BlackBerry UEM

Managing email, calendar, and contacts

Administration

12.22

Contents

Setting up work email for devices

The following options are available if you want to set up work email for devices.

Work email option	Key features
BlackBerry Work	BlackBerry Work securely synchronizes work email, calendar, and contacts. You can also view online presence and access work documents. Unlike built-in email clients, BlackBerry Work integrates these features in a single, easy-to-use app. For more information about managing BlackBerry Work, see Managing apps and the BlackBerry Work Administration Guide.
Email profiles	You can use email profiles to connect devices to your organization's mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler. For example, you can use email profiles to help set up built-in email apps. Email profiles are not required for BlackBerry Work.
IMAP/POP3 email profiles	You can use IMAP and POP3 email profiles to allow devices to connect to IMAP or POP3 mail servers to synchronize email messages only.

Controlling which devices can access Exchange ActiveSync for work email and organizer data

If your organization uses Microsoft Exchange ActiveSync, you can stop unauthorized devices from accessing Exchange ActiveSync unless they are explicitly added to the allowed list. Devices that are not on the allowed list can't access work email and organizer data.

The BlackBerry Gatekeeping Service makes it easier to add devices to the allowed list by automatically adding them. You can use the BlackBerry Gatekeeping Service whether you are using BlackBerry Dynamics apps (such as BlackBerry Work) or email profiles to manage email, calendar, and contact access on users devices.

To configure and use the BlackBerry Gatekeeping Service, you do the following:

1. Create a gatekeeping configuration for Microsoft Exchange Server or Microsoft 365.
2. Assign a gatekeeping profile to user accounts, user groups, and device groups.
3. Configure an email profile or BlackBerry Work to reference the automatic gatekeeping server.

If the gatekeeping profile, email profile, or email app is removed from a user, the user's device is removed from the allowed list and can no longer connect to Microsoft Exchange unless it is allowed using other means (for example, Windows PowerShell).

Most devices allow only one email client to be added to the allowed list for each device. For Android Enterprise and Samsung Knox devices that use an app configuration that contains Exchange Server allowed data, the priority for allowing email applications is as follows:

1. Email applications with application configurations that contain Exchange Server allowed data
2. BlackBerry Work
3. Email client for which the Exchange ActiveSync ID is sent during enrollment

If your organization uses BlackBerry UEM 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 instance of the BlackBerry Gatekeeping Service. Each instance must be able to access your organization’s gatekeeping server. If you want gatekeeping data to be managed only by the BlackBerry Gatekeeping Service that is installed with the primary UEM components, you can change the default settings to disable the BlackBerry Gatekeeping Service in each BlackBerry Connectivity Node.

If your organization uses UEM Cloud, you can install one or two additional 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 instance of the BlackBerry Gatekeeping Service. Each instance must be able to access your organization’s Exchange ActiveSync server. If you want to manage the Exchange ActiveSync access settings only by the BlackBerry Gatekeeping Service that is installed with the main BlackBerry Connectivity Node, you can change the default settings to disable the BlackBerry Gatekeeping Service in the additional BlackBerry Connectivity Node instances.

You can set up BlackBerry Connectivity Node server groups to direct device connectivity traffic to a specific regional connection to the BlackBerry Infrastructure. When you associate a gatekeeping profile with a server group, any user that is assigned that gatekeeping profile uses any active instance of the BlackBerry Gatekeeping Service in that server group. When you configure a server group, you can choose to disable the instances of the BlackBerry Gatekeeping Service in the group. See Create a server group to manage regional connections in the Configuration content.

Steps to configure Exchange ActiveSync and the BlackBerry Gatekeeping Service

When you configure the BlackBerry Gatekeeping Service, you perform the following actions:

Step	Action
1	Configure permissions for gatekeeping.
2	If your organization uses Microsoft Exchange Server, see Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync. If your organization uses Microsoft 365, see Configure the mobile device access policy in Microsoft 365.
3	Configure Microsoft IIS permissions for gatekeeping.
4	Add an Entra app and obtain its Entra details for configuring modern authentication
5	Create a gatekeeping configuration.
6	Create a gatekeeping profile and assign it to user accounts, user groups, or device groups.

Configure permissions for gatekeeping

To use Exchange ActiveSync gatekeeping, you must create a user account in Microsoft Exchange Server or Microsoft 365 and give it the necessary permissions for gatekeeping.

If you are using Microsoft 365, create a Microsoft 365 user account and assign it the Mail Recipients and Organization Client Access roles.

If you are using Microsoft Exchange Server, follow the instructions below to configure management roles with the correct permissions to manage mailboxes and client access for Exchange ActiveSync. To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions to create and change management roles.

Before you begin:

- On the computer that hosts Microsoft Exchange, create an account and mailbox to manage gatekeeping in BlackBerry UEM (for example, BUEMAdmin). You must specify the login information for this account when you create an Exchange ActiveSync configuration. Note the name of this account, you will specify it at the end of the task below.
- WinRM must be configured with the default settings on the computer that hosts the Microsoft Exchange Server that you configure for gatekeeping. You must run the command `Winrm quickconfig` from a

command prompt as an administrator. When the tool displays `Make these changes [y/n]`, type `y`. After the command is successful, you see the following message.

```
WinRM has been updated for remote management.

WinRM service type changed to delayed auto start.
WinRM service started.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on
 this
 machine.
```

1. Open the Microsoft Exchange Management Shell.
2. Type `New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`. Press ENTER.
3. Type `New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`. Press ENTER.
4. Type `New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`. Press ENTER.
5. Type `Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`. Press ENTER.
6. Type `Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`. Press ENTER.
7. Type `Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`. Press ENTER.
8. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`. Press ENTER.
9. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`. Press ENTER.
10. Type `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox`. Press ENTER.
11. Type `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox`. Press ENTER.
12. Type `Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`. Press ENTER.
13. Type `New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"`. Press ENTER.
14. Type `Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`. Press ENTER.
15. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"`. Press ENTER.
16. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`. Press ENTER.
17. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`. Press ENTER.

After you finish:

- If your organization uses Microsoft Exchange Server, see Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync.
- If your organization uses Microsoft 365, see Configure the mobile device access policy in Microsoft 365.

Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync

You must configure Microsoft Exchange Server to allow only authorized devices to access Exchange ActiveSync. Devices for existing users that are not explicitly added to the allowed list in Microsoft Exchange must be quarantined until BlackBerry UEM allows them access.

To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions for the Set-ActiveSyncOrganizationSettings command. Visit https://technet.microsoft.com to find more information about the command and managing devices that access Exchange ActiveSync.

Before you begin:

- Configure permissions for gatekeeping.
- Verify with your Microsoft Exchange administrator whether or not there are any users currently using Exchange ActiveSync. If your organization's default access level for Exchange ActiveSync is set to allow, and you have users set up and successfully synchronizing their devices, you must make sure that these users have a personal exemption or device rule associated to their user account or device before you set the default access level to quarantine. If they do not, then they are quarantined and their devices do not synchronize until they are allowed by BlackBerry UEM. For more information about setting the default access level for Exchange ActiveSync to quarantine, visit support.blackberry.com/community to read article 36800.

1. On a computer that hosts the Microsoft Exchange Management Shell, open the Microsoft Exchange Management Shell.
2. Type `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine`. Press ENTER.

After you finish: Configure Microsoft IIS permissions for gatekeeping.

Configure the mobile device access policy in Microsoft 365

To use the BlackBerry Gatekeeping Service with Microsoft 365, you must configure the mobile device access policy in Microsoft 365 to quarantine devices by default.

Before you begin:

- Configure permissions for gatekeeping.
- If your organization's default access level for Exchange ActiveSync is set to allow, and you have users setup and successfully synchronizing their devices, you must make sure that these users have a personal exemption or device rule associated to their user account or device before you set the default access level to quarantine. If they do not, then they are quarantined and their devices do not synchronize until they are allowed by BlackBerry UEM. For more information about setting the default access level for Exchange ActiveSync to quarantine, visit support.blackberry.com/community to read article 33531.

1. Log in to the Microsoft 365 administration portal.
2. On the menu, click **Admin**.
3. Click **Exchange**.
4. In the **Mobile** section, click **mobile device access**.
5. Click **Edit**.
6. Click **Quarantine - Let me decide to block or allow later**.

After you finish: Configure Microsoft IIS permissions for gatekeeping.

Configure Microsoft IIS permissions for gatekeeping

BlackBerry UEM uses Windows PowerShell commands to manage the list of allowed devices. To use the BlackBerry Gatekeeping Service, you must configure Microsoft IIS permissions.

Before you begin:

- If your organization uses Microsoft Exchange Server, see Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync.
- If your organization uses Microsoft 365, see Configure the mobile device access policy in Microsoft 365.

1. On the computer that hosts the Microsoftclient access server role, open the Microsoft Internet Information Services (IIS) Manager.
2. In the left pane, expand the server.
3. Expand **Sites** > **Default Web Site**.
4. Right-click the PowerShell folder. Select **Edit Permissions**.
5. Click the **Security** tab. Click **Edit**.
6. Click **Add** and enter the <new_group> that was created when you configured the Microsoft Exchange permissions for gatekeeping.
7. Click **OK**.
8. Confirm that **Read & execute**, **List folder contents**, and **Read** are selected. Click **OK**.
9. Select the **PowerShell** folder. Double-click the **Authentication** icon.
10. Select **Windows Authentication**. Click **Enable**.
11. Close the Microsoft Internet Information Services (IIS) Manager.

After you finish: Create a gatekeeping configuration.

Add an Entra app and obtain its Entra details for configuring modern authentication

If you want to configure BlackBerry UEM to connect to Microsoft 365 using modern authentication, you will need to provide two app details: Application ID and Organization. When you perform these steps, the Entra app ID displays in the Select members(s) section. The Entra organization information displays on the Microsoft Entra ID page as a property of the directory. Record these two entries for use when you configure BlackBerry UEM for modern authentication in the gatekeeping profile.

1. Sign in to portal.azure.com.
2. Click **App registrations**.
3. Click **New registration**.
4. In the **Name** field, enter a name for the app.
5. Click **Register**.
6. Click **API permissions > Add a permission**.
7. Find the **Exchange** or **Office 365 Exchange Online** permissions group.
8. Click **Application permissions > Exchange.ManageAsApp > Add permission**.
9. To grant the administrator consent, select **Exchange.ManageAsApp > Grant admin consent**.
10. In the Manage section, click **Certificates & secrets > Upload certificate** and select the public key (cert.pem).
11. To assign a role to the app, on the Entra home page, click **Microsoft Entra ID** .

12. Click **Roles and Administrators**.
13. In the **Administrative roles** section, type "Exchange" to view the supported roles for Microsoft Exchange.
14. Click on a role to view the role details.
15. Click **Add assignments**.
16. Under **Select member(s)**, click **No member selected**.
17. Search for the Entra app ID by app ID or app name.
18. Select the app to move it to the **Selected items** section.
19. Click **Select**.
20. Click **Next**.
21. On the **Add assignments** page, ensure that the **Assignment type** is set to **Active**. For more information about assignment types, refer to the information from Microsoft.
22. Click **Assign**.

After you finish: Associate a certificate with the Entra app ID of UEM for modern authentication

Associate a certificate with the Entra app ID of UEM for modern authentication

You can request and export a new client certificate from your CA server or use a self-signed certificate. The private key must be in .pfx format. The public key can be exported as a .cer or .pem file to upload to Microsoft Entra ID.

1. Complete one of the following tasks:

Certificate	Task
If you are using an existing CA server	**a.** Request the certificate. The certificate that you request must include the app name in the subject of the certificate. Where <*app name*> is the name you assigned the app in step 4 of Add an Entra app and obtain its Entra details for configuring modern authentication. **b.** Export the public key of the certificate as a .cer or .pem file. The public key is used for the Entra app ID that is created. **c.** Export the private key of the certificate as a .pfx file.

Certificate	Task
If you are using a self-signed certificate	**a.** Create a self-signed certificate using the New-SelfSignedCertificate command. For more information, visit docs.microsoft.com and read New-SelfSignedCertificate. **1.** On the computer running Microsoft Windows, open the Windows PowerShell. **2.** Enter the following command: `$cert=New-SelfSignedCertificate -Subject "CN=<app name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`. Where <*app name*> is the name you assigned the app in step 4 of Add an Entra app and obtain its Entra details for configuring modern authentication. The certificate that you request must include the Entra app name in the subject field. **3.** Press **Enter**. **b.** Export the public key from the Microsoft Management Console (MMC). Make sure to save the public certificate as a .cer or .pem file. The public key is used for the Entra app ID that is created. **1.** On the computer running Windows, open the Certificate Manager for the logged in user. **2.** Expand **Personal**. **3.** Click **Certificates**. **4.** Right-click the <*user*>@<*domain*> and click **All Tasks > Export**. **5.** In the **Certificate Export Wizard**, click **No, do not export private key**. **6.** Click **Next**. **7.** Select **Base-64 encoded X.509 (.cer)**. Click **Next**. **8.** Provide a name for the certificate and save it to your desktop. **9.** Click **Next**. **10.** Click **Finish**. **11.** Click **OK**. **c.** Export the private key from the Microsoft Management Console (MMC). Make sure to include the private key and save it as a .pfx file. **1.** On the computer running Windows, open the Certificate Manager for the logged in user. **2.** Expand **Personal**. **3.** Click **Certificates**. **4.** Right-click the <*user*>@<*domain*> and click **All Tasks > Export**. **5.** In the **Certificate Export Wizard**, click **Yes, export private key**. **6.** Click **Next**. **7.** Select **Personal Information Exchange – PKCS #12 (.pfx)**. Click **Next**. **8.** Select the security method. **9.** Provide a name for the certificate and save it to your desktop. **10.** Click **Next**. **11.** Click **Finish**. **12.** Click **OK**.

2. Upload the public certificate (.pem or .cer file) that you exported in step 1 to associate the certificate credentials with the Entra app ID of UEM.

a) In portal.azure.com, open the <*app name*> you assigned the app in step 4 of Add an Entra app and obtain its Entra details for configuring modern authentication.
b) Click **Certificates & secrets**.
c) In the **Certificates** section, click **Upload certificate**.
d) In the **Select a file** search field, navigate to the location where you exported the certificate.
e) Click **Add**.

