

# BlackBerry MDS Connection Service Integrated Authentication

Version: 5.0 | Service Pack: 2

## Security Note



# Contents

<b>1</b>	<b>Protecting your organization's resources when using BlackBerry MDS Connection Service integrated authentication</b>	<b>2</b>
	Architecture: BlackBerry MDS Connection Service integrated authentication.....	2
	How the BlackBerry MDS Connection Service uses Kerberos to help protect your organization's resources.....	3
	Identifying the resources that users can access using BlackBerry MDS Connection Service integrated authentication	3
	.....	3
<b>2</b>	<b>Process flow: Retrieving a resource when using BlackBerry MDS Connection Service integrated authentication</b>	<b>5</b>
	.....	5
<b>3</b>	<b>Configuring Integrated Windows authentication so that users can access resources on your organization's network</b>	<b>7</b>
	.....	7
	System requirements for your organization's environment.....	7
	Configuring the Microsoft Active Directory account to delegate access.....	8
	Prerequisites: Configuring the Microsoft Active Directory account to delegate access to an intranet site.....	8
	Configure the Microsoft Active Directory account to delegate access to an intranet site.....	8
	Prerequisites: Configuring the Microsoft Active Directory account to delegate access to a shared folder.....	9
	Configure the Microsoft Active Directory account to delegate access to a shared folder.....	9
	Configuring the BlackBerry MDS Connection Service when the messaging server is located in a remote Microsoft Active Directory domain.....	10
	Configure the BlackBerry MDS Connection Service when Microsoft Exchange is located in a remote Microsoft Active Directory domain.....	11
	Configure the BlackBerry MDS Connection Service when IBM Lotus Domino is located in a remote Microsoft Active Directory domain.....	11
	Turn on Integrated Windows authentication so that users can access resources on your organization's network.....	12
<b>4</b>	<b>Related resources.....</b>	<b>14</b>
<b>5</b>	<b>Glossary.....</b>	<b>15</b>
<b>6</b>	<b>Provide feedback.....</b>	<b>17</b>
<b>7</b>	<b>Legal notice.....</b>	<b>18</b>

