IMPERVA®

# SECURESPHERE®

## Release Notes

v11.5 Patch 6
January 2016

www.imperva.com

# Copyright Notice

© 2015 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. 7,640,235, 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.

**Imperva Inc.**

3400 Bridge Parkway, Suite 200

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

Imperva-SecureSphere-v11.5-Release-Notes-Patch-6-v3

# Release Highlights

## Database Security

### SecureSphere Database Security on AWS

SecureSphere Database Security on AWS is now available on Amazon Web Services (AWS). Starting with version v11.5, SecureSphere customers can monitor, audit, and protect databases deployed on Amazon Web Services. Database Security on AWS can be deployed as an Elastic Compute Cloud (EC2) AMI and supports easy and quick deployment using AWS CloudFormation templates. It delivers all the benefits of the on-premises SecureSphere Database Activity Monitoring (DAM) and Database Firewall (DBF), thereby allowing enterprises to enjoy the same security level for their cloud based deployments as they do in their physical data centers.

### Big Data

- **New big data support**:
  - **Hadoop Distribution**: SecureSphere now supports IBM BigInsights.
  - **MongoDB**: SecureSphere now supports the auditing and protection of MongoDB databases.
  - **HDFS**: SecureSphere now supports the Hadoop Distributed File System (HDFS) Service with BigInsights, Hortonworks and Cloudera distributions.
- **Separate Licensing**: Starting in 11.5, the SecureSphere Agent for Big Data is licensed separately.

### Discovery and Assessment Server (DAS)

- **DAS Automation APIs**: A set of new APIs has been added, enabling the configuration of SecureSphere DAS options via the API, and the automation of their configuration. These new APIs enable editing database connections, OS connections and database tags.
- **Database Connection Tags**: The ability to tag database connections has been added, allowing the association of databases or database tags to scans so scans are automatically run on tagged resources.
- **Scan Based Tags**: More than one policy may now be associated with a scan by adding the relevant tags to the scan.
- **Automatically Applied Policies**: Audit and security policies can be configured so they are applied automatically when new services are added in SecureSphere.
- **Windows OS Assessments**: A new connection mode – CIFS RPC, was added to database assessments for Windows OS assessments.

### Gateway Cluster

- **Additional Cluster Dual Network Topologies**: Users can configure a cluster in a dual topology so that the management server is either on the agent network, or on the cluster network.
- **Cluster Multiple Hardware Types**: Clusters now support mixing new generation hardware (e.g. x4510) with previous gateway models (e.g. x4500) in a single cluster.
- **Agent Bulk Move within Cluster**: A number of agents can be moved within a cluster without data loss.

## General Database Enhancements

- **Splunk Integration**: SecureSphere now supports exporting audit data via the syslog interface to Splunk. Enterprise customers may use Splunk to conduct advanced analytics on data generated by SecureSphere together with data collected from other enterprise systems. Customers who want to use the Splunk Integration must download and install the SecureSphere patch for v11.5 located on the Imperva FTP to fully enable this feature.
- **Database Audit Report Scalability**: SecureSphere audit reporting performance has been improved for deployments with very large scale auditing requirements.

## SecureSphere Agents - GA

- **Windows 2003 Inline Monitoring and Blocking for MSSQL Databases**: SecureSphere Agents for database on Windows now supports inline monitoring and blocking on Windows 2003 servers for MSSQL databases on the following Channels: TCP Local and TCP Remote.
- **Informix Shared Memory (SHM)**: SecureSphere now supports Shared Memory on IBM Informix v11.5 database management systems running on AIX.
- **Oracle Network Data Encryption (NDE, also known as Oracle ASO)**: SecureSphere Agents for database now support Oracle Network Data Encryption for Oracle 11.1, 11.2 and 12.1 on RHEL 5 and 6. Supported interfaces include External and Local TCP, and BEQ. This feature is disabled by default. Contact support for instructions on enabling it.
- **Directory Services Agent**: SecureSphere Agents now support SecureSphere Directory Services Monitoring on the Windows 2012 R2 operating system.
- **SUSE Enterprise Linux 12**: SecureSphere Database Agents now support SUSE Enterprise Linux 12.

# Web Application Security

## SecureSphere ThreatRadar Account Takeover

ThreatRadar Account Takeover Protection helps businesses protect against hackers looking to compromise website user accounts. ThreatRadar Account Takeover includes the following protections:

- **Device Intelligence**: Recognizes new and returning devices logging into your web application. SecureSphere admins can identify and block malicious site visitors authenticating to your website to prevent account takeover, which could result in fraud or loss of intellectual property.
- **Privileged Account Brute Force**: Detects brute force attacks on privileged web application accounts, and puts controls in place to block this unauthorized access.
- **Credential Stuffing**: SecureSphere maintains a protected database of compromised credentials from data breaches. It detects credential stuffing attacks by identifying repeated failures from IP addresses requesting access to various user accounts, and identifies if compromised credentials were used in gaining access to a website.
- **Dictionary Attack**: SecureSphere maintains a list of weak and common passwords, which is constantly updated by the Imperva Active Defense Center (ADC). When SecureSphere encounters repeated, failed logins with credentials using weak passwords tracked by Imperva, the action is considered risky and is blocked by SecureSphere.

## ThreatRadar Bot Protection Services: CAPTCHA Challenges

SecureSphere ThreatRadar Bot Protection Services users can now add CAPTCHA challenges to different areas of a website, helping to distinguish legitimate users from automated traffic. SecureSphere uses the simplified "No Captcha reCaptcha" implementation.

CAPTCHA challenges can be triggered when abnormal non-human activity is observed by the SecureSphere Web Application Firewall, or can be used in conjunction with SecureSphere ThreatRadar Bot Classification.

## Hybrid Mode on AWS

Users can now have Gateway servers on AWS working with On-Premise Management Servers (MX and SOM) in the data center. Users interested in activating hybrid mode must download and install a SecureSphere patch to enable this capability. Those not interested in this capability should not use this patch. Please contact support for assistance.

## Web Automation (APIs)

A set of new APIs has been added enabling the configuration of SecureSphere web options via the API and the automation of their configuration. These new APIs enable the configuration of IP groups, firewall policies, web application signature policies, and web signatures.

## HTML 5 WebSocket Compatibility

SecureSphere now enables users to decide whether or not to block or issue alerts on WebSocket connections.

# Platform and Management

## New SSL Ciphers

SecureSphere support for SSL Ciphers is enhanced with the addition of TLS RSA ciphers for WAF reverse proxy and bridge modes and DAM, as well as new TLS Diffie-Hellman and ECDHE ciphers for WAF reverse proxy mode.

## IE 11 Support

The list of browsers supported by SecureSphere has been updated to include Microsoft Internet Explorer 11.

## MX-HA on AWS

A CloudFormation Template file is now available that allows the AWS deployment of a Management Server with full High Availability.

## MX-HA Maintenance

The MX-HA capabilities of SecureSphere offer new IMPCTL commands that facilitate the ongoing maintenance of SecureSphere. With these commands you can stop and start the entire MX-HA environment, change physical and virtual IP addresses, and change management and database passwords.

## Security – Old Key Support

SecureSphere Key Management was enhanced to support the regeneration and transfer of the default encryption and signature keys. This assists with importing audit data that was previously archived from SecureSphere back into SecureSphere.

# Patch 4 Additions

## Updated Database and Big Data Support

SecureSphere now offers support for the following updated database and big data versions:

- MySQL 5.6
- Netezza 7.0 through 7.2
- Cloudera 5.4.5
- MondgoDB 3.0.6 and 3.0.7
- Teradata 15.1

## Enhanced Classification Support

SecureSphere now supports data classification on Teradata, Netezza, Postgre, Progress and DB2 on zOS databases.

# Database Support

This version of SecureSphere supports the following databases:

**v11.5 Supported Databases**

| Database | Supported Database Versions |
|---|---|
| **DB2 LUW** | 7.2, 8, 9, 9.5, 9.7, 10.0, 10.5 |
| **Informix** | 7.31, 9.x, 10.x, 11.0-11.5, 11.7, 12.1 |
| **MS-SQL** | 7, 2000, 2005, 2008, 2008 R2, 2012, 2014 |
| **MySQL** | 4.1-5.9 |
| **Netezza** | 4.x, 5.0, 6.0, 7.0- 7.2 |
| **Oracle** | 8i, 9i, 10g, 11g, 12c |
| **Sybase ASE** | 11.9, 12.0, 12.5.x, 15.0-15.7 |
| **Sybase IQ** | 12.5, 12.6, 12.7, 15.0-15.4 |
| **Progress Openedge** | 10.1c, 10.2a, 10.2b, 11.3 |
| **Teradata** | 2.6, 12, 13.0, 13.1, 14, 14.1, 15.0, 15.1<br>**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 - 9.3 |
| **IMS for z/OS** | 11, 12, 13 |
| **DB2 for z/OS** | 10, 11 |

**v11.5 Supported Big Data Distributions**

| Distribution | Supported Distribution Versions | Supported Services |
|---|---|---|
| **Hadoop - Cloudera** | 5.1.0, 5.1.2, 5.3.0, 5.3.1, 5.4.5 | Hive, HBase, HDFS |
| **Hadoop - Hortonworks** | 2.1.1, 2.1.3, 2.1.5, 2.2 | Hive, HBase, HDFS |
| **Hadoop - IBM BigInsights** | 2.1.2, 3.0.0 | Hive, HBase, HDFS |
| **MongoDB** | 2.4, 2.6.5, 2.6.6, 3.0.6, 3.0.7 | MongoDB |

