CARBON BLACK

ARM YOUR ENDPOINTS

Carbon Black Enterprise Protection Diagnostic File Transfer

February 2016

Introduction

Carbon Black Enterprise Protection has a feature called Diagnostic File Transfer. This feature simplifies the process of providing diagnostic data to Carbon Black support personnel during issue investigation. Prior to this feature, the process of generating and then sending diagnostic information was a manual and time-consuming process. Enabling Diagnostic File Transfers automates this process by giving Cb support personnel direct access to diagnostic files during issue investigation.

Data Collection

Diagnostic File Transfer provides Cb support personnel with access to data often requested when investigating product and performance issues. This data is comprised of the following:

1. Agent Diagnostic Files

   A Cb Enterprise Protection Administrator can initiate collection of agent diagnostic files from the console. These files are listed in the Cb Enterprise Protection console under *Tools -> Requested Files -> Diagnostic Files.* Cb personnel are **not** able to generate these files. Cb support personnel can then access these files to transfer for analysis.

   Log files are placed in the Bit9\Server\Support folder on the Cb Enterprise Protection server. Any additional files placed in this folder will also be accessible to Carbon Black.

2. Snapshot of the Cb Enterprise Protection Server Logs

   During issue investigation, Cb support personnel can initiate a snapshot and transfer of the following Cb Enterprise Protection server logs:

   - Server
   - Reporter
   - Console
   - Connector

3. Database expensive query trace (On Demand)

   This is used by Cb support personnel when working on support cases related to DB performance and allows them to initiate a timed trace of Expensive SQL Queries in the Cb Enterprise Protection DB.

NOTE: The data collected is no different than what is collected when support requests that you send it manually.

Actions Enabled

When the option for Diagnostic File Transfer is checked, it allows Cb Support personnel to:

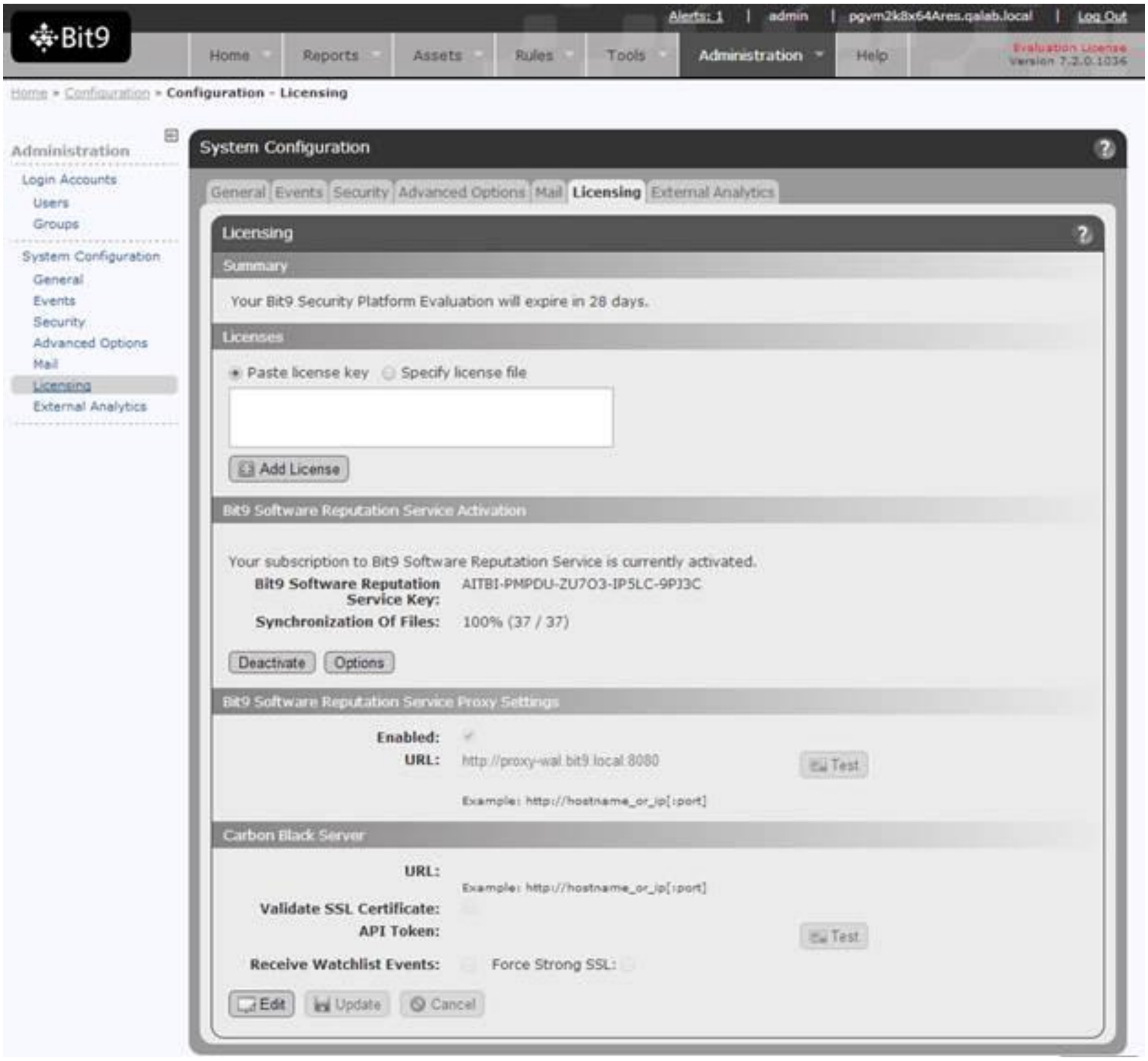
1. View and transfer files listed in the *Tools -> Requested Files -> Diagnostic Files* tab in the Cb Enterprise Protection console

2. Initiate a snapshot of the Bit9 Platform server logs (Server, Reporter, Console, Connector) and transfer the files

3. Initiate a timed trace of Expensive SQL Queries in the DB

How to enable Diagnostic File Uploads?

1. In the Console UI Go to *Administration -> System Configuration -> Licensing*



Your Bit9 Security Platform Evaluation will expire in 28 days.

● Paste license key ○ Specify license file

Your subscription to Bit9 Software Reputation Service is currently activated.

Bit9 Software Reputation Service Key: AITBI-PMPDU-ZU7O3-IP5LC-9PJ3C

Synchronization Of Files: 100% (37 / 37)

Enabled: ✓

URL: http://proxy-wal.bit9.local:8080

Example: http://hostname_or_ip[:port]

URL:

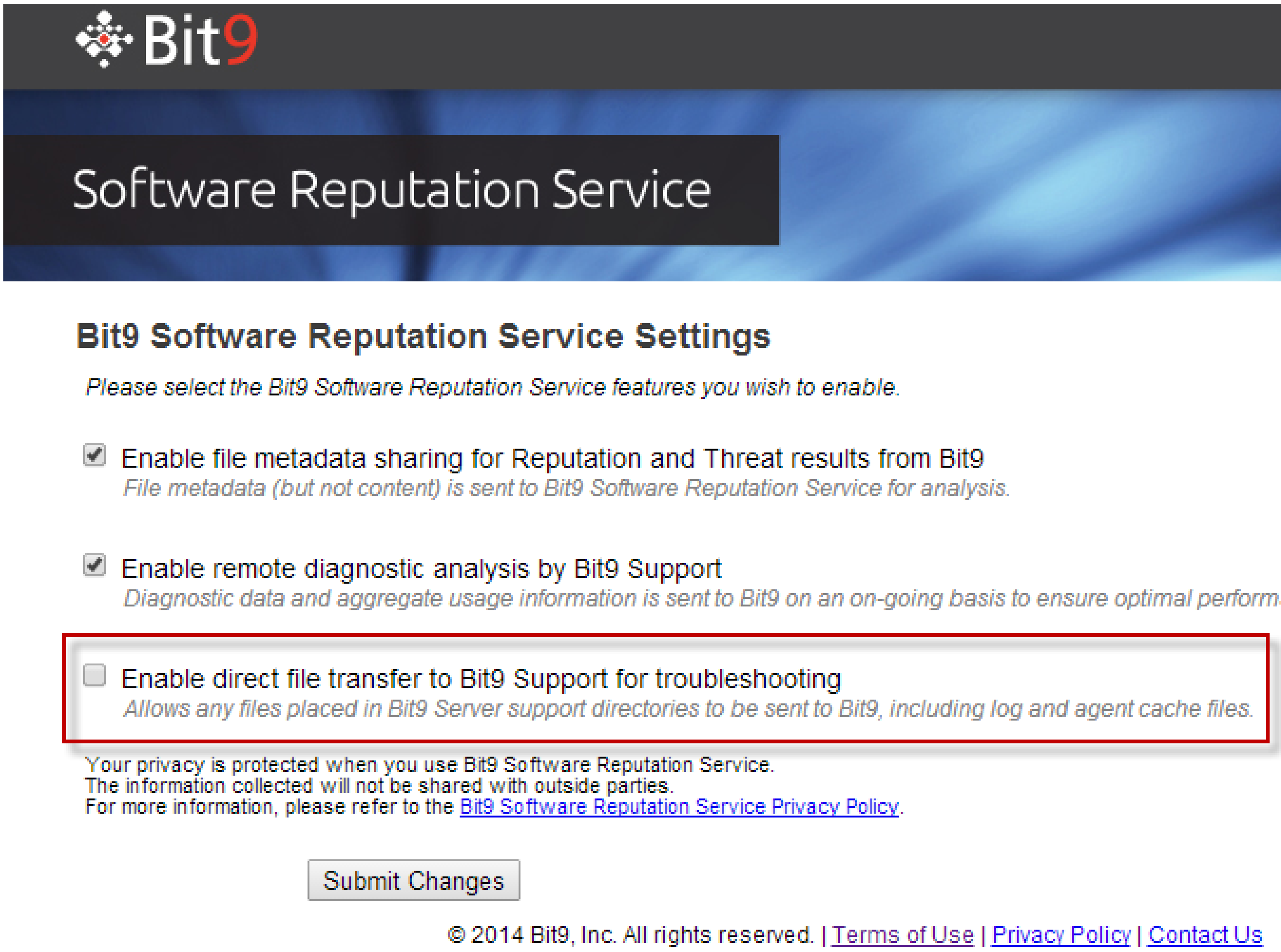
Example: http://hostname_or_ip[:port]

Validate SSL Certificate: □

API Token:

Receive Watchlist Events: □ Force Strong SSL: □

2. In the Bit9 Software Reputation Service Activation, section click on *Options*.



Software Reputation Service

Bit9 Software Reputation Service Settings

Please select the Bit9 Software Reputation Service features you wish to enable.

☑ Enable file metadata sharing for Reputation and Threat results from Bit9
File metadata (but not content) is sent to Bit9 Software Reputation Service for analysis.

☑ Enable remote diagnostic analysis by Bit9 Support
Diagnostic data and aggregate usage information is sent to Bit9 on an on-going basis to ensure optimal perform

□ Enable direct file transfer to Bit9 Support for troubleshooting
Allows any files placed in Bit9 Server support directories to be sent to Bit9, including log and agent cache files.

Your privacy is protected when you use Bit9 Software Reputation Service.
The information collected will not be shared with outside parties.
For more information, please refer to the Bit9 Software Reputation Service Privacy Policy.

© 2014 Bit9, Inc. All rights reserved. | Terms of Use | Privacy Policy | Contact Us

3. Click on *Enable direct file transfer to Bit9 Support for troubleshooting*.
4. Click *Submit Changes* button

Benefits

Why should you enable this feature?

- Minimize time involved to resolve support issues
- Reduce your workload if you need help from support