Create a gatekeeping configuration

You can create a gatekeeping configuration so that devices that comply with your organization's security policies can connect to the Microsoft Exchange Server or Microsoft 365.

Before you begin:

- Configure Microsoft IIS permissions for gatekeeping.
- If you want to use modern authentication, Add an Entra app and obtain its Entra details for configuring modern authentication. Note that when you enable modern authentication in the steps below, you do not need to specify the credentials of a Microsoft 365 administrator account, you just select the authentication certificate and specify the certificate password, then specify the Entra Application ID and Entra Organization values.

1. Do one of the following:
   - If you have BlackBerry UEM in an on-premises environment, on the menu bar, click **Settings > External integration > Microsoft Exchange gatekeeping**.
   - If you have BlackBerry UEM Cloud, in the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > BlackBerry Gatekeeping Service**.
2. In the Microsoft Exchange Server list section, click +.
3. Perform one of the following tasks:

Task	Steps
Connect to Microsoft 365 using modern authentication	Before you configure BlackBerry UEM to use modern authentication, you must generate a certificate that has public and private keys. You can use OpenSSL or PowerShell to generate the certificate. For more information, refer to Associate a certificate with the Entra app ID for modern authentication. **a.** Select the **Modern authentication** check box. **b.** In the **Exchange Online connection name** field, type a name for the connection. **c.** Click **Browse** and select the certificate to use for authentication. **d.** In the **Certificate password** field, type the password for the certificate. **e.** Specify your **Entra Application ID**. **f.** Specify your **Entra organization**.

Task	Steps
Connect to your Microsoft Exchange Server or Microsoft 365 using basic authentication	a. In the **Server name** field, type the name of the Microsoft Exchange Server or Microsoft 365 environment that you want to manage access to. b. Type the username and password for the account that you created to manage Exchange ActiveSync gatekeeping. c. In the **Authentication type** drop-down list, select the type of authentication that is used for the Microsoft Exchange Server or Microsoft 365. d. To enable SSL authentication between BlackBerry UEM and the Microsoft Exchange Server or Microsoft 365, select the **Use SSL** check box. Optionally, select additional certificate checks. e. In the **Proxy type** drop-down list, select the type of proxy configuration, if any, that is used between BlackBerry UEM and the Microsoft Exchange Server or Microsoft 365. f. If you selected a proxy configuration in the previous step, select the authentication type that is used on the proxy server. g. If necessary, select **Authentication required** and type the username and password.

4. Click **Test Connection** to verify that the connection is successful.
5. Click **Save**.

After you finish:

- Create a gatekeeping profile and assign it to user accounts, user groups, or device groups.
- If you configured a BlackBerry Connectivity Node server group with one or more active instances of the BlackBerry Gatekeeping Service, associate the gatekeeping profile with the appropriate server group. Any user that is assigned that gatekeeping profile can use any active instance of the BlackBerry Gatekeeping Service in that server group.

Create a gatekeeping profile

After configuring the BlackBerry Gatekeeping Service for automatic gatekeeping, you need to create a gatekeeping profile and assign it to user accounts, user groups, or device groups. The gatekeeping profile allows you to select the Microsoft Exchange gatekeeping servers or BlackBerry Connectivity Node server groups for automatic gatekeeping.

If you are using BlackBerry Connectivity Node server groups, select the appropriate server group that has one or more active instances of the BlackBerry Gatekeeping Service. Any user that is assigned this gatekeeping profile can use any active instance of the BlackBerry Gatekeeping Service in that server group.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Email, calendar and contacts > Gatekeeping**.
3. Click +.
4. Type a name and description for the profile.
5. Click **Select servers**.
6. Select one or more servers and click ➔.
7. Click **Save**.

After you finish:

- Assign the gatekeeping profile to user accounts, user groups, or device groups.
- For users to access work email, you need to assign an email profile or the BlackBerry Work app to them. If you are administering BlackBerry Work, you need to enable the BlackBerry Gatekeeping Service service in the app config.

Verify that a device is allowed to access Exchange ActiveSync

When your organization uses BlackBerry Gatekeeping Service to control which devices are allowed to access work email and organizer data from Exchange ActiveSync, you can verify the connection status between the device and Exchange ActiveSync. To establish a connection, users are assigned an email profile that has at least one gatekeeping server associated with it. The connection status is shown on the device details page of the user account, beside the email profile in the IT policy and profiles section.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Search for and click the name of a user account.
3. Select the tab for the device that you want to verify.
4. In the **IT policy and profiles** section, note the following statuses.
   - **Connection allowed**: This status is displayed when BlackBerry UEM knows the ID of the device and the device is on the allowed list.
   - **Connection pending**: This status is displayed when BlackBerry UEM knows the ID of the device and the device is in queue to be added to the allowed list.
   - **Unknown**: This status is displayed when BlackBerry UEM cannot determine the ID of the device. The device is listed in the Restricted device list and must be manually added to the allowed list.

Manually allow or block access to Exchange ActiveSync

If a device is not automatically added to the allowed list to access Exchange ActiveSync, you can manually allow access to it from the BlackBerry UEM management console. For example, if UEM cannot obtain the Exchange ActiveSync ID of the device, such as for an Android device that is activated using the MDM activation type, you must manually allow the device if you want to grant access to it.

You can also block a previously allowed device from accessing Exchange ActiveSync. Blocking a device prevents it from retrieving email messages and other information from the Microsoft Exchange Server.

1. In the management console, on the menu bar, click **Users > Exchange gatekeeping**.
2. In the **Restricted devices** list, search for a device.
3. In the **Action** column, do one of the following:
   - To allow access to Exchange ActiveSync, click ✓.
   - To block access to Exchange ActiveSync, click ⊘.

Creating email profiles

You can use email profiles to specify how devices connect to your organization's mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.

You don't need to use an email profile if your organization uses BlackBerry Work to manage email, calendar, and contacts for users devices. For more information about managing BlackBerry Work, see Managing apps and the BlackBerry Work Administration Guide.

If you want to use Exchange ActiveSync, you should note that:

- Exchange ActiveSync can be configured to control which devices can access it.
- For extended email security, you can enable S/MIME for iOS and Android devices.
- If you enable S/MIME, you can use other profiles to allow devices to automatically retrieve S/MIME certificates and check certificate status.

If you want to use Notes Traveler, you should note that to use it with iOS devices, you must enable the BlackBerry Secure Gateway.

You can also use IMAP/POP3 email profiles to specify how iOS, macOS, Android, and Windows devices connect to IMAP or POP3 mail servers and synchronize email messages. Devices activated to use Knox MDM do not support IMAP or POP3.

Create an email profile

The required profile settings vary for each device type and depend on the mail server used in your organization's environment.

Before you begin: If you use certificate-based authentication between devices and your mail server, you must create a CA certificate profile and assign it to users. You must also make sure that devices have a trusted client certificate.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Email, calendar and contacts > Email**.
3. Click +.
4. Type a name and description for the profile.
5. If necessary, type the domain name of the mail server. If the profile is for multiple users who may be in different Microsoft Active Directory domains, you can use the `%UserDomain%` variable.
6. In the **Email address** field, perform one of the following actions:
   - If the profile is for one user, type the email address of the user.
   - If the profile is for multiple users, type `%UserEmailAddress%`.
7. Type the host name or IP address of the mail server.
8. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
   - If the profile is for multiple users in an IBM Notes Traveler environment, type `%UserDisplayName%`.
9. If you configured server groups to direct BlackBerry Secure Gateway traffic to a specific regional connection to the BlackBerry Infrastructure, in the **BlackBerry Secure Gateway Service server group** drop-down list, click the appropriate server group.

