Cb Protection (Bit9 Platform) 7.2.x Technical Bulletin: Changing Agent SSL/TLS Protocols

About this Bulletin

By default, Cb Protection (Bit9 Platform) is configured for SSL2, SSL3 and TLS 1.0. The procedure described here allows configuration of different SSL/TLS network communication protocols, including TLS versions 1.1 and 1.2, in Cb Protection (Bit9 Platform) 7.2.1 Patch 7 and later.

Important Information

Care must be taken when changing the SSL/TLS configuration on an agent system. If you configure the agent to use only TLS 1.2, then push that new flag setting down to the agent on a system that currently uses a weaker protocol. If TLS 1.2 is not available on the underlying network/OS settings for that machine, the agent will be disconnected from the server, and you will not be able to revert this setting from the server since the agent is now disconnected; in this case, the agent can be managed only via its own command line interface.

Using the procedures described here – reconfiguring some agents, verifying communications using the new protocol(s), and then rolling the changes out to the rest of the agents – helps avoid problems such as the one described above.

It is strongly recommended that you test this procedure on representative operating systems, protocols, and ciphers before switching an entire site to only strong TLS protocols.

Enabling Agents to Use TLS 1.1 and 1.2

Configure Representative Agents to use these protocols: SSL3, TLS 1.0, 1.1 and 1.2

1. Go to the agent configuration page using the URL:
   - https://*yourserver*/agent_config.php
2. Click the **Add agent config** button and add the following flag:
   - **Property name:** Winhttp protocol flags
   - **Host ID:** (0 for All agents or the host id of the individual agent)
     Note: Performing the procedure on one representative system for each OS, protocol, and cipher in your environment is recommended before applying this to all agents.
   - **Value:** winhttp_secure_protocol_flags=0xAA0 // 0xAA0 = SSLv3, TLS 1.0, 1.1 and 1.2. This is a combination flag that enables multiple protocols at the same time. See the table below for more details on flags.
   - **Status:** Enabled
3. Click **Save** and then allow time for the changed config list to propagate down to the agent(s). You can refresh the Computers page to compare the current server CL version to the version on each endpoint.

Verify that the change is applied to the agent

1. Launch an elevated cmd tool "as administrator".
2. In the command window, cd to the Bit9 install directory. The default is shown here:
   - `cd c:\Program Files (x86)\Bit9\Parity Agent`
3. Enter the agent management password for your site:
   - `dascli password`
   - Enter your agent management password when prompted.
4. Validate the communication protocol:
   - `dascli configprops filter *winhttp*`
     `// The default setting is 168 (0xA8) for SSLv2 SSLv3 and TLS 1.0`
5. Now gradually disable the weaker protocols at the operating system and network levels (consult with your OS and network support for these steps). Be sure these changes are fully tested and easily reversible.

   Success on one machine does not mean a change will work across an entire network. We recommend testing a new SSL/TLS setting on different endpoint configurations (especially older platforms and systems in different network segments) before rolling it out globally.
6. When you are satisfied that the procedure has been successful on all system types, repeat the configuration steps (previous page) on all systems.

SSL/TLS Protocol Flags

The table below explains how the flags are recognized:

Protocol	Hexadecimal Value	Enabled by default in v7.x	Enabled by default in v8.x	Supported OS
SSL 2.0*	0x8	Yes	No	All
SSL 3.0**	0x20	Yes	Yes	All
TLS 1.0	0x80	Yes	Yes	All
TLS 1.1	0x200	No	Yes	Windows 7+ Windows 2008R2+****
TLS 1.2***	0x800	No	Yes	Windows 7+ Windows 2008R2+****

Notes:
* If SSL 2.0 is specified, agents running Windows 7 and earlier will not be able to connect to a Cb Protection 8.0 Server running on Microsoft Server 2016 server without further configuration.
** SSL 3.0 has been deprecated and may not be supported by default in new Windows versions.
*** TLS 1.2 and SSL 2.0 are mutually exclusive. You cannot specify both at the same time.
**** For TLS 1.1/1.2 to work on Windows 7, you must update the operating system. The steps for this are described in the following knowledge base article:
https://support.microsoft.com/en-us/kb/3140245
For more information regarding these flags, you can visit:
https://msdn.microsoft.com/en-us/library/windows/desktop/aa384066(v=vs.85).aspx

Additional Notes

- If you find that certain protocols or ciphers are not working, refer to your network or OS vendor support to determine which of these are available and how to enable, disable or otherwise alter their settings.
- This solution only addresses how to configure the agent to select certain SSL/TLS protocols. Additional configuration may be needed on the server to accept the protocols configured on the agent. Please see the table above. Not all cipher suites will work across all versions of Windows. Depending on the server's configuration (i.e., its cipher suite order) it is possible that the cipher suite order will need to be adjusted as well.
- TestSSLServer is an easy-to-use, public troubleshooting tool that will report back available SSL/TLS protocols and their cipher suites from a remote server. It is located at:

  http://www.bolet.org/TestSSLServer/

  TestSSLServer requires that .NET2 or .NET4 be installed on the system being tested.

  This tool only reports on available remote protocols and it will not actually test the protocols.

Troubleshooting

If the agent is not connected to the Cb Protection (Bit9) server, the winhttp flag can be set using the following series of client management (dascli) commands:

- `dascli password <cli password>`
- `dascli configprops filter *winhttp*` // shows default value of 168 or 0xA8
- `dascli setconfigprop winhttp_secure_protocol_flags=0xAA0`
- `dascli configprops filter *winhttp*` // should show updated value 2720 or 0xAA0

Setting config properties via *dascli setconfigprops*, including *win_http_secure_protocols*, only lasts until the *parity.exe* process is restarted. If you restart the machine, or if the agent service is restarted for some other reason, the property reverts back to either the config property assigned by the server or its default value (if no server config was specified).

Also, a property change via the command line does not take effect immediately in version 7.x. After you set this property, you must log off and log back in (but don't reboot) before the new property becomes effective. (52062)