# Known Issues

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-21352** | 24589 | All products - gateway | 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. |
| **SPHR-53874** | | All products - gateway | Gateway performance profiling may cause major performance degradation. On virtual gateways the gateway profiling feature was disabled. |
| **SPHR-56910** | | All products - gateway, Web | In bridge mode, when blocking an SSL connection after negotiating the GCM ciphers, the Error Page sent by the gateway may be incorrectly encrypted. If this happens, a web browser may terminate its connection with an SSL error or endlessly wait for a response. |
| **SPHR-14189** | 16166 | All products - management | 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. |
| **SPHR-17221** | 19669 | All products - management | Lookup data sets: The last inserted row cannot be edited if it is close to the bottom of the page. |
| **SPHR-17788** | 20308 | All products - management | SIEM: Action sets - Audit - If a secondary host is defined, then UDP should not be available as an option for the protocol. |
| **SPHR-21014** | 24137 | All products - management | 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. |

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-29683** | 31071 | All products - management | The archived .mprv (e.g. SysEvents, Reports) files are encrypted by default. When trying to unpack, the decryption process fails.<br>Workaround: This issue can be solved by adding the following unpack command:<br>keystore /opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kstto |
| **SPHR-29734** | 31126 | All products - management | 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. |
| **SPHR-3894** | 4144 | All products - management | System events privileges are not enforced. |
| **SPHR-52218** | | All products - management | Limitation: Safari browsers are only supported on clients running Mac OS and not Windows. |
| **SPHR-55043** | | All products - management | Notification that MX Server name was populated from SOM is missing. |
| **SPHR-55865** | | All products - management | When running full export from one MX and importing into another MX the prompt to upload a new license is skipped and the MX is left in an "invalid license" state. Workaround: Go to Admin > Licensing > Action > Upload License File and upload a new license file. |
| **SPHR-22432** | 23094 | All products - platform | When installing from a USB drive, the final screen presents that centOS was installed instead of SecureSphere. |
| **SPHR-29940** | 31401 | All products - platform | All products - platform: Failover fails when gateways 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. |
| **SPHR-42847** | | All products - platform | 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. |
| **SPHR-47733** | | All products - platform | Hardware - All Products: Running the poweroff command results in system halt, not<br>shutdown. Impacted appliances include M160, X2510, X4510, X6510, X8510 and<br>X10K. |
| **SPHR-53221** | | All products - platform | When configuring Posix Time zone using impcfg to GST time zone, SecureSphere refers to GST as GMT, though the GST definition is UTC+4. |
| **SPHR-15069** | 17239 | DB | Risk Explorer: Multi-byte character sets are not properly displayed. |
| **SPHR-17493** | 19973 | DB | DB Agent Central Management: Setup > Agents > General Information > Gateways, Gateway might appear as Active although it is disconnected. |

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-18193** | 20778 | DB | 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. |
| **SPHR-18577** | 21214 | DB | Data Discovery: Content based search returns incorrect results for tables with fewer than 200 records or tables whose first 200 records include NULLs. |
| **SPHR-18650** | 21296 | DB | Solaris 10: Unclear status information in data interface channel when working with zones. |
| **SPHR-30333** | 31954 | DB | Migration: The Log Collector password does not survive the upgrade. |
| **SPHR-35455** | 38981 | DB | URM: Users are incorrectly identified as hashed users when MSSQL is used with Kerberos encryption algorithms not supported by SecureSphere. |
| **SPHR-36999** | 41350 | DB | Migration: After upgrading, loaded audit archive is missing from the DB Audit Data screen.<br>Workaround: Reload the archive data after upgrading. |
| **SPHR-44380** | | DB | Gateway Cluster: After configuring Selected Columns in the cluster window, then moving to another screen, the column selection is not preserved. |
| **SPHR-45639** | | DB | 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. |
| **SPHR-45673** | | DB | Gateway Cluster: In some cases, gateway failover may result in loss of data. |
| **SPHR-45790** | | DB | Gateway Cluster/Agent: When agent move fails, no description is given in resulting system event. |
| **SPHR-45848** | | DB | Limitation - Gateway Cluster: Screen data doesn't refresh when moving between tabs. Workaround: click the Refresh button. |
| **SPHR-47052** | | DB | Gateway Cluster/Agent: Configuring an agent while being moved results in a failed partial configuration and gateway failover. Workaround: don't move an agent in the process of configuration. |
| **SPHR-51037** | | DB | Retrieving audit event data may fail once after first time installation of the management server.<br>Workaround: Close the popup window and retrieve the data again. |
| **SPHR-51993** | | DB | When moving an agent between gateways in a cluster, the source gateway shown in the system event is wrong. |
| **SPHR-55098** | | DB | Limitation: Cannot establish a database connection with MSSQL databases when SSL is required as jTDS does not support SSL connections to SQL Server 2008 R2. |
| **SPHR-55274** | | DB | Lookup data set search doesn't capture events when using the "Database" criteria. |

