BlackBerry 2FA

Configuration Guide

Server

Contents

Steps to configure the BlackBerry 2FA server

When you configure the BlackBerry 2FA server, you perform the following actions.

Task	Description
1	If necessary, download and install the BlackBerry 2FA server. After you install the server, you must generate and download an activation file and use it to enable communication between the BlackBerry 2FA server and BlackBerry UEM. For more information, see the BlackBerry 2FA server installation and upgrade content.
2	On the VPN server, create a profile for the BlackBerry 2FA server. For more information, see Configuring a connection between the BlackBerry 2FA server and a VPN gateway.
3	Configure the BlackBerry 2FA server to connect to a VPN gateway
4	Configure the connection to the REST API endpoint
5	Create a REST API client in the BlackBerry 2FA server
6	Enable MS-CHAP authentication for users in a domain
7	Configure the BlackBerry 2FA app
8	Assign a VPN gateway or REST client configuration to a user group
9	If needed, send the BlackBerry 2FA app to devices. For more information, see Installing the BlackBerry 2FA app on devices.

Configuring a connection between the BlackBerry 2FA server and a VPN gateway

On your VPN server, the BlackBerry 2FA server must be configured as a RADIUS server to which authentication requests are forwarded. The BlackBerry 2FA server completes the following tasks to authenticate users so that they can connect to a VPN gateway:

- Authenticates the user's device or one-time password (OTP)
- Acts as a proxy for password authentication
- Combines the two results to determine whether authentication is successful

You must also configure a VPN client profile or client that permits users to select BlackBerry 2FA when they log in to VPN from their computers.

For each BlackBerry 2FA server in your environment, the RADIUS server must have the following options:

- IP address or FQDN of the computer that hosts the BlackBerry 2FA server
- Timeout between 60 and 90 seconds for the connection between the VPN server and the BlackBerry 2FA server
- Unique shared secret
- Authentication port set to 1812
- Depending on the available authentication options, one of PAP, MS-CHAP v1, MS-CHAP v2, or EAP-MSCHAP

The VPN client profile must have the timeout set between 30 and 60 seconds for the connection between the VPN client on user's computers and the VPN server.

For instructions on how to configure a RADIUS server or VPN client profile, see the documentation for the VPN server that you are using.

For a list of supported VPN servers, see the BlackBerry 2FA server compatibility matrix content.

Supported authentication protocols for each authentication option

The following table shows the authentication protocols that are available for each authentication option that BlackBerry 2FA supports.

Note: If your users are authenticating with one-time password (OTP) tokens, the VPN server must be configured to authenticate them using PAP. OTPs are not supported using MSCHAPv1, MSCHAPv2 or EAP-MSCHAP.

Authentication option	Supported authentication protocols
Two-factor authentication with passive device password	PAP
Two-factor authentication with active device password	PAP
Two-factor authentication with enterprise password	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP
Single factor authentication with enterprise password	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP

Configuring the connection to the BlackBerry 2FA server on a Cisco ASA Series VPN gateway

If you are using a Cisco ASA Series VPN gateway, you can create the VPN profile using the information below.

For detailed instructions on how to configure the VPN profile, visit http://www.cisco.com to read the Cisco ASA Series documentation.

When you create the profile, you must set the following options to support BlackBerry 2FA:

- For each BlackBerry 2FA server in your environment, create a RADIUS AAA Server Group with the following options:
  - IP address or FQDN of the computer that hosts the BlackBerry 2FA server
  - Timeout between 60 and 90 seconds for the connection between the VPN gateway and the BlackBerry 2FA server
  - Unique shared secret
  - Authentication port set to 1812
  - MS-CHAP v2 compatible
- For the connection between the VPN client on user's computers and the VPN gateway, set the timeout between 30 and 60 seconds. You must configure the timeout in the Cisco AnyConnect VPN client profile file (an XML file) that must be installed on users' computers.
- Password management option, if you are configuring the profile to support MS-CHAP v2 authentication

You must complete the following actions to finish the profile creation process:

- Enable the VPN tunnel payload encapsulation protocol (for example, the IPSEC-IKE v2 protocol)
- All the commands that are required for the associated VPN policy group
- All the commands that are required for the associated Cisco AnyConnect VPN client profile and the creation of the XML file itself
- All the commands that are required for the associated VPN tunnel group

You do not need to configure additional certificate authentication.

When you configure VPN gateway connectivity in the BlackBerry 2FA server, you must provide the RADIUS shared secret that you create in the VPN profile.

Configuring the connection to the BlackBerry 2FA server on Citrix NetScaler

If you are using Citrix NetScaler, you can configure the connection to the BlackBerry 2FA server by adding it as a RADIUS server. If you have more than one BlackBerry 2FA server in your environment, you must configure a separate RADIUS server for each.

For detailed instructions on how to configure NetScaler to connect to the BlackBerry 2FA server, visit http://docs.citrix.com/en-us/netscaler.html to read about "Configuring RADIUS Authentication" in the NetScaler system documentation.

For example, you can configure a connection to one BlackBerry 2FA server and use BlackBerry 2FA as the default authentication method. If you want to configure this example, in the configuration utility for NetScaler, you must set the authentication settings under the global settings as follows:

- "Maximum Number of Users", "Max Login Attempts", and "Failed Login Timeout" as required by your organization

- Authentication type set to RADIUS
- IP address set to the BlackBerry 2FA server
- Port set to 1812
- Timeout between 60 and 90 seconds for the connection between NetScaler and the BlackBerry 2FA server
- Unique shared secret
- "Enable NAS IP address extraction" selected
- "Password Encoding" set to the authentication protocol supported by the VPN authentication option you've chosen (BlackBerry 2FA does not support the "chap" option)
- Accounting set to Off

Configuring the connection to the BlackBerry 2FA server on F5 BIG-IP

If you are using F5 BIG-IP with an AAA server, you can create an access policy with the Access Policy Manager using the information below.

For detailed instructions on how to configure authentication using AAA servers , visit https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm_config_10_2_0/apm_config_server_auth.html to read the F5BIG-IP documentation.

When you create the policy, you must set the following options to support BlackBerry 2FA:

- Set the authentication type to RADIUS
- Specify the IP address or FQDN of the computer that hosts the BlackBerry 2FA server
- Configure a timeout between 60 and 90 seconds for the connection between the VPN gateway and the BlackBerry 2FA server
- Set a unique shared secret
- Set the authentication port to 1812
- Verify MS-CHAP v2 is supported
- Turn off Accounting
- Specify the maximum number of login attempts

The policy must be assigned to each BlackBerry 2FA server in your environment.

Configuring the connection to the BlackBerry 2FA server on a Barracuda SSL VPN

If you are using Barracuda SSL VPN, you can configure the connection to the BlackBerry 2FA server by adding it as a RADIUS server. If you have more than one BlackBerry 2FA server in your environment, you must configure a separate RADIUS server for each.

For detailed instructions on how to configure Barracuda SSL VPN to connect to the BlackBerry 2FA server, visit https://www.barracuda.com/support/knowledgebase/50160000000HZG9AAO.

You must configure a RADIUS server with the following options to support BlackBerry 2FA:

- Set the authentication type to RADIUS
- Specify the IP address or FQDN of the computer that hosts the BlackBerry 2FA server
- Configure a timeout between 60 and 90 seconds for the connection between the VPN gateway and the BlackBerry 2FA server
- Set a unique shared secret
- Set the authentication port to 1812

- Verify MS-CHAP v2 is supported
- Turn off Accounting
- Specify the maximum number of login attempts

Configuring the connection to the BlackBerry 2FA server on a strongSwan server

To configure connectivity to the BlackBerry 2FA server on a strongSwan server, you must modify the ipsec.conf and the eap-radius.conf files.

For more information about these files and how to configure strongSwan, visit https://www.strongswan.org/.

ipsec.conf configuration

The ipsec.conf file is located in the /etc directory. You must add a new “conn” section for the BlackBerry 2FA server. For example:

```
conn <name>
 keyexchange=ikev2
 rightauth=eap-radius
 rightsendcert=never
 eap_identity=%any
 auto=add
```

Setting	Description
<name>	This is the unique name for the new connection section. It is a common practice for that name to reflect some key characteristics of the connection itself (for example, IPSec-IKEv2-radius).
keyexchange=ikev2	This setting specifies the key exchange method (for example, IKEv1, IKEv2). The BlackBerry 2FA server does not use this setting, but you must include it in the conn section to enable proper key exchange with VPN clients. You must make sure that the VPN clients that connect to the strongSwan server use the same key exchange method.
rightauth=eap-radius	This setting specifies that the strongSwan server must use EAP over RADIUS to authenticate VPN clients for this type of connection.
rightsendcert=never	This setting specifies that user certificates are not used for client authentication.
eap_identity=%any	This setting specifies the identity of the VPN client to use for authentication. The BlackBerry 2FA server does not use this setting, but you must include it in the conn section. The "%any" value instructs the strongSwan server to pass the identity provided by the VPN client.
auto=add	This setting specifies that this connection section is active. The BlackBerry 2FA server does not use this setting, but you must include it in the conn section.

eap-radius.conf configuration

The eap-radius.conf file is located in the /etc/strongswan.d/charon directory. It specifies the details for EAP over RADIUS authentication. The default configuration file has all the settings that you must configure, but most of them are commented out and some of them do not have any value assigned. You must modify the required settings by removing the number sign (#) and setting their values as described in the following table.

