BlackBerry UEM

Securing network connections

Administration

12.18

Contents

Managing Wi-Fi, VPN, BlackBerry Secure Connect Plus, and other work connections

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.

Managing work connections using profiles

You can configure how devices connect to work resources using the following profiles:

Profile	Description
Wi-Fi	A Wi-Fi profile specifies how devices connect to a work Wi-Fi network.
VPN	A VPN profile specifies how devices connect to a work VPN.
Proxy	A proxy profile specifies how devices use a proxy server to access web services on the Internet or a work network.
Enterprise connectivity	The enterprise connectivity profile specifies how devices can connect to your organization's resources using enterprise connectivity and BlackBerry Secure Connect Plus.
BlackBerry 2FA	A BlackBerry 2FA profile enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.
Single sign-on extension	A single sign-on extension profile specifies how iOS and iPadOS devices authenticate with secure domains automatically after users type their username and password for the first time.
BlackBerry Dynamics connectivity profile	A BlackBerry Dynamics connectivity profile defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.
Email	An email profile specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.
IMAP/POP3 email	An IMAP/POP3 email profile specifies how devices connect to an IMAP or POP3 mail server and synchronize email messages.

Best practice: Creating work connection profiles

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.

Consider the following guidelines:

- Determine which work connections are required for devices in your organization.
- Create profiles that you can associate with other profiles before you create the work connection profiles that use them.
- Use variables where appropriate.

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 the Wi-Fi profiles stored on the device 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.

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.
  Note: Samsung Knox Workspace devices don't support using certificates sent to devices by BlackBerry UEM for Wi-Fi authentication. Users must set up certificate-based authentication manually on Samsung Knox Workspace devices.
- 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. Perform the following actions:
   a) Click the tab for a device type.
   b) Configure the appropriate values for each profile setting to match the Wi-Fi configuration in your organization's environment. If your organization requires that users provide a username and password to connect to the Wi-Fi network and the profile is for multiple users, in the **Username** field, type `%UserName%`.
8. Repeat step 7 for each device type in your organization.
9. Click **Add**.

Wi-Fi profile settings

You can use a variable in any profile setting that is a text field to reference a value instead of specifying the actual value. Wi-Fi profiles are supported on the following device types:

- iOS
- iPadOS
- macOS
- Android
- Windows

Common: Wi-Fi profile settings

Common: Wi-Fi profile setting	Description
SSID	This setting specifies the network name of a Wi-Fi network and its wireless access points. The SSID is case-sensitive and must contain alphanumeric characters. Possible values are limited to 32 characters.
Hidden network	This setting specifies whether the Wi-Fi network hides the SSID.

iOS and macOS: Wi-Fi profile settings

Settings for iOS also apply to iPadOS devices.

macOS applies profiles to either user accounts or devices. You can configure a Wi-Fi profile to apply to one or the other.

iOS 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. Possible values: • User • Device This setting is valid only for macOS.
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. This setting applies only to devices that are running iOS and iPadOS 14 and later.
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. Possible values: • Standard • Legacy hotspot • Hotspot 2.0 The default value is "Standard."

iOS and macOS: Wi-Fi profile setting	Description
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."
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." Possible values: • None • WEP personal • WEP enterprise • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA3-Personal • WPA3-Enterprise The default value is "None."

iOS and macOS: Wi-Fi profile setting	Description
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." Possible selections: • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM • EAP-AKA
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." Possible values: • None • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP The default value is "MS-CHAPv2."
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."

iOS and macOS: Wi-Fi profile setting	Description
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	
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."

iOS and macOS: Wi-Fi profile setting	Description
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." Possible values: • None • Shared certificate • SCEP • User credential The default value is "None."
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." Possible values: • Single reference • Variable injection The default value is "Single reference."
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."
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 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	

iOS and macOS: Wi-Fi profile setting	Description
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." Possible values: • Single reference • Variable injection The default value is "Single reference."
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.
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 an Android devices use to connect to a proxy server when the device is connected to the Wi-Fi network. Android 8.0 and later devices with MDM controls or User privacy activations don't support Wi-Fi profiles with proxy settings. If a device with one of these activation types is upgraded to Android 8.0, Wi-Fi profiles that have an associated proxy profile will be removed from the device.
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. Possible values: • None • Personal • Enterprise The default value is "None."
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." Possible values: • None • WEP personal • WPA-Personal/WPA2-Personal The default value is "None."

Android: Wi-Fi profile setting	Description
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."
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." Possible values: • TLS • TTLS • PEAP • LEAP The default value is "TLS." 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." Possible values: • None • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC The default value is "MS-CHAPv2." CHAP is not supported by devices that use Samsung Knox.