10. Click the tab for each device type in your organization and configure the appropriate values for each profile setting.
11. Click **Add**.

After you finish:

- If necessary, rank the profile.
- For Android devices with MDM controls activations, BlackBerry UEM sends the email profile to the device but the user must configure the connection to the mail server manually.

Email 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. Email profiles are supported on the following device types:

- iOS
- macOS
- Android
- Windows

Common: Email profile settings

Common: Email profile setting	Description
Domain name	This setting specifies the domain name of the mail server.
Email address	This setting specifies the user's email address. If the profile is for multiple users, you can use the %UserEmailAddress% variable.
Host name or IP address	This setting specifies the host name or IP address of the mail server.
Username	This setting specifies the user's username. If the profile is for multiple users, you can use the %UserName% variable. If the profile is for multiple users in an IBM Notes Traveler environment, use %UserDisplayName%.
Automatic gatekeeping servers	If you configured server groups to direct BlackBerry Secure Gateway traffic or BlackBerry Gatekeeping Service traffic to a specific regional connection to the BlackBerry Infrastructure, this setting specifies the appropriate server group.

iOS: Email profile settings

These settings also apply to iPadOS devices

iOS: Email profile setting	Description
Delivery settings	
Allow messages to be moved	This setting specifies whether users can move email messages from this account to another existing email account on a device.

iOS: Email profile setting	Description
Allow recent addresses to be synced	This setting specifies whether a user can sync recently used addresses across devices.
Use only in Mail	This setting specifies whether apps other than the Mail app can use this account to send email messages.
Enable S/MIME	This setting specifies whether a user can send S/MIME protected email messages.
Enable digitally signed S/MIME messages	This setting specifies whether a device sends outgoing messages with a digital signature. This setting is valid only if the "Enable S/MIME" setting is selected.
Signing credentials	This setting specifies how devices find the certificates required to sign messages. This setting is valid only if the "Enable S/MIME" setting is selected. After you choose the profile type you want to use, you specify the shared certificate, SCEP, or user credential profile. This setting is valid only if the "Enable S/MIME" setting is selected.
Signing shared certificate	This setting specifies the shared certificate profile for a client certificate that a device uses to sign email messages. This setting is valid only if the "Enable S/MIME" setting is selected.
Signing SCEP	This setting specifies the SCEP profile that devices can use to retrieve the certificates required to sign email messages using S/MIME. This setting is valid only if the "Enable S/MIME" setting is selected.
Signing user credential	This setting specifies the user credential profile that devices can use to obtain the client certificates required to sign email messages using S/MIME. This setting is valid only if the "Enable S/MIME" setting is selected.
User can turn on or turn off S/MIME signing	This setting specifies whether a user is allowed to turn on or turn off S/MIME signing. This setting is valid only if the "Enable S/MIME" setting is selected.
User can change signing credentials	This setting specifies whether a user can override signing credentials. This setting is valid only if the "Enable S/MIME" setting is selected.
Enable S/MIME message encryption	This setting specifies whether a device encrypts outgoing email messages with S/MIME encryption. This setting is valid only if the "Enable S/MIME" setting is selected.

iOS: Email profile setting	Description
Encryption credentials	This setting specifies how devices find the certificates required to encrypt messages. After you select the profile type, you select the shared certificate, SCEP, or user credential profile that you want to use. This setting is valid only if the "Enable S/MIME" setting is selected.
Encryption shared certificate	This setting specifies the shared certificate profile for a client certificate that a device can use to encrypt email messages. Devices choose the appropriate certificate for the recipient to encrypt messages using S/MIME. This setting is valid only if the "Enable S/MIME" setting is selected.
Encryption SCEP	This setting specifies the SCEP profile that devices can use to retrieve the certificates required to encrypt email messages using S/MIME. This setting is valid only if the "Enable S/MIME" setting is selected.
Encryption user credential	This setting specifies the user credential profile that devices can use to retrieve the client certificates required to encrypt email messages using S/MIME. This setting is valid only if the "Enable S/MIME" setting is selected.
User can override S/MIME encryption	This setting specifies whether a user can turn on or turn off the encryption setting. This setting is valid only if the "Enable S/MIME" setting is selected.
User can override S/MIME encryption credentials	This setting specifies whether a user can override S/MIME encryption credentials. This setting is valid only if the "Enable S/MIME" setting is selected.
Encrypt messages	This setting specifies whether all email messages must be encrypted when the user sends them (Required), or if the user can choose which messages to encrypt at the time they send them (Allow). This setting takes effect only if the "Enable S/MIME" setting is selected. This setting is valid only if the "Enable S/MIME" setting is selected.
Allow Mail Drop	This setting specifies whether users with the MDM controls activation type can send files from this account using Mail Drop.
Days to synchronize	This setting specifies the number of days in the past to synchronize email messages and organizer data to a device. **Note:** This setting applies only to the default mail and organizer apps on devices with the MDM controls activation type.
Per-account VPN	This setting specifies the VPN profile that is used for this account’s network communication. This setting applies only to iOS 14 and later and iPadOS 14 and later devices.

iOS: Email profile setting	Description
Authentication	
Enable BlackBerry Secure Gateway	This setting specifies whether devices with the MDM controls activation type use the BlackBerry Secure Gateway to connect to the mail server. The BlackBerry Secure Gateway provides a secure connection to your organization's mail server through the BlackBerry Infrastructure and BlackBerry UEM. If you configured server groups to direct BlackBerry Secure Gateway traffic to a specific regional connection to the BlackBerry Infrastructure, you must associate the email profile with the appropriate server group.
Authentication type	This setting specifies the type of authentication a device uses to connect to the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected.
Shared certificate profile	This setting specifies the shared certificate profile for the client certificate that a device uses to connect to the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected and the "Authentication type" setting is set to "Shared certificate."
Associated SCEP profile	This setting specifies the associated SCEP profile that a device uses to enroll a client certificate to use for authentication with the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected and the "Authentication type" setting is set to "SCEP".
Associated ACME profile	This setting specifies the associated ACME profile that a device uses to enroll a client certificate to use for authentication with the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected and the "Authentication type" setting is set to "ACME".
Associated user credential profile	This setting specifies the associated user credential profile that a device uses to enroll a client certificate to use for authentication with the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected and the "Authentication type" setting is set to "User credential."
Use credentials and certificate	This setting specifies whether a device uses credentials and a client certificate obtained using the associated SCEP profile to authenticate with the mail server. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected and the "Authentication type" setting is set to "SCEP."
Use OAuth for authentication	This setting specifies whether the connection should use OAuth for authentication.