Setting	Description
accounting=no	This setting prevents strongSwan from sending RADIUS accounting information to the BlackBerry 2FA server.
nas_identifier	This optional setting specifies the NAS-Identifier to include in RADIUS messages. You can use this setting if multiple strongSwan servers are using the same BlackBerry 2FA server.
port=1812	This setting specifies the port used by the BlackBerry 2FA server to receive RADIUS requests for authentication.
secret=<*shared secret*>	This setting specifies the shared secret between strongSwan and the BlackBerry 2FA server. When you configure VPN server connectivity in the BlackBerry 2FA server, you must type the RADIUS shared secret that you specify here.
server=<*IP of VPNAuth server*>	This setting specifies the IP address or FQDN of the BlackBerry 2FA server.
ike_to_radius=1, 2, 311:1, 311:11, 311:25	This setting specifies a comma-separated list of numbers that represent the list of RADIUS attributes that strongSwan needs to forward to the BlackBerry 2FA server. Numbers separated by colons indicate vendor-specific attributes. The first number identifies the vendor (for example, 311 is the number for Microsoft), and the second number identifies the attribute type. This setting is in the “forward” section of the configuration file.
radius_to_ike=311:26, 311:17, 311:16	This setting specifies a comma-separated list of numbers that represent the list of RADIUS attributes that the BlackBerry 2FA server needs to forward to strongSwan. Numbers separated by colons indicate vendor-specific attributes. The first number identifies the vendor (for example, 311 is the number for Microsoft), and the second number identifies the attribute type. This setting is in the “forward” section of the configuration file.

Configure the BlackBerry 2FA server to connect to a VPN gateway

Before you begin: Obtain the IP address and shared secret for the VPN gateways.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.

2. Click the BlackBerry 2FA server that you want to configure a VPN gateway for.
3. In the **VPN configuration** section, click +.
4. In the **VPN server name** field, type a unique name for the VPN gateway that you are connecting to.
5. In the **VPN host** field, type the IP address of the VPN gateway.
6. In the **Shared secret** and **Confirm shared secret** fields, type and confirm the shared secret of the VPN gateway.
7. Optionally, override the BlackBerry 2FA app configuration. You can configure the following fields independent of one another. Fields left empty are ignored and the default values in the **Default device prompt** section are used.
   a) Select **BlackBerry 2FA prompt for this VPN**.
   b) In the **Title** field, type the title that you want the app to display in its message. For example, "Example Organization's VPN."
   c) In the **Message** field, type the message that you want the app to display to users. This message explains to users what is required from them.
   d) In the **Confirm button text** field, type the text that appears on the button users can tap to confirm second-factor authentication.
   e) In the **Decline button text** field, type the text that appears on the button users can tap to decline second-factor authentication.
   f) In the **Timeout (seconds)** field, type the amount of time, in seconds, before the authentication transaction expires.
8. Click **Add**.
9. Repeat these steps for each VPN gateway that you want to add.
10. Click **Save**.

Update a connection to a VPN gateway

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Click the name of the 2FA server that you want to configure.
3. Click the name of the VPN server that you want to update.
4. Update the configuration as needed. For more information, see steps 4 through 7 of Configure the BlackBerry 2FA server to connect to a VPN gateway.
5. Click **Add**.
6. Click **Save**.

Delete a connection to a VPN gateway

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Beside the VPN server that you want to delete, click ×.
3. Click **Yes**.
4. Click **Save**.

Configure the connection to the REST API endpoint

The BlackBerry 2FA server's REST API endpoint is protected using server-authenticated HTTPS. You must configure your custom services to trust the BlackBerry 2FA server. You have the following options:

- You can use the default self-signed certificate generated during installation of the BlackBerry 2FA server. The default self-signed certificate is located in bb2fa-config/restkeystore.jks. Your client application must be configured to trust this certificate explicitly. The default server port is 5443.
- You can supply your own CA-signed certificate by importing it into a Java keystore under the “bb2fa” alias (RSA 2048 is recommended as the key algorithm). Copy the keystore file into the bb2fa-config directory and update the keystore file name and password on the BlackBerry 2FA server configuration page in BlackBerry UEM.