# Protecting your organization's resources when using BlackBerry MDS Connection Service integrated authentication

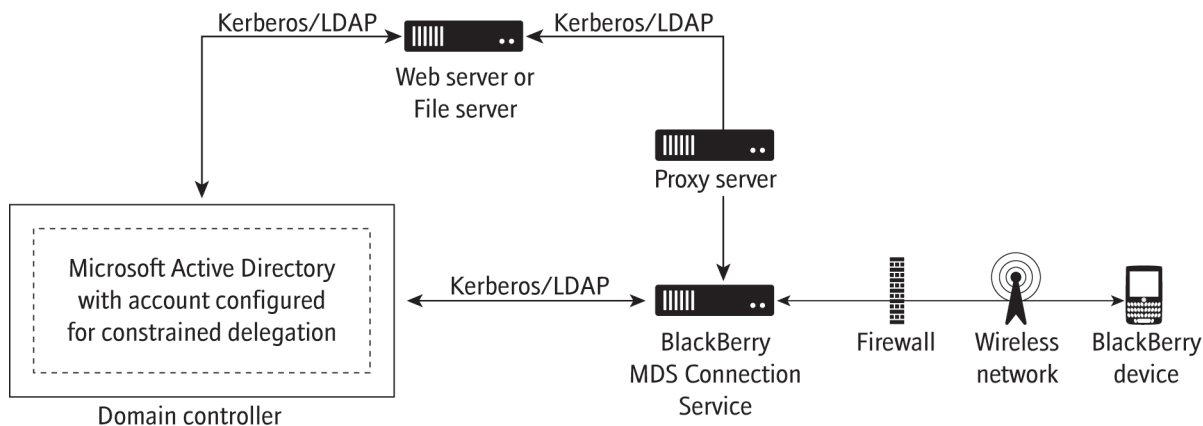
1

You can configure the BlackBerry® MDS Connection Service to support Integrated Windows® authentication so that BlackBerry device users can access the intranet or shared files from the BlackBerry® Browser or the Files application on BlackBerry devices. By default, if you configure the BlackBerry MDS Connection Service and users access the intranet or a shared file, the users must authenticate with your organization's domain controller by providing their Microsoft® Active Directory® account passwords. In BlackBerry® Enterprise Server 5.0 SP2, you can configure the BlackBerry MDS Connection Service so that users are not required to type a password each time they want to access a resource.

If you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, the BlackBerry MDS Connection Service uses the Kerberos™ protocol and constrained delegation to help protect your organization's environment and authenticate and authorize users. The Kerberos protocol is designed to permit the BlackBerry MDS Connection Service to verify user accounts in Microsoft Active Directory. Constrained delegation is designed to limit the resources that the BlackBerry MDS Connection Service can provide authenticated users access to.

If you want to configure both BlackBerry Administration Service single sign-on and BlackBerry MDS Connection Service integrated authentication, you should configure separate Microsoft Active Directory accounts for the BlackBerry Administration Service and BlackBerry MDS Connection Service.

## Architecture: BlackBerry MDS Connection Service integrated authentication



Component	Description
BlackBerry® MDS Connection Service	The BlackBerry MDS Connection Service permits BlackBerry device users to access web content, the Internet, or your organization's intranet. It also permits applications on devices to connect to your organization's application servers or content servers for application data and updates.
domain controller	A domain controller is a server that authenticates and authorizes Windows® users and Windows servers with a Windows domain.
Microsoft® Active Directory®	Microsoft Active Directory is an LDAP directory that stores user information.

## How the BlackBerry MDS Connection Service uses Kerberos to help protect your organization's resources

BlackBerry® MDS Connection Service integrated authentication is designed to use the Kerberos™ protocol and constrained delegation to authenticate BlackBerry device users in your organization's network in a highly secure manner. BlackBerry MDS Connection Service authenticates with Microsoft® Active Directory® on behalf of users, verify the users' identities, and retrieve the resource on behalf of the users.

The BlackBerry MDS Connection Service hosts a Kerberos service that permits it to verify users. To support BlackBerry MDS Connection Service integrated authentication, you must configure Microsoft Active Directory accounts in the Microsoft Active Directory domains that include the resources and configure constrained delegation for the Microsoft Active Directory accounts. To configure constrained delegation, you must configure the Microsoft Active Directory accounts to trust only the Kerberos service that is hosted by the BlackBerry MDS Connection Service.

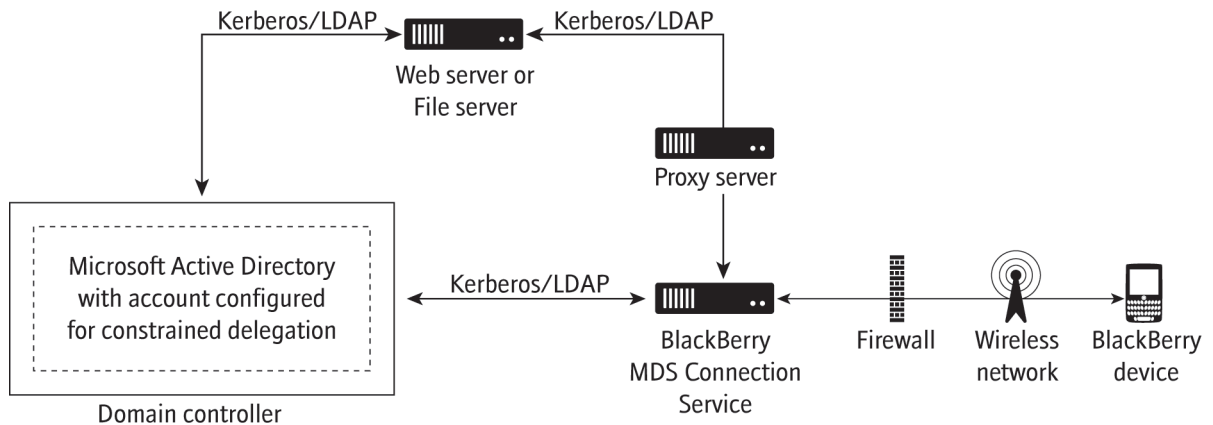
When the BlackBerry MDS Connection Service starts, it authenticates with the Microsoft Active Directory domain using the Microsoft Active Directory account. The domain controller issues the Kerberos keys and Kerberos service ticket to the Kerberos service. The Kerberos keys permit the BlackBerry MDS Connection Service to verify the Kerberos service tickets for users.