Android: Wi-Fi profile setting	Description
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.
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." Possible values: • None • Shared certificate • SCEP • User credential The default value is "None."

Android: Wi-Fi profile setting	Description
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." Possible values: • Single reference • Variable injection The default value is "Single reference."
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."

Android: Wi-Fi profile setting	Description
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." Possible values: • Single reference • Variable injection The default value is "Single reference."
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. Possible values: • Open • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal The default value is "Open."

Windows: Wi-Fi profile setting	Description
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. Possible values: • None • WEP • TKIP • AES
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." The possible values are from 1 to 4. The default value is 2.
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."
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."

Windows: Wi-Fi profile setting	Description
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 your organization’s Active Directory. When set to “Perform immediately after user login”, single sign-on is performed immediately after the user logs in to your organization’s Active Directory. This setting is valid only if the “Enable single sign-on" setting is selected. Possible values: • Perform immediately before user login • Perform immediately after user login The default value is “Perform immediately before user login.”
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. The possible values are from 0 to 120 seconds. The default value is "10 seconds."
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.

Windows: Wi-Fi profile setting	Description
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.
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. The possible values are from 5 to 1440 minutes. The default value is 720 minutes.
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. The possible values are from 1 to 255. The default value is 128.

Windows: Wi-Fi profile setting	Description
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. The possible values are from 1 to 16. The default value is 3.
Proxy type	This setting specifies the type of proxy configuration for the Wi-Fi profile. Possible settings: • None • PAC configuration • Manual configuration • Web Proxy Autodiscovery The default setting is "Manual configuration." 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."

Windows: Wi-Fi profile setting	Description
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." By default, the check box is not selected.
Turn off Internet connectivity checks	This setting specifies whether to turn off Internet connectivity checks. By default, the check box is not selected.
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.
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

You can use CylanceGATEWAY to create a zero trust network access (ZTNA) profile that is recognized by devices as a VPN provider. CylanceGATEWAY trusts nothing and no one by default. For more information on CylanceGATEWAY, see Integrating BlackBerry UEM with CylanceGATEWAY to create a ZTNA profile.

The required profile settings vary for each device type and depend on the VPN connection type and authentication type that you select.

Note: Some devices may be unable to store the xAuth password. For more information, visit support.blackberry.com/community to read 30353.

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 user credential, SCEP, or shared certificate 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. (The proxy server for Windows 10 devices is configured in 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 and Juniper.

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. Perform the following actions:
   a) Click the tab for a device type.
   b) Configure the appropriate values for each profile setting to match the VPN configuration in your organization's environment. If your organization requires that users provide a username and password to connect to the VPN and the profile is for multiple users, in the **Username** field, type `%UserName%`.
6. Repeat step 5 for each device type in your organization.
7. Click **Add**.

Integrating BlackBerry UEM with CylanceGATEWAY to create a ZTNA profile

CylanceGATEWAY is a cloud-native, artificial intelligence (AI) assisted zero trust network access (ZTNA) solution. When CylanceGATEWAY is enabled on a device, you create a ZTNA profile that the device recognizes as a VPN provider. CylanceGATEWAY trusts nothing and no one, by default.

- CylanceGATEWAY protects your users' iOS, Android, Windows 10, Windows 11, and macOS devices devices by allowing you to block connections to Internet destinations that you don't want devices to reach, even when the device isn't connected to your network.
- In addition to protecting devices, CylanceGATEWAY protects access to your organization's private network and cloud-based applications by continuously analyzing whether users' usage patterns are expected or anomalous behavior. If the percentage of anomalous events exceeds a set threshold, CylanceGATEWAY can dynamically override the user's network access control policy to block network access and require the user to authenticate before they can continue.

CylanceGATEWAY administrators can configure which Internet and private network destinations users can access or block access to.

For more information on how to set up CylanceGATEWAY, see Setting up BlackBerry Gateway in the Cylance Endpoint Security setup content.

VPN profile settings

You can use a variable in any profile setting that is a text field to reference a value instead of specifying the actual value. VPN profiles are supported on the following device types:

- iOS
- iPadOS
- macOS
- Samsung Knox
- Windows 10

iOS and macOS: VPN profile settings

Settings for iOS also apply to iPadOS devices.