In all cases, the custom services are authenticated using HTTP basic authentication (username and password), which are sent as headers in the request.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Click the name of the 2FA server that you want to configure.
3. In the **REST interface configuration** section, enter the information.
4. Click **Save**.

Configuring REST API endpoint connectivity

To configure connectivity between client apps and the BlackBerry 2FA server's REST API endpoint, you must configure your client applications to trust the BlackBerry 2FA server.

The client apps are authenticated using HTTP basic authentication (user name and password) which are sent as headers in the request. The REST API endpoint is protected using server authenticated HTTPS (https://<*hostname*>:<*port*>/<*prefix*>/) . The default port is 5443 and the default prefix is "rest." The following REST requests are supported on the endpoint:

Path	Type	Description	Notes
/<*prefix*>/twofactor	POST	Two-factor authentication request	

The request message is sent using HTTP POST and is formatted as JSON, with the following parameters:

Parameter	Type	Description	Notes
username	String	User name	
password	String	User password, or one-time password and user password	Optional, depending on policy

Parameter	Type	Description	Notes
policy	Integer	Authentication option: • 0: Single-factor authentication using enterprise password • 1: Two-factor authentication with enterprise password • 2: Two-factor authentication with passive device password • 3: Two-factor authentication with active device password	
oneTimePassword	String	One-time password	Optional
messageTitle	String	Dialog title text	Optional
message	String	Dialog message text	Optional
confirmButtonText	String	Dialog confirm button text	Optional
declineButtonText	String	Dialog decline button text	Optional
timeout	Integer	Dialog timeout (seconds)	Optional

The response message body is formatted as JSON, with the following parameter:

Parameter	Type	Description	Notes
info	String	Informational message	

The response message also includes the following HTTP status codes:

Status	Description	Notes
200	OK	Authentication successful
400	Bad request	Invalid parameters
401	Unauthorized	Authentication failed
403	Declined	User declined authentication
500	Internal server error	Internal error

Create a REST API client in the BlackBerry 2FA server

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Click the name of the 2FA server that you want to configure.
3. In the **REST client configuration** section, click +.
4. In the **REST client name** field, type a friendly name for the client.
5. In the **REST client ID** field, type a name for the client that will be associated with the password.
6. In the **Password** field, type a password.The password must have a minimum of eight characters
7. In the **Confirm password** field, retype the password.
8. Click **Add**.
9. Repeat these steps for each client that you want to add.
10. Click **Save**.

Enable MS-CHAP authentication for users in a domain

You can enable a BlackBerry 2FA server to support MS-CHAPv1 and MS-CHAPv2 authentication for RADIUS requests (for example, requests that come from a VPN gateway) for users that are a member of the selected domain. The domain is available for this option because the 2FA server is running on a host that is joined to an Active Directory domain to which BlackBerry UEM is also connected.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Click the name of the 2FA server that you want to configure.
3. In the **Active directory configuration** section, select the domain for which you want to enable MS-CHAP authentication. To disable MS-CHAP authentication, deselect the domain.
4. Click **Save**.

Configure the BlackBerry 2FA app

You can customize the default message that BlackBerry 2FA displays to users when they connect to your resources. You can also set the amount of time, in seconds, before the authentication prompt expires.

You can also override these settings for each VPN gateway that you configure. For more information about configuring VPN gateways, see Configure the BlackBerry 2FA server to connect to a VPN gateway.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.
2. Click the name of the 2FA server that you want to configure.
3. In the **Default device prompt** section, do the following:
   a) In the **Title** field, type the title that you want the app to display in its message. For example, "Example Organization's VPN."
   b) In the **Message** field, type the message that you want the app to display to users. This message explains to users what is required from them.
   c) In the **Confirm button text** field, type the text that appears on the button users can tap to confirm second-factor authentication.
   d) In the **Decline button text** field, type the text that appears on the button users can tap to decline second-factor authentication.
   e) In the **Timeout (seconds)** field, type the amount of time, in seconds, before the authentication transaction expires.
4. Click **Save**.

Assign a VPN gateway or REST client configuration to a user group

To authorize users to use VPN or REST clients, you must assign a VPN gateway or REST client configuration to user groups. You can create user groups that include the users that you want to assign the configurations to. Users can only use the configurations that are assigned to them.