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-55345** | | DB | When using a Gateway Syslog action interface with the TCP protocol, the secondary syslog server may not receive the events if the primary server is down. |
| **SPHR-55349** | | DB | Agents may indicate wrong status for few seconds after being moved between gateways. |
| **SPHR-56832** | | DB | When working with Netzza databases, the Schema column in audit may be empty if no "SET SCHEMA" command executed. |
| **SPHR-30255** | 31856 | File | 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.<br>Workaround: Add IP and host name as two different match criteria to protect them both. |
| **SPHR-36833** | 41048 | File | DB, File and SharePoint - Agent: The "Source Restriction" option is supported for Gateway monitoring but not for Agent monitoring. |
| **SPHR-21099** | 24247 | DB | Track Changes active module Registry Key object type is displayed in the GUI, even though it's not supported. |
| **SPHR-32625** | 35056 | DB | DB2 URM - Active Directory Forest Configuration is not supported. |
| **SPHR-35339** | 38813 | SharePoint | SharePoint Agent: In Forward Compatibility mode, the SharePoint Agent version must be the same as the MX version (though not as the gateway version). |
| **SPHR-47215** | | All products - management | 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. |
| **SPHR-16044** | 18349 | Web | Limitation - Active Module: If a scanner_integration.jar is replaced, it takes effect only after the server is restarted. |
| **SPHR-22318** | 19171 | Web | Limitation: Web/DB correlation requires the query group to operate in the Static Protect mode in order to work properly. |
| **SPHR-56954** | | Web | Limitation: FPS is not supported in KRP mode when applying a policy configured in In-Transaction mode and the client-server connection is encrypted. |

# Resolved Issues

The following table lists some of the issues resolved in the SecureSphere 11.5 GA release. For a list of bugs resolved as a part of patches, see Patch Change Logs - v11.5 "Patch Change Logs" on page 17.

**v11.5 Resolved Issues**

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-53429** | | All products - gateway | Increased granularity of SSL untraceable violations to support required configuration of alerting and sufficient identification surrounding certain types of attacks. |
| **SPHR-41204** | 47657 | All products - management | When deleting a gateway group, the Management Server could become unresponsive. |
| **SPHR-56460** | | All products - management | After installation of either v10.5 Patch 14 or v11.0 Patch 4, should Get Tech Info be run, an upgrade to v11.5 might, on occasion, have failed. |
| **SPHR-54162** | | All products - management | Lookup data set data is incorrect when same attribute is used in more than one column |
| **SPHR-53712** | | All products - management | Couldn't import two certificates with same CA issuer. |
| **SPHR-53449** | | All products - management | Couldn't modify reports because add button in the Tabular tab of alerts report not working. |
| **SPHR-52930** | | All products - management | Quick search didn't work in the Violations screen. |
| **SPHR-52124** | | All products - management | A user not having an "Administrator" role failed to send sync request to the Package Repository in offline mode. |
| **SPHR-51944** | | All products - management | Could not sort audit jobs by last execution time. |
| **SPHR-51607** | | All products - management | MX-HA secondary server wouldn't respond due lack of disk space. |
| **SPHR-51201** | | All products - management | Importing a policy when attributes list was very long caused the Management Server to crash. |
| **SPHR-51085** | | All products - management | Syslog couldn't send information via a non-standard port. |
| **SPHR-49532** | | All products - management | After upgrading the Management Server to v10.0 and performing a configuration change in IMPCFG the gateway started disconnecting from the Management Server |
| **SPHR-47966** | | All products - management | Couldn't import exported server group into Management Server. |
| **SPHR-47631** | | All products - management | IP addresses in the database connections table were truncated when browser window wasn't fully expanded. |
| **SPHR-53859** | | All products - management, SOM | Large amount of entries in dataset sent from SOM to Management Server caused the MX to experience an out of memory error. |

