IMPERVA®

SECURESPHERE®

Release Notes

Version 10.5

March 2014

www.imperva.com

COPYRIGHT NOTICE

© 2014 Imperva, Inc. All Rights Reserved.

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

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

This document is for informational purposes only. Imperva, Inc. makes no warranties, expressed or implied.

No part of this document may be used, disclosed, reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Imperva, Inc. To obtain this permission, write to the attention of the Imperva Legal Department at: 3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065.

Information in this document is subject to change without notice and does not represent a commitment on the part of Imperva, Inc. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of this agreement.

This document contains proprietary and confidential information of Imperva, Inc. This document is solely for the use of authorized Imperva customers. The information furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by Imperva, Inc. for the use of this material.

TRADEMARK ATTRIBUTIONS

Imperva and SecureSphere are trademarks of Imperva, Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

PATENT INFORMATION

The software described by this document is covered by one or more of the following patents:
US Patent Nos. 7,752,662, 7,743,420, 7,640,235, 8,024,804, 8,051,484, 8,056,141, 8,135,498 and 8,181,246.

Imperva Contact Information

US Headquarters Imperva Inc. 3400 Bridge Parkway, Suite 200 Redwood Shores, CA 94065 USA Tel: (650) 345 9000 Fax: (650) 345 9004	Email: info@imperva.com Website: www.imperva.com

1. Release Highlights

1.1 Database Enhancements

1.1.1 Gateway Cluster

The SecureSphere gateway cluster available for the first time in SecureSphere v10.5 introduces N+1 gateway redundancy, and a new level of ease and scale with agent deployment and management. It delivers lower total cost of ownership through automated agent deployment tasks and provides benefits that include:

- **Efficient redundancy**: Gateways are backed up in an N+1 structure. When one gateway fails, its agents are automatically moved to the redundant gateway in the cluster.
- **Management robustness**: One gateway manages the cluster, the cluster's agent assignments, and gateway redundancy.
- **Load sharing**: When registered to the gateway cluster for the first time, database agents are automatically assigned to the gateway with the least load.
- **Session state persistence**: Session information (e.g. users, specific database transactions) is shared between the gateways in the cluster so that in cases of a gateway failure, the database audit contains the traceable activity of the user.
- **Cluster Management Dashboard**: The management server introduces a new tab **Cluster Management** that shows the health, performance, and resource utilization of all assets in the cluster.

1.1.2 Deployment Automation

The following sections describe the new deployment automation features introduced in SecureSphere v10.5.

1.1.2.1 Default Application Group

SecureSphere now assigns all applications to a default application group when they are created. Subsequently, when agents are installed on databases and the agent registers with SecureSphere, the new database is added to the default application group if a specific application group is not indicated.

1.1.2.2 Application Level Audit Policy

Policies can now be assigned at the application level. This allows new applications to be automatically monitored upon creation, as they are assigned automatically to the default application group, and are immediately monitored by an application level audit policy that applies to that group.

1.1.2.3 Agent Registration to a Server Group

Database agents can now be registered to a server group. If the server group does not exist during registration, it will be automatically created in SecureSphere. When the agent runs data interface discovery, the management server sees that the agent has discovered new data interfaces and automatically creates a new service and new default application per database type. If a service for that database type does exist, then the management server associates the newly discovered data interface with the service of its type. From that moment on, all traffic that arrives from the agent and is connected to the discovered data interface is monitored under the new service and application.

1.1.3 Tagging and Automatic Assignment of Monitoring Rules

SecureSphere enables streamlining the monitoring of traffic by defining properties known as tags. Tags can be used in agent monitoring rules, applied to existing agents in bulk, and automatically applied to new agents. Tags can automatically exclude monitored traffic related to agents with the defined tag.

1.1.4 Traffic Distribution Analysis

SecureSphere v10.5 provides traffic distribution analysis in the user interface. This provides additional insight in enterprise environments where there are varying constraints on the usage of database server resources (for example, available network bandwidth, CPU usage, etc.). Traffic Distribution Analysis displays statistical information that allows you to easily set up monitoring and exclusion rules based on which processes, IP addresses, users, etc., are creating the most traffic. You can then use this information to create rules and exclude traffic that does not require auditing, preserving resources on the database server and providing flexibility and scale needed for your enterprise.

1.1.5 Personal Information Masking

Personal information can now be masked by default in specific SecureSphere views and reports, facilitating compliance and data privacy in environments that require control over who can see personal data. Data is encrypted, resulting in hashed data being displayed in these views and reports. The ability to unmask this information can be given by SecureSphere administrators to specific users and roles.

1.1.6 Progress ABL Privileged Operations Support

SecureSphere now extends support for Progress OpenEdge by providing out-of-the-box configuration for auditing and monitoring Progress ABL privileged operations, in a user-friendly format.

1.1.7 DB2 Discovery for Unix

SecureSphere v10.5 introduces DB2 interface discovery on SecureSphere Unix agents.

1.1.8 Shared Memory for DB2 on Windows

SecureSphere v10.5 also introduces auditing and monitoring of DB2 database traffic on the shared memory interface when using Windows agents.

1.1.9 New Database Support

New database support in SecureSphere includes:

- Sybase ASE 15.7, Informix 11.7 and 12.1

1.1.10 DISA STIG and CIS Updates

DISA STIG and CIS updated include:

- DISA 8.1.9 - Oracle 10g, 11g
- DISA 8.1.7 - MS-SQL 2005
- CIS 1.2.0 - DB2 for Linux, Unix and Windows 8, 9, and 9.5

1.2 SecureSphere Agents

1.2.1 Agent Enhancements

As part of the gateway cluster infrastructure, a number of features have been added to enhance the management of agents which include:

- **Automatic deployment of agents**: Agents are registered to a cluster, which then assigns them dynamically to gateways according to available capacity.
- **Ease of management**: Agents can be moved in to, within, and out of a cluster from the management server, without accessing the agent.
- **State retention**: When a gateway in a cluster fails, the agents are simply transitioned to a redundant gateway in the cluster.