Before you begin: Do one of the following:

- Configure the BlackBerry 2FA server to connect to a VPN gateway
- Create a REST API client in the BlackBerry 2FA server

1. In the BlackBerry UEM management console, on the menu bar, click **Groups** > **User**.
2. Either create a new group or click the name of the group you want to assign a configuration to.
3. Click the **BlackBerry 2FA** tab.
4. Click +.
5. Choose a device client configuration from the drop-down.
6. Click **Assign**.

Installing the BlackBerry 2FA app on devices

BlackBerry 2FA is available for iOS,Android, and BlackBerry 10 devices.

iOS and Android devices

For iOS and Android devices, BlackBerry 2FA features are included in the BlackBerry UEM Client app. Users must download the BlackBerry UEM Client to activate their device with BlackBerry UEM to use 2FA.

Users can download the BlackBerry UEM Client app from Google Play and the App Store.

BlackBerry 10 devices

For BlackBerry 10 devices, you must send the BlackBerry 2FA app to the devices using BlackBerry UEM. Perform the following actions using BlackBerry UEM :

- If necessary, use the BlackBerry UEM management console to specify a shared network location for internal apps.
- In the BlackBerry UEM management console, add the BlackBerry 2FA app file (.bar) as an internal app. The BlackBerry 2FA app is located here: https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B
- In the BlackBerry UEM management console, assign the app to user accounts or groups.

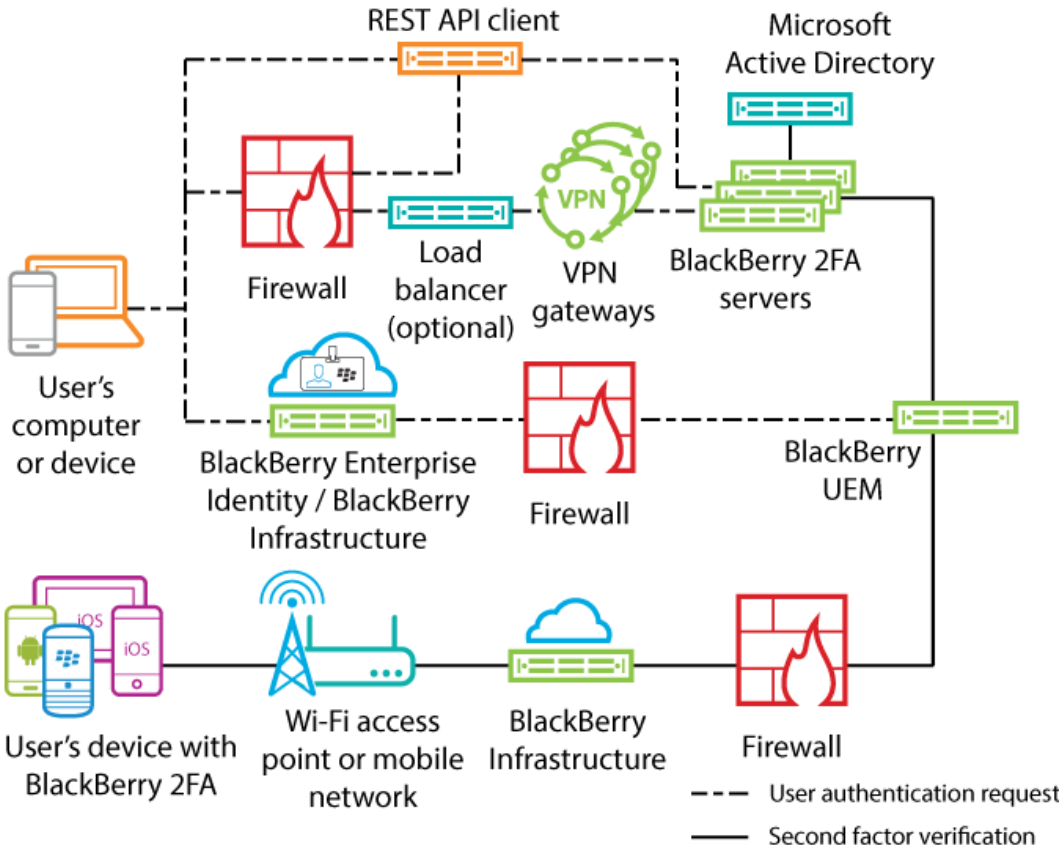
For devices with a work space, the app is installed in the work space. Users can also install it using BlackBerry World for Work if you do not make the installation mandatory.