| ID | Legacy ID | Product | Description |
|---|---|---|---|
| **SPHR-52535** | | All products - management, SOM | Re-registration of existing MX to SOM cause not synchronized MX state in SOM due to duplicate lookup data set. |
| **SPHR-46626** | | All products - management, Web | The Management Server only generated a single alert for events with multiple violations of the same type. |
| **SPHR-53764** | | All products - platform | MX-HA would failover to secondary server because of PCE memory leak. |
| **SPHR-53904** | | All products - platform | Error encountered when trying to configure Radius server as the result of a special character in the Radius password. |
| **SPHR-54067** | | All products - platform | Limited space in /var partition led to disk space issues in large environments, even though there was enough space on the disk. |
| **SPHR-54692** | | DB | URM scans fails to filter when MSSQL users had an extra space after their user name, or used a different letter case letter case in filter. |
| **SPHR-53739** | | DB | Gateway unexpectedly crashed when using the shutdown" / "poweroff command and agent tunnel compression was enabled. |
| **SPHR-52458** | | DB | Agent unexpectedly disconnected from the gateway for the period of a few minutes every few days. |
| **SPHR-51614** | | DB | Single quotes in custom assessment test name caused the 'edit test button' to become unresponsive. |
| **SPHR-51223** | | DB | Assigned channels were overridden by the auto-assignment feature resulting in the loss of manual configurations like disable/enable following upgrade. |
| **SPHR-50792** | | DB | Could not select lookup dataset of type "LDAP" when selecting "Application User." |
| **SPHR-50520** | | DB | Application user criteria doesn't work with enrichment application username. |
| **SPHR-50437** | | DB | Error message "Allocated space for audit data is full" was encountered even though there wasn't a problem with space for audit. |
| **SPHR-52261** | | File | When using a SharePoint only license, there were missing views in the Profile Overview tab. |
| **SPHR-51760** | | File | When the "Hours of the day" column was added, FAM event data was retrieved, and selected row was clicked, nothing was displayed. Additionally when all rows were clicked, only data for the current day was displayed. |
| **SPHR-50536** | | SOM, Web | Two Management Servers that had the same identifier on SOM caused their statistics information to be overridden in SOM. |

# Obtaining the Latest Image Files



**Note:** Starting with v11.0, SecureSphere only offers a 64 bit installation package.

**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 | Bit | Location |
|---|---|---|
| **SecureSphere Physical Appliance** | 64 bit | **/Downloads/SecureSphere_Setup/v11.5/64Bit/USB/** |
| **SecureSphere Virtual Appliances** | 64 bit | **/Downloads/SecureSphere_Setup/v11.5/64Bit/VM/** |

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.

# Installing the SecureSphere Software

The appliance is shipped from the factory with SecureSphere already installed on it. You can install a different version of SecureSphere on the appliance, or from a USB device, by following these instructions.



**Note:** SecureSphere v11.5 cannot be installed on X1000, G2 or 32 bit V1000 platforms.

This section contains the following information:

Connecting to a X or M Series Appliance Using a Serial Console 14
Installing X and M Series Appliances From USB 15
Creating a Bootable USB Device Containing the Installation Image 16

## Connecting to a X or M Series Appliance Using a Serial Console

**To connect to the appliance using a serial console:**

1. 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:

**Serial Console Settings**

| Setting | Value for models: X2000, X2500, X4500, X6500, M100, M150 | Value for models: X1010, X2010, X8510, X10K, 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) |

**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 Hypterterminal, you can avoid this problem by using the DEL option or Ctrl-H (delete character).

# Installing X and M Series Appliances From USB

**To install from a USB device:**

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 a X or M Series Appliance Using a Serial Console on page 14).
4. Power on the appliance.
5. After the appliance boots, select the required option, as follows:
   - Select the second installation option (baudrate 9600) for X1010, X2010, X2510, X4510, X6510, X8510, X10K and M110
   - Select the third installation option (baudrate 38400) for X2000, X2500, X4500, X6500, M100, M150

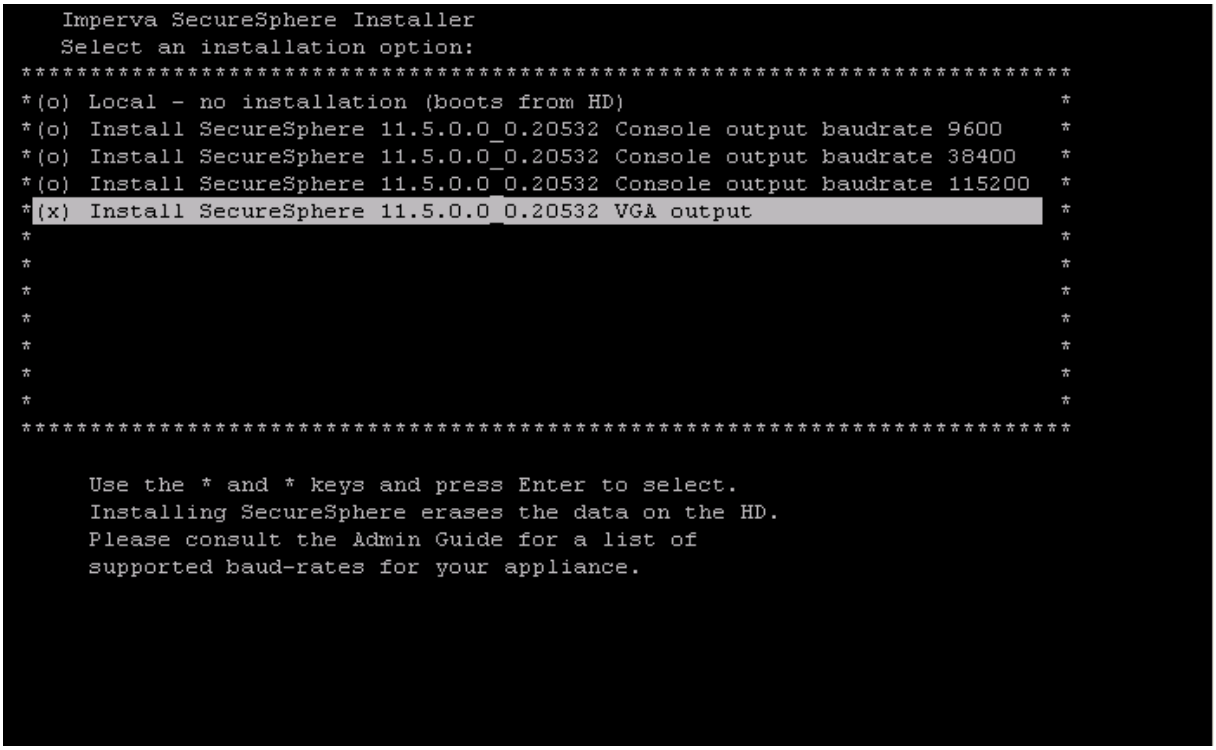



**Figure 1: USB Boot Menu**

# Creating a Bootable USB Device Containing the Installation Image

To install SecureSphere from a USB device, you must first create an image of the installation file on the device. You will need the following:

- A USB device (for example, a disk on key) with a capacity of at least 4GB.

**Note:** All data on the device will be erased, so back up the data before starting this procedure.

- Access to the Internet

**To create a bootable USB device:**

1. Download the image of the USB file from the Imperva FTP site.
   - **64 bit**: `/Downloads/SecureSphere_Setup/v11.5/64Bit/USB/`
2. Download and install the Image Writer for Windows executable file from the following URL:
   http://launchpad.net/win32-image-writer/ http://launchpad.net/win32-image-writer/
3. Attach your USB device to your computer.
4. Start the Image Writer for Windows application.

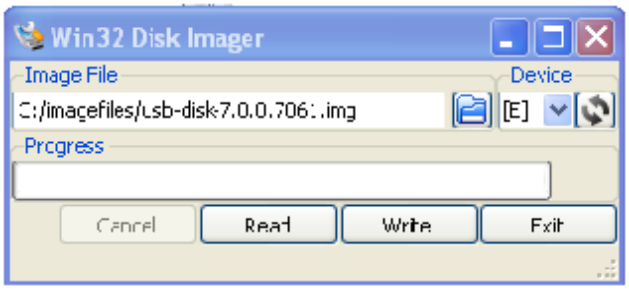



**Figure 2: Win32 Disk Imager window**

5. Under **Device**, select your USB device.
6. If your USB device is not listed under **Device**, refresh the list by clicking the icon to its right.
7. If the image file you downloaded in step 1 is not listed under **Image File**, browse to the image file you downloaded in step 1.
8. Confirm that **Image File** and **Device** are correct.

**Note:** Make sure you are not formatting the wrong disk, for example, your hard drive.

9. Click **Write**.

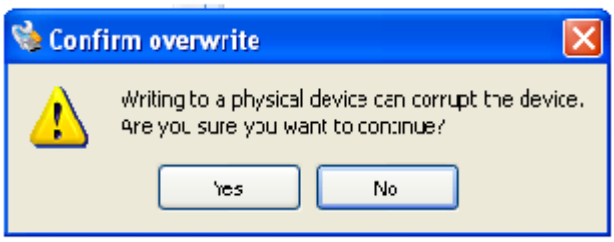



**Figure 3: Confirm overwrite window**

10. In the **Confirm Overwrite** window, click **Yes**.
11. After the image has been copied to the USB device, you can use it to install SecureSphere.

# Patch Change Logs

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


- Patch Bug Fixes on page 17
- Patch Installation Instructions on page 20
- MX-HA Installation Instructions on page 20


## Patch Bug Fixes

### Patch 6 - Release Date: 2015-12-20

SPHR-57195 All products - gateway, Web : In some cases, when TLS sessions in which both client and server indicated support for session resume via ticket IDs, SecureSphere was unable to recover a session when resume was initiated, resulting in not being able to parse the resumed session traffic (specific to Microsoft servers).

SPHR-57356 All products - platform: The patch reboot command was not available when SecureSphere Patch installation was terminated before completion.

## Patch 4 - Release Date: 2015-12-7

SPHR-57033 DB, Web: SecureSphere could not decrypt TLS connections as the result of a Microsoft Update that included support for a new RFC. This Microsoft Update impacted SecureSphere Gateways, both with WAF products in bridge/sniffing mode when protecting IIS servers, and with DAM products monitoring MSSQL. Users running Microsoft Windows servers patched with the MS15-121 Security patch (KB3081320) and using the above mentioned features are encouraged to install this patch. See this Support Knowledge Base article for details.

SPHR-54560 All products - gateway: The Gateway crashed when using a policy with a dictionary search criteria configured as Location=URLs And Parameters.

SPHR-55957 All products - gateway: Gateway crashed when enabling ssl supportability.

SPHR-56147 All products - gateway: Gateway crashed when handling Agent LSO packets.

SPHR-56181 All products - gateway: Gateway crashed when handling IP fragments

SPHR-56394 All products - gateway: Nzcounters were missing non-zero values that appear in counters.

SPHR-56584 All products - gateway: Gateway crashed after upgrading to v11.5, when an agent sent a channel ID that is not found in the Gateway configuration.

SPHR-56663 All products - gateway: The Gateway crashed when parsing SSL traffic with the GCM cipher.

SPHR-56958 All products - gateway: The Gateway crashed when seeing SSL traffic encrypted with the SHA384 cipher.

SPHR-54988 All products - management: Added the ability to enable up to 4000 Latin Characters in OS command parameters

SPHR-55433 All products - management: Unclear error messages appeared when deleting a lookup dataset which was used by other objects.

SPHR-55855 All products - management: Checksum mismatch encountered after upgrading from v9.0\9.5 to v11.5.

SPHR-56460 All products - management: After upgrading to August 2015 Patch, should Get Tech Info be run, an upgrade to v11.5 would on occasion fail.

SPHR-56583 All products - management: MX with memory larger than 16 GB did not log new alerts.

SPHR-55294 All products - management, SOM: MX-HA on AWS was not supported with the SOM running on premises (on customer's local network).

SPHR-57215 All products - management: Agent would consistently fail to register to the gateway. Additionally agent and gateway status that appeared in SecureSphere would not update.

SPHR-54428 All products - platform: AutoScaling thresholds were wrong in the CloudFormation templates.

SPHR-55326 All products - platform: Rebooting SecureSphere machine in the middle of patch installation caused a mixed version rpm base which prevented patch installation.

SPHR-56373 All products - platform: AWS CloudFormation templates change. Default SSH access is now limited to private networks (in security group cidr): 10.0.0.0/8 192.168.0.0/16 172.16.0.0/16"

SPHR-49485 DB: Source Application columns are populated with jobnames of dependent regions like BMPs, JBPs, IFPs, MPPs, JMPs.

SPHR-52363 DB: Scheduled database assessment scan occasionally failed if the scan applied to duplicated DB connections

SPHR-52541 DB: When filtering by "Pending Settings Activation" in Agents pane, agents that are configured with "Automatic" activation settings appears in the list although it shouldn't

SPHR-54536 DB: Loading the audit archive did not show the events, even though there were three events showing in Archive Management.

SPHR-54729 DB: When using privileged operation where we do not split the "DB Name" and "Table Name" in operation thus cannot show the correct "Database Name" in audit.

SPHR-54811 DB: Audit data with TLS encrypted MySQL traffic was not decrypted.

SPHR-54935 DB: Event duplication caused override of the Application User in audit data.

SPHR-55013 DB: Exclusion of search criteria that uses lookup data set and empty values for the 'OS Host Name' and 'Source Application' did not trigger the policy.

SPHR-55045 DB: Database User Group criteria did not trigger on non-profiled users when the operation is Exclude All.

SPHR-55238 DB: In Agents type reports, when a Server Group was selected as a Data Scope criteria, only the first configured server group would be matched in the report, i.e. data would be missing from the report.

SPHR-55308 DB: Management Server upgrade failed.

SPHR-55367 DB: When a query included characters such as '\\', '=', '\n', '\r', '\0', the gateway sent a ""normalized"" message to the Splunk server which included an additional backslash added to the message.

SPHR-55398 DB: SharePoint slowed down due to high Agent traffic utilization.

SPHR-55421 DB: A potential improvement to the number of discovered tables during MSSQL Stored Procedure Retrieval.

SPHR-55429 DB: Added a Lookup Dataset search criteria for Operating System User Chaining.

SPHR-55522 DB: In DB2 audit, the schema name was seen as database name.

SPHR-55562 DB: Gateway crashed when parsing Progress ABL traffic.

SPHR-55581 DB: Garbled (Japanese character) information in the alerts.

SPHR-55653 DB: Added: Debug messages regarding Duplicate Agent ID issue

SPHR-55867 DB: Gateway crashed when parsing Progress ABL traffic.

SPHR-55891 DB: Extremely long SQL request rule exceptions did not work.

SPHR-55925 DB: Gateway crashed when parsing Progress ABL traffic.

SPHR-55964 DB: Gateway crashed when parsing Progress ABL traffic and issuing "impctl gateway stop" command.