1.2.2 MySQL IPC Data Interface Support

A user-defined MySQL IPC data interface type is now supported for Imperva SecureSphere agents.

1.2.3 Traffic Compression

Users can optimize network performance bandwidth consumption by managing the amount of traffic between the agent and the gateway, particularly if it is excessive. This is accomplished using data compression which, when activated, compresses the data being sent by the agents to the gateway.

1.2.4 Exclusion Rules by Windows Process Names

SecureSphere v10.5 introduces the ability to exclude out-of-scope processes on Windows servers. To increase auditing and monitoring efficiency, SecureSphere administrators can now filter out irrelevant processes. For example, a nightly backup process may create a lot of database traffic, but does not need to be audited. This is the same functionality that exists in SecureSphere today for UNIX/Linux based database servers.

1.3 Web Enhancements

1.3.1 Integration with Amazon Web Services

SecureSphere Web Application Firewall now supports Amazon Web Services (AWS). With version v10.5, SecureSphere customers can monitor and protect web applications deployed on Amazon Web Services.

AWS offers a complete set of infrastructure and application services that enable enterprises to run all of their applications in the cloud.

The SecureSphere WAF can be deployed as an Elastic Compute Cloud (EC2) AMI and supports easy and quick deployment using AWS CloudFormation templates. SecureSphere for AWS delivers all of the benefits of the on-premise SecureSphere Web Application Firewall along with cloud computing features like auto-scaling and disaster recovery, thereby allowing enterprises to enjoy the same security level for their cloud based deployments as they do in their physical data centers.

1.3.2 Low Data Rate Attack Mitigation

SecureSphere v10.5 introduces the ability to mitigate low data rate attacks. This enables SecureSphere to detect and prevent this type of Application Distributed Denial of Service (DDoS) Attack.

Low data rate attacks, such as Slowloris, are characterized by opening many TCP connections to a server and transmitting very slow requests without terminating connections. Low data rate attacks can be launched by one or multiple attackers. SecureSphere's Low Data Rate protection mitigates this class of attacks by closing connections to clients that match the profile of an attack.

1.3.3 Enhanced Fraud Integrations

SecureSphere v10.5 presents improved integration with fraud prevention vendors such as ThreatMetrix and iovation, providing the following enhancements:

- Ability to receive data directly from fraud prevention vendors rather than only from the client. End user clients no longer need to send threat information as this is now done from SecureSphere directly. A request to the server is delayed and after the results are received from the fraud prevention vendor, the gateway interprets them in the same manner as it would interpret fraud prevention results from the client.
- Enhanced troubleshooting and verification capabilities for debugging. An optional debugging feature displays information that helps SecureSphere administrators troubleshoot issues.
- Improved interface and easier policy configuration: The user interface has been improved to centralize fields shared by different providers in the ThreatRadar screen, subsequently reducing the complexity of configuring policies by only needing to configure certain fields upon installation.
- A streamlined fraud policy configuration process.

1.3.4 SecureSphere Integration with nShield Connect

Starting with version v10.5, SecureSphere supports the use of HSM and provides integration with network-attached Hardware Security Module (HSM) provided by Thales, namely the nShield Connect 500.

1.3.5 Installing/Upgrading Mod-SSL

SecureSphere has been upgraded to CentOS 6.3. As part of this upgrade, the Apache web server has also been upgraded. In order to provide FIPS compliance users can now configure Mod-SSL with ARP and KARP configurations.

1.3.6 ThreatRadar and Community Defense Feeds

A new set of ThreatRadar feeds have been added that include:

- **Comment Spam IPs**: Policy based on list of IP addresses whose source is suspected of creating comment spam.
- **Scanner IPs**: A list of IP addresses that Imperva ADC has received from Community Defense that have recently conducted scanner activity based on fingerprints that were identified.

1.4 File Enhancements

1.4.1 Data Owner Portal

SecureSphere v10.5 introduces a web-based portal which displays the results of SecureSphere user rights scans. Data owners, such as team or group leaders who are most familiar with corporate data, use this user-friendly portal to review and manage access control to files relevant to their business unit. Scan results are first transferred from SecureSphere to the Data Owner Portal, and the data owner then conducts a review of existing permissions and either accepts them or rejects access. The results of the review are transferred back into SecureSphere, where IT personnel follow easy-to-use reports to guide them through the rights revocation process.

1.4.2 File Explorer

The SecureSphere File Explorer has an enhanced user interface with new functionality. The File Explorer now includes a classification scan view, a comment field for each data type applied to an entity, and an option to flag a data type that has been applied to an entity as a false positive.

1.4.3 Data Owner Assignment

SecureSphere can now import CSV files to map data items to corresponding data owners. With this functionality, only a single action is required to assign owners to any number of data items.

1.4.4 File Classification Report

A new report based on both manual classification and scan results imported from 3rd party classification and data discovery tools has been added. This report provides information in an intuitive, configurable, and distributable format.

1.4.5 SharePoint Blocking

SecureSphere v10.5 now offers the ability to block access to SharePoint files based on data type, file name, and users, or a combination of these properties. For example, after classifying files (either manually or through DLP import), and running file User Rights scans to identify users with access to these files, you can configure a policy that blocks specific users if they try to access a specific file, or files classified as containing a specific type of data.

