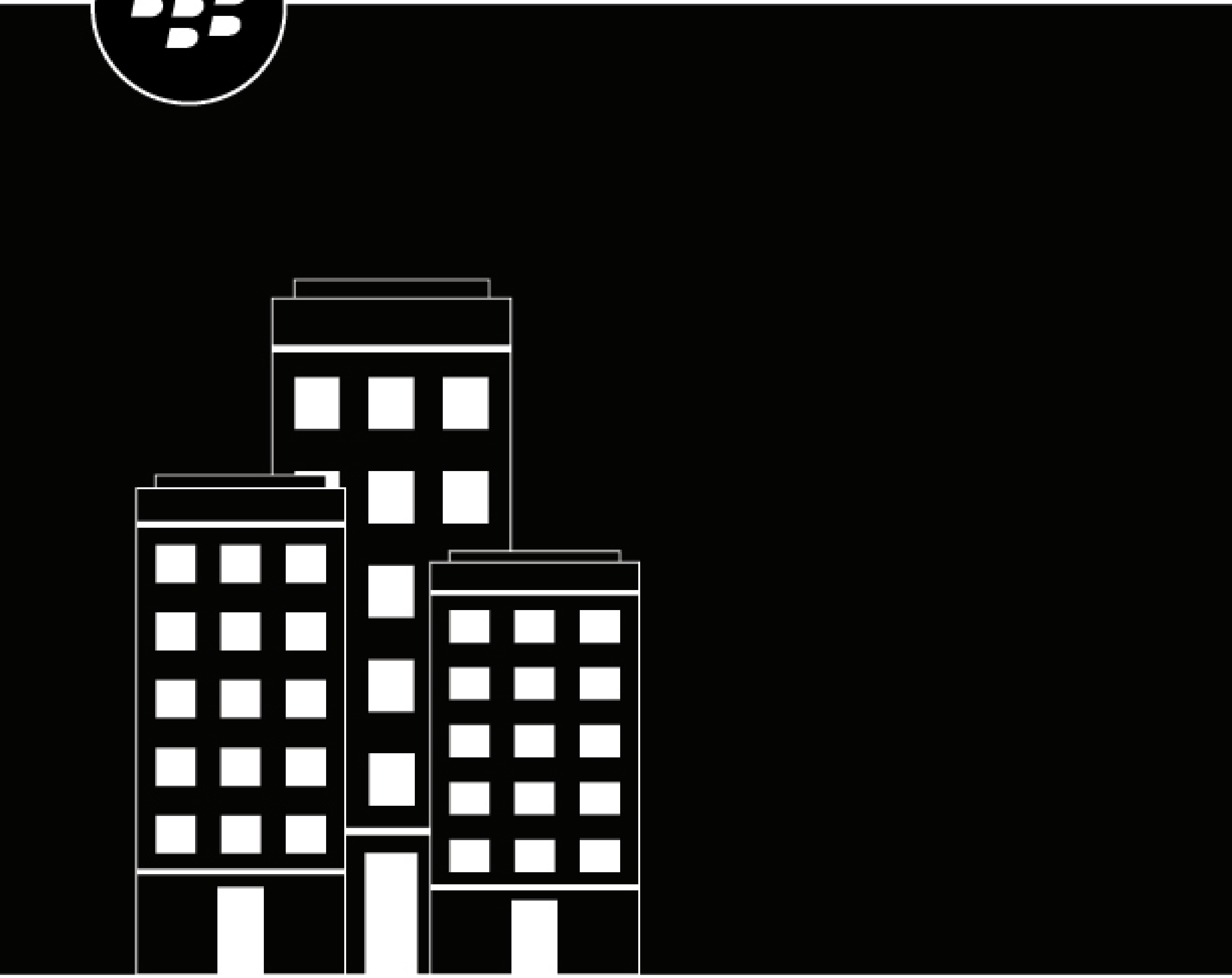


Configuring Direct Connect with BlackBerry UEM

Contents

What is Direct Connect?

By default, the BlackBerry Dynamics apps on users' devices connect to the BlackBerry Dynamics NOC to connect to a BlackBerry Proxy instance behind your organization's firewall. Depending on the physical distance between devices and the BlackBerry Dynamics NOC, connections might experience some network latency.