iOS: Email profile setting	Description
OAuth sign-in URL	This setting specifies the URL that this account should use to sign in to OAuth. When you specify this URL you must specify a host because auto-discovery is not used. This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected.
OAuth token request URL	This setting specifies the URL that this account should use for token requests using OAuth This setting is valid only if the "Enable BlackBerry Secure Gateway" setting is not selected.
Use SSL	This setting specifies whether a device must use SSL to connect to the mail server.
Accept all SSL certificates	This setting specifies whether all SSL certificates are accepted. This setting is valid only if the "Use SSL" setting is selected.
External email domains	
External email domain allowed list	This setting specifies the list of domains that a user can send work email or calendar entries to. For example, when a user adds a recipient who has an email address in the allowed domain to an email message or calendar entry, no warning message is displayed. This setting applies to the work space only. If you list multiple domain names, separate the domain names with a comma (,), semicolon (;), or space.
External email domain restricted list	This setting specifies the list of domains that users cannot send work email or calendar entries to. For example, if a user tries to add a recipient with an email address from the restricted domain to an email message or calendar invitation, the Work Connect app prevents the user from completing the task. This setting applies to the work space only. If you list multiple domain names, separate the domain names with a comma (,), semicolon (;), or space.
Enabled services	
Mail	This setting specifies whether users can access their work email on the device.
Contacts	This setting specifies whether users can access their work contacts on the device.
Calendars	This setting specifies whether users can access their work calendar on the device.
Reminders	This setting specifies whether users can access their work reminders on the device.
Notes	This setting specifies whether users can access their work notes on the device.
Account modification	

iOS: Email profile setting	Description
Mail	This setting specifies whether users can change whether access to work email is enabled or disabled on the device.
Contacts	This setting specifies whether users can change whether access to work contacts is enabled or disabled on the device.
Calendars	This setting specifies whether users can change whether access to their work calendar is enabled or disabled on the device.
Reminders	This setting specifies whether users can change whether access to their work reminders is enabled or disabled on the device.
Notes	This setting specifies whether users can change whether access to their work notes is enabled or disabled on the device.

macOS: Email profile settings

macOS applies profiles to user accounts or devices. Email profiles are applied to user accounts.

macOS: Email profile setting	Description
Path	This setting specifies the network path of the mail server.
Port	This setting specifies the port that is used to connect to the mail server.
Use SSL	This setting specifies whether a device must use SSL to connect to the mail server.
External host name or IP address	This setting specifies the external host name or IP address of the mail server.
Use external SSL	This setting specifies whether a device must use SSL to connect to the external mail server.
External path	This setting specifies the network path of the external mail server.
External server port	This setting specifies the port that is used to connect to the external mail server.

Android: Email profile settings

Android: Email profile setting	Description
Delivery settings	
Profile type	This setting specifies whether you want this profile to support Exchange ActiveSync or IBM Notes Traveler. The default value is "Exchange ActiveSync."

Android: Email profile setting	Description
Days to synchronize	This setting specifies the number of days in the past to synchronize email messages and organizer data to an Android device with the MDM controls activation type. For Android devices that use Samsung Knox MDM, if you set the value to Unlimited, only one month is synchronized. **Note:** This setting applies only to the default mail and organizer apps on Android devices with the MDM controls activation type.
Authentication type	This setting specifies the type of authentication an Android device uses to connect to the mail server.
Associated SCEP profile	This setting specifies the associated SCEP profile that an Android device uses to obtain a client certificate to authenticate with the mail server. This setting is valid only if the "Authentication type" setting is set to "SCEP."
Use credentials and certificate	This setting specifies whether a device uses credentials and a client certificate obtained using the associated SCEP profile to authenticate with the mail server. This setting is valid only if the "Authentication type" setting is set to "SCEP."
Shared certificate profile	This setting specifies the shared certificate profile for the client certificate that an Android device uses to connect to the mail server. This setting is valid only if the "Authentication type" setting is set to "Shared certificate."
Associated user credential profile	This setting specifies the user credential profile for the client certificate that an Android device uses to connect to the mail server. This setting is valid only if the "Authentication type" setting is set to "User credential."
Use SSL	This setting specifies whether a device must use SSL to connect to the mail server.
Accept all SSL certificates	This setting specifies whether a device automatically accepts untrusted SSL certificates from the mail server. If this setting is not selected, devices can connect only to mail servers that use a trusted SSL certificate.
Maximum email attachment size	This setting specifies the maximum size allowed for email attachments (in MB). This setting applies only to Android Enterprise devices.
Default email signature for new messages	This setting specifies an email signature that is automatically appended to new email messages. This setting applies only to Android Enterprise devices.

Android: Email profile setting	Description
Enable S/MIME	This setting specifies whether devices can send S/MIME-protected email messages. For devices that use the BlackBerry Productivity Suite, you must set a value for the "S/MIME support" setting instead.
Sign messages	This setting specifies whether devices send all outgoing email messages with a digital signature. This setting is valid only if the "Enable S/MIME" setting is selected. For Android Enterprise devices, this setting applies only to devices that use Divide Productivity. For devices that use the BlackBerry Productivity Suite, you must set a value for the "Digitally signed S/MIME messages" setting instead.
Signing credentials	This setting specifies the credentials that a device uses to sign email messages. This setting is valid only if the "Sign messages" setting is selected.
Signing shared certificate	This setting specifies the shared certificate profile for a client certificate that a device uses to sign email messages. This setting is valid only if the "Signing credentials" setting is set to "Shared certificate."
Signing SCEP	This setting specifies the SCEP profile for a client certificate that a device uses to sign email messages. This setting is valid only if the "Signing credentials" setting is set to "SCEP."
Signing user credential	This setting specifies the user credential profile for a client certificate that a device uses to sign email messages. This setting is valid only if the "Signing credentials" setting is set to "User credential."
Encrypt messages	This setting specifies whether devices encrypt outgoing email messages using S/MIME encryption. This setting is valid only if the "Enable S/MIME" setting is selected. For Android Enterprise devices, this setting applies only to devices that use Divide Productivity. For devices that use the BlackBerry Productivity Suite, you must set a value for the "Digitally signed S/MIME messages" setting instead.
Encryption credentials	This setting specifies the credentials that a device uses to encrypt email messages. This setting is valid only if the "Encrypt messages" setting is selected.

Android: Email profile setting	Description
Encryption shared certificate	This setting specifies the shared certificate profile for a client certificate that a device uses to encrypt email messages. This setting is valid only if the "Encryption credentials" setting is set to "Shared certificate."
Encryption SCEP	This setting specifies the SCEP profile for a client certificate that a device uses to encrypt email messages. This setting is valid only if the "Signing credentials" setting is set to "SCEP."
Encryption user credential	This setting specifies the user credential profile for a client certificate that a device uses to encrypt email messages. This setting is valid only if the "Signing credentials" setting is set to "User credential."
Require smart card authentication for email	This setting specifies whether a smart card is required for Samsung Knox devices to authenticate with the mail server.
Allow user to edit settings	Specify whether the user can edit delivery settings. This setting applies only to Samsung Knox devices.
External email domains	
External email domain allowed list	This setting specifies the list of domains that a user can send work email or calendar entries to. For example, when a user adds a recipient who has an email address in the allowed domain to an email message or calendar entry, no warning message is displayed. This setting applies to the work space only. If you list multiple domain names, separate the domain names with a comma (,), semicolon (;), or space.
External email domain restricted list	This setting specifies the list of domains that users cannot send work email or calendar entries to. For example, if a user tries to add a recipient with an email address from the restricted domain to an email message or calendar invitation, the Email app or Calendar app prevents the user from completing the task. This setting applies to the work space only. If you list multiple domain names, separate the domain names with a comma (,), semicolon (;), or space.