SPHR-56107 DB: Added the ability to see the User when failing to login to the database.

SPHR-56126 DB: Query "begin insert into" was missing in audit.

SPHR-56141 DB: Gateway crashed when parsing Progress ABL traffic after issuing "impctl gateway stop" command.

SPHR-56229 DB: DAM query was missing when working with SharePoint.

SPHR-56266 DB: Exported data was malformed when using Splunk Integration.

SPHR-56289 DB: There was a path traversal vulnerability in the “Params” parameter in the Functionality Manager / Capability Manager in the Gateways web interface, which could have been exploited by submitting a value that starts with a valid folder.

SPHR-56345 DB: LDAP authentication for the Log Collector was added.

SPHR-56472 DB: Audit Policy - Match Criteria with Enrichment Data was not working with empty values.

SPHR-56476 DB: Gateway crashed while parsing zOS agent traffic.

SPHR-56592 DB: Audit syslog was sent with a comma appearing after the ${Event.createTime} placeholder.

SPHR-53444 DB, All products - management, Web: Could not create PDF report on profile screen.

SPHR-54355 File: FAM URM and service discovery failed on NetApp.

SPHR-55076 File: A URM File Permissions report could not be saved with the correct Scanned Object.

SPHR-55834 File: URM scan did not run on Solaris with NFS, for local users.

SPHR-56416 File: SecureSphere allows partial success and enables Vampire debug prints in Kerberos key extractions.

SPHR-54955 SharePoint: Added the ability to let customers decide if the native audit collector process will be moved automatically/manually to another server in case of process failure.

SPHR-48449 SOM: The user could not add the Applied to Assets filter field to Security policies reports which SOM sent to the MX.

SPHR-55585 SOM: SOM upgrade failed due to report that has "Apply To Method" selected as part of DataScope.

SPHR-56516 SOM: SOM v10.5 was missing MySQL driver.

SPHR-52157 Web: The gateway was crashing after a v10.8 patch 8 installation due to JSON parameter.

SPHR-55094 Web: Multipart/chunked feature did not work properly.

SPHR-55285 Web: The "too many URL parameters" alert was being sent when it should not have been - even though the source IP address existed in the ignore IP list.

SPHR-55322 Web: Partial upgrade failure was encountered.

SPHR-55481 Web: The cookies returned by the ThreatRadar bot protection feature subsequently caused the web server to respond with an error, so the pages became unavailable.

SPHR-56031 Web: JSON parameter parsing issues.
SPHR-56039 Web: Bot Protection WhiteList was not available.
SPHR-56103 Web: Enhancement of best-effort blocking in sniffing mode.
SPHR-56137 Web: Error resulting from trying to add an exception on illegal response code with empty response code.
SPHR-56154 Web: FPS in transaction mode caused the web server to return HTTP status code "400 Bad request."
SPHR-56196 Web: Gateway crashed due to json parser issue.
SPHR-56235 Web: Gateway used first XFF header name, instead of list of header names causing missing trusted IPs in other header names.
SPHR-56307 Web: "Source GeoLocation" match criteria got stuck loading.
SPHR-56421 Web: Fewer API calls than expected were seen on the ThreatMetrix portal.
SPHR-56576 Web: Gateways in the AWS environment were being continually terminated.
SPHR-56717 Web: Gateway crashed when using Data Tampering with GCM ciphers.

## Patch 1 - Release Date: 2015-8-31

SPHR-56266 DB: Exported data was malformed when using Splunk Integration.

# Patch Installation Instructions



**Note:** For instructions on Patching AWS, see the AWS Configuration Guide.

1. Download the latest patch (and corresponding MD5 or SHA-256 file) from the FTP server **/Downloads/SecureSphere_Patches/V11.5/64Bit**
2. If you are unsure of your installation's bit size, type: uname -m
3. In Linux, run one of the following commands (Windows requires a third-party verification program):
   - sha256sum -c <binary file name>.sha256
   - md5sum -c <binary file name>.md5
4. Copy the patch to /tmp of the machine you want to patch
5. Change permissions by typing chmod +x [filename]
   For example: chmod +x SecureSphereV11.5.0-x86_64-Patch1_0.x
6. Run the patch by typing ./[patch filename]
   For example: ./SecureSphereV11.5.0-x86_64-Patch1_0.x
7. Reboot the machine only after receiving the message that the patch has been successfully installed.
8. Using the web GUI, download the ADC content file from the Imperva site and upload it to the system (Admin -> ADC ).

# MX-HA Installation Instructions

1. Login to the secondary MX and deploy the patch (BUT DO NOT REBOOT).
2. Login to the primary MX and deploy the patch.
3. Reboot the primary MX.
4. When the primary MX is up and running, reboot the secondary MX.

5. Deploy the patch on the gateway and reboot.