To mitigate these issues, you can enable BlackBerry Dynamics Direct Connect. Direct Connect allows BlackBerry Dynamics apps to bypass the connection to the NOC and connect directly to a BlackBerry Proxy instance behind your organization's firewall. If devices are physically closer to the BlackBerry Proxy instances in your domain than they are to the BlackBerry Dynamics NOC, Direct Connect can reduce network latency.

You can also configure BlackBerry Dynamics apps to connect through a web proxy server in the DMZ when they connect to a BlackBerry Proxy instance.

This feature provides benefits in the following situations:

- **Enhanced control over work data:** App data flows only between devices and the work network. Direct Connect can be used when organizations have additional data privacy requirements that restrict user data from leaving their networks and do not want their user and enterprise data to be routed through the BlackBerry Dynamics NOC. When this feature is enabled, BlackBerry Dynamics apps make a connection to the BlackBerry Proxy directly instead of connecting through the BlackBerry Dynamics NOC to connect to an app server inside your organization's network.
- **Improved network performance:** Depending on the physical distance between devices and the BlackBerry Dynamics NOC, connections might experience some network latency. To mitigate these issues, when Direct Connect is enabled, BlackBerry Dynamics apps bypass the connection to the BlackBerry Dynamics NOC and connect directly to a BlackBerry Proxy instance behind your organization's firewall. If devices are physically closer to the BlackBerry Proxy instances in your domain than they are to the BlackBerry Dynamics NOC, network latency is reduced.
- **Improved user experience:** Faster app response times and support for additional types of apps such as VoIP and video.
- **Easy implementation of mixed mode:** Direct Connect is configured individually for each BlackBerry Proxy instance, so that in larger environments some BlackBerry Proxy servers can use the standard NOC connection and some can use Direct Connect. BlackBerry Proxy servers within the same cluster should be configured the same way (either Direct Connect-enabled, or standard NOC-enabled).

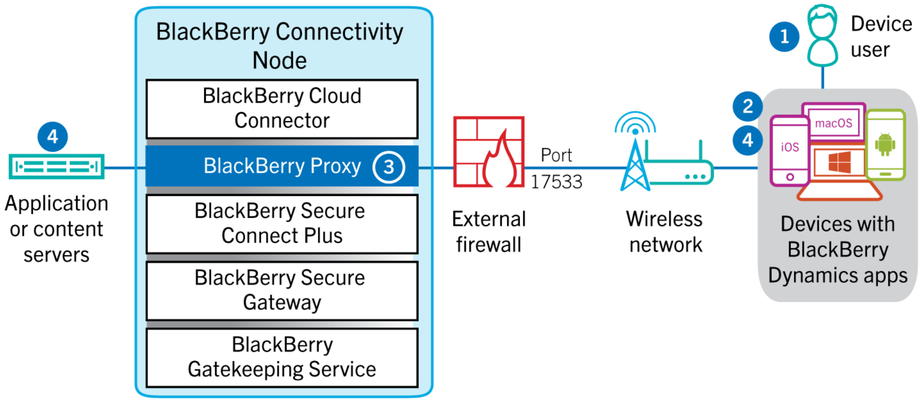
Even with Direct Connect configured, the BlackBerry Dynamics NOC is still a critical part of the architecture. Connectivity to the NOC is required for:

- Provisioning of apps on mobile devices
- Notifications of policy updates to active (open) BlackBerry Dynamics containers. For inactive containers, the policy updates take place the next time the container opens. Real-time notification requires a connection to the NOC.

Direct Connect requires a public DNS record for inbound connections on the external firewall.

Data flow: Sending and receiving work data from a BlackBerry Dynamics app using BlackBerry Dynamics Direct Connect

This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization using BlackBerry Dynamics Direct Connect in its most basic configuration. In this configuration, the BlackBerry Proxy server is directly accessible to the Internet on port 17533. Installation of a BlackBerry Connectivity Node is recommended when configuring BlackBerry Proxy servers for Direct Connect. For other configuration options, see Deployment options.


BlackBerry Connectivity Node
BlackBerry Cloud Connector
BlackBerry Proxy
3
BlackBerry Secure Connect Plus
BlackBerry Secure Gateway
BlackBerry Gatekeeping Service
4
Application or content servers
External firewall
Port 17533
Wireless network
1
Device user
2
4
macOS
iOS
Devices with BlackBerry Dynamics apps

1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a TLS connection to the BlackBerry Proxy server on port 17533.
3. BlackBerry Proxy authenticates to the BlackBerry Dynamics app using its server certificate. BlackBerry Proxy validates the app using a MAC key with a session key known only to BlackBerry Proxy and the app.
4. The BlackBerry Dynamics app creates a connection to the app server behind the firewall inside the previous connection. When the secure end-to-end connection is established, work data can travel between the device and application or content servers behind the firewall using BlackBerry Proxy.