Windows: Email profile settings

Windows: Email profile setting	Description
Delivery settings	
Profile type	This setting specifies whether you want this profile to support Exchange ActiveSync or IBM Notes Traveler.

Windows: Email profile setting	Description
Account name	This setting specifies the work email account name that appears on the Windows device. You can use a variable such as %UserEmailAddress%.
Synchronization interval	This setting specifies how often a Windows device downloads new email messages from the mail server.
Days to synchronize	This setting specifies the number of days in the past to synchronize email messages and organizer data to a Windows device.
Use SSL	This setting specifies whether a Windows device must use SSL to connect to the mail server.
Content to synchronize	
Email	This setting specifies whether a Windows device synchronizes email messages with the mail server.
Contacts	This setting specifies whether a Windows device synchronizes contacts with the mail server.
Calendar	This setting specifies whether a Windows device synchronizes calendar entries with the mail server.
Task	This setting specifies whether a Windows device synchronizes task data with the mail server. This setting is valid only if the "Profile type" setting is set to "Exchange ActiveSync."

Protecting email data sent to iOS devices using the BlackBerry Secure Gateway

You can use the BlackBerry Secure Gateway to protect email data and allow iOS and iPadOS devices to send and receive work email. The gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry UEM to your organization's mail server without requiring you to expose your mail server outside the firewall or locate your mail server in a DMZ.

The devices must be activated with the MDM controls activation type.

Step	Action
1	In the email profile, select the "Enable BlackBerry Secure Gateway" setting.
2	If your environment includes iOS or iPadOS 13.0 or later devices and your organization's mail server is configured to use modern authentication (OAuth): • In the email profile, select the "Use OAuth for authentication" setting. • Configure BlackBerry UEM to trust the Exchange ActiveSync server or identity provider certificate • Configure the BlackBerry Secure Gateway to use OAuth with the mail server.
3	If you configured server groups to support regional connections to the BlackBerry Infrastructure and direct BlackBerry Secure Gateway traffic, select the appropriate server group the "BlackBerry Secure Gateway Service server group" setting in the email profile.

Configure BlackBerry UEM to trust the Exchange ActiveSync server or identity provider certificate

If your environment includes iOS and iPadOS 13.0 and later devices and you use modern authentication (OAuth) to connect to Microsoft Exchange Online, you must add the certificate (or the root certificate) of the identity provider to BlackBerry UEM. The BlackBerry Secure Gateway requires the certificate to trust the identity provider when it establishes the connection.

If your Exchange ActiveSync server is configured to require a TLS connection, you must also add the certificate (or the root certificate) of the Exchange ActiveSync server to BlackBerry UEM. The BlackBerry Secure Gateway requires the certificate to trust the server when it establishes the TLS/SSL connection.

Before you begin: Export the certificates in X.509 format (*.cer, *.der) from the following servers and store them in a network location that you can access from the management console:

- Active Directory identity provider, if your environment supports modern authentication
- Exchange ActiveSync server, if your Exchange ActiveSync is configured to require a TLS connection

1. In the management console, on the menu bar, click **Settings > External Integration > Trusted certificates**.
2. Click + beside **Exchange ActiveSync server trusts**.
3. Click **Browse**.
4. Select the certificate file that you want to use.
5. Click **Open**.

6. Type a description for the certificate.
7. Click **Add**.

After you finish: Configure the BlackBerry Secure Gateway to use OAuth with supported TLS versions and ciphers.

Configure the BlackBerry Secure Gateway to use OAuth with supported TLS versions and ciphers

You can configure the BlackBerry Secure Gateway to use OAuth for modern authentication. To use OAuth, you need to specify the mail server URL from the email profile, and the URL to retrieve the identity provider discovery document. For more information on the discovery document, see the Microsoft documentation.

You can also specify the TLS version and Microsoft Exchange SSL ciphers that the BlackBerry Secure Gateway uses for connections to Exchange ActiveSync. You may need to update this list according to the security requirements of yourExchange ActiveSync server.

Before you begin: Configure BlackBerry UEM to trust the Exchange ActiveSync server or identity provider certificate

1. In the management console, on the menu bar, click **Settings > External Integration > BlackBerry Secure Gateway**.
2. To add or remove a TLS version or SSL cipher, click + in the appropriate table.
3. Click the TLS version or cipher that you want to add or remove from the **Selected** list.
4. Click the arrow to move the item to the desired list.
5. Click **Assign**.
6. To use modern authentication, select **Enable OAuth for mail server authentication**.
7. In the **Discovery endpoint** field, type the URL that the BlackBerry Secure Gateway uses to retrieve and cache the identity provider discovery document.
   - Format:`https://<identity provider>/.well-known/openid-configuration`
   - Example: `https://login.microsoftonline.com/common/.well-known/openid-configuration`
   - Example: `https://login.windows.net/common/.well-known/openid-configuration`

   The BlackBerry Secure Gateway retrieves both the unversioned and v2.0 discovery documents and periodically refreshes the cached documents.
8. In the **Mail server resource** field, type the URL for the mail server specified in the email profile, starting with "https://" (for example. `https://outlook.office365.com`).
9. Click **Save**.

Enable the BlackBerry Hub app for Android Enterprise devices

BlackBerry Hub is an Android app that allows users to view messages, notifications, and events in one spot.

To allow users with Android Enterprise devices to view both work and personal messages in BlackBerry Hub, you need to verify some settings in BlackBerry UEM.

1. For the IT policy that is assigned to users, in the BlackBerry Productivity Suite section, verify that the **Allow unified account view in BlackBerry Hub** IT policy rule is selected.
2. In the app configuration for BlackBerry Hub, verify that the following items are selected:
   - **IPC across profiles**
   - **Access work content**

After you finish: For information about using the BlackBerry Hub on devices, such as adding an email account or customizing the BlackBerry Hub settings, see the BlackBerry Hub content.

For troubleshooting information, see KB 37721.

Extending email security using S/MIME

From the email profile, you can enable S/MIME so that iOS and Android device users can choose to extend email security. S/MIME provides a standard method of encrypting and signing email messages. When using a work email account that supports S/MIME-protected messages, users can specify whether to use S/MIME to encrypt, sign, or encrypt and sign work email messages. Note that S/MIME cannot be enabled for personal email accounts.

S/MIME settings take precedence over PGP settings. When S/MIME support is set to "Required," PGP settings are ignored.

Retrieving S/MIME certificates

You can use certificate retrieval profiles to allow Android and iOS devices to search for and retrieve recipients' S/MIME certificates from each of the specified LDAP certificate servers. If a required S/MIME certificate is not already in a device's certificate store, the device retrieves it from the server and imports it into the certificate store automatically. If there is more than one S/MIME certificate and a device is unable to determine the preferred one, the device displays all the S/MIME certificates so that the user can choose which one to use.

You can require that devices use either simple authentication or Kerberos authentication to authenticate with LDAP certificate servers. You can include the required authentication credentials in the certificate retrieval profiles so that devices can automatically authenticate with LDAP certificate servers. If you do not include the required credentials, the device prompts the user for the credentials the first time that the device attempts to authenticate with an LDAP certificate server.

If you do not create a certificate retrieval profile and assign it to user accounts, user groups, or device groups, users must manually import S/MIME certificates from a work email attachment or a computer.

Create a certificate retrieval profile

Before you begin:

- To allow devices to trust LDAP certificate servers when they make secure connections, you might need to distribute CA certificates to devices. If necessary, create CA certificate profiles and assign them to user accounts, user groups, or device groups. For more information about CA certificates, see Sending CA certificates to devices and apps.
- If you implement Kerberos authentication for S/MIME certificate retrieval, you must assign a single sign-on profile to the applicable users or user groups. For more information about single sign-on profiles, see Enable automatic authentication for iOS devices.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Certificates > Certificate retrieval**.
3. Click +.
4. Type a name and description for the certificate retrieval profile.
5. In the table, click +.
6. In the **Service URL** field, type the FQDN of an LDAP certificate server using the format ldap://<*fqdn*>:<*port*>. (For example, ldap://server01.example.com:389).
7. In the **Search base** field, type the base DN that is the starting point for LDAP certificate server searches.
8. In the **Search scope** drop-down list, perform one of the following actions:
   - To search the base object only (base DN), click **Base**. This option is the default value.
   - To search one level below the base object, but not the base object itself, click **One level**.

- To search the base object and all levels below it, click **Subtree**.
- To search all levels below the base object, but not the base object itself, click **Children**.

9. If authentication is required, perform the following actions:
   a) In the **Authentication type** drop-down list, click **Simple** or **Kerberos**.
   b) In the **LDAP user ID** field, type the DN of an account that has search permissions on the LDAP certificate server (for example, cn=admin,dc=example,dc=com).
   c) In the **LDAP password** field, type the password for the account that has search permissions on the LDAP certificate server.
10. If necessary, select the **Use secure connection** check box.
11. In the **Connection timeout** field, type the amount of time, in seconds, that the device waits for the LDAP certificate server to respond.
12. Click **Add**.
13. Repeat steps 5 to 12 for each LDAP certificate server.
14. Click **Add**.

After you finish: If necessary, rank the profile.

Determining the status of S/MIME certificates on devices

You can use OCSP and CRL profiles to allow iOS and Android devices to check the status of S/MIME certificates to see if it's a valid certificate. You can assign an OCSP profile and a CRL profile to user accounts, user groups, or device groups.

You can use the OSCP profile to specify the OSCP responders where you want the devices to retrieve the status of S/MIME certificates from.

You can use CRL profiles to allow devices check the responders defined within the S/MIME certificate. You can also configure it so that BlackBerry UEM requests the status of S/MIME certificates using HTTP, HTTPS, or LDAP. If you use Exchange ActiveSync for certificate retrieval, devices use Exchange ActiveSync to check the status of S/MIME certificates. If you use LDAP for certificate retrieval, devices uses the OCSP (Online Certificate Status Protocol) to check the status of certificates.

Certificate status indicators may vary between devices. For more information, see the user guide for the device to read about secure email icons.

Create an OCSP profile

OCSP profiles are supported for iOS and Android devices.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Certificates > OCSP**.
3. Click +.
4. Type a name and description for the OCSP profile.
5. Perform the following actions:
   a) In the table, click +.
   b) In the **Service URL** field, type the web address of an OCSP responder.
   c) In the **Connection timeout** field, type the amount of time, in seconds, that the device waits for the OCSP response.
   d) Click **Add**.
6. Repeat step 3 through step 5 for each OCSP responder.

7. Click **Add**.

After you finish: If necessary, rank the profile.

Create a CRL profile

CRL profiles are supported for iOS and Android devices.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Certificates > CRL**.
3. Click +.
4. Type a name and description for the CRL profile.
5. To allow devices to use responder URLs defined in the certificate, select the **Use certificate extension responders** check box.
6. Perform any of the following tasks:

Task	Steps
Use HTTP or HTTPS for CRL	a. In the **HTTP for CRL** section, click +. b. Type a name and description for the HTTP CRL configuration. c. In the **Service URL** field, type the web address of an HTTP or HTTPS server. d. Click **Add**. e. Repeat these steps for each HTTP or HTTPS server.
Use LDAP for CRL	a. In the **LDAP for CRL** section, click +. b. Type a name and description for the LDAP CRL configuration. c. In the **Service URL** field, type the FQDN of an LDAP server using the format ldap://<*fqdn*>:<*port*> (for example, ldap://server01.example.com:389). For secure connections, use the format ldaps://<*fqdn*>:<*port*>. d. In the **Search base** field, type the base DN that is the starting point for LDAP server searches. e. In the **Search scope** drop-down list, select the appropriate search scope for LDAP servers searches. f. If necessary, select the **Use secure connection** check box. g. In the **LDAP user ID** field, type the DN of an account that has search permissions on the LDAP server (for example, cn=admin,dc=example,dc=com). h. In the **LDAP password** field, type the password for the account that has search permissions on the LDAP server. i. Click **Add**. j. Repeat these steps for each LDAP server.

7. Click **Add**.

After you finish: If necessary, rank the profile.

Extending email security using PGP

For iOS and Android devices, you can extend email security for device users by enabling PGP. PGP protects email messages on devices using OpenPGP format. Users can sign, encrypt, or sign and encrypt email messages using PGP protection when they use a work email address. PGP cannot be enabled for personal email addresses.

You enable PGP for users in an email profile. You can force iOS and Android device users to use PGP, disallow the use of PGP, or make it optional. When PGP use is optional (the default setting), a user can enable PGP on the device and specify whether to encrypt, sign, or encrypt and sign email messages.

To sign and encrypt email messages, users must store PGP keys for each recipient on their devices. Users can store PGP keys by importing the files from a work email message.

You can configure PGP using the appropriate email profile settings.

Enforcing secure email using message classification

Message classification allows your organization to specify and enforce secure email policies and add visual markings to email messages on iOS and Android devices. You can use BlackBerry UEM to provide iOS and Android device users with similar options for message classification that you make available on their computer email applications. You can define the following rules to apply to outgoing messages, based on the messages' classifications:

- Add a label to identify the message classification (for example, Confidential)
- Add a visual marker to the end of the subject line (for example, [C])
- Add text to the beginning or end of the body of an email (for example, This message has been classified as Confidential)
- Set S/MIME or PGP options (for example, sign and encrypt)
- Set a default classification

For iOS and Android devices, you can use message classification to require users to sign, encrypt, or sign and encrypt email messages, or add visual markings to email messages that they send from their devices. You can use email profiles to specify message classification configuration files (with .json file name extensions) to send to users' devices. When users either reply to email messages that have message classification set or compose secure email messages, the message classification configuration determines the classification rules that devices must enforce on outgoing messages.

The message protection options on a device are limited to the types of encryption and digital signing that are permitted on the device. When a user applies a message classification to an email message on a device, the user must select one type of message protection that the message classification permits, or accept the default type of message protection. If a user selects a message classification that requires signing, encrypting, or signing and encrypting of the email message, and the device does not have S/MIME or PGP configured, the user cannot send the email message.