For more information about sending apps, see the BlackBerry UEM administration content.

Architecture: BlackBerry 2FA high availability

BlackBerry 2FA supports active-active high availability. You can install multiple instances of the BlackBerry 2FA server to provide load-balancing for authentication requests and to promote reliability.

The following diagram shows a high availability scenario. Some VPN solutions might include a load balancer, and in that scenario a separate load balancer is not required.



Configuring the BlackBerry 2FA server for high availability

You can use the same ports for all BlackBerry 2FA servers.

To maintain the unique encryption of configuration information, it is recommended that you do not copy the bb2fa-config.json file between BlackBerry 2FA servers. You must configure each server separately in the BlackBerry UEM management console.

Task	Description
1	If you have not already done so, set up high availability for your VPN gateway. For more information, see the documentation for your VPN gateway.

Task	Description
2	Install two or more BlackBerry 2FA servers. For each server, generate and download an activation file. During subsequent installations, you can choose not to select the BlackBerry 2FA app files. You do not need to install the files more than once. For more information, see the BlackBerry 2FA server installation and upgrade content.
3	Create a profile for the BlackBerry 2FA servers on the VPN server. For more information, see Configuring a connection between the BlackBerry 2FA server and a VPN gateway.
4	Connect each BlackBerry 2FA server, to a VPN gateway. For more information, see Configure the BlackBerry 2FA server to connect to a VPN gateway.
5	Configure the connection to the REST API endpoint
6	Create a REST API client in the BlackBerry 2FA server.
7	Enable MS-CHAP authentication for users in a domain
8	Configure the BlackBerry 2FA app
9	Assign a VPN gateway or REST client configuration to a user group
10	If needed, send the BlackBerry 2FA app to devices. For more information, see Installing the BlackBerry 2FA app on devices.

Logging and reporting

The BlackBerry 2FA stores its log files in <*install_dir*>\logs. There are four log files:

- The bb2fa.log is the main log file that includes all the messages that the BlackBerry 2FA server writes. For example, it includes startup and shutdown messages and messages related to the progress of authentication.
- The key_log.txt is the file that contains messages related to the creation and status of the keys that the BlackBerry 2FA server requires to protect sensitive information such as passwords.
- The bb2fa-audit.log is a comma-delimited audit file that records each authentication request that the BlackBerry 2FA server made.
- The winrun_log.txt is the file that contains messages specific to the startup and running of the BlackBerry 2FA server when you run it in Windows Services.

BlackBerry 2FA uses the Apache log4j logging tool for logging. By default, the BlackBerry 2FA server writes log messages at the Info level.

The BlackBerry 2FA server creates new log and audit files daily. When the log or audit file is created, the previous log or audit file is time-stamped as bb2fa.<*date*>.log or b2fa-audit.log.<*date*>.

You can change the logging level and where BlackBerry 2FA stores the log and audit files using the log4j.properties file in <*install_dir*>\bb2fa-config. For more information, visit http://logging.apache.org/log4j/2.x/ to read the *Apache log4j 2 User's Guide*.

Auditing authentication requests

BlackBerry 2FA server

The BlackBerry 2FA server records each authentication request that it makes in an audit log file when the request expires. The audit log file includes the following information about each request:

- Date
- Time
- Transaction ID
- Client name
- Client IP address
- Username
- Authentication option
- BlackBerry 10 devices assigned to the user
- Third-party devices assigned to the user
- BlackBerry OS devices assigned to the user
- Device that responded to the authentication request
- Time (in seconds) it took to complete the authentication request
- Result of the request

For example:

```
2015-11-05,13:27:17.822,50dbe1cc,radtest,10.135.41.74,caperez,ENTERPRISE_PW,
[BESNameOne:BB10:2fff369:OK],[BES12-TEST:THIRDPARTY: 1fdf6d37-4f21-4516-b43f-
c90be83f646c:OK],[BESNameOne:BBOS:2fff367:OK],[BBOS:2fff367],6.742,AUTH_SUCCEEDED
```

The audit log file is a comma-delimited file that you can open in any software that supports CSV. It is named bb2fa-audit.log and is stored in <*install_dir*>\logs.

BlackBerry UEM

For information about BlackBerry UEM logging, see the BlackBerry UEM administration content.

Centralize logging or auditing using syslog

You can configure the BlackBerry 2FA server so that it writes its log files, its audit files, or both to a centralized syslog server instead of local files.

Note: This task demonstrates one way to centralize logging. For more information about how to configure logging, visit http://logging.apache.org/log4j/2.x/ to read the *Apache log4j 2 User's Guide* .