Deployment options

The recommended deployment configurations for Direct Connect are:

- Port forwarding
- Proxy forwarding
- Reverse proxy with SSL bridging

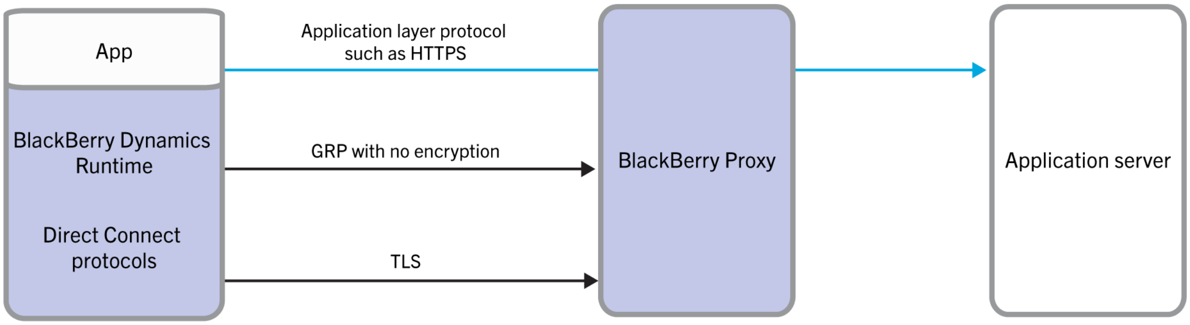
Note: These are sample configurations for typical environments. However, DMZ architecture is optional as long as you ensure the correct ports are open. For information about port requirements, see the BlackBerry UEM Planning Guide. For assistance in designing a custom environment, contact BlackBerry Enterprise Consulting.

Note: BlackBerry UEM does not support deep packet inspection in the network segment between the external firewall and BlackBerry Proxy. Even though the Direct Connect connection is TLS, the protocol to the BlackBerry Proxy server is Good Relay Protocol (GRP), which is a binary protocol. Also, the payload of the GRP may be encrypted with TLS if the application layer established an HTTPS/TLS connection to the application server.

A BlackBerry Dynamics app establishes a TLS connection to the BlackBerry Proxy and authenticates to the BlackBerry Proxy over GRP. The BlackBerry Proxy then uses the SSL certificate signed by BlackBerry UEM to authenticate to the BlackBerry Dynamics app. If SSL bridging is used, you must replace the default BlackBerry UEM signed certificate with a custom third-party certificate that can be used to authenticate BlackBerry Dynamics apps.

Connections to the application server are never attempted through the BlackBerry Dynamics NOC when configured for Direct Connect.

The following image shows the layers and protocols used in Direct Connect.



The following table compares the connection models supported by BlackBerry Dynamics.

Connection Model	Authentication	Encryption	Connection requirements	Intranet connection requirements
Through the BlackBerry Dynamics NOC	By the BlackBerry Dynamics NOC and BlackBerry Connectivity Node	AES 256 by GRP	Outbound	Outbound
Direct Connect configured for port forwarding	By the BlackBerry Connectivity Node	AES 256 by TLS protocol	One inbound IP address per BlackBerry Connectivity Node	Multiple inbound IP addresses, one per app server

Connection Model	Authentication	Encryption	Connection requirements	Intranet connection requirements
Direct Connect configured using a forward proxy	By the BlackBerry Connectivity Node	AES 256 by TLS protocol	One inbound IP address per proxy	One inbound IP address per BlackBerry Connectivity Node
Direct connect configured using a reverse proxy with SSL bridging	First by the SSL bridging appliance and then by the BlackBerry Connectivity Node	AES 256 by TLS protocol	One inbound IP address per proxy	One inbound IP address per BlackBerry Connectivity Node