## Identifying the resources that users can access using BlackBerry MDS Connection Service integrated authentication

If you configure the BlackBerry® MDS Connection Service to support the Kerberos™ protocol and constrained delegation, you must use the BlackBerry Administration Service to specify the pull rules that identify the shared files or intranet resources that you want to permit Integrated Windows® authentication for. You must assign the pull rules to groups or user accounts so that the BlackBerry MDS Connection Service can determine which user accounts to apply the pull rules to. Pull rules permit you to specify the shared files or intranet resources in your organization's network that you want users to access from BlackBerry devices and the authentication method that you want users to use to access the shared files or Intranet resources.

For information about configuring pull rules, see the *BlackBerry Enterprise Server Administration Guide*.

## Process flow: Retrieving a resource when using BlackBerry MDS Connection Service integrated authentication 2



1. The BlackBerry® device user navigates to a resource on your organization's intranet or on a file share (for example, a web page or shared file) using the BlackBerry® Browser or Files application on the BlackBerry device.
2. The device encrypts and compresses an HTTP request for the resource and sends the encrypted HTTP request to the BlackBerry Router using BlackBerry transport layer encryption.
3. The BlackBerry Router forwards the encrypted HTTP request to the BlackBerry Dispatcher.
4. The BlackBerry Dispatcher decrypts and decompresses the HTTP request and forwards the request to the BlackBerry MDS Connection Service.
5. The BlackBerry MDS Connection Service performs the following actions:
  - verifies whether the resource is located in a Microsoft® Active Directory® domain that is configured for Integrated Windows authentication
  - checks the pull rules assigned to the user accounts and verifies that the user must use Integrated Windows authentication to access the resource
  - connects to the Microsoft Active Directory using its Microsoft Active Directory account that is configured for constrained delegation
  - retrieves the Microsoft Active Directory user name for the user from Microsoft Active Directory
  - retrieves the Kerberos™ service ticket for the user from Microsoft Active Directory using the S4U2proxy extension
  - encodes the service ticket using Base-64 encoding and adds the service ticket to the header of the HTTP request
  - resends the request for the resource to the web server or file system that hosts the resource
6. The web server or file system returns the resource to BlackBerry MDS Connection Service.
7. The BlackBerry MDS Connection Service forwards the resource to the BlackBerry Dispatcher.

8. The BlackBerry Dispatcher encrypts and compresses the resource and splits it into packages and sends the packages to the BlackBerry Router.
9. The BlackBerry Router sends the packages to the device using BlackBerry transport layer encryption.
10. The device decrypts and decompresses the packages and displays the resource to the user.

# Configuring Integrated Windows authentication so that users can access resources on your organization's network

3

To permit BlackBerry® device users to access resources on your organization's network using BlackBerry devices without requiring the users to type a user name and password each time they access the network resources, you can configure the BlackBerry MDS Connection Service to support Integrated Windows® authentication. Users can then access network resources such as intranet sites and network shared folders on their devices using the BlackBerry® Browser or Files application without typing a user name and password.

Before you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, you must create a Microsoft® Active Directory® account in each Microsoft Active Directory domain that includes resources that you want to turn on Integrated Windows authentication for. You must configure constrained delegation for the Microsoft Active Directory accounts so that they delegate access to each intranet site or network shared folder in the Microsoft Active Directory domain.

You must also configure two-way trust between the Microsoft Active Directory domain that the BlackBerry MDS Connection Service is running on and other Microsoft Active Directory domains in other forests that the BlackBerry MDS Connection Service must connect to. The S4U2proxy extension that the BlackBerry MDS Connection Service uses to retrieve the Kerberos™ service tickets for users requires a two-way trust between Microsoft Active Directory domains.

After you turn on Integrated Windows authentication and specify a Microsoft Active Directory account in the BlackBerry Administration Service, you must specify web address patterns for the network resources that you want to permit users to access, create a pull rule for the web address patterns, permit access to the web address patterns using the pull rule, and assign the pull rule to users or a group.

After you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, the BlackBerry MDS Connection Service uses the Microsoft Active Directory account to verify login information for a user and access the network resources on behalf of the user. The BlackBerry Enterprise Server then sends information from the network resources to the user's device.

## System requirements for your organization's environment

The following system requirements apply when you configure single sign-on authentication for the BlackBerry® Administration Service and BlackBerry® Web Desktop Manager or configure the BlackBerry MDS Connection Service to support Integrated Windows® authentication.

Item	Requirement
network services	Microsoft® Active Directory® running at Windows Server® 2003 domain functional level or higher

Item	Requirement
application server	For the BlackBerry MDS Connection Service to support Integrated Windows authentication, Microsoft® IIS 6.0 or 7.0 using Integrated Windows authentication
file server	For the BlackBerry MDS Connection Service to support Integrated Windows authentication, Windows Server 2003 file services or Windows Server 2008 file services

## Configuring the Microsoft Active Directory account to delegate access

### Prerequisites: Configuring the Microsoft Active Directory account to delegate access to an intranet site

- Verify that you configured Integrated Windows® authentication for the application server that hosts the intranet site.
- Verify that the application server that hosts the intranet site and the web application that runs on the application server support Kerberos™ authentication.
- Verify that you have permission to update the Microsoft® Active Directory® account in Microsoft Active Directory.
- Verify that you have access to the Windows Server® setspn tool that is included with the Windows Server Support Tools. For more information about the setspn tool, visit <http://technet.microsoft.com> to read *Setspn Overview*.
- If you did not configure a Microsoft Active Directory account to delegate access to an intranet site or shared folder, in Microsoft Active Directory, you must create a Microsoft Active Directory account that should have the following conditions:
  - a password that meets the security requirements of your organization
  - the user is not required to change their password the next time that the user logs in
  - the user's password never expires
- If you configured a pool of application servers to host the intranet site, and the pool is running on Microsoft® IIS and is located behind a load balancer, specify a user account (also known as the identity) for the pool that hosts the intranet site. For more information, see [http://technet.microsoft.com/en-us/library/cc771170\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771170(WS.10).aspx).

### Configure the Microsoft Active Directory account to delegate access to an intranet site

You are required to have only one Microsoft® Active Directory® account in each Microsoft Active Directory domain that includes the resources that you want to turn on Integrated Windows® authentication for.

For more information about configuring the Microsoft Active Directory account using setspn and Microsoft Active Directory, visit [www.blackberry.com/btsc](http://www.blackberry.com/btsc) to read article KB22726.

1. If a pool of application servers host a intranet site and the pool is running on Microsoft® IIS and is located behind a load-balancer, use setspn or ADSI to add the SPNs of the intranet site to the user account (also known as the identity) of the pool. You must configure the SPNs using the FQDN and the name of the intranet site that users type into their browsers (for example, if users type `http://intranet_site` in their browsers, the name of the intranet site is `intranet_site`).

2. In Microsoft Active Directory, in the Microsoft Active Directory account properties, if the **Delegation** tab does not display, update the default HOST SPN registrations for the Microsoft Active Directory account.
3. In the Microsoft Active Directory account properties, on the **Delegation** tab, configure the following settings:
  - trust this user for delegation to specified services only
  - use any authentication protocol
4. Click **Add**.
5. Perform one of the following tasks:
  - If a pool of application servers hosts the intranet site and the pool is running on Microsoft IIS and is located behind a load-balancer, select the user account that runs the application pools in the Microsoft IIS servers.
  - If the intranet site is hosted by one application server, select the application server that hosts the intranet site.
6. Select the HTTP service type for the user account or application server that you specified.
7. Repeat steps 1 to 6 for each intranet site that you want to turn on integrated Windows authentication for.

**After you finish:**

- If required, configure BlackBerry® MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.
- Turn on Integrated Windows authentication when users access resources on your organization's network.

## Prerequisites: Configuring the Microsoft Active Directory account to delegate access to a shared folder

- Verify that you configured Integrated Windows® authentication for the file server that hosts the shared folders.
- Verify that you have permission to update the Microsoft® Active Directory® account in Microsoft Active Directory.
- Verify that you have access to the Windows Server® setspn tool that is included with the Windows Server Support Tools. For more information about the setspn tool, visit <http://technet.microsoft.com> to read *Setspn Overview*.
- If you did not configure a Microsoft Active Directory account to delegate access to an intranet site or shared folder, in Microsoft Active Directory, you must create a Microsoft Active Directory account that should have the following conditions:
  - the password meets the security requirements of your organization
  - the user is not required to change their password the next time that the user logs in
  - the user's password never expires

## Configure the Microsoft Active Directory account to delegate access to a shared folder

You are required to have only one Microsoft® Active Directory® account in each Microsoft Active Directory domain that includes the resources that you want to turn on Integrated Windows® authentication for.

For more information about configuring the Microsoft Active Directory account using setspn and Microsoft Active Directory, visit [www.blackberry.com/btsc](http://www.blackberry.com/btsc) to read article KB22726.

1. In Microsoft Active Directory, in the Microsoft Active Directory account properties, if the **Delegation** tab does not display, update the default HOST SPN registrations for the Microsoft Active Directory account.
2. In the Microsoft Active Directory account properties, on the **Delegation** tab, configure the following settings:
  - trust this user for delegation to specified services only
  - use any authentication protocol
3. Click **Add**.
4. Select the the file server that hosts the shared folder.
5. Select the CIFS service type for the file server that you specified.
6. Repeat steps 3 to 5 for each shared folder that you want to turn on Integrated Windows authentication for.

**After you finish:**

- If required, configure BlackBerry® MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.
- Turn on Integrated Windows authentication when users access resources on your organization's network.

## Configuring the BlackBerry MDS Connection Service when the messaging server is located in a remote Microsoft Active Directory domain

If the computer that hosts the BlackBerry® MDS Connection Service is not located in the same Microsoft® Active Directory® domain as the global catalog server or messaging server and you want to configure support for Integrated Windows® authentication, you must create a Microsoft Active Directory account that the BlackBerry MDS Connection Service can use to connect to the global catalog server.

In a Microsoft® Exchange environment, you must create the Microsoft Active Directory account in the Microsoft Active Directory domain that includes the messaging server.

In an IBM® Lotus® Domino® environment, if the messaging server is located in the same Microsoft Active Directory domain as the global catalog server, you must create the Microsoft Active Directory account in that domain. If the messaging server is located in a different Microsoft Active Directory domain than the global catalog server, you must create the Microsoft Active Directory account in the Microsoft Active Directory domain that includes the global catalog server.

You do not need to configure constrained delegation for the Microsoft Active Directory account that you create in the Microsoft Active Directory domain that includes the messaging server or global catalog server.

## Configure the BlackBerry MDS Connection Service when Microsoft Exchange is located in a remote Microsoft Active Directory domain

**Before you begin:** Create a Microsoft® Active Directory® account in the Microsoft Active Directory domain that the messaging server or global catalog server is located in.

1. On the computer that hosts the BlackBerry® MDS Connection Service, navigate to `<drive>\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config`.
2. In a text editor, open the **rimpublic.properties** file.
3. In the **rimpublic.properties** file, type **application.handler.exchange.domain=<domain\_name>** where `<domain_name>` is the Microsoft Active Directory domain that contains the messaging server. For example, type **application.handler.exchange.domain=domain123.example.com**.
4. Save and close the **rimpublic.properties** file.
5. In the Windows® Services, restart the BlackBerry MDS Connection Service service.

**After you finish:** Turn on Integrated Windows authentication when users access resources on your organization's network.

## Configure the BlackBerry MDS Connection Service when IBM Lotus Domino is located in a remote Microsoft Active Directory domain

**Before you begin:** Create a Microsoft® Active Directory® account in the Microsoft Active Directory domain that the messaging server or global catalog server is located in.

1. On the computer that hosts the BlackBerry® MDS Connection Service, navigate to `<drive>\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config`.
2. In a text editor, open the **rimpublic.properties** file.
3. Perform one of the following actions:
  - If the IBM® Lotus® Domino® server is installed in a Microsoft Active Directory domain with a global catalog server, in the **rimpublic.properties** file, type **application.handler.exchange.domain=<domain\_name>** where `<domain_name>` is the Microsoft Active Directory domain that contains the messaging server. For example, type **application.handler.exchange.domain=domain123.example.com**.
  - If the Lotus Domino server is not installed in a Microsoft Active Directory domain with a global catalog server, in the **rimpublic.properties** file, type **application.handler.exchange.domain=<domain\_name>** where `<domain_name>` is the Microsoft Active Directory domain that contains the global catalog server. For example, type **application.handler.exchange.domain=domain123.example.com**.
4. Save and close the **rimpublic.properties** file.
5. In the Windows® Services, restart the BlackBerry MDS Connection Service service.

**After you finish:** Turn on Integrated Windows authentication when users access resources on your organization's network.

## Turn on Integrated Windows authentication so that users can access resources on your organization's network

### Before you begin:

- Configure the Microsoft® Active Directory® account to access resources on your organization's network.
  - If required, configure BlackBerry® MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.
1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology > BlackBerry Domain > Component view**.
  2. Click **MDS Connection Service**.
  3. Click **Edit component**.
  4. In the **Integrated authentication turned on** drop-down list, click **Yes**.
  5. For each Microsoft Active Directory account, provide the following information:
    - In the **Delegation user domain** field, type the FQDN (for example, **ldap.example.com**).
    - In the **Delegation user name** field, type the user name.
    - In the **Password** and **Confirm** fields, type the password.
  6. Click **Save all**.
  7. On the **HTTP** tab, click **Edit component**.
  8. In the **Authentication support enabled** drop-down list, click **Yes**.
  9. Click **Save all**.
  10. On the **Pull URL Patterns** tab, specify web address patterns for the intranet sites or shared folders that you want to permit BlackBerry device users to access (for example, **intranet\_site(:80)?(\/.\*?)**). The web address patterns are based on Java® regular expressions. Consider specifying the following web address patterns:
    - Specify **\*\.\*\.\*** as the web address pattern so that you can prevent users from using any other web address patterns to access intranet sites or shared network folders.
    - Specify **\*** as the web address pattern for OCSP, LDAP, and TCP to permit users to communicate with OCSP servers, LDAP servers, or TCP servers.
  11. On the **Access control rules** tab, create a pull rule for each of the web address patterns that you specified. When you create the pull rule, in the **Authentication** drop-down list, click **Integrated** or **Integrated and RSA**.
  12. Click **Save all**.
  13. Assign the pull rules to the users or groups that you want to access intranet sites or shared network folders.
  14. On the **Servers and components** menu, expand **BlackBerry solution topology > BlackBerry Domain > Component view > MDS Connection Service**.

15. Click a BlackBerry MDS Connection Service instance.
16. Click **Edit instance**.
17. In the **Pull Authorization** drop-down list, click **Yes**.
18. Click **Save all**.
19. Repeat step 16 to 20 for each BlackBerry MDS Connection Service instance.

## Related resources

## 4

You can use the following related resources to find out more about Kerberos™ and constrained delegaton:

- [Kerberos authentication and troubleshooting delegation issues](#)
- [Kerberos Authentication Technical Reference](#)
- [Windows Server® 2003 Kerberos Extensions](#)
- [Kerberos Protocol Transition and Constrained Delegation](#)
- [Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification](#)
- [Exploring S4U Kerberos Extensions in Windows Server 2003](#)
- [IIS and Kerberos. Part 2 - Service Principal Names](#)
- [IIS and Kerberos. Part 3 - A simple scenario](#)
- [BlackBerry security](#)

# Glossary

## 5

### **BlackBerry transport layer encryption**

BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.

### **CIFS**

common Internet file system

### **FQDN**

fully qualified domain name

### **HTTP**

Hypertext Transfer Protocol

### **IIS**

Internet Information Services

### **KDC**

A Key Distribution Center (KDC) is a server that performs the trusted arbitrator role for the Kerberos™ protocol. The KDC issues service tickets and maintains a list of tickets that it issued. Domain controllers are KDCs.

### **Kerberos protocol**

The Kerberos™ protocol is a Microsoft® Active Directory® authentication protocol that permits a trusted third-party application to authenticate clients by exchanging encrypted service tickets with Microsoft Active Directory.

### **LDAP**

Lightweight Directory Access Protocol

### **OCSP**

Online Certificate Status Protocol

### **S4U2proxy extension**

The S4U2proxy (Service-for-User-to-Proxy) extension completes the constrained delegation process. It permits a Kerberos™ enabled service to retrieve the service ticket of another Kerberos enabled service from the KDC on behalf of a client.

### **service ticket**

A service ticket is a Kerberos™ key that a client of a Kerberos enabled service can use to open a trusted session with the Kerberos enabled service. The client of the Kerberos enabled service retrieves the service ticket for the Kerberos enabled service from the KDC.

### **SPN**

A service principal name (SPN) is an attribute of a user or group in Microsoft® Active Directory® that supports mutual authentication between a client of a Kerberos™ enabled service and the Kerberos enabled service. A Microsoft Active Directory account can have one or more SPNs.

**TCP**

Transmission Control Protocol

## Provide feedback

6

To provide feedback on this deliverable, visit [www.blackberry.com/docsfeedback](http://www.blackberry.com/docsfeedback).

## Legal notice

## 7

©2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

IBM, Domino, and Lotus are trademarks of International Business Machines Corporation. Java is a trademark of Sun Microsystems, Inc. Kerberos is a trademark of Massachusetts Institute of Technology. Microsoft, Active Directory, Windows, and Windows Server are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at [www.blackberry.com/go/docs](http://www.blackberry.com/go/docs) is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM 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 web sites (collectively the "Third Party Products and Services"). RIM 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 RIM 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 RIM 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 RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM 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 RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM 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 RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM 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 RIM OR ANY AFFILIATES OF RIM 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 RIM'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 RIM'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 RIM and RIM 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 RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

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

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

Research In Motion Limited  
295 Phillip Street  
Waterloo, ON N2L 3W8  
Canada

Research In Motion UK Limited  
Centrum House  
36 Station Road  
Egham, Surrey TW20 9LF  
United Kingdom

Published in Canada