



Bit9 Security Platform Diagnostic File Transfer

December 2015

Introduction

The Bit9 Security Platform has a feature called Diagnostic File Transfer. This feature simplifies the process of providing diagnostic data to Bit9 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 Bit9 support personnel direct access to diagnostic files during issue investigation.

Data Collection

Diagnostic File Transfer provides Bit9 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 Bit9 Administrator can initiate collection of agent diagnostic files from the console. These files are listed in the Bit9 console under *Tools -> Requested Files -> Diagnostic Files*. Bit9 personnel are **not** able to generate these files. Bit9 support personnel can then access these files to transfer for analysis.

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

2. Snapshot of the Bit9 Platform Server Logs

During issue investigation, Bit9 support personnel can initiate a snapshot and transfer of the following Bit9 server logs:

- Server
- Reporter
- Console
- Connector

3. Database expensive query trace (On Demand)

This is used by Bit9 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 Bit9 DB.

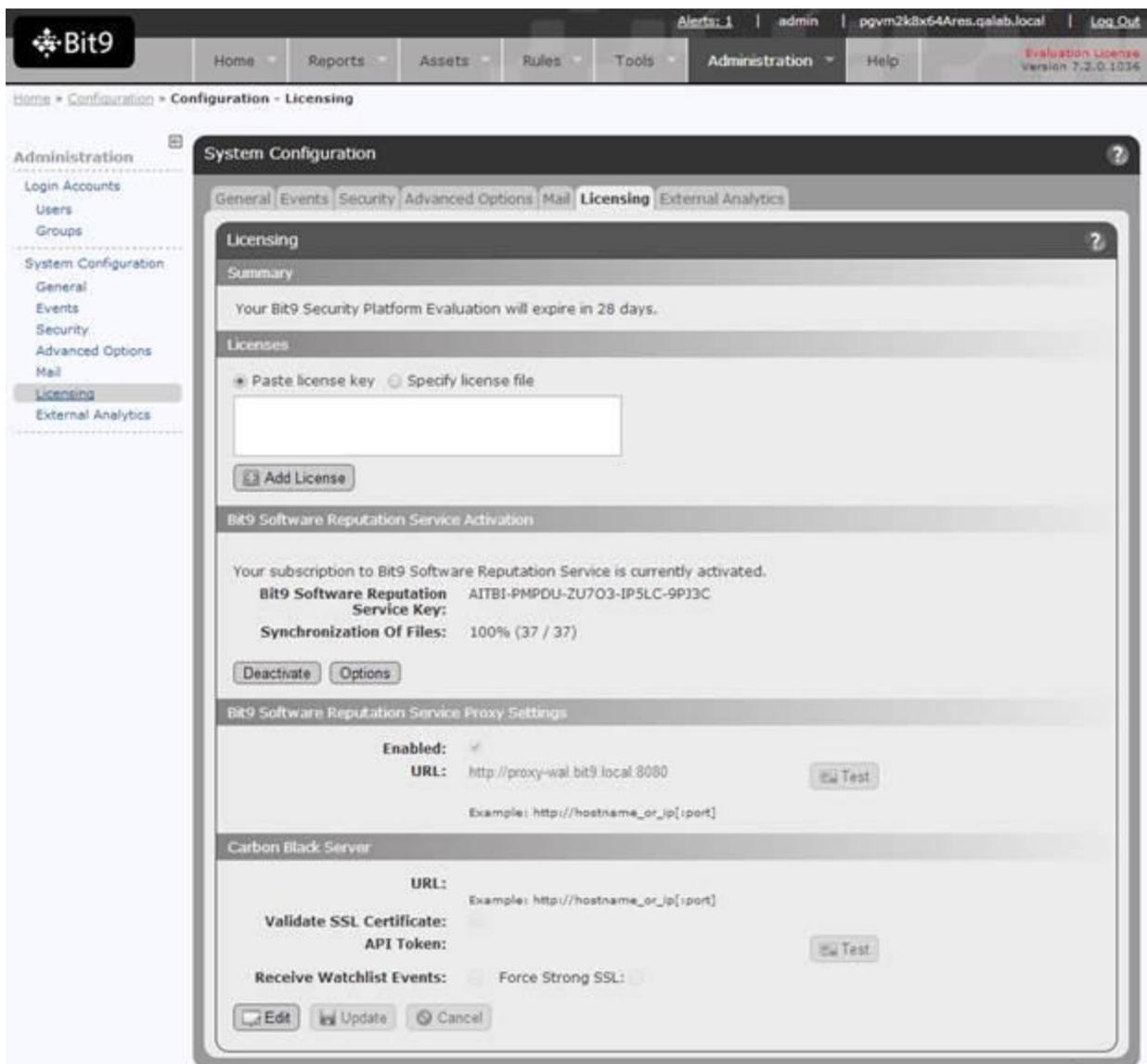
Actions Enabled

When the option for Diagnostic File Transfer is checked, it allows Bit9 Support personnel to:

1. View and transfer files listed in the *Tools -> Requested Files -> Diagnostic Files* tab in the Bit9 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*



The screenshot displays the Bit9 console interface. At the top, the Bit9 logo is on the left, and navigation links for Alerts, admin, pgvm2k8x64Ares.qalab.local, and Log Out are on the right. Below this is a main navigation bar with Home, Reports, Assets, Rules, Tools, Administration, and Help. The breadcrumb trail reads Home > Configuration > Configuration - Licensing. On the left, a sidebar menu shows Administration, Login Accounts, Users, Groups, System Configuration, General, Events, Security, Advanced Options, Mail, Licensing (highlighted), and External Analytics. The main content area is titled 'System Configuration' and has tabs for General, Events, Security, Advanced Options, Mail, Licensing, and External Analytics. The 'Licensing' tab is active, showing a 'Summary' section with the message: 'Your Bit9 Security Platform Evaluation will expire in 28 days.' Below this is a 'Licenses' section with radio buttons for 'Paste license key' (selected) and 'Specify license file', followed by a text input field and an 'Add License' button. The next section is 'Bit9 Software Reputation Service Activation', which states the subscription is currently activated. It shows the 'Bit9 Software Reputation Service Key' as AITBI-PMPDU-ZU7O3-IPSLC-9PJ3C and 'Synchronization Of Files' as 100% (37 / 37). There are 'Deactivate' and 'Options' buttons. The 'Bit9 Software Reputation Service Proxy Settings' section has 'Enabled' checked, a 'URL' field with the value http://proxy-wal.bit9.local:8080, and a 'Test' button. Below that is the 'Carbon Black Server' section with a 'URL' field, 'Validate SSL Certificate' and 'API Token' fields, and a 'Test' button. At the bottom, there are 'Edit', 'Update', and 'Cancel' buttons.

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 performance.

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](#).

Submit Changes

© 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