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

iOS 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. Possible values: • User • Device This setting is valid only for macOS devices.
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. Possible values: • L2TP • PPTP • IPsec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Custom • IKEv2 • IKEv2 Always On The default value is "L2TP." If you select "IKEv2 Always On," many settings have separate values for cellular and Wi-Fi connections. Some values are not valid for macOS devices.
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."

iOS and macOS: VPN profile setting	Description
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. Possible values: • Password • RSA SecurID • Shared secret • Shared secret/Group name • Shared certificate • SCEP • User credential
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."

iOS and macOS: VPN profile setting	Description
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 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."
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." Possible values: • None • Automatic • Maximum The default value is "None."
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."

iOS and macOS: VPN profile setting	Description
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."
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" setting is set to "IKEv2" and the "Authentication type" is set to "Shared certificate."

iOS and macOS: VPN profile setting	Description
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. Possible values for "On demand action": • Always establish • Establish if needed • Never establish
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 disconnect when 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. The default value is "120" 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." This setting applies only to devices running iOS and iPadOS 14 and later.
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. This setting applies only to devices running iOS and iPadOS 13 and later.
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." This setting applies only to devices running iOS and iPadOS 14.2 and later.

iOS 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.” Possible values: • 1.0 • 1.1 • 1.2 The default setting is “1.0.”

iOS and macOS: VPN profile setting	Description
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.” Possible values: • 1.0 • 1.1 • 1.2 The default setting is “1.2.”
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.”
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." Possible values: • Disabled • 30 minutes • 10 minutes • 1 minute The default setting is "10 minutes."
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."

iOS and macOS: VPN profile setting	Description
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. The minimum value and the default value is 20.
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."
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."

iOS and macOS: VPN profile setting	Description
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 applies only to devices running iOS and iPadOS 14 and later. 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 applies only to devices running iOS and iPadOS 13.4 and later. 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 AirPrint are sent through the VPN tunnel, sent outside of the VPN tunnel, or are blocked. This setting applies only to devices running iOS and iPadOS 13.4 and later. 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.
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.

iOS and macOS: VPN profile setting	Description
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. Possible values: • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 • 19 • 20 • 21 • 31 The default setting is "2."
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. Possible values: • DES • 3DES • AES 128 • AES 256 • AES 128 GCM • AES 256 GCM • ChaCha20Poly1305 The default setting is "3DES."

iOS and macOS: VPN profile setting	Description
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. Possible values: • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 The default value is "SHA1-96."
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. The possible values are from 10 to 1440 minutes. The default value is 1440.
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," "IKEv2," or "IKEv2 Always On."
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.
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. This setting applies only to iOS and iPadOS 13.0 and later devices.
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. This setting applies only to iOS and iPadOS 13.0 and later devices.

iOS and macOS: VPN profile setting	Description
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. This setting applies only to iOS and iPadOS 13.0 and later devices.
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. This setting applies only to iOS and iPadOS 14.0 and later devices.
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. This setting applies only to iOS and iPadOS 14.0 and later devices.
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. This setting applies only to iOS and iPadOS 13.0 and later devices. Possible values: • Application layer • IP layer The default setting is "Application layer."
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 Workspace devices.

For more information about the VPN profile settings supported by Samsung Knox Workspace devices, see Samsung Knox VPN JSON Parameters.

Android: VPN profile setting	Description
Server address	This setting specifies the FQDN or IP address of a VPN server.

Android: VPN profile setting	Description
VPN type	This setting specifies whether a device uses IPsec or SSL to connect to the VPN server. Possible values: • IPsec • SSL The default value is "IPsec." 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.
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. Possible values: • Disabled • Manual • Auto If the "VPN type" setting is set to "IPsec," this setting must be set to “Disabled." The default value is "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."

Android: VPN profile setting	Description
IKE version	This setting specifies the version of IKE protocol to use with the VPN connection. Possible values: • IKEv1 • IKEv2 The default value is "IKEv1." 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. Possible values: • Certificate • Preshared key • EAP MD5 • EAP MSCHAPv2 • Hybrid RSA • CAC-based authentication 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. Possible values: • Default • IPv4 address • Fully qualified domain name • User FQDN • IKE key ID 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."

Android: VPN profile setting	Description
IKE phase 1 key exchange mode	This setting specifies the exchange mode for the VPN connection. Possible values: • Main mode • Aggressive mode The default value is "Main mode." This setting is valid only if the "VPN type" setting is set to "IPsec."
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. The possible values are 0, 1, 2, 5, and from 14 to 26. The default value is 0. 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."

Android: VPN profile setting	Description
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. Possible values: • None • Certificate-based authentication • CAC-based authentication The default value is "None." 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."
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. Possible values: • Support chaining • Outer tunnel • Inner tunnel The default value is "Support chaining."
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. Possible values: • Vendor key-value pairs • Vendor JSON value The default value is "Vendor key-value pairs."
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."

Android: VPN profile setting	Description
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 Workspace 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. Possible values: • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • Manual connection definition The default value is "Microsoft."

Windows: VPN profile setting	Description
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." Possible values: • Split tunnel • Force tunnel The default value is "Force tunnel."
Native 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." Possible values: • L2TP • PPTP • IKEv2 • Automatic The default value is "Automatic."
Authentication	This setting specifies the method of authentication used for the native VPN. The "Native protocol type" setting determines which authentication methods are supported and the default value for this setting: • If you select L2TP or PPTP, the possible values are MS-CHAPv2 and EAP. The default value is MS-CHAPv2 • If you select IKEv2, the possible values are User method and Machine method. The default value is User method. • If you select Automatic, the only possible value is EAP. Possible values: • EAP • MS-CHAPv2 • User method • Machine method

Windows: VPN profile setting	Description
EAP configuration	This setting specifies the XML of the EAP configuration. For information about how to generate the EAP configuration XML, visit https://docs.microsoft.com/en-us/windows/client-management/mdm/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." Possible values: • EAP
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." Possible value: • Certificate
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.
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`. For more information, visit http://technet.microsoft.com/en-us/library/hh856044.aspx • 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.

Windows: VPN profile setting	Description
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`. For more information, visit http://technet.microsoft.com/en-us/library/hh856044.aspx • 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. Possible values: • All • TCP • UDP The default value is "All."
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.

Windows: VPN profile setting	Description
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. Possible values: • Split tunnel • Force tunnel The default setting is "Force tunnel."
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	Possible values: • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 The default setting is "MD596."

Windows: VPN profile setting	Description
Cipher transform constants	Possible values: • DES • DES3 • AES128 • AES192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 The default setting is "DES."
Encryption method	Possible values: • DES • DES3 • AES128 • AES192 • AES256 The default setting is "DES."
Integrity check method	Possible values: • MD5 • SHA196 • SHA256 • SHA384 The default setting is "MD5."
Diffie-Hellman Group	Possible values: • Group1 • Group2 • Group14 • ECP256 • ECP384 • Group24 The default setting is "Group1."

Windows: VPN profile setting	Description
PFS Group	Possible values: • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 The default value is "PFS1."
Proxy type	This setting specifies the type of proxy configuration for the VPN. Possible values: • None • PAC configuration • Manual configuration The default value is "None."
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 per-app VPN

You can set up per-app VPN for iOS, iPadOS, Samsung Knox, and Windows 10 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.

For iOS and iPadOS devices, apps are associated with a VPN profile when you assign the app or app group to a user, user group, or device group.

For 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.

For Windows 10 devices, apps are added to the "App trigger list" setting in the VPN profile.

How BlackBerry UEM chooses which per-app VPN settings to assign to iOS devices

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 that are associated with an app directly take precedence over per-app VPN settings associated indirectly by an app group.
- Per-app VPN settings that are associated with a user directly take precedence over per-app VPN settings associated indirectly by a user group.
- Per-app VPN settings that are assigned to a required app take precedence over per-app VPN settings assigned to an optional instance of the same app.
- Per-app VPN settings that are 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 noted otherwise, 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 the profiles that your organization uses, which can include any of the following: • Wi-Fi • VPN You can also assign a proxy profile to user accounts, user groups, or device groups. **Note:** 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.
Android	For Android Enterprise devices, create a proxy profile and associate it with a Wi-Fi profile. Android 8.0 and later devices with MDM controls or User privacy activations don't support Wi-Fi profiles with proxy settings.

Device	Proxy configuration
Samsung Knox	Create a proxy profile and associate it with the profiles that your organization uses. 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. **Note:** To use a proxy profile with an enterprise connectivity profile, BlackBerry Secure Connect Plus must be enabled. You can also 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. **Note:** 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

If your organization uses a PAC file to define proxy rules, you can select PAC configuration to use the proxy server settings from the PAC file that you specify. Otherwise, you can select manual configuration and specify the proxy server settings directly in the 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, verify that **PAC configuration** is selected. **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 BlackBerry UEM or any of its components. **c.** On the **BlackBerry** tab, perform the following actions: **1.** 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>*. **2.** In the **User can edit** drop-down list, click the proxy settings that BlackBerry 10 device users can change. The default setting is **Read only**.
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>*. **e.** On the **BlackBerry** tab, perform the following actions: **1.** In the **User can edit** drop-down list, click the proxy settings that BlackBerry 10 device users can change. The default setting is **Read only**. **2.** Optionally, you can specify a list of addresses that users can access directly from their BlackBerry 10 devices without using the proxy server. In the **Exclusion list** field, type the addresses (FQDN or IP) and use a semicolon (;) to separate the values in the list. You can use the wildcard character (*) in an FQDN or IP (for example, *.example.com or 192.0.2.*).

7. Repeat steps 4 and 5 for each device type in your organization.
8. Click **Add**.

After you finish:

- Associate the proxy profile with a Wi-Fi, VPN, or enterprise connectivity profile.
- If necessary, rank profiles. The ranking that you specify applies only if you assign a proxy profile to user groups or device groups.

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 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.

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.

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.

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.

For iOS and iPadOS devices, if you configure per-app VPN for BlackBerry Secure Connect Plus, 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.

Supported devices communicate with BlackBerry 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 BlackBerry 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.

For more information about how BlackBerry Secure Connect Plus transfers data to and from devices, see the on-premises Architecture content or the Cloud Architecture content.

Steps to enable BlackBerry Secure Connect Plus

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	If you have BlackBerry UEM Cloud, install the BlackBerry Connectivity Node or upgrade the BlackBerry Connectivity Node to the latest version.
3	Enable BlackBerry Secure Connect Plus in the Default enterprise connectivity profile or in a custom enterprise connectivity profile that you create.

Step	Action
4	Optionally, specify the DNS settings for the BlackBerry Connectivity app.
5	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.
6	Assign the enterprise connectivity profile to user accounts, or user groups.

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:

- Your organization's firewall must allow outbound connections over port 3101 to <*region*>.turnb.bbsecure.com and <*region*>.bbsecure.com. If you configure BlackBerry UEM to use a proxy server, verify that the proxy server allows connections over port 3101 to these subdomains. For more information about domains and IP addresses to use in your firewall configuration, visit http://support.blackberry.com/community to read article 36470.
- In each BlackBerry UEM instance, the BlackBerry Secure Connect Plus component must be running.
- By default, Android Enterprise 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 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 have BlackBerry UEM Cloud, you must install the BlackBerry Connectivity Node or upgrade it to the latest version.

Note: If your on-premises environment includes Knox Workspace or Android Enterprise devices with BlackBerry Dynamics apps, see Optimize secure tunnel connections for Android devices that use BlackBerry Dynamics apps.

Note: 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. For more information about the BlackBerry Secure Gateway, see Protecting email data using the BlackBerry Secure Gateway.

For supported devices:

Device	Requirements
iOS and iPadOS	• Devices must be activated using the BlackBerry UEM Client, available from the App Store • MDM controls activation type

Device	Requirements

Android Enterprise	• 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	• Samsung Knox MDM 5.0 or later
	• Samsung Knox 2.3 or later
	• Any of the following activation types:
	  • Work space only (Samsung Knox)
	  • Work and personal - full control (Samsung Knox)
	  • Work and personal - user privacy (Samsung Knox)

Installing additional BlackBerry Secure Connect Plus components in an on-premises environment

You can install one or more instances of the BlackBerry Connectivity Node to add additional instances of the device connectivity components to your organization's domain. Each BlackBerry Connectivity Node contains an active instance of BlackBerry Secure Connect Plus that can process device data and establish secure connections.

You can also create server groups. A server group contains one or more instances of the BlackBerry Connectivity Node. When you create a server group, you specify the regional data path that you want the components to use to connect to the BlackBerry Infrastructure. For example, you can create a server group to direct device connections for BlackBerry Secure Connect Plus and the BlackBerry Secure Gateway to use the path for the United States to the BlackBerry Infrastructure. You can associate email and enterprise connectivity profiles with a server group. Any device that is assigned those profiles uses that server group's regional connection to the BlackBerry Infrastructure when it uses any of the components of the BlackBerry Connectivity Node.

If a domain includes more than one BlackBerry UEM instance, the BlackBerry Secure Connect Plus component in each instance runs and processes data. Data is load-balanced across all BlackBerry Secure Connect Plus components in the domain.

High availability failover is available for BlackBerry Secure Connect Plus. If a device is using a secure tunnel and the current BlackBerry Secure Connect Plus component becomes unavailable, the BlackBerry Infrastructure assigns the device to a BlackBerry Secure Connect Plus component on another BlackBerry UEM instance. The device resumes use of the secure tunnel with minimal disruption.

For more information about planning for and installing a BlackBerry Connectivity Node, see the Planning content and the Installation and upgrade content.

Installing or upgrading the BlackBerry Secure Connect Plus component in a cloud environment

When you install the BlackBerry Connectivity Node, the setup process also installs the BlackBerry Secure Connect Plus component on the same computer. If you upgrade the BlackBerry Connectivity Node to the latest version and BlackBerry Secure Connect Plus is not installed, the upgrade process installs BlackBerry Secure Connect Plus. If

BlackBerry Secure Connect Plus was installed previously, the process upgrades BlackBerry Secure Connect Plus to the latest version.

For instructions to install or upgrade the BlackBerry Connectivity Node, see "Installing and upgrading the BlackBerry Connectivity Node" in the BlackBerry UEM Cloud Configuration content. You must activate the BlackBerry Connectivity Node before you can enable BlackBerry Secure Connect Plus.

You have the option to 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).

Note: If you specify proxy information that is not valid, BlackBerry Secure Connect Plus stops running and cannot restart. If this issue occurs, correct the proxy information and restart the BlackBerry UEM - BlackBerry Secure Connect Plus service in the Windows Services.

You can install a second BlackBerry Connectivity Node for redundancy. Both instances of BlackBerry Secure Connect Plus run and process data. Data is load-balanced across both instances. If a device is using a secure tunnel and the current BlackBerry Secure Connect Plus instance becomes unavailable, the BlackBerry Infrastructure assigns the device to the other instance. The device resumes use of the secure tunnel with minimal disruption.

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 devices, the app is installed automatically from Google Play; for iOS and iPadOS devices, the app is installed automatically from the App Store).

BlackBerry releases new versions of the app to support new features and enhancements. For instructions on upgrading the app, and to learn about the latest known and fixed issues, see the BlackBerry Connectivity app Release Notes.

1. In the management console, on the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > Enterprise connectivity**.
3. Click +.
4. 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.
5. Configure the appropriate values for the profile settings for each device type. For more information about each profile setting, see Enterprise connectivity profile settings.
6. Click **Add**.
7. Assign the profile to groups or user accounts.
8. If you configured per-app VPN for iOS and iPadOS devices, when you assign an app or app group, associate it with the appropriate enterprise connectivity profile.

After you finish:

- On Android Enterprise 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. iOS, iPadOS, Android Enterprise and Knox Workspacedevice 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 are troubleshooting a connection issue with an iOS, iPadOS, Android Enterprise or Knox Workspace device, 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.

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. This setting is valid only if you have installed one or more instances of the BlackBerry Connectivity Node and set up server groups.

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).
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.

Setting	Description
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	Click + to specify the domains that are allowed to start a VPN connection in Safari.
Calendar domains	Specify the domains that can start the VPN connection in Calendar. This setting applies only to devices that are running iOS 13 and later or iPadOS 13 and later.
Contacts domains	Specify the domains that can start the VPN connection in Contacts. This setting applies only to devices that are running iOS 13 and later or iPadOS 13 and later.
Mail domains	Specify the domains that can start the VPN connection in Mail. This setting applies only to devices that are running iOS 13 and later or iPadOS 13 and later.
Associated domains	Specify the associated domains. This setting applies only to devices that are running iOS 14 and later or iPadOS 14 and later.
Excluded domains	Specify the excluded domains. This setting applies only to devices that are running iOS 14 and later or iPadOS 14 and later.
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 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 devices that are not allowed to use BlackBerry Secure Connect Plus. Click + and type the app package ID. Repeat as necessary to restrict additional apps. By default, Google Play and underlying services (com.android.providers.media, com.android.vending, com.google.android.gms, and com.google.android.apps.gcs) are restricted because Google Play does not have proxy support. It is recommended to keep these restrictions in place. If you remove any of these restrictions, you must contact Google Play support for the firewall configuration required to allow connections to Google Play using BlackBerry Secure Connect Plus. By default, the packages are added to new enterprise connectivity profile, however you must add them to any existing profiles. 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 BlackBerry UEM Client to communicate with the BlackBerry Infrastructure through BlackBerry UEM. For more information about opening ports in the firewall when work apps use BlackBerry Secure Connect Plus, visit support.blackberry.com/community to read article 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. This setting is valid only if the "Enterprise connectivity for Android devices with a work space" setting is set to "Container wide VPN."
Apps allowed to use Enterprise Connectivity	This setting specifies apps in the work space on Android Enterprise 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	If you want to route secure tunnel traffic from Samsung Knox devices with Android Enterprise activations and Samsung Knox Workspace 2.5 and later devices to the work network through a proxy server, select the appropriate proxy profile. This setting does not apply to Android Enterprise devices other than Samsung Knox devices or to devices with Samsung Knox Workspace version 2.4 and earlier.