Port forwarding

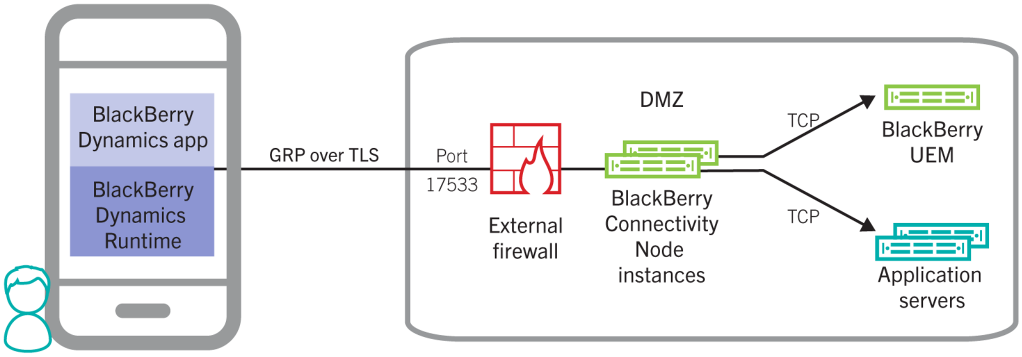
You can port forward all incoming client traffic to a BlackBerry Proxy server in a DMZ. The benefit of this approach compared to the other deployment options is that no extra appliance is required in the DMZ.

Because the BlackBerry Proxy is a component of the BlackBerry Connectivity Node, to install the BlackBerry Proxy in a DMZ, you must install the entire BlackBerry Connectivity Node in the DMZ. For more information on distributed architecture, see BlackBerry UEM distributed installation.

You must open additional ports between the DMZ and the work network so that the BlackBerry UEM Core servers and all enterprise application servers used in the BlackBerry Dynamics deployment are reachable from the BlackBerry Connectivity Node in the DMZ.

Requirements:

- The BlackBerry Connectivity Node must be reachable from the internet on port 17533.
- You must configure each BlackBerry Connectivity Node instance separately.
- Each BlackBerry Proxy server must have a publicly routable DNS name (for example, bp01.domain.com). You can create a unique public DNS entry for each BlackBerry Connectivity Node instance or use the same public DNS entry for all BlackBerry Connectivity Node instances by using round robin DNS. You can configure the external FQDN for the BlackBerry Proxy in the BlackBerry UEM management console.



Note: A BlackBerry Connectivity Node inside a DMZ is not required. You can port forward from the edge of the perimeter network directly into the work network where the BlackBerry Proxy server resides. The BlackBerry Proxy server requires only one inbound port, TCP 17533. As long as the perimeter firewall is configured to allow only this port to the BlackBerry Proxy server, then access is secured.

Configure Direct Connect using port forwarding

Before you begin:

- Configure a public DNS entry for each BlackBerry Connectivity Node server (for example, bp01.mydomain.com, bp02.mydomain.com, and so on).
- Configure the external firewall to allow inbound connections on port 17533 and to forward that port to each BlackBerry Connectivity Node server.
- If the BlackBerry Connectivity Node instances are installed in a DMZ, ensure that the appropriate ports are open between each BlackBerry Connectivity Node and any application servers that the BlackBerry Dynamics apps need to access (for example, Microsoft Exchange, internal web servers, and the BlackBerry UEM Core).

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Direct Connect**.
3. Click a BlackBerry Proxy instance.
4. To turn on Direct Connect, select the **Turn on Direct Connect** check box. In the **BlackBerry Proxy host name** field, verify that the host name is correct. If the public DNS entry you created is different from the FQDN of the server, specify the external FQDN instead.
5. Repeat steps 3 and 4 for all BlackBerry Proxy instances in the cluster.

   To enable only some BlackBerry Proxy instances for Direct Connect, create a new BlackBerry Proxy cluster. All servers in a cluster must have the same configuration. For more information, see Manage BlackBerry Proxy clusters in the Configuration content.
6. Click **Save**.

Proxy forwarding

You can install an HTTP forward proxy server that supports HTTP Connect in the DMZ. The BlackBerry Connectivity Node remains inside the corporate network. In this configuration, only the BlackBerry Connectivity Node is reachable from the DMZ proxy instead of exposing multiple app servers to the DMZ. BlackBerry Dynamics apps make an HTTP Connect request to the DMZ proxy and request a connection to the BlackBerry Connectivity Node. The DMZ proxy then makes the connection to the BlackBerry Connectivity Node. When it is connected to the BlackBerry Connectivity Node, the BlackBerry Dynamics app establishes a TLS connection and authenticates to the BlackBerry Proxy.

You can configure one DMZ proxy for multiple BlackBerry Connectivity Node instances, or configure a unique DMZ proxy for each BlackBerry Connectivity Node instance. You must provide the FQDN of the DMZ proxy in the BlackBerry UEM management console for each BlackBerry Connectivity Node.

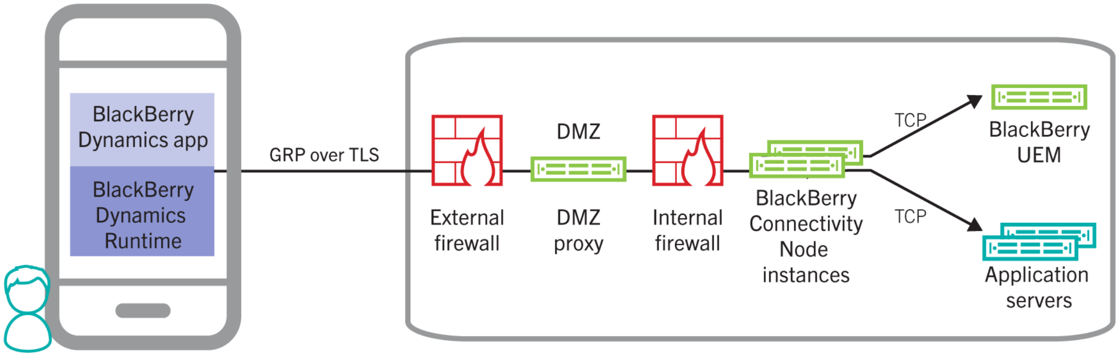
The benefits of this approach are:

- You don't need to port forward directly from the edge network to the internal corporate network as with the port forwarding option. You can set up a DMZ. The web proxy in the DMZ connects to the BlackBerry Connectivity Node servers in the internal corporate network.
- The internal BlackBerry Connectivity Node address is not exposed to the internet as it is in the port forwarding option.

BlackBerry Dynamics apps make an HTTP Connect request to the DMZ proxy and request a connection to BlackBerry Connectivity Node. The DMZ proxy then makes the connection to the BlackBerry Connectivity Node. When connected to the BlackBerry Connectivity Node, the BlackBerry Dynamics app establishes a TLS connection and authenticates to the BlackBerry Proxy.

Forward proxy servers used for Direct Connect must meet the following requirements:

- Support the HTTP Connect method
- Be able to communicate with the BlackBerry Proxy server via TCP port 17533
- Be able to resolve the BlackBerry Proxy server's hostname
- Allow an inbound port (this port is arbitrary)
- Have a publicly resolvable DNS hostname



Configure Direct Connect using a forward proxy

Before you begin:

- Configure a single public DNS entry for the forward proxy (for example, bp-proxy.mydomain.com).
  Note: You can configure multiple proxy servers with separate DNS names (for example, if you have multiple Direct Connect-enabled proxy clusters that you want to identify separately).
- Configure the external firewall to allow inbound connections on the port that the proxy will listen on. This can be any port you specify.
- If the forward proxy is installed in a DMZ, ensure that port 17533 is open from the proxy to each BlackBerry Connectivity Node.

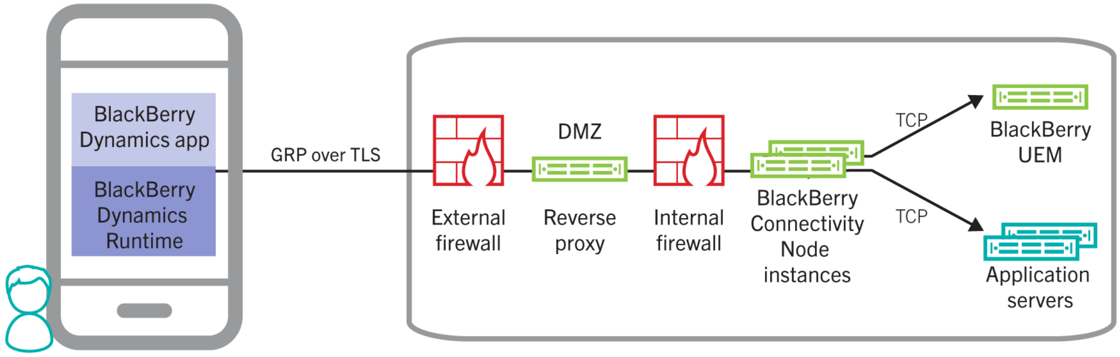
1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Direct Connect**.
3. Click a BlackBerry Proxy instance.
4. To turn on Direct Connect, select the **Turn on Direct Connect** check box. In the BlackBerry Proxy host name field, verify that the host name is correct.
5. Select the **Use web proxy** check box. Specify the FQDN of the public DNS entry and the listening port that is configured for the proxy.
6. Repeat steps 4 and 5 for all BlackBerry Proxy instances in the cluster.