1. Browse to the `<install_dir>\bb2fa-config` folder.
2. Back up the log4j.properties file.
3. Open the log4j.properties file in a text editor.
4. To send log messages to a central syslog server, perform the following actions:
   a) Change the value of `log4j.rootLogger` to one of the following:
      - To write log messages only to a syslog server, `ALL, syslog`
      - To write log messages locally and to a syslog server, `ALL, logfile, syslog`
   b) Add the following lines:

```
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.SYSLOG.Threshold=INFO
log4j.appender.SYSLOG.syslogHost=<hostname>:<port>
log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.SYSLOG.layout.ConversionPattern=[%-5p] %c - %m%n
```

   c) Set the value of `log4j.appender.syslog.syslogHost` to the host name and port of your syslog server.
   d) Optionally, to remove local logging, delete the following lines:

```
# Log file output
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c -
 %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log
```

5. To send audit messages to a central syslog server, perform the following actions:
   a) Change the value of `log4j.logger.auditLogger` to one of the following:
      - To write audit messages only to a syslog server, `ALL, auditsyslog`
      - To write audit messages locally and to a syslog server, `ALL, auditfile, auditsyslog`
   b) Add the following lines:

```
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=<hostname>:<port>
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

c) Set the value of `log4j.appender.syslog.syslogHost` to the host name and port of your syslog server. You must use a different port for the audit file than for the log file.
d) Optionally, to remove local auditing, delete the following lines:

```
# Audit log output
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log
```

6. Save your changes.
7. In Windows Services, restart the BlackBerry 2FA service.

Example log4j.properties file with syslog and local logging

```
log4j.rootLogger=ALL, logfile, syslog

log4j.logger.auditLogger=ALL, auditfile, auditsyslog

# We want to control the output Apache CFX and Jetty,
# which are very verbose at the DEBUG level
log4j.logger.org.apache.cxf=INFO
log4j.logger.org.eclipse.jetty=INFO

# Redirect logs to a local log file
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c - %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log

# Redirect logs to a remote syslog server
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.Threshold = INFO
log4j.appender.syslog.syslogHost=syslog.example.com:514
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=[%-5p] %c - %m%n

# Redirect audit messages to a local audit file
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},%d{HH:mm:ss.SSS},
%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log

# Redirect audit messages to a remote syslog server
#(you need a different port to generate a different file)
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
```

```
log4j.appender.auditsyslog.syslogHost=syslog.example.com:515
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

Authentication options

BlackBerry 2FA offers the following authentication options:

Note: If a user is assigned any two-factor option, they are also automatically allowed to use an OTP token if one is assigned to the user.

Authentication option	Description	Useful when
Two-factor authentication with enterprise password	When a user logs in, they supply a username and a directory password and then receive a prompt to confirm the authentication request on the device. If a user is assigned this option, they are automatically allowed to use an OTP token if one is assigned to the them. This option is supported on all devices.	Your organization places security as its most important goal for any deployment.
Two-factor authentication with passive device password	When a user logs in, they only supply a username and then receive a prompt to confirm the authentication request. If the device is locked, the user must provide the device password before they can confirm the prompt. If a user is assigned this option, they are automatically allowed to use an OTPtoken if one is assigned to the them. For BlackBerry 10 devices, users must provide the work space password if the work space is locked. This option is supported on all devices.	Your organization places usability as its most important goal for any deployment.

Authentication option	Description	Useful when
Two-factor authentication with active device password	When a user logs in, they only supply a username and then they receive a prompt to confirm the authentication request on their device. The user must always provide the device password before they can confirm the prompt. If a user is assigned this option, they are automatically allowed to use an OTP token if one is assigned to the them. For BlackBerry 10 devices, users must provide the work space password. This option is supported for BlackBerry 10 and BlackBerry OS (version 6.0 to 7.1) devices only.	Your organization stresses usability but wants to guard against someone picking up an unlocked device and accepting the device prompt.
Single-factor authentication using enterprise password	Users log in using Microsoft Active Directory authentication only.	• The user does not have a device. • The user has forgotten or lost their device. • The user does not need to use a second factor of authentication.

Note: In BlackBerry 2FA version 2.5, you can configure user authentication options in several different ways. By default, authentication options are configured using a BlackBerry 2FA profile in BlackBerry UEM. However, you can override this default configuration for authentication requests sent through the REST API or through VPN gateways and other RADIUS clients. For more information, see Configuring REST API endpoint connectivity or Configuring a connection between the BlackBerry 2FA server and a VPN gateway.