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. You can also specify DNS search suffixes. 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.

If you create and configure one or more server groups to direct BlackBerry Secure Connect Plus connections to a specific regional path to the BlackBerry Infrastructure, you can specify DNS settings specific to each server group. If you do, the DNS settings for a server group take precedence over the global DNS settings that you specify using the following steps. For more information about creating and configuring server groups, see the on-premises Installation and upgrade content or the UEM Cloud Configuration content.

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 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. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > BlackBerrry Dynamics connectivity**.
3. Select the profile that is assigned to Android Enterprise and Samsung Knox Workspace devices.
4. Click ✎
5. Clear the **Route all traffic** check box.
6. Click **Save**.

Troubleshooting BlackBerry Secure Connect Plus

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

The BlackBerry Secure Connect Plus Adapter goes into an "Unidentified network" state and stops working

Cause

This issue might occur if you restart the computer that hosts BlackBerry Secure Connect Plus.

Solution - Windows Server 2012

1. In Server Manager, click **Manage > Add Roles and Features**. Click **Next** until you get to the **Features** screen. Expand **Remote Server Administration Tools > Role Administration Tools** and select **Remote Access Management Tools**. Complete the wizard to install the tools.
2. Click **Tools > Remote Access Management**.
3. Under **Configuration**, click **DirectAccess and VPN**.
4. Under **VPN**, click **Open RRAS Management**.
5. Right-click the Routing and Remote Access Server and click **Disable Routing and Remote Access**.
6. Right-click the Routing and Remote Access server and click **Configure and Enable Routing and Remote Access**.
7. Complete the setup wizard, selecting these options:
   a. On the **Configuration** screen, select **Network address translation (NAT)**.
   b. On the **NAT Internet Connection** screen, select **Use this public interface to connect to the Internet**. Verify that BlackBerry Secure Connect Plus is displayed in the list of network interfaces.
8. Open **Routing and Remote Access >** <*server_name*> **> IPv4** and click **NAT**. Open the **Local Area Connection** properties and select **Public interface connected to the Internet** and **Enable NAT on this interface**. Click **OK**.
9. Open the **BlackBerry Secure Connect Plus** properties and select **Private interface connected to private network**. Click **OK**.
10. Right-click the Routing and Remote Access Server and click **All Tasks > Restart**.
11. In the Windows Services, restart the **BlackBerry UEM – BlackBerry Secure Connect Plus** service.

Download and install the hotfix in the Windows KB article NAT functionality fails on a Windows Server 2012-based RRAS server.

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 BlackBerry 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, located by default at *<drive>*:\Program Files\BlackBerry\UEM\Logs*<yyyymmdd>*, 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

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>*.

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
Verify that BlackBerry Secure Connect Plus is using custom transcoder settings	BSCP	"configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Verify that devices are using a custom transcoder	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

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 single sign-on authentication for devices

You can enable iOS devices to authenticate automatically with domains and web services in your organization's network. After you assign a single sign-on profile or sign-on extension profile, the user is prompted for a username and password the first time they try to access a secure 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 domains specified in the profile. When the user changes the password, the user is prompted the next time they try to access a secure domain.

For devices running iOS or iPadOS 13 and later, you use a single sign-on extension profile to enable the devices to authenticate automatically with domains and web services in your organization's network. Devices running a version of iOS earlier than 13 used single sign-on profiles.

- Kerberos
- NTLM
- SCEP certificates for specified trusted domains

BlackBerry Dynamics apps also support Kerberos authentication. For more information, see Configuring Kerberos for BlackBerry Dynamics apps.

Create a single sign-on extension profile

Single sign-on extensions are supported for devices running iOS and iPadOS 13 and later. You can specify settings for a custom extension or use the Kerberos extension provided by Apple.

Before you begin: If you want to use certificate-based authentication, create the necessary certificate profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections** > **Single sign-on extension**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Single sign-on extension type** drop-down, specify whether you are using a custom extension or the Kerberos extension provided by Apple.

Task	Steps
If you select **Custom extenstion**	**a.** In the **Extension identifier** field, type the identifier for the app that performs the single sign-on. **b.** Specify whether the sign-on type is **Credential** or **Redirect** **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 domain. **3.** In the **Name** field, type the domain for which the app extension performs single sign-on. **4.** Add additional 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 select **Kerberos built-in extenstion**	**a.** In the **Domains** section, click + to add a 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.

6. Click **Save**.

Setting up DNS profiles 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 on devices that are running iOS and iPadOS 14 and later and macOS 11 and later.