1.5 Platform

1.5.1 Software Update Enhancements

Software Updates in v10.5 includes enhancements that provide administrators with a range of functionality that include:

- A complete picture of available updates for all SecureSphere components.
- Notifications about every release and upgrade.
- The ability to remotely perform agent upgrades from the management server.

1.5.2 Navigation Permission

The Navigation Permissions feature allows administrators to define which screens are accessible by which users/roles. This prevents unauthorized users from accessing features they should be blocked from.

1.5.3 CentOS

SecureSphere v10.5 is now running on CentOS version 6.3.

1.5.4 Secure LDAP Access

This v10.5 feature ensures that SecureSphere accesses customers' real LDAP servers and not a malicious LDAP by verifying the LDAP certificate against the certificate provided by the customer.

1.5.5 Job Management

The Jobs Status window in the Admin workspace has been enhanced, making it easier to analyze jobs and troubleshoot performance issues that may be the result of multiple jobs running at once. Additional enhancements include job duration and the ability to edit (reschedule) and abort jobs.

1.5.6 REST API

SecureSphere now offers a web based API using REST, enabling the configuration of various aspects of SecureSphere outside the GUI. The API can be used to automate a number of tasks such as creating Sites, Server Groups, Servers and Applications, applying policies, associating agent interfaces with server groups, and more.

1.5.7 Environment Export to XML

The Export to XML capability enables comparing different SecureSphere configurations, tracking changes performed on a SecureSphere environment, and using version control tools.

When changing definitions or adding new definitions to a SecureSphere environment, users might want to validate the changes on a test environment before performing them on the production environment. Once the new definitions have been tested, they can be applied to the production environment.

The Export to XML capability can be used to track all the changes that were performed on the environment to ensure change control and validation, thereby avoiding mistakes.

1.5.8 Report Scalability

Database Audit reports have been made scalable, eliminating limits to the size of the reports. In the past reports were limited to 100,000 records, beyond which they may have been truncated. Report scalability is achieved by limiting the output to csv, and producing several csv "chunks" each containing a portion of the overall record.

1.5.9 Failed Login Password Lockout

In SecureSphere v10.5, multiple unsuccessful attempts to log into SecureSphere using an incorrect password causes the user to be locked out for a certain period of time.

2. Database Support

2.1 Supported Databases

This version of SecureSphere supports the following databases:

Table 1 Version 10.5 Supported Databases

Database	Supported Database Versions
Caché	2011.1
DB2	7.2, 8, 9, 9.5, 9.7, 10.0
Informix	7.31, 9.x, 10.x, 11.0-11.5, 11.7, 12.1
MS-SQL	7, 2000, 2005, 2008, 2008 R2, 2012
MySQL	4.1, 5.x
Netezza	4.x, 5.0, 6.0
Oracle	8i, 9i, 10g, 11g
Sybase ASE	11.9, 12.0, 12.5.x, 15.0-15.7
Sybase IQ	12.5, 12.6, 12.7, 15.0
Progress Openedge	10.1c, 10.2a, 10.2b
Teradata	2.6, 12, 13.0, 13.1, 14 **Note:** Auditing Teradata versions 2.6 and 12 requires enabling of native auditing and is supported using the SecureSphere Log Collector framework.
PostgreSQL	8.4 - 9.1
IMS	10, 11

3. Known Issues

The following table lists the open issues for this release.

Table 2 Release 10.5 Known Issues

	ID	Description
Web Related Issues		
1	SPHR-21027 (24155)	ThreatRadar tab cannot be viewed with Safari browser. Workaround: • Use a different browser • Change the security settings in Safari to - Accept cookies always
2	SPHR-46974	Web: When configuring an FPS API policy to connect with Incapsula, connection fails. Workaround: In the SecureSphere bootstrap.XML kssl definition, disable SSL_RSA_WITH_RC4_128_SHA.
3	SPHR-46893	Reports - Alerts: When trying to create a report based on Slow HTTP/S, an error is displayed.
Database Related Issues		
4	SPHR-15772 (18049)	MySQL environment variables are not correctly parsed.
5	SPHR-22318 (19171)	Web/DB correlation requires the query group to operate in the Static Protect mode in order to work properly.
6	SPHR-16884 (19290)	In Main > Audit > Audit Data > Select Columns window, the aggregation function “None” does not appear.
7	SPHR-17221 (19669)	Lookup data sets: The last inserted row cannot be edited if it is close to the bottom of the page.
8	SPHR-17493 (19973)	DB Agent Central Management: Setup > Agents > General Information > Gateways, Gateway might appear as Active although it is disconnected.
9	SPHR-18193 (20778)	Data Discovery: When accepting two discovered columns, each one on a different data category but on the same table group, only one table group is created with one of the data categories.
10	SPHR-18577 (21214)	Data Discovery: Content based search returns incorrect results for tables with fewer than 200 records or tables whose first 200 records include NULLs.
11	ADCU-573 (21398)	Data Discovery: SSN defined with data type INT with a leading 0 is not being discovered.
12	SPHR-15069 (17239)	Risk Explorer: Multi-byte character sets are not properly displayed.
13	SPHR-21099 (24247)	Track Changes active module Registry Key object type is displayed in the GUI, even though it's not supported.
14	SPHR-32505 (34911)	DB2 URM: Configuring an OS authority name longer than 8 characters generates an error during the scan. Workaround: Authority name should be truncated to no more than 8 characters.
15	SPHR-32625 (35056)	DB2 URM - Active Directory Forest Configuration is not supported.

