, select **Allow optional certificate enrollment**. Optional certificate enrollment is supported for iOS and Android devices for the following user credential profile types: Device (App) Based Provider, Entrust Smart Credential and Native Keystore.
   b) If you want the device to delete duplicate credentials, select **Delete duplicate certificates**. The device deletes the credential that has the earliest start date.
   c) If you want the device to delete expired credentials, select **Delete expired certificates**.
   d) To allow all BlackBerry Dynamics apps to use the smart credentials, select **Allow all apps to use certificates**.
   e) 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.
8. 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 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 UEM Client before you unassign the profile or remove the certificate.

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

You can configure the user credential profile to use certificates from the native keystore in the following situations:

- To allow BlackBerry Dynamics apps to use a certificate from the native keystore on Android devices.
- To allow BlackBerry Dynamics apps to use a certificate from the native keystore to access cryptographic tokens from PKI apps on iOS devices.
- To allow the BlackBerry Access app to use a certificate from the native keystore on macOS or Windows 10 devices.

You can allow the 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.

Note: "Native keystore" refers to the keystore on the device. All user credential profiles with Native keystore connectors should be assigned to the user before they start discovering certificates. If a certificate meets the requirements of more than one UCP the best match is chosen.

1. On the menu bar, click **Policies and profiles > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile. Each certificate profile must have a unique name.
4. In the **Certificate authority connection** drop-down list, select **Native keystore**.
5. In the **Supported platforms** section, select the device OS types that you want this profile to support.
6. In the **Certificate enrollment** section, select the **Allow optional certificate enrollment** check box if you want to allow Android users to dismiss certificate enrollment and complete it later.
7. 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
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 the **Remove duplicate certificate**check box.
10. Click **Add**.

After you finish:

- To allow BlackBerry Dynamics apps to use certificates, on the menu bar, click **Apps**. Click the BlackBerry Dynamics app that you want to change, then on the **Settings > BlackBerry Dynamics** tab, select the **Allow BlackBerry Dynamics apps to use user certificates SCEP profiles, and user credential profiles** checkbox.
- 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 > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Certificate authority connection** drop-down list, click the BlackBerry Dynamics PKI connection that you configured.
5. If the user must provide a password to request a certificate, select **Require user-entered password or OTP**.
6. 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.
7. If you want the device to delete expired certificates, select the **Delete expired certificate** check box.
8. If you want the device to delete duplicate certificates, select the **Remove duplicate certificate** check box.
9. Click **Add**.

After you finish:

- To allow BlackBerry Dynamics apps to use certificates, on the menu bar, click **Apps**. Click the BlackBerry Dynamics app that you want to change, then on the **Settings > BlackBerry Dynamics** tab, select the **Allow BlackBerry Dynamics apps to use user certificates SCEP profiles, and user credential profiles** checkbox.
- 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.
- If you want to renew the certificates that are enrolled though the PKI connector, click **Refresh PKI capabilities > 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 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.

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 the 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	Use the app-based PKI solution with the following devices: • iOS devices: create a user credential profile to use app-based certificates. • 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 management console, on the menu bar, click **Apps**.
2. In the app list, click the BlackBerry UEM Client.
3. In the **App configuration** section, click + **> Create new**.
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. If you are using the Purebred app, use one of the following schemes:
   - Purebred Registration 2025 app: `purebred2025.select.all-user`, `purebred2025.select.no-filter`, `purebred2025.zip.all-user`, `purebred2025.zip.no-filter`
   - Pre-2025 Purebred app: `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter`

   Note that the UTI schemes for the Purebred 2025 app take precedence over the UTI schemes for the pre-2025 Purebred app. It is recommended to not use both sets of Purebred UTI schemes, and to not have both the 2025 and pre-2025 Purebred apps on the same device, as it can cause issues when importing Purebred certificates into the UEM Client.
6. Click **Save**.

After you finish:

- Assign the UEM Client with the app configuration that you created to the users and devices you want to use the app-based PKI solution.
- If you are using the pre-2025 Purebred app, you must turn off the following rule in the IT policy assigned to users: “Do not allow copying data from non BlackBerry Dynamics apps into BlackBerry Dynamics apps”.

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.

Before you begin: Make sure you have completed one of the following:

- If your environment uses an app-based PKI solution with iOS devices, connect BlackBerry UEM to your organization’s app-based PKI solution.
- If your environment uses an app-based PKI solution with iOS devices, and the PKI app is not a BlackBerry Dynamics app, configure the BlackBerry UEM Client to support app-based certificates.

1. In the 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, SCEP profiles, and user credential profiles** check box.
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 **Basic Configuration** tab, in the **Security Settings** section, select the **Use client certificate in place of login/password**checkbox. **b.** To enable automatic discovery of the Microsoft Exchange server that the users are on, in the **Client Settings** section, select the **Use BEMS to perform Autodiscover of the EAS/EWS endpoint for the user**checkbox. **c.** On the **Advanced Configuration** tab, in the **TLS Certificate Settings** section, type the name of the user credential profile for the device.
Configure BlackBerry Work when your organization is not using BEMS	**a.** Click the **Basic Configuration** tab. **b.** If your server uses the domain name\user login format, in the **Exchange ActiveSync Settings** section, 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 **Autodiscover URL** field, specify the autodiscover URL, if known. This speeds up the auto discover setup process (for example, https://autodiscover.mydomain.com). **e.** In the **Autodiscover Connection Timeout in Seconds (iOS only)** field, specify the autodiscover connection timeout in seconds. **f.** In the **TLS Certificate Settings**section, in the **User Credential Profile Name** field, type the name of the user credential profile.

5. Click **Save**.

After you finish: Create app-based PKI solution to use with the following devices:

- iOS devices: create a user credential profile to use app-based certificates.
- Android devices: create a user credential profile to use certificates from the native keystore.

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

Before you begin:

- Configure the BlackBerry UEM Client to support app-based certificates.
- Ensure that the PKI app (for example, Purebred) is installed on users' devices.

1. On the menu bar, click **Policies and Profiles > Certificates > User credential**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Certificate authority connection** drop-down list, click 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.
5. 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
      ```
6. If you want the device to delete expired certificates, select **Delete expired certificates**.
7. If you want the device to delete duplicate certificates, select **Remove duplicate certificates**.
8. Click **Add**.

After you finish:

- To allow BlackBerry Dynamics apps to use certificates, on the menu bar, click **Apps**. Click the BlackBerry Dynamics app that you want to change, then on the **Settings > BlackBerry Dynamics** tab, select the **Allow BlackBerry Dynamics apps to use user certificates SCEP profiles and user credential profiles** checkbox.
- Assign the profile to user accounts and user groups.
- If your organization uses Purebred, instruct users to import the Purebred certificates into the UEM Client. For instructions, see Import Purebred certificates.

Use Intercede MyID to provide derived credentials certificates to devices

You can use the Intercede MyID PIV credential management solution to provide derived credentials certificates to iOS and Android devices activated on UEM. Follow the steps below to create and assign an Intercede user credential profile to users and groups. After the profile is delivered to a device, the user can scan the Intercede QR code from the UEM Client to activate with MyID and download derived credentials certificates from MyID to the device's BlackBerry Dynamics keystore, or to the BlackBerry Dynamics keystore and the device's native key chain.

Note that the settings that you configure in the profile apply to both iOS and Android devices.

The following UEM administrator permissions control how administrators can work with standard user credential profiles and Intercede user credential profiles: View user credential profiles, Create and edit user credential profiles, Delete user credential profiles.

Before you begin:

- To support this feature for iOS devices, "Enable UEM Client to enroll in BlackBerry Dynamics" must be enabled in the assigned BlackBerry Dynamics profile. By default, this setting is enabled.
- Verify that devices are running UEM Client for iOS version 12.51.x or later or the UEM Client for Android version 12.45.x or later.
- Create and assign a CA certificate profile to users and groups to deliver the certificates for your organization's Intercede MyID server to devices.