S/MIME and PGP settings take precedence over message classification. Users can raise, but not lower, the message classification levels on their devices. The message classification levels are determined by the secure email rules of each classification.

When message classification is enabled, users cannot use the BlackBerry Assistant to send email messages from their devices.

You can configure message classification using the appropriate email profile settings.

For more information about how to create message classification configuration files, see KB 36736 to read article 36736.

Create an IMAP/POP3 email profile

IMAP/POP3 email profiles to specify how iOS, iPadOS, macOS, Android, and Windows devices connect to IMAP or POP3 mail servers and synchronize email messages.

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

Note: BlackBerry UEM sends the email profile to Android devices, but the user must manually configure the connection to the mail server.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Email, calendar and contacts > IMAP/POP3 email**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Email type** field, select the type of email protocol.
6. In the **Email address** field, perform one of the following actions:
   - If the profile is for one user, type the email address of the user.
   - If the profile is for multiple users, type `%UserEmailAddress%`.
7. In the **Incoming mail settings** section, type the host name or IP address of the mail server for receiving mail.
8. If necessary, type the port for receiving mail.
9. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
10. In the **Outgoing mail settings** section, type the host name or IP address of the mail server for sending mail.
11. If necessary, type the port for sending mail.
12. If necessary, select **Authentication required for outgoing mail** and specify the credentials used for sending mail.
13. Click the tab for each device type in your organization and configure the appropriate values for each profile setting. See the following:
    - iOS and macOS: IMAP/POP3 email profile settings
    - Android: IMAP/POP3 email profile settings
    - Windows: IMAP/POP3 email profile settings
14. Click **Add**.

iOS and macOS: IMAP/POP3 email profile settings

These settings also apply to iPadOS devices

macOS applies profiles to user accounts or devices. IMAP/POP3 profiles are applied to user accounts.

iOS: IMAP/POP3 email profile setting	Description
IMAP path prefix	This setting specifies the IMAP path prefix, if necessary. If necessary, contact your ISP for more information. This setting is valid only if the value for the "Email type" setting is set to "IMAP."

iOS: IMAP/POP3 email profile setting	Description
Allow messages to be moved	This setting specifies whether users can move email messages from this account to another email account on an iOS device.
Allow recent addresses to be synced	This setting specifies whether an iOS device user can synchronize recently used email addresses across devices.
Use only in Mail	This setting specifies whether apps other than the Mail app on an iOS device can use this account to send email messages.
Enable S/MIME	This setting specifies whether an iOS device user can send S/MIME protected email messages. S/MIME is supported only on devices that are activated with MDM controls.
Signing credentials	This setting specifies the credentials that a device uses to sign email messages. This setting is valid only if the "Enable S/MIME" setting is selected.
Signing shared certificate	This setting specifies the shared certificate profile for a client certificate that a device uses to sign email messages. This setting is valid only if the "Signing credentials" setting is set to "Shared certificate."
Signing SCEP	This setting specifies the SCEP profile that devices can use to retrieve the certificates required to sign email messages using S/MIME. This setting is valid only if the "Signing credentials" setting is set to "SCEP."
Signing user credential	This setting specifies the user credential profile that devices can use to obtain the client certificates required to sign email messages using S/MIME. This setting is valid only if the "Signing credentials" setting is set to "User credential."
Encryption credentials	This setting specifies how devices find the certificates required to encrypt messages. This setting is valid only if the "Enable S/MIME" setting is selected. After you select the profile type, you select the shared certificate, SCEP, or user credential profile that you want to use.
Encryption shared certificate	This setting specifies the shared certificate profile for a client certificate that a device uses to encrypt email messages. Devices choose the appropriate certificate for the recipient to encrypt messages using S/MIME. This setting is valid only if the "Encryption credentials" setting is set to "Shared certificate."

iOS: IMAP/POP3 email profile setting	Description
Encryption SCEP	This setting specifies the SCEP profile that devices can use to retrieve the certificates required to encrypt email messages using S/MIME. This setting is valid only if the "Encryption credentials" setting is set to "SCEP."
Encryption user credential	This setting specifies the user credential profile that devices can use to retrieve the client certificates required to encrypt email messages using S/MIME. This setting is valid only if the "Encryption credentials" setting is set to "User credential."
Encrypt messages	This setting specifies whether all email messages must be encrypted when the user sends them (Required), or if the user can choose which messages to encrypt at the time they send them (Allow). This setting takes effect only if the "Enable S/MIME" setting is selected.
Allow Mail Drop	This setting specifies whether users can send files from this account using Mail Drop.
Per-account VPN	This setting specifies the VPN profile that is used for this account’s network communication.

Android: IMAP/POP3 email profile settings

Android: IMAP/POP3 email profile setting	Description
IMAP path prefix	This setting specifies the IMAP path prefix, if necessary. If necessary, contact your ISP for more information. This setting is valid only if the value for the "Email type" setting is set to "IMAP."
Delete email from server	This setting specifies when to delete an email from the mail server. This setting is valid only if the value for the "Email type" setting is set to "POP3."

Windows: IMAP/POP3 email profile settings

Windows: IMAP/POP3 email profile setting	Description
Delete email from server	This setting specifies how email messages are treated when a user deletes them. Email messages can be deleted from the server (hard delete) or removed from the inbox but kept in the Trash folder (soft delete). This setting is valid only if the value for the "Email type" is set to "IMAP."

Windows: IMAP/POP3 email profile setting	Description
Domain	This setting specifies the domain of the mail server.
Synchronization interval	This setting specifies how often a Windows device downloads new content from the mail server.
Initial retrieval amount	This setting specifies the number of days in the past to synchronize email messages and organizer data to a Windows device.
Only use the cellular network and not Wi-Fi	This setting specifies whether email messages are sent and received only over the wireless network.

Setting up CardDAV and CalDAV profiles for iOS and macOS devices

You can use CardDAV and CalDAV profiles to allow iOS, iPadOS, and macOS devices to access contact and calendar information on a remote server. You can assign CardDAV and CalDAV profiles to user accounts, user groups, or device groups. Multiple devices can access the same information.

CardDAV and CalDAV profiles are applied to user accounts.

Create a CardDAV profile

Before you begin: Verify that the device can access an active CardDAV server.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Email, calendar and contacts > CardDAV**.
3. Click +.
4. Type a name and description for the profile.
5. Type the server address for the profile. This is the FQDN of the computer that hosts the calendar application.
6. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
7. If required, enter the port for the CardDAV server.
8. If required, select the **Use SSL** check box and enter the URL for the SSL server.
9. If required, in the **Per-account VPN** field, select the VPN profile that you want to use for this account's network communication.
10. Click **Add**.

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

Create a CalDAV profile

Before you begin: Verify that the device can access an active CalDAV server.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Email, calendar and contacts > CalDAV**.
3. Click +.
4. Type a name and description for the profile.
5. Type the server address for the profile. This is the FQDN of the computer that hosts the calendar application.
6. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
7. If required, enter the port for the CalDAV server.
8. If required, select the **Use SSL** check box and enter the URL for the SSL server.
9. If required, in the **Per-account VPN** field, select the VPN profile that you want to use for this account's network communication.

10. Click **Add**.

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

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