



# **BlackBerry AtHoc**

## **Smart Card Authentication Configuration Guide**

7.9



# Contents

- What is Smart Card Authentication?..... 4**
  - How smart card authentication works in BlackBerry AtHoc..... 4
- Enable smart card authentication for operators..... 5**
  - BlackBerry AtHoc management system configuration..... 5
  - IIS configuration..... 5
- Enable smart card authentication for the Desktop App.....6**
  - BlackBerry AtHoc management system configuration..... 6
  - IIS configuration..... 6
- Update the application server..... 7**
- Update the database server..... 8**
- Determine the regular expression..... 10**
  - Regular expression test tool..... 10
  - Update the database..... 11
- Troubleshooting smart card authentication..... 12**
- Appendix A: Retrieve certification information..... 13**
- BlackBerry AtHoc customer portal..... 14**
- Legal notice..... 15**

# What is Smart Card Authentication?

When smart card authentication is enabled in addition to regular username/password authentication, users have the option of logging in to BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN.

If you choose to require Operators to log in using smart cards, the following changes occur in the administrative side of the BlackBerry AtHoc system:

- All sub organizations of the main organization inherit the smart card-only authentication method.
- The log in screen continues to display **Username** and **Password** fields because until a user attempts to log in, the system has no way of knowing what organization the user belongs to and what restrictions, if any, the user's organization has imposed on authentication.
- After the user attempts to log in with a username or password combination, the system returns an error message informing them that they must use their smart card for system authentication.

## How smart card authentication works in BlackBerry AtHoc

When Smart Card authentication is enabled, the operator's mapping ID (MID) attribute is used to authenticate at log in. The data in the mapping ID comes from one of the following sources:

- A sync with Active Directory's attribute (sAMAccountName, userprincipalname, or mail) when using either the AD Sync module or the CSV Importer tool.
- A user import using the Import option in the End Users manager in BlackBerry AtHoc that includes the mapping ID column.
- A manual update of an operator's mapping ID in the End Users manager in BlackBerry AtHoc.

BlackBerry AtHoc uses a regular expression to extract the value for the mapping ID from one of the HTTP header fields that contains the certificate data. BlackBerry AtHoc then compares this mapping ID with the operator's mapping ID to determine their identity. The values for the HTTP header field and the regular expression are specified in the database and can be modified. However, the values apply system-wide and cannot be different for each organization.

The middle tier code attempts to use the primary HTTP\_CAC\_VARIABLE, if present, and validates the operator. If a valid operator is not found, the middle tier code then attempts to use ALT\_HTTP\_CAC\_VARIABLE to validate the operator.

In BlackBerry AtHoc release 7.3 or later, if a valid operator is still not found, the middle tier code then attempts to use the Subject Alternative Name to validate the operator.

**Table 1: Login source code by BlackBerry AtHoc release**

BlackBerry AtHoc release	File
6.1.8.85R3SP4CP1	wwwroot\client\dotnet\Controllers\AuthController.cs
7.0.0.2	wwwroot\client\dotnet\Controllers\SmartCardController.cs


# Enable smart card authentication for operators

When smart card authentication is enabled in addition to regular username/password authentication, users have the option of logging in to BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. When smart card authentication is required, users can *only* access BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN.

**Note:** In order to use this option, you must set up mapping IDs for each user through the users manager in the BlackBerry AtHoc management system.

## BlackBerry AtHoc management system configuration

Use the BlackBerry AtHoc management system to enable smart card log in for operators.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. Change to the System Setup (3) organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **Security Policy**.
5. In the **Smart Card Authentication** section, select **Smart Card Login**.
6. Optionally, to require smart card authentication, select **Require Smart Card**.
7. Click **Save**.

**Note:** This is a system-wide setting that applies to all organizations.

## IIS configuration

Smart card authentication for operator log in requires the following settings in IIS. In the SSL Settings feature under the client web application, select the **Require SSL** check box and the **Require** option under “Client certificates.”

**Table 2: SSL settings by BlackBerry AtHoc version**


Version	Notes
All	Default web site > SSL Settings: Required + Ignore
6.1.8.87 CP1CHF2 and earlier	Default web site > Client > SSL Settings: Required + Accept
6.1.8.87 CP1CHF4 and later	Default Web Site > Client > SmartCard > SSL Settings: Required + Accept Default Web Site > SelfService > AuthCAC > SSL Settings: Required + Accept

# Enable smart card authentication for the Desktop App

This section includes information about configuration updates in the BlackBerry AtHoc management system and IIS that are needed to enable smart card authentication for the BlackBerry AtHoc desktop app.

## BlackBerry AtHoc management system configuration

You can enable smart card authentication for the desktop app in the BlackBerry AtHoc management system.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. In the navigation bar, click .
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select **Enable** beside **Smart Card**.
5. In the **Assign Authentication Methods to Applications** section, select **Smart Card** from the **Authentication Method** list.
6. Select the number of client certificates to collect from the list. The recommended value is 3.
7. Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=( ? <edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.
8. Click **Save**.

**Note:** This setting must be configured for each organization.

## IIS configuration

Smart card authentication for the desktop app requires the following settings in IIS.

In the **SSL Settings** feature under the client web application, select the **Require SSL** check box. Smart card authentication for the desktop app works with any of the options under Client certificates. However, to avoid end users receiving a PIN prompt every few minutes, select the **Ignore** option.

# Update the application server

The BlackBerry AtHoc application server is supported on Windows 2012R2 and later versions.

To enable smart card authentication, you must add the following new key in the registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL Value  
name: ClientAuthTrustMode Value type: REG_DWORD Value data: 2.
```

# Update the database server

Values in the database server that are used in smart card authentication are stored in the GLB\_CONFIG\_TAB in the ngaddata database. These values include the following items:

- The name of the HTTP header that contains the information.
- The regular expression that is used to extract the information.

**Table 3: Version-specific notes**

Version	Notes
6.1.8.84 CP9 and earlier	BlackBerry AtHoc version 6.1.8.84 CP9 and earlier do not have a value in the GLB_CONFIG_TAB for the default HTTP header variable. It is hard-coded as SubjectCN.
7.0.0.2 and later	A Require Smart Card option is available that appears when you select Smart Card Login.

**Table 4: Smart card settings in PRV\_SECURITY\_POLICY\_TAB**

KEY_NAME	6.1.8.90 and earlier	7.0.0.2 and later
SMART_CARD_ENFORCED	Value is not present.	Value is present.

Y = value is present. N = value is not present.

**Table 5: Smart card settings in GLB\_CONFIG\_TAB**

KEY_NAME	6.1.8.84 CP9	6.1.8.85 R3SP4 CP1	6.1.8.85 R3SP4CP1 (and hot-fixes)	7.3
ALT_HTTP_CAC_REGEX	Y	Y	Y	Y
ALT_HTTP_CAC_VARIABLE	Y	Y	Y	Y
CAC_CHECK_PRESENT	N	N	Y	Y
CAC_CHECK_VALID	N	N	Y	Y
CAC_REGEX	Y	Y	Y	Y
CAC_SAN_REGEX	N	N	N	Y
HTTP_CAC_REGEX	N	Y	Y	Y
HTTP_CAC_VARIABLE	N	Y	Y	Y



**Table 6: Definitions of smart card settings**

KEY_NAME	Notes
ALT_HTTP_CAC_REGEX	(Operator log on) Alternate regular expression for extracting the mapping ID from the CAC certificate.
ALT_HTTP_CAC_VARIABLE	(Operator log on) Alternate HTTP header variable that contains the mapping ID from the CAC certificate.
CAC_CHECK_PRESENT	(Operator log on) Specifies if the system should check that the CAC certificate is present.
CAC_CHECK_VALID	(Operator log on) Specifies if the system should check that the CAC certificate is valid.
CAC_REGEX	Primary regular expression for extracting the mapping ID from the certificate data passed by the BlackBerry AtHoc desktop app during sign on.
CAC_SAN_REGEX	(Operator log on) Alternate regular expression to extract the email address from the Subject Alternative Name in the certificate.
HTTP_CAC_REGEX	Primary regular expression for extracting the mapping ID from the certificate during operator log on.
HTTP_CAC_VARIABLE	Primary HTTP header variable to search for mapping ID during Operator log on.

**Table 7: Correlation of smart card settings between the database and user interface**

KEY_NAME	Visible in management system
ALT_HTTP_CAC_REGEX	No
ALT_HTTP_CAC_VARIABLE	No
CAC_CHECK_PRESENT	No
CAC_CHECK_VALID	No
CAC_REGEX	No
CAC_SAN_REGEX	No
HTTP_CAC_REGEX	No
HTTP_CAC_VARIABLE	No

# Determine the regular expression

The following three regular expression values are provided to extract the user's Mapping ID:

1. HTTP\_CAC\_REGEX: The primary regex in BlackBerry AtHoc for operator login.
2. ALT\_HTTP\_CAC\_REGEX: The first alternate regex in BlackBerry AtHoc for operator login.
3. CAC\_SAN\_REGEX: The second alternate regex in BlackBerry AtHoc for operator login.

The BlackBerry AtHoc server tries HTTP\_CAC\_REGEX first. If ALT\_HTTP\_CAC\_REGEX results in an empty string, the server tries to use CAC\_SAN\_REGEX. If none of these regular expressions extracts a value or retrieves incorrect information, smart card log in fails.

To determine what the issue is, check the certificate and verify that at least one of the regular expressions extracts the value. For more information, see [Appendix A: Retrieve certification information](#).

## Regular expression test tool

You can use an online regular expression test tool to test regular expressions. Enter the data and adjust the regular expression until the mapping ID is extracted from the data.

The SQL to retrieve the current regular expression from the database is:

```
SELECT value FROM GLB_CONFIG_TAB where KEY_NAME = 'ALT_HTTP_CAC_REGEX'
```

When the preconfigured regular expression values do not extract the correct information, modify the regular expression stored in ALT\_HTTP\_CAC\_REGEX. The default value is:

```
(?<MID>\d{8,10})(?!.*\d)
```

Where:

- ?<MID> is the named group MID that the middle tier code requires. The remaining regex inside the parenthesis with ?<MID> is the sub expression: \d{8,10}.
- \d matches any decimal digit, and \d{8,10} matches any number between 8 and 10 digits.
- (?!.\*\d) matches a dot 0 or more times, a decimal digit once, and that expression is used by (?<MID>\d{8,10}) to extract numbers with 8 to 10 digits. For example:
  - 0069651550.CBP evaluates to 0069651550 (Good—Extracts between 8 and 10 digits to the left of the decimal.)
  - FIRST.LAST.MI.1233837489 evaluates to 1233837489 (Good—Extracts between 8 and 10 digits to the right of last decimal.)
  - 1234567890.CBP.11223344 evaluates to 11223344 (Good—Extracts between 8 and 10 digits of the last number.)
  - 1234567890.CBP.112233445566 evaluates to 2233445566 (Bad—Truncates digits when there are more than 10. You need to update the regex: (?<MID>\d{8,12}) will work.)

For information on .Net regular expression syntax see:

<https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>

If changes are required to accommodate a different format, you have two options:

1. Send the data found above to BlackBerry AtHoc customer support with a request to have engineering determine the new regular expression.
2. Determine the regular expression yourself.

## Update the database

Once you have a good regular expression, update the database with it. Use the following SQL to update the database with the new regular expression. Replace 'new\_expression' with the new regular expression:

```
UPDATE GLB_CONFIG_TAB SET VALUE = 'new_expression' WHERE KEY_NAME =  
'ALT_HTTP_CAC_REGEX'
```

# Troubleshooting smart card authentication

If smart card authentication fails after it has been configured, it could be due to the format of the CN string in the certificate. BlackBerry AtHoc has three regular expressions for validating the mapping ID:

- HTTP\_CAC\_REGEX
- ALT\_HTTP\_CAC\_REGEX
- CAC\_SAN\_REGEX

These regular expressions are in the `ngaddata.glb_config_tab`. BlackBerry AtHoc attempts to parse the MID using HTTP\_CAC\_REGEX. If that fails, it attempts to parse the MID using ALT\_HTTP\_CAC\_REGEX. If that also fails, it attempts to parse the MID using CAC\_SAN\_REGEX.

Sometimes the certificate can be stripped from the header by a proxy server, which causes the validation to fail. In other cases, the regular expression could not parse the data. As a first step, verify that the certificate details are making it through to BlackBerry AtHoc. Use the Test Page described in [Appendix A: Retrieve certification information](#).

See the sample verbose log entry below, and note that the subject is missing.

If you are getting a 403 error that prevents the login page from displaying, deselect Require SSL in IIS. Otherwise, the call to GetCACMID is not made.

If the certificate information does not appear, it may be due to SSL settings in IIS, or due to a proxy removing the information from the request.

It is possible that the information from the certificate is available, but the certificate is not. Version 6.1.8.87 CP1 with CHF3 and later BlackBerry AtHoc releases have a new property, CAC\_CHECK\_PRESENT, which can be set to N to work around this issue. This setting is not exposed in the user interface.

Sample verbose log entry

```
<event>
<eventId>12445</eventId>
<type>VERBOSE</type>
<time>02/03/2015 15:36:53.350</time>
<server>DlASEPRIC090</server>
<categorySource>Management System</categorySource>
<assembly>MSDotNetClient.dll</assembly>
<module>AuthController</module>>
<member>GetCACMID</member>
<shortMessage> CAC: Issuer: SerialNumber: Subject: Valid From: 2/3/2015 3:36:53 PM
Valid Until: 2/3/2015 3:36:53 PM IsValid: True CertEncoding: 0 Cookie: Present:
False </shortMessage>
. . . .
```

# Appendix A: Retrieve certification information

You can retrieve certificate information using the following two methods:

- Use the test page in the management system
- Use a sample certificate

Use the test page in the management system

For BlackBerry AtHoc release 6.1.8.88 and later releases, the test page is located at:

<https://<server>/client/smartcard/info>

For BlackBerry AtHoc release 6.1.8.87 and earlier releases, the test page is located at:

<https://<server>/client/auth/ccd>

If this test URL does not work, enable verbose logging and search the BlackBerry AtHoc event log for the certificate details. Search for the AuthController module, or the GetCACMID member. Turn off verbose logging after finding the certificate details.

For BlackBerry AtHoc release 6.1.8.84 and earlier releases, check the `servervars.asp` file at:

<https://<server>servervars.asp>

## Use a sample certificate

Have the customer provide a sample of the certificate to determine if the regular expression can parse the MID. You may need to request several samples for comparison.

To open a customer's certificate, complete the following steps:

1. From the **Start Menu**, type **MMC** in the search area and hit **Enter**.
2. Once the MMC is open, click **FILE** and select **Add / Remove Snap-in**.
3. Select the Certificates Snap-in on the left hand side and click **Add**.
4. When prompted, select **My user account**.
5. Click **Finish**.
6. Click **OK** to close the menu and return to the main console page.
7. Find the user's Certificate and open it.
8. On the **Certificate** window, click the **Details** tab.
9. Ensure **Show:** is set to **<All>**.
10. Scroll down and select **Subject**. The MID is displayed in the field below. It is displayed beside the value for CN.
11. Copy the details or click **Copy to File....** The information in CN is used to determine the proper regular expression to use, which will write over the existing value in `glb_config_tab`.

Some customers with OnPrem systems use more than one type of smart card and will already use one of the regular expressions successfully. In this case, it is necessary to coordinate with the customer on which regex to update (CAC\_REGEX or ALT\_HTTP\_CAC\_REGEX) when you have a solution for the CAC/PIV with the issue.

Try to obtain three or four user certificates and compare them.

# BlackBerry AtHoc customer portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Portal:

<https://support.athoc.com/customer-support-portal.html>

The BlackBerry AtHoc Customer Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and users guides.

# Legal notice

©2019 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. 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 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  
200 Bath Road  
Slough, Berkshire SL1 3XE  
United Kingdom

Published in Canada