1. In the management console, on the menu bar, click **Policies and profiles > Managed devices > Certificates > Intercede user credential**.
2. Click +.
3. Type a name and description for the profile.
4. Under **BlackBerry Dynamics app list**, choose one of the following:
   - **Allow all BlackBerry Dynamics apps to use certificates**: The certificates delivered by MyID are stored in the BlackBerry Dynamics keystore and can be used by any BlackBerry Dynamics apps on the device.
   - **Allow specified BlackBerry Dynamics apps to use certificates**: The certificates delivered by MyID are stored in the BlackBerry Dynamics keystore and can be used only by the specified BlackBerry Dynamics apps.
5. Configure the following settings:

Setting	Supported for	Description
Allow additional QR scan methods	iOS Android	If enabled, the UEM Client can scan the Intercede QR code using the camera, a saved image, or the clipboard. If not selected, the UEM Client can scan the Intercede QR code using the camera only. If you want to allow users to scan the QR code from the clipboard (for example, from a non-BlackBerry browser or email application), verify that "Do not allow copying data from non-BlackBerry Dynamics apps into BlackBerry Dynamics apps" is turned off in the assigned BlackBerry Dynamics profile.

Setting	Supported for	Description
Deliver to built-in key chain	iOS Android	If enabled, certificates delivered by MyID are also stored in the device's native key chain and can be used by native apps (for example, Safari). Storing certificates in the native key chain is not supported for devices with the iOS User privacy and User privacy - User enrollment activation types. If you enable this setting, you cannot change it after the profile is saved. If you want to turn this setting off, you must create a new profile that does not have this setting enabled and assign it to users and groups.
Hide certificate on Android Enterprise devices	Android	If enabled, Android Enterprise users cannot view the derived credentials certificates on the device. This setting is available only if you enable Deliver to built-in key chain. If you enable this setting, you cannot change it after the profile is saved. If you want to turn this setting off, you must create a new profile that does not have this setting enabled and assign it to users and groups.

6. Click **Save**.

After you finish:

- Assign the profile to user accounts and groups.
- After the profile is delivered to devices, instruct users to open the UEM Client and navigate to Assigned profiles > Import certificates to scan the Intercede QR code that is shared by the MyID administrator. The QR code will allow the device to activate with MyID and download the derived credentials certificates.
- If the MyID administrator changes the derived credentials certificates, you can instruct users to use the UEM Client to import the certificates again (Assigned profiles > Import certificates > scan the Intercede QR code). The reimport will replace the existing certificates with the new ones that it downloads from MyID.
- On iOS devices, the MyID integration is dependent on the BlackBerry Dynamics user certificate. If you remove the BlackBerry Dynamics certificate for a user from the user summary in the management console, the MyID integration is deactivated.
- If you configured Entra ID conditional access and you assigned an Intercede user credential profile to users before they activate, when a user activates a device, they must complete Intercede enrollment before they are prompted to register with Entra conditional access.

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 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 > Certificates > SCEP**.
2. Click +.
3. Type a name and description for the profile.
4. 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. Note that 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. For Windows devices, only static passwords are supported.
5. In the **URL** field, type the URL for the SCEP service. The URL should include the protocol, FQDN, port number, and SCEP path.
6. In the **Instance name** field, type the instance name for the CA.
7. Optionally, clear the check box for any device type that you do not want to configure the profile for.
8. 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. See the following:
      - Common: SCEP profile settings
      - iOS: SCEP profile settings
      - macOS: SCEP profile settings
      - Android: SCEP profile settings
      - Windows 10: SCEP profile settings
      - BlackBerry Dynamics: SCEP profile settings
9. Repeat step 8 for each device type in your organization.
10. 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.

Common: SCEP profile settings

Common: SCEP profile setting	Description
Certificate authority connection	This setting specifies whether the CA is Entrust, OpenTrust, or another CA.
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.
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 UEM certificate store to allow 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. For Windows devices, only "static" passwords are supported.
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). 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."
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."

Common: SCEP profile setting	Description
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. 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 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.
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.
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service.
Key size	This setting specifies the key size for the certificate.
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.

iOS: SCEP profile setting	Description
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. To meet a Microsoft requirement for strong certificate to user identity mapping, if the SAN type is set to URI, you must add the following to the value that you specify: `tag:microsoft.com,2022-09-14:sid:%UserAdSid%`
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.

macOS: SCEP profile settings

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.
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.
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service.

macOS: SCEP profile setting	Description
Key size	This setting specifies the key size for the certificate.
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.
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

For devices with Android Management activation types, see Considerations for Android Management activation types.

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 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.
Hide certificate on Android Enterprise devices	This setting specifies whether the certificate is visible to Android Enterprise users. 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 UEM Cloud.
Encryption algorithm	This setting specifies the encryption algorithm that Android devices use for the certificate enrollment request.
Hash function	This setting specifies the hash function that Android devices use for the certificate enrollment request.

Android: 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. 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.
Android work profiles and Samsung KNOX	
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.
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. To meet a Microsoft requirement for strong certificate to user identity mapping, if the SAN type is set to URI, you must add the following to the value that you specify: `tag:microsoft.com,2022-09-14:sid:%UserAdSid%`
Key algorithm	This setting specifies the algorithm that devices use to generate the client key pair. You must select an algorithm that is supported by your CA.
RSA strength	This setting specifies the RSA strength that 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".
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate.
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate.

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%.
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required.
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.
Retry delay	This setting specifies the time in seconds to wait before retrying to connect to the SCEP service.
Key size	This setting specifies the key size for the certificate.
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate.
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate.
SCEP key storage	This setting specifies the storage location for the private key.
Hash function	This setting specifies the hash function that a Windows 10 device uses for the certificate enrollment request.
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 maximum value is 365 days.

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: "/CN=%UserDistinguishedName%, %UserDistinguishedName%...".
SAN type	This setting specifies the subject alternative name type for the certificate, if it is required.
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.
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.".
Encryption algorithm	This setting specifies the encryption algorithm used for the certificate enrollment request.
Hash function	This setting specifies the hash function used for the certificate enrollment request.
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.
Key usage	This setting specifies the cryptographic operations that can be performed using the public key that is contained in the certificate.
Extended key usage	This setting specifies the purpose of the key that is contained in the certificate.
App restrictions	This setting specifies which BlackBerry Dynamics apps can use the certificate.

BlackBerry Dynamics: SCEP profile setting	Description
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.

Send client certificates to devices using ACME

Automated Certificate Management Environment (ACME) solutions allow organizations to automate lifecycle management operations between a Certificate Authority and devices, including the issuance, renewal, and revocation of client certificates. If your organization uses an ACME solution, you can create and assign ACME profiles to enable iOS devices that are activated on UEM to communicate with the ACME server to obtain and manage the use of client certificates. The devices that you assign the profile to require access to the ACME server (for example, through a VPN or through BlackBerry Secure Connect Plus).

Note that BlackBerry Dynamics apps do not currently support the use of ACME to obtain and manage client certificates.

1. In the management console, on the menu bar, click **Policies and profiles > Certificates > ACME**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Directory URL** field, type the URL of the ACME server.

   Include the protocol, FQDN, port, and directory path defined in the ACME specification. For example: https://<*acme_server*>/directory
5. In the **Subject** field, type the subject name for certificate requests.

   The value must be a distinguished name, for example, /C=CA/O=BlackBerry Limited/CN=user01or C=CA,O=BlackBerry Limited,CN=user01. You can use the %UserDistinguishedName% variable.
6. If you want to specify a subject alternative name for certificate requests, in the **SAN type** drop-down list, select the appropriate SAN type and do the following:
   a) In the **SAN Value** field, specify the appropriate value. For RFC822, specify a valid email address (you can use the %UserEmailAddress% variable). For DNS name, specify the FQDN. For URI, specify the IP address or URL including the protocol and FQDN.
   b) In the **NT principal name** field, specify the principal name for certificate requests. You can use the %UserPrincipalName% variable.
7. In the **Key algorithm** drop-down list, select the appropriate algorithm that devices will use to generate the client key pair.
8. In the **RSA strength** drop-down list, select the appropriate key size that will be used to generate the client key pair.
9. If you do not want to export the private key from the keychain, clear the **Extractable key** check box.
10. If you want all apps on a device to access the private key, select the **Access private key** check box.
11. In the **Key usage** section, select the cryptographic operations that you want the public key in the certificate to be used for.

12. If you want to extend the use of the public key for other operations, in the **Extended key usage** section, click + and specify the object identifier (OID) for the operation. Repeat as necessary.
13. Click **Save**.

After you finish:

- Assign the profile to users and groups as necessary.
- If devices use the client certificate to authenticate with a work Wi-Fi network, work VPN, or work mail server, associate the ACME profile with a Wi-Fi, VPN, or email profile.
- If you create more than one ACME profile, rank the profiles.

Send 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.

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 > Certificates > Shared certificate**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Password** field, type a password for the shared certificate profile.
5. In the **Certificate file** field, click **Browse** to locate the certificate file.
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**.
7. If you are managing macOS devices, on the **macOS** tab, in the **Apply profile to** drop-down list, select **User** or **Device**.
8. Click **Add**.

After you finish: Assign the Shared certificate profile to user accounts, user groups, or device groups.

Specify the certificate used by an app using a certificate mapping profile

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.

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 > Certificates > Certificate mapping**.
2. Click +.
3. Type a name and description for the profile.
4. In the mapping table, click +.
5. 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.

6. 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 click 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.
   - To specify that the app must use a certificate sent to the device by another profile, select **Selected certificate** and click the profile name from the drop-down list.
7. 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.
8. If necessary, repeat steps 5 to 8 to add to additional mappings to the profile.
9. Click **Add**.

After you finish:

- Assign the profile to user accounts and user groups.
- If you create more than one certificate mapping profile, rank the profiles as necessary. Select a profile and click ↓↑ to move the profile up or down the ranking. Click **Save**.

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 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 and manage a client certificate for a user account

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Search for and click a user account.
3. Do any of the following:

Task	Steps
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. **a.** In the **IT policy and profiles** section, click +. **b.** Click **User certificate**. **c.** Type a description for the certificate. **d.** In the **Apply certificate to** section, select one of the following: 1. **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. 2. **BlackBerry Dynamics enabled devices**: Choose this option to send the certificate to devices to use with BlackBerry Dynamics apps. **e.** In the **Certificate file** field, click **Browse**. Navigate to and select the certificate file. **f.** If you select **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 if the device is running the latest version of the UEM Client. If you don't set a password, the user must enter the device password. **g.** Click **Add**. **h.** Configure the time to live for client certificates. The default time to live before the client certificates are removed is 24 hours. 1. On the menu bar, click **Settings > General settings > Certificates**. 2. Specify the time to live for PKCS#12 certificates on the server.

Task	Steps
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, and you are using the BlackBerry Dynamics PKI connector, the PKI connector sends a notification to the CA that the certificate is no longer in use, but the certificate is not automatically revoked. In the **User certificates** section, perform one of the following actions: **a.** Click  to request certificate renewal from the CA. **b.** Click ✕ to remove the certificate from the user's devices. 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 UEM Self-Service. Uploading certificates to user credential profiles is supported for 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. **a.** In the **IT policy and profiles** section, beside the user credential profile, click **Add a certificate**. **b.** Click **Browse**. Navigate to and select the certificate. **c.** 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 UEM if the device is running the latest version of the UEM Client. If you don't specify the password, the user must enter the device password. **d.** Click **Add**.
Change a client certificate for a user credential profile	The new certificate will replace the existing certificate on the device. **a.** In the **IT policy and profiles** section, beside the user credential profile, click **Update**. **b.** Click **Browse** to locate the certificate. **c.** 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 UEM if the device is running the latest version of UEM Client. If you don't specify the password, the user must enter the device password. **d.** Click **Save**.

Legal notice

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