Create a DNS profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > DNS**.
3. Click +.
4. Type a name and description for the profile.
5. Click the tab for a device type.
6. Select the DNS protocol used to communicate with the DNS server.
7. 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.
8. Select the **Do not allow user to disable DNS settings** option to prevent users from disabling the settings. This option affects supervised devices only.
9. 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.
10. In the **Domains** field, specify the list of domain strings that will be used to determine which DNS queries will use the DNS servers.
11. In the **DNS on demand rules** field, specify the DNS on demand rules using the sample payload format.
12. Click **Save**.
13. Repeat steps 5 to 12 for another device type.

Managing 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.

Create a managed domains profile

Managed domains profiles apply only to iOS and iPadOS devices.

1. On the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > Managed domains**.
3. Click +.
4. Type a name and description for the profile.
5. Optionally, in the **Description** field, type a description for the profile.
6. In the **Managed email domains** section, click +.
7. In the **Email domains** field, type a top-level domain name (for example, `example.com` instead of `example.com/canada`).
8. Click **Add**.
9. In the **Managed web domains** section, click +. For examples of web domain formats, see Managed Safari Web Domains in the iOS Developer Library.
10. In the **Web domains** field, type a domain name.
11. 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.
12. Click **Add**.
13. Click **Add**.

Controlling 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.

Create a network usage profile

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 user groups or user accounts.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > Network usage**.
3. Click +.
4. Type a name and description for the profile.
5. Click +.
6. Perform one of the following actions:
   - Tap **Add an app** and click on an app in the list.
   - Select **Specify the app package ID** 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.***).
7. To prevent the app or apps from using data when the device is roaming, clear the **Allow data roaming** check box.
8. 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.
9. Click **Add**.
10. Repeat steps 5 to 9 for each app that you want to add to the list.

After you finish: If necessary, rank profiles.

Filtering web content 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, 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. **Note:** 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.
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.

Create a web content filter profile

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).

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > Web content filter**.
3. Click +.
4. Type a name and description for the web content filter profile.
5. 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 2 and 3 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 steps 2.a and 2.b for each allowed website. **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 steps 3.a and 3.b for each restricted website.

6. Click **Add**.

Configuring AirPrint and AirPlay profiles 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 aid in specifying where resources are located. You can assign AirPrint profiles to iOS andiPadOS devices so that users don’t have to configure printers manually.

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.

Create an AirPrint profile

You can configure AirPrint profiles and assign them to iOS and iPadOS devices so that users don’t have to configure printers manually.

For more information about the Bonjour protocol and printing with a BlackBerry Dynamics app, visit support.blackberry.com/community to read article 40030.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > AirPrint**.
3. Click +.
4. Type a name and description for the AirPrint profile.
5. In the **AirPrint configuration** section, click +.
6. In the **IP Address** field, type the IP address of the printer or AirPrint server.
7. 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
8. Optionally, if AirPrint connections are secured by TLS, select the **Force TLS** checkbox.
9. Optionally, if the port differs from the default for the Internet Printing Protocol, type the port number in the **Port** field.
10. Click **Add**.
11. Click **Add**.

Create an AirPlay profile

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

2. Click **Networks and connections > AirPlay**.
3. Click +.
4. Type a name and description for the AirPlay profile.
5. Click + in the **Allowed destination devices** section.
6. 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.
7. In the **Password** field, type a password.
8. Click **Add**.
9. Click + in the **Allowed destination devices for supervised devices** section.
10. 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.
11. Click **Add**.

Configuring Access Point Names 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 Android 9 and later devices with Work space only activations and Android 9 and 10 devices 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" IT policy rule in the Android Global (all Android devices) IT policy rules.

Create an Access Point Name profile

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

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

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.

Access Point Name profile setting	Description
APN type bitmask	This setting specifies the types of data communication that use this APN configuration. Different types of communications may use different configurations. Possible values: • Default data traffic • MMS traffic • SUPL assisted GPS • DUN traffic • High priority traffic • Access carrier's FOTA portal • IMS • CBS • IA Initial Attach APN • Emergency PDN • MCX (Mission Critical Service)
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.
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. Possible values: • NONE • PAP • CHAP • PAP or CHAP
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.

Access Point Name profile setting	Description
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. Possible values: • IP • IPV6 • IPV4V6 • PPP
Roaming protocol	This setting specifies whether to enable IPv4, IPv6, or both while roaming for devices that support IPv6 networking. Possible values: • IP • IPV6 • IPV4V6 • PPP
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. Possible values: • SP • IMSI • GID • ICCID

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