Table 2 Release 10.5 Known Issues

	ID	Description
16	SPHR-35455 (38981)	URM: Users are incorrectly identified as hashed users when MSSQL is used with Kerberos encryption algorithms not supported by SecureSphere.
17	AGNT-3875 (41027)	DB: In audit, TCP local traffic with NTLM authentication is shown as local access user for short connections.
18	SPHR-40514 (46608)	DB Enrichment: When configuring an enrichment policy and customizing Target Field Names, the field names aren't updated in the policy, though the updated names appear when selecting them as columns in Audit views.
19	SPHR-42402	SOM: Configuring a policy in SOM v10.5 and applying it in v10.0 is not prevented.
20	SPHR-43628	Direct Access Information: Cannot change direct access information to a database once configured. Workaround: delete and recreate direct access information.
21	SPHR-44380	Gateway Cluster: After configuring Selected Columns in the cluster window, then moving to another screen, the column selection is not preserved.
22	SPHR-45639	Gateway Cluster/Agents: After adding agents to a cluster, the MX overview screen in the cluster doesn't show the updated number of agents. Workaround: wait 30 seconds for data to update.
23	SPHR-45673	Gateway Cluster: In some cases, gateway failover may result in loss of data.
24	SPHR-45694	DB Agent: Kerberos keys aren't added together with an agent after adding the agent to the management server, resulting in hashed users. Workaround: restart the agent then try again.
25	SPHR-45790	Gateway Cluster/Agent: When agent move fails, no description is given in resulting system event.
26	SPHR-45848	Gateway Cluster: Screen data doesn't refresh when moving between tabs. Workaround: click the Refresh button.
27	SPHR-46013	Gateway Cluster: In some cases, when trying to register a large number of agents at one time, SecureSphere incorrectly shows some agents as disconnected after registration is complete. Workaround: Restarting the management server may resolve the issue.
28	SPHR-46071	Gateway Cluster: When a new cluster is created and is empty, there is no information in the overview pane and information from other active clusters may be displayed.
29	SPHR-46175	Gateway Cluster: After moving an agent from a cluster to a gateway not in that cluster, the gateway name in the cluster management page is not updated.
30	SPHR-46441	DB Audit: When configuring a lookup dataset column for database audit that includes an aggregation function, Audit screen crashes. Workaround: To work around this issue, access Oracle and configure as follows: • su - oracle • sqlplus secure/secure12 • SQL> delete from conf_user_preferences where key like 'ui.selectedColumns.viewStmt.DBAuditData%'; • SQL> commit;"
31	SPHR-46645	Gateway Cluster: An agent can be moved to another gateway even though the target gateway has no listener configured, rendering the agent unavailable. Workaround: define a listener for the target Gateway outside the cluster before moving the agent.
32	SPHR-46736	Gateway Cluster: Following a gateway move operation, some status indicators may change for up to a minute.

Table 2 Release 10.5 Known Issues

	ID	Description
33	**SPHR-47052**	Gateway Cluster/Agent: Moving an agent that is being configured results in a failed partial configuration and gateway failover. Workaround: don't move an agent in the process of configuration.
34	**SPHR-47088**	Gateway Cluster: In rare cases, the first time moving a gateway into an inactive cluster fails.
35	**SPHR-47111**	Gateway Cluster: When moving 100 or more agents, the status bar doesn't progress. Though the agents are moved.
SecureSphere Management Issues		
36	**SPHR-29734 (31126)**	All products: Policies > Action Sets > Archiving, when using the Action Interface SCP, it does not allow archiving to the local location on the MX with user ROOT. Workaround: Use the NFS Archive action interface instead.
37	**SPHR-29683 (31071)**	All products: The archived .mprv (e.g. SysEvents, Reports) files are encrypted by default. When trying to unpack, the decryption process fails. Workaround: This issue can be solved by adding the following unpack command: `keystore /opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kstto`
38	**SPHR-29940 (31401)**	All products - platform: Failover fails when GWs are connected to UDLD, which enables switching ports. This is due to the switched port entering an "error disabled" state. Workaround: Disable the UDLD protocol from the switch ports.
39	**SPHR-3894 (4144)**	System events privileges are not enforced.
40	**SPHR-36999 (41350)**	Migration: After upgrading, loaded audit archive is missing from the DB Audit Data screen. Workaround: Reload the archive data after upgrading.
41	**SPHR-14189 (16166)**	Archives: If archiving location is not available the system events are archived locally to /var/tmp but there is no indication in the job status.
42	**SPHR-16044 (18349)**	Active Module: If a scanner_integration.jar is replaced, it takes effect only after the server is restarted.
43	**SPHR-17788 (20308)**	SIEM: Action sets - Audit - If a secondary host is defined, then UDP should not be available as an option for the protocol.
44	**SPHR-22432 (23094)**	When installing from a USB drive, the final screen presents that centOS was installed instead of SecureSphere.
45	**SPHR-30333 (31954)**	Migration: The Log Collector password does not survive the upgrade.
46	**SPHR-40360 (46401)**	During the deployment process of SecureSphere Open Virtualization Format, the VMware vSphere may show warnings. Workaround: When the following message occurs: "The OVF package is valid but consider the following warnings. ", click Yes and continue the installation process. At the end of the process, the machine will be installed successfully. If you expect that the settings of network device should differ from the settings of VMXNET 3, configure it manually.

Table 2 Release 10.5 Known Issues

	ID	Description
47	**SPHR-41850**	Platform: When installing the Aug. 2013 patch, warning messages regarding securesphere.kst are displayed but are the result of design changes and can be ignored.
48	**SPHR-42590**	Hardware - All Products: Running the poweroff command With X2500, X4500, X6500, and M160 appliances results in system halt, not shutdown.
49	**SPHR-42847**	Hardware - All Products: Pressing the power button on appliance X2500, X4500, X6500, and M150 appliances immediately shuts down SecureSphere, which may result in data corruption.
50	**SPHR-46168**	Software Updates - Agents: Following failed installation manager self-update and failed rollback, Rollback or Install options appear even though they are not available. Workaround: Access machine on which agent is installed and manually install the new installation manager.
51	**SPHR-47090**	All Products: SecureSphere 32 bit onebox may crash in rare instances when using a U2P plugin.
52	**SPHR-47215**	Online Help: In some browsers, opening the online help may take a few moment and temporarily may not be optimally displayed. Workaround: recommended to use Firefox browser for viewing help.
DB Agent Related Issues		
53	**AGIM-2**	Agent Installation Manager: Installing package to a network drive is not supported. Workaround: Install in a local folder.
54	**AGIM-10**	Agent Installation Manager: When installing an agent and setting the download location to a folder missing the required permissions, no error is displayed.
55	**AGIM-13**	Agent Installation Manager: Folder names with special characters are not supported for package download.
56	**AGIM-23**	Agent Installation Manager: Cannot install agent or installation manager to folder with non-latin based characters.
57	**AGNT-994 (14325)**	Solaris 10 (Zones): The SecureSphere Agent encapsulates inter-zones traffic, which means that the inter-zone traffic will appear as local traffic.
58	**SPHR-18650 (21296)**	Solaris 10: Unclear status information in data interface channel when working with zones.
59	**AGNT-1517 (21371)**	Exclusions: Time of day criteria does not work properly.
60	**AGNT-1587 (22300)**	DB2: When two DB2 data interfaces (local and external) are configured, TCP external traffic is intercepted on both interfaces, resulting in doubled data on audit.
61	**AGNT-329 (22599)**	A network exclusion can be configured for the loopback address (127.0.0.1) even though they are not supported.
62	**AGNT-1770 (24079)**	The SecureSphere Agent's bootstrap.xml file is updated with internal IP address when the gateway is behind a NAT device. To work around this issue, you need to manually edit the agent bootstrap.xml file.
63	**SPHR-21352 (24589)**	Agent HA: After removing a gateway through the GUI, the SecureSphere Agent cannot be re-registered to the gateway until it is unregistered from both gateways.
64	**AGNT-331 (23124)**	Windows 2000 - MSSQL: Autodiscovery does not discover TCP interfaces.

Table 2 Release 10.5 Known Issues

	ID	Description
65	**AGNT-3512 (37083)**	DB Agent: Windows 2000 - User shown in audit as "local access user" in MSSQL2000 on TCP local and loopback interfaces.
66	**AGNT-3589 (37989)**	DB Agent: When Agent was installed in non-default directory, the silent installation logs were still written to the default directory (/opt/imperva/ragent/etc).
67	**AGNT-376 (38969)**	DB Agent - MSSQL: Data being written to pcap file is not audited while the MSSQL certificate is being modified.
68	**AGNT-3699 (39492)**	DB Agent: During Agent registration, if the user does not enter a site name, he is still asked to enter a server group name.
69	**AGNT-3716 (39721)**	DB Agent: The Agent cannot be registered to a site/service/server group whose name includes Hebrew characters. Workaround: Use only English-language characters for site/service/server group names.
70	**SPHR-36833 (41048)**	DB, File and SharePoint - Agent: The "Source Restriction" option is supported for Gateway monitoring but not for Agent monitoring.
71	**AGNT-3987 (41818)**	DB Windows: An Agent cannot be restarted for 10-12 seconds after it is stopped.
72	**AGNT-4002 (41975), AGNT-4073 (42770)**	DB NIX: SSL encrypted local DB connections are not monitored by the DB agent, relevant for Oracle and MYSQL.
73	**AGNT-4105 (43149)**	DB Agent cannot be installed by local admin user.
74	**AGNT-4148 (43583)**	DB: The Solaris Agent is not able to monitor the IXGBE TCP data channel out of the box. Workaround: run the following command: ln -s /devices/pseudo/clone@0:ixgbe / dev/ixgbe.
75	**AGNT-4482 (46060)**	Windows Agent: When configuring TCP external data interface, the configuration fails. Relevant for Windows Itanium. Workaround: • Delete the external interfaces. • In SecureSphere versions 9.5 and later for Win 2008, configure the support for external traffic in Kernel.
76	**AGNT-4495 (46159)**	NIX: When a SHELL script does not contain the interpreter declaration header, "Process Details" Agent Monitoring Rule does not work in AIX.
77	**SPHR-40304 (46324)**	As/400agent: In Log Collector, in case there is a running agent and the customer tries to add an in-product application journal to the list of in-product applications monitored by the Agent, the following action needs to be done: 1. In Setup > Sites, select the relevant service. 2. Clear the Enable checkbox under the relevant log collector settings. 3. Save the configuration. Wait for 1 min for configuration to be applied. 4. Select the Enable checkbox and click Save.
78	**AGNT-4416 (45597)**	When running agent CLI in the interactive mode on the server machine, it is impossible to see the SecureSphere Agent status. Relevant for all the NIX agents. Workaround: Check if **`/tmp`** is not full, if it is full, free some disk space.

Table 2 Release 10.5 Known Issues

	ID	Description
79	**SPHR-46799**	Agents: When moving an agent while the installation manager is not available, the move operation fails. Workaround: move the agent back to the original gateway, the try the move again.
80	**AGNT-5150**	DB Windows: In-line mode is not supported when working with DB2 Shared Memory.
81	**AGNT-5242**	Solaris: After installing the agent on server with Solaris 5.11 Update 1, some system services stop functioning. Workaround: Install the latest patch for Solaris 5.11 update 1.
82	**AGNT-5657**	DB2 Windows: In some cases, DB2 agent monitoring rules with long paths are truncated, resulting in the rule not being matched and traffic not being excluded. Workaround: Use a suffix that is short, one directory.
83	**AGNT-5723**	DB Windows: In some cases, when installing an agent using silent mode, error messages are displayed, requiring manual intervention in the installation. This also applies to installation via Software Updates.
84	**AGNT-5773**	DB AIX: Installing the v10.5 agent on AIX 5.2 fails when the .libc file is not updated. Workaround: Install a .libc file version 9.0.0.12 or newer.
85	**AGNT-5782**	DB HPUX: The database server crashes if the flag for remote-login-ip-enabled is set to true.
86	**AGNT-5827**	DB Informix: In order to monitored external traffic with EIK enabled, set the parameter kernel-socket_handoff-enabled to true.
87	**AGNT-5835**	DB: Attempting to grade agents that are stopped and not registered fails and an error is displayed in Software Updates. Workaround: Register unregistered agents before performing agent upgrade.
88	**AGNT-5838**	NIX Agents: FAM agent can be upgraded to v10.5 on NIX platform even though its not supported. Workaround: Disable FAM monitoring on the agent before upgrading it to v10.5.
89	**AGNT-5844**	Agent Windows: In some cases when working on Windows 2000 using BEQ, users appear in audit data as "Connected User." Workaround: In the Advanced Configuration pane of the agent in SecureSphere, add the following: <monitor-oracle-beq-in-server>1</monitor-oracle-beq-in-server>.
File Agent Related Issues		
90	**SPHR-35339 (38813)**	SharePoint Agent: In Forward Compatibility mode, the SharePoint Agent version must be the same as the MX version (though not as the gateway version).
91	**AGNT-4862 (43173)**	SharePoint Agent: WSS is not supported.
92	**AGNT-4872 (43549)**	Directory Service Agent: When using Powershell, the client's IP address is shown as 0.0.0.0 or 127.0.0.1 rather than the actual IP address.
File Related Issues		
93	**SPHR-21014 (24137)**	In Main > Setup > Sites > Definitions Direct Access Information, Samba connections for Windows are supported through SSH connections. Connections work although test connection shows an error.
94	**SPHR-30255 (31856)**	If the Advanced File Location match criteria is defined with a hostname, there is no match when the event specifies the IP address, and vice versa. Workaround: Add IP and host name as two different match criteria to protect them both.

Table 2 Release 10.5 Known Issues

	ID	Description
95	SPHR-36833 (41048)	The source restriction option in the server group does not work with the Agent.

4. Resolved Issues

The following table lists some of the issues resolved in the SecureSphere 10.5 release.

Table 3 Release 10.5 Resolved Issues

	ID	Description
Web Related Issues		
96	**SPHR-31783 (33958)**	When configuring a Web Custom (Service or Application) Policy with the 'Violations' criteria, and selecting the violation 'Bot Activity' in the criteria, the policy isn't invoked by the Bot Alert of type 'Non Browser Access,' though it is invoked with alert types 'Corrupted Data (Response)' and 'Corrupted Data (Cookie).'
97	**SPHR-34033 (36989)**	KRP - SSL: In MX-Gateway communication, DHE ciphers do not function correctly with TLS 1.2.
98	**SPHR-34075 (37042)**	KRP - SSL: Web Fraud Detection -- When using Chrome or Firefox, the gateway failed to obtain the provider's status because the certificate was self-signed and not certified.
99	**SPHR-36331 (40182)**	Fraud Protection: If two invocation policies are configured for the same URL, one of them modal and the other non-modal, only one is invoked. Workaround: Applying a modal policy and a non-modal policy on the same URL causes unpredictable results, and there is no benefit in applying both on same URL. The user should evaluate and decide which mode works best.
100	**SPHR-36730 (40850)**	Fraud Detection: If a service is configured to "Run on Every Request," and a static URL such as *.ico file is configured under the Match Criteria, then in certain cases there is the possibility of the policy invocation entering a loop.
101	**SPHR-37000 (41351)**	The Fraud Prevention Service does not invoke on non UTF-8 response pages. Workaround: If the string after which you place the snippet is composed of regular Latin characters (including digits and punctuation), snippet injection will work perfectly and FPS policy will invoke on UTF-8 pages. This includes the <head> and <body> tags.
102	**SPHR-38431 (43607)**	When SecureSphere is deployed behind the trusted Proxy and X-Forwarded-For is enabled, then if requests do not contain X-Forwarded-For headers, the IP Block followed action is disabled.
Database Related Issues		
103	**SPHR-15038 (17208)**	Scheduled reports are not created when Audit fast viewing task is running.
104	**SPHR-33539 (36259)**	DB Assessment: The Assessment test "Latest CPU Security Patch not Installed" fails on Oracle version 10.1.0.4 because this Oracle version is old and the examined DB table sys.registry$history does not exist in this Oracle version.
SecureSphere Management Issues		
105	**SPHR-40514 (46608)**	Server DB: When selecting columns for Audit data view, the user defined fields are not displayed with their specific names.
106	**AGNT-3991 (41850)**	All Products: During the upgrade process, as a result of change in the SecureSphere.kst file, a warning message appears, notifying that new SecureSphere.kst and bootstrap.properties files were created. The warning is meaningless and should be ignored.

Table 3 Release 10.5 Resolved Issues

ID		Description
107	**SPHR-9681 (10782)**	Loading a key for archive encryption lower than 1024 is not allowed. Error is received if trying to load it.
Agent Related Issues		
108	**AGNT-4588 (46824)**	Agent fails configuration in case it is registered to monitor both, Directory Service agent and DB agent and Directory Service monitoring rules are configured.
SharePoint Related Issues		
109	**SPHR-39643 (45372)**	SharePointRevoke group assignments permissions fails.
Platform Related Issues		
110	**SPHR-40296 (46300)**	X1010/X2010 Gateway Appliances: A “Detected Hardware Unit Hang” message may be displayed on the appliance console or in the **/var/log/messages** file when you: • Connect or disconnect network cables • Run **ifconfig** up or down commands Workaround: You should ignore the message.

5. Obtaining the Latest Image Files

To obtain the latest image files:

The ISO files of this version of SecureSphere are located on the Imperva FTP site ftp-us.imperva.com, under:

Edition		Location
SecureSphere Physical Appliance	**32 bit**	**`/Downloads/SecureSphere_Setup/v10.5/32Bit/USB/`**
	64 bit	**`/Downloads/SecureSphere_Setup/v10.5/64Bit/USB/`**
SecureSphere Virtual Appliances	**32 bit**	**`/Downloads/SecureSphere_Setup/v10.5/32Bit/VM/`**
	64 bit	**`/Downloads/SecureSphere_Setup/v10.5/64Bit/VM/`**



Note:

- On physical appliances with less than 4GB of RAM, install the 32 bit version.
- On all other physical appliances, install the 64 bit version.
- The same guidelines apply to SecureSphere VM installations, based on the RAM allocated to the SecureSphere virtual appliance. For SecureSphere VM installation instructions, refer to the SecureSphere Virtual Appliance Quick Start Guide.

1. Download and install on a USB drive. For instructions on preparing a USB for SecureSphere installation, see the **SecureSphere Administration Guide**.

   Hash values for the iso files are available on the FTP site in **`md5sums.txt`**
2. When installing a distributed environment (e.g., SecureSphere management Server and SecureSphere Gateway on different platforms), install the SecureSphere management server before installing the gateways.

6. Installing the SecureSphere Software

This section reviews how to install the SecureSphere software.



Notes:

- If you are a File, SharePoint or Directory Services Monitoring user, follow the below procedure, then install the v10.5 **patch 1** or higher. Until you apply patch 1, functionality for these products will not be available.
- FAM v10.5 Agent will only be compatible with SecureSphere v10.5 patch 1.

The following appliances are available for SecureSphere 10.5:

- G Series Appliances (Except G2 and G2-2) on page 19
- G2 and G2-2 Appliances, see the ***SecureSphere Administration Guide***.
- X and M Series Appliances on page 21

6.1 G Series Appliances (Except G2 and G2-2)

6.1.1 Installation Monitoring

Before you begin, connect either a serial or VGA device. The factory-installed default is VGA.

For information about connecting a serial console, see Connecting to the G Series Appliance Using a Serial Console on page 20.

6.1.2 Installing From USB



Note: For instructions on how to prepare a USB to install SecureSphere, see the SecureSphere **Administration Guide**.

To install from a USB device:

1. If there is a disk in the CD drive, remove it.
2. Turn off the appliance.
3. Plug a USB flash drive with the SecureSphere recovery image into the appliance USB port.
4. Boot the appliance and press the F2 key to enter the BIOS.
5. Go to **Boot Options**.
6. Set **Boot Option #1** to **CD**.
7. Set **Boot Option #2** to **RAID**.
8. Set **Boot Option #3** to **GE**.
9. Set **Boot Option #4** to **ERI Shell**.
10. Set **USB Boot Priority** to **Enabled**.
11. Save and exit the BIOS.
12. Turn off the appliance.
13. Plug a USB device with the SecureSphere recovery image into the appliance USB port.
14. Connect to the appliance using a keyboard and VGA or serial monitor.

    For information about connecting a serial console, see Connecting to the G Series Appliance Using a Serial Console on page 20.
15. Turn the appliance on.