Usernames, passwords, and directories

BlackBerry 2FA authenticates users that are available in a directory. Both the BlackBerry 2FA server and BlackBerry UEM are connected to these directories. Based on how these connections are configured, BlackBerry 2FA supports four user types:

- Users in a Microsoft Active Directory domain that is connected to both a BlackBerry 2FA server and BlackBerry UEM
- Users in a Microsoft Active Directory domain that is not connected to a BlackBerry 2FA server but is connected to BlackBerry UEM
- Users in an LDAP directory that is connected to BlackBerry UEM
- Users in a local BlackBerry UEM directory

When a user logs in, they must supply a username, and optionally, a password.

Username

The username must resolve to a unique user entry in a directory. If the user cannot be uniquely resolved, an authentication request will fail. To specify the directory in which the user resides, the user must be identifed according to following usernanes for each type of user:

- The following usernames are supported for users in a Microsoft Active Directory domain that is connected to both a BlackBerry 2FA server and BlackBerry UEM. These users can authenticate using PAP, MSCHAPv1, MSCHAPv2 and EAP-MSCHAPv2 and can be configured to use authorization groups for each REST API client and authentication override groups for each VPN gateway.

  <username> (e.g. jsmith)

  <username>@<NetBIOS domain name> (e.g. jsmith@company)

  <NetBIOS domain name>\<username> (e.g. company\jsmith)

  <email address> (e.g. jsmith@company.com)
- The following usernames are supported for users in a Microsoft Active Directory domain that is not connected to a BlackBerry 2FA server but is connected to BlackBerry UEM. These users can authenticate using only PAP.

  <username> (e.g. jsmith)

  <username>@<NetBIOS domain name> (e.g. jsmith@company)

  <NetBIOS domain name>\<username> (e.g. company\jsmith)

  <email address> (e.g. jsmith@company.com)
- The following usernames are supported for users in a LDAP directory that is connected to BlackBerry UEM. These users must authenticate with PAP.

  Note: The BlackBerry 2FA server cannot connect to this directory.

  <username> (e.g. jsmith)

  <username>@<directory FQDN> (e.g. jsmith@company.ldap.net)

  <directory FQDN>\<username> (e.g. company.ldap.net\jsmith)

  <email address> (e.g. jsmith@company.com)
- The following usernames are supported for users in a local BlackBerry UEM directory. These users must authenticate with PAP.

  Note: The BlackBerry 2FA server cannot connect to this directory.

  <username> (e.g. jsmith)

  <username>@local (e.g. jsmith@local)

  local\<username> (e.g. local\jsmith)

  <email address> (e.g. jsmith@company.com)

Password

When a user logs in, they must supply a directory password depending on the authentication option they are configured to use.

If a user is authenticating using a one-time password (OTP) token, they must supply the OTP and their directory password regardless of the two-factor authentication option they are configured to use.

- To log in to a VPN, the user must enter both the OTP and the directory password in the password field. The OTP is typed first, then the directory passord, and no spaces or separators may be added.
- When logging in from a client connected to a REST API, the user must enter the directory password in the password field and then enter the OTP in a dedicated OTP field.

REST API endpoint

The BlackBerry 2FA server has an external REST API endpoint that extends BlackBerry 2FA to custom services like web applications and SIP client applications. You can use the BlackBerry 2FA server configuration page in the BlackBerry UEM management console to create a REST client. For more information, see Configuring REST API endpoint connectivity.

VPN gateways

You can use the BlackBerry 2FA server configuration page in the BlackBerry UEM management console to create a connection to a VPN gateway. The connection between a VPN gateway and the BlackBerry 2FA server is established using RADIUS. For more information, see Configuring a connection between the BlackBerry 2FA server and a VPN gateway.

Glossary

API	application programming interface
CA	certification authority
DNS	Domain Name System
ECDH	Elliptic Curve Diffie-Hellman
EAP	Extensible Authentication Protocol
EMM	Enterprise Mobility Management
FQDN	fully qualified domain name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP	Internet Protocol
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
IKE	Internet Key Exchange
MAM	mobile application management
MDM	mobile device management
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAS	network-attached storage
NTLM	NT LAN Manager
OTP	one-time password
PAP	Push Access Protocol
RADIUS	Remote Authentication Dial In User Service
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol

SSL	Secure Sockets Layer
TLS	Transport Layer Security
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

BlackBerry Limited
2200 University Avenue East

Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada