



BlackBerry Dynamics

Critical Issue Advisory

BlackBerry Dynamics Upcoming TLS Protocol and Cipher Changes

Contents

BlackBerry Dynamics Upcoming TLS Protocol and Cipher Changes.....4

Legal notice..... 8

BlackBerry Dynamics Upcoming TLS Protocol and Cipher Changes

Summary

BlackBerry will be making changes to the list of supported cipher suites for BlackBerry infrastructure connections on June 30, 2020. These cipher suite changes will impact the legacy Good Control server version 2.0.3.11 and earlier, and BlackBerry Dynamics SDK version 3.1 and earlier.

The impacted Good Control versions have been out of support since 2016; for more information refer to the [BlackBerry Software Lifecycle Overview](#) page. This is a courtesy reminder for any customers running these older, non-supported Good Control and BlackBerry Dynamics SDK versions to upgrade to a supported version or transition to BlackBerry UEM for continued support. For more information about the benefits of upgrading, refer to the [Benefits Guide](#).

BlackBerry Dynamics Supported Cipher Suites

Cipher Suites	BlackBerry Dynamics NOC	Dynamics SDK Infrastructure Connections	Dynamics SDK Application Connections
TLSv1.2	Yes	Yes	Yes
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	Yes	Yes	Yes
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	Yes	Yes	Yes
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)	No	Yes	Yes
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	No	Yes	Yes
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)	No	No	Yes
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	Yes	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	Yes	No	Yes
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)	No	No	Yes
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	No	No	Yes
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	No	No	Yes

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	Yes	Yes	Yes
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	Yes	No	Yes
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	No	No	Yes
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	Yes	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	Yes	No	Yes
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	No	No	Yes
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	No	No	Yes
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	No	No	Yes
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	No	No	Yes
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	No	No	Yes
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)	No	No	Yes
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)	No	No	Yes
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	No	No	Yes
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	No	No	Yes
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)	No	No	Yes
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)	No	No	Yes
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)	No	No	Yes
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)	No	No	Yes
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	Yes	No	No
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	Yes	No	No

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	Yes	No	No
TLSv1.1	No	No	Yes (Policy Controlled)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	No	No	Yes
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	No	No	Yes
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	No	No	Yes
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	No	No	Yes
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	No	No	Yes
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	No	No	Yes
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)	No	No	Yes
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)	No	No	Yes
TLSv1.0	No	No	Yes (Policy Controlled)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	No	No	Yes
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	No	No	Yes
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	No	No	Yes
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	No	No	Yes
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	No	No	Yes
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)	No	No	Yes
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)	No	No	Yes
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038) (Android only)	No	No	Yes

TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032) (Android only)	No	No	Yes
---	----	----	-----

Impact

- **Good Control 1.9 and Good Proxy 1.9 and earlier:** Good Control will no longer work due to loss of connectivity to the BlackBerry Infrastructure. Active containers will not be wiped but will no longer work. To restore functionality, customers must upgrade first to Good Control 2.0.3.11 and Good Proxy 2.0.3.7, and then to Good Control 2.2.511.26 and Good Proxy 2.2.511.16.
- **Good Control 2.0.3.11 and Good Proxy 2.0.3.7:** Good Control will no longer work due to loss of connectivity to the BlackBerry Infrastructure. Active containers will not be wiped but will no longer work. To restore functionality, customers must upgrade to Good Control 2.2.511.26 and Good Proxy 2.2.511.16.
- **BlackBerry Dynamics SDK versions 3.1 and earlier:** BlackBerry Dynamics SDK versions 3.1 and earlier will no longer compile. Ensure you are using BlackBerry Dynamics SDK version 3.4 and later.
- **Good Control 2.2.511.26 and Good Proxy 2.2.511.16 and later:** No impact.

Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE 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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada