v14.4 Agent Release Notes

Contents

14.4 Data Protection Agent Release Notes. 3
- **Features Released with Agent v14.1. . . . . 4**
  - Patch 20 Additions. 5
- **Features Released with Agent v14.4. . . . . 6**
- **Database Support - Data Security Coverage Tool. 7**
- **SecureSphere Agent Installation Files. 9**
  - Note on Agent Package Numbers. 10
  - Determining Which non-Windows SecureSphere Agent Package to Install. 11
  - SecureSphere Agent Package Installation File Names. 13
  - Database and File Agent Packages Released with v14.1. 14
  - Database and File Agent Packages Released with v14.1 Patch 20. 19
  - Database and File Agent Packages Released with v14.4 Patch 10. 21
  - Database and File Agent Packages Released with v14.4 Patch 20. 23
- **Agent Installation Requirements. 24**
  - Agent Memory Requirements. 25
  - Agent Disk Space Requirements. 26
  - Platform Specific Notes for the SecureSphere Agent. 27
  - Special Considerations for Certain Linux Platforms. 28
  - SecureSphere Agents on Microsoft Windows. 29
  - SecureSphere Agents on Ubuntu. 30
- **Installing SecureSphere Agents. 31**
  - Installing and Upgrading SecureSphere Agents. 32
  - Required Permissions for Agent Installation/Configuration. 33
  - SecureSphere Agent Package. 34
  - Upgrading SecureSphere Agents. 35
  - After Installing the SecureSphere Agent. 37
  - AIX Post Installation Information. 38
  - Locally Caching Monitored Traffic. 39
- **Open Issues with Imperva Data Protection Agent - v14.4. . . . . 40**
- **Agent Patch Bug Fixes. 59**
  - Fixed Issues with Imperva Data Protection Agent - v14.1. 60
  - Fixed Issues with Imperva Data Protection Agent - v14.1 Patch 20. 62
  - Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 10. 63
  - Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 20. 66

Proprietary Rights Notice. 68

Welcome to the Data Protection Agent Release Notes. What would you like to read about:

- Features Released with Agent v14.1
- Features Released with Agent v14.4
- Database Support - Data Security Coverage Tool
- SecureSphere Agent Installation Files
- Agent Installation Requirements
- Installing SecureSphere Agents
- Open Issues with Imperva Data Protection Agent - v14.4
- Agent Patch Bug Fixes

74863 14.4 Data Protection Agent Release Notes Last modified: 6/24/2020 9:54:43 AM

Features Released with Agent v14.1

Agents for Data Protection (formerly SecureSphere) now support the following:

- **Kernel System Capping**: Data Protection Agents now allow users to define CPU capping for the entire system or for the Kernel. Capping will occur when the indicated item (system or Kernel) hits the designated threshold
- **Oracle v12.2 Sharding**: Data Protection Agents now support Oracle v12.2 Sharding, supporting the use of a pool of databases that don't share hardware or software but are presented as a single entity
- **Oracle User Space Agents for SUSE v12**: Data Protection Agents now support Oracle Databases operating in the SUSE v12 user space. This significantly reduces the need to upgrade agents when the underlying operating system's kernel is updated and creates a more stable operating environment
- **MS SQL Server Advanced Mode Blocking**: Data Protection Agents now support blocking for MS SQL Servers operating with Advanced-Mode encryption while the agent is in sniffing mode
- **Oracle Enterprise Linux (OEL) 6**: Data Protection Big Data Agents now support Oracle Enterprise Linux (OEL) 6 Operating System
- **Solaris 11.4**: Data Protection Agents now support the Solaris 11.4 Operating System
- **Data Security Coverage Tool:** Imperva's new interactive coverage tool allows you to view every certified combination of database and operating system supported by Imperva's Data Security suite. The tool provides the required Agent version, and also the supporting versions of the Management Server, Gateway, Data Risk Analytics and the underlying platforms on which they can be deployed, On-Premises or in the cloud. This allows planning in advance operational activities including database and OS upgrades, while making sure databases stays both secure and compliant to the various applicable regulations. The tool is available at https://www.imperva.com/data-security-coverage-tool/

Coverage: Data Protection Agents can now be used on the following databases:

- Maria DB 10.3
- Cloudera 6.1
- Hortonworks 3.0 - 3.1
- DataStax Cassandra 6.7

72407 Features Released with Agent v14.1 Last modified: 6/17/2020 11:21:23 AM

Patch 20 Additions

- **MySQL, PostgreSQL and MariaDB User Space**: Data Protection Agents now support MySQL, PostgreSQL and MariaDB databases operating in the SUSE v12 and OEL-7-UEK user spaces
- **Oracle User Space Agents for OEL-6-UEK and OEL-7-UEK**: Data Protection Agents now support Oracle databases operating in the OEL-6-UEK and OEL-7-UEK user spaces

73344 Patch 20 Additions Last modified: 5/19/2019 1:56:52 PM

Features Released with Agent v14.4

Coverage: Data Protection Agents can now be used on the following databases:

- MSSQL 2019 (on Windows and Linux)
- MongoDB 4.2
- Cloudera CDH 6.3

SUSE Enterprise Linux Server 15 SPS 0,1: Data Protection Agents for Database now support SUSE Enterprise Linux Server 15 with Service Packs 0 and 1

RHEL 8, Centos 8 and OEL 8: Data Protection Agents for Database now support RHEL 8, Centos 8 and OEL 8

75835 Features Released with Agent v14.4 Last modified: 6/17/2020 12:22:18 PM

Database Support - Data Security Coverage Tool

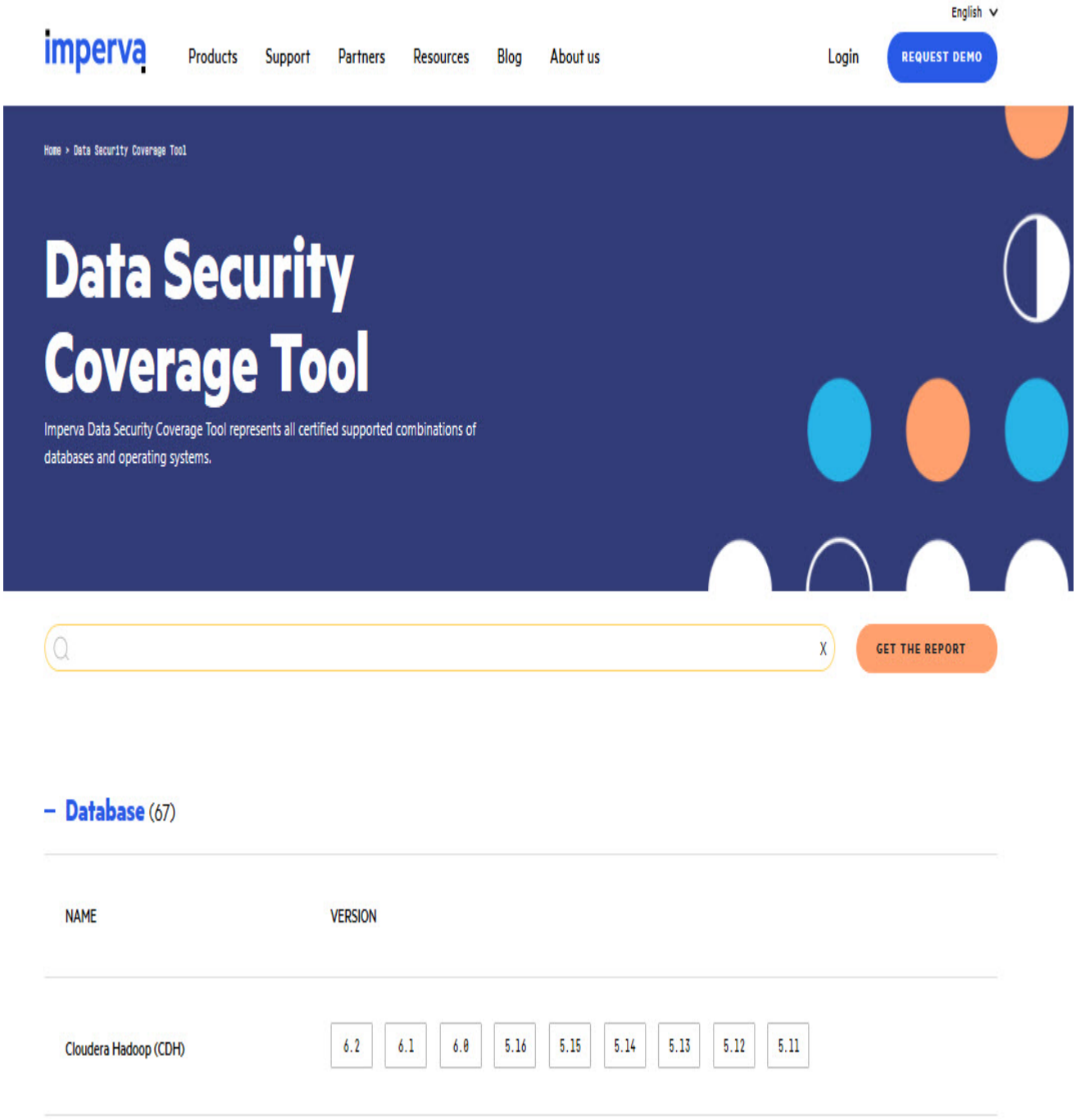
Imperva database coverage is now available through the Imperva **Data Security Coverage Tool**, a dynamic intuitive and easy to use interface that helps you identify coverage requirements for your agent deployment.

See the tool at https://www.imperva.com/data-security-coverage-tool/

Using the tool is simple:

- Click an item, for example Database Cloudera Hadoop (CDH) 6.2; all supported environment variables become highlighted
- Scroll down the page to see those variables such as Agent version, MX and Gateway version, supported hypervisor and cloud platforms, etc.

Note: The Data Security Coverage Tool is replacing the database and OS coverage tables in the Release Notes, those tables are no longer available.



74910 Database Support - Data Security Coverage Tool Last modified: 4/5/2020 2:34:11 PM

SecureSphere Agent Installation Files

This section reviews topics related to the SecureSphere Agent installation files and includes the following:

- Note on Agent Package Numbers
- Determining Which non-Windows SecureSphere Agent Package to Install
- SecureSphere Agent Package Installation File Names

59039 SecureSphere Agent Installation Files Last modified: 1/27/2019 4:34:32 PM

Note on Agent Package Numbers

Starting with v13.0, Agent version build numbers (all digits that appear in the last part of the version string) are composed of six numbers, they were previously composed of four numbers. This change has no impact on operation.

72419 Note on Agent Package Numbers Last modified: 3/17/2019 2:22:45 PM

Determining Which non-Windows SecureSphere Agent Package to Install

Note: This section is not relevant to Windows SecureSphere Agents, because there is only one installation package for all supported versions of Windows.

To determine which non-Windows SecureSphere Agent package to download and install, see SecureSphere Agent Package.

Alternatively, you can use the **which_ragent_package_xxxx.sh** script (where **xxxx** is the version number of the script) which you can download from the Imperva FTP site at **/Downloads/SecureSphere_Agents/Misc/**

The script should be run on the database server and takes a single parameter, the SecureSphere Agent version number you want to install.

Table 1 which_ragent_package_xxxx.sh Parameters

Parameter	Description
-v	The SecureSphere Agent version number you want to install.

For example:

```
[root@agents-system tmp]# ./which_ragent_package_[version].sh -v 14.4
```

This means that you want the script to return the name of the SecureSphere Agent version **14.4** package for the platform on which the script is run.

The script returns the OS, OS version, platform, kernel version and the name of the SecureSphere Agent package you should download and install.

The following is an example of the output. Real output will reflect the current version.

```
[root@prod-rhel6-64-smp ~]# ./which_ragent_package_0157.sh -v 13.0

OS: RHEL

Version: 6
```

```
Platform: x86_64

Kernel: SMP

Latest DAM Agent package is: Imperva-ragent-RHEL-v6-kSMP-px86_64-
b13.3.0.10.0.551148.tar.gz

Latest Big Data Agent package is: Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-
b13.3.0.10.0.551148.tar.gz

The above is a recommendation only. It is not a guarantee of agent support.

For an official list of agent packages and their supported platforms, please see
the latest SecureSphere Agent Release Notes.

*** Please verify that you run the latest version of which_ragent_package
available at https://ftp-us.imperva.com ***
```

Notes:

- For servers that can host both regular and Big Data Agents, output includes the requisite package for both scenarios, as seen in the above example.
- Always download the latest version of the **which_ragent_package_xxxx.sh** before using it, otherwise it may point you to an out-of-date Imperva Agent package.
- Before downloading the Imperva Agent package, verify that the script has correctly identified your OS, OS version, platform and kernel version.

75798 Determining Which non-Windows SecureSphere Agent Package to Install Last modified: 6/1/2020 10:26:01 PM

SecureSphere Agent Package Installation File Names

The installation package is used to install the SecureSphere Agent.

- For a list of standard agents for Database, File ,and SharePoint , see:
  - Database and File Agent Packages Released with v14.1
  - Database and File Agent Packages Released with v14.1 Patch 20

The SecureSphere Agent's build number is embedded in the name of the installation file.

Notes:

- The SecureSphere Agent for DB2 z/OS installation files and procedure are given in the **Imperva Administration Guide**.
- Other SecureSphere Agents are available in this release only for the OS Versions listed in the table below.

For minimum SecureSphere Agent disk space and memory requirements, see Agent Installation Requirements. Once the SecureSphere Agent begins to monitor traffic, it requires additional memory and disk space, depending on the volume of monitored traffic. For additional information, see the "SecureSphere Agents" chapter in the relevant product's **User Guide**, under the **Advanced Configuration** section of the **Settings** tab.

72421 SecureSphere Agent Package Installation File Names Last modified: 5/2/2019 9:00:02 AM

Database and File Agent Packages Released with v14.1

OS / Version	Installation File Name
Note: All platforms listed below additionally support patches installed on the listed versions.	
Unix-based Agents	
AIX	
AIX 7.1 64-bit	Imperva-ragent-AIX-v71-ppowerpc64-b14.1.0.10.0
AIX 7.2 64-bit	Imperva-ragent-AIX-v72-ppowerpc64-b14.1.0.10.0
HP-UX	
HP-UX B11.31 Itanium	Imperva-ragent-HPUX-v11.31-pia64-b14.1.0.10.0.5
HP-UX B11.31 PA-RISC	Imperva-ragent-HPUX-v11.31-phppa-b14.1.0.10.0.
OEL	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
OEL 5 UEK 1 64-bit (2.6.32-100.26.2)	Imperva-ragent-OEL-v5-kUEK-v1-ik1-px86_64-b14
OEL 5 UEK 1 64-bit (2.6.32-300.7.1 to 2.6.32-300.39.2)	Imperva-ragent-OEL-v5-kUEK-v1-ik2-px86_64-b14

OS / Version	Installation File Name
OEL 5 UEK 1 64-bit (2.6.32-400.21.1)	Imperva-ragent-OEL-v5-kUEK-v1-ik3-px86_64-b14
OEL 5 UEK 1 64-bit (2.6.32-400.23 to the latest version of 2.6.32-400 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v5-kUEK-v1-ik4-px86_64-b14
OEL 5 UEK 2 64-bit (2.6.39-400.17.1 to the latest version of 2.6.39-400 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v5-kUEK-v2-px86_64-b14.1.0.
OEL 6 UEK 2 64-bit (2.6.39-400.17.1 to the latest version of 2.6.39-400 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v2-px86_64-b14.1.0.
OEL 6 UEK 3 64-bit (3.8.13-16 to the latest version of 3.8.13 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v3-px86_64-b14.1.0.
OEL 6 UEK 4 64-bit (4.1.12-32.1.2 to the latest version of 4.1.12 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v4-px86_64-b14.1.0.
OEL 6 64-bit BigData	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.1.0.10.0.562096.tar.gz
OEL 7 UEK 3 64-bit (3.8.13-35.3.1 to the latest version of 3.8.13 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v7-kUEK-v3-px86_64-b14.1.0.
OEL 7 UEK 4 64-bit (4.1.12-32.1.2 to the latest version of 4.1.12 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v7-kUEK-v4-px86_64-b14.1.0.
Red Hat (includes Oracle Linux and CentOS)	
RHEL 5 32-bit PAE	Imperva-ragent-RHEL-v5-kPAE-pi386-b14.1.0.10.0.

OS / Version	Installation File Name
RHEL 5 32-bit SMP	Imperva-ragent-RHEL-v5-kSMP-pi386-b14.1.0.10.0
RHEL 5 64-bit SMP	Imperva-ragent-RHEL-v5-kSMP-px86_64-b14.1.0.1
RHEL 5 64-bit XEN	Imperva-ragent-RHEL-v5-kXEN-px86_64-b14.1.0.1
RHEL 6 32-bit SMP	Imperva-ragent-RHEL-v6-kSMP-pi386-b14.1.0.10.0
RHEL 6 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.1.0.10.0.562096.tar.gz
RHEL 6 64-bit SMP	Imperva-ragent-RHEL-v6-kSMP-px86_64-b14.1.0.1
RHEL 7 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v7-kSMP-px86_64-b14.1.0.10.0.562096.tar.gz
RHEL 7 64-bit SMP	Imperva-ragent-RHEL-v7-kSMP-px86_64-b14.1.0.1
Solaris	
Sun 5.10 SPARC	Imperva-ragent-SunOS-v5.10-psparcv9-b14.1.0.10
Sun 5.10 x86 64-bit	Imperva-ragent-SunOS-v5.10-px86_64-b14.1.0.10.
Sun 5.11 SPARC	Imperva-ragent-SunOS-v5.11-psparcv9-b14.1.0.10
Sun 5.11 x86 64-bit	Imperva-ragent-SunOS-v5.11-px86_64-b14.1.0.10.

OS / Version	Installation File Name
SUSE	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
SUSE 10 64bit SP3 for Teradata (2.6.16.60-0.91.TDC.1.R.0 to 2.6.16.60-0.9999.TDC.1.R.0)	Imperva-ragent-TD-SLE-v10SP3-kTD-px86_64-b14 **Note**: Due to technical issues. This package was re new package for this version will be released in an
SUSE 11 64-bit SP4	Imperva-ragent-SLE-v11SP4-kSMP-px86_64-b14.1
SUSE 11 64bit SP1 for Teradata (2.6.32.54-0.23.TDC.1.R.2)	This agent is not available in v14.1.
SUSE 11 64bit SP1 for Teradata (2.6.32.54-0.35.TDC.1.R.1 to 2.6.32.54-0.9999.TDC.1.R.1)	This agent is not available in v14.1.
SUSE 11 64bit SP3 for Teradata (3.0.101-0.101.TDC.1.R.0 to 3.0.101-0.9999.TDC.1.R.0)	Imperva-ragent-TD-SLE-v11SP3-kTD-px86_64-b14 **Note**: Due to technical issues. This package was re new package for this version will be released in an
SUSE 12 64-bit SP2	Imperva-ragent-SLE-v12SP2-kSMP-px86_64-b14.1
SUSE 12 64-bit SP3	Imperva-ragent-SLE-v12SP3-kSMP-px86_64-b14.1
Ubuntu	
Ubuntu 14.04 (4.2.0-27 and 4.4.0-34 and 4.4.0-112)	Imperva-ragent-UBN-v14-kUBN-px86_64-b14.1.0.1

OS / Version	Installation File Name
Ubuntu 16.04+	Imperva-ragent-UBN-px86_64-b14.1.0.10.0.562096
Windows-based Agents	
For more information on Windows platforms that are supported by the Imperva agent, see the **Imperva on-Premises Release Notes**.	
Windows	Imperva-ragent-Windows-b14.1.0.10.0.562097.zip

73052 Database and File Agent Packages Released with v14.1 Last modified: 7/22/2019 8:32:11 AM

Database and File Agent Packages Released with v14.1 Patch 20

OS / Version	Installation File Name
Note: All platforms listed below additionally support patches installed on the listed versions.	
Unix-based Agents	
OEL	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
OEL 6 UEK 2 64-bit (2.6.39-400.17.1 to the latest version of 2.6.39-400 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v2-px86_64-b14.1.0.
OEL 6 UEK 3 64-bit (3.8.13-16 to the latest version of 3.8.13 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v3-px86_64-b14.1.0.
OEL 6 UEK 4 64-bit (4.1.12-32.1.2 to the latest version of 4.1.12 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v6-kUEK-v4-px86_64-b14.1.0.
OEL 7 UEK 3 64-bit (3.8.13-35.3.1 to the latest version of 3.8.13 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v7-kUEK-v3-px86_64-b14.1.0.
OEL 7 UEK 4 64-bit (4.1.12-32.1.2 to the latest version of 4.1.12 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v7-kUEK-v4-px86_64-b14.1.0.
OEL 6 64-bit BigData	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.1.0.20.0.569078.tar.gz
Red Hat (includes Oracle Linux and CentOS)	

OS / Version	Installation File Name
RHEL 6 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.1.0.20.0.569078.tar.gz
RHEL 7 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v7-kSMP-px86_64-b14.1.0.20.0.569078.tar.gz
SUSE	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
SUSE 12 64-bit SP2	Imperva-ragent-SLE-v12SP2-kSMP-px86_64-b14.1
SUSE 12 64-bit SP3	Imperva-ragent-SLE-v12SP3-kSMP-px86_64-b14.1

73329 Database and File Agent Packages Released with v14.1 Patch 20 Last modified: 7/22/2019 9:51:46 AM

Database and File Agent Packages Released with v14.4 Patch 10

OS / Version	Installation File Name
Note: All platforms listed below additionally support patches installed on the listed versions.	
Unix-based Agents	
Red Hat (includes Oracle Linux and CentOS)	
RHEL 6 64-bit SMP BigData (4.1.12-32.1.2 to 4.1.12)	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.4.0.10.0.589966.tar.gz
RHEL 7 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v7-kSMP-px86_64-b14.4.0.10.0.589966.tar.gz
RHEL 8 64-bit SMP	Imperva-ragent-RHEL-v8-kSMP-px86_64-b14.4.0.10.0.589965.tar.gz
SUSE	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
SUSE 12 64-bit	Imperva-ragent-SLE-v12-kSMP-px86_64-b14.4.0.10.0.589965.tar.gz
SUSE 15 64-bit	Imperva-ragent-SLE-v15-kSMP-px86_64-b14.4.0.10.0.589965.tar.gz
Windows-based Agents	

Windows	**Note**: This version of the Windows-based agent does not support FAM. Imperva-ragent-Windows-b14.4.0.10.0.590285.zip

75946 Database and File Agent Packages Released with v14.4 Patch 10 Last modified: 8/17/2020 10:26:09 AM

Database and File Agent Packages Released with v14.4 Patch 20

OS / Version	Installation File Name
Note: All platforms listed below additionally support patches installed on the listed versions.	
Unix-based Agents	
OEL	
Note: These agents require downloading both the installation file listed here and the kabi_<n>.txt file. For more information, see Special Considerations for Certain Linux Platforms.	
OEL 7 UEK 6 64-bit (5.4.17-2011.2.2 to the latest version of 5.4.17 UEK kernel series supported by Oracle)	Imperva-ragent-OEL-v7-kUEK-v6-px86_64-b14.4.0.20.0.596369.tar.gz
Red Hat (includes Oracle Linux and CentOS)	
RHEL 6 64-bit SMP BigData (3.8.13-16 to 3.8.13)	Imperva-ragent-bigdata-RHEL-v6-kSMP-px86_64-b14.4.0.20.0.596391.tar.gz
RHEL 7 64-bit SMP BigData	Imperva-ragent-bigdata-RHEL-v7-kSMP-px86_64-b14.4.0.20.0.596391.tar.gz
Windows-based Agents	
Windows	Imperva-ragent-Windows-b14.4.0.20.0.596392.zip

76153 Database and File Agent Packages Released with v14.4 Patch 20 Last modified: 8/20/2020 9:02:38 AM

Agent Installation Requirements

This section reviews SecureSphere Agent installation requirements, including the following:

- Agent Memory Requirements
- Agent Disk Space Requirements
- Platform Specific Notes for the SecureSphere Agent

59035 Agent Installation Requirements Last modified: 12/19/2016 3:39:42 PM

Agent Memory Requirements

The SecureSphere Agent requires memory for operation based on different factors. The following lists the amount of memory that is required for operation based on the number of CPU cores:

Name	Windows	Linux/Unix
1-32 cores	300MB	360MB
32-128 cores	500MB	660MB
>128 cores	2GB	2GB

66114 Agent Memory Requirements Last modified: 1/31/2018 3:39:45 PM

Agent Disk Space Requirements

The SecureSphere Agent uses up to 500 MB of database server disk space for its normal operation, logging, storing configuration, and more. In addition, to ensure audit information is preserved in the event of network problems, the SecureSphere Agent reserves 8 GB of database server disk space by default. You can change the amount of disk space being reserved, as well as the location where this information is saved. For information on how to change this value, see the article **Agents - Modifying the PCAP quota created on the Database** in the Imperva Customer Portal.

Diskspace Requirements

Operation	AIX	Solaris	HPUX	Linux	Windows
Normal operation, logging, storing configuration, and more (Installation folder)	500 MB	500 MB	500 MB	500 MB	500 MB
Ensure audit information is preserved in the event of network problems	8 GB	8 GB	8 GB	8 GB	8 GB
Required when Upgrading Agents*	750 MB	1500 MB	1250 MB	250 MB	300 MB

*Disk space allocation used when upgrading is divided between the tmp folder and Agent folder. For more information see the following article titled **What is the minimum disk space requirement to install the agent** in the Imperva Customer Portal**.**

67118 Agent Disk Space Requirements Last modified: 3/10/2019 2:42:41 PM

Platform Specific Notes for the SecureSphere Agent

This section reviews platform specific information for SecureSphere Agents.

Note: The topics in this section explicitly related to standard SecureSphere Agents, they are not relevant for SecureSphere Agent for Big Data.

This section reviews the following:

- Special Considerations for Certain Linux Platforms
- SecureSphere Agents on Microsoft Windows
- SecureSphere Agents on Ubuntu

70853 Platform Specific Notes for the SecureSphere Agent Last modified: 3/10/2019 2:36:07 PM

Special Considerations for Certain Linux Platforms

Some Linux platforms maintain several versions of their OS, and service packs for each version. Additionally, **SUSE**, **Teradata**, and **OEL UEK**, periodically release updates to service packs, which sometimes include updated versions of the kernel.

As such, there are a number of items that should be taken into account and understood before installing Imperva Data Security Agents on these Operating Systems. For more information, see topics in the **Agent Installation** chapter of the **Imperva Administration Guide** that discuss special considerations.

72410 Special Considerations for Certain Linux Platforms Last modified: 3/17/2019 2:22:48 PM

SecureSphere Agents on Microsoft Windows

When working with the SecureSphere Agent on Microsoft Windows 2008 and newer, Base Filtering Engine (BFE) service must be enabled on the database server. For more information, see Microsoft Windows documentation.

72415 SecureSphere Agents on Microsoft Windows Last modified: 3/17/2019 2:22:46 PM

SecureSphere Agents on Ubuntu

Please note the following considerations for the SecureSphere Agent when installed on Ubuntu:

- The installation folder for the SecureSphere Agent on Ubuntu is **/usr/imperva** and cannot be modified.
- Databases that support the SecureSphere Agent on Ubuntu include Postgre SQL and MySQL.

63095 SecureSphere Agents on Ubuntu Last modified: 7/12/2017 9:15:13 AM

Installing SecureSphere Agents

This section reviews topics related to the installing of SecureSphere Agents and includes the following:

- Installing and Upgrading SecureSphere Agents
- Required Permissions for Agent Installation/Configuration
- SecureSphere Agent Package
- Upgrading SecureSphere Agents
- After Installing the SecureSphere Agent

59029 Installing SecureSphere Agents Last modified: 1/27/2019 4:32:31 PM

Installing and Upgrading SecureSphere Agents

Before downloading the SecureSphere Agent installation file(s), please read carefully the "Installing SecureSphere Agents" chapter in the **Imperva Administration Guide**.

Note: In Unix and Unix-like systems, the **bash** shell must be available before installing the SecureSphere Agent.

72408 Installing and Upgrading SecureSphere Agents Last modified: 3/17/2019 2:22:48 PM

Required Permissions for Agent Installation/Configuration

To install and configure agents, you require administrator privileges. To run with administrator privileges:

- **In Windows:** Open the Windows **Start** Menu, search for '**cmd,**' then right-click **cmd.exe** and select "**Run as administrator**." In command window, navigate to location of installation package and run as required.
- **In Unix/Linux**: Run as root user (uid=0)

59031 Required Permissions for Agent Installation/Configuration Last modified: 12/19/2016 3:39:40 PM

SecureSphere Agent Package

Imperva supports downloading and deploying agents from the Software Updates screen in the Management Server GUI. The agent is provided as a compressed file (.tar.gz for Unix, .zip for Windows), which includes a number of other files.

The content of the compressed file include:

- An installation file for the SecureSphere Agent. This file is a .bsx for Unix or .msi for Windows and its name contains the string ragent.
- An installation file for the SecureSphere Agent Installation Manager. This file is a .bsx for Unix or .msi for Windows and its name contains the string ragentinstaller.
- An installation batch file (install.sh). This file is only part of the Unix installation package. It is not included with the Windows installation package.
- A readme file.
- A file with the suffix "metadata" which is used by the agent installation manager.

59032 SecureSphere Agent Package Last modified: 12/19/2016 3:39:39 PM

Upgrading SecureSphere Agents

Note: For information on upgrading SecureSphere Agent via Software Update see the Administration Guide.

To manually upgrade the SecureSphere Agent, you simply install it.

Notes:

- In both Windows and Unix, there is no need to re-register an upgraded SecureSphere Agent.
- When upgrading SecureSphere Agent's for AIX, you need to restart the database after agent upgrade is complete.
- When installing or upgrading the SecureSphere Agent for SharePoint, the web frontend servers may become unavailable for a several minutes.
- When upgrading the SecureSphere Agent to v13.0, EIK is enabled by default. You can disable it by setting **<external-traffic-monitoring-in-kern>** to **false** under Agent Advanced Configuration. For more information see the topic **Monitoring External Traffic Using PCAP and EIK** in the Database Security User Guide.

To upgrade a Unix Agent to v14.4:

1. Download the new agent package.
   - To determine what installation package you need to download, see Determining Which non-Windows SecureSphere Agent Package to Install
   - For a list of available agent package file names, see SecureSphere Agent Package Installation File Names
2. Untar (uncompress) the agent package as follows:

   cd <folder>

   gunzip <filename>.tar.gz | xargs tar xvf <agent-tar-filename>

3. Install the new SecureSphere Agent using the following upgrade parameters:

   ./install.sh

Note: If installing on SUSE or UEK for the first time you need to add the following to the above command

```
-k kabi_<n>.txt
```

For more information on using this command see the **Imperva Admin Guide**.

To upgrade a Windows agent to v14.4:

1. Download and unzip the new agent package file (.zip).
2. Double-click the file named **Imperva-ragent-Windows-<fileversion>.msi,** the agent is upgraded.
3. Install the installation manager: Double-click the file named **Imperva-ragentinstaller-Windows-<fileversion>.msi**, the agent installation manager is installed. Note: this step is only relevant when installing with a management server version 10.5 or newer.

66344 Upgrading SecureSphere Agents Last modified: 1/13/2018 5:39:00 PM

After Installing the SecureSphere Agent

The following topics review important post installation information for the SecureSphere Agent:

- AIX Post Installation Information
- Locally Caching Monitored Traffic

59045 After Installing the SecureSphere Agent Last modified: 12/19/2016 3:39:41 PM

AIX Post Installation Information

- You must restart the database server after the first time you start the Imperva Agent
- If you want to enable the source IP address feature, you must restart the login servers (SSH, Telnet, Rlogin) after the first time you start the Agent
- There is no need to reboot the machine

76073 AIX Post Installation Information Last modified: 7/23/2020 8:34:16 AM

Locally Caching Monitored Traffic

When the SecureSphere Agent is unable to send database traffic to the Gateway (for example, if the communication link to the Gateway is down) it stores the data to disk until such time as the data can be sent to the Gateway. Parameters controlling the location and size of these disk files can be configured in the **Advanced Configuration** section of the SecureSphere Agent's **Settings** tab. For more information, see the relevant product's **User Guide**.

72423 Locally Caching Monitored Traffic Last modified: 3/17/2019 2:22:47 PM

Open Issues with Imperva Data Protection Agent - v14.4

ID	Agent OS	Agent DB/ Product	Description
AGNT-10788	AIX	All Databases	On AIX, in order to audit correctly the remote user of local connections, processes which handle remote login (such as sshd and telnet) must be restarted after the agent installation.
AGNT-6537	AIX	All Databases	When working in PCAP mode on TCP external, when all channels are removed from a specific interface, the agent process is restarted.
AGNT-7542	AIX	All Databases	'User name' is not part of the process argument, and therefore cannot be excluded as part of the 'argument' in the process details criteria. Workaround: use the 'user name' field instead of the 'process argument' field.
AGNT-7249	AIX	Informix	When monitoring Informix SHM, audit data may be missing for large responses.
AGNT-7513	AIX	Informix	In AIX 7.1, in rare cases, when monitoring Informix SHM large responses, part of the response is missing in the audit.
AGNT-9115	AIX	Informix	Traffic might not be audited for local connections for Informix v10.
AGNT-10796	AIX	Oracle	When Oracle DB is configured in 'shared mode' there is no audit.
AGNT-11278	AIX	Oracle	The Exclude operation doesn't work with agent and gateway combined criteria with BEQ connections.
AGNT-11539	AIX	Oracle	Watchdog/InjectionManager/crashes counter might increase due to early wakeup of Injection manager.
AGNT-11973	AIX	Oracle	In rare cases there is no audit in open mode ASO connections.

ID	Agent OS	Agent DB/ Product	Description
AGNT-8223	AIX	Oracle	Audit loss of up to 0.3% of the traffic was encountered.
AGNT-8446	AIX	Oracle	Limitation: ASO is not supported on AIX WPAR.
AGNT-9353	AIX	Oracle	Open mode ASO connections are not being monitored after Agent upgrade or after uninstalling and then installing a different Agent version.
AGNT-9801	AIX	Oracle	Only 126 ASO connections out of 200 that are opened concurrently are monitored.
AGNT-10234	AIX, Linux, Solaris	Oracle	If ASO interception is disabled in the Agent, and there are ASO connections in the Database, alarm won't be generated until a new ASO connection starts.
AGNT-8556	AIX, Solaris, Windows	All Databases	When monitoring external traffic in PCAP mode, an agent move to a gateway that was not a part of the original cluster (the cluster when the agent registered to it) could have caused packet loss. Relevant to AIX, Windows and Solaris 11.
AGNT-10194	All	All Databases	If the RemoteAgent listener in the Imperva Gateway is changed from non SSL to SSL, the Imperva Agents registered to this Gateway will no longer be able to communicate with the gateway. Workaround: re-register relevant Imperva Agents.
AGNT-10206	All	All Databases	On rare occasions, when unregistering an Agent from the gateway that was in 'full-trust' trust mode, and then registering it without trust enabled, the agent will not be able to start. Workaround: uninstall and reinstall the agent.
AGNT-10228	All	All Databases	Combining two or more monitoring rules, with some of them Agent criteria and others gateway criteria does not work properly.

ID	Agent OS	Agent DB/ Product	Description
AGNT-10281	All	All Databases	The equals sign (=) is not supported for the password of the Imperva user when registering agent to the gateway using command line. Using the equals sign in the password when registering from the CLI works.
AGNT-10908	All	All Databases	The Imperva Agent cannot be installed in a root directory (C:\ for example), but only in a subfolder.
AGNT-11337	All	All Databases	If there is no traffic on a connection for longer than 10 minutes, the following packet might be not audited.
AGNT-11408	All	All Databases	Cannot create agent get-tech-info in folder other than /tmp.
AGNT-6402	All	All Databases	On rare occasions, Time Of Day exclusions do not work.
AGNT-7057	All	All Databases	On rare occasions when a local connection to a database is open for a very long period, and there is large number of connections being opened and closed, the "user" in audit data may appear as "connected user."
AGNT-7676	All	All Databases	After gateway restart, wrong event capture time is reported for logout operations.
AGNT-8084	All	All Databases	In cases when the system parameter max_pid was modified after ragent was loaded, some audit will be lost.
AGNT-8151	All	All Databases	During agent move, Agent status might temporarily change to Running With Errors 'Data connection to gateway has been lost'.
AGNT-8268	All	All Databases	Agent and gateway cannot communicate when the gateway is configured as Reverse Proxy and to accept only ECDH ciphers.

ID	Agent OS	Agent DB/ Product	Description
AGNT-8395	All	All Databases	During an automatic agent move, the agent's status might temporarily change to "Bad Connectivity."
AGNT-8487	All	All Databases	When the agent is disconnected from the Gateway, audit loss may occur.
AGNT-8558	All	All Databases	In cases where the server had no free disk space, after freeing some space the RACLI interface may show errors. Agent stop/start via the Agent CLI may resolve the issue.
AGNT-8559	All	All Databases	On rare occasions, the Remote Agent process crashes during shutdown.
AGNT-8790	All	All Databases	After re-registering the agent to a different MX, the hostname might not be correctly reflected in the MX.
AGNT-8949	All	All Databases	Traffic on sub network interface might still be audited even though the channel is configured as disabled.
AGNT-8981	All	All Databases	When installing the SecureSphere Agent Installation Manager only, users cannot change the path of the download directory in the MX GUI.
AGNT-9034	All	All Databases	Advanced configuration of "kernel-max-pid" and of "kernel-max-pid-limit" will not affect the agent if their value is higher than maximum number of process defined in the operating system.
AGNT-9151	All	All Databases	Agent crashes when enabling "send-ack" configuration from additional-configuration. Workaround: disable configuration. Additionally, agent crashes working with a gateway earlier than v10.5 GA.
AGNT-9247	All	All Databases	If PCAP is used to monitor external traffic (i.e., EIK is disabled), Remote Agent process may crash when it's stopped or when an IPv4 interface is removed.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9362	All	All Databases	In rare cases the agent may fail to get a valid certificate when starting trust migration.
AGNT-9850	All	All Databases	Remote Agent CTRL process uses high CPU when setup has trust and gateway cluster.
AGNT-9882	All	All Databases	In rare scenarios, agent log files can take more disk space than defined.
AGNT-9939	All	All Databases	The agent cannot communicate with Gateways v10.0 and earlier.
AGNT-11524	All	All RDBMS Databases	Using the Dbeaver client, when setting inline sniffing and the followed action after blocking is IP/User block the Dbeaver may accept few more queries until blocking is applied. This could happen when the Dbeaver opens more than 1 connection to the Server and each open connection will accept one query before being blocked.
AGNT-11565	All	DB2 All	Import/export were not audited in DB2.
AGNT-7232	All	DB2 All	When monitoring DB2 Shared memory connections, the response size in audit appears as 0.
AGNT-7272	All	Informix	When configuring Traffic Monitoring Rule with Process details - Agent criteria, and using the arguments parameter, the character @ is not supported.
AGNT-10844	All	Oracle	"An active shared server has been detected" alert could appear even though Oracle is not in shared server mode.
AGNT-11507	All	PostgreSQL	Import/export were not audited in PostgreSql.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9919	All	Progress	SecureSphere doesn't audit activity that takes place in shared memory, for example activity of the Progress Openedge utility.
AGNT-7821	HP-UX	All Databases	Agent may fail to start and then provides a non-informative error message.
AGNT-9141	HP-UX	All Databases	In a trusted environment, the SecureSphere Agent could temporarily have high CPU usage when renewing its certificate.
AGNT-9262	HP-UX	All Databases	Pcap on HP-UX may use promiscuous mode without explicit request.
AGNT-10549	HP-UX	PostgreSQL	No audit data is available for local connections.
AGNT-10315	Linux	All Databases	On rare occasions, when there are issues with the rpm database, the agent can cause performance degradation.
AGNT-10512	Linux	All Databases	In some cases, the SecureSphere Agent might create an empty /boot/ System.map file.
AGNT-11244	Linux	All Databases	Large responses are sometime not audited if the database is monitored in the user-space.
AGNT-7660	Linux	All Databases	RHEL6 K0 (kernel patches lower than p5): the SecureSphere Agent cannot coexist with the Vormetric Agents.
AGNT-11976	Linux	DataStax Cassandra	Big Data Agents might experience audit loss when running multiple connections on Cassandra.
AGNT-12054	Linux	DataStax Cassandra	The DataBase field in MX audit data might be incorrect when running commands without explicitly specifying the relevant keyspace.

ID	Agent OS	Agent DB/ Product	Description
AGNT-11743	Linux	DB2 for LUW	After agent restart, audit of few transactions might be lost.
AGNT-11605	Linux	MongoDB	Create index command might report the incorrect object in audit data.
AGNT-11739	Linux	MongoDB	Audit for commands "db.collection.findOneAndReplace()" and "db.collection.watch()" may report the command succeeded although it failed.
AGNT-11747	Linux	MongoDB	"Object" column in audit for "db.collection.copyTo()" command shows the database name instead of the collection name.
AGNT-11748	Linux	MongoDB	"Object" column in audit is empty for commands adb.testData.storageSize(), db.testData.totalIndexSize() and db.testData.totalSize().
AGNT-11771	Linux	MongoDB	Create view command is reported in audit as create table.
AGNT-11791	Linux	MongoDB	Audit events may be reported on a user that failed to authenticate to the database.
AGNT-11834	Linux	MongoDB	Audit loss may occur when high traffic is running in MongoDB.
AGNT-11912	Linux	MongoDB	Event capture time for logout event might be wrong if the time on agent machine is different than the gateways.
AGNT-10127	Linux	MSSQL	Connections that are established just after the database starts might be audited as a 'connected user.'
AGNT-11757	Linux	MSSQL	No audit is available for IPC connections.

ID	Agent OS	Agent DB/ Product	Description
AGNT-11763	Linux	MSSQL	When working in sniffing mode, certain clients of Mssql might not be blocked at all, even though a they should be according to a security policy.
AGNT-10072	Linux	MSSQL, Teradata	Changing the ragent installation directory while upgrading ragent version may cause audit loss until next database restart.
AGNT-10128	Linux	MSSQL, Teradata	If Data Interface discovery is disabled, there is no audit for MsSQL on Linux and Teradata version 16.1 and up.
AGNT-10195	Linux	MSSQL, Teradata	User space monitoring will not work when the agent installation directory is larger than 75 characters.
AGNT-11641	Linux	MySQL	MySQL upgrade fails with errors in collector log starting with [ERROR]UnifiedLogsPeriodicThread.cpp:218 Cant open dir for scan. Work around is available in the customer knowledgebase at https://www.imperva.com/sign_in.asp?retURL=/articles/Solution/Agents--Mysql-upgrade-fail-when-upgrading-from-14-1
AGNT-10561	Linux	Oracle	When inline mode is configured, ASO shared mode results in a connection delay.
AGNT-10942	Linux	Oracle	SQL exception is not detected for non-existing table on Diffie Hellman open mode connections.
AGNT-11324	Linux	Oracle	Oracle Recovery Manager (RMAN) jobs might get stuck when agent is active and ASO Monitoring is enabled in the agent.
AGNT-11655	Linux	Oracle	When Oracle is configured to work in shared mode with ASO encryption, connections might not be audited after agent restart when the DB server had been started before the agent and there were no external connections to the DB when the agent went up.

ID	Agent OS	Agent DB/ Product	Description
AGNT-10280	Linux, Unix	All Databases	In rare scenarios and on servers with mounts, the database discovery process might hang and channels are not be discovered.
AGNT-9148	Linux, Unix	All Databases	Agent requires a loop-back interface with address of 127.0.0.1 to be present in the server.
AGNT-11654	Linux, Unix	Oracle	On rare occasions, logout notification missing for tcp connections of DB2.
AGNT-11581	OEL (non-UEK), OEL-UEK, RHEL	Cloudera Hive, Hortonworks Hive	Missing audit may be encountered when a query command hasn't fetched all the data that the query returned, e.g., when using Hue UI, the fetches are done in chunks of 1000 rows and the next fetch is done when the user scrolls down the UI.
AGNT-12048	OEL-UEK	Oracle	Memory leak may be encountered in the ragent process.
AGNT-11053	OEL-UEK, RHEL	Cloudera Hive, Hortonworks Hive	On some occasions, a response size of zero may be encountered.
AGNT-9964	RHEL	All Databases	Vendor Meltdown patches for RHELv7 and for RHELv6 operating systems cause the SecureSphere Agent to fail during start.
AGNT-10210	RHEL	Cloudera HBase	Username may not be reported for old versions of HBase (up to Cloudera 5.6).
AGNT-9999	RHEL	Cloudera HBase	Column names in HBase are missing in some of the translated queries in Cloudera 5.7.1 and up.
AGNT-10655	RHEL	Cloudera HDFS, Hortonworks HDFS	When performing an operation in HDFS through REST API, the source IP in MX audit is always be the local IP of the server.

ID	Agent OS	Agent DB/ Product	Description
AGNT-10006	RHEL	Cloudera Impala	A few types of SQL exceptions are not reported in Impala.
AGNT-10328	RHEL	MongoDB	SecureSphere Agent does not support authentication in MongoDB client versions older than 3.0.
AGNT-10367	RHEL	MongoDB	The following opcodes are not supported on MongoDB with version lower than 3.0: op_insert, op_update, op_delete, op_reply.
AGNT-10120	RHEL	Oracle	If the Agent driver fails to start, the Injection Manager process might eventually crash.
AGNT-7722	RHEL, Solaris	NFS	Registering a File Agent for local traffic monitoring will result in monitoring external traffic as well.
AGNT-10705	RHEL, Ubuntu	MariaDB, MSSQL, MySQL, PostgreSQL	Audit loss may be experienced with connections that are opened shortly (seconds) after database restart when user-space interception is active.
AGNT-7856	Solaris	All Databases	When running GTI on Solaris 10, the error message "ln: cannot create [...]: File exists" may appear.
AGNT-10249	Solaris	Oracle	When upgrade from v13.0 to v13.1 or later, open mode connections won't be audited. Workaround: Restart the Database after the upgrade.
AGNT-8958	Solaris	Oracle	'Source of activity' field mistakenly displays 'remote' for local connection on Solaris global zone.
AGNT-9378	Solaris	Oracle	GTI doesn't collect ASO logs when "shared" folder is defined in non default location.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9681	Solaris	Oracle	Agent ASO on Solaris SPARC monitors databases in Global Zone only.
AGNT-9785	Solaris	Oracle	When 200 simultaneous ASO connections are open, some are not being monitored.
AGNT-9847	Solaris	Oracle	When the Oracle database is installed on a Solaris zone which isn't Global and the Agent ASO is enabled, Agent may display error with message "Oracle ASO monitoring failed".
AGNT-10146	SUSE	All Databases	In rare cases, due to startup scheduling, a complete loss of audit data may occur. Workaround: restart the agent.
AGNT-9946	SUSE	All Databases	Vendor Meltdown patches for SUSE Operating Systems cause the SecureSphere Agent to fail during startup. Partial work around, for external traffic only, is the use PCAP mode.
AGNT-11850	SUSE	Oracle	When Oracle is configured to work in shared mode with ASO encryption, connections might not be audited after agent restart when the database server had been started before the agent and there were no external connections to the database when the agent went up.
AGNT-11801	SUSE	SAP-HANA	When layer-C is enabled, there might be invalid audit of the responses from the database.
AGNT-8696	SUSE	SAP-HANA	When using SAP-HANA 12, moving from sniffing to inline mode and vise versa doesn't work with local TCP connections.
AGNT-9471	SUSE	Teradata	In Teradata 16.1 and above the CPU consumption of ragent process is higher than in older Teradata versions. Work around: Client may disable TD-API method using advanced config in order to work the same as older Teradata versions.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9959	SUSE	Teradata	On rare occasions, uninstalling the SecureSphere Agent might cause the Teradata database to freeze up.
AGNT-11611	SUSE-Teradata	Teradata	If more than a single PDE is installed on the machine, GTI will fail. Workaround: Collect the required information manually.
AGNT-9947	Ubuntu	All Databases	The Ubuntu 14.04 agent can't be installed or upgraded using Software Update.
AGNT-11974	Ubuntu	MariaDB	Discovery does not detects MariaDB version 10.5 and above. Workaround: Add the channels manually using MX UI setting > Agent > Data interfaces > press + > MariaDB.
AGNT-10165	Unix	All Databases	First queries received with an Agent with open mode connections are not audited.
AGNT-7381	Unix	All Databases	When using EIK and upgrading from agent version 11.0 and earlier to version 11.5 "connected user" is displayed on connections opened before the upgrade was conducted.
AGNT-7654	Unix	All Databases	When using LDAP authentication on a 64bit machine without the 32bit LDAP libraries installed, the users in OS user chain are displayed as GUID instead of user names.
AGNT-9265	Unix	All Databases	When connecting to a machine before the agent is working, the remote login isn't detected. Some applications (such as SecureCRT) reuse previous SSH connections thereby preventing the remote login from being detected.
AGNT-9456	Unix	All Databases	Agent fails to start if the agent folder is located on XFS with 64bit i-nodes.

ID	Agent OS	Agent DB/ Product	Description
AGNT-10266	Unix	MySQL	Incomplete audit for TCP local traffic. Workaround: Add the following item in the SecureSphere Agent's Advanced Configuration pane: <kernel_support_local_traffic_in_server_side>0</ kernel_support_local_traffic_in_server_side>.
AGNT-10040	Unix	Oracle	When agent is being update from a version that does not support open-mode to a version that supports open mode, open-mode ASO connections are not monitored.
AGNT-10042	Unix	Oracle	If Oracle is configured to work in shared-server-mode, Diffie-Hellman connections will not be monitored.
AGNT-7902	Unix	Oracle	ASO | No audit is available for Diffie Hellman encrypted traffic if the Oracle database being audited is configured to work in 'shared mode.'
AGNT-8409	Unix	Oracle	Open mode is not supported for encrypted and non-encrypted Oracle connections during upgrade from Agent version less than v12 to Agent version v12 and newer, when ASO monitoring is enabled prior to the upgrade.
AGNT-9389	Unix	Oracle	If monitoring Diffie-Helman traffic while ASO in the agent is disabled, agent enters running with errors. If disabling DH traffic on the database while ASO is still disabled in the agent, running-with-errors persists.
AGNT-8054	Unix	Progress	When working with connections that utilize high ports with Progress DB, open mode is not supported.
AGNT-11888	Windows	Active Directory, CIFS, IMS, NFS	Windows Agent FAM monitoring is not supported on v14.4 P10.
AGNT-11831	Windows	All Databases	In some cases when connections are created when the agent is in slim monitoring mode, later audit won't appear.

ID	Agent OS	Agent DB/ Product	Description
AGNT-11851	Windows	All Databases	When an Agent reconnects to the gateway, some of the traffic audit that was intercepted during the disconnection time might be lost.
AGNT-11916	Windows	All Databases	No IPv6 listener system event is generated if the channel is added manually.
AGNT-6189	Windows	All Databases	When upgrading from agent versions earlier than 11.0, server might cause lower agent performance. Workaround: Reboot the database server after upgrade.
AGNT-6256	Windows	All Databases	On rare occasions, agent uninstall may fail.
AGNT-7084	Windows	All Databases	Upgrading the Windows Agent to the same Agent version will fail.
AGNT-7109	Windows	All Databases	When working in PCAP mode, if WINPCAP is not installed and the TCP external data interface exists, then the TCP loopback data interface might not be monitored.
AGNT-7369	Windows	All Databases	When executing first time installation of the SecureSphere Agent or upgrading from v11.0 and earlier and working with EIK on Windows Server 2008 and newer, SecureSphere cannot monitor previously established connections.
AGNT-7533	Windows	All Databases	On rare occasions, process details are missing.
AGNT-8158	Windows	All Databases	On rare occasions, after uninstalling the SecureSphere Agent, its related processes might still be running.
AGNT-8680	Windows	All Databases	When a MySQL, Oracle or DB2 database is accessed using Windows authentication and Kerberos authentication is used, the username will not be audited.

ID	Agent OS	Agent DB/ Product	Description
AGNT-8764	Windows	All Databases	On Windows Server 2012, if open connections exist prior to installing the agent, running new short connections could cause non-existent logouts to appear in audit of open mode connections.
AGNT-8765	Windows	All Databases	Updating a channel (etc. disabling then re-enabling) causes audit loss.
AGNT-8915	Windows	All Databases	DrWeb antivirus mistakenly detects Imperva agent as a Trojan.
AGNT-8920	Windows	All Databases	When external traffic is monitored by pcap on windows platforms, disabling and enabling network interface while agent is running will cause complete audit loss. Workaround: restart the Agent.
AGNT-8960	Windows	All Databases	On Windows 2000 servers, the SecureSphere Agent might report the wrong number of cores.
AGNT-8127	Windows	CIFS	Audit is missing for shared folders with a name longer than 260 characters.
AGNT-8129	Windows	CIFS	Source IP address may be missing for access on path longer than 260 characters.
AGNT-8303	Windows	CIFS	When configuring a user exclusion, only users that appear in remote traffic are excluded, while users in local access are not excluded.
AGNT-8771	Windows	CIFS	Multichannel connections may be audited with 0.0.0.0 source IP in cases that the server network adapter enables IPv6.
AGNT-8772	Windows	CIFS	Limitation: "Source IP" audit parameter not supported with IPv6 related file operations. "0.0.0.0" is displayed under these conditions.

ID	Agent OS	Agent DB/ Product	Description
AGNT-8797	Windows	CIFS	When two clients access the same file at the same time, source IP address is reported as 0.0.0.0 for both clients.
AGNT-8919	Windows	CIFS	Missing source IP on Create and Read when accessing a Windows share from Linux smbclient.
AGNT-9595	Windows	CIFS	When using an SMB1 client and trying to access a file without permission no source IP is audited.
AGNT-9596	Windows	CIFS	When trying to access a folder without permission, the attempt is audited as access to a file, rather than a folder.
AGNT-8678	Windows	DB2 All	If the DB client connects to the DB server via 'shared memory,' the source IP address in audit is missing.
AGNT-8393	Windows	MariaDB	Maria DB IPC channel is not supported.
AGNT-10137	Windows	MSSQL	Certificate discovery might not work properly if two different databases are running with the same user but with different domains.
AGNT-10217	Windows	MSSQL	Incorrect OS user chain in MX appears for external connections when MSSQL Advanced Monitoring is enabled.
AGNT-10390	Windows	MSSQL	When applying non-exportable certificate for MSSQL2008 32 bit, no external audit is monitored and there is no hashed user for local traffic.
AGNT-10575	Windows	MSSQL	If Advanced Monitoring Mode is enabled, open-mode connections are not monitored with some clients (such as the Querier).
AGNT-10712	Windows	MSSQL	When the MSSQL process is 32 bits, the server IP is not displayed.

ID	Agent OS	Agent DB/ Product	Description
AGNT-11228	Windows	MSSQL	Channel over LocalTCP traffic is displayed on MX as MsSqlIPC.
AGNT-11241	Windows	MSSQL	The client remote session IP address might be missing if the MSSQL server user has insufficient permissions to obtain it. This results in the inability to block the connection by its source IP.
AGNT-11944	Windows	MSSQL	Blocking in sniffing mode for MSSQL connections was not supported. Support added starting with Imperva agent v14.x.
AGNT-6398	Windows	MSSQL	After blocking in sniffing mode for local TCP connections, it takes about a minute for the client to close the local TCP session.
AGNT-6505	Windows	MSSQL	In order for an MSSQL NP interface to be monitored, the MSSQL service needs write privileges to the agents folders.
AGNT-7947	Windows	MSSQL	Local (loop-back) TCP traffic that is generated by client applications based on the JDBC driver is not monitored by SecureSphere Agent.
AGNT-7994	Windows	MSSQL	When changing the login user of MSSQL server, its corresponding IPC channel log directory needs to be manually deleted. Otherwise, there will be no audit.
AGNT-8087	Windows	MSSQL	In cases where there is more than one MSSQL database on a server, all databases are running and RC4 user is used for Kerberos, Hashed Users may appear in audit.
AGNT-8923	Windows	MSSQL	Agent fails to discover certificate after changing user that runs the MSSQL service. Workaround: Restart the database to discover the new certificate. Relevant for MSSQL 2016.
AGNT-8988	Windows	MSSQL	In advanced mode, if a user ignores IPC channel and then un-ignores it, existing connections are not monitored.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9032	Windows	MSSQL	Open mode connections are not monitored on remote-named-pipe channel.
AGNT-9138	Windows	MSSQL	With an open mode connection in advanced monitoring mode, the user name isn't displayed if the SecureSphere version is older than v12 Patch 1.
AGNT-9140	Windows	MSSQL	User name is not displayed for open mode connections in advanced monitoring mode if the database is 32bit MSSQL.
AGNT-9234	Windows	MSSQL	Advanced monitoring mode does not support MSSQL 2008 32 bit.
AGNT-9235	Windows	MSSQL	User name detection in advanced monitoring mode is not supported in MSSQL 32 bit.
AGNT-9874	Windows	MSSQL	When a machine has more than one MsSql server installed that are running under the same user name but from different domains, the default MsSql certificate might not be extracted for some of the servers.
AGNT-8606	Windows	MySQL	MySQL connections may not be monitored if Diffie-Hellman authentication is used.
AGNT-5730	Windows	SharePoint	Revoke permissions for an attachment under a list item is not supported.
AGNT-6330	Windows	SharePoint	A SharePoint security policy configured to block upon file object modification also blocks list objects.
AGNT-9116	Windows	SharePoint	Operations on checked out files are not blocked.

ID	Agent OS	Agent DB/ Product	Description
AGNT-9123	Windows	SharePoint	On SharePoint sites authenticated using "Claims," security polices using a group based match criteria cannot block the activity
AGNT-9193	Windows	SharePoint	SharePoint security policy blocking cannot be disabled by changing the action to "None."
AGNT-9205	Windows	SharePoint	In rare cases when uploading files to a SharePoint 2013 site by dragging the files to the browser, the deletion of these files is not blocked by the security policy.
AGNT-9610	Windows	SharePoint	SharePoint Blocking doesn't always block folder delete operation.
AGNT-9611	Windows	SharePoint	SharePoint Blocking doesn't always block folder creation.
AGNT-11857	Windows	Sybase ASE	Audit is only partially available from traffic running on a local TCP channel.
AGNT-8913	Windows 2012	All Databases	When sending a query from a client in one domain to an MSSQL server in another domain with MSSQL service running an AD user in the first domain, hashed user is received.
AGNT-11846	Windows 2016, Windows 2019	MSSQL	Local connections are not monitored unless agent is in mssql advanced mode. Work Around: Enable mssql advanced mode by configuring mssql-advanced-monitoring flag under Advanced Configuration for the Agent in the MX to true, then restart the agent.
AGNT-11948	Windows 2019	All Databases	Database server operating system displayed in MX is Windows 2016 although it should be Windows 2019.

76151 Open Issues with Imperva Data Protection Agent - v14.4 Last modified: 8/27/2020 9:04:55 AM

Agent Patch Bug Fixes

This section includes information regarding bugs that were resolved in patches including the following:

- Fixed Issues with Imperva Data Protection Agent - v14.1
- Fixed Issues with Imperva Data Protection Agent - v14.1 Patch 20
- Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 10
- Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 20

73550 Agent Patch Bug Fixes Last modified: 6/6/2019 3:59:39 PM

Fixed Issues with Imperva Data Protection Agent - v14.1

ID	Agent OS	Agent DB/ Product	RN Bug Description
AGNT-10854	AIX	Informix	Adding Informix shared memory channel caused configuration failures.
AGNT-10887	AIX, Linux, Solaris	Oracle	Oracle ASO monitoring might suffer from audit loss on rare cases.
AGNT-10767	All	All Databases	In multi-core environments competition for agent resources resulted in reduced transactions per second (TPS).
AGNT-10907	All	All Databases	Agent monitoring rules (AMR) was not excluding traffic.
AGNT-10565	Linux	Cloudera HDFS, Hortonworks HDFS	RemoteAgent monitored only the first 10,000 HDFS connections.
AGNT-10230	Linux, RHEL, SUSE, UEK	All Databases	Spectre v2 mitigation retpoline might have been disabled in kernel when Agent was installed on newer kernel versions.
AGNT-10801	Linux, ubuntu	MariaDB, MSSQL, MySQL, PostgreSQL	E2E userspace monitoring may fail on rare occasions when working on: MsSQL on Linux; MySQL, PostgreSQL, and MariaDB on Ubuntu.
AGNT-10768	RHEL	DataStax Cassandra	Cassandra queries could have had a semicolon at the end of the queries.
AGNT-10528	RHEL	MongoDB	The following commands were not monitored: createRole,updateRole, grantPrivilegesToRole, and revokePrivilegesFromRole.

ID	Agent OS	Agent DB/ Product	RN Bug Description
AGNT-10563	RHEL	MongoDB	Some commands interpreted arguments under the "Parsed Query" and "Query" columns in MX as hexadecimal strings instead of real string arguments.
AGNT-10772	RHEL	MongoDB	Audit of insert commands didn't show documents that were inserted.
AGNT-10894	RHEL	MongoDB	On some occasions, Imperva Agent may be Running With Errors when using Memory Capping.
AGIM-344	Solaris	All Databases	Get Tech Info could not be created due to syntax error.
AGNT-10330	Solaris	All Databases	Get Tech Info could not be created due to syntax error.
AGNT-10668	Solaris	All Databases	Imperva Agent v13.3 didn't support Solaris 11.4.
AGNT-10669	Solaris	All Databases	Imperva Agent caused a crash on Solaris 11.4 and above.
AGNT-10748	SUSE, ubuntu, UEK	PostgreSQL	On rare occasions, due to unexpected races, agent may enter running with errors due to corrupted synchronization objects in the PostgreSQL.
AGNT-10737	Windows	All Databases	Agent displayed the wrong Windows version in the MX.
AGNT-10494	Windows	MSSQL	Logs were created containing no information.
AGNT-10706	Windows	Oracle	If the RemoteAgent was started after a server reboot with an IPC channel enabled, it could be running with errors with the message "Couldn't apply agent configuration".

72403 Fixed Issues with Imperva Data Protection Agent - v14.1 Last modified: 6/16/2020 6:54:16 PM

Fixed Issues with Imperva Data Protection Agent - v14.1 Patch 20

ID	Agent OS	Agent DB/ Product	Description
AGNT-11065	RHEL, UEK	MongoDB	MongoDB may not have been audited when a domain user was running the MongoDB process and the domain controller wasn't accessible from the MongoDB server when the Agent Controller started. Agent would be Running with Errors.
AGNT-11102	RHEL, UEK	All Databases	discoveryCtrl and discoveryRagent logs might have flooded the disk.
AGNT-11017	RHEL, UEK	Hortonworks Hive	Agent failed to monitor Hive on Hortonworks 3.1.X
AGNT-11018	RHEL, UEK	Cloudera HBase, Hortonworks HBase	HBase server process could have crashed when more than 10K connections were audited by the Agent on RHEL6 or OEL6.
AGNT-11019	RHEL, UEK	Cloudera HBase, Hortonworks HBase	Agent would not audit more than first 10K connections on HBase with a version lower than 2.0.0.

73339 Fixed Issues with Imperva Data Protection Agent - v14.1 Patch 20 Last modified: 6/16/2020 6:55:42 PM

Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 10

ID	Agent OS	Agent DB/ Product	Bug Description
AGNT-11574	AIX	All Databases	A single process with many threads could have resulted in high CPU.
AGNT-11250	All	All Databases	On rare occasions, once the agent started working in slim monitoring, it got stuck in that mode.
AGNT-11550	All	All Databases	On rare occasions, the controller was unable to stop.
AGNT-11368	Linux	All Databases	In rare cases, where agent memory capping occurred when using local connections and userspace interception agent didn't respond due to deadock.
AGNT-11411	Linux	All Databases	On databases with a high load that were monitored with user-space interception, the agent was slow to respond.
AGNT-11644	Linux	All Databases	Audit loss for user-space intercepted databases when the agent was installed on a soft link.
AGNT-11528	Linux	DB2 for LUW	High system CPU encountered on RHEL 7.
AGNT-11558	Linux	DB2 for LUW	In rare cases, audit loss was experienced with external TCP connections in DB2.
AGNT-11322	Linux	MongoDB	When the Remote Agent was restarted multiple times, the MongoDB process could have crashed with a SIGTRAP signal.
AGNT-11170	Linux	MongoDB	When the Remote Agent was restarted multiple times, for example, due to a capping event, the MongoDB process could have crashed with a SIGABRT signal.

ID	Agent OS	Agent DB/ Product	Bug Description
AGNT-11237	Linux	Oracle	Database server crashed after upgrading Imperva Agent to v14.1
AGNT-11391	Linux	Oracle	Agent 13.5p20 crashed SUSE 12 sp2 on syscall replacement.
AGNT-11508	Linux	Oracle	In regular mode, around 10% of audit is lost when using BEQ connections. To work around this issue, see the following article in the customer knowledge base: https://www.imperva.com/sign_in.asp?retURL=/articles/Solution/Agents-Resolving-connected-users-when-running-BEQ-traffic
AGNT-11619	Linux, OEL (non-UEK), OEL-UEK	Cloudera HDFS, Hortonworks HDFS	HDFS traffic might have been slow due to Imperva Agent.
AGNT-11262	Linux, Unix	All Databases	Sticky bit for permissions was missing for folders.
AGNT-11264	Linux, Unix	Oracle	Running with error message was encountered stating that the an ASO misconfiguration was not cleared after restarting the Agent.
AGNT-11036	Linux, Unix, Windows	All RDBMS Databases	When thousands of local connections are being opened and closed while another local connection is still opened, the database user might appear as 'connected user' instead of the right database user name.
AGNT-11158	OEL-UEK, RHEL	Cloudera Hive, Hortonworks Hive	Logout events in Hive only appeared in audit after 24 hours.
AGNT-10499	RHEL	Oracle	In rare scenarios ASO monitoring with Imperva Agent was not working.
AGNT-11121	Solaris	Oracle	ASO monitoring failed on Oracle minor version.

ID	Agent OS	Agent DB/ Product	Bug Description
AGNT-11498	SUSE	All Databases	Agent installation failed when /lib/ directory was read-only.
AGNT-11736	SUSE	Oracle	Agent failed to intercept traffic on new SUSE 12 SP3 kernels (starting in 4.4.178-94).
AGNT-10311	SUSE-Teradata	Teradata	Running GTI on Teradata SLES machine, which has 2 or more Teradata DB instances, will produce output for all the instances.
AGNT-11593	SUSE-Teradata	Teradata	In TD16.1 and higher, restart of Imperva Agent might have resulted in a database crash.
AGNT-11375	Ubuntu	MariaDB	Agent failed to monitor MariaDB traffic.
AGNT-11162	Unix	Greenplum, MariaDB, PostgreSQL	With Management Server versions 12 and lower automatically discovered data interfaces did not always appear.
AGNT-11253	Windows	DB2 All	Agent could have caused DB2 process to crash when shared memory connections were used.
AGNT-9013	Windows	MSSQL	Blocking was not supported with MSSQL Advanced Monitoring.
AGNT-11041	Windows	MSSQL	Multiple recurring blocked connections would lead to a memory leak, eventually causing the sql server to block new connections.
AGNT-11357	Windows	MSSQL	MS-SQL server panic was encountered.

75950 Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 10 Last modified: 8/17/2020 10:38:30 AM

Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 20

ID	Agent OS	Agent DB/ Product	Description
AGNT-11250	All	All Databases	On rare occasions, once the agent started working in slim monitoring, it got stuck in that mode.
AGNT-11550	All	All Databases	On rare occasions, the controller was unable to stop.
AGNT-11994	All	Oracle	No audit was available for Oracle when using the following combination: sqlplus version 19, OCM, Encrypted traffic.
AGNT-11952	Linux	All Big Data Databases	Big Data agent could experience memory capping when exclusion monitoring rules were applied to it in MX.
AGNT-11036	Linux, Unix, Windows	All RDBMS Databases	When thousands of local connections are being opened and closed while another local connection is still opened, the database user might appear as 'connected user' instead of the right database user name.
AGNT-11264	Linux, Unix, Windows	Oracle	Running with error message was encountered stating that the an ASO misconfiguration was not cleared after restarting the Agent.
AGNT-11331	OEL-UEK, Rhel	All Big Data Databases	When a new ACP (Agent Compatibility Package) was sent to the Big Data Agent, an Agent restart via MX UI was required in order to support a database that wasn't supported with the previous ACP update.
AGNT-11552	OEL-UEK, RHEL	MongoDB	MongoDB memory consumption may have increased when the Agent was used.
AGNT-10938	OEL-UEK, SUSE	MariaDB, MySQL	If there are several instances of MySql or MariaDB installed on one DB server (several of the same type) then in certain scenarios audit for one might be missing.

ID	Agent OS	Agent DB/ Product	Description
AGNT-11839	RHEL	MSSQL	No audit was available in MSSQL over Redhat 8.
AGNT-11866	RHEL	Oracle	In RHEL7, Oracle BEQ connections were not monitored once the connection was opened by any user that is not oracle.
AGNT-10499	RHEL	Oracle	In rare scenarios ASO monitoring with Imperva Agent was not working.
AGIM-369	Unix	All Databases	Agent tech info left temp files behind.
AGNT-11856	Windows	DB2 for LUW	DB2 process crashed when trying to access an uninitialized global variable.
AGNT-11855	Windows	DB2 for LUW	DB2 process crashed when trying to access an uninitialized global variable.
AGNT-11945	Windows	MSSQL	Agent was sometimes failing to discover MSSQL.
AGNT-11197	Windows	MSSQL	SQL server crashed after upgrading agent to v13.5p20.
AGNT-11357	Windows	MSSQL	MS-SQL server panic was encountered.

76155 Fixed Issues with Imperva Data Protection Agent - v14.4 Patch 20 Last modified: 8/17/2020 1:38:32 PM

Proprietary Rights Notice

Follow this link to see the Imperva copyright notices and certain open source license terms:

https://www.imperva.com/sign_in.asp?retURL=/articles/Reference/SecureSphere-License-and-Copyright-Information

TRADEMARK ATTRIBUTIONS

PATENT INFORMATION

The software described by this document may be covered by one or more of the following patents:

US Patent Nos. 7,640,235, 7,743,420, 7,752,662, 8,024,804, 8,051,484, 8,056,141, 8,135,948, 8,181,246, 8,392,963, 8,448,233, 8,453,255, 8,713,682, 8,752,208, 8,869,279 and 8,904,558, 8,973,142, 8,984,630, 8,997,232, 9,009,832, 9,027,136, 9,027,137, 9,128,941, 9,148,440, 9,148,446 and 9,401,927.

Imperva Inc.

3400 Bridge Parkway

Redwood Shores, CA 94065

United States

Tel: +1 (650) 345-9000
Fax: +1 (650) 345-9004

- **Website**: http://www.imperva.com
- **General Information**: info@imperva.com
- **Sales**: sales@imperva.com
- **Professional Services**: consulting@imperva.com
- **Technical Support**: support@imperva.com

v14.1-Agent-Release-Notes-v2

75948 Proprietary Rights Notice Last modified: 6/16/2020 7:01:39 PM