16. After the appliance boots, select the VGA output installation option.

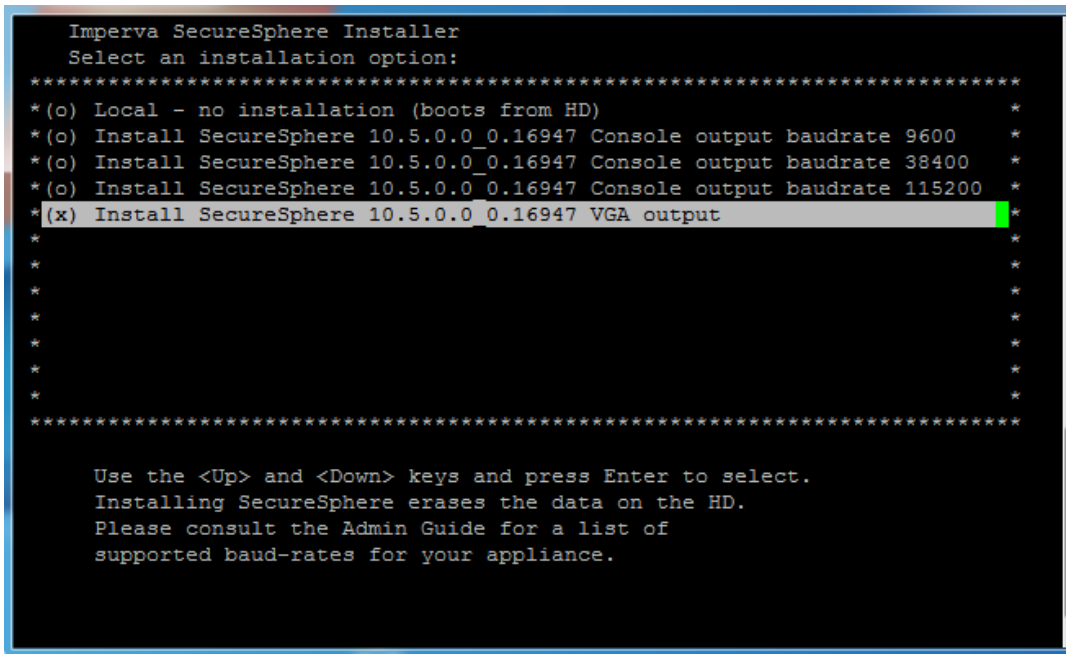


Figure 1 Installing from USB

17. Remove the USB key after the installation is complete.

Note: If you do not remove the USB key, you will be unable to use SecureSphere when the appliance is rebooted.

6.1.3 Connecting to the G Series Appliance Using a Serial Console

To connect to the appliance using a serial console:

- Connect a computer or a terminal to the serial port on the gateway using a serial cable. If you are using a program such as Hyperterminal™, configure the serial console settings as follows:

Table 4 Serial Console Settings

Setting	Value
Baud rate	9600, 38400, or 115200
Data bits	8
Parity	none
Stop bits	1
Flow control	none
Terminal emulation	VT-100 or VT-UTF8

Note: Some terminal emulators correctly interpret the Backspace key to delete the previous character from the stream sent to the application as well as from the displayed text, while others send a control sequence, so that the stream the application sees is different from the displayed text. You should determine the behavior of your terminal emulator before using the Backspace key.
In Hyperterminal, you can avoid this problem by using the DEL option.

6.2 X and M Series Appliances

6.2.1 Connecting to an X or M Series Appliance Using a Serial Console

To connect to the appliance using a serial console:

- Connect a computer or a terminal to the serial port on the appliance using a serial cable. If you are using a program such as Hyperterminal™, configure the serial console settings as follows:

Table 5 Serial Console Settings

Setting	Value for models: X1000, X2000, X2500, X4500, X6500, M100, M150	Value for models: X1010, X2010, M110
Baud rate	38400	9600
Data bits	8	8
Parity	none	none
Stop bits	1	1
Flow control	none	none
Terminal emulation	VT-100 or VT-UTF8 (supports colors)	VT-100 or VT-UTF8 (supports colors)

6.2.2 Installing From USB



Note: For instructions on how to prepare a USB to install SecureSphere, see the SecureSphere **Administration Guide**.

1. Turn off the appliance.
2. Plug a USB device with the SecureSphere recovery image into the appliance USB port.
3. Connect to the appliance using a serial console (see Connecting to an X or M Series Appliance Using a Serial Console on page 21).
4. Power on the appliance.
5. After the appliance boots, select the installation option for your model.
   - For X1000, X2000, X2500, X4500, X6500, M100, and M150, select:

     `Install SecureSphere version_number Console output baudrate 38400`. See Figure 2.

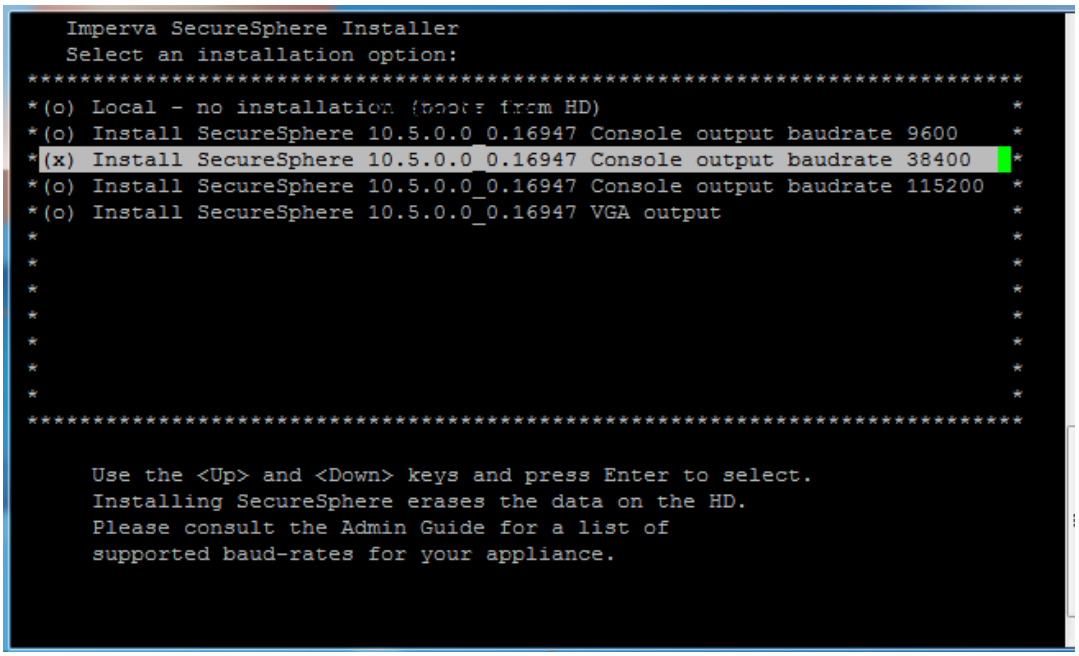


Figure 2 Installing from USB - Baud Rate 38400

   - For X1010, X2010, and M110, select:

     `Install SecureSphere version_number Console output baudrate 9600`.