   To enable only some BlackBerry Proxy instances for Direct Connect, create a new BlackBerry Proxy cluster. All servers in a cluster must have the same configuration. For more information, see Manage BlackBerry Proxy clusters in the Configuration content.
7. Click **Save**.

Reverse proxy

Use reverse proxy for server-side load balancing using your own scheme, instead of a round robin scheme using DNS. In addition, using a reverse proxy with SSL bridging allows you to authenticate BlackBerry Dynamics apps in the DMZ using client certificates issued by your own certificate authority.

You can set up Direct Connect with a reverse proxy server using an appliance like F5 BIG-IP Local Traffic Manager (LTM) or Citrix NetScaler.



Configure direct connect using a reverse proxy

Before you begin:

- Create a public DNS entry for the BlackBerry Proxy cluster. This is the address that clients will use to connect to the externally facing reverse proxy appliance.
  Note: You must configure multiple public DNS entries if you have multiple Direct Connect-enabled proxy clusters.
- Configure the external firewall to allow inbound connections on port 17533 to the reverse proxy or appliance.
- If the reverse proxy or appliance is installed in a DMZ, ensure that port 17533 is open from the proxy to each BlackBerry Connectivity Node.
- If the BlackBerry Connectivity Node instances are also installed in a DMZ, ensure that the appropriate ports are open between each BlackBerry Connectivity Node and any application servers that the BlackBerry Dynamics apps need to access (for example, Microsoft Exchange, internal web servers, and the BlackBerry UEM Core).

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Direct Connect**.
3. Click a BlackBerry Proxy instance.
4. To turn on Direct Connect, select the **Turn on Direct Connect** check box. In the **BlackBerry Proxy host name** field, specify the public FQDN entry you created for the BlackBerry Proxy cluster. The same host name value will be used for all BlackBerry Proxy instances. Load balancing must be handled by the reverse proxy or appliance.
5. Repeat steps 3 and 4 for all BlackBerry Proxy instances in the cluster.

   To enable only some BlackBerry Proxy instances for Direct Connect, create a new BlackBerry Proxy cluster. All servers in a cluster must have the same configuration. For more information, see Manage BlackBerry Proxy clusters in the Configuration content.
6. Click **Save**.

Configure the authentication of BlackBerry Dynamics apps in the DMZ

To authenticate BlackBerry Dynamics apps in the DMZ, you must configure your own TLS server certificate for Direct Connect from the BlackBerry UEM management console (**Settings** > **Infrastructure** > **Server certificates** and select the **BlackBerry Dynamics certificates** tab). This allows the BlackBerry Dynamics app to trust the TLS server certificate that will be used by the SSL bridging appliance to terminate the Direct Connect TLS connection.

Server certificate requirements

When you replace the Direct Connect certificate through the UEM management console (see Changing BlackBerry UEM certificates), the certificate file must include the entire certificate chain. You must provide the PKCS 12 file, which has the key-pair for the BlackBerry Proxy and the complete certificate chain ending in the root Certificate Authority (CA). These required root CA and Intermediate certificate authorities are then automatically sent to the BlackBerry Dynamics containers, while the full certificate chain is also sent to the BlackBerry Proxy. You do not need to create a CA certificate profile to send to the BlackBerry Dynamics app.

This is the server certificate that the SSL bridging appliance uses for the TLS connection to the BlackBerry Proxy.

Client certificate requirements

To authenticate BlackBerry Dynamics apps in the DMZ, you must provide client certificates to the BlackBerry Dynamics apps from your enterprise certificate authority using one of the certificate distribution mechanisms supported by BlackBerry UEM. You must also configure the load balancer to challenge the BlackBerry Dynamics apps to authenticate the TLS connection with the client certificates.

Legal notice

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada