

SECURESPHERE®

SecureSphere v10.5

Admin Guide

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 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-v10.5-Administration-Guide-Patch-2-v2

End User License and Services Agreement

BY CLICKING ON THE "ACCEPT" BUTTON, TAKING AN ACTION TO INDICATE ACCEPTANCE, OR USING THE PRODUCTS (AS DEFINED BELOW) END USER AGREES TO THE TERMS OF THIS END USER LICENSE AND SERVICES AGREEMENT ("AGREEMENT") WITH IMPERVA, INC. ("IMPERVA"). IN THE EVENT THE INDIVIDUAL IS ENTERING INTO THIS AGREEMENT ON BEHALF OF A CORPORATE OR OTHER PUBLIC OR PRIVATE ENTITY, END USER REFERS TO THAT ENTITY, AND SUCH INDIVIDUAL CERTIFIES THAT HE/SHE IS AN AUTHORIZED REPRESENTATIVE OF THE END USER. IF END USER DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "CANCEL" BUTTON, DISCONTINUE THE SET-UP AND INSTALLATION OR DISCONTINUE USE OF THE PRODUCT. IF THE TERMS OF THE AGREEMENT ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.

1. **Definitions**. The following capitalized terms shall have the meanings set forth below:
   a) "**Appliance**" means the Imperva branded computer hardware on which the Software operates.
   b) "**Delivery**" shall mean, (i) in the case of Software, when the Software is made available by Imperva for End User to electronically download; (ii) in the case of Subscription Services, when the Subscription Service has been provisioned and made available to End User to access; and (iii) in the case of an Appliance, when the Appliance has been tendered by Imperva for shipment.
   c) "**Documentation**" means Imperva's technical specifications that accompany and describe the installation, use and operation of a Product.
   d) "**End User**" means the party that has purchased the Products for its own use, either directly from Imperva or through an authorized third party.
   e) "**Licensed Volume**" means the volume or other measurement of permitted use for the Products as agreed to by Imperva.
   f) "**Open Source Software**" means third party software that Imperva distributes with the Software pursuant to a license that requires, as a condition of use, modification and/or distribution of such software, that the software or other software combined and/or distributed with it be (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge.
   g) "**Products**" mean Appliances, Software or Subscription Services, as the case may be.
   h) "**Services**" mean Professional Services or Support, as the case may be.
   i) "**Software**" means Imperva's or its licensors' software (in object code format) or content, any updates or upgrades thereto provided to End User by Imperva and any Documentation pertaining thereto. Software may be delivered to End User on Appliances or on a standalone basis. The term "Software" does not include Open Source Software.
   j) "**Subscription Services**" mean the subscription services, including content, updates and upgrades thereto, that may be made available to End User by Imperva directly or through its partners and suppliers. Subscription Services include, without limitation, the ThreatRadar service and Imperva offered services that are "powered by Incapsula."
   k) "**Support**" means the technical support and maintenance services for the Product and periodic bug fixes and updates to the Software that Imperva may make generally available at an annual subscription cost to end users.
   l) "**Professional Services**" mean the installation, configuration, and training services that Imperva may provide to an End User.
2. **Licenses and Restrictions.**
   a) **Software**. Conditioned on the terms and conditions of this Agreement, Imperva grants End User a perpetual (subject to Section 11 or any term license restrictions), nonexclusive, nontransferable, nonsublicensable license to use the Software in accordance with its Documentation only for End User's internal business purposes on the Appliances or in the Licensed Volume licensed by End User. If End User purchases Software on a standalone basis, the license granted herein shall include the right to copy the Software up to the Licensed Volume.
   b) **Subscription Services**. Conditioned on the terms and conditions of this Agreement, Imperva grants End User a nonexclusive, nontransferable, nonsublicensable, revocable right to use and access the Subscription Services in accordance with its Documentation only for End User's internal business purposes.

c) **Restrictions**. End User may not (and may not permit any third party to): (i) modify, incorporate or use in any other works, translate, reverse engineer (except to the limited extent applicable statutory law expressly prohibits reverse engineering restrictions), decompile, disassemble, otherwise attempt to derive source code from or create derivative works based on the Products; (ii) make unauthorized copies of the Products; (iii) disclose, distribute, transfer or market the Products to third parties; (iv) remove or modify any proprietary notices, labels or marks on or in any copy of the Products; (v) distribute, sell, sublicense, rent, lease or use the Products (or any portion thereof) for time sharing, hosting, service provider or other computer services to third parties or otherwise make the functionality of the Software available to third parties; (vi) publicly disseminate performance information or analysis (including, without limitation, benchmarks and performance tests) from any source relating to the Products; (vii) access the database or any other third party product that is embedded in the Software with applications other than the Software; or (viii) use the Products other than as permitted herein.

d) **Appliance**. End User acknowledges that the Software included with the Appliance is licensed and not sold. Such Software is licensed solely in conjunction with such Appliance (and not separately or apart from such Appliance). If End User sells, leases, lends, rents, distributes or otherwise transfers any Appliance to any third party or if Imperva terminates this Agreement under Section 11.b or for a breach of Section 2.c, then End User will erase all Software from such Appliance.

e) **Open Source Software**. Open Source Software is copyrighted and licensed under the GPL/LGPL and other licenses. Copies of or references to those licenses are included with Software in the "Help" section. End User may obtain the complete corresponding Open Source Software source code for a period of three years after Imperva's last shipment of the Software, by sending a money order or check for $10 to: Legal Department – Open Source Software Request, Imperva, Inc., 3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065, United States.

f) **US Government End User**. For purposes of this Agreement, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government End User Section 2(f) is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

3. **Support and Subscription Services**. Provided End User has an active and fully paid contract for Support, Imperva will provide Support in accordance with its standard Support terms then in effect. Provided End User has an active and fully paid contract for Subscription Services, Imperva will provide such services in accordance with its standard Service Level Agreement (SLA) then in effect.

4. **Additional Terms for Subscription Services**.

a) **Accessing and Use of Subscription Services**. Except as explicitly set forth herein, End User is solely responsible for acquiring and maintaining all of the equipment, software, services and items necessary to access and make use of the Subscription Services, including without limitation paying all charges, taxes, and other costs and fees related to internet access. End User may access the Subscription Services only through the interfaces and protocols provided or authorized by Imperva and its partners, and agrees to set up, maintain and use the Subscription Services in strict compliance with Imperva's and its partners' instructions. End User is solely responsible for maintaining the confidentiality of any passwords and account information required to access Subscription Services, for all acts that occur in connection with End User's account and to immediately notify Imperva of any unauthorized use of End User's account. In the event of expiration or termination of any Subscription Services that require DNS routing, End User will be solely responsible for rerouting its DNS traffic and Imperva, its partners and suppliers shall have no liability for End User's failure to do so.

b) **Authorization**. Certain Subscription Services are offered to cache, monitor and optimize web pages and web sites. As such, End User hereby grants Imperva and its partners a nonexclusive, worldwide, fully paid-up, royalty-free license to use, transfer, display, minimize and compress the content and material on End User web sites ("**End User Content**"), in any media formats, solely as necessary for the performance of the Subscription Services. Imperva and its partners do not provide backup services for End User Content, and if End User's use of the Subscription Services terminates for any reason, Imperva and its partners may, without notice, delete or deny End User access to any of content or meta data that may remain in its/their possession or control. In addition, End User agrees that if, at Imperva's and its partners' sole determination, End User is using the Subscription Services in a manner that violates laws, rules or regulations or creates an excessive burden or potential adverse impact on Imperva's, its partners' or its suppliers' systems, business or customers, Imperva, its partners or its suppliers may suspend or terminate End User's access to the Subscription Services without notice to or liability to End User.

5. **Professional Services**. Professional Services, if any, to be provided by Imperva to an End User will be subject to a separate statement of work ("**SOW**") agreed to by Imperva and Imperva's standard Professional Services terms then in effect.

6. **Fees, Payment Terms, Shipment and Delivery**.

a) For orders accepted directly by Imperva, End User shall pay Imperva the applicable fees designated by Imperva. Overage fees may apply if End User exceeds its allowance for any Subscription Services at Imperva's then-current overage rates. Any fees payable to Imperva are non-refundable and payable in US Dollars. End User shall also pay all sales, use, value-added and other taxes, tariffs and duties of any type assessed against End User, except for taxes based on Imperva's income. Should End User be required under any law or regulation of any governmental entity or authority outside of the United States, to withhold or deduct any portion of the payments due to Imperva, then End User shall increase the sum payable to Imperva by the amount necessary to yield to Imperva an amount equal to the sum it would have received had no withholdings or deductions been made. Fees shall be invoiced as follows: (a) fees for all Subscription Services and Support shall be invoiced in advance; (b) fees for Software licenses and Appliance purchases will be invoiced upon Delivery. All payments from End User to Imperva are due net thirty (30) days after the date of invoice. If End User's account for Subscription Services or Support is thirty (30) days or more overdue, in addition to any of its other rights or remedies, Imperva reserves the right to suspend such services to End User, without liability to End User, until such amounts are paid in full. Imperva shall have the right to conduct and/or direct an independent accounting firm to conduct, during normal business hours, an audit of End User's facilities, computers and records to confirm End User's use of Products is in compliance with this Agreement. End User shall provide reasonable cooperation with any such audit.

b) Imperva will use commercially reasonable efforts to ship the Appliances and the Software license keys at the times requested in Orders (in partial or full shipments); provided, however, that Imperva shall in no event be liable for any delay in Delivery or for failure to give notice of delay. Without liability to any person and without prejudice to any other remedy, Imperva may withhold or delay shipment of any Order if End User is late in payment or is otherwise in default under this Agreement. Title to Appliances and risk of loss shall pass to End User upon Delivery, and Products shall be deemed accepted by End User upon Delivery. Appliances shall be delivered Ex Works (Incoterms 2000) Imperva's designated manufacturing facility. End User may specify shipping instructions with the Order. In the absence of specific shipping instructions from End User, Imperva will ship by the method it deems most advantageous. End User shall pay and be exclusively liable for all costs associated with shipping and delivery including without limitation, freight, shipping, customs charges and expenses, cost of special packaging or handling and insurance premiums incurred by Imperva in connection with the shipment of Appliances to End User. In its discretion, Imperva may advance shipping charges on behalf of End User on Appliances shipped to End User, and End User agrees to reimburse Imperva for any such advanced charges and expenses.

7. **Confidentiality**.

a) As used herein, "**Confidential Information**" means all confidential and proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes, without limitation, the Products, their performance (including any benchmarking information) and Imperva's pricing of the Products and Services. Confidential Information shall not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (iii) was independently developed by the Receiving Party without breach of any obligation owed to the Disclosing Party; or (iv) is received from a third party without breach of any obligation owed to the Disclosing Party.

b) The Receiving Party agrees that it will (i) use Confidential Information for the sole purpose of exercising its rights and performing its obligations under this Agreement, (ii) divulge Confidential Information only to those of its employees, directors, independent consultants or agents who have a need to know such Confidential Information and who are bound by professional duty or in writing (in advance) to confidentiality and non-use obligations at least as protective of such information as this Agreement, and (iii) not disclose any Confidential Information to any third party. The Receiving Party shall notify and cooperate with the Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information of the Disclosing Party. The Receiving Party may disclose Confidential Information to comply with an order from a court of competent jurisdiction or with a mandatory requirement of a governing regulatory body, provided such party, to the extent permitted by law and as soon as reasonably practicable under the circumstances, informs the Disclosing Party and allows the Disclosing Party the opportunity to object to the disclosure order or to take action to preserve the confidentiality of the information. The Receiving Party shall cooperate with the Disclosing Party in such party's reasonable efforts to limit the disclosure of the Information.. End User acknowledges, understands and agrees that Imperva may, as part of its provision of the Product and/or Services to End User, collect, store and use information obtained from End User, including, but not limited to, information about End User's users and customers ("**Information**") for the purposes of the provision of the Product, Services and other services to End User and may use such information for analysis and improvement of Imperva's products and services. End User represents and warrants that it has all rights and permissions necessary to grant Imperva access to such Information as contemplated herein.

c) Upon termination of this Agreement for any or no reason, the Receiving Party shall (i) immediately cease all use of the Disclosing Party's Confidential Information, (ii) at the instruction of the Disclosing Party, either promptly destroy all Confidential Information of the Disclosing Party or return all Confidential Information of the Disclosing Party.

d) If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of this Section 7, the Disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the parties that any other available remedies are inadequate.

8. **Proprietary Rights; Indemnity**.

a) All title and intellectual property rights in and to the Products are owned exclusively by Imperva and its partners and suppliers. Other than as expressly set forth in this Agreement, no license or other rights in or to the Products and intellectual property rights thereto are granted to End User, and all such licenses and rights are hereby expressly reserved. Any ideas, suggestions, modifications and the like made by End User with respect to a Product will be the property of Imperva regardless of whether Imperva chooses to exercise its rights to incorporate such ideas, suggestions or modifications into the Product.

b) Subject to the remainder of this Section 8.b, Imperva will indemnify End User from any Liability (as defined below) to a third party resulting from infringement of a U.S. patent or any copyright, or misappropriation of any third party trade secrets by the Product as delivered ("**Infringement Claim**"); provided that End User (1) promptly notifies Imperva of any and all threats, claims and proceedings of such Infringement Claim, (2) gives reasonable assistance in response to Imperva's request for assistance, and (3) grants Imperva sole control over defense and settlement thereof. For purposes of this section "Liability" means the resulting costs (including reasonable attorneys' fees) and damages awarded against End User to the third party making such Infringement Claim by a court of competent jurisdiction or agreed in settlement. The foregoing obligations do not apply with respect to Products or portions or components thereof, (i) that are modified after delivery by Imperva, (ii) combined with other products, processes or materials, where the alleged infringement relates to such combination, (iii) where End User continues allegedly infringing activity after being notified thereof or modifications that would have avoided the alleged infringement have been made available to End User, or (iv) where End User's use of such Product is not strictly in accordance with this Agreement. In the event that Products are held to or believed by Imperva to infringe, Imperva at its discretion, will have the option to (A) modify the allegedly infringing Products to be non-infringing, (B) obtain for End User a license to continue using the Products, or (C) request the return of the Product and upon receipt thereof terminate this Agreement as to the infringing Product and refund to End User the unused portion of the fees paid under this Agreement for such infringing Product, depreciated on a straight-line basis over a three (3) year period. End User will defend, indemnify and hold Imperva harmless against any claims, damages settlements and expenses (including attorneys' fees) excluded from Imperva's indemnity obligations in (i) – (iv) above. THIS SECTION SETS FORTH IMPERVA'S SOLE OBLIGATION AND END USER'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF VIOLATION OF THIRD PARTY RIGHTS.

9. **Warranty and Disclaimer**.

a) Imperva warrants that during the sixty (60) day period commencing on the date of first Delivery, the Software and the Appliances will perform substantially in accordance with their Documentation. In the event of a breach of the foregoing warranty with respect to the Software, as End User's sole and exclusive remedy, Imperva shall, at its sole expense, use reasonable efforts to modify the Software, so that it performs substantially in accordance with its Documentation. In the event of a breach of the foregoing warranty with respect to an Appliance, as End User's sole and exclusive remedy, Imperva shall, at its sole expense and at its option, repair the Appliance or replace the Appliance with a new or reconditioned Appliance that performs materially in accordance with its Documentation. The foregoing warranty extends only to the original purchaser and will not apply to the misuse of or damage to the Products. The rights and remedies granted End User under this Section state Imperva's entire liability, and End User's exclusive remedy, with respect to any breach of the warranty set forth in this Section 9(a).

b) EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9(a), THE PRODUCTS OR SERVICES ARE PROVIDED "AS-IS' AND IMPERVA MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. IMPERVA, ITS PARTNERS AND SUPPLIERS MAKE NO WARRANTY THAT USE OF THE PRODUCTS OR SERVICES WILL BE UNINTERRUPTED, ERROR-FREE OR DEFECT-FREE, OR AVAILABLE AT ALL TIMES. IMPERVA HEREBY SPECIFICALLY DISCLAIMS, ON BEHALF OF ITSELF AND ITS PARTNERS AND SUPPLIERS, ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

10. **Limitations of Liability**. IN NO EVENT WILL END USER'S OR IMPERVA'S (AND ITS PARTNERS' OR SUPPLIERS') LIABILITY FOR DIRECT DAMAGES HEREUNDER EXCEED THE TOTAL VALUE OF AMOUNTS TO BE PAID BY END USER FOR THE PRODUCT OR SERVICE AT ISSUE. IN NO EVENT SHALL END USER OR IMPERVA (OR ITS PARTNERS' OR SUPPLIERS') HAVE ANY LIABILITY TO THE OTHER FOR ANY LOST PROFITS OR REVENUES, LOSS OF DATA OR USE, INTERRUPTION OF THE SERVICES, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO END USER WITH RESPECT TO ANY CLAIMS ARISING UNDER SECTION 2 (LICENSES AND RESTRICTIONS), OR TO EITHER PARTY UNDER SECTION 7 (CONFIDENTIALITY).

11. **Term and Termination**.

a) The term of this Agreement will commence upon Delivery of the Products to End User and will continue in effect for such time as End User continues to have the right to access the Products. Support for Software and/or Appliances will automatically renew at the end of the applicable Support term unless either party gives the other at least thirty (30) days' notice of non-renewal prior to the end of the then current term.

b) Either party may terminate this Agreement due to a material breach of this Agreement by the other party if such material breach remains uncured for a period of thirty (30) days following receipt of written notice by the breaching party; provided that Imperva may terminate this Agreement and/or all licenses granted to End User hereunder immediately upon written notice to End User if End User breaches any provision of Section 2 (License & Restrictions), Section 4 (Additional Terms for Subscription Services) or Section 7 (Confidentiality).

c) Upon the earlier of expiration of End User's rights or termination of the Agreement, Imperva will cease providing Subscription Services, Support and Professional Services, and each party shall promptly return or destroy the other party's Confidential Information. Termination shall not relieve End User of the obligation to pay any fees accrued or payable to Imperva prior to the effective date of expiration or termination. The following sections shall survive termination of this Agreement: Sections 2(c), 2(d), 2(f), 4, 6 -12, and 16.

12. **Compliance with Laws; Export**. End User acknowledges that the Software contains encryption technology that is subject to export restrictions by the U.S. government and import restrictions by certain other governments. End User will not and will not allow any third-party to remove or export from the U.S. or allow the export or re-export of any part of the Software or any direct product thereof: (i) into (or to a national or resident of) Cuba, Iran, North Korea, Sudan or Syria (to the extent the U.S. government or any agency thereof restricts export or re-export to such countries); (ii) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals; (iii) to any country to which such export or re-export is restricted or prohibited, or as to which the U.S. government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval; or (iv) otherwise in violation of any export or import restrictions, laws or regulations of any U.S. or foreign agency or authority. End User agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list. The Software is restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology without the prior permission of the U.S. government. End User agrees to indemnify and hold Imperva, its partners and suppliers harmless against any claims, losses or expenses arising out of End User's breach of this Section 12.
13. **End User Mention**. End User consents to Imperva using its name and logo to identify End User as a customer of Imperva, such as use on Imperva's web site. Any use shall be subject to Imperva complying with any guidelines that End User may deliver to Imperva from time-to-time regarding the use of its name and logo. This consent terminates upon termination of this Agreement.
14. **Force Majeure**. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events, which occur after the signing of this Agreement and which are beyond the reasonable control of the parties, such as strikes, blockade, war, terrorism, riots, natural disasters, refusal of license by the government or other governmental agencies, in so far as such an event prevents or delays the affected party from fulfilling its obligations and such party is not able to prevent or remove the force majeure at reasonable cost.
15. **Evaluation**.
    a) **Evaluation Product**. If the order is for End User to evaluate Product and its related Documentation on a temporary basis for non-commercial use in a non-production environment ("Evaluation Product") and Imperva agrees to such evaluation, conditioned on End User's compliance with the terms and conditions of this Agreement, Imperva grants to End User during the Evaluation Period (as defined below), a cost-free, nonsublicensable, nontransferable, nonassignable and nonexclusive, revocable license to use the Evaluation Product, solely at the location identified in writing by End User and solely for End User's internal evaluation of the Evaluation Product. End User may only grant access to the Evaluation Product to employees, contractors, agents or consultants who are bound to confidentiality and non-use obligations no less protective of Imperva's proprietary rights than this Agreement. Notwithstanding anything to the contrary as stated in this Agreement, all worldwide right, title and interest to the Evaluation Product, and all intellectual property rights in and to them, are and will remain the exclusive property of Imperva.
    b) **Evaluation Period**. Unless otherwise agreed to by the parties in writing or terminated earlier in accordance with this Agreement, an evaluation shall commence upon delivery of the Evaluation Product and continue for thirty (30) days thereafter ("Evaluation Period"). Upon the expiration or termination of the Evaluation Period, (i) all licenses granted under this Section 15 for such evaluation will cease, and (ii) End User will immediately return the Evaluation Product to Imperva and destroy or erase any intangible copies of the Evaluation Product, and certify in a writing signed by an officer of End User and delivered to Imperva that all such copies of have been returned, destroyed or erased.

c) **Additional Evaluation Terms**. Notwithstanding anything to the contrary as contained in this Agreement, End User acknowledges and agrees that the Evaluation Product is provided for evaluation "AS-IS" and Imperva and its suppliers make no representations or warranties of any kind, express or implied, with respect to the Evaluation Product, including, without limitation, any implied warranties of merchantability, title, fitness for a particular purpose, informational content, system integration, enjoyment, non-infringement or any other warranties arising out of course of dealing, usage or trade, and no obligation under Section 8.b (Indemnity) shall arise with respect to an Evaluation Product.

16. **Miscellaneous Provisions**. The parties are independent contractors under this Agreement and nothing in this Agreement authorizes a party to act as an agent of the other or bind the other to any transaction or agreement. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign or transfer this Agreement in whole or in part by operation of law or otherwise, without the other party's prior written consent. Any attempt to transfer or assign this Agreement without such written consent will be null and void. Notwithstanding the foregoing, however, Imperva may assign this Agreement without consent to the acquiring or surviving entity in a merger or acquisition in which Imperva is the acquired entity (whether by merger, reorganization, acquisition or sale of stock) or to the purchaser of all or substantially all of Imperva's assets. Imperva's licensors are intended third party beneficiaries of this Agreement. In the event any provision of this Agreement shall be determined to be invalid or unenforceable under law, all other provisions of this Agreement shall continue in full force and effect. Except as specifically provided in this Agreement, the exercise by either party of any rights and remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. This Agreement contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous communications, representations, understandings and agreements, either oral or written between the parties with respect to said subject matter. This Agreement may be modified or waived only in a written instrument signed by both parties. A waiver of any breach under this Agreement shall not constitute a waiver or any other breach or future breaches. Notwithstanding the foregoing, if a separate, written and mutually signed agreement for the acquisition of the Products and/or Services exists between End User and Imperva, the terms of that written agreement (excluding any pre-printed terms of any purchase order, confirmation or similar document, all of which will have no effect and will not be considered agreed to by Imperva) shall take precedence over this Agreement. All notices, requests, demands and other communications hereunder shall be in writing to the address set forth below for Imperva and on the applicable order for End User and shall be deemed to have been duly given: (i) upon receipt if by personal delivery; (ii) upon receipt if sent by certified or registered mail (return receipt requested); or (iii) two (2) days after it is sent if by overnight delivery by a major commercial delivery service. This Agreement will be interpreted and construed in accordance with the laws of the State of California and the United States of America, without regard to conflict of law principles. The parties hereby consent to the exclusive jurisdiction and venue of the state and federal courts located in Santa Clara County, California for resolution of any disputes arising out or relating to this Agreement. The provisions of the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act will not apply to this Agreement in any manner whatsoever.

Imperva, Inc.

3400 Bridge Parkway, Suite 200

Redwood Shores, CA 94065 USA

Table of Contents

Copyright Notice 2
End User License and Services Agreement 3
Introduction to the SecureSphere Administration Guide 19
Intended Audience 19
What this Publication is About 20
The Admin Workspace 21
Document Conventions 22
Topologies and Deployment 23
Choosing a Deployment 23
CPU Affinity 24
Sniffing Mode 24
Topologies 24
Inline Gateways 25
Bridge Deployments 25
Fail Safe and Fail Open Modes 26
Reverse Proxy Deployments 26
Reverse Proxy Overview 26
Transparent Reverse Proxy Overview 27
Non-Transparent Reverse Proxy Overview 28
Reverse Proxy with Load Balancer 31
Features Available in the Each Deployment Mode 32
Platforms and Installation 34
Forward Compatibility 34
Preparing the Appliance 35
Installing the SecureSphere Software 35
G Series Appliances (Except G2 and G2-2) 35
G2 and G2-2 Appliances 37
X and M Series Appliances 39
Creating a Bootable USB Device Containing the Installation Image 40
Working with Management Servers After the Installation 41
Connecting to the Management Server 41
MySQL Users 42
Replacing Gateways 43
Replacing a Faulty Gateway 43
Replacing a Faulty Gateway Using an Already-Configured Gateway 44
Configuring SecureSphere 46
Initial Configuration 47
Automating First Time Login 47
Mandatory Arguments 48
General Optional Arguments 49
Optional Cluster Arguments 49
Optional Listener Arguments 49
Optional Sniffing Arguments 50

Common Arguments 50
IPv6 50
SecureSphere Features Which Support IPv6 50
Overview 50
IPv4 / IPv6 Dual Stack 51
SecureSphere MX and Gateway 52
IPv6 in impcfg and impctl 52
External Systems 53
SecureSphere Users 54
The Different SecureSphere Users 54
Appliance OS 55
CLI Users 55
Gateway/Management Server Appliance Initial Configuration 57
First-Time Login (Configuration) 57
Registering a Gateway 57
Configuring SecureSphere Using the Command Line Tools 58
Command Line Tools and MX-HA 58
impcfg 59
impcfg Functionality Map 62
Configuring a Management Server 67
Configuring a Gateway 68
Gateway Actions 71
Configuring a Gateway as a Bridge 72
Configuring a Gateway as a Sniffing Gateway 74
Configuring a Gateway for a Cluster 75
Managing SecureSphere Agents 79
Configuring a Data Assessment Server (DAS) 85
Reconfiguring the DAS as a Onebox 88
Configuring the Platform 89
Network Management 91
Time Management 98
Users Management 100
Hostname Management 105
Bootloader Password Management 106
Configuring SecureSphere Routes 107
Configuring SecureSphere Agent Routes 107
Configuring Transparent Reverse Proxy 108
Configuring Kernel Reverse Proxy 109
Configuring the Management Server for High Availability 109
Configuring Apache Reverse Proxy 109
Changing the Gateway's Mode to ARP 109
Configuring ARP 109
Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway 111
Switching Deployments 112
Overview 112
From a Onebox to a Gateway 112

From a Gateway to a Onebox 112
Changing the MX of a Gateway 112
Installing SecureSphere Agents 113
Installing a New SecureSphere Agent as part of Software Update 114
SecureSphere Agent Configuration Tasks 116
Installing the SecureSphere Agent 117
Preparing for Installation 117
Configuring the SecureSphere Gateway Before Installation 122
Installing the SecureSphere Agent and Installation Manager 124
After Installing the SecureSphere Agent 139
First-Time Configuration Wizard 140
Uninstalling the SecureSphere Agent 144
Uninstalling the SecureSphere Agent on a non-Windows System 144
Uninstalling the SecureSphere Agent on a Windows System 145
Upgrading the SecureSphere Agent 145
Starting and Stopping the SecureSphere Agent 146
Starting and Stopping the SecureSphere Agent from the Management Console 146
Starting the non-Windows SecureSphere Agent from the Command Line 146
Stopping the non-Windows SecureSphere Agent from the Command Line 147
Starting the Windows SecureSphere Agent from the Command Line 147
Stopping the Windows SecureSphere Agent from the Command Line 147
SecureSphere Agent Management Console 148
SecureSphere Agent Management Console Conventions 148
Starting the SecureSphere Agent Management Console 149
Registering the SecureSphere Agent to the Gateway 149
Activating Settings Manually 151
Agent Information Displayed in the Console 151
Agent Troubleshooting Using the Management Console 151
Working with High Availability 152
Configuring the Gateways to Operate in the HA Mode with Agents 152
Configuring the SecureSphere Agent to Operate in the HA Mode 154
Diagnostic Tools 155
SecureSphere Agent Logs 155
SecureSphere Agent Error Messages 155
Maintenance Tasks 156
SecureSphere Agents in a Hypervisor (Virtualized) Environment 156
Prerequisite Tests for non-Windows Agents 157
Supported Interfaces for the Gateway Listener 160
Advanced Agent Configuration 161
Working with a NATed Listener 161
Working with Multiple Oracle Instances 164
Monitoring Solaris Zones Using SecureSphere Agents 165
Monitoring MySQL Traffic 165
Working with DAC (Dedicated Administrator Connection) 165
Command Line Scripting Language 166
Conventions for Command Line Scripting 166

Syntax for Command Line Scripting 167
Gateways 170
Configuring Gateways and Gateway Groups 170
Gateways 170
Gateway Groups 176
Configuring a Kernel Reverse Proxy 180
Exporting Technical Information from Gateway and Onebox 187
Licenses 189
License Overview 189
Uploading Licenses 190
Viewing Licenses 190
Managing Database Scanning and Assessment Licenses 192
Users and Permissions 193
Understanding Permissions 193
Permission Models in SecureSphere 194
Roles and Users 194
Permission Types 195
Understanding the Permissions Window 195
Adding and Removing Permissions 196
Notes on Permission Behavior 196
Permissions Workflow 197
Working with Roles 197
PreDefined Roles 198
Custom Role Examples 198
Creating a Role 199
Working with Users 199
Creating a SecureSphere User 200
Assigning Roles to Users 200
Configuring Object or Category Level Permissions 201
Configuring Navigation Permissions 202
Configuring the Authorization to Activate Settings 203
Granting Masking/Unmasking Capability to SecureSphere Roles and Users 204
Configuring User Information 205
Locking a User Account 206
Resetting a User Password 206
Read-Only User 208
Sessions 210
Connected Users 210
Sessions 211
ADC 212
Viewing ADC Content and Status 213
Updating ADC Content 214
ADC History 215
Job Status 216
Jobs Status 217
Displaying the Jobs Status Window 218

Editing a Job **218**
Aborting a Job **219**
Using the Log to Analyze Jobs **220**
Miscellaneous Audit Data Operations **220**
Changing the Audit Directory Path 221
Configuring Encryption 221
Maintenance **223**
Audit Fast Viewing **223**
Audit Purge **224**
Assessment Results Archive **225**
Discovery Results Archive **227**
Exporting and Importing the Management Server **229**
Export Using the SecureSphere GUI 230
Export / Import Manually Using the Interactive CLI 232
Export / Import Manually Using the Non-Interactive CLI 233
Listing the Contents of an Exported File 235
Miscellaneous Maintenance Tasks 235
File Explorer Maintenance **236**
Reports Archive **236**
Risk Score Update **238**
Kerberos Key Update **238**
System Events Archive **240**
Vulnerabilities Purge **241**
Extracting Archives for Viewing **243**
Audit Archive Conversion **244**
Exporting an Archive to TAR Format with CSV Values 244
Converting an MPRV file to TAR Format with CSV Values 245
Analyzing Converted Files 246
System Definitions **252**
Dynamic Profiling **252**
Learning Exceptions 253
Profile Optimization 253
Profile Size Limits 253
Switching to Protect Mode Thresholds (SQL) 257
Switching to Protect Mode Thresholds (Web) 260
Gateway Settings **262**
Audit Settings 263
Response Page Display in Alerts Settings 263
Web to Database User Tracking Settings 264
Configuring Traffic Distribution Analysis 264
Security and Authentication **266**
Authentication and Authorization Configuration 266
FIPS Settings 267
Password Settings 268
SSL Certificate Expiration Monitoring 269
User Lockout Settings 269

Management Server Settings **270**
Action Interfaces 270
Agents 273
Alert Aggregation Configuration 273
Application Groups Settings 274
Assessments 274
CSV Upload Default Settings 274
Data Owner Settings 275
External HTTP Settings 276
External Systems 277
Remote DB Connectivity 287
File URM 289
Keywords Settings 289
Log Collectors 291
Lookup Data 293
Policy Settings 293
Report Settings 293
Server Definitions 294
Software Update Settings 295
Stored Procedures Settings 295
System Events Notifications 295
User Interface Settings **296**
Display Limits 296
Language Settings 297
ThreatRadar Settings **297**
General ThreatRadar Settings 297
System Performance **298**
Management Server **298**
Exporting Technical Information from Management Servers **300**
Gateways and Agents **300**
Troubleshooting Performance **302**
Management Server 302
Gateways and Agents 303
Installing SecureSphere Agent for z/OS **305**
Installing SecureSphere Agent for z/OS - Version 3.1 ..... **305**
Upgrading from Previous Versions to Version 3.1 305
Configuring SecureSphere Agent Agent for z/OS Tasks 306
Before Installing and Configuring SecureSphere Agent for z/OS 306
Downloading and Installing SecureSphere Agent for z/OS 310
Configuring SecureSphere Agent for z/OS (on z/OS) 313
Starting, Managing, and Stopping SecureSphere Agent for z/OS 322
Installing SecureSphere Agent for z/OS - Version 2.1 ..... **323**
Configuring SecureSphere Agent for z/OS Tasks 324
Before Installing and Configuring SecureSphere Agent for z/OS 324
Downloading and Installing SecureSphere Agent for z/OS 328
Configuring SecureSphere Agent for z/OS (on z/OS) 331

Starting, Managing, and Stopping SecureSphere Agent for z/OS 341
Gateway High Availability 343
Layer 2 High Availability Deployments 343
At the Network Level 343
At the SecureSphere Level 344
Layer 3 (Proxy) High Availability Deployments 347
At the Network Level 348
At the SecureSphere Level 349
Other High Availability Deployments 349
Fail-Open Bridge 350
Sniffing Gateway High Availability 350
Management Server High Availability (MX-HA) 353
Management Service-High Availability(MX-HA) Overview 353
Management Server-High Availability(MX-HA) Implementation 354
Management Server High Availability (MX-HA) Components 354
Linux Heartbeat 355
Oracle Standby Database (Data Guard) 355
SecureSphere Server 355
HA Health Check 355
Imperva Watchdog 355
Before Installing Management Server High Availability (MX-HA) 355
Hardware and Software Requirements 356
Pre-Installation Tasks 356
Installing Management Server High Availability (MX-HA) 361
After Installing Management Server High Availability (MX-HA) 365
Verify the Primary Server is Active 365
Register the Gateway 365
Monitoring Management Server High Availability (MX-HA) 368
MX-HA Status 368
Confirming that MX-HA is Correctly Configured 369
MX-HA Logs 370
Heartbeat Behavior 372
Known Issues 372
File List 373
Network High Availability 376
Network High Availability Support 376
Configuring Network High Availability 377
Network Services 378
SecureSphere Component Communication 378
Configuring Firewall Ports 379
Serial Console Access to SecureSphere 380
Supported Versions and Upgrades 381
Supported Serial Console Settings 381
Before You Begin: Checking OS Layer Serial Console Access 383
Configuring BIOS Settings for Serial Console 383
Editing the GRUB Configuration File 383

Add-Ons **385**
Hardware Security Modules (HSM) **385**
nCipher Card 386
nCipher netHSM 393
Storage Area Networks (SAN) **397**
SAN Overview 398
Supported SAN Hardware 398
Configuring SecureSphere for SAN 399
Disabling the SAN 408
SSL Accelerator **408**
LOM (Lights Out Management) **408**
Overview 409
Connecting to the LOM 409
Managing the LOM 410
Command Line Interface **422**
impcfg **422**
impcfg Functionality Map 422
impctl **426**
"Safe" impctl Commands 427
Stopping and Starting the MX in an MX-HA Environment 427
Miscellaneous impctl Commands 428
Miscellaneous Commands **430**
Powering Down the Appliance 430
Changing the Password for Management Server - Gateway Communication 430
FIPS 140 Compliance **431**
2.1 Encrypted Communications **431**
2.2 MX Encrypted Communications **431**
2.2.1 FIPS-Approved Algorithms 432
2.2.2 FIPS-Non-Approved Algorithms 432
2.3 SecureSphere Gateway and Platform Communications **433**
2.3.1 FIPS-Approved Algorithms 433
2.3.2 FIPS-Non-Approved Algorithms 433
2.4 HSM solution **433**
2.5 SecureSphere WAF in FIPS Mode **433**
Limitations **433**
Activating FIPS Mode **434**
Disaster Recovery **435**
Disaster Recovery **435**
Preparing for Disaster Recovery 435
Recovery 436
PCI Compliance **438**
PCI Data Security Standard **438**
SecureSphere and PCI DSS 438
PCI Compliance **439**
Protecting the SecureSphere Appliance 439
Protecting Cardholder Data 439

Index 441

CHAPTER 1

Introduction to the SecureSphere Administration Guide

This section provides an introduction to the SecureSphere Administration guide and reviews the following topics:

Intended Audience 19
What this Publication is About 20
The Admin Workspace 21
Document Conventions 22

Intended Audience

This publication is intended for system administrators who are tasked with the installation, configuration and ongoing maintenance of Imperva SecureSphere.

What this Publication is About

This publication describes the functionality of the Imperva SecureSphere and provides information on its installation, deployment, configuration and maintenance. This Administration Guide comprises the following chapters:

Administration Guide Chapters and Appendices

Chapter or Appendix Name	Description
Introduction to the SecureSphere Administration Guide on page 19	This chapter describes the SecureSphere Administration Guide.
Topologies and Deployment on page 23	This chapter describes the different ways that SecureSphere can be deployed to protect Web and database applications.
Platforms and Installation on page 34	This chapter describes how to install SecureSphere.
Configuring SecureSphere on page 46	This chapter describes how to configure SecureSphere appliances.
Installing SecureSphere Agents on page 113	This chapter describes how to install SecureSphere SecureSphere Agents.
Gateways on page 170	This chapter describes how to configure SecureSphere Gateways.
Licenses on page 189	This chapter describes the SecureSphere licensing process.
Users and Permissions on page 193	This chapter describes how to define SecureSphere administrators, users and their privileges.
Sessions on page 210	This chapter describes how to track SecureSphere sessions.
ADC on page 212	This chapter describes how to configure SecureSphere to download content from Imperva's ADC (Application Defense Center).
Job Status on page 216	This chapter describes how to track jobs initiated by SecureSphere.
Maintenance on page 223	This chapter describes how to maintain, backup and restore SecureSphere.
System Definitions on page 252	This chapter describes the SecureSphere system definitions.
System Performance on page 298	This chapter describes the system performance data SecureSphere provides about Management Servers, Gateways and SecureSphere Agents.
Installing SecureSphere Agent for z/OS on page 305	This chapter describes the system performance data SecureSphere provides about Management Servers, Gateways and SecureSphere Agents.
Gateway High Availability on page 343	This chapter describes how to configure High Availability for SecureSphere Gateways.
Management Server High Availability "Management Server High Availability (MX-HA)" on page 353	This chapter describes how to configure High Availability for SecureSphere Management Servers.

Chapter or Appendix Name	Description
Network High Availability on page 376	This chapter describes how to provide High Availability for SecureSphere using the network.
Network Services on page 378	This appendix describes how to configure the network in which SecureSphere appliances are deployed.
Add-Ons on page 385	This appendix describes various SecureSphere add-ons, such as HSM, SAN etc.
Command Line Interface on page 422	This appendix describes the SecureSphere command line tools: impcfg and impctl.
FIPS 140 Compliance on page 431	This appendix describes SecureSphere's FIPS 140-x compliance.
Disaster Recovery on page 435	This appendix details disaster recovery procedures for the SecureSphere Management Server.
PCI Compliance on page 438	This appendix describes how SecureSphere can help administrators achieve PCI compliance for their sites.

The Admin Workspace

To perform administrative tasks in SecureSphere, open the **Admin** workspace, by clicking **Admin** in the upper right-hand corner.

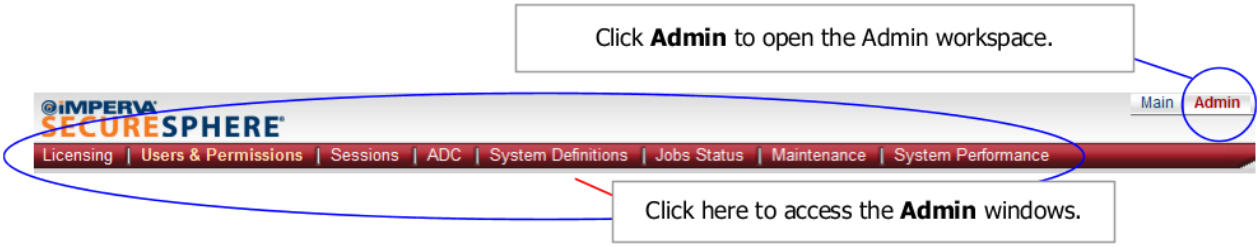


Figure 1: The Admin Workspace

The **Admin** workspace consists of the following windows:

Admin workspace

	Description	For more information, see
Licensing	Install SecureSphere licenses	Licenses on page 189
User and Permissions	Define SecureSphere administrators, users and their privileges.	Users and Permissions on page 193
Sessions	Track open SecureSphere sessions.	Sessions on page 210
ADC	Configure SecureSphere to download content from Imperva's ADC (Application Defense Center).	ADC on page 212
System Definitions	Define system-wide parameters.	System Definitions on page 252
Jobs Status	Track jobs initiated by SecureSphere.	Job Status on page 216
Maintenance	Export SecureSphere system data, maintain archives etc.	Maintenance on page 223
System Performance	Monitor system performance.	System Performance on page 298

To access one of these windows, click its name.



Note: The **Admin** tab is visible only to users with administrative permissions. For more information, see Users and Permissions on page 193.

Document Conventions

In this document, the following typographical and formatting conventions are used:

Typographical and Formatting Conventions

Convention	Meaning	Example
`command`	The `monospaced font` is used for CLI commands or output, and for file names.	`cd /tmp`
|	separates optional values in lists	`oranges | apples`

CHAPTER 2

Topologies and Deployment

This chapter describes the different deployments of SecureSphere, and includes:

Choosing a Deployment 23
Sniffing Mode 24
Inline Gateways 25
Reverse Proxy Deployments 26
Features Available in the Each Deployment Mode 32

Choosing a Deployment

A SecureSphere Gateway can be deployed either inline, where traffic passes through the SecureSphere Gateway, or as a sniffing Gateway, where traffic does not pass through the Gateway but is copied to it for analysis. The most important differences between these deployments are:

- An inline Gateway can block malicious traffic so that it never reaches the protected network, but on the other hand, it introduces some latency.
- A sniffing Gateway introduces no latency, and it can prevent malicious traffic from reaching the protected network by issuing TCP resets to the server on its blocking interface.

Inline Gateways can be deployed in a number of configurations:

- **Transparent bridge**: The SecureSphere Gateway acts as a transparent bridge, monitoring traffic entering and leaving the protected network and applying the various policies. In transparent bridge mode, the SecureSphere Gateway can also act as a transparent reverse proxy for Web applications.
- **Reverse proxy**: In addition to the bridge functionality, for Web applications the SecureSphere Gateway can act as a reverse proxy, configured as:
  - **Transparent Reverse Proxy – in bridge mode** (see Reverse Proxy Deployments on page 26)

Transparent Reverse Proxy is configured for specific Web services, so a SecureSphere Gateway can act as a proxy for some services but not for others. For more information, see Transparent Reverse Proxy - Selected Web Servers on page 28.

- **Kernel Reverse Proxy** – see Kernel Reverse Proxy (KRP) on page 29
- **Apache Reverse Proxy** – see Apache Reverse Proxy (ARP) on page 30

Additionally, Kernel Reverse Proxy and Apache Reverse Proxy can be deployed on the same SecureSphere Gateway. For more information, see Apache and Kernel Reverse Proxy on the Same Gateway on page 34 "Apache and Kernel Reverse Proxy on the Same Gateway" on page 30.



Note: Onebox mode (where both the SecureSphere Management Server and SecureSphere Gateway are integrated in a single machine) is available for all deployments except High Availability.

Kernel Reverse Proxy and Apache Revere Proxy must be configured during installation, using `impcfg`. Additionally, configuring Apache Revere Proxy requires manually editing configuration files. For more information, see Configuring SecureSphere on page 46.

SecureSphere Gateways can also be deployed in High Availability mode. For more information, see Gateway High Availability on page 343.

SecureSphere Gateways can also be deployed in conjunction with Load Balancers. For more information, see Reverse Proxy with Load Balancer on page 31.



Note: SecureSphere Agents, installed on the Database and File servers, enable SecureSphere to monitor local database and file traffic. SecureSphere Agents are compatible with both inline and sniffing Gateways. For more information about SecureSphere Agents, see the **SecureSphere User Guide**.

This chapter presents some typical examples of these deployments. Not all possible deployments are covered here.

CPU Affinity



Note: CPU affinity does not apply in sniffing mode.

For all SecureSphere Gateways with more than one core, SecureSphere implements IRQ affinity (CPU affinity), meaning that each core handles interrupts from specific interfaces.

SecureSphere version 8.0 allocates cores to interfaces at boot time. Beginning with version 8.5, SecureSphere implements dynamic allocation of cores to 10G interfaces, depending on the load. For other interfaces, the boot time allocation remains unchanged.

Sniffing Mode

Topologies 24

Topologies

In a sniffing mode deployment, traffic does not pass through the SecureSphere appliance but is only copied to it. A sniffing appliance can monitor both Web and database traffic, and blocks malicious Web traffic by issuing TCP resets to the server. A sniffing appliance's advantage is that it introduces no latency in either Web or database application traffic.

The disadvantages of sniffing mode are:

- Issuing TCP resets is not as dependable a method of blocking traffic as is dropping packets.
- Overloaded SPAN ports sometimes drop packets, so SecureSphere will not inspect them.

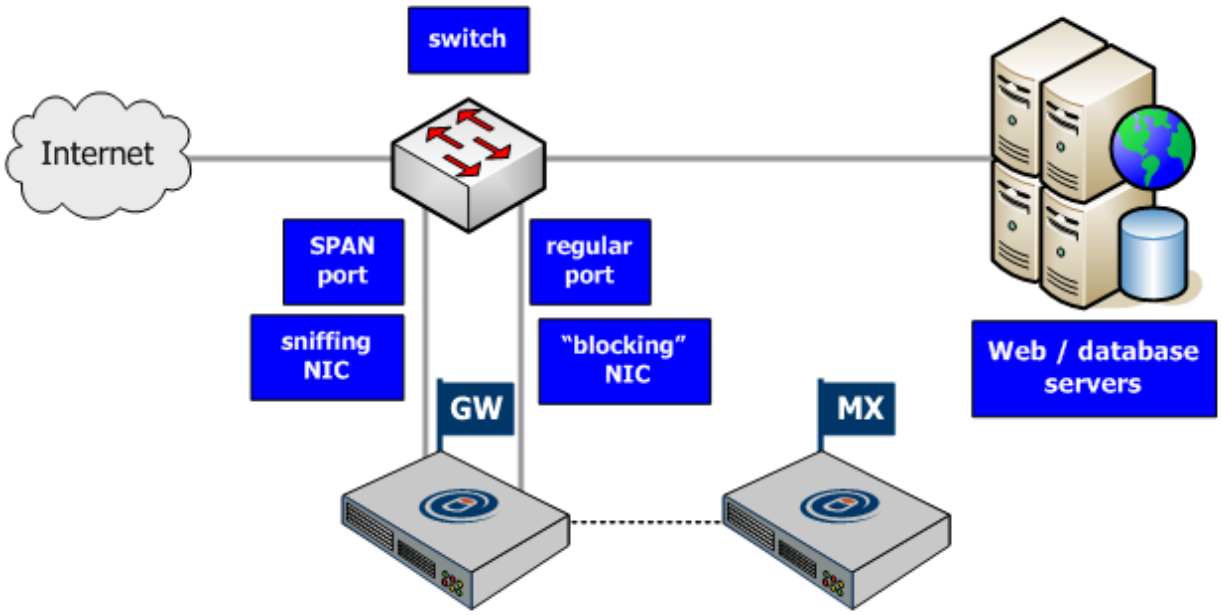


Figure 2: Sniffing Deployment

There are two methods to "sniff" the traffic:

- using a SPAN (mirror) port on the switch, or
- using a dedicated TAP

The SPAN port is less reliable since it depends on the switch resources and has lower priority than forwarding traffic, so it might miss packets. TAP does not have this disadvantage.

Aggregation taps can also be used.

Inline Gateways

Bridge Deployments

Topologies

In a bridge deployment, all traffic passes through the SecureSphere Gateway, which monitors the traffic and blocks malicious connections by dropping packets.

SecureSphere supports two bridge topologies

- Transparent bridge for DXG and WAF

- Non-transparent bridge (for WAF only) using RP (transparent and non transparent RP)

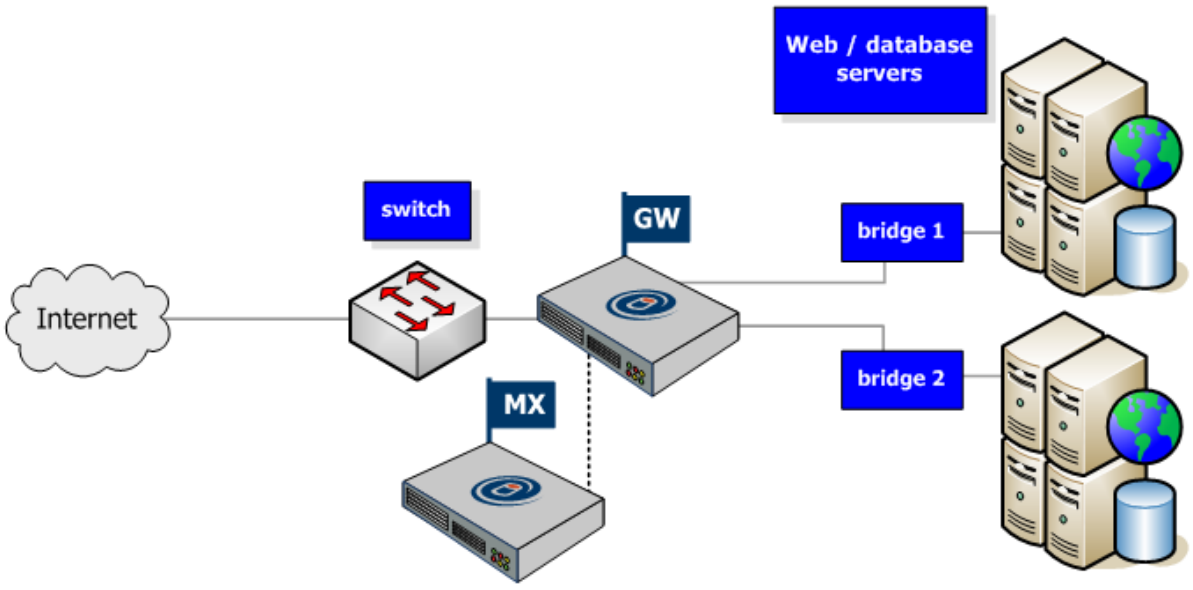


Figure 3: Inline Bridge Deployment

The bridge can be invisible (transparent) to both clients and servers, which would then see each others' real IP addresses.

Fail Safe and Fail Open Modes

A transparent bridge can be configured to maintain connectivity in the event of failure. In Fail Open mode, traffic will continue to pass through the bridge, but SecureSphere will not inspect it.

Reverse Proxy Deployments

For Web traffic only, an inline Gateway can be configured as a Reverse Proxy. In a Reverse Proxy, traffic intended for a Web server first passes through the Reverse Proxy.

This section contains the following:

Reverse Proxy Overview 26
Transparent Reverse Proxy Overview 27
Non-Transparent Reverse Proxy Overview 28
Reverse Proxy with Load Balancer 31

Reverse Proxy Overview

There are three kinds of Reverse Proxies:

- Transparent Reverse Proxy (TRP)
- Non-Transparent Reverse Proxies (two types):

- Kernel Reverse Proxy (KRP)
- Apache Reverse Proxy (ARP)

Reverse Proxy Mode Advantages

Some of the advantages of Reverse Proxy mode are:

- A Reverse Proxy assembles packets into a complete message, inspects the message and confirms that it complies with the relevant policies, and only then transmits the packets to the server.
- Reverse Proxy mode supports features that require changing data, for example, cookie signing, SSL decryption, *etc*.
- Reverse Proxy mode supports features that require changing the destination IP address.
- Traffic is decrypted only once, by the SecureSphere. The server sees only unencrypted traffic, improving server performance.
- In the same way, SSL decryption is offloaded from the server to the SecureSphere Gateway.
- Reverse Proxy mode enables SecureSphere to be implemented in legacy deployments without the need to reconfigure networks (drop-in replacement).

Transparent Reverse Proxy Overview

This section reviews the different types of Transparent Proxies and includes the following:

Transparent Reverse Proxy 27
Transparent Reverse Proxy - Selected Web Servers 28

Transparent Reverse Proxy

In Transparent Reverse Proxy mode, the client is unaware of the Reverse Proxy, and connects directly to the server. The SecureSphere Gateway is not visible to the client or to the server, which see each others' real IP addresses.

The SecureSphere Gateway is in bridge mode, but additionally functions as a Reverse Proxy for the servers specified in the SecureSphere GUI (in the **Transparent Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**). All other traffic, including non-Web traffic, is bridged through. In this way, the same SecureSphere Gateway protecting many Web and database server groups can act as a Reverse Proxy for some or all of the Web server groups it protects, and as a bridge for the other server groups.

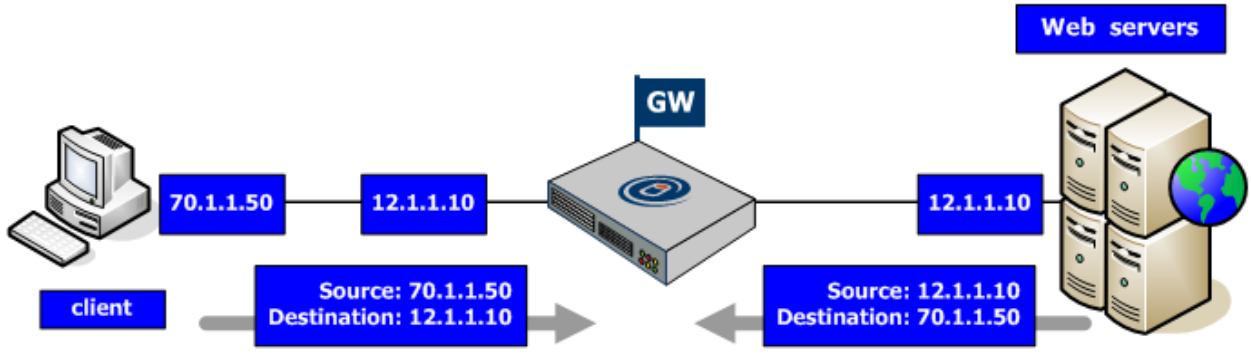


Figure 4: Transparent Reverse Proxy Deployment

The client begins the session by sending packets to the server's IP address (12.1.1.10). The SecureSphere Gateway intercepts connections destined for the server, inspects them and forwards them on to the server.

The server sees the connections as coming from the client's IP address (70.1.1.50) and replies to that address. The return connection passes through the SecureSphere Gateway, which inspects them and forwards them on to the client.

For information on configuring a SecureSphere Gateway in Transparent Reverse Proxy, see Configuring Transparent Reverse Proxy on page 108.

Transparent Reverse Proxy - Selected Web Servers

In the deployment depicted in below, the SecureSphere Gateway acts as a bridge, protecting all the servers (the two Web servers and the database server), but for one of the Web servers, the SecureSphere Gateway also acts as a Transparent Reverse Proxy.

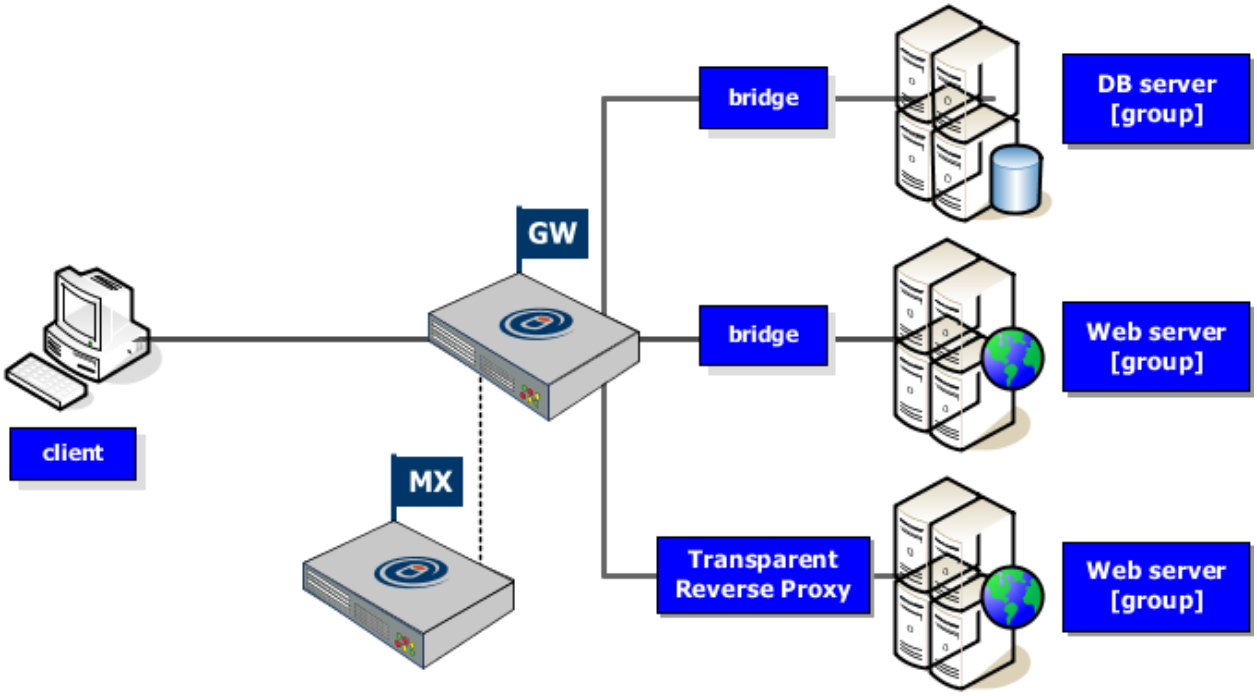


Figure 5: Transparent Reverse Proxy - Selected Web Servers

Non-Transparent Reverse Proxy Overview

There are two kinds of non-Transparent Reverse Proxy: Kernel Reverse Proxy (KRP) and Apache Reverse Proxy (ARP). These can be deployed on a SecureSphere Gateway as follows:

- Kernel Reverse Proxy only
- Apache Reverse Proxy only
- Kernel Reverse Proxy and Apache Kernel Reverse Proxy together on the same Gateway, where the ARP is deployed between the KRP and the Web server.

In non-Transparent Reverse Proxy mode, **c**lients connect to the IP address of the SecureSphere Gateway, which acts as a Reverse Proxy for the Web servers it protects. In contrast to transparent deployments, in non-transparent deployments the SecureSphere Gateway is visible to both client and server, while the client and server are not directly visible to each other.

The Web server groups are specified in the SecureSphere GUI (in the **Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**). The SecureSphere Gateway does not act as a bridge. The Non-Transparent Reverse Proxy listens on the specified ports and ignores all other traffic.

Among the advantages of non-Transparent Reverse Proxies are:

- SSL off-loading: the ability to terminate SSL sessions, reducing the load on the server
- The ability to sign and encrypt cookies
- The ability to protect web servers located in multiple subnets, not necessarily close to each other or to the Gateway

Some of the advantages of Kernel Reverse Proxy mode are:

- Improved proxy functionality (connection termination, including SSL termination)
- Improved proxy performance

Note: In Non-Transparent Reverse Proxy deployments, if the SecureSphere Gateway fails, the Web server becomes unreachable, so High Availability is usually implemented to maintain connectivity. For more information, see Gateway High Availability on page 343.

Kernel Reverse Proxy (KRP)

In a Kernel Reverse Proxy deployment, the client begins the session by sending packets to the SecureSphere Gateway's inbound IP address. The SecureSphere Gateway inspects the packets and, based on the rules, opens a second connection to the server, changing the packet's source IP address to the SecureSphere Gateway's outbound IP address and the destination IP address to the real IP address of the server.

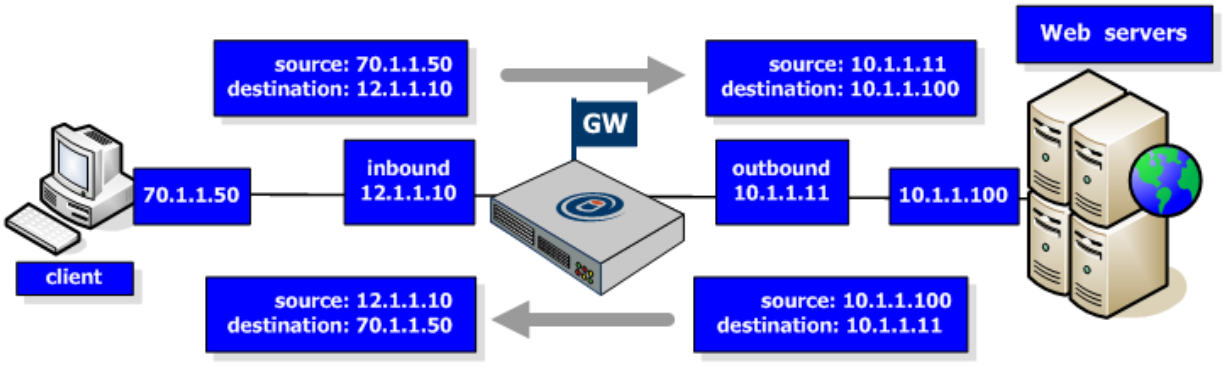


Figure 6: Non-Transparent Reverse Proxy Deployment

The server sends the return packets to the SecureSphere Gateway, which inspects the packets and forwards them to the client, changing the source IP address to the SecureSphere Gateway's inbound IP addresses, and the destination IP address to that of the client.

From the client's point of view, the server is the SecureSphere Gateway's inbound IP address. From the server's point-of-view, the client is the Gateway's outbound IP address.

Notes:

- In KRP mode, the maximum length of a POST request without multi-parts is 2MB.
- When there is a request sent to the non existing page or the protected server is down, it returns blocking response and no alert is generated, as it is not an attack. For example, when the protected server is down, an error page is sent, but it does not indicate that the user attacked the server or performed a violation to the server.

The SecureSphere Gateway does not act as a bridge. The Kernel Reverse Proxy listens on the specified ports and ignores all other traffic.

The following sections describe a number of possible non-Transparent Reverse Proxy deployments.

Kernel Reverse Proxy ("One Arm")

A "one arm" Kernel Reverse Proxy deployment is one where the inbound and outbound interfaces are the same. This configuration simplifies routing.

Apache Reverse Proxy (ARP)

In contrast to a Kernel Reverse Proxy, the Apache Reverse Proxy runs in user space. Otherwise it is similar to the Kernel Reverse Proxy.

In this case too, the SecureSphere Gateway does not act as a bridge. The Apache Reverse Proxy listens on the specified ports and ignores all other traffic.

Apache and Kernel Reverse Proxy on the Same Gateway

SecureSphere's Kernel Reverse Proxy has the advantage of speed and efficiency, but with some limitations such as the capability to rewrite full body content or to directly work with external authentication processes (SSO). In most scenarios these capabilities are not required. When they are required, they can be implemented by combing SecureSphere's Kernel Reverse Proxy with an Apache Reverse proxy running in user space on the same SecureSphere Gateway.

When Apache Reverse Proxy and Kernel Reverse Proxy are implemented together, the Kernel Reverse Proxy redirects matching traffic (based on URl and/or hostname) to the Apache Reverse Proxy, which manipulates the session as required and communicates with the backend server. Return traffic follows the opposite route.

In the configuration shown in the below figure, the client connects to the SecureSphere Gateway, and the packets pass through both the SecureSphere Kernel Reverse Proxy (KRP) and the Apache Reverse Proxy (ARP).

Altogether there are three connections:

- Client <-> Kernel Reverse Proxy
- Kernel Reverse Proxy <-> Apache Reverse Proxy
- Apache Reverse Proxy <-> Backend Web server

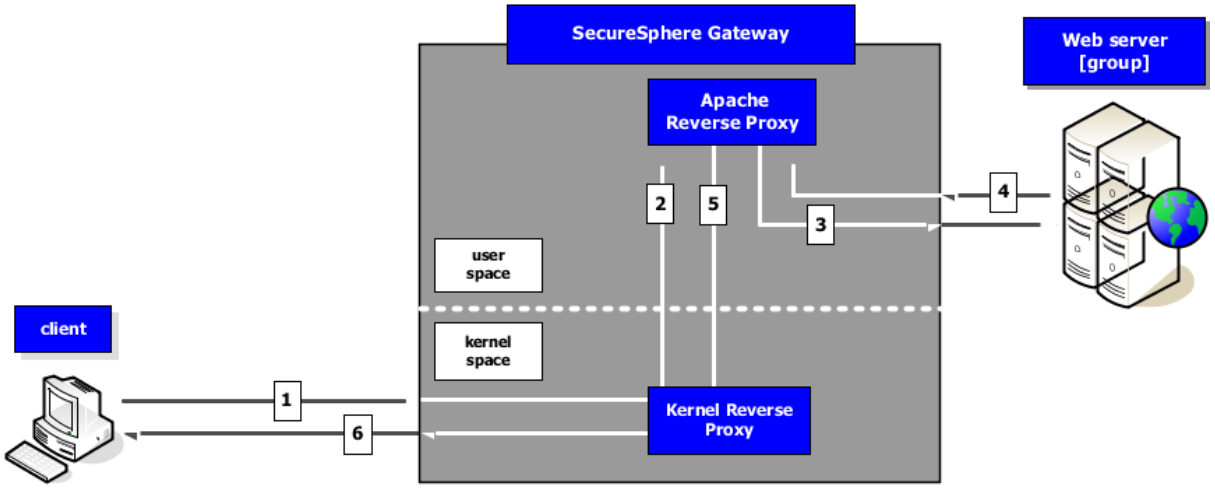


Figure 7: Inline Mode - Apache and Kernel Reverse Proxies

1. The client connects to the SecureSphere Gateway's Kernel Reverse Proxy.
2. The Kernel Reverse Proxy inspects the packets and, based on the rules, opens a second connection to the Apache Reverse Proxy, running in user mode on the same SecureSphere Gateway.
3. The Apache Reverse Proxy opens a third connection to the Web server.
4. The Web server sends the response to the Apache Reverse Proxy.

5. The Apache Reverse Proxy sends the response to the Kernel Reverse Proxy.
6. The Kernel Reverse Proxy inspects the response and sends it to the client.

For information on configuring a SecureSphere Gateway as a Kernel Reverse Proxy and an Apache Reverse Proxy, see Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 111.

Reverse Proxy with Load Balancer

Load Balancers provide a number of advantages:

- High Availability — If one of the SecureSphere Gateways fails, the Load Balancer will direct traffic to one of the other Gateways.
- Increased Bandwidth — Since the processing load is shared among SecureSphere Gateways, more total bandwidth is available.

Both Kernel Reverse Proxy and Apache Reverse Proxy can be implemented with Load Balancers.

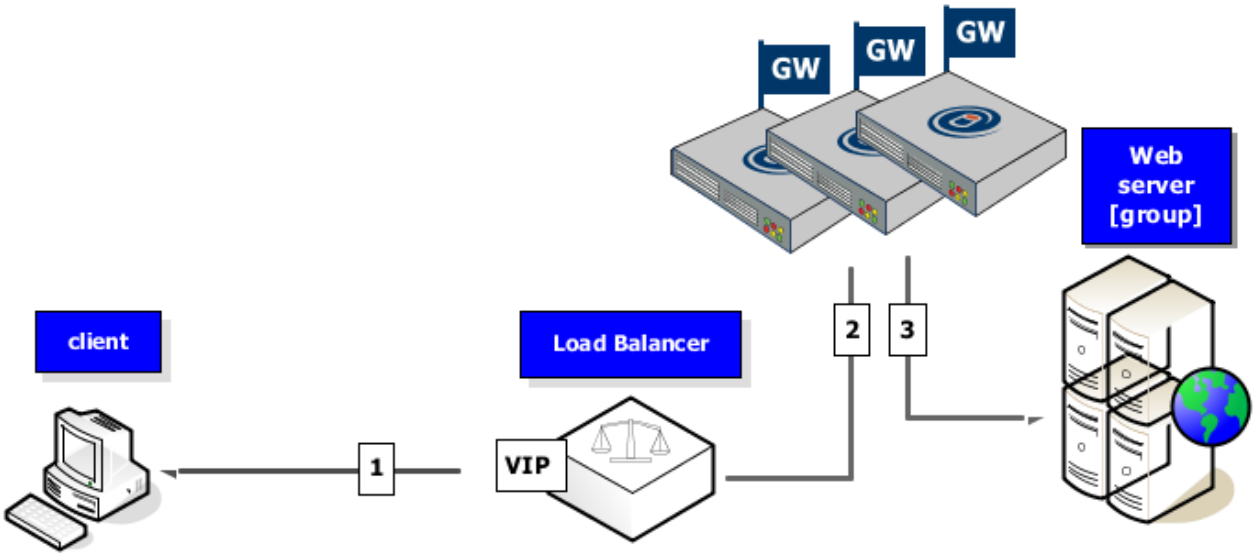


Figure 8: Inline Gateway - NonTransparent RP with Load Balancer

1. The client connects to the external VIP (Virtual IP) address of the Load Balancer.
2. The Load Balancer opens a connection to a Reverse Proxy on one of the SecureSphere Gateways.
3. The Reverse Proxy inspects the packets and, based on the rules, sends the connection to one of the Web servers.

Return traffic follows the opposite path.

Features Available in the Each Deployment Mode

The table below lists some of the SecureSphere features for which the deployment mode affects the feature's availability. Note that sniffing deployments do not support proxies.

Some SecureSphere Features for which the Deployment Mode Affects the Feature's Availability

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes		
			Transparent RP	Kernel RP (Non-Transparent)	Apache RP (Non- Transparent)
Inspect TCP handshake	V	V	V	V	V
Normalize traffic (decode encoded content, such as URL-encoded or UTF-encoded content)	V	V	V	V	V
Decrypt and inspect SSL (either interface to a FIPS-compliant HSM or store an encrypted copy of the SSL key)	V	V	V	V	V
HTTP / SQL protocol conformance	V	V	V	V	V
Session / cookie protection	V	V	V	V	V
Input validation (white list)	V	V	V	V	V
Attack detection (black list, including application, network, Web server and OS attacks)	V	V	V	V	V
Correlated attack validation	V	V	V	V	V
Block attacks	**V**	V*	**V**	**V**	**V**
Block data leaks (inspect outgoing traffic for sensitive data such as SSN, credit card numbers, CVV numbers and data matching custom signatures)	**V**	X*	**V**	**V**	**V**
Rewrite content	X	X	**V**	**V**	**V**

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes		
			Transparent RP	Kernel RP (Non-Transparent)	Apache RP (Non- Transparent)
Application level auditing (record complete HTTP request and server response code)	V	V	V	V	V
Ignore IP Group (Server Groups)	**V**	**V**	X	X	X
Application user tracking	V	V	V	V	V
Firewall and Network Protocol Violation Policies enforced	**V**	X	X	X	X
Redirect client to an error page	**V**	X*	**V**	**V**	**V**

*A SecureSphere Gateway in sniffing mode cannot send an error page or block a connection. Instead, it sends a TCP reset to the server. The client sees a timeout message.

CHAPTER 3

Platforms and Installation

This chapter describes the installation and configuration for SecureSphere appliances, and includes:

Forward Compatibility 34
Preparing the Appliance 35
Installing the SecureSphere Software 35
Working with Management Servers After the Installation 41
Replacing Gateways 43

Forward Compatibility

In the past, Gateways and MXs had to be the same version in order for the MX to manage the Gateway.

Beginning with SecureSphere version 9.5, this is no longer the case. SecureSphere MXs are forward compatible with SecureSphere Gateways version 9.5 and higher. For example, a version 9.5 Gateway can be managed by a SecureSphere version 9.0 Patch 1 MX (but not by a pre-version 9.0 Patch 1 MX).

This means that when upgrading from SecureSphere version 9.0 or higher, you should upgrade the Gateways first and then upgrade the MX. This results in significantly reduced downtime during the upgrade process.

If, however, you are upgrading from SecureSphere versions prior to 9.0, you should follow the previous scenario: upgrade the MX first and then upgrade the Gateway.



Note:

- The MX must be version 9.0 Patch 1 or higher.
- This feature is not available for Onebox.
- If the MX and the Gateway are different SecureSphere versions, features added to SecureSphere after the version of the MX are not available. For example, a version 9.5 Gateway

feature cannot be configured on a version 9.0 MX. The feature cannot be used until the MX is also upgraded.

Preparing the Appliance

The steps for installing and configuring the SecureSphere appliance are as follows:

1. Connect the appliance to the network as described in the appliance's **Quick Start Guide**, which is packaged with the appliance.
2. If necessary, install the SecureSphere software, as described in Installing the SecureSphere Software on page 35.
3. Execute the First Time Login procedure, as described in Initial Configuration on page 47. During this procedure, you will define passwords, interfaces and other networking parameters.
4. Review the section Working with Management Servers After the Installation on page 41 and perform the procedures relevant to your deployment, as described there.
5. Configure SecureSphere using the GUI, connect to the Management Server by pointing your browser to https://<IP address>:8083, where <IP address> is the IP address of the management port on the MX.

Before configuring the SecureSphere software, you should open the required ports on firewalls in the network. For more information, see Configuring Firewall Ports on page 379.

Additionally, it is recommended that you provide an uninterrupted power source (UPS) for the appliance.

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.

This section contains the following information:

G Series Appliances (Except G2 and G2-2) 35
G2 and G2-2 Appliances 37
X and M Series Appliances 39
Creating a Bootable USB Device Containing the Installation Image 40

G Series Appliances (Except G2 and G2-2)

Installation Monitoring for G Series

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 37.

Installing G Series Appliances From USB

To install from a USB device:

1. Turn off the appliance.
2. Boot the appliance and press the F2 key to enter the BIOS.

3. Go to **Boot Options**.
4. Set **Boot Option #1** to **CD**.
5. Set **Boot Option #2** to **RAID**.
6. Set **Boot Option #3** to **GE**.
7. Set **Boot Option #4** to **ERI Shell**.
8. Set **USB Boot Priority** to **Enabled**.
9. Save and exit the BIOS.
10. Turn off the appliance.
11. Plug a USB device with the SecureSphere recovery image into the appliance USB port.
12. Connect to the appliance using keyboard and VGA or serial monitor.

    For information about connecting a serial console, see Connecting to the G2 or G2-2 Appliance Using a Serial Console on page 39.
13. Turn the appliance on.
14. After the appliance boots, select the fifth installation option (VGA).

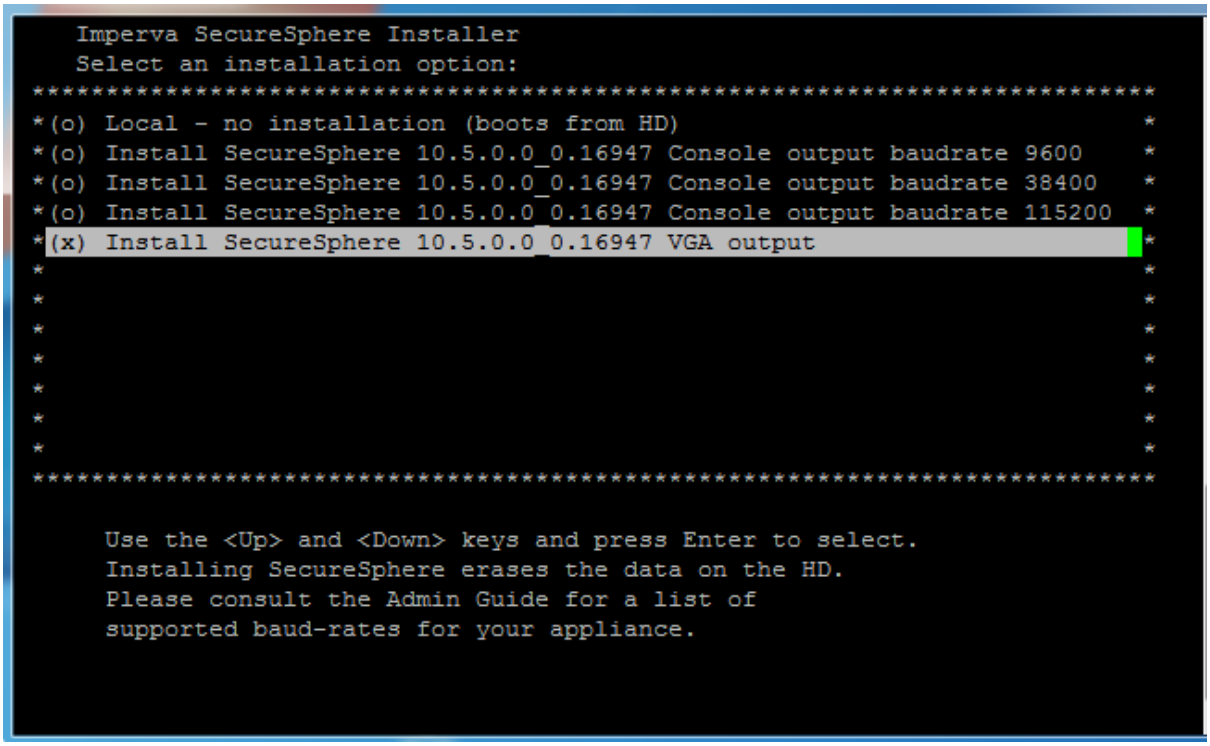


Figure 9: Installing from USB

15. 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.

Connecting to the G Series Appliance Using a Serial Console



Note: This section is not relevant to G2 and G2-2 appliances. See Installation Monitoring "Installation Monitoring for G2 and G2-2 Appliances" on page 37 for information about commenting a serial device to these appliances.

To connect to the appliance using a serial console:

1. 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 described in the table **Serial Console Settings** below.

   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.

2. Power ON the appliance
3. Press F2 and enter BIOS configuration.
4. Select **Main->Quiet Boot [Disable]**
5. Select **Advanced->PCI Configuration->On Board NIC 1/2 ROM [Enable]**
6. Configure Server Management > Console Redirection, as follows:
   - Console Redirection [Serial Port A] (DB9)
   - Flow Control [None]
   - Baud Rate [38.4K]
   - Terminal Type [VT100+]
   - Legacy OS Redirection [Enable]

Serial Console Settings

Setting	Value
baud rate	38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	VT-100 or VT-UTF8

G2 and G2-2 Appliances

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

Installation Monitoring for G2 and G2-2 Appliances

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 G2 or G2-2 Appliance Using a Serial Console on page 39.

Installing G2 and G2-2 Appliances from USB

To install from a USB device:

1. Turn off the appliance.
2. Plug a USB flash drive with the SecureSphere recovery image into the appliance USB port.
3. Boot the appliance and press the F2 key to enter the BIOS.
4. Go to **Advanced Bios Features**.
5. Change **USB Flash Disk Type** to **HDD**.
6. Change **First Boot device** to **USB-HDD**.
7. Change **Second Boot Device** to **USB-HDD**.
8. Change **Third Boot Device** to **USB-HDD**.
9. Set **Boot Other Device** to **Disabled**.
10. Set **USB emulation** to **HDD**.
11. Save and exit the BIOS.
12. Turn off the appliance.
13. Connect to the appliance using keyboard and VGA or serial monitor.

    For information about connecting a serial console, see Connecting to the G2 or G2-2 Appliance Using a Serial Console on page 39.
14. Turn the appliance on.
15. After the appliance boots, select the fifth installation option.

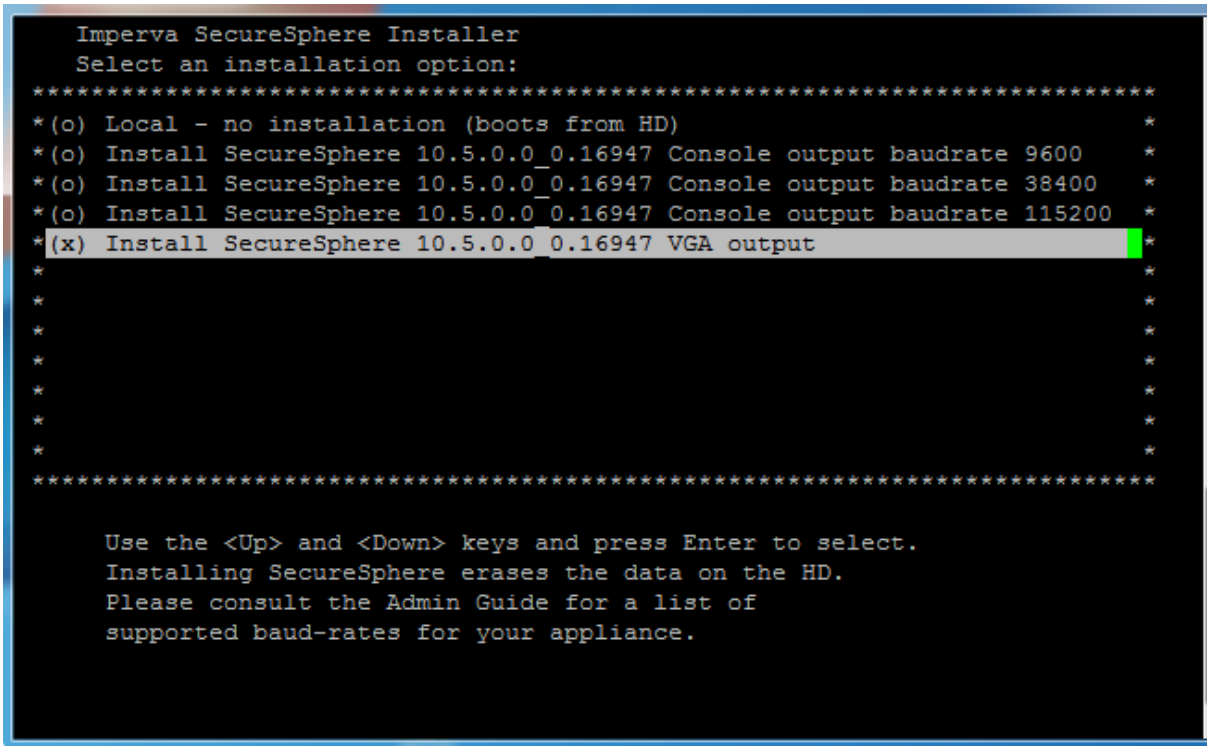


Figure 10: Installing from USB

16. 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.

17. Reboot the appliance.

Connecting to the G2 or G2-2 Appliance Using a Serial Console

To connect to the appliance using a serial console:

1. Boot the appliance and press the DEL key to enter the BIOS.
2. Go to **Advanced Bios Features**.
3. Set **Console Redirection** to **Enabled**.
4. Set **Baud Rate** to **38400**.
5. Set **Agent Connect via** to **NULL**.
6. Set **Agent wait time (sec)** to **3**.
7. Set **Agent after boot** to **Enabled**.
8. Save and exit the BIOS.

X and M Series Appliances

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
baud rate	9600/38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	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 Creating a Bootable USB Device Containing the Installation Image on page 40).
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, M110
   - Select the third installation option (baudrate 38400) for X1000, X2000, X2500, X4500, X6500, M100, M150

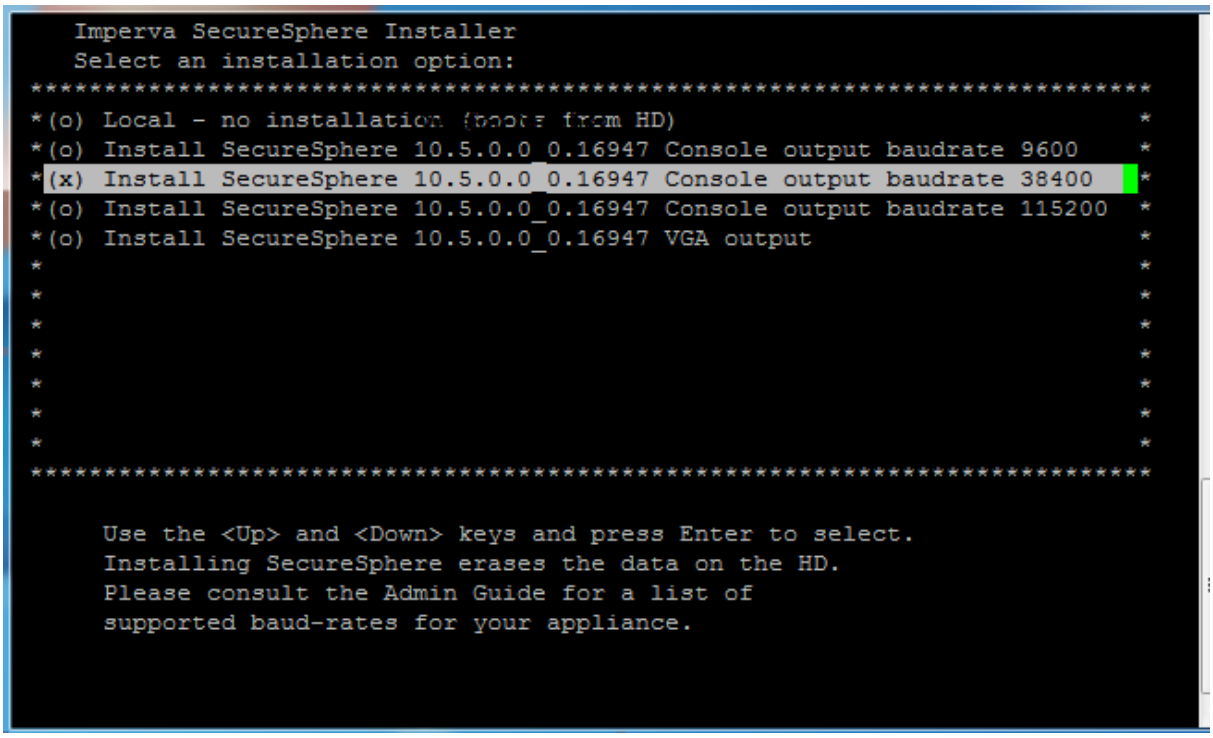


Figure 11: USB Boot Menu

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.
   - **32 bit**: `/Downloads/SecureSphere_Setup/v11.0/32Bit/USB/`

- **64 bit**: `/Downloads/SecureSphere_Setup/v11.0/64Bit/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.

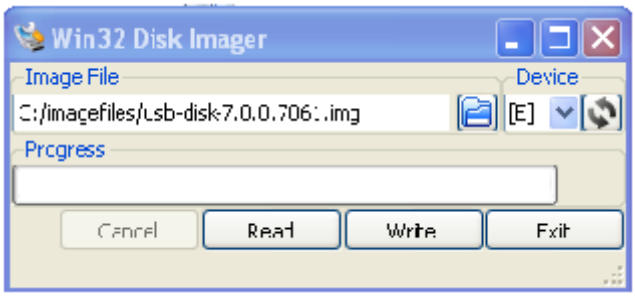


Figure 12: Win32 Disk Imager window

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**.

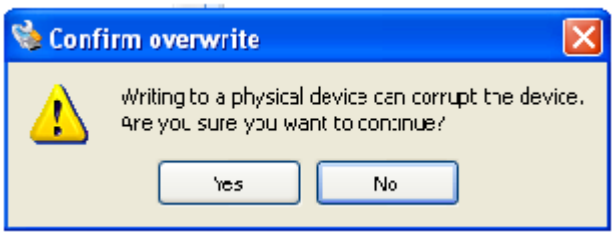


Figure 13: Confirm overwrite window

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.

Working with Management Servers After the Installation

Connecting to the Management Server

To configure SecureSphere using the GUI, connect to the Management Server by pointing your browser to https://<IP address>:8083, where <IP address> is the IP address of the management port on the MX.

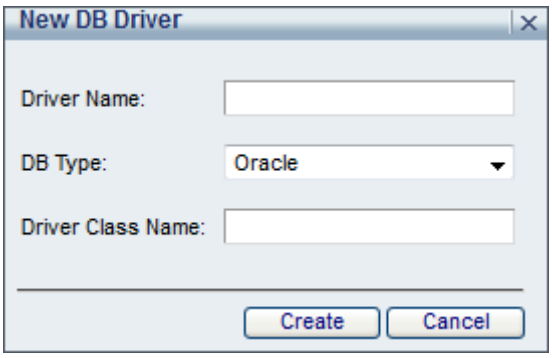
Note: For more information, see the **Quick Start Guide** for your MX appliance.

MySQL Users

When using a MySQL Database, you need to install the driver.

To install the MySQL driver:

1. In the Admin workspace, select **System Definitions**.
2. In the **System Definitions** pane, under **Management Server Settings**, select **Remote DB Connectivity**.
3. Under **User Defined Drivers**, click the **New** button. The **New DB Driver** dialog opens.



4. Enter a **Driver Name** of your choice.
5. Under **DB Type**, select **MySQL**.
6. Enter `com.mysql.jdbc.Driver` as the **Driver Class Name**, and click **Create**. The new driver appears under **User Defined Drivers**.
7. Open the newly-created driver.
8. Under **Driver Jar Files**, click the **New** button. The **Upload Driver Jar File** dialog opens.
9. Browse to the driver jar file: `mysql-connector-java-5.1.7-bin.jar`. Click **Upload**.

Note: You can find the driver file at the MySQL website, http://dev.mysql.com/. Download it to your computer.

10. Under **User Defined Connections**, click the **New** button.
11. In the **Name** field, enter a name of your choice.
12. In the **Connection String** field, enter: `jdbc:mysql://$host:$port/$dbname?useInformationSchema=true&;defaultFetchSize=40`.

Notes:

- The parameter `useInformationSchema` sets whether or not DB metadata is accessible. This data is required for DB classification, DB URM and DB assessments. The default value `is false`.
- The parameter `defaultFetchSize` sets the size of the data that is returned from the database on a query. The default value `is 0`. Leaving the default value may lead to out of memory errors.

13. Click **Save**.

Replacing Gateways

Replacing a Faulty Gateway

You can replace a faulty gateway with a new gateway without losing its configuration. You must take care to configure the new gateway so that it retains the original IP and listener. In this way, MX is unaware of the hardware change. The Agents continue to work as before. It requires installation of the latest patch for v10.0 on both the gateway and the management server.



Note: Carry out First-Time Login only after the patch has been installed.



Note: This procedure is not relevant for Onebox.

To perform gateway pre-installation (applicable to RMA or similar scenario):

1. Ensure the faulty gateway is disconnected from the network.
2. In **Setup > Gateways**, ensure that the gateway's status is **Disconnected**.
3. Connect the replacement gateway to both the network, and to a KVM or console. If connected to a console, see Connecting to the G Series Appliance Using a Serial Console on page 37.
4. Logon to the console.
   `localhost login:` appears.
5. Logon to the system using the username `root` and the password `webco123`.
6. Copy SecureSphere v10.0 patch 1 to your SecureSphere appliance in one of the following ways:
   - Copy the patch using a USB device. See the procedure **To copy the patch using a USB device** below.
   - Copy the patch using the local network. See the procedure **To copy the patch over the network** below.
7. Once you have copied the patch, complete the installation and then register the new gateway in place of the faulty gateway, see the procedure **To register the new gateway in place of the faulty gateway** below.

To copy the patch using a USB device:

1. Plug in the USB device containing the patch.
2. Enter the command `dmesg`. The following is an example of the output displayed.

```
[191682.326208] USB Mass Storage support registered.
[191687.392733] Vendor: Kingston Model: DataTraveler G3 Rev: PMAP
[191687.392753] Type: Direct-Access ANSI SCSI revision: 00
[191688.688480] SCSI device sdb: 30481152 512-byte hdwr sectors (15606 MB)
[191688.689104] sdb: Write Protect is off
[191688.689107] sdb: Mode Sense: 23 00 00 00
[191688.689110] sdb: assuming drive cache: write through
[191688.691972] SCSI device sdb: 30481152 512-byte hdwr sectors (15606 MB)
[191688.692596] sdb: Write Protect is off
[191688.692599] sdb: Mode Sense: 23 00 00 00
```

```
[191688.692602] sdb: assuming drive cache: write through
[191688.692606]  sdb: sdb1 sdb2 sdb3 sdb4 < sdb5 sdb6 >
[191688.715805] sd 2:0:0:0: Attached scsi removable disk sdb
```

3. Note the sd value of the USB device. In this case, it is **b**.
4. Create the mounting directory on the new gateway by entering `mkdir /mnt/usb`.
5. Execute the mount by entering `mount /dev/sd<sd value>/mnt/usb`". In this case the sd value is **b**.
6. Copy the desired patch to the **/tmp** directory by entering `cp <patchName> /tmp`.

To copy the patch over the network:

1. Assign an IP address to the new gateway by entering `ifconfig eth<interface number> <IP address> netmask <subnet mask>`.

   For example: `ifconfig eth0 10.0.1.100 netmask 255.255.255.0`.
2. Define a default gateway for networking by entering `route add -net 0.0.0.0/0 gw <default gateway ip>`.

   For example: `route add -net 0.0.0.0/0 gw 10.0.1.254`.
3. Enable mounting over a network by entering `service portmap start`.

   You are now able to mount a NFS share, SCP or FTP to copy the desired patch to your **/tmp** directory.

To complete the gateway installation:

1. Grant execution permissions by entering `chmod a+x /tmp/<PatchName.x>`.
2. Install the patch by entering `./tmp/<PatchName.x>`.

   A message appears stating that the patch has been successfully installed.
3. Reboot your machine.

   The `localhost login :` prompt appears. Type `reboot`

To register the new gateway in place of the faulty gateway:

1. Execute First-Time Login using user `secure` and password `secure`.
2. In **Setup > Gateways**, configure the new gateway so that its IP address and listener parameters are identical to those of the replaced gateway. The listener parameters are case-sensitive.
3. During First-Time Login, answer the following questions as shown:
   - `Is this gateway deployed in order to replace another gateway ? [y/n]` - enter `y`.
   - `Name of gateway to be replaced [Case sensitive]:` - enter the name of the old gateway to be replaced exactly as it appears in the SecureSphere GUI, in the **Setup > Gateways** tab.
   - When prompted for the machine's management IP address, enter the same IP address as that of the gateway you are replacing. Failure to do so may require reregistration of your SecureSphere Agents.

   On successful completion of the procedure, the new gateway's status is Connected.
4. Set up your agent listener on the new gateway by entering `impcfg` and then following the on-screen instructions. Use the same listener parameters as those of the previous gateway. See Configuring Listeners in the Administrator's Guide.

   The agents appear as Connected.

Replacing a Faulty Gateway Using an Already-Configured Gateway

In the event where a new gateway was inadvertently installed without using the proper procedure at the First-Time Login so that it has different parameters from the gateway it is intended to replace, carry out the following procedure.

To replace a faulty gateway using an already-configured gateway:

1. Use SSH to connect to the new gateway.
2. Ensure that the SecureSphere v10.0 patch 1 is installed.
3. Reboot the gateway. Type `reboot`

4. Use SSH to connect to the new gateway.
5. Stop the gateway by entering `impctl gateway stop`.
6. Unregister the gateway by entering `impct gateway unregister`.
7. In the SecureSphere GUI, select **Setup > Gateways**.
8. When the stopped and unregistered gateway shows a Disconnected status, delete it by selecting it and clicking **x**.
   A confirmation dialog appears.
9. To confirm deletion, click **Yes**.
10. Re-register the gateway. Type `impctl gateway register --name-of-gateway-to-replace=<gw_name>`
11. Restart the gateway. Type `impctl gateway start`
12. Configure the IP address using impcfg. See Configuring a Gateway on page 68. Ensure that the IP address is the same as that of the gateway you replaced.
    On successful completion of the procedure, the new gateway's status is Connected.
13. Set up your agent listener on the new gateway by entering `impcfg` and then following the on-screen instructions. Use the same listener parameters as those of the previous gateway. See Configuring Listeners on page 122.

The agents appear as Connected.

CHAPTER 4

Configuring SecureSphere

This chapter describes the initial installation procedure for SecureSphere, and also the additional configuration steps required before SecureSphere can become operational, including:

Initial Configuration 47

Automating First Time Login 47

IPv6 50

SecureSphere Users 54

Appliance OS 55

Gateway/Management Server Appliance Initial Configuration 57

Configuring SecureSphere Using the Command Line Tools 58

Configuring a Management Server 67

Configuring a Gateway 68

Configuring a Data Assessment Server (DAS) 85

Configuring the Platform 89

Configuring SecureSphere Routes 107

Configuring Transparent Reverse Proxy 108

Configuring Kernel Reverse Proxy 109

Configuring Apache Reverse Proxy 109

Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway 111

Switching Deployments 112

Initial Configuration

For instructions for the physical configuration of the SecureSphere appliance, see the **Getting Started Guide**. For instructions on automating first time login, see Automating First Time Login on page 47.

During the First Time Login, the administrator is required to define the following:

- Password for the appliance's `root` user.
- Password for the `secure` user (the SecureSphere administrative "superuser").
- For Management Servers, for the `system` user (the password for the internal SecureSphere database).
- Additional OS users (CLI users), who are able to run a restricted set of OS commands (see CLI Users on page 55).
- Appliance's management interface IP address (in CIDR format).

  This interface is usually used for managing SecureSphere Gateways, so that the interface used to manage the Management Server is distinct from the interface the Management Server uses to communicate with the Gateways.
- Appliance's management interface (NIC) for out-of-band management.
- Appliance's hostname.
- Appliance's default Gateway.
- Appliance's operation mode (sniffing, bridge, *etc.*).
- For virtual appliances, the appliance model number.
- Time zone.

Once these parameters have been defined, the administrator defines the additional configuration parameters required to make the SecureSphere operational. The additional parameters which must be defined depend on the appliance's operational mode (Management Server, sniffing Gateway, bridge, *etc.*).



Note: A SecureSphere Management Server is also known as an **MX**.

Automating First Time Login

First time login is typically run using the CLI and is guided with a set of prompts. You can alternatively configure a script to run, thereby enabling you to automate the process. This may be useful when provisioning a number of SecureSphere gateways at once.

Notes:

- This procedure cannot be conducted to configure SecureSphere in bridge mode, it can only be used to configure the SecureSphere gateway in sniffing mode
- This procedure can only be conducted when running first time login on a gateway. It cannot be conducted to install a management server.

To run first time login:

- Use the following command:

```
impctl auto-ftl --management-interface=<value>  --management-ip-with-cidr=<value>
--default-gateway=<value> --root-password=<value> --user-name=<value>
--user-password=<value> --host-name=<value> --set-sniffing --secure-password=<value>
--imperva-password=<value> --grub-password=<value> --management-server-ip=<value>
--appliance-type=<value>
```

Note the arguments listed above are mandatory arguments, whose descriptions are listed below.

You additionally have optional arguments for the following:

Mandatory Arguments 48

General Optional Arguments 49
Optional Cluster Arguments 49
Optional Listener Arguments 49
Optional Sniffing Arguments 50
Common Arguments 50

Mandatory Arguments

This section lists mandatory arguments that need to be used when conducting first time login.

Argument	Description
--management-interface=<value>	Sets the management interface for this appliance. For example, eth0.
--management-ip-with-cidr=<value>	Sets the IP address of the management interface. IP address should be IPv4.
--default-gateway=<value>	Sets the IP address of the default gateway. IP address should be IPv4.
--root-password=<value>	Creates a password for the Linux root user.
--user-name=<value>	Creates an individual named account. This account will be used to access the CLI on the appliance. This is done to achieve a higher level of security by introducing an additional layer which provides improved auditing of the appliance users.
--user-password=<value>	Creates a password for the individual named account.
--host-name=<value>	Sets the host name. Host name will also be used as the Gateway name. If you enter a Fully Qualified Domain Name (FQDN) the leftmost part of the name will be used for hostname. For example, if you enter mycomputer.mydomain.com the host name will be mycomputer.
--set-sniffing	Sets the SecureSphere gateway operation mode to sniffing.
--secure-password=<value>	Configures a password for the secure user. The user secure (the SecureSphere administrative user) is used to register the SecureSphere Gateway with a SecureSphere Management Server.
--imperva-password=<value>	Configures an imperva password. This password is primarily used to register remote agents to the gateway.
--grub-password=<value>	Changes the bootloader password: Protecting the bootloader with a password is essential to denying unauthorized persons physical access to the console.
--management-server-ip=<value>	Sets the IP Address (IPv4) of the Management Server. The Management Server must be accessible over the management interface of this Gateway.
--appliance-type=<value>	Sets the SecureSphere virtual gateway model. For example v1000, v2500, v4500, v6500.

General Optional Arguments

This section lists general arguments that can to be used when conducting first time login (optional).

Argument	Description
--root-allowed-ips=<value>	Sets IP addresses from which users can login as root user.
--gateway-group=<value>	Sets the gateway group name.
--timezone=<value>	Sets the time zone. You must use Posix TZ format. For example, GST-10 is a zone named GST that is 10 hours ahead (east) of UTC.
--time-servers=<value>	Sets the IP address of NTP servers. Must be an IPv4 address. To add more than one NTP server IP address, separate IP addresses with a space.
--dns-servers=<value>	Sets the IP address of the DNS name servers. Must be an IPv4 address. To add more than one name server, separate name server IP addresses with a space.
--dns-domain=<value>	Sets the DNS domain name.

Optional Cluster Arguments

This section lists arguments specifically related to configuring a cluster that can to be used when conducting first time login (optional).

Argument	Description
--cluster-enabled	Enables cluster configuration.
--cluster-interface=<value>	Sets the network interface of the cluster. For example, eth1.
--cluster-ip-with-cidr=<value>	Sets the IP address of the cluster.
--cluster-port=<value>	Sets the port of the cluster.

Optional Listener Arguments

This section lists arguments specifically related to configuring a listener that can to be used when conducting first time login (optional).

Argument	Description
--listener-ip-with-cidr=<value>	Sets the IP Address of the listener. Use a [IPv4 address/CIDR].
--listener-port=<value>	Sets the port of the listener.
--listener-device=<value>	Sets the network interface of the listener. For example, eth1.
--listener-ssl=<value>	Enables SSL. The SecureSphere gateway can be configured to utilize SSL to encrypt the remote agent listener. Note this option may increase CPU consumption on the Agent host. Choose true if you would like to enable SSL (otherwise - choose false).

Optional Sniffing Arguments

This section lists arguments specifically related to configuring sniffing or blocking options that can to be used when conducting first time login (optional).

Argument	Description
--sniffing-device=<value>	Sets the network interface for sniffing. For example, eth1.
--blocking-device=<value>	Sets the network interface for blocking. For example, eth1.
--blocking-net=<value>	Sets/modifies the subnet used for blocking.

Common Arguments

This section lists options that can to be used to set the location of the command log or display help when conducting first time login (optional).

Argument	Description
--log-file=<VALUE>	Changes the command's log file location (default- /var/log/auto-ftl.log).
--help	Displays help for first time login.

IPv6

This section describes IPv6 support, which is implemented in SecureSphere beginning with Version 9.0.



Note: Additional information regarding IPv6 support is given in the "Basic Configuration" chapter of the **SecureSphere User Guide**.

SecureSphere Features Which Support IPv6

SecureSphere supports IPv6 in the following SecureSphere features:

- WAF
- MX-Gateway communications
- VRRP
- communications with external systems which support IPv6 (see External Systems on page 53)

Overview

The section provides an overview of IPv6 support. It reviews the following:

IPV6 Address Formats 51
CIDR Notation 51

IPV6 Address Formats

IPv6 addresses are 128 bits long and are written in eight groups of four hexadecimal digits separated by colons, for example, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**. The hexadecimal digits are case-insensitive.

An IPv6 address can be abbreviated according to following rules:

- Leading zeroes within a 16-bit value may be omitted. For example, the address **fe80:0000:0000:0000:0202:b3ff:fe1e:8329** may be written as **fe80:0:0:0:202:b3ff:fe1e:8329**.
- A single occurrence of any number of consecutive groups of zeroes within an address may be replaced by a double colon. For example, **fe80:0:0:0:202:b3ff:fe1e:8329** becomes **fe80::202:b3ff:fe1e:8329**.

So the same IPv6 address can be represented in several different ways. For example, the following are all equivalent:

2001:db8:0:0:1:0:0:1	2001:0db8::1:0:0:1
2001:0db8:0:0:1:0:0:1	2001:db8:0:0:1::1
2001:db8::1:0:0:1	2001:db8:0000:0:1::1
2001:db8::0:1:0:0:1	2001:DB8:0:0:1::1

Whenever an IPv6 address is entered into SecureSphere, after it is saved it is displayed in the "long" format. For an example, when the IPv6 address as "**2001:DB8::**" is entered in the GUI and saved, it is then displayed as "**2001:0DB8:0000:0000:0000:0000:0000:0000**", except in `impcfg`, where one of the short forms (not necessarily the shortest) of the address is used.



Note: SecureSphere is able to recognize the equivalence of these different forms of the same IPv6 address, except in certain cases where the IPv6 address is treated as a character string, for example, in lookup datasets and in ThreatRadar.

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation explicitly specifies the number of bits in an IP address denoting the network, in contrast to the netmask notation which indirectly specifies the number of bits. For example, a netmask of **255.255.255.0** indicates (for IPv4 addresses) a network in which the first 24 bits of an IP address denote the network. In CIDR notation, one simply writes "/24" after the IP address (for example, **123.124.125.126/24**). The advantages of CIDR notation over the netmask notation are simplicity and scalability from IPv4 to IPv6.

The IP address/netmask notation is no longer permitted for both IPv4 and IPv6 addresses. Instead, CIDR notation is used both in the SecureSphere GUI and `impcfg`.



Note: CIDR notation is used only when specifying a network or when configuring a local IP address where it is necessary to specify the subnet. CIDR is not to be used when specifying a remote IP address, for example, that of an NTP server or a DNS server, or when defining the Management Server of a SecureSphere Gateway.
When `impcfg` requires that CIDR notation be used, it specifies so in the prompt, for example, "Enter IP address/CIDR". If "CIDR" is not specified in the prompt, it must not be entered.

IPv4 / IPv6 Dual Stack

The source and destination IP addresses of an IP packet must both be either IPv4 or IPv6. It is not possible for one of the addresses to be IPv4 and the other to be IPv6. The solution is to assign to a device both an IPv4 and an IPv6 address, so that the device can communicate on both protocols.

So, for example, if an MX manages both IPv4 and IPv6 Gateways, the MX's management or LAN interface (whichever one the Gateways communicate with) must have both an IPv4 and an IPv6 address.

At various points in the SecureSphere GUI and in `impcfg`, users are prevented from trying to define an IPv4-IPv6 connection.

SecureSphere MX and Gateway

SecureSphere Management Servers and Gateways can have IPv6 addresses. An MX can simultaneously manage Gateways with IPv4 addresses together with Gateways with IPv6 addresses, if the MX's management interface or its LAN interface has both an IPv4 and an IPv6 address.

A SecureSphere GUI user can point his browser to an IPv6 SecureSphere MX.

IPv6 is supported for Gateway syslog, MX syslog and MX-Gateway communications.

Hostnames

When entering a hostname, the ":" is not allowed.

IPv6 in impcfg and impctl

The following points are relevant specifically to `impcfg` and `impctl`.

1. `impcfg` and `impctl` accept both IPv4 and IPv6 addresses, for example for DNS and NTP servers. In all cases where IPv6 is supported (note the exceptions below) the user can assign to the same entity:
   - both IPv4 and IPv6 addresses
   - an IPv4 address only
   - an IPv6 address only
   - An IPv6 address can be specified for external servers (for example, DNS or NTP), only if either the appliance's management or LAN interface has an IPv6 address.
2. When `impcfg` asks the user to enter an IP address for a management or LAN interface, it allows the user to enter either an IPv4 or IPv6 address, and then asks the user if he wants to enter an address of the other type (so, for example, if he enters an IPv4 address, he will be asked if he wants to enter an IPv6 address, and he can either enter one or not enter one).
3. As noted above, network masks have been replaced by CIDR notations for both IPv4 and IPv6 addresses. While in the past, users were asked to enter an IP address/netmask pair (for local IP addresses and network addresses - for example, when specifying a static route - and for sniffing mode blocking masks), users are now asked (for both IPv4 and IPv6 addresses) to enter an IP address in CIDR notation.

   For example, instead of entering an IP address of **144.234.123.0** and a netmask of **255.255.255.0**, the user enters only one field: **144.234.123.0/24**.

   Note: CIDR notation is used only when specifying a network or when configuring a local IP address where it is necessary to specify the subnet. CIDR is not to be used when specifying a remote IP address, for example, that of an NTP server or a DNS server, or when defining the Management Server of a SecureSphere Gateway.
   When `impcfg` requires that CIDR notation be used, it specifies so in the prompt, for example, "Enter IP address/CIDR". If "CIDR" is not specified in the prompt, it must not be entered.
4. Link-local addresses (**fe80::/10**) are not supported and cannot be entered anywhere in `impcfg`.
5. Default Gateway - this is unchanged (for both IPv4 and IPv6), that is, the user is not required to specify the device (interface).
6. VRRP routes (KRP and legacy, that is, pre version 7.0, SecureSphere Agents) - `impcfg` tries to deduce the device (interface) from the aliases, and if it cannot, it asks the user.
7. `portguard` supports IPv6. Access to the appliance's link-local addresses is blocked.

8. When configuring a SecureSphere Gateway, the user will not be able to specify an IPv6 management interface if the MX management and LAN interfaces both have only IPv4 addresses. If the Gateway's management or LAN interface has both IPv4 and IPv6 addresses, then the communication will depend on whether the user specifies the IPv4 or IPv6 address as the management interface on the Gateway.
9. `ping6` is not blocked for SecureSphere appliances (as `ping` is).

Exceptions

The following exceptions apply:

1. IPv6 addresses for SecureSphere Agent and SecureSphere Agent for DB2 z/OS listeners are not supported in this version. Users will not be able to enter IPv6 addresses for them in `impcfg`. This means that a SecureSphere Gateway which listens to a SecureSphere Agent or a SecureSphere Agent for DB2 z/OS must have an IPv4 address.
2. IPv6 is not supported in MX-HA.
3. IPv6 VRRP static routes are not supported.
4. IPv6 DHCP is not supported (DAS).
5. The following commands have been deprecated:
   - `impctl vrrp gateway show`
   - `impctl vrrp gateway config`

External Systems

SecureSphere MX can communicate over IPv6 with the external systems listed below:

External System	
HTTP Proxy	Admin > System Definitions > External HTTP Settings
SMTP	SMTP servers with IPv6 addresses.
SNMP	SNMP nodes with IPv6 addresses.
LDAP endpoint access	LDAP servers with IPv6 addresses.
LDAP authentication	
FTP archive	Archiving audit files to an IPv6 archive via FTP.
SCP archive	Archiving audit files to an IPv6 archive via SCP.
Remote Access to Infra to IPv6	Enables remote access to servers, to run shell scripts remotely.

SecureSphere MX **cannot** communicate over IPv6 with the external systems listed below:

External System		Reason
Oracle Server	Admin > System Definitions > External Systems	
MSSQL Server		
MySQL Server		This product is not yet IPv6 compliant.
SQL		
HTTP/HTTPS archive	Admin > System Definitions > Action Interfaces	
BMC Remedy		This product is not yet IPv6 compliant.

SecureSphere Users

The Different SecureSphere Users

Several users are created for a SecureSphere appliance, each for a different purpose. Each of these users has its own password.

SecureSphere Users and Passwords

SecureSphere User	Description
CLI Users	
root	This is the all-powerful superuser of the appliance's Linux-based OS. This user is created automatically by SecureSphere when it is installed. **Note:** You cannot login to the appliance as root over SSH. To administer the appliance remotely, login as a CLI user other than `root` and `secure` over SSH and enter the `admin` command. For more information, see CLI Users on page 55. For information about changing this user's password, see Configuring the Platform on page 89.
secure	This is the SecureSphere administrative superuser, who has complete read-write access to all SecureSphere components, including configuring the appliance with the command line application `impcfg`. This user is created automatically by SecureSphere when it is installed. This user is not the same as the internal SecureSphere "admin" GUI user (see below). **Note:** You cannot login to the appliance as `secure` over SSH. For information about changing this user's password, see Configuring a Management Server on page 67 and Configuring a Gateway on page 68.
system	This is the user of the internal SecureSphere database, and is required only on a SecureSphere Management Server. This user is created automatically by SecureSphere when it is installed. For information about changing this user's password, see Configuring a Management Server on page 67.
Other CLI users	These are OS users, at least one of whom must be defined during the First Time Login, who are allowed to run a restricted number of OS commands in order to administer the appliance. The sessions of other CLI users (but not of `root` and `secure`) are logged to the file `/var/log/secure` to enforce accountability. For information on logging these sessions to `syslog`, see the Imperva Knowledge Base. For more information, see CLI Users on page 55.
SecureSphere GUI users	
These are the users of the SecureSphere GUI, some of whom are defined within SecureSphere as administrators. One user ("admin") is pre-defined and has complete read-write privileges, including that of defining other SecureSphere GUI administrators and users. For more information, see Users and Permissions on page 193.	

Appliance OS

The appliance OS is based on a "hardened" version of Linux.

CLI Users

At least one other CLI user (in addition to the CLI users created automatically by SecureSphere: `root`, `secure` and `system`) must be defined during the First Time Login. You can define any number of additional CLI users using `impcfg`.

Other CLI users are allowed to run only the following OS commands:

- `impcfg` - This command opens a shell session as the `secure` user.
- `passwd`
- `admin` - This command opens a shell session as the `root` user.

All commands issued by CLI users (except `root` and `secure`) are logged to the file `/var/log/secure`. For information on logging these sessions to `syslog`, see the Imperva Knowledge Base.



Note:

- It is possible to connect to the appliance as a CLI user over the SFTP protocol (for example, using WinSCP) but not over SCP.
- By default, you cannot connect to the appliance as `root` or `secure` over SSH. To login as `root`, you must first connect as a CLI user and use the `admin` command. However, you can specify an IP address from which user `root` is allowed to login over SSH using the following command:

```
impctl hardening config --root-source-ip-exception=<IP address>
```

- A CLI is limited to a maximum length of 14 characters.
- Only lowercase letters can be used to create CLI usernames. Uppercase is not supported

Authentication Failure

CLI users other than `root` and `secure` who fail authentication 6 times are locked out for 30 minutes. An administrator can release the lock before this time using `impcfg` (see Manage User on page 103).

Passwords

The minimum length for SecureSphere passwords (`root` and `secure` and other CLI users) is 7 characters, and the maximum length is 255 characters. Passwords may consist only of alphabetic characters, numeric characters, and some special characters.

The password for `system` must be less than 30 characters long.



Warning: It is of the utmost importance that all these passwords be "strong" (that is, difficult to guess), and that they be treated with discretion.

Passwords for other CLI users (not those of `root` and `secure`) expire after 90 days, and users are warned, starting 7 days before the expiration date, that they must change their password. After the 90 day period, users have an additional 7 day grace period to change their password. If they do not change their password during that time they are locked out until an administrator releases the lock (see Manage User on page 103).

After changing their passwords, users must wait at least 7 days before changing their passwords again.

Passwords are hashed using SHA-2.

Timeout

Shell sessions for all users are timed out after 15 minutes.

Date Changes

Whenever the system date is changed, a log event is sent to syslog, so that administrators are notified.

Locally, the events are stored in `/var/log/secure`.

Gateway/Management Server Appliance Initial Configuration

When configuring an appliance for the first time (the first-time login), the `impcfg` wizard guides you through a question and answer procedure. After confirming that all the information is correct, this initial configuration is applied to the system components using the `impctl` application. This process takes between 45 minutes and 1 hour for a Management Server, where a database must be created and initialized. On a Gateway the process takes between 10-15 minutes.



Note: The instructions for the initial configuration (first-time login) are given in the appliance's Quick Start Guide, which is packaged with the appliance.

- If you configure a DNS client during the first-time login, make sure you specify the IP address of a real DNS server.

Additional configuration is performed using the menu-driven `impcfg` command line application. For more information, see Configuring SecureSphere Using the Command Line Tools on page 58.

If you run the First-Time configuration script after the appliance has already been configured, the previous configuration is overwritten.

First-Time Login (Configuration)

The First-Time Login is usually via the console port. Once the appliance has a management IP address, further interactions can be via the console, or SSH. Make sure that SSH communication is possible for remote appliance configuration (port 22 on the firewall must be open).



Note: You cannot login to the appliance as `root`, `secure`, or `system` over SSH.

For more information on which firewall ports must be open, see Configuring Firewall Ports on page 379.

If you are configuring a Management Server and a Gateway, configure the Management Server first. The reason is that when a Gateway is configured, the Management Server must be running and reachable. If not, the Gateway must be restarted when the Management Server is alive and reachable. Check the Gateway status from the Gateway Management screen (see Configuring a Gateway on page 68).

After the First-Time Login, you can configure SecureSphere using the GUI by pointing the browser to `https://<IP address of MX>:8083`.

Registering a Gateway

In order to establish the relationship between a SecureSphere Gateway and its Management Server, you must register the Gateway to the Management Server. Registration is part of the First Time Login procedure for the Gateway, during which you will be asked to specify the IP address of the Management Server.



Note: You cannot specify a CIDR address for a SecureSphere Gateway's Management Server. For more information about when CIDR can be used, see CIDR Notation on page 51.

You can unregister a Gateway from one Management Server and register it to a different Management Server using the `impcfg` application. For more information, see Configuring a Gateway on page 68.

Configuring SecureSphere Using the Command Line Tools

There are two command line interface (CLI) tools with which you can configure SecureSphere on the Management Server and Gateways:

- `impcfg` is a menu-based configuration tool that can be used to configure both the Management Server and the Gateway.

  `impcfg` is described in this section.
- `impctl` is a lower level configuration tool. `impcfg` runs `impctl` on the SecureSphere appliance to deploy the configuration which the administrator defines in `impcfg`.

  `impctl` is described in Command Line Interface on page 422.

Command Line Tools and MX-HA

This section describes command line tools and how to use them in an MX-HA environment. It includes the following:

Changing MX Properties in an MX-HA Environment 58
Stopping and Starting the MX in an MX-HA Environment 59

Changing MX Properties in an MX-HA Environment



Note: For more information about MX-HA, see Management Server High Availability (MX-HA) on page 353.

In an MX-HA environment, it is not possible to perform any of the following appliance-level actions on the MX using the command line tools `impcfg` and `impctl`:

- change the MX's network properties, for example, its IP addresses, interfaces (devices), *etc.*
- change the MX's hostname
- change MX passwords (`system` and `secure` - see SecureSphere Users on page 54 for more information)



Warning: `impcfg` and `impctl` will let you make these changes, and you will not receive an error message, but the MX and the MX-HA environment may become non-operational and you will have to re-install MX-HA.

If you need to perform any of the above changes, you must uninstall MX-HA on both the primary and secondary MXs, make the changes and then reinstall MX-HA.

Stopping and Starting the MX in an MX-HA Environment

The correct way start and stop the MX in an MX-HA environment is by using the following commands:

```
impctl server ha start
impctl server ha stop
```



Warning: Do not use `impcfg` or `impctl` to start and stop the MX as you would in a non-MX-HA environment (as described in Configuring a Management Server on page 67). Use only the above commands.

impcfg

By default, there are two ways to run `impcfg`:

- Log in to the appliance remotely over SSH as another CLI user and run `impcfg`.
- Log in to the appliance remotely over SSH as another CLI user and use the `admin` command, and then run `impcfg`.



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.

Top Screen

The first screen displayed is the **Top** screen, shown in the following figure.

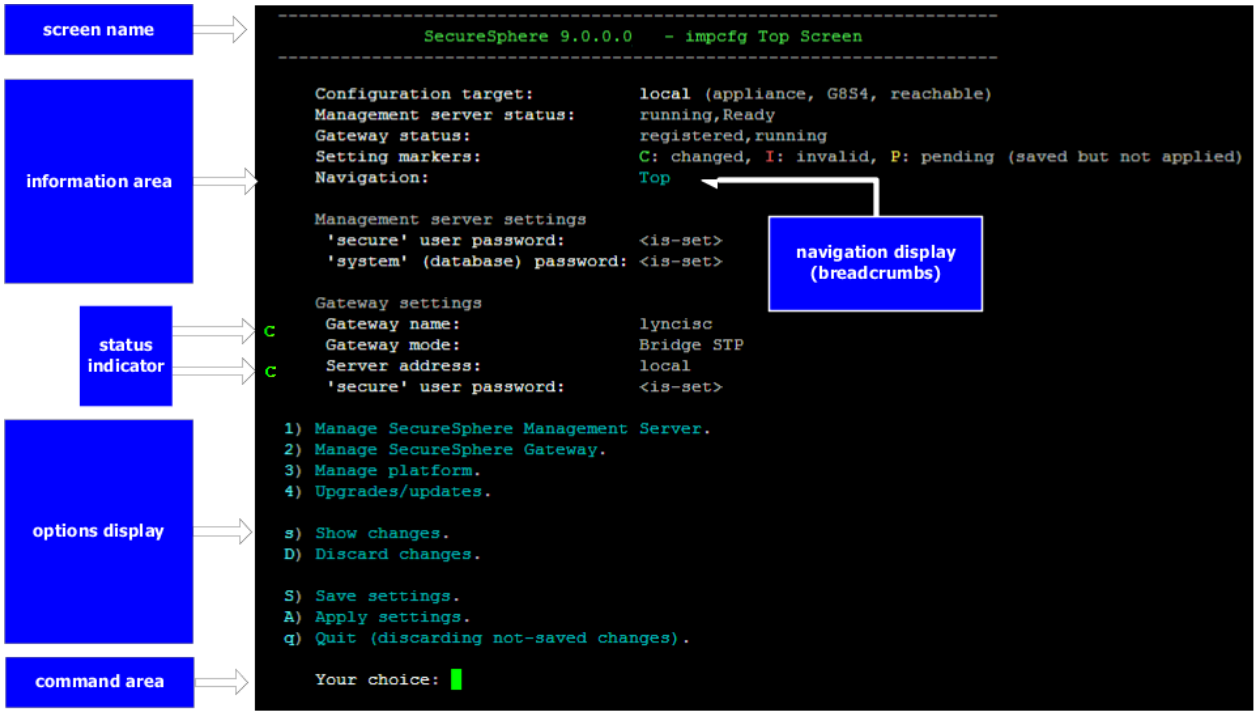


Figure 14: impcfg Top Screen

The following table lists the components of all `impcfg` screens.

impcfg Screen Components

Screen Component	color	Description
screen name	**green**	The name of the screen and the SecureSphere version number.
information area		Displays information about the Gateway or Management Server being configured.
status indicator		Entries in the information area may be shown with the following status indicators: • I (red I) = invalid setting • C (green C) = changed (unsaved setting) • P (yellow P) = pending (saved but not applied)
options display	**blue**	A list of command numbers with their meanings. In addition to the numbered commands, you can choose one of the following: • e = End this level • j = Jump up to a previous level • t = Jump up to the top level • q = Quit (discarding non-saved changes) • S = Save settings • A = Apply settings • C = Confirm action
command area	**green**	The area in which the administrator enters commands and their arguments. Often, the default value [in square brackets] is displayed here.
navigation display	**blue**	"Breadcrumbs" indicating which screen is currently being displayed and the path followed to reach it. In the example shown in tje figure **impcfg Screen Layout** above. We are in the Gateway Management screen, so the path is **Top -> Gateway**.

In the **Top** screen, you can configure SecureSphere by entering the number of one of the displayed options, as listed below.

Top Screen Configuration Options

Option	Name	Description
The numbers of these options change, depending on the appliance's configuration	Manage Secure Sphere Server	Configure and manage a SecureSphere Management Server. For more information, see Configuring a Management Server on page 67.
	Manage SecureSphere Gateway	Configure and manage a SecureSphere Gateway. For more information, see Configuring a Gateway on page 68.
	Manage SecureSphere DAS	Configure and manage a SecureSphere Data Assessment Server (DAS). For more information, see Configuring a Data Assessment Server (DAS) on page 85.

Option	Name	Description
	Manage platform	Configure and manage an appliance. For more information, see Configuring the Platform on page 89.
	Upgrades / updates	This option is reserved for future use.
	Reconfigure as OneBox (immediate)	Reconfigure the DAS as a Onebox. For more information, see Reconfiguring the DAS as a Onebox on page 88
s	Show changes	Display a list of changes made in this session.
D	Discard changes	Discard all the changes made in this session.
S	Save settings	Save all the configuration changes made in this session without applying them.
A	Apply settings	This option performs the following: • Saves all the configuration changes made in this session. • Applies all pending configuration changes (including changes made in previous sessions which were saved but not applied) to the Management Server and/or Gateways as appropriate. Except for those `impcfg` menu items which explicitly indicate that they are executed immediately, all changes take effect only when they are applied using this option.

impcfg Functionality Map

The table impcfg Functionality Map below shows the complete `impcfg` functionality.



Note: (I) means immediate activation, that is, the command is executed and, if relevant, the SecureSphere database is updated immediately.

impcfg Functionality Map

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Server	Deactivate server			Configuring a Management Server on page 67
	Restart server (I)			
	Stop server (I)			
	Change management password			

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
	Change database password			
	Deactivate server			
Manage SecureSphere Gateway	Perform actions (start, stop, etc.)	Unregister gateway **(I)**		Configuring a Gateway on page 68
		Soft gateway restart **(I)**		
		Hard gateway restart (teardown/prepare resources) **(I)**		
		Stop gateway **(I)**		
		Refresh gateway status **(I)**		
Manage SecureSphere Gateway *(continued)*	Change gateway name			
	Change server address /password			
	Change operation mode	Sniffing		Configuring a Gateway as a Sniffing Gateway on page 74 **Note:** The management server must be running when you execute this command.
		Bridge STP		Configuring a Gateway as a Bridge on page 72
		Bridge IMPVHA		
		Reverse Proxy Apache		Configuring Apache Reverse Proxy on page 109
		Reverse Proxy Kernel		Configuring Kernel Reverse Proxy on page 109
		vPath		
	Manage hardware	enable nCipher HSM		Hardware Security

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
	security modules (HSM)	enable SafeNet HSM		Modules (HSM) on page 426 XXX
	Manage remote agentSecureSphere Agents	Add a legacy (pre 7.0) agent		Managing Remote AgentSecureSphere Agents "Managing SecureSphere Agents" on page 79
		Modify a legacy (pre 7.0) agent		
		Delete a legacy (pre 7.0) agent		
		Add agent listener		
		Delete agent listener		
		Add z/OS agent listener(s)		
		Delete z/OS agent listener		
		Manage remote agentSecureSphere Agent routes		
Manage SecureSphere Gateway *(continued)*	Manage interfaces and routes *(for a bridge)*	Create bridge		Configuring a Gateway as a Bridge on page 72
		Delete bridge		
		Toggle STP on a bridge		
		Toggle High Availability on a Bridge		
	Manage interfaces and routes *(for a sniffing gateway)*	Set sniffing interface(s)		Configuring a Gateway as a Sniffing Gateway on page 74
		Set blocking interface		
		Add/modify blocking mask		
		Delete blocking mask		
	Manage interfaces and routes *(for an Apache Reverse Proxy)*	Add alias		Configuring Apache Reverse Proxy on page 109
		Modify Alias		
		Delete Alias		

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
		Enable high availability		
		Manage reverse proxy (kernel) routes		
	Change Cluster Configuration	Add/Modify Cluster Configuration		SecureSphere Database Security User Guide
		Delete Cluster		
		Change IPv4 Address		
		Change Device		
		Change Port		
Manage SecureSphere DAS	Deactivate server			Configuring a Data Assessment Server (DAS) on page 85
	Restart server (I)			
	Stop server (I)			
	Change management password			
	Change database password			
	Deactivate server			
Manage platform	Manage network	Management interface	Change device	Management Interface on page 93
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		LAN interface	Change device	LAN Interface on page 94
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		Default gateway		Default Gateway on page 96
		Static routes	Add route	Static Routes on page 96
			Delete route	
		Name Resolution (DNS client)	Enable DNS client	Name Resolution (DNS client) on page 97
			Set domain	
			Set search list	
			Set name servers	

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
		Locate network devices		Locate Network Devices on page 98
	Manage time	Add time server		Time Servers on page 100
		Delete time server		
	Manage users			Users Management on page 100
	Manage hostname			Hostname Management on page 105
	Manage bootloader password			Bootloader Password Management on page 106
	Reboot the appliance **(I)**			Configuring the Platform on page 89
	Shutdown the appliance **(I)**			Configuring the Platform on page 89
Upgrade / updates				This option is reserved for future use.

Configuring a Management Server

You can:

- Activate/deactivate the Management Server
- Start/stop/reactivate the Management Server
- Change management and database passwords



Note: The management and database passwords cannot be changed form the OS command line.

To configure the Management Server:

1. In the **Top** Screen, select option **1) Manage SecureSphere Server**.
   The **Server Management** screen is displayed.

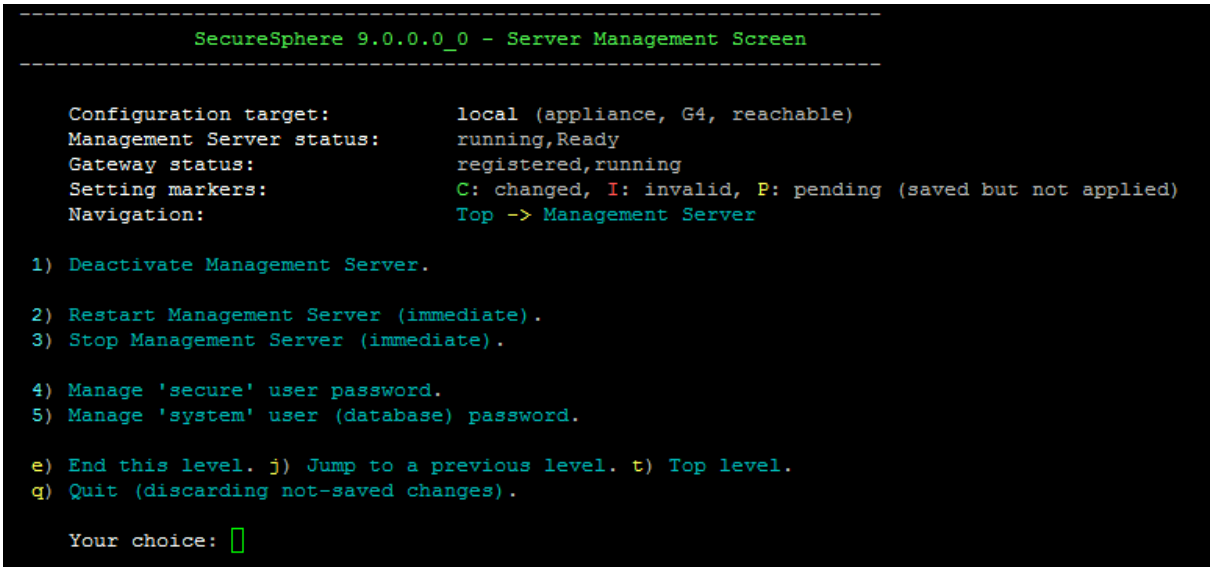


Figure 15: Server Management screen

2. Select one of the following options, as listed below.

Appliance Management Configuration Options

Option	Name	Description
1	**Deactivate Management Server**	Stop the Management Server and do not restart it when the appliance boots. This would be done, for example, when converting a Onebox to a Gateway (which will be managed by another Management Server).
	Activate Management Server	Start the Management Server the next time the appliance boots. This would be done, for example, when converting a Gateway to a Onebox.

Option	Name	Description
2	**Restart Management Server (immediate)**	Stop and then start the Management Server.
3	**Stop Management Server (immediate)**	Stop the Management Server.
4	**Manage 'secure' user password**	Change the password of the `secure` user. **Note:** This option restarts the Management Server and is not supported in Management Server High Availability deployments. For more information about Management Server High Availability, see Management Server High Availability (MX-HA) on page 353. For more information about passwords, see SecureSphere Users on page 54.
5	**Manage 'system' user (database) password**	Change the password of the internal SecureSphere database. **Note:** This password must be less than 30 characters. **Note:** This option restarts the Management Server and is not supported in Management Server High Availability deployments. For more information about Management Server High Availability, see Management Server High Availability (MX-HA) on page 353. For more information about passwords, see SecureSphere Users on page 54.

Configuring a Gateway

You can:

- Activate/deactivate, register/unregister, start/stop/reactivate the Gateway
- Change the Gateway name, server address/password, and operation mode
- Manage HSM, high availability, SecureSphere Agents, and interfaces
- Configure a Cluster



Note: When a Gateway is registered to an MX, the Gateway sends the MX information about its network interfaces, and users may configure the Gateway on the basis of that information. If any of the Gateway network interfaces is deleted or removed, the MX's Gateway configuration based on the deleted interface becomes invalid. The user must then either restore the network interface on the Gateway or modify the Gateway configuration on the MX accordingly.

To configure the Gateway:

1. In the **Top** Screen, select option **2) Manage SecureSphere Gateway**. The **Gateway Management** Screen is displayed.

```
-------------------------------------------------------------------------
              SecureSphere 10.5.0.0 - Gateway Management Screen
-------------------------------------------------------------------------

    Configuration target:          local (appliance, V2500, reachable)
    Gateway status:                registered,running
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway

    Gateway settings
     Gateway name:                 dan-gw
     Gateway mode:                 Sniffing
     Server address:               10.100.46.163
     'secure' user password:       <is-set>
     Cluster Configurtion:         Disable

 1) Perform actions (start, stop, etc.).

 2) Change gateway name.
 3) Change Management Server address/password.
 4) Change operation mode.
 5) Manage hardware security modules (HSM).
 6) Manage remote agents.
 7) Manage interfaces and routes.
 8) Change virtual gateway model.
 9) Change Cluster configuration.

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice:
```

Figure 16: Gateway Management Screen

2. Select one of the following options, as listed below.

Appliance Management Configuration Options

Option	Name	Description
1	**Perform actions (start, stop, *etc.*)**	Start, stop or unregister the Gateway.
2	**Change gateway name**	Change the Gateway's name. This option is used, for example, when a Gateway is moved to another network.
3	**Change Management server address/password**	Specify a different Management Server for the Gateway. This option is used, for example, when a Gateway is moved to another network, and will be managed by a different Management Server. **Note:** You cannot specify a CIDR address for a Gateway's Management Server. For more information about when CIDR can be used, see CIDR Notation on page 51. When you apply this change, the Gateway registers with the Management Server.
4	**Change operation mode**	Change the mode of the Gateway to one of the following: • **sniffing**: For more information, see Configuring a Gateway as a Sniffing Gateway on page 74. • **bridge STP**: For more information, see Configuring a Gateway as a Bridge on page 72. • **bridge IMPVHA**: For more information, see Configuring a Gateway as a Bridge on page 72. • **Reverse Proxy Apache**: For more information, see Configuring Apache Reverse Proxy on page 109. • **Reverse Proxy Kernel**: For more information, see Configuring a Kernel Reverse Proxy on page 180. **See also**: Topologies and Deployment on page 23.
5	**Manage hardware security modules (HSM)**	For more information, see Hardware Security Modules (HSM) on page 385.
6	**Manage SecureSphere Agents**	For more information, see Managing SecureSphere Agents on page 79.
7	**Manage Interfaces and Routes**	For more information, see Configuring a Gateway as a Bridge on page 72.
8	**Change Virtual Gateway Model**	Fore more information, see Configuring a Gateway for a Cluster as Part of First Time Login on page 75.

Option	Name	Description
9	**Change Cluster Configuration**	For more information, see Configuring a Cluster "Configuring a Gateway for a Cluster" on page 75.
Note: Beginning with version 10.0 of SecureSphere, Kernel Reverse Proxy (KRP) is configured in the SecureSphere GUI (**Setup** > **Gateways**, >**Details** tab). For more information, see Configuring a Kernel Reverse Proxy on page 180.		

Gateway Actions

You can:

- Register/unregister the Gateway
- Restart the Gateway (soft or hard restart)
- Stop the Gateway
- Refresh the Gateway's status

To perform Gateway actions:

1. In the **Top** Screen, select option **2) Manage SecureSphere Gateway**.
2. In the **Gateway Management** screen, select **1) Perform actions (start, stop, etc.)**.

```
-------------------------------------------------------------------
             SecureSphere 9.0.0.0_0 - Gateway Management Screen
-------------------------------------------------------------------

    Configuration target:          local (appliance, G4, reachable)
    Management Server status:      running,Ready
    Gateway status:                registered,running
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway -> Actions

    Gateway settings
     Gateway name:                 pavonis
     Gateway mode:                 Bridge STP
     Server address:               local
     'secure' user password:       <is-set>

 1) Unregister gateway (immediate).
 2) Soft gateway restart (immediate).
 3) Hard gateway restart (teardown/prepare resources) (immediate).
 4) Stop gateway (immediate).
 5) Refresh gateway status (immediate).

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice:
```

Figure 17: Gateway Actions screen

3. Select one of the following options, as listed below.

Gateway Actions Options

Option	Name	Description
1	**Register / Unregister gateway (immediate)**	Register or unregister the Gateway from the Management Server.
2	**Soft gateway restart (immediate)**	
3	**Hard gateway restart (immediate)**	
4	**Stop gateway (immediate)**	
5	**Refresh gateway status (immediate)**	

Configuring a Gateway as a Bridge

To configure a Gateway as a bridge:

1. In the **Gateway Management** screen (as described in Configuring a Gateway on page 68), select option **4) Change operation mode**.
2. From the list of operation modes (shown below), select one of the bridge modes:
   - Bridge STP or
   - Bridge IMPVHA.

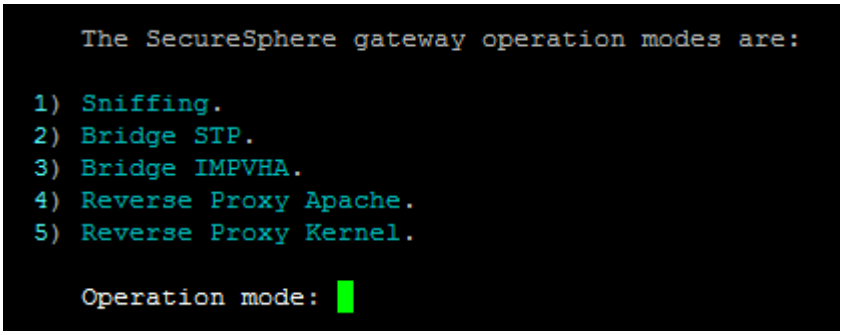


Figure 18: Gateway Operation Modes

Note: Bridge STP mode does not correctly pass Cisco PVST PDU packets. Use Bridge IMPVHA mode if you need to pass these packets.

3. In the **Gateway Management** screen (as described in Configuring a Gateway on page 68), select option **7) Manage interfaces and routes**.

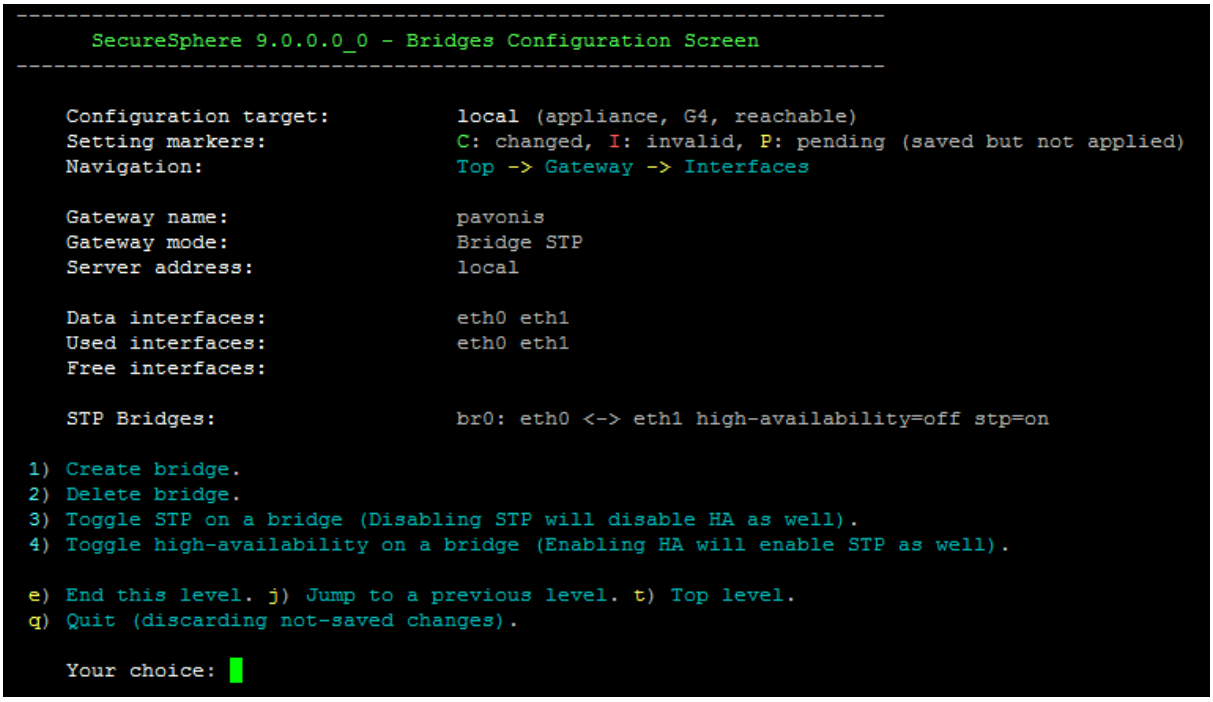


Figure 19: Bridges Configuration Screen

4. In the **Bridges Configuration** screen, select one of the following options, as listed below.

Bridges Configuration Options

Option	Name	Description
1	**Create bridge**	Create a bridge on available interfaces.
2	**Delete bridge**	Delete an existing bridge.
3	**Toggle STP on a bridge**	Select an existing bridge and toggle STP on it. For more information, see Topologies and Deployment on page 23.
4	**Toggle High Availability on a Bridge**	Select an existing bridge and toggle High Availability on it. **Note:** To enable High Availability on a bridge, you must enable STP on that bridge. For more information, see Gateway High Availability on page 343.



Note:

- If the Gateway is not in a High Availability deployment, it is recommended that the Gateway be configured as Bridge IMPVHA with HA disabled.
- SecureSphere supports jumbo frames.

Configuring a Gateway as a Sniffing Gateway

To configure a sniffing Gateway:

1. In the **Gateway Management** screen (shown in Configuring a Gateway on page 68), select option **4) Change operation mode**.
2. From the list of operation modes (as described in Configuring a Gateway as a Bridge on page 72), select **1) Sniffing**.



Warning: The Management Server must be running when you execute this command, otherwise the Gateway will switch to bypass mode.

3. In the **Gateway Management** screen (shown in Configuring a Gateway on page 68), select option **7) Manage interfaces and routes**.

```
-------------------------------------------------------------------------
      SecureSphere 9.0.0.0_0 - Sniffing Configuration Screen
-------------------------------------------------------------------------

    Configuration target:          local (appliance, G4, reachable)
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway -> Interfaces


    Allowed devices:               eth0 eth1 eth2
    Interfaces:                    Sniffing:      eth0
                                   Blocking:      eth2
                                   Blocking net: <not-set>

 1) Set sniffing interface(s).
 2) Set blocking interface.
 3) Add/modify blocking net.
 4) Delete blocking net.

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice:
```

Figure 20: Sniffing Configuration Screen

4. In the **Sniffing Configuration** screen, select one of the following options, as listed below.

Sniffing Configuration Options

Option	Name	Description
1	**Set sniffing interface(s)**	Specify the interface to be used for sniffing.
2	**Set blocking interface**	Specify the interface to be used for blocking, that is, the interface from which SecureSPhere sends RST packets.
3	**Add/modify blocking mask**	Specify the following for the blocking interface: • the blocking device (one of the interfaces) • the blocking interface IP address • the blocking interface IP mask
4	**Delete blocking mask**	Select the blocking mask to be deleted.

Configuring a Gateway for a Cluster

You can configure a Gateway for a Cluster in the following ways:

Configuring a Gateway for a Cluster as Part of First Time Login 75
Configuring a Gateway for a Cluster - Gateway Already Registered 77
Configuring a Gateway Registered in a Cluster 78
Removing Cluster Configuration from a Gateway 79

Configuring a Gateway for a Cluster as Part of First Time Login

When you register a Gateway for the first time (First Time Login), you can configure that Gateway as the first Gateway in a new Cluster. Configuring a Gateway for a Cluster as part of First Time Login defines the following Cluster-relevant parameters for the Gateway:

- Cluster name
- Port
- Interface/device
- IP

Should one of the following conditions not be met, you will be asked to repeat the appropriate step in the procedure until said condition is met:

- The Gateway is in sniffing mode.
- The Gateway model is not a X1000 or a X2000.
- If a virtual machine is being configured, it is not a V1000 or a V2500.
- The port is between 3000 and 65535.
- The Cluster Gateway Group Name is correct and inlcudes letters, digits, dashes, and underscores, only.
- The selected Cluster interface exists.
- The selected IP address is valid.

To configure a Gateway for a Cluster as part of First Time Login:

1. Execute the First Time Login procedure. For more information, see Initial Configuration on page 47.

2. When told `The SecureSphere gateway operation modes are:` select **Sniffing** mode.

```
    The SecureSphere gateway operation modes are:

 1) Sniffing.
 2) Bridge STP.
 3) Bridge IMPVHA.
 4) Reverse Proxy Apache.
 5) Reverse Proxy Kernel.
 6) vPath.

    Operation mode: 1

    Choose the virtual gateway model


    The SecureSphere virtual gateway models are:

 1) V1000.
 2) V2500.
 3) V4500.
 4) V6500.

    Gateway virtual mode: 3
    Do you want to set a cluster configuration ? [y/n]:
```

3. If you are told `The SecureSphere virtual gateway models are:` select the desired **Gateway Model**. This applies to virtual machines only.
4. When asked `Do you want to set a cluster configuration`, enter **y**. The Cluster configuration screen appears.

```
    Do you want to set a cluster configuration ? [y/n]: y

    Cluster configuration


    Cluster port [0-65535]: 3001
    Cluster gateway group name [letters, digits or '_']: dan
    Cluster interface [eth1 eth2 eth3]: eth1
    Cluster IP address [IPv4 Address/CIDR]: 100.10.23.121/24
    Do you want to conifgure agent Listener ? [y/n]: y
```

5. Enter values for the parameters as follows:
   a) `Cluster port:` Enter the value of the port
   b) `Cluster gateway group Name:` - You must enter the name of an existing cluster
   c) `Cluster interface`: Enter the value of the interface/device
   d) `Cluster ip address`: Enter the value of the IP address
6. When asked `Do you want to configure agent Listener`, enter **y**. You must configure an Agent listener for the Gateway to be registered to a Cluster.
7. Respond to the remaining questions as per the Gateway configuration procedure. See Configuring a Gateway on page 68.

   The Gateway is configured for a Cluster.

Configuring a Gateway for a Cluster - Gateway Already Registered

You use this procedure to configure an already registered Gateway for an existing Cluster.

This procedure is an alternative to moving a Gateway into a Cluster using the management server UI. It is best to use this procedure when you need to change the parameters of the Gateway to match those of the existing Cluster.

Should one of the following conditions not be met, you will be asked to repeat the appropriate step in the procedure until said condition is met:

- The Cluster into which you intend to register the Gateway exists. If it does not, the Gateway will be configured for a Cluster, but not registered to any specific Cluster
- The Gateway is in sniffing mode
- The Gateway model is not a X1000 or a X2000
- If a virtual machine is being configured, it is not a V1000 or a V2500
- The port is between 3000 and 65535
- The Cluster Gateway Group Name is correct and includes letters, digits, dashes and underscores only
- The selected Cluster interface exists
- The selected IP address is valid

To configure a Gateway for a Cluster - Gateway already registered:

1. SSH to the Gateway.
2. Run impcfg.
3. Select **Manage SecureSphere Gateway**. The **Top -> Gateway Screen** appears.

4. Select **Change Cluster Configuration**. The **Cluster Configuration Screen** appears.

```
------------------------------------------------------------------------
      SecureSphere 10.5.0.0 - Cluster Configuration Screen
------------------------------------------------------------------------

    Configuration target:          local (appliance, V2500, reachable)
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway -> Cluster


    Cluster Status:                Disable
    Cluster Configurtion:          Disable

 1) Add Cluster configuration.

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice: 1

    Cluster port [3000-65535 and no using port]: 4002
    Do you want to register into Cluster Group ? [y/n]: y
    Cluster gateway group name [letters, digits , '_' or '-']: SomeClusterGroup
    Cluster interface [eth0 eth1 eth2]: eth1
    Cluster ip address [IPv4 Address/CIDR]: 1.1.1.1/24
```

5. Select **Add Cluster Configuration**.
6. Enter values for the parameters as follows:
   a) `Cluster port:` Enter the value of the port
   b) `Do you want to register into Cluster Group ?`: Enter **y** to register the Gateway to an existing Cluster. If you enter **N**, the Gateway is configured for a Cluster, but not registered to any specific Cluster. For more information, see the SecureSphere User Guide.
   c) `Cluster gateway group Name:` - You must enter the name of an existing cluster
   d) Cluster interface: Enter the value of the interface/device
   e) Cluster ip address: Enter the value of the IP address

7. Select **Confirm**.
8. Select **Top level**.
9. Select **Apply Settings**.

Configuring a Gateway Registered in a Cluster

Use this procedure to configure the three parameters of the Gateway that do not impinge on the Cluster: IP, Port, Device.

You can configure the parameters of an existing Cluster via one of its Gateways.

Should one of the following conditions not be met, you will be asked to repeat the appropriate step in the procedure until said condition is met:

- The port is between 3000 and 65535.
- The Cluster Gateway Group Name is correct and includes letters, digits,hyphens and underscores, only.
- The selected Cluster interface exists.
- The selected IP address is valid.

To configure a Gateway registered in a Cluster:

1. SSH to the Gateway.
2. Run impcfg.
3. Select **Manage SecureSphere Gateway**. The **Top -> Gateway Screen** appears.

4. Select **Change Cluster Configuration**. The **Cluster Configuration Screen** appears.

```
------------------------------------------------------------------
      SecureSphere 10.5.0.0 - Cluster Configuration Screen
------------------------------------------------------------------

    Configuration target:          local (appliance, V2500, reachable)
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway -> Cluster


    Cluster Status:                Enable
    Cluster Configurtion:          Cluster interface:     eth1
                                   Cluster port:          4002
                                   Cluster ip:            1.1.1.1/24

 1) Change Cluster configuration.
 2) Delete Cluster.
 3) Change IPv4 address.
 4) Change device.
 5) Change port.

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice:
```

5. Choose one of the following:
   - To change more than one of the Gateway's Cluster parameters, select **Change Cluster Configuration**. The **Cluster Parameters** screen appears.

     ```
     Cluster port [0-65535]: 3001
     Cluster gateway group name [letters, digits or '_']: dan
     Cluster interface [eth1 eth2 eth3]: eth1
     Cluster IP address [IPv4 Address/CIDR]: 100.10.23.121/24
     ```

     Enter values for the desired parameters.

- To change one of the Gateway's Cluster parameters only, select either **Change IPv4 address**, **Change device**, or **Change port**. Enter a value for the parameter.

6. Select **Confirm**.
7. Select **Top level**.
8. Select **Apply Settings**.

Removing Cluster Configuration from a Gateway

Before you can delete a Cluster via the CLI, you must first deactivate that Cluster. For more information, see the SecureSphere Database Security User Guide.

To remove Cluster configuration from a Gateway:

1. SSH to the Gateway.
2. Run impcfg.
3. Select **Manage SecureSphere Gateway**. The **Top -> Gateway Screen** appears.

4. Select **Change Cluster Configuration**. The **Cluster Configuration Screen** appears.

```
------------------------------------------------------------------------
      SecureSphere 10.5.0.0 - Cluster Configuration Screen
------------------------------------------------------------------------

    Configuration target:          local (appliance, V2500, reachable)
    Setting markers:               C: changed, I: invalid, P: pending (saved but not applied)
    Navigation:                    Top -> Gateway -> Cluster


    Cluster Status:                Enable
    Cluster Configurtion:          Cluster interface:     eth1
                                   Cluster port:          4002
                                   Cluster ip:            1.1.1.1/24

 1) Change Cluster configuration.
 2) Delete Cluster.
 3) Change IPv4 address.
 4) Change device.
 5) Change port.

 e) End this level. j) Jump to a previous level. t) Top level.
 q) Quit (discarding not-saved changes).

    Your choice:
```

5. Select **Delete Cluster**.
6. Select **Confirm**.
7. Select **Top level**.
8. Select **Apply Settings**.

Managing SecureSphere Agents

You can:

- Add/modify/delete SecureSphere Agents
- Add and delete agent listeners
- Add and delete SecureSphere Agent for DB z/OS listeners

SecureSphere SecureSphere Agents, installed on the database server, provide visibility into database activity by monitoring all database communications and forwarding these communications, via a TCP tunnel, to a listener application configured on a SecureSphere Gateway.

Note: Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.

Usually, when a SecureSphere Agent is installed and configured, it registers with the SecureSphere Gateway. Upon successful registration, the Gateway configures the SecureSphere Agent with the listener port used for the tunnel.

For more information about SecureSphere Agents, see **SecureSphere User Guide**.

To manage SecureSphere Agents:

1. In the **Gateway Management** screen (shown in Configuring a Gateway on page 68), select **7) Manage remote agents**. The **Remote Agents** Screen is displayed.

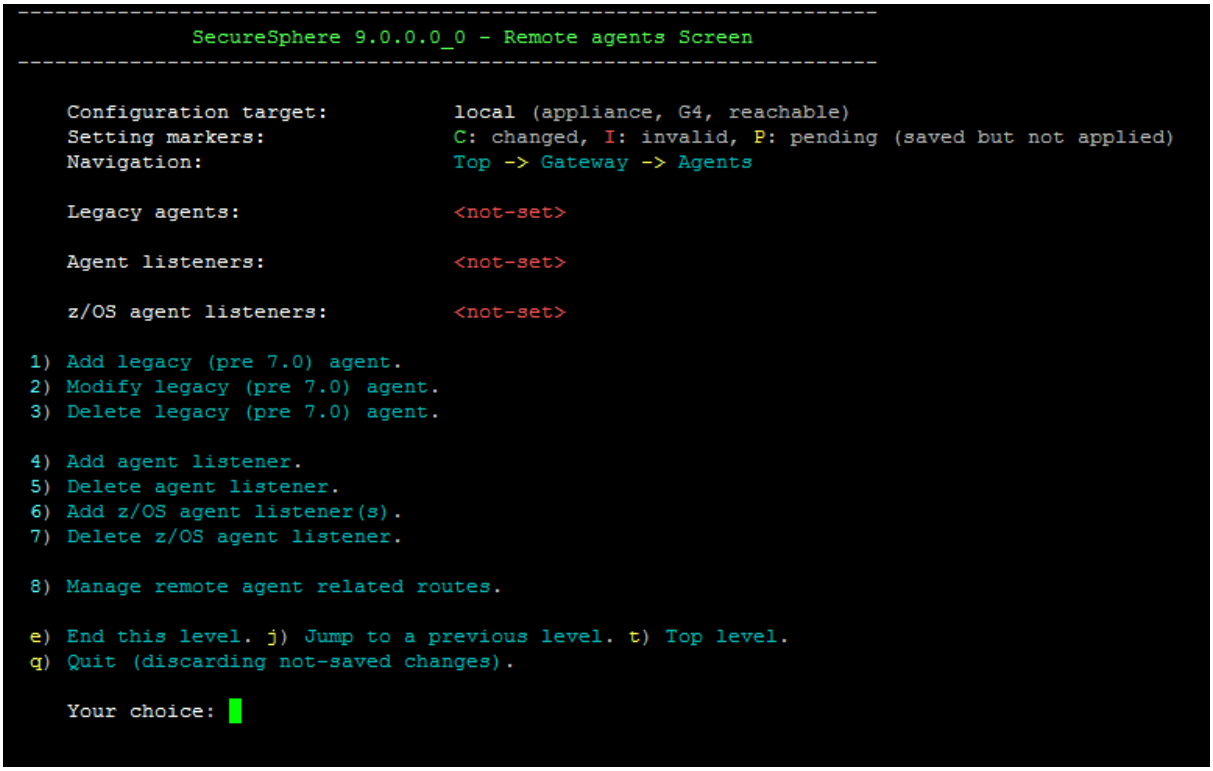


Figure 21: Remote Agent Screen

2. Select one of the following options, as listed below.

SecureSphere Agent Configuration Options

Option	Name	Description
1	**Delete a legacy (pre 7.0) agent**	Delete a pre-version 7.0 SecureSphere Agent. For more information, see Deleting a Legacy (pre-version 7.0) SecureSphere Agent on page 82.
2	**Add agent listener**	Add a listener for a SecureSphere Agent. This option is not relevant to SecureSphere Agent for DB2 z/OS. **Note:** A SecureSphere Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. For more information, see Adding a Remote AgentSecureSphere Agent Listener "Adding a SecureSphere Agent Listener" on page 82.
3	**Delete agent listener**	Delete a listener for a SecureSphere Agent. This option is not relevant to SecureSphere Agent for DB2 z/OS. For more information, see Deleting a SecureSphere Agent Listener on page 83.
4	**Add z/OS agent listener(s)**	Add a SecureSphere Agent for DB2 z/OS listener. **Note:** A SecureSphere Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port. For more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.
5	**Delete z/OS agent listener**	Delete a SecureSphere Agent for DB2 z/OS listener. For more information, see Deleting a SecureSphere Agent for DB2 z/OS Listener on page 84.
6	**Manage remote-agent related routes**	Manage SecureSphere Agent routes. For more information, see Managing SecureSphere Agent Related Routes on page 85.

Adding a Legacy (pre-version 7.0) SecureSphere Agent

To add a legacy (pre-version 7.0) agent:

1. Enter the SecureSphere Agent name.
   This field corresponds to the **Agent Name** in the Agents Workbench.
2. Enter the SecureSphere Agent ID.
3. Enter a description for the SecureSphere Agent.

Modifying a Legacy (pre-version 7.0) SecureSphere Agent

To modify a legacy (pre-version 7.0) agent:

1. Select the SecureSphere Agent from the displayed list.
2. Enter a new SecureSphere Agent name.
   This field corresponds to the **Agent Name** in the Agents Workbench.
3. Enter a new SecureSphere Agent ID.
4. Enter a new description for the SecureSphere Agent.

Deleting a Legacy (pre-version 7.0) SecureSphere Agent

To delete a legacy (pre-version 7.0) agent:

1. Select the SecureSphere Agent from the displayed list.
   The SecureSphere Agent will be immediately deleted.

Adding a SecureSphere Agent Listener

To add a SecureSphere Agent listener:



Note:

- These parameters must also be specified in the SecureSphere Agent configuration on the database server. For more information, see SecureSphere Agent Management Console.
- You can define multiple TCP listeners on a Gateway, and you can direct different SecureSphere Agents to different listeners.
- Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
- A SecureSphere Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

1. Enter the listener protocol (TCP).

```
Your choice: 4
Listener protocol [TCP UDP]: TCP

Enable SSL [y/n]: n
Listener IP address [IP address]: 10.1.2.3
Listener IP mask [IP mask]: 255.255.255.240
Listener port [1-65355]: 3456
Listener interface [eth0 eth1 eth2 eth3 eth4 eth5]: eth

Do you want to add a virtual IP for this listener? [y/n
Virtual instance name [a letter then digits, letters, d
Virtual IP address [IP address]: 10.3.4.5
Virtual IP mask [IP mask]: 255.255.255.240
Virtual router id [1..255]: 3
Virtual router mode [MASTER BACKUP]: MASTER
```

Figure 22: Remote Agent Listener

2. Select whether to use SSL.
3. Enter the listener IP address.



Note: Only IPv4 addresses are allowed for SecureSphere Agent listeners.

4. Enter the listener network mask.
5. Enter the listener port.
6. Enter a SecureSphere Agent listener interface.
7. Specify whether to add a virtual IP address for the listener.
   If you choose to specify a virtual IP address, you will be asked to define some additional parameters:
   - Virtual instance name
   - Virtual IP address
   - Virtual IP mask
- Virtual router id
- Virtual router mode

Deleting a SecureSphere Agent Listener

To delete a SecureSphere Agent listener:

1. Select the SecureSphere Agent listener from the displayed list (by number).
   The SecureSphere Agent listener will be immediately deleted.

Adding a SecureSphere Agent for DB2 z/OS Listener



Note:

- These parameters must also be specified in the SecureSphere Agent for DB2 z/OS configuration on the database server. For more information, see **SecureSphere User Guide**.
- A SecureSphere Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

1. Select the listener type.

```
    Your choice: 6

1) Data Receiver Listener Type.
2) Plan Provider Listener Type (configuration).

    Listener tunnel type [1..2]: 1
    Listener IP address [IP address]: 10.1.2.3
    Listener IP mask [IP mask]: 255.255.255.240
    Listener port [1-65355]: 2345
    Listener interface [eth0 eth1 eth2 eth3 eth4 eth5]: eth0

    You are now configuring Plan Provider Listener Type (configuration)
    Listener IP address [IP address]: 10.2.4.5
    Listener IP mask [IP mask]: 255.255.255.240
    Listener port [1-65355]: 3333
    Listener interface [eth0 eth1 eth2 eth3 eth4 eth5]: eth2
```

Figure 23: Remote Agent Listener Definition

Data Receiver listeners are for audit events, and messages sent from the SecureSphere Agent for DB2 z/OS to the SecureSPhere Gateway.

Plan Provider listeners are for the policies, plans and messages sent between the Gateway and the SecureSphere Agent for DB2 z/OS.

2. Enter the other parameters as requested.
3. You must define one listener of each type, so after you have defined the first listener, you will be asked to define the other listener as well.

Deleting a SecureSphere Agent for DB2 z/OS Listener

To delete a SecureSphere Agent for DB2 z/OS listener:

1. Select the SecureSphere Agent for DB2 z/OS listener from the displayed list (by number).

   The SecureSphere Agent for DB2 z/OS listener will be immediately deleted.

Managing SecureSphere Agent Related Routes

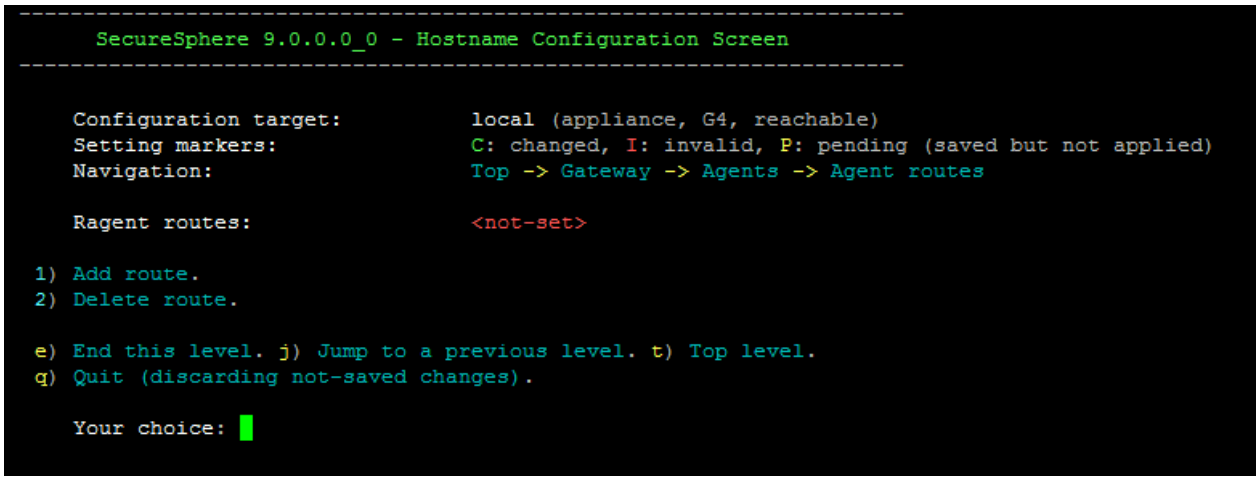


Figure 24: Remote Agent Routes Definition

1. From the SecureSphere Agent Routes screen, select one of the following options, as listed below.
2. Enter the route parameters, as requested.

Static Routes Screen Configuration Options

Option	Name	Description
1	**Add route**	Add a SecureSphere Agent route.
2	**Delete route**	Delete an existing SecureSphere Agent route.

Configuring a Data Assessment Server (DAS)

For an appliance configured as a Data Assessment Server (DAS), you can:

- Activate/deactivate the DAS
- Start/stop/reactivate the DAS
- Change management and DAS passwords
- Reconfigure the DAS as a Onebox



Note: If the appliance has not been configured as a DAS, the DAS options are not available.

To configure the DAS:

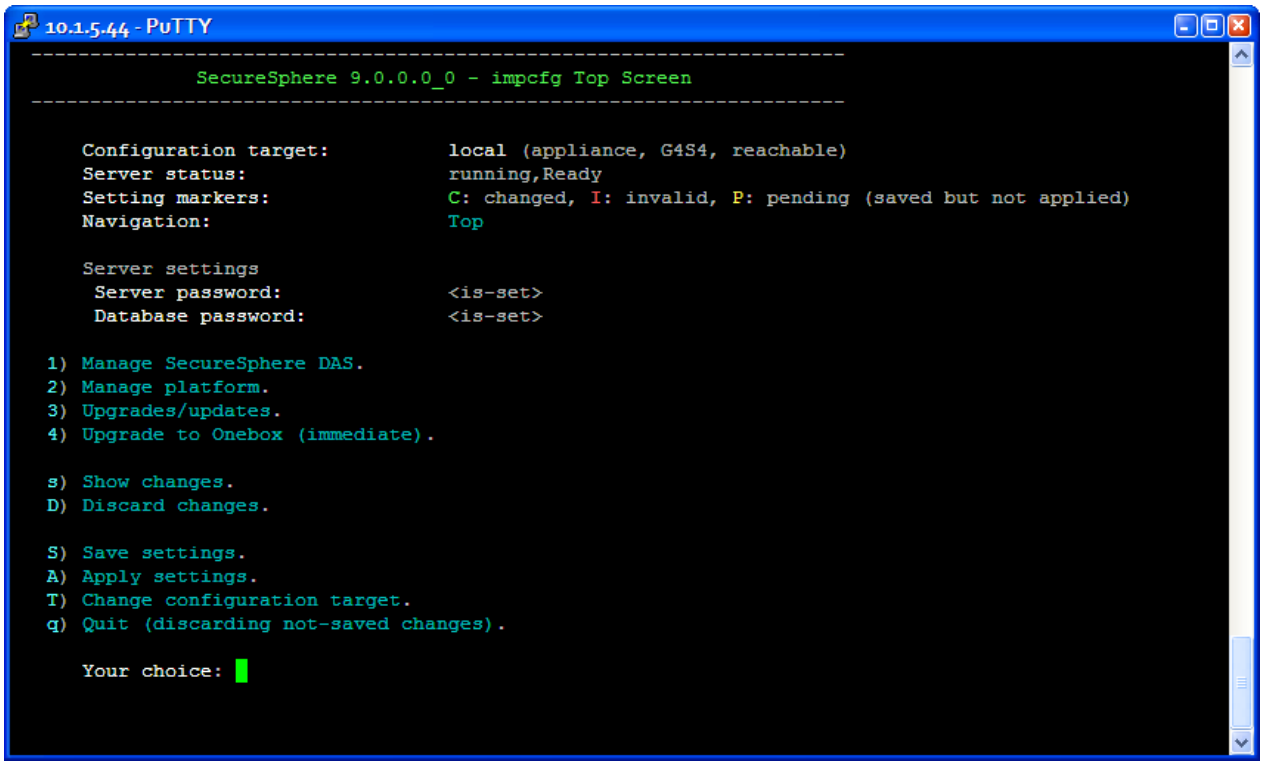


Figure 25: impcfg Top Screen (DAS)

1. In the **Top** Screen (shown in the figure above), select option **1) Manage SecureSphere DAS**.
   The **Gateway Management** Screen (the figure below) is displayed.



Note: A DAS appliance can only discover vulnerabilities but cannot mitigate them.

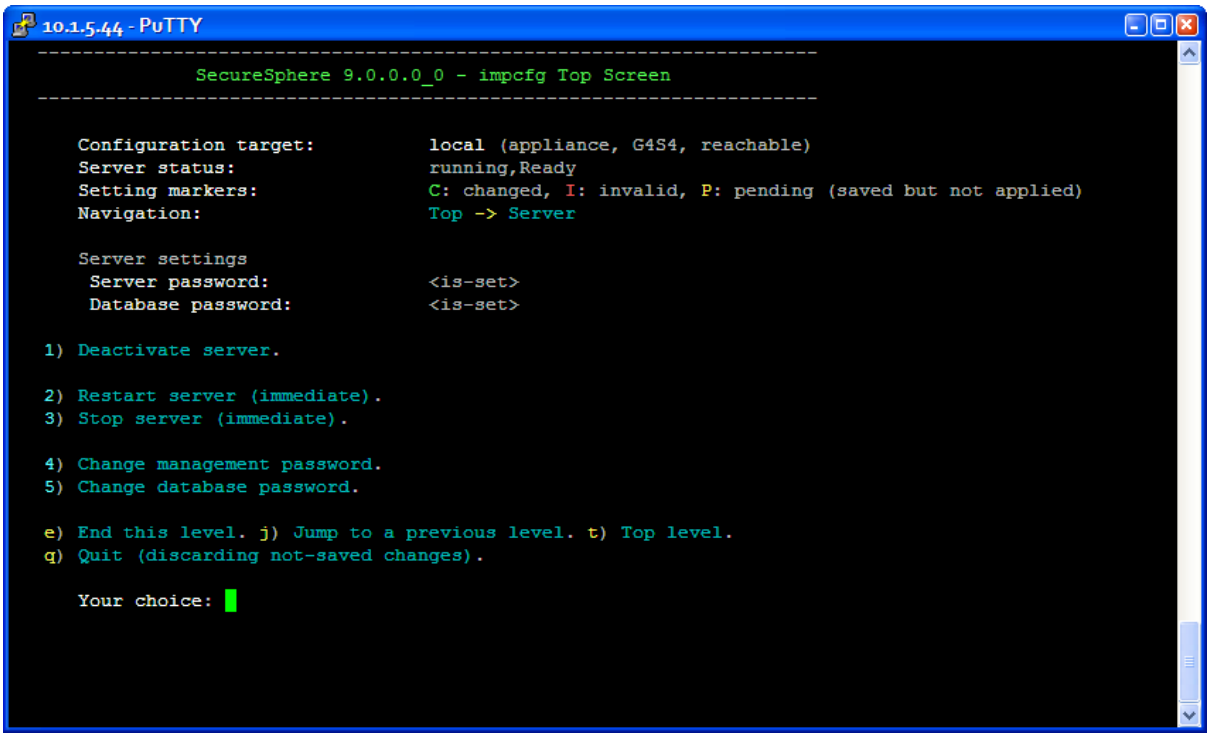


Figure 26: DAS Server Configuration Screen

2. Select one of the following options, as listed below.

DAS Configuration Options

Option	Name	Description
1	**Deactivate server**	Stop the DAS and do not restart it when the appliance boots. This would be done, for example, when converting a DAS to a Onebox.
	Activate Server (immediate)	Start the DAS the next time the appliance boots. This would be done, for example, after a Onebox has been converted to a DAS.
2	**Restart server (immediate)**	Stop and then start the DAS.
3	**Stop server (immediate)**	Stop the DAS.
4	**Change management password**	Change the password of the `secure` user. For more information about passwords, see SecureSphere Users on page 54.
5	**Change database password**	Change the password of the internal SecureSphere database. For more information about passwords, see SecureSphere Users on page 54.

Reconfiguring the DAS as a Onebox

You can reconfigure a DAS as a Onebox.

To reconfigure the DAS as Onebox:

1. In the **Top** Screen, select option **4) Reconfigure as Onebox**. The **Reconfigure DAS to Onebox** Screen is displayed.

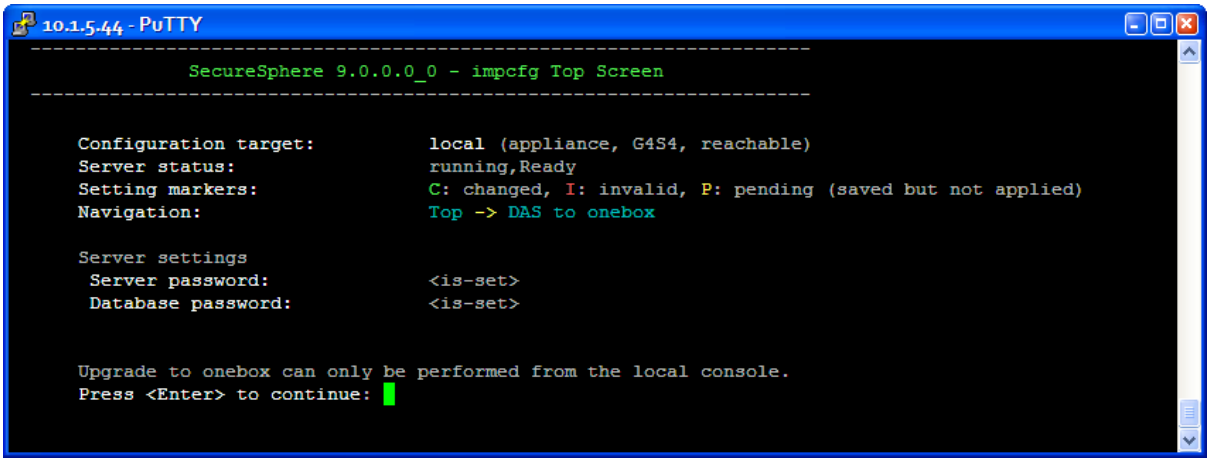


Figure 27: Reconfigure DAS as Onebox Screen

Note: You will need to install a new license for the Onebox.

A message will be displayed stating that all IP configurations will be deleted and that you will have to rewire the network cables, and asking whether you want to continue.

2. Enter `y` to continue. `impcfg` will exit and you will be asked to run `impcfg` again.
3. Run `impcfg`. `impcfg` will start in it s initialization mode, that is, you will be asked to configure the appliance from scratch.

Configuring the Platform

You can:

- Manage network and time settings, users and root password
- Reboot/shutdown the appliance

To configure the platform:

1. In the **Top** Screen, select **3) Manage platform**. The **Platform Management** screen is displayed.

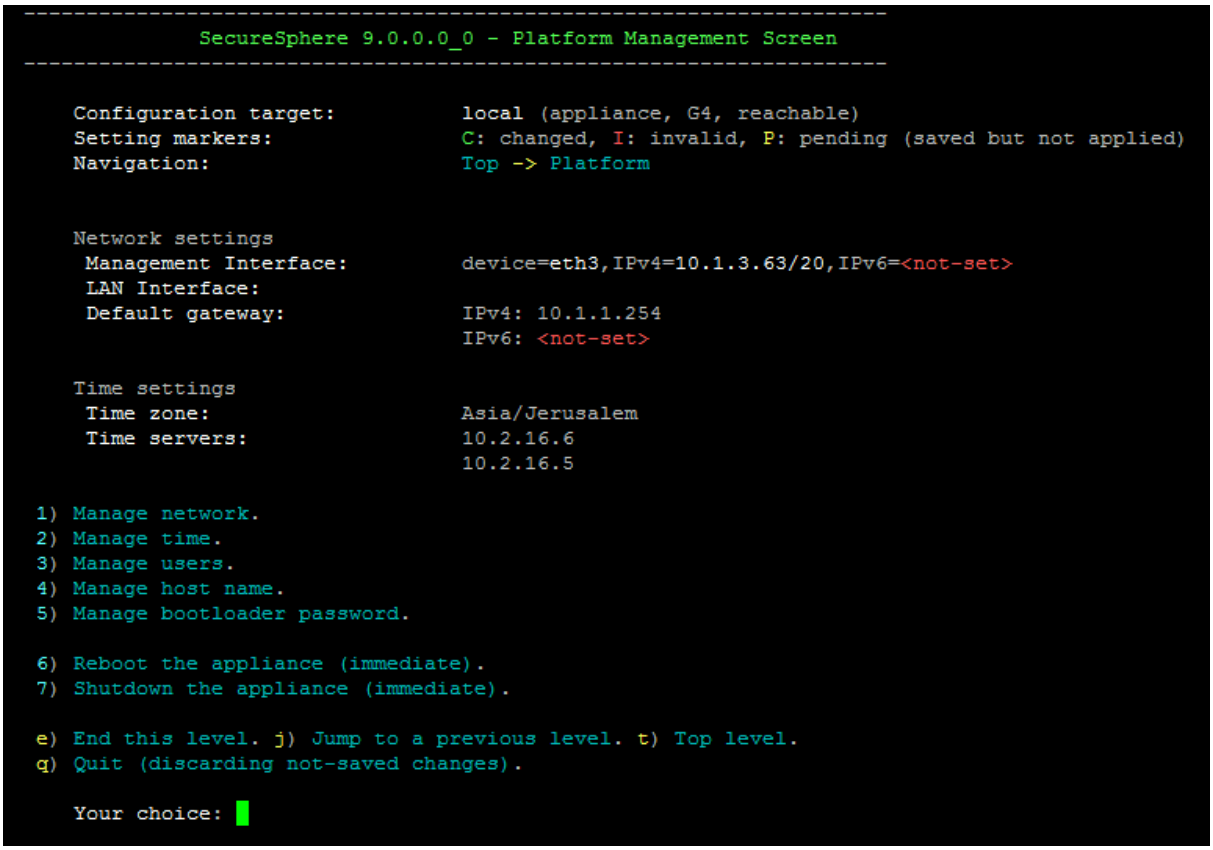


Figure 28: Platform Management Screen

2. Select one of the following options, as listed below.

Platform Management Screen Configuration Options

Option	Name	Description
1	**Manage network**	Change the management and LAN interfaces, the default Gateway, *etc*. For more information, see Network Management on page 91.
2	**Manage time**	Change the time zone, date and/or time, or configure NTP on the appliance. For more information, see Time Management on page 98.
3	**Manage users**	Manage CLI users. For more information, see Users Management on page 100.
4	**Manage host name**	Manage the appliance host name. For more information, see Hostname Management on page 105.
5	**Manage bootloader password**	Manage the bootloader (GRUB - Grand Unified Bootloader) password. For more information, see Bootloader Password Management on page 106.
6	**Reboot the appliance (immediate)**	Reboot the appliance.
7	**Shutdown the appliance (immediate)**	Shutdown the appliance.

Network Management

In the **Network Management** screen, you can:

- Specify the management interfaces, and default Gateway
- Configure the DNS client
- Locate network devices

To manage network settings:

1. In the **Platform Management** Screen (see Configuring the Platform on page 89), select **1) Manage network**. The **Network Management** screen is displayed.

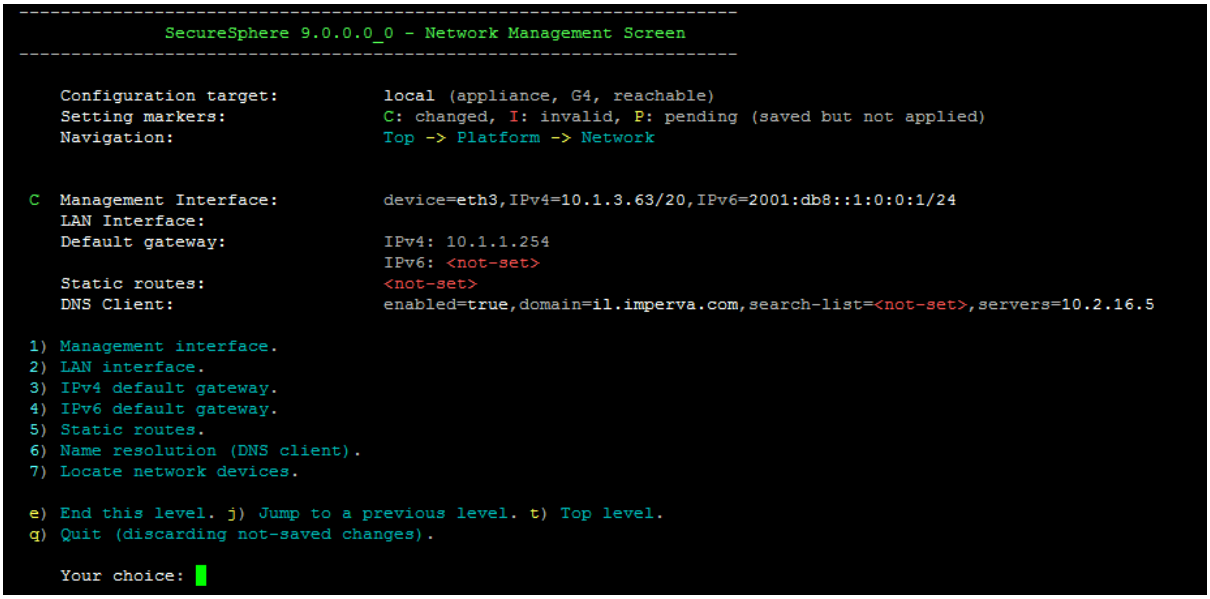


Figure 29: Network Management Screen

2. Select one of the following options, as listed below.

Network Management Screen Configuration Options

Name	Description
Management interface	Change the network interface and/or IP address (including CIDR) of the management interface. You can specify: • an IPv4 address only • and IPv6 address only • both an IPv4 address and an IPv6 address Physically locate the network interface used as the management interface. For more information, see Management Interface on page 93.
LAN interface	Change the network interface and/or IP address (including CIDR) of the LAN interface. You can specify: • an IPv4 address only • and IPv6 address only • both an IPv4 address and an IPv6 address Physically locate the network interface used as the LAN interface. For more information, see LAN Interface on page 94.
IPv4 default gateway **IPv6 default gateway**	Change the appliance's default Gateway. Whether IPv4 or IPv6 default Gateway options (or both) are available depends on whether the management interface and/or LAN interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and an IPv6 address, so both "IPv4 default gateway" and "IPv6 default gateway" options are listed in the menu. For more information, see Default Gateway on page 96.
Static routes	Add and delete static routes. For more information, see Static Routes on page 96.
Name Resolution (DNS client)	Enable or disable the DNS client. You must enable the DNS client if the Management Server will be using LDAP to authenticate SecureSphere administrators (see Authentication and Authorization Configuration on page 266). Define the domain name and search list, and specify a list of name servers. For more information, see Name Resolution (DNS client) on page 97.
Locate network devices	Physically locate an network interface. For more information, see Locate Network Devices5 "Locate Network Devices" on page 98.

Management Interface

The management interface is used, by default, by administrators for communication with the MX GUI. Optionally, SecureSphere administrators can also communicate with the MX GUI over the LAN interface.

In the **Management Interface** screen, you can:

- Change the network interface and/or IP address (including CIDR)
- Physically locate the network interface used as the management interface

To manage the management interface:

1. In the **Network Management** screen (as described in Network Management on page 91), select **1) Management interface**. The **Management Interface** screen is displayed.

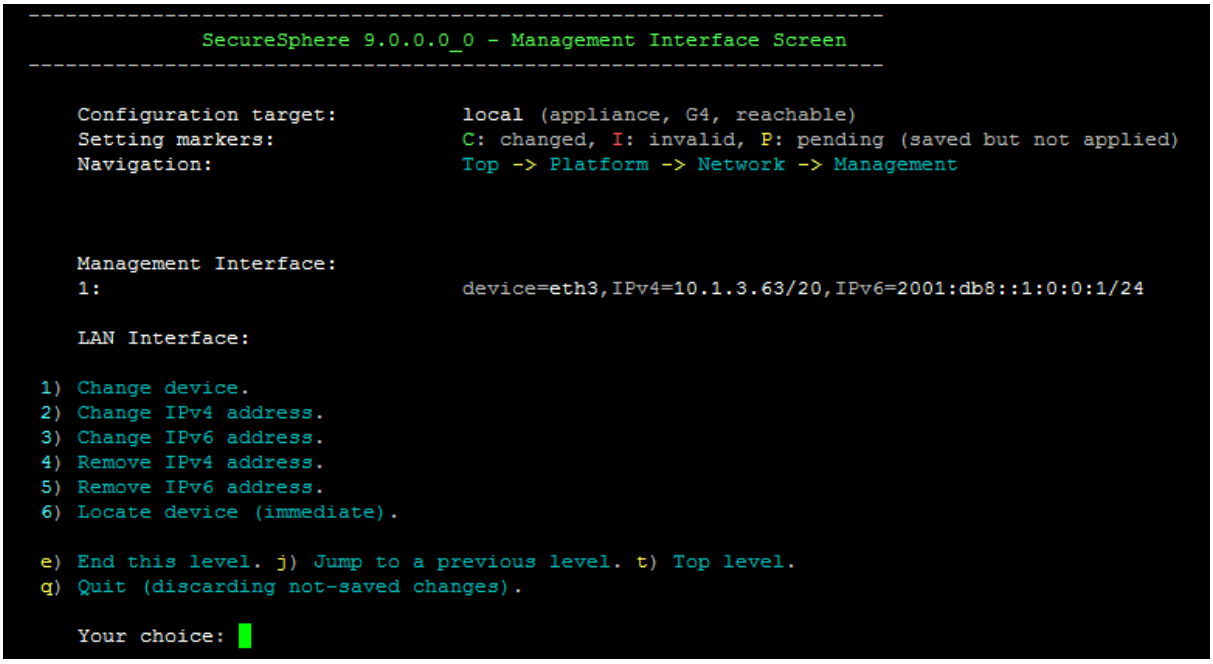


Figure 30: Management Interface Screen

2. Select one of the following options, as listed below.

Management Interface Screen Configuration Options

Name	Description
Set/Change device	Set or change the network interface to be used as the management interface. Specify the name, for example "eth4", of one of the available network interfaces.
Set/Change IPv4 address **Set/Change IPv6 address**	Set or change the IP address of the network interface used as the management interface. Whether IPv4 or IPv6 address options (or both) are available depends on whether the management interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and an IPv6 address, so both "Change IPv4 address" and "Change IPv6 address" options are listed in the menu.
Remove IPv4 address **Remove IPv6 address**	Remove the IP address of the network interface used as the management interface. Whether IPv4 or IPv6 address options (or both) are available depends on whether the management interface has only an IPv4 or only an IPv6 address, or both. In the screen shown above, the management interface has both an IPv4 and an IPv6 address, so both "Remove IPv4 address" and "Remove IPv6 address" options are listed in the menu.
Locate device (immediate)	This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the management network interface. **Note:** Before activating this option, disconnect, if possible, all the network cables attached to the device.

LAN Interface

The LAN interface is used, by default, for communication between Gateways and the MX. Optionally, SecureSphere administrators can also communicate with the MX GUI over the LAN interface.

In the **LAN Interface** screen, you can:

- Change the network interface, IP address and netmask of the LAN interface
- Physically locate the network interface used as the LAN interface

To manage the LAN interface:

1. In the **Network Management** screen (as described in Network Management on page 91), select **2) LAN interlace**. The **LAN Interface** screen is displayed.

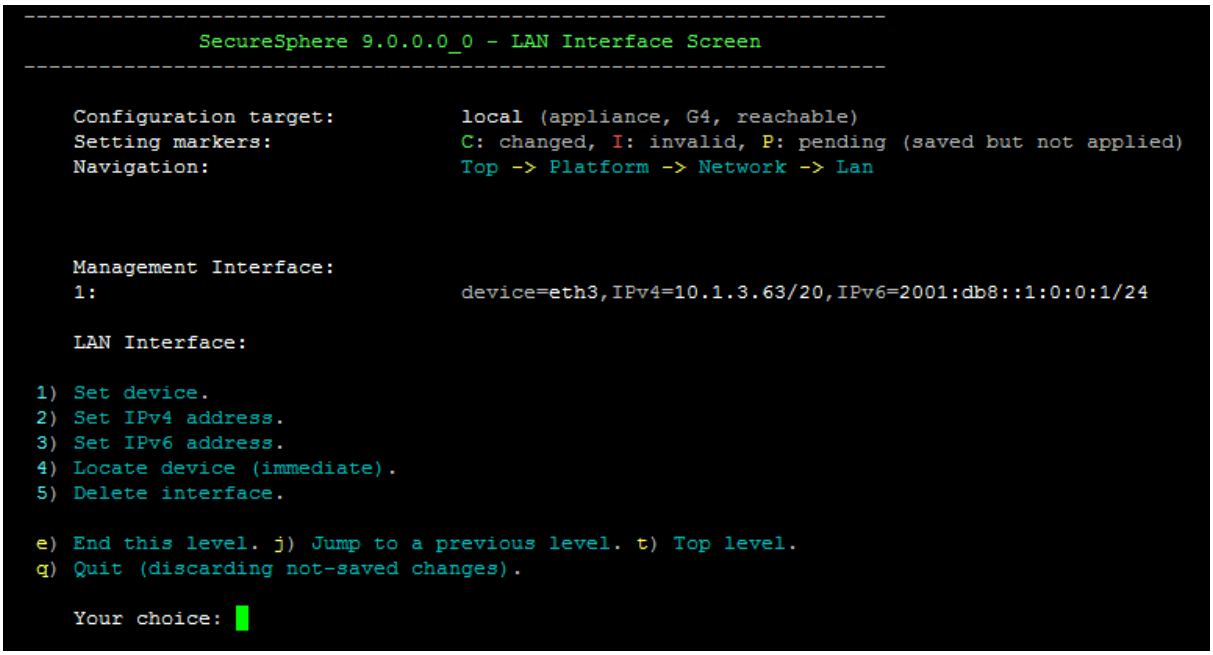


Figure 31: LAN Interface Screen

2. Select one of the following options, as listed below.

LAN Interface Screen Configuration Options

Name	Description
Set/Change device	Set or change the network interface to be used as the LAN interface. Specify the name, for example "eth4", of one of the available network interfaces.
Set/Change IPv4 address **Set/Change IPv6 address**	Set or change the IP address of the network interface used as the LAN interface.
Locate device (immediate)	This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the LAN network interface. You will be asked to specify an Activation time. **Note:** Before activating this option, disconnect, if possible, all the network cables attached to the device.
Delete interface	

Default Gateway

You can:

- Change the appliance's default Gateway

To change the appliance's default Gateway:

1. In the **Network Management** screen (as described in Network Management on page 91), select **IPv4 Default gateway** or
   IPv6 Default gateway.
2. You will be asked to specify an IP address and, optionally, a device (network interface) for the default Gateway.

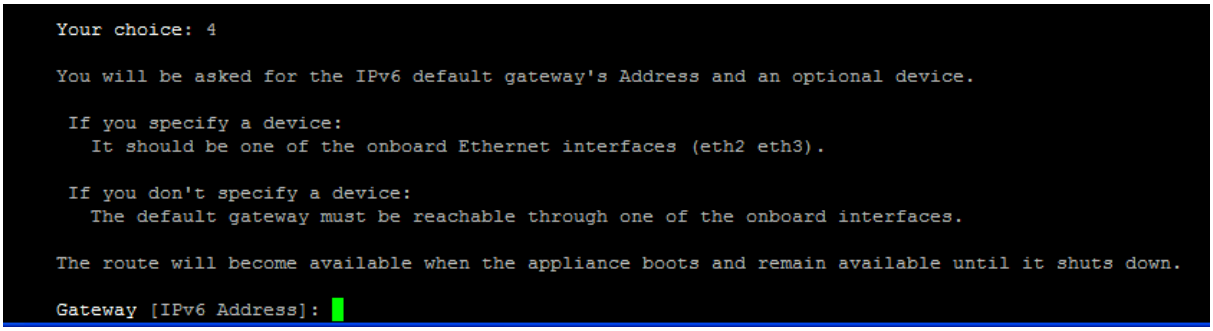


Figure 32: Default Gateway

Static Routes

In the **Static Routes** screen, you can:

- Add and delete static routes

To configure static routes:

1. In the **Network Management** screen (as described in Network Management on page 91), select **Static routes**. The Static Routes screen is displayed.

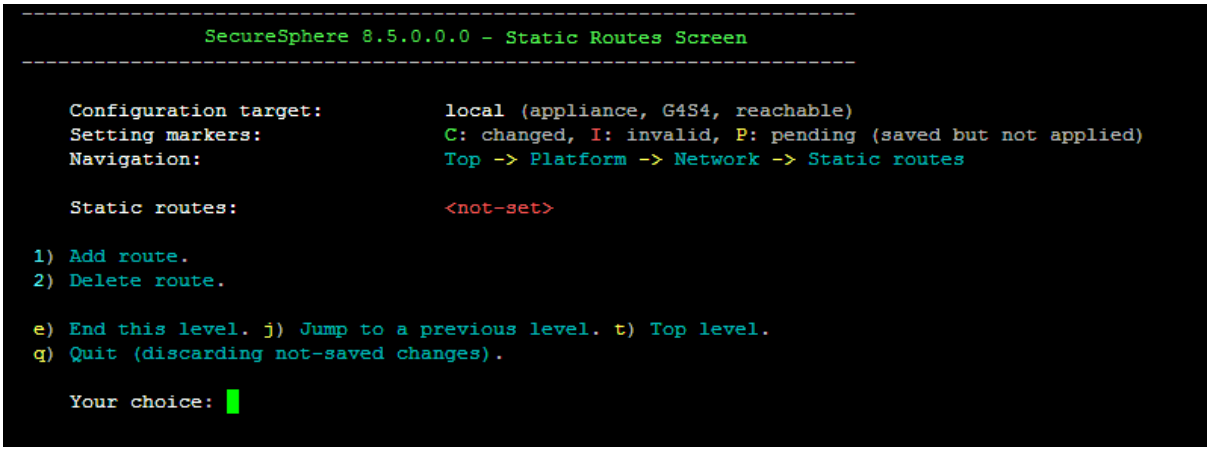


Figure 33: Static Routes Screen

2. Select one of the following options, as listed below.

Static Routes Screen Configuration Options

Option	Name	Description
1	**Add route**	Add a static route. You will be asked to specify the type (host or net), the IP address, the Gateway and optionally, a network interface. When defining static routes, the user must define the device (interface). `impcfg` presents the user with a list of relevant devices (interfaces) as a hint, and the user should select one of these.
2	**Delete route**	Delete an existing static route.

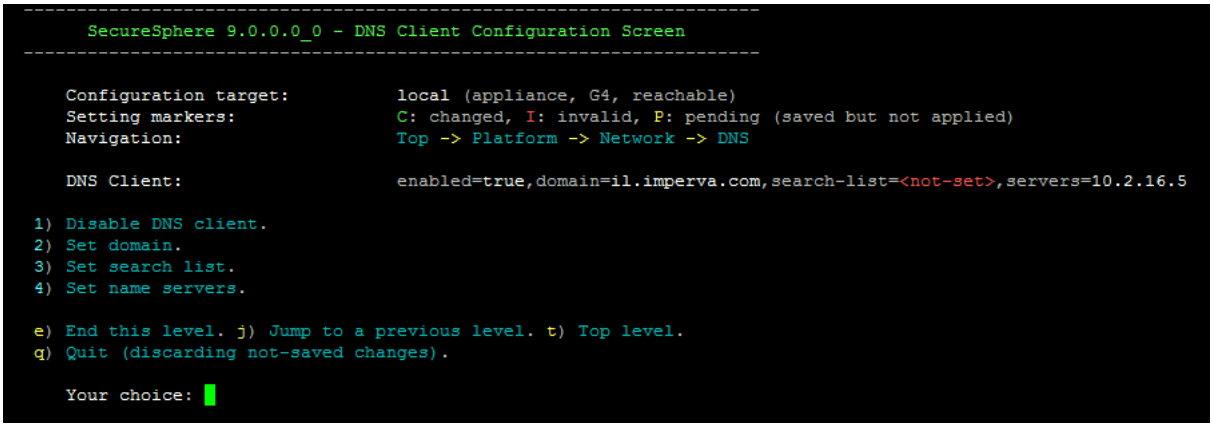
Name Resolution (DNS client)

In the **DNS Client Configuration** screen, you can:

- Enable or disable the DNS client
- Define the domain name and search list
- Specify a list of name servers

To configure DNS:

1. In the **Network Management** screen (as described in Network Management on page 91), select **5) Name resolution (DNS client)**. The **DNS Client Configuration** screen is displayed.



2. Select one of the following options, as listed below.

DNS Client Configuration Screen Configuration Options

Option	Name	Description
1	**Enable/Disable DNS client**	Enable or disable the DNS client. You must enable the DNS client if the Management Server will be using LDAP to authenticate SecureSphere administrators (see Authentication and Authorization Configuration on page 266).
2	**Set domain**	Define the domain name.
3	**Set search list**	Define the domain search list.
4	**Set name servers**	Specify a comma-separated list of name servers. Make sure these are real DNS servers, not "dummy" IP addresses.

Locate Network Devices

This option will help you physically locate a network interface by attempting to blink one of the LEDs associated with the network interface.



Note: Before activating this option, disconnect, if possible, all the network cables attached to the device.

To physically locate a network interface:

1. In the **Network Management** screen (as shown inNetwork Management on page 91), select **6) Locate network device**.
2. Select an interface from the list of available interfaces.
3. Specify an Activation time.

Time Management

You can:

- Change the date, time, and time zone
- Configure the NTP server.

To manage time settings:

1. In the **Platform Management** screen (as described in Configuring the Platform on page 89), select **2) Manage time**. The **Time Management** screen is displayed.

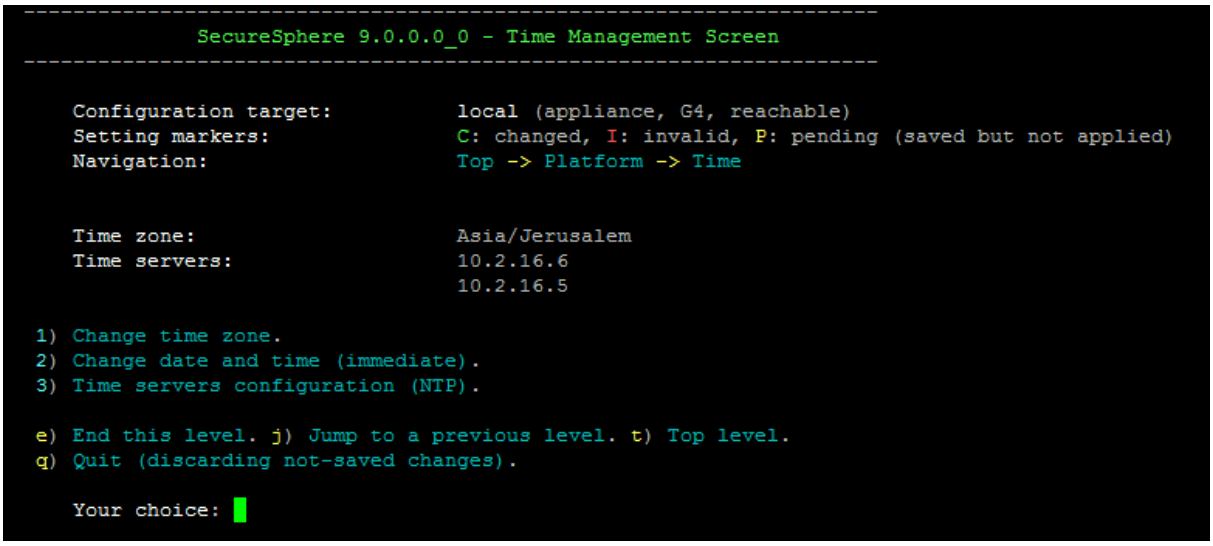


Figure 34: Time Management Screen

2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	**Change time zone**	Change the appliance's time zone. You will be asked to select a time zone and then a country, or to specify the time zone using the Posix TZ format.
2	**Change date and time (immediate)**	
3	**Time servers configuration (NTP)**	For more information, see Time Servers on page 100.

Time Servers

You can:

- Add and delete NTP servers

To manage NTP servers:

1. In the **Time Management** screen (as described in Time Management on page 98), select **2) Manage time**. The **Time Management** screen is displayed.

   A list of previously-added time servers is displayed under **Time Server(s)**.

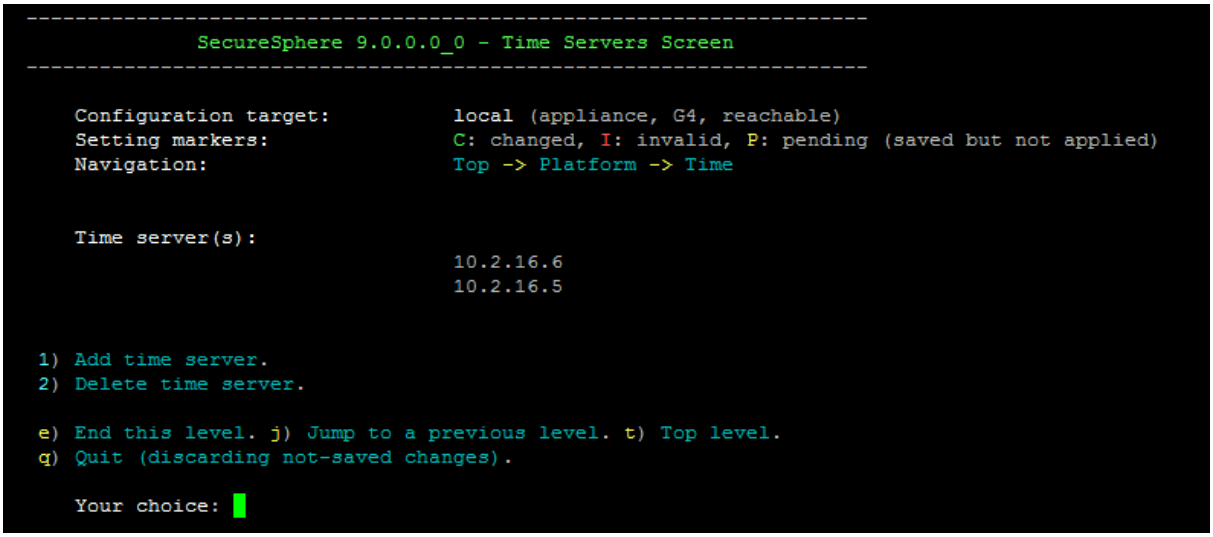


Figure 35: Time Servers Screen

2. Select one of the following options, as listed below.

Time Servers Screen Configuration Options

Option	Name	Description
1	**Add time server**	Add an NTP server. You will be asked to enter the IP address of the NTP server to be added. You can add an IPv4 address or an IPv6 address, depending on whether the appliance's LAN interface has an IPv4 or IPv6 address, or both. **Note:** Synchronization will be not take place if the time difference between the appliance and the NTP server is too great. You should manually set the time on the appliance to be correct (within 2-3 minutes) before the initial synchronization attempt.
2	**Delete time server**	Delete a previously-added NTP server. You will be asked to enter the IP address of the NTP server to be deleted. This must be one of the IP addresses displayed under **Time Server(s)**.

Users Management

You can:

- Change the root user's password
- Create a new user

- Manage an existing user
- Configure external authentication

To manage users:

1. In the **Platform Management** screen (as shown inConfiguring the Platform on page 89), select **3) Manage users**. The **Users Management** screen is displayed.

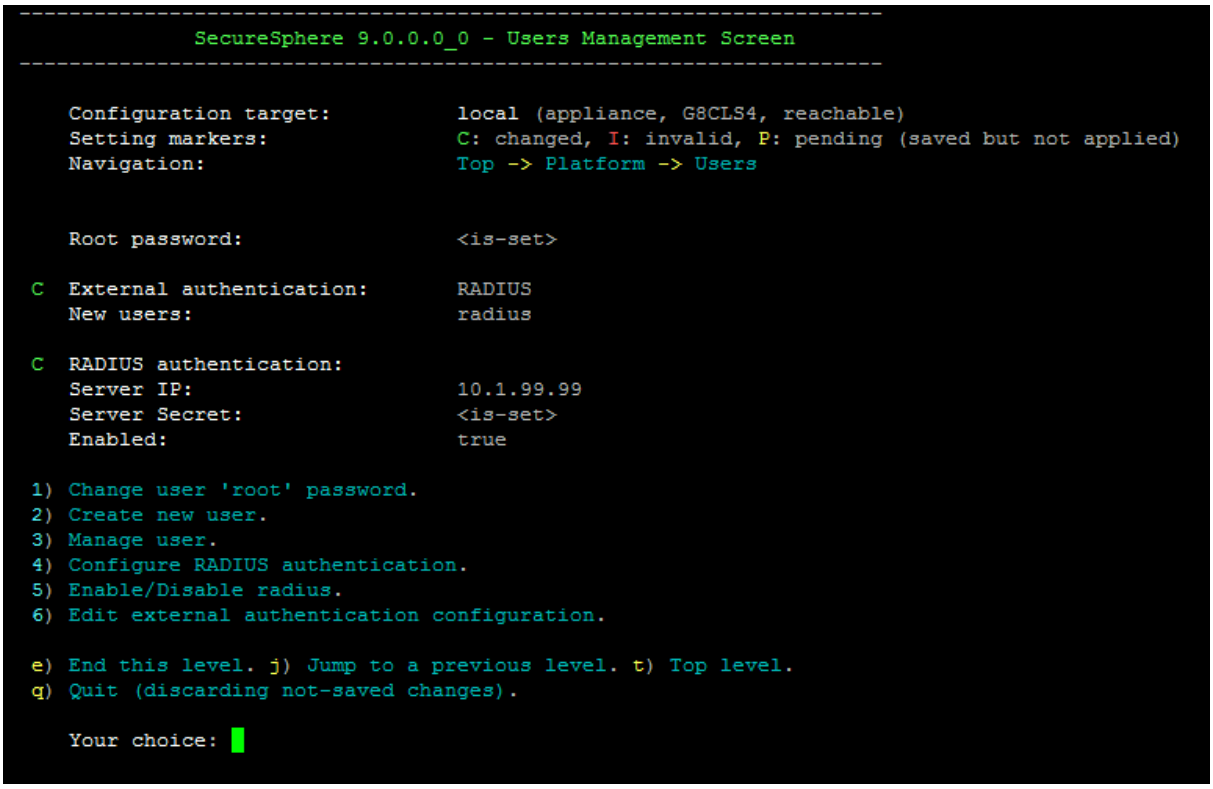


Figure 36: Users Management Screen

2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	**Change user 'root' password.**	For more information, see Change Root User Password on page 102.
2	**Create new user.**	For more information, see Create New User on page 102.
3	**Manage user.**	For more information, see Manage User on page 103.
4	**Configure RADIUS authentication.**	For more information, see Configure RADIUS Authentication on page 104.
5	**Enable / disable RADIUS.**	For more information, see Configuring RADIUS Authentication "Configure RADIUS Authentication" on page 104.
6	**Edit external authentication configuration.**	For more information, see Edit External Authentication Configuration on page 105.

Change Root User Password

1. Enter the root user's existing password.
2. Enter a new password for the root user.
   You can also enter the string "nochange", in which case you will be returned to the previous menu.
3. Enter the new password again.

Create New User

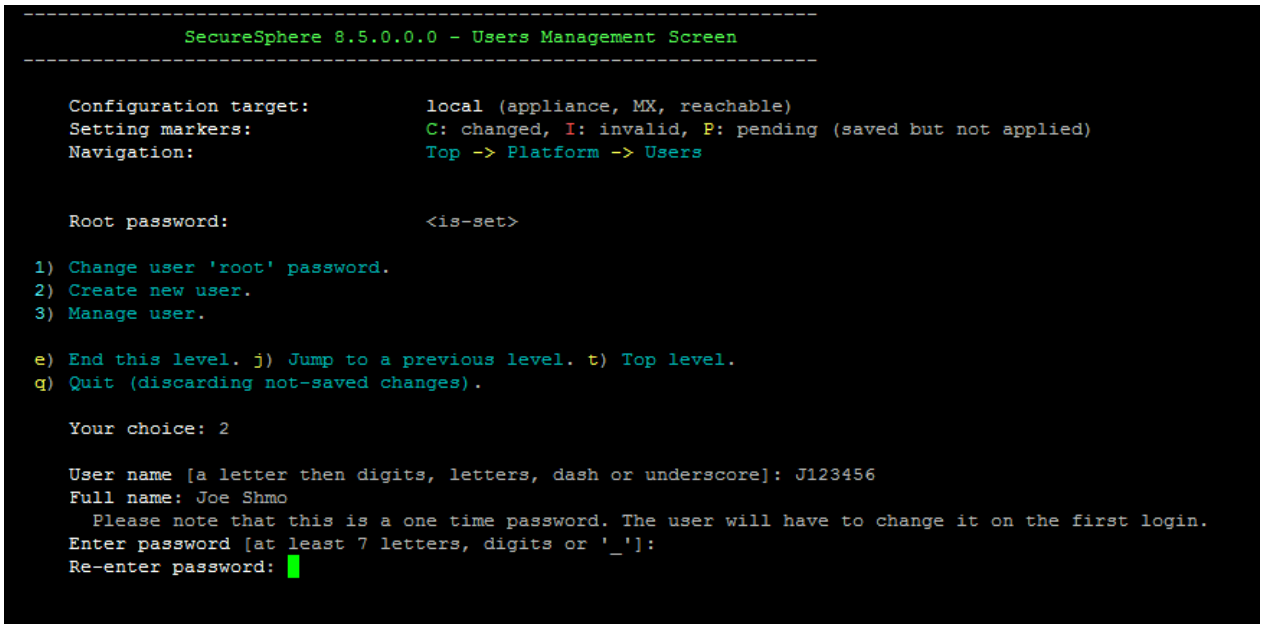


Figure 37: Creating a New User

1. Enter a user name.



Note:

- The user name must begin with a letter followed by letters, digits, dash or underscore characters.
- You cannot create a user whose name is one of the existing system users, for example, root, secure, *etc*.
- Only lowercase letters can be used to create user names. Upper case is not supported.

2. If the authentication method (see Configure RADIUS Authentication on page 104) is "user-defined" , you will be asked to specify whether authentication for this user is local or external.
   - If you choose external, then you have finished creating the new user. All the information about the user will be obtained from the external authentication server (RADIUS) when the user logs in.
   - If you choose "local", then continue with the next step.
3. Enter a full name for the user (see the figure above).
4. Enter a password for the user. The password is a one-time password, and the user will have to change it when he or she logs in for the first time.
5. Enter the password again. The new user will be saved in the SecureSphere database when you apply the pending changes (**Apply changes** in the **Top** screen).

Manage User

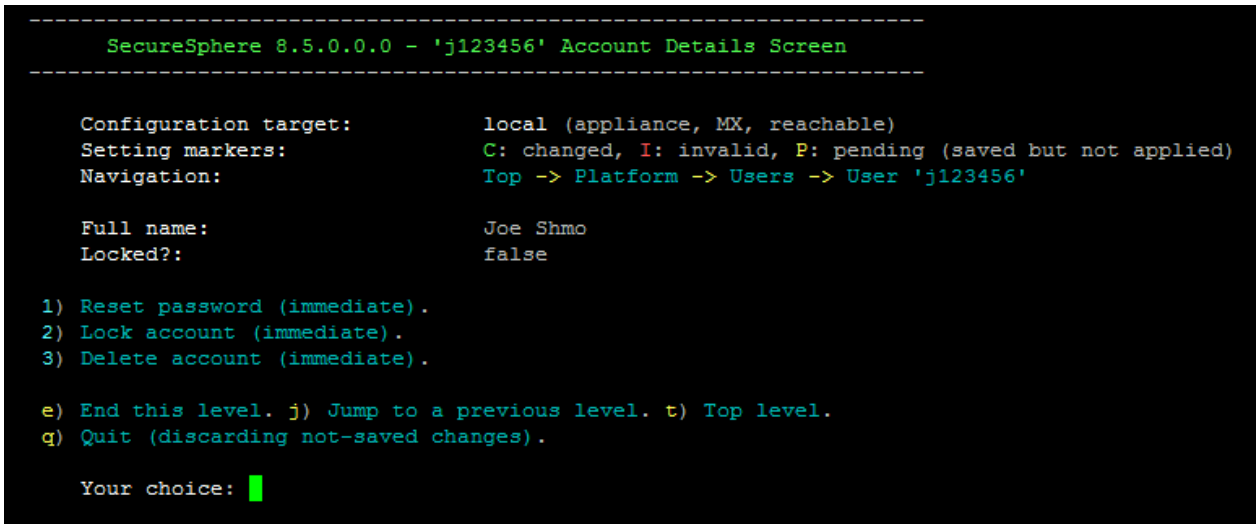


Figure 38: User Account Details Screen

- In the **User Account Details** screen (above), select one of the following options, as listed below.

User Account Details Options

Option	Name	Description
1	**Reset password (immediate).**	Reset (change) the user's password. You will be asked to enter a new password, and then to re-enter the same password. The password will be changed immediately. The new password is a one-time password, and the user will be asked to change it the next time he or she logs in. You can also enter the string "nochange", in which case you will be returned to the previous menu.
2	**Lock account (immediate).**	If the user's account is not locked, you can lock it by selecting this option.
3	**Unlock account (immediate).**	If the user's account is locked, you can unlock it by selecting this option.
4	**Delete account (immediate).**	Delete this user's account. You will be asked to confirm the deletion.

Configure RADIUS Authentication

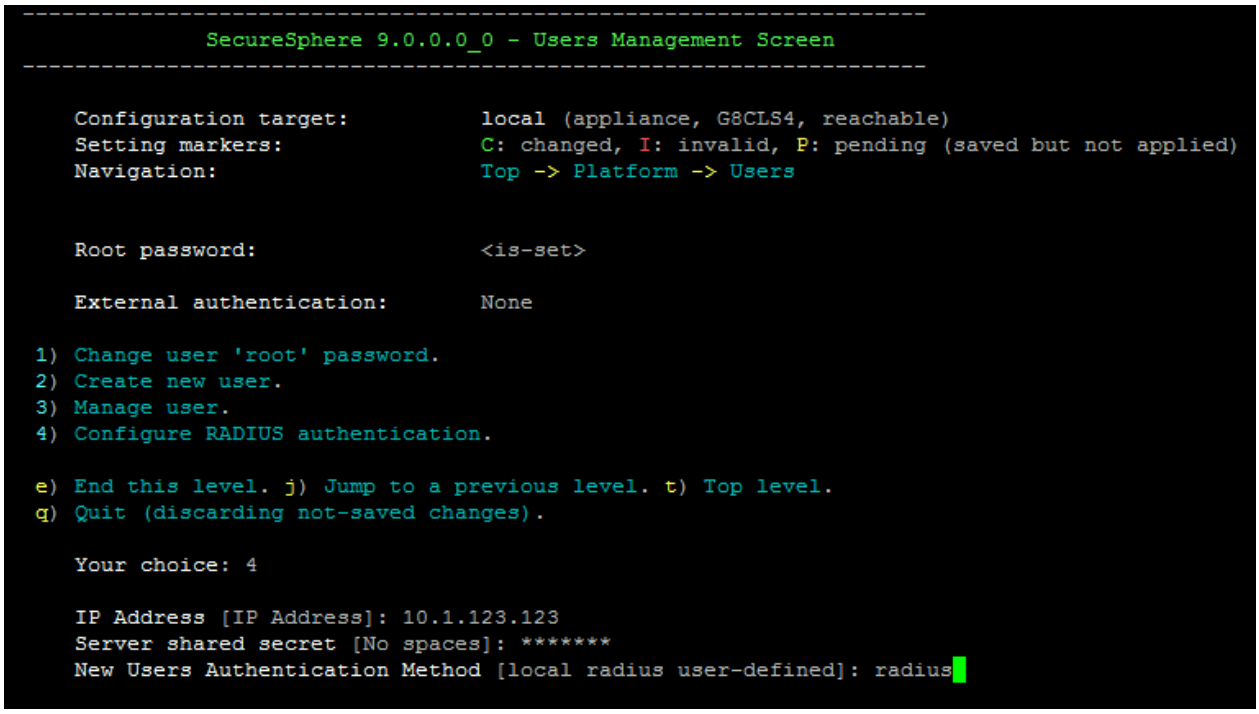


Figure 39: Configuring RADIUS Authentication

Specify the following information:

Name	Description
IP Address	The IP address of the RADIUS server.
Server shared secret	The shared secret between the RADIUS server and the SecureSphere appliance.
New Users Authentication Method	Select one of: • local - All new users will be authenticated by a password, locally on the SecureSphere appliance. • radius - All new users will be authenticated by the RADIUS server. • user-defined - The authentication method for new users will be specified at the time they are created. For more information, see Create New User on page 99 "Create New User" on page 102.



Note: To enable RADIUS authentication, you must also:

- Enable RADIUS (see Enable / Disable RADIUS on page 105 and Edit External Authentication Configuration on page 105 below).
- On the RADIUS server, establish trusted communication with the SecureSphere appliance.

Enable / Disable RADIUS

```
Your choice: 5

Radius enabled [true false]:
```

Figure 40: Enabling / Disabling RADIUS Authentication

Specify the following information:

Name	Description
RADIUS enabled	Specify "true" or "false".

Note: CLI RADIUS authentication, supports only PAP. SecureSphere MX RADIUS authentication supports PAP, CHAP, and MS-CHAP.

Edit External Authentication Configuration

```
Your choice: 6

External authentication [none radius]:
```

Figure 41: Enabling / Disabling External Authentication Configuration

Specify the following information:

Name	Description
External authentication	Specify "none" or "RADIUS".

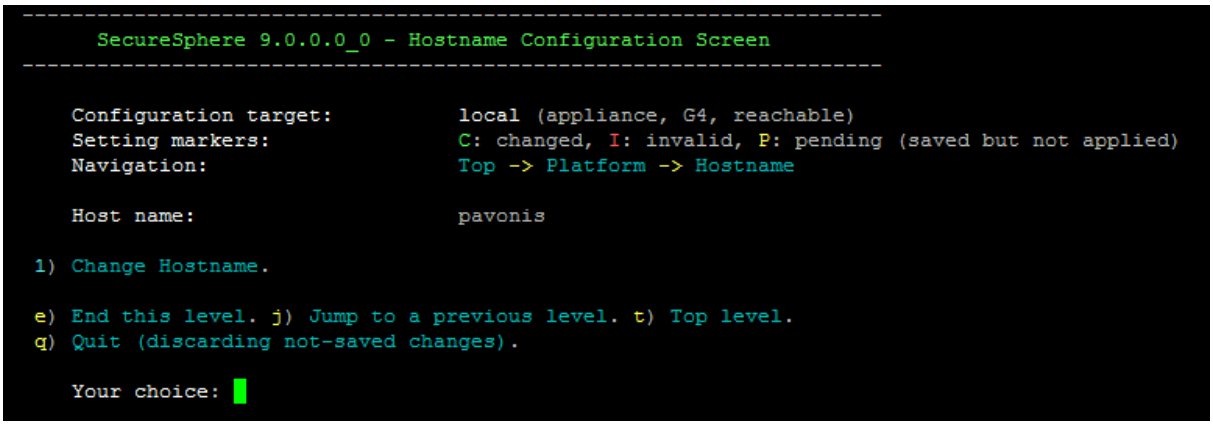
Hostname Management

You can:

- Change the hostname.

To manage the hostname:

1. In the **Platform Management** screen (as described in Configuring the Platform on page 89), select **4) Manage host name**. The **Hostname Configuration** screen is displayed.



2. Select one of the following options, as listed below.

Time Management Screen Configuration Options

Option	Name	Description
1	**Change Hostname**	Change the appliance's hostname.

Bootloader Password Management

1. Enter the bootloader user's existing password.
2. Enter a new password for the bootloader user.
   You can also enter the string "nochange", in which case you will be returned to the previous menu.
3. Enter the new password again.

Configuring SecureSphere Routes

You must define the SecureSphere routes listed in the table below using `impcfg`.

Static Routes Screen Configuration Options

Routes	Description	Data stored in
Platform Routes	These routes are related to the appliance, Management Server or Gateway, management interfaces. For more information, see Static Routes on page 96.	• `/etc/sysconfig/static-routes` (executed at boot time) • `bootstrap.xml`
Kernel Reverse Proxy **Apache Reverse Proxy** **SecureSphere Agent**	These routes are executed and added automatically according to the Gateway mode. They are deleted when the Gateway is stopped with the "`teardown`" option, and added when the Gateway is started with the "`prepare`" option. For more information, see: • Configuring Kernel Reverse Proxy on page 109 • Configuring Apache Reverse Proxy on page 109 • Configuring SecureSphere Agent Routes on page 107	`bootstrap.xml`
VRRP listeners for Agents **VRRP Reverse Proxy**	These routes are executed with relation to the VRRP status, either master or backup. For more information, see Configuring a Kernel Reverse Proxy on page 180.	`/etc/keepalived.conf`

Configuring SecureSphere Agent Routes

To configure SecureSphere Agent routes:

1. In the **Top** Screen, select option **1) Manage gateway.** The **Gateway Management** screen is displayed.
2. In the **Gateway Management** screen, select **6) Manage Remote Agents**. The **Remote Agents** screen is displayed

3. In the **Remote Agents** screen, select **6 - Manage remote-agent related routes**. The **Remote Agent Routes** screen is displayed.

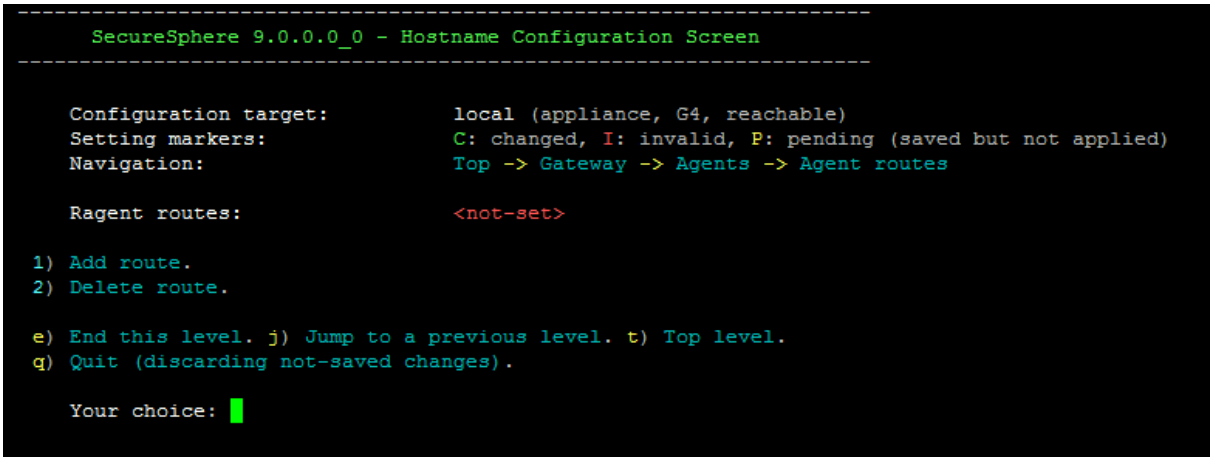


Figure 42: Remote Agent Routes Definition

4. Select one of the following options, as listed below.

Reverse Proxy (apache) Screen Configuration Options

Option	Name	Description
1	**Add Route**	Add a route.
2	**Delete Route**	Delete a route.

Configuring Transparent Reverse Proxy

To configure Transparent Reverse Proxy, perform the following tasks after the First Time Login is complete, as listed below.

Transparent Reverse Proxy Configuration Task Overview

	Task Overview	Step-By-Step
1	In `impcfg`, configure the appliance as a bridge.	**Manage SecureSphere Gateway** > **Change operation mode** and select **Bridge STP** or **Bridge IMPVHA**.
2	In the SecureSphere GUI, configure the server group. For more information, see the **SecureSphere User Guide**.	In the **Transparent Reverse Proxy** section of the **Definitions** tab of the server group (**Main** > **Setup** > **Sites**), select **Enable Transparent Reverse Proxy**.
3		Define the server IP addresses and ports for which the Gateway will act as Transparent Reverse Proxy.



Note: In the event of a conflict between a Transparent Reverse Proxy rule (**Main** > **Setup** > **Sites**) and another service's port configuration, the Transparent Reverse Proxy rule takes precedence.

Configuring Kernel Reverse Proxy



Note: Beginning with version 10.0 of SecureSphere, Kernel Reverse Proxy (KRP) is configured in the SecureSphere GUI (**Setup** > **Gateways**, in the **Networking** section of the Gateway's **Details** tab).

Configuring the Management Server for High Availability

For information on configuring High Availability for Management Servers, see Management Server High Availability (MX-HA) on page 353.

Configuring Apache Reverse Proxy

This section contains the following:

- Changing the Gateway's Mode to ARP on page 109
- Configuring ARP on page 109



Note: For information about configuring Kernel Reverse Proxy and Apache Reverse Proxy on the same Gateway, see Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway on page 111.

Changing the Gateway's Mode to ARP



Warning: Skip this step if either of the following is true:

- During the First Time Login, you configured this Gateway as ARP.
- This Gateway will be configured with both KRP and ARP, in which case it must be configured in impcfg `as KRP`.

Otherwise, follow these instructions.

To configure a Gateway as an Apache Reverse Proxy:

1. In the **Gateway Management** screen (as described in Configuring a Gateway on page 68), select option **4) Change operation mode**.
2. From the list of operation modes (as described in Configuring a Gateway as a Bridge on page 72), select **4) Reverse Proxy Apache**.
3. Configure an alias. See Configuring an Alias on page 184.

Configuring ARP

Configuring Apache Reverse Proxy consists of the following:

- Changing the HTTP listener port
- Configuring the `httpd.conf` file to include the protected hosts (virtual hosts)

To configure Apache Reverse Proxy:

1. Log on to the Gateway as the user `root`.

2. `cd` to the directory where the default Apache configuration file is located (`/etc/httpd/conf/httpd.conf`).
3. Back up the following files:
   - `httpd.conf`
4. Edit `httpd.conf` using a text editor (for example, `vi`).
5. Look for the following string: `Listen 80`
6. Comment out the line containing the above string by inserting the `#` character at the beginning of the line.
7. Add a new listening port.

   If ARP will be deployed together with KRP on this Gateway, then the listening port should be restricted to the loopback interface.

   In any case, the listening port should be restricted to the protected host.
8. The protected host is defined inside the virtual host tags. Each protected host has its own virtual host definition. Change the backend server IP address according to your setup.

   If you decide to use fully qualified domain names, you must have a resolving mechanism in place. To achieve this, configure the DNS server using `impcfg` or both.
9. Add the following at the end of the `httpd.conf` file:

```
Listen 127.0.0.1:88
NameVirtualHost X.X.X.X:88
<VirtualHost X.X.X.X:88>
        ServerName 10.3.220.22
        DocumentRoot /var/www/html/
        ProxyPreserveHost On
        RewriteEngine On
        RewriteRule ^/(.*) http://Y.Y.Y.Y/$1 [P]
        Header unset "WWW-Authenticate: NTLM"
        Header add WWW-Authenticate "Basic realm=SERVER-NAME"
</VirtualHost>
```

   If ARP and KRP are deployed on the same SecureSphere Gateway, then X.X.X.X should be `127.0.0.1` (the loopback interface).

   `Y.Y.Y.Y` is the backend server on port 80 (default to HTTP).

   For example, to redirect to the backend server 10.3.220.22 on port 90, the `RewriteRule` line would be:

   `RewriteRule ^/(.*) http://10.3.220.22:90/$1 [P]`
10. Repeat the last step for any additional hosts you may need to use. If you need to redirect to multiple servers, use different ports, where each port represents a server. The ports should not be already in use by another process.
11. Save the file.
12. Close the file.

    `httpd.conf` includes the `nss.conf` file, which is configured to listen to port 443. To avoid conflicts when ARP and KRP are deployed on the same SecureSphere Gateway, and KRP is configured to listen to port 443, comment out or reconfigure Apache to listen on a different port, as follows:

    `cd` to the `/etc/httpd/conf.d` directory.
13. Edit `nss.conf` using a text editor (for example, `vi`).
14. Look for the following string: `Listen 443`
15. Comment out the line containing the above string by inserting the `#` character at the beginning of the line.
16. Save the file.
17. Close the file.
18. Restart the HTTPD service by executing the following command:

```
service httpd start
```

The following is displayed on the screen:

```
starting httpd: [OK]
```

If the status is something other than `[OK]`, there is probably a conflict preventing the service from starting. Consult the Apache error log for details at `/etc/httpd/logs/error_log`.

For example, port conflict can prevent the service from starting.

19. Force `httpd` to start after reboot. by executing the following command:

```
ln -s /etc/init.d/httpd /etc/rc3.d/S99zhttpd
```

20. **Optional**: To check which ports are included in your configuration, execute the following command:

```
netstat -na | grep -I listen
```

This command lists all ports, not only the ones you have configured. On a Onebox appliance, it lists the server ports as well.



Note: The `/etc/httpd/logs/error_log` file logs debug information for the Apache configuration. Apache log levels are set up by default at `httpd.conf`. The `LogLevel` tag controls the number of messages logged to the error_log. Possible values include: `debug`, `info`, `notice`, `warn`, `error`, `crit`, `alert`, `emerg`.

Encryption (SSL)

Apache encryption to the backend server is not supported.



Note: If you are redirecting from HTTP to HTTPS or vice versa, make sure server hyper links are relative

Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway

When Kernel Reverse Proxy and Apache Reverse Proxy are deployed together on the same SecureSphere Gateway, the Kernel Reverse Proxy redirects matching traffic (based on URL and/or hostname) via the loopback interface to the Apache Reverse Proxy, which manipulates the session as required and communicates with the backend server.

For more information about this deployment, see Apache and Kernel Reverse Proxy on the Same Gateway on page 30.

To configure Kernel Reverse Proxy and Apache Reverse Proxy on the same SecureSphere Gateway:

1. Configure the Gateway as a Kernel Reverse Proxy, specifying that the outbound interface is the loopback interface.

   For information on how to configure Kernel Reverse Proxy, see Configuring Kernel Reverse Proxy on page 109.
2. Configure Apache Reverse Proxy on the same Gateway, specifying that the ARP listens on the loopback interface.

   For information on how to configure Apache Reverse Proxy, see Configuring Apache Reverse Proxy on page 108 "Configuring Apache Reverse Proxy" on page 109
3. Edit the Apache Reverse Proxy `httpd.conf` file and change the HTTP listener to listen to localhost on port 88 (for example, `listen 127.0.0.1:88`).
4. Edit `httpd.conf` to include protected hosts (virtual hosts).
5. Edit the Apache Reverse Proxy `nss.conf` file and comment out the line containing "`listen 443`" by inserting a `#` sign at the beginning of the line.

Switching Deployments

This section describes how to switch a SecureSphere appliance from one deployment mode to another, for example, from an inline gateway to a network monitor (sniffing) gateway, and includes:

Overview 112
From a Onebox to a Gateway 112
From a Gateway to a Onebox 112
Changing the MX of a Gateway 112

Overview

It is not possible to convert a gateway appliance to an MX applicance, because of their different hardware configurations. However, a Onebox appliance can be reconfigured as a gateway only or as a management server only, and this reconfiguration can be later reversed.

From a Onebox to a Gateway

To convert an appliance from a Onebox to a gateway:

1. Start `impcfg`.
2. Select **Manage SecureSphere Server**.
3. Select **1) Deactivate server.**

From a Gateway to a Onebox

To convert an appliance from a gateway to a Onebox:

1. Start `impcfg`.
2. Select **Manage SecureSphere Server**.
3. Select **1) Activate server.**

Changing the MX of a Gateway

To change the MX of a gateway:

1. Delete the audit data from the gateway.
2. Start `impcfg`.
3. Select **Manage SecureSphere Gateway** > **Perform Actions** > **Stop gateway**.
4. Select **Manage SecureSphere Gateway** > **Perform Actions** > **Unregister gateway**.
5. On the gateway, start `impcfg`.
6. Select **Manage SecureSphere Gateway** > **Change server address / password** and specify the new MX.

CHAPTER 5

Installing SecureSphere Agents

This chapter describes how to install the SecureSphere Agent from scratch and configure it using the CLI. For information on upgrading an existing SecureSphere Agent, see Upgrading the SecureSphere Agent on page 145.



Note: Information about AS/400 SecureSphere Agent installation can be found in the **SecureSphere User Guide**.

It includes the below sections:

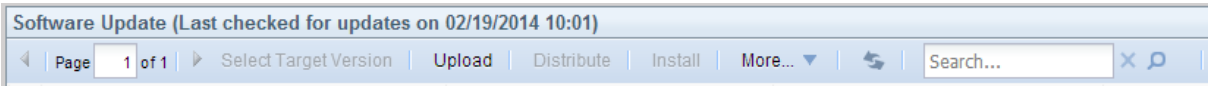
Installing a New SecureSphere Agent as part of Software Update 114
SecureSphere Agent Configuration Tasks 116
Installing the SecureSphere Agent 117
Uninstalling the SecureSphere Agent 144
Upgrading the SecureSphere Agent 145
Starting and Stopping the SecureSphere Agent 146
SecureSphere Agent Management Console 148
Working with High Availability 152
Diagnostic Tools 155
Prerequisite Tests for non-Windows Agents 157
Supported Interfaces for the Gateway Listener 160
Advanced Agent Configuration 161
Command Line Scripting Language 166

Installing a New SecureSphere Agent as part of Software Update

This procedure describes how to install a new SecureSphere Agent from the **Software Update** window.

To install a new SecureSphere Agent:

1. Before installing a new SecureSphere Agent, confirm that the SecureSphere Agent Installation Manager is installed on the protected server.
2. If you are installing a pre-version 10.5 SecureSphere Agent, confirm that:
   - No SecureSphere Agent is already installed on the protected server.
   - No SecureSphere Agent driver is in memory.
   - If either of the above is true, then you must uninstall the SecureSphere Agent and/or driver according to the instructions given in the **Administration Guide** for that SecureSphere Agent version.
3. In the Main workspace, select **Setup > Software Update**. The **Software Update** window is displayed.
4. In the **Software Update** window, confirm that the snapshot is up to date, that is, that the last check for updates occurred recently.



5. If the **Software Update** status is not up-to-date, then perform **synchcronization** (see The Software Update Synchronization Process).
6. Select the version you want to install as follows:

a) In the **Available Updates** column, click **View**. The **Available Updates** window is displayed.

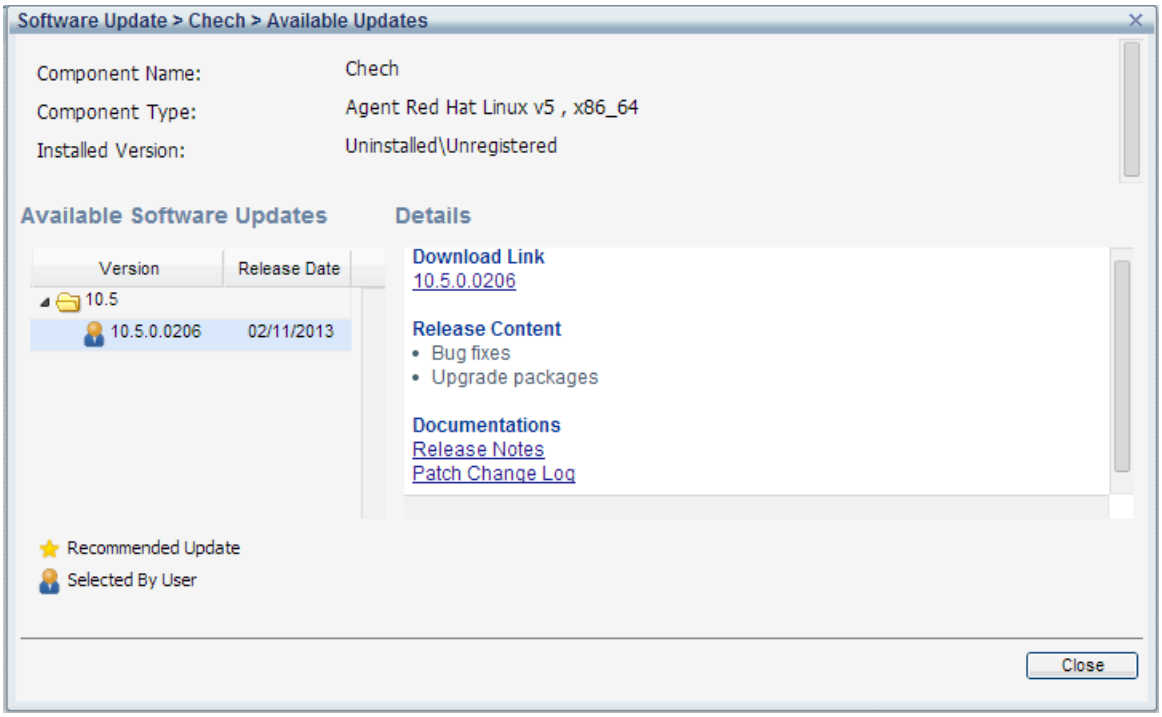


Figure 43: Available Updates

b) View the available options for SecureSphere Agent installation and close the window. You can also select the SecureSphere Agent(s) that you want to install.

c) In the **Software Update** window, select the SecureSphere Agent(s) that you want to install and click **Change Target Version**. The **Change Target Version** dialog box opens.

d) In the **Change Target Version** dialog box, select the version from the drop-down box and click **Save**. The **Change Target Version** dialog box closes and the **Target Version** column shows the version you want.

7. In the **Download** column, click on the button and download the installation package from the Imperva FTP site.
8. Save the downloaded file and perform the required tests to make sure this file is suitable.
9. In the **Software Update** window, click **Upload** and browse your computer to locate the update package file that you have tested. The status of all the relevant SecureSphere Agents changes to **Ready for Distribution**.
10. To distribute the uploaded package to all the relevant servers, click **Distribute**.
11. For information about how to install the SecureSphere Agents you have distributed, see the **SecureSphere Administration Guide** and the Release Notes for the SecureSphere Agents.

Note that you can only install a SecureSphere Agent using Software Update if the SecureSphere Agent Installation Manager is already installed on the target machine.

SecureSphere Agent Configuration Tasks

Installing and configuring the SecureSphere Agent is a straightforward process, as outlined in the following table.



Note: DB2 SecureSphere Agents on z/OS are installed and configured differently from other agents.

- For information on installing DB2 SecureSphere Agents on z/OS, see Chapter 15, Installing SecureSphere Agent for z/OS.
- For information on configuring DB2 SecureSphere Agents on z/OS, see the **SecureSphere User Guide**.

To install and configure the SecureSphere Agent (most typical scenarios):

SecureSphere Agent Configuration Task Checklist

Step		Action	Description	For more information, see
1		**Obtain the latest version of the SecureSphere Agent for your platform from the Imperva FTP site or from Software Update.**	Make sure you download the correct agent installation file for your platform. Carefully review the Release Notes before continuing to the next step.	Preparing for Installation on page 117
2		**Check the database or file server OS configuration.**	Confirm that the proper version of the database software (including patches) is installed and that communications are correctly configured.	Preparing the Database on page 120
3		**Configure the SecureSphere Gateway.**	Configure the Gateway so that it can communicate with the SecureSphere Agent.	Configuring the SecureSphere Gateway Before Installation on page 122
4		**Install the SecureSphere Agent.**	Install the SecureSphere Agent on the database and/or file server.	Installing the SecureSphere Agent "Installing the SecureSphere Agent and Installation Manager" on page 124
5		**Register the SecureSphere Agent to the Gateway.**	Register the Agent to the Gateway, so that it can start monitoring.	Installing the SecureSphere Agent "Installing the SecureSphere Agent and Installation Manager" on page 124
6		**Configure the SecureSphere Agent using the SecureSphere GUI.**	Configure the SecureSphere Agent in the **Agents** window in SecureSphere.	**SecureSphere User Guide**
7		**Troubleshooting and control.**	Use the management console for troubleshooting and control purposes.	SecureSphere Agent Management Console on page 148



Note: SecureSphere supports SecureSphere Agent versions earlier than 7.0, in a non-centrally managed mode.

The configuration is composed of:

- The first time configuration wizard (registration)
- The SecureSphere GUI for most of the configuration
- The management console, used primarily for troubleshooting and control (start/stop)

Installing the SecureSphere Agent

This section reviews the various stages of installing the SecureSphere Agentand includes the following information:

Preparing for Installation 117
Configuring the SecureSphere Gateway Before Installation 122
Installing the SecureSphere Agent and Installation Manager 124
After Installing the SecureSphere Agent 139
First-Time Configuration Wizard 140

Preparing for Installation

Before installing the SecureSphere Agent, perform the following:

- Obtaining the Latest Version of the SecureSphere Agent on page 117
- Verifying Prerequisites on page 118
- Preparing the Database on page 120

Obtaining the Latest Version of the SecureSphere Agent

The latest version of the SecureSphere SecureSphere Agent and the accompanying Release Notes are available from the Software Update screen in the SecureSphere GUI and also on the Imperva FTP site. See the **SecureSphere Agent Release Notes** for the exact location and file name on the FTP server, which depend on the OS under which the SecureSphere Agent will be running.

After downloading the SecureSphere Agent **but before installing the SecureSphere Agent**, carefully read the **SecureSphere Agent Release Notes**.



Note: You can also distribute SecureSphere Agent installation packages to the server using the Software Update feature for later installation. For more information, see, **SecureSphere User Guide**.

SharePoint

There are some special considerations for installing a SecureSphere Agent for SharePoint monitoring.

1. The SecureSphere Agent for SharePoint monitoring should be installed on only one of the WFEs. There is no need to install it on each of them.
2. Beginning with version 10.0, the SecureSphere Agent for SharePoint is compatible with SecureSphere versions 9.5 and above.
3. To install a SecureSphere Agent for SharePoint monitoring, a user requires local/domain (Windows) administrator permissions.

4. Installing and deploying a SecureSphere Agent for SharePoint monitoring may take some time in large-scale environments. You should verify the status of the SecureSphere Agent in the Agent Workbench before running the configuration wizard.
5. Once the SecureSphere Agent installation process is completed and the SecureSphere Agent is started, it deploys the Imperva web service (farm solution) on the customer's SharePoint site. This operation takes place automatically.

Verifying Prerequisites

Prerequisites are verified depending on the type of agent being installed.

- Verifying Prerequisites for non-Windows Agents on page 118
- Verifying Prerequisites for Windows Agents on page 119

Verifying Prerequisites for non-Windows Agents

The SecureSphere Agent installation file is an executable which runs a pre-install script that verifies the system is ready for installing the SecureSphere Agent and that all prerequisites are met. For more information, see Prerequisite Tests for non-Windows Agents on page 157.

- The agent requires 8GB of disk space for normal operation, and to ensure audit information is preserved in the event of network problems. This quota of 8 GB can be increased if needed.

The installation tool requires that the `df` program be in the defined `PATH` so that the available disk space can be determined. If this program is not in the `PATH`, then:

- If you are installing using the standard installation script, you will be asked to confirm that there is enough disk space available.
- If you are installing using the silent installation script, the installation will fail with an appropriate error message.



Note:

- You must install the SecureSphere Agent from the root user account (`su -root`).
- Before running the pre-install script, make sure that the `/tmp` directory free space is at least twice the size of the package (`bsx`) file.

If the pre-install script discovers no problems, the SecureSphere Agent is immediately installed.

You can also run only the pre-install script, in which case all tests performed by the pre-install script are run whether or not they fail and the script aborts before making any change to the system.

To run the pre-install script:



Note: The pre-install script is also run as part of the install script.

1. Make sure the SecureSphere Agent installation file has executable permissions.
2. Run the SecureSphere Agent installation file with the `-c` flag.

```
./ragent-<OS>-<OS version>-p<platform>-b<agent build>-r<agent release> [-k kabi_<n>.txt] -c
```



Note: The -k kabi_<n>.txt parameter is required only for SUSE and OEL UEK installations. See Special Considerations for SUSE and OEL UEK Platforms on page 130 below.

1. The following question appears:

```
Package root directory is /opt/imperva. "To change press 'n', otherwise
press 'y':"
```

   Answer no ('n') only if you will install the SecureSphere Agent in a location different from the default location.

SSH and Root Access

To complete the installation, you must have root user access to the DB host and SSH/Terminal connectivity.

HP-UX

For HP-UX, there are the following additional requirements:

- The HP-UX `swinstall` utility is used to install the SecureSphere Agent. For `swinstall` to run properly, forward (IP address to hostname) and reverse (hostname to IP address) resolution must be enabled. Note that this is a general HP-UX issue, not an Imperva-specific issue.

Verifying Prerequisites for Windows Agents

The following prerequisites must be met before the agent can be installed.

Windows Update Installer Version

Confirm that the Windows Installer version is 3.1 V1 (3.1.4000.1823) or later.

To determine the version of the Windows Installer:

1. Locate the file `MSI.DLL` (this file is usually in `C:\WINDOWS\SYSTEM32`).
2. Right-click on the file name.
3. From the menu, select **Properties**.
4. Click the **Version** tab.
5. If the version number is not as required, use Windows Update to update Windows Installer to the latest version.

Winpcap



Note: This section is relevant only for database SecureSphere Agents.

Winpcap is a packet capture application which is used by the SecureSphere Agent to monitor network database traffic on external interfaces. If you are using the SecureSphere Agent to monitor database traffic on external interfaces, you must install winpcap 4.1.2 or higher before you install the SecureSphere Agent, because of issues with earlier versions of winpcap.

If you do not install winpcap 4.1.2 or higher, there is a possibility that the server will crash due to these winpcap issues, regardless of whether the SecureSphere Agent is installed or running.

You can download the winpcap from the Imperva FTP server under the SecureSphere Agent directory.

User Privileges

To complete the installation, you must have administrator user privileges on the database, file server or SharePoint server, as appropriate, and terminal connectivity.

SharePoint SecureSphere Agents



Note: Installing and deploying a SharePoint SecureSphere Agent may take some time in large-scale environments. You should verify the status of the SecureSphere Agent in the Agent Workbench before running the configuration wizard.

Preparing the Database



Note: This section is relevant only for database SecureSphere Agents.

Many databases support several communication methods. In general, these fall into three categories: TCP/IP, TCP-local, and local inter-process communications (IPC).

The SecureSphere Agent monitors database activity by listening on three channels:

Channel	Visibility to SecureSphere
External interfaces	This SQL/TCP activity can also be visible to a SecureSphere Gateway.
Loopback interface	This activity **is not visible** to a SecureSphere Gateway, but it is visible to a SecureSphere Agent.
Inter-process communications (IPC)	This activity **is not visible** to a SecureSphere Gateway, but it is visible to a SecureSphere Agent. See the Release Notes for more information on the supported methods.

If the monitored database uses unsupported internal communication methods, you must configure the database to use the loopback for monitoring the local traffic. For example, if an Informix database is to be monitored locally, you must verify that its service is bound to the loopback interface.

If a SecureSphere Gateway is also monitoring the database activity, the relevant SecureSphere Agent should be configured so that it does not also monitor that same activity.

Automating the Registration of an Agent

You can configure SecureSphere so that agents will be registered automatically. To do this, you need to configure two capabilities:

Enabling Registration of an Agent with a Non-Existent Server Group 120

Enabling Automatic Creation of a Service for a Discovered Data Interface 121

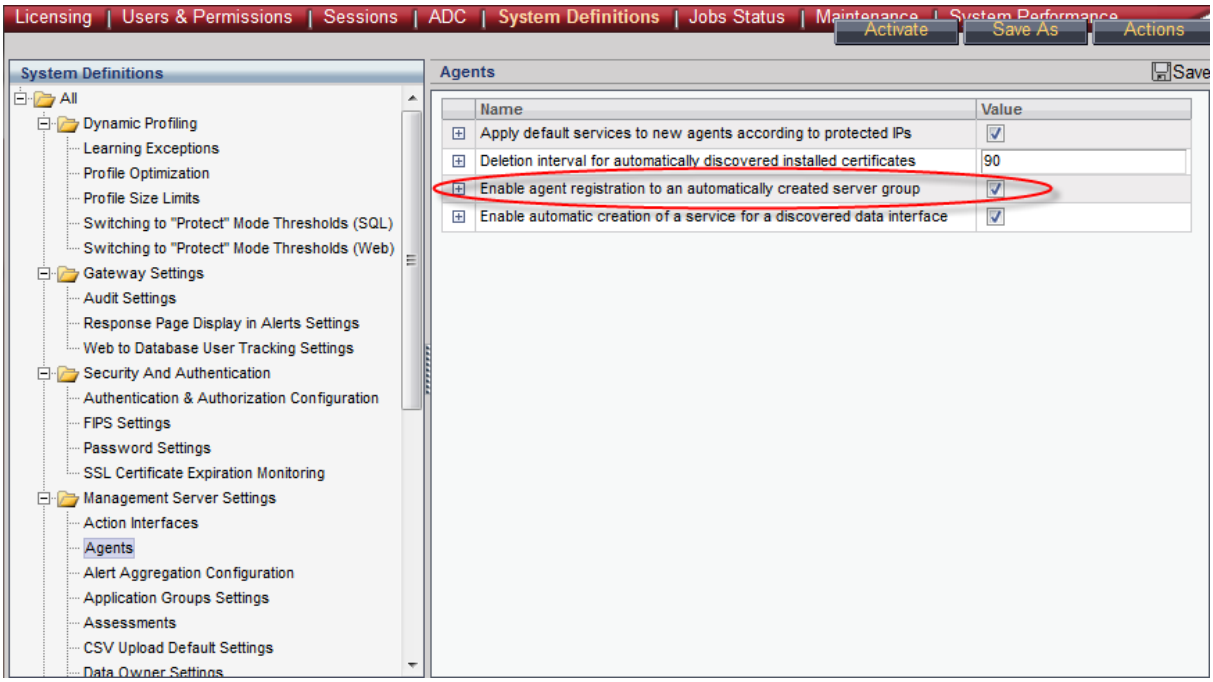
Enabling Registration of an Agent with a Non-Existent Server Group

In order to enable SecureSphere to accept the registration of agents with non-existent server groups you must first configure SecureSphere correctly. Thereafter, when you register an agent with a non-existent server group, that group is created automatically.

To enable registration of an agent with a non-existent server group:

1. Select **Admin > System Definitions**.
2. In the **System Definitions** tree, select **Management Server Settings > Agents**.

3. In the right pane, check **Enable agent registration to an automatically created server group**.

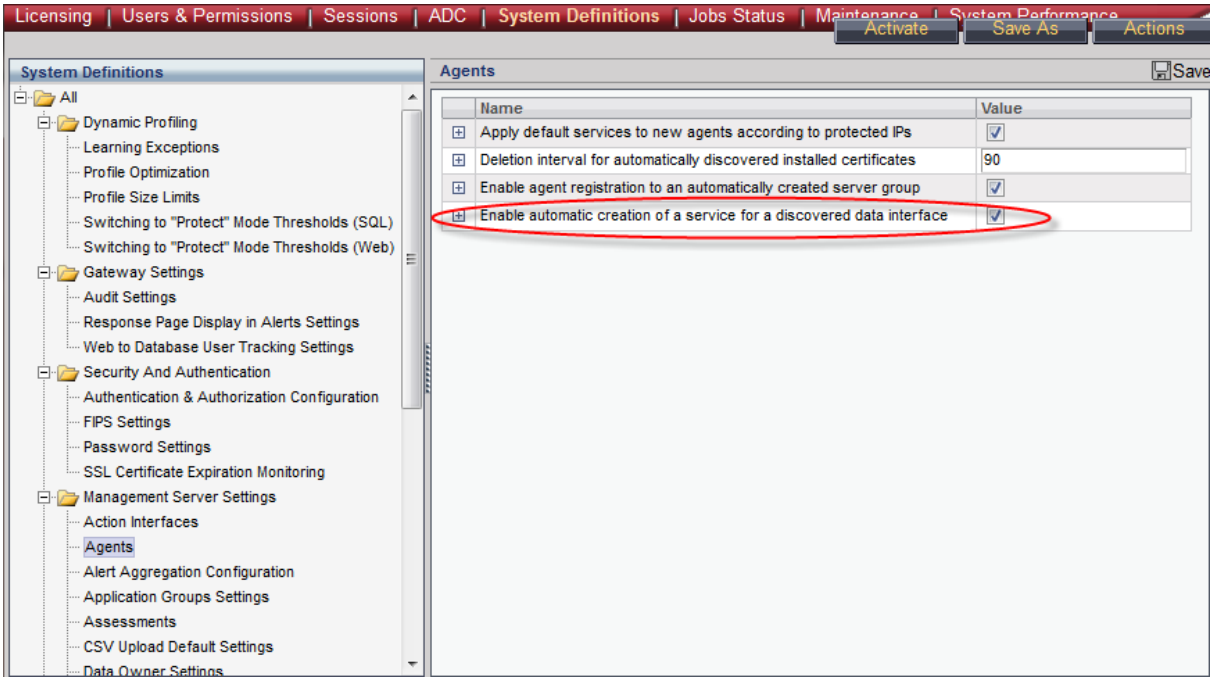


Enabling Automatic Creation of a Service for a Discovered Data Interface

In order to enable automatic creation of a service for a discovered data interface, you must first configure SecureSphere correctly. When a new database is discovered thereafter, if there is no existing service for that database type, a new service and application is created and associated with the relevant data interface.

To enable automatic creation of a service for a discovered data interface:

1. Select **Admin > System Definitions**.
2. In the **System Definitions** tree, select **Management Server Settings > Agents**.
3. In the right pane, check **Enable automatic creation of a service for a discovered data interface**.



Configuring the SecureSphere Gateway Before Installation

The following configuration procedures must be performed on the Gateway before installing a SecureSphere Agent:

- **Configure the listeners**. For more information, see Configuring Listeners on page 122.
- **Configure routing**. For more information, see Manage SecureSphere Agent Related Routes on page 123.

Configuring Listeners

SecureSphere Agent communicates with the SecureSphere Gateway in two ways. It uses port 443 (this can be changed during the Gateway configuration) for registration, status, configuration and discovery of new data interfaces and a user defined port to transfer the captured DB activity. Communication is over a secure TCP connection to a listener IP address defined on the Gateway. The listener is typically configured on the Gateway management IP address.



Note:

- You can define multiple listeners on a Gateway, and you can direct different SecureSphere Agents to different listeners.
- Bridge and sniffing interfaces cannot be defined as listener interfaces.
- A SecureSphere Agent listener and a SecureSphere Agent for DB2 z/OS listener cannot be defined on the same port.

To configure a listener on SecureSphere Gateway:

1. Start the `impcfg` CLI application on the Gateway.
2. Select **Manage the SecureSphere gateway** from the Top menu.
3. Select **Manage remote agents**.
4. Select **Add a listener**.
5. Configure the listener parameters (see following table).

Listener Parameters

Option	Description
Listener type	The communication protocol between the SecureSphere Agent and the Gateway. Only TCP can be used. The listener is the end point for the SecureSphere Agent communication.
Listener IP address	The IP address to which the SecureSphere Agent sends data. The IP address is assigned to the selected interface. Typically, you will select the IP address of the Gateway's management interface. This IP address must be routable from the DB host. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. If there is a firewall between the SecureSphere Agent and the listener IP address, you must ensure that communication between them is allowed by the firewall. If the listener IP address is NATed, see Working with a NATed Listener on page 161
Listener IP mask	The network mask for the listener IP address. When Gateway management IP address is used, enter its mask as defined on the Gateway.
Listener port	The data port to which the SecureSphere Agent sends its data. The port should be accessible and available. Choose a high port, for example 5555. If there is a firewall between the SecureSphere Agent and the listener IP address, you must ensure that communication between them is allowed by the firewall. **Note:** Allowed values: 1 - 65355.
Listener interface	The physical Gateway interface used for the listener. Typically, you will select the Gateway's management interface. For more information, see Supported Interfaces for the Gateway Listener on page 160. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces. Possible value: eth5 | eth4 | eth3 | eth2 | eth1 | eth0
Virtual IP	When asked whether to enable virtual IP for the listener enter "n", unless you are using high availability Gateways. For more information, see Working with High Availability on page 152. Possible value: y | n
Enable SSL	Enter "y" to encrypt traffic between the SecureSphere Agent and its listener. Possible value: y | n

Manage SecureSphere Agent Related Routes

The Gateway listener and SecureSphere Agent communicate over a secure TCP tunnel. In some environments, specific routes must be explicitly defined to enable the Gateway to reach the DB host or file server IP address. SecureSphere allows setting these routes using the `impcfg` application on the Gateway.

To define SecureSphere Agent-related routes on the Gateway:

1. Start the `impcfg` CLI application on the Gateway.
2. Select **Manage the SecureSphere gateway**.
3. Select **Manage remote agents**.
4. Select **Manage remote-agent related routes**.
5. Add or delete a route (see following tables):

Adding a Route

Option	Description
Will this be a virtual route, belonging to one of them?	Choose `n`, unless you are using high availability Gateways. For more information, see Working with High Availability on page 152. Possible values: y| n.
Type	Define whether this route is per subnet or specific to host. Enter "host" unless you want the route to be valid for the whole network. Possible values: net | host.
Address	Available only when Type is "host". Enter the IP address of the DB host.
Network	Available only when Type is "net". Enter the IP address of the network base on the network subnet. For example, if the DB host's IP address is 192.168.10.10 and its subnet mask is 255.255.0.0, the net IP address will be 192.168.0.0.
Subnet mask	Available only when Type is "net". Enter the subnet mask of the network. Using the same example, the net subnet mask will be 255.255.0.0.
Gateway	The default Gateway IP address used for the listener. Enter the default Gateway IP address, which must be reachable from the listener subnet. If the listener IP address is the management IP address, you can choose a default Gateway from the management subnet.
Device	The specific Gateway physical interface to be used. If no interface is specified, the best available interface will be selected when routing.

Deleting a Route

Option	Description
Delete route	A list of available routes is displayed. Choose the route you wish to delete.

Agent routes are executed and added automatically when the Gateway starts and are deleted automatically when Gateway is stopped. The routes are maintained in the Gateway's `bootstrap.xml` file.

Installing the SecureSphere Agent and Installation Manager

The SecureSphere Agent installation file is self-executable.

This section includes the following:

Installing the SecureSphere Agent and Installation Manager on a non-Windows System 124

Special Considerations for SUSE and OEL UEK Platforms 130

Installing the SecureSphere Agent and Installation Manager on a Windows System 131

Silent Registration Parameters 135

Installing the SecureSphere Agent and Installation Manager on a non-Windows System

The installation tool requires that the `df` program be in the defined `PATH` so that the available disk space can be determined. If this program is not in the `PATH`, then:

- If you are installing using the standard installation script, you will be asked to confirm that there is enough disk space available.
- If you are installing using the silent installation script, the installation will fail with an appropriate error message.



Note: If you have installed the SecureSphere Agent Installation Manager, then instead of the procedure described here, you can distribute and install SecureSphere Agents from the Management Server using the Software Update feature.

To install the SecureSphere Agent on a non-Windows system:

1. Login to the machine as user `root` by entering the following command:

```
su - root
```

2. Download and save the installation package, for example, to the `/tmp` directory.

   For information on obtaining the latest version of the SecureSphere Agent software and release notes, see Obtaining the Latest Version of the SecureSphere Agent on page 117.

   The installation package file name is given in the Release Notes.
3. Untar the installation package file, which contains the following files:
   - An installation file for the SecureSphere Agent. This file is a `.bsx` file and its name contains the string `ragent`.
   - An installation file for the SecureSphere Agent Installation Manager. This file is a `.bsx` file and its name contains the string `ragentinstaller`.
   - An installation batch file (`install.sh`)
   - A readme file.
   - A file with the suffix "`metadata`" which is used by the installation files.
4. Verify that the installation files have executable permissions.
5. You can install both the SecureSphere Agent and the SecureSphere Agent Installation Manager by running the following commands (assuming that you downloaded the files to the `/tmp` directory):

```
cd /tmp
install.sh [-k kabi_<n>.txt]
```



- **Notes:**
  Installing using the `install.sh` script is the recommended option.
- The `-k` argument is required only for SUSE and OEL UEK installations. See Special Considerations for SUSE and OEL UEK Platforms on page 130 below.
- The `-h` parameter means print the help for this command.
- The `install.sh` script performs an interactive installation, not a silent one.

   Alternatively, advanced users can install the SecureSphere Agent and the SecureSphere Agent Installation Manager separately as described in the next steps.
6. Install the SecureSphere Agent using either:
   - The standard installation script, which installs the SecureSphere Agent, registers the SecureSphere Agent by running the interactive configuration wizard, and then starts the SecureSphere Agent. For more information, see Installing the SecureSphere Agent on a Non-Windows System Using the Standard Script on page 126.
   - A silent installation script, which installs the SecureSphere Agent, registers the SecureSphere Agent by running a non-interactive CLI command, and then starts the SecureSphere Agent. For more information, see Silently Installing the SecureSphere Agent on a non-Windows System on page 126.
7. If your Management Server is version 10.5 or higher, install the SecureSphere Agent Installation Manager using either:

- The standard installation script, which installs the SecureSphere Agent Installation Manager, registers the SecureSphere Agent Installation Manager by running the interactive configuration wizard, and then starts the SecureSphere Agent Installation Manager. For more information, see Installing the SecureSphere Agent Installation Manager on a Non-Windows System Using the Standard Script.
- A silent installation script, which installs the SecureSphere Agent Installation Manager, registers the SecureSphere Agent Installation Manager by running a non-interactive CLI command, and then starts the SecureSphere Agent Installation Manager. For more information, see Silently Installing the SecureSphere Agent Installation Manager on a non-Windows System on page 128.

Installing the SecureSphere Agent on a Non-Windows System Using the Standard Script

To install the SecureSphere Agent on a non-Windows system using the standard script:

1. Uncompress (untar) manual-settings-activation=
2. the installation package.
3. Execute the following commands (assuming that you uncompressed the installation package to the `/tmp` directory).

```
cd /tmp
<SecureSphere Agent installation file> [-k kabi_<n>.txt]
```



Note: The `-k` parameter is required only for SUSE and OEL UEK installations. See Special Considerations for SUSE and OEL UEK Platforms on page 130 below.

4. You are asked to specify a package root directory or to accept the default.
5. The package and system configurations are displayed and verification tests run.

   If any of the tests fails, the installation is aborted.

Silently Installing the SecureSphere Agent on a non-Windows System

Silent installation enables you to install, register and start the SecureSphere Agent without running the interactive configuration wizard.

To silently install the non-Windows agent:

1. Execute the following command:

```
<remote agent package full path> -n
```

2. Register the SecureSphere Agent to the Gateway by executing the following command:

```
<remote agent directory>/ragent/bin/cli --dcfg <remote agent
directory>/ragent/etc --dtarget <remote agent directory>/ragent/etc
--dlog <remote agent directory>/ragent/etc/logs/cli --dvar <agent
directory>/var registration advanced-register
registration-type=<Primary | Secondary> ragent-name=<remote agent
name>
site=mysite server-group="my server gropup"
gw-ip=<gateway IP | hostname> gw-port=<443>
manual-settings-activation=<Automatic | Manual>
monitor-network-channels=<Both | Local> password=<secure>
```

The parameters are explained in Silent Registration Parameters below.

Alternatively, if you want to accept all the defaults, then execute the following command:

```
<remote agent directory>/ragent/bin/cli [--dcfg <remote agent
directory>/ragent/etc --dtarget <remote agent directory>/ragent/etc
--dlog <remote agent directory>/ragent/etc/logs/cli] registration
advanced-register ragent-name=<remote agent name> gw-ip=<gateway IP |
hostname>
```



Note: The parameters within the "[ ]" need to specified only if you installed the SecureSphere Agent in a directory different from the default directory.

If you want to change one of the other parameters, you can add it to the command (see the full command above). For example:

```
<remote agent directory>/ragent/bin/cli [--dcfg <remote agent
directory>/ragent/etc --dtarget <remote agent directory>/ragent/etc
--dlog <remote agent directory>/ragent/etc/logs/cli] registration
advanced-register ragent-name=<remote agent name> gw-ip=<gateway IP |
hostname>
gw-port=<gateway management port>
```

3. Start the agent by executing the following command:

```
<remote agent directory>/ragent/bin/rainit start
```

Silent Registration Parameters

Parameter	Description
`-d`	The target directory for the installation. If not specified, the SecureSphere Agent will be installed in the default directory. **Note:** This option cannot be used together with the -u option.
`-u`	Upgrade the SecureSphere Agent from a previous installed version. **Note:** This option cannot be used together with the -d option. For more information, see ""Upgrading the SecureSphere Agent on page 145.
-k `kabi_<n>.txt`	The `-k` argument is required only for SUSE and OEL UEK installations. See Special Considerations for SUSE and OEL UEK Platforms on page 130 below.
`-c`	Run the check installation script and then exit without installing the SecureSphere Agent. **Note:** This option implies the -n option.
`-f`	Do not check whether there is sufficient available disk space before installing.
`-i`	Do not perform checksum validation of the installation package.
`-n`	Do not run the CLI registration script after the installation completes. **Note:** This option should not be used together with the -u option.

Parameter	Description
-s	Start the SecureSphere Agent after the upgrade completes. **Note:** This option can only be used together with the -u option.
-h	Display this help.

EXAMPLE: SILENT SECURESPHERE AGENT INSTALLATION

For example, the following commands silently install the SecureSphere Agent, register the SecureSphere Agent to the Gateway at IP address 10.10.10.10, and then start the SecureSphere Agent:

```
/tmp/agent.bsx -n -d /opt/imperva
/opt/imperva/ragent/bin/cli --dcfg /opt/imperva/ragent/etc --dtarget
/opt/imperva/ragent/etc --dlog /opt/imperva/ragent/etc/logs/cli
registration advanced-register registration-type=Primary
ragent-name=`hostname' gw-ip=mygateway gw-port=443
manual-settings-activation=Automatic monitor-network-channels=Both
password=secure
/opt/imperva/ragent/bin/rainit start
```

Silently Installing the SecureSphere Agent Installation Manager on a non-Windows System

Silent installation enables you to install, register and start the SecureSphere Agent Installation Manager without running the interactive configuration wizard.

You have two alternatives.

- You can copy the SecureSphere Agent Installation Manager installation parameters from an existing SecureSphere Agent installation.
- You can explicitly specify the SecureSphere Agent Installation Manager installation parameters.

To silently install the non-Windows SecureSphere Agent Installation Manager and copy the installation parameters from an existing SecureSphere Agent installation:

The SecureSphere Agent must already be installed and registered before you can do this.

1. You have two alternatives. If you want to copy the installation parameters from an existing SecureSphere Agent, execute the following command:

   ```
   <agent installation manager executable full path> -n -x
   ```

   The executable file is a `.bsx` file, for example, `./Imperva-ragentinstaller-RHEL-v5-kSMP-pi386-b1.0.0.0008.bsx`

   The `-x` argument specifies that the installation parameters (for example, directory) are copied from the SecureSphere Agent.

2. Next, register the SecureSphere Agent Installation Manager to the Gateway by executing the following command:

   ```
   <agent installation manager directory>/installer/bin/cliinstaller
   --dcfg <agent installation manager directory>/installer/etc --dvar
   <agent installation manager directory>/installer/var --dtarget <agent
   installation manager directory>/installer/etc --dlog <agent
   installation manager directory>/installer/etc/logs/cli registration
   register-use-existing package-folder-path="."
   package-folder-size=1024
   ```

   The parameters are explained in Silent Registration Parameters below.

3. Finally, start the SecureSphere Agent Installation Manager by executing the following command:

```
<agent installation manager directory>/installer/bin/rainstallerinit
start
```

To silently install the non-Windows SecureSphere Agent Installation Manager and explicitly specify the SecureSphere Agent Installation Manager installation parameters:

1. Alternatively, if you do not want to copy installation parameters from an existing SecureSphere Agent, execute the following command:

   ```
   <agent installation manager executable full path> -n -d <directory>
   ```

   The executable file is a `.bsx` file, for example, `./Imperva-ragentinstaller-RHEL-v5-kSMP-pi386-b1.0.0.0008.bsx`

   The `-d` argument specifies the installation directory.

2. Next, register the SecureSphere Agent Installation Manager to the Gateway by executing the following command:

   ```
   <agent installation manager directory>/bin/cliinstaller --dcfg <agent
   installation manager directory>/etc --dvar <agent installation manager
   directory>/var --dtarget <agent installation manager directory>/etc
   --dlog /<agent installation manager directory>/etc/logs/cli
   registration advanced-register registration-type=Primary gw-ip=myGW
   gw-port=443 password=secure ragent-name=gil_agent123
   package-folder-path="." package-folder-size=1024
   ```

3. Start the SecureSphere Agent Installation Manager by executing the following command:

   ```
   <agent installation manager directory>/bin/rainstallerinit start
   ```

Silent Registration Parameters

Parameter	Description
`-d`	The target directory for the installation. If not specified, the SecureSphere Agent Installation Manager will be installed in the default directory. **Note:** This option cannot be used together with the -u option.
`-u`	Upgrade the SecureSphere Agent Installation Manager from a previous installed version. **Note:** This option cannot be used together with the -d option. For more information, see ""Upgrading the SecureSphere Agent on page 145.
`-f`	Do not check whether there is sufficient available disk space before installing.
`-i`	Do not perform checksum validation of the installation package.
`-n`	Do not run the CLI registration script after the installation completes. **Note:** This option should not be used together with the -u option.
`-s`	Start the SecureSphere Agent Installation Manager after the upgrade completes. **Note:** This option can only be used together with the -u option.
`-h`	Display this help.

EXAMPLE: SILENT SECURESPHERE AGENT INSTALLATION MANAGER INSTALLATION

For example, the following commands silently install the SecureSphere Agent Installation Manager, register the SecureSphere Agent Installation Manager to the Gateway at IP address 10.10.10.10, and then start the SecureSphere Agent Installation Manager:

```
/tmp/agent.bsx -n -d <agent installation manager directory>
   <agent installation manager directory>/bin/cliinstaller --dcfg <agent
   installation manager directory>/etc --dvar <agent installation manager
   directory>/var     --dtarget     <agent     installation     manager
   directory>/installer/etc    --dlog    <agent    installation    manager
   directory>/installer/etc/logs/cli    registration    advanced-register
   registration-type=Primary       gw-ip=10.100.43.116       gw-port=443
   password=secure      ragent-name=myAgent      package-folder-path="."
   package-folder-size=1024
/opt/imperva/ragentinstaller/bin/rainstallerinit start
```

Special Considerations for SUSE and OEL UEK Platforms

SUSE and OEL UEK maintains several version of their OS, and service packs for each version. In addition, SUSE periodically releases updates to service packs, which sometimes include updated versions of the kernel.

Imperva SUSE and OEL UEK SecureSphere Agents are specific to SUSE and OEL UEK versions and service packs, and are certified by Imperva as compatible with all kernel versions of a given service pack which were current at the time of the SecureSphere Agent's release. When a new kernel version is released, Imperva tests the SecureSphere Agent for compatibility with the new kernel.

Incompatibilities can arise in the following situations:

- You are trying to install a SecureSphere Agent on a platform whose kernel is incompatible with that SecureSphere Agent version.
- You are trying to start a SecureSphere Agent on a platform whose kernel you have upgraded to a version incompatible with that SecureSphere Agent version.

  In this case, the SecureSphere Agent will not start, and a message will be displayed on the system console, and also in the log file `<installation directory>/ragent/etc/logs/agentstart.log`.

When Installing a SUSE or OEL UEK SecureSphere Agent

The SUSE and OEL UEK SecureSphere Agent installation package includes, in addition to the files listed in Installing the SecureSphere Agent and Installation Manager on a non-Windows System on page 124, a supported kernel versions file (`kabi_<n>.txt`), where `<n>` is the version number of the `kabi` file.

The `kabi` file is in the `\Downloads\SecureSphere_Agents\Misc` directory, and applies to all SUSE and OEL UEK versions.

The pre-install script tests the compatibility of the SecureSphere Agent with the kernel version by comparing the kernel version with the list in the supported kernel versions file. If the test fails, an error message is displayed and the installation is terminated.

If you receive this error message, download the correct file.

When Starting a SUSE or OEL UEK SecureSphere Agent

Each time the SecureSphere Agent starts, it tests its compatibility with the kernel version. If the test fails, an error message is displayed on the system console (and written to the log file in the log file `<installation directory>/ragent/etc/logs/agentstart.log`) and the SecureSphere Agent is not started. This can happen if you have upgraded the kernel to a version with which the SecureSphere Agent is not compatible.

If you receive this error message, it may be that the kernel version is indeed supported, but because the supported kernel versions file is out-of-date, the SecureSphere Agent fails the test.

If your Management Server and SecureSphere Agent are both version 10.0 or higher then the nightly Software Update synchronization will update your supported kernel versions (kabi) file with the latest version, which will automatically solve this problem. For more information, see the "Software Update" chapter in the **SecureSphere User Guide**.

Otherwise, to solve this problem, proceed as follows:

1. Go to the Imperva FTP site.
2. Download the file `update_ragent_supported_suse_kernels_<n>.bsx` (where `<n>` is the version number) from the `\Downloads\SecureSphere_Agents\Misc` directory.
3. Run the file you just downloaded.

   This updates the `kabi_<n>.txt` file to the latest version.
4. Start the SecureSphere Agent.
5. If the problem persists, contact support.

   It may be that the kernel version to which you have upgraded is not compatible with the SecureSphere Agent. Consult with Imperva support about what you should do next.

Installing the SecureSphere Agent and Installation Manager on a Windows System

To install the SecureSphere Agent on a Windows system:



Note: If you have installed the SecureSphere Agent Installation Manager, then instead of the procedure described here, you can distribute and install SecureSphere Agents from the Management Server using the Software Update feature.

1. Login to the machine as administrator or as a user with administrator privileges.
2. Download and save the installation file.

   For information on obtaining the latest version of the SecureSphere Agent software and release notes, see Obtaining the Latest Version of the SecureSphere Agent on page 117.

   The installation package name is given in the Release Notes.
3. Save the installation package on the local hard disk.
4. Unzip the installation package file, which contains the following files:
   - An installation file for the SecureSphere Agent. This file's name contains the string `ragent`.
   - An installation file for the SecureSphere Agent Installation Manager. This file's name contains the string `ragentinstaller`.
   - A readme file.
   - A file with the suffix "`metadata`" which is used by the installation files.
5. Install the SecureSphere Agent using either:
   - The standard installation script, which installs and registers the SecureSphere Agent by running the interactive configuration wizard, and then starts the SecureSphere Agent (see Installing the SecureSphere Agent on a Windows System Using the Standard Script on page 132)
   - A silent installation script, which installs the SecureSphere Agent, registers the SecureSphere Agent by running a non-interactive CLI command, and then starts the SecureSphere Agent (see Silently Installing the SecureSphere Agent on a Windows System on page 132)
6. Install the SecureSphere Agent Installation Manager, using either:
   - The standard installation script, which installs and registers the SecureSphere Agent Installation Manager by running the interactive configuration wizard, and then starts the SecureSphere Agent Installation Manager. For more information, see Installing the SecureSphere Agent Installation Manager on a Windows System Using the Standard Script on page 134.

- A silent installation script, which installs the SecureSphere Agent Installation Manager, registers the SecureSphere Agent Installation Manager by running a non-interactive CLI command, and then starts the SecureSphere Agent Installation Manager. For more information, see Silently Installing the SecureSphere Agent Installation Manager on a Windows System.



Note: You should install the SecureSphere Agent Installation Manager only if your Management Server is version 10.5 or higher.

Installing the SecureSphere Agent on a Windows System Using the Standard Script

To install the SecureSphere Agent on a Windows system using the standard script:

1. Run the MSI installation file you downloaded as administrator.

   If you do not have administrator privileges, proceed as follows:

   - Open Windows Explorer and navigate to the MSI file (the installation file you saved in step 2 in Installing the SecureSphere Agent on a Windows System "Installing the SecureSphere Agent and Installation Manager on a Windows System" on page 131).
   - Shift-right-click the MSI file and select **Run as different user** from the menu.
   - In the **Run As** window, select **The Following User.**
   - Choose a user with administrator privileges.
   - Enter the password.
   - Click **OK**

   Otherwise, run the SecureSphere Agent installation file by executing the following command:

```
msiexec /i "<agent full path>\<package name.msi>"
```



Note: When you open a CLI, make sure that it is opened with administrator privileges.

Silently Installing the SecureSphere Agent on a Windows System

Silent installation enables you to install, register and start the SecureSphere Agent without running the interactive configuration wizard.

To silently install the Windows SecureSphere Agent:



Note: When you open a CLI, make sure that it is opened with administrator privileges.

1. Execute the following command:

```
msiexec /i "<remote agent package full path>\<package name.msi>"
NOSCRIPT=true /quiet
```

2. Replace `<remote agent package full path>` with the full path name of the directory to which you downloaded the installation package, and `<package name.msi>` with the name of the installation file. Enclose the whole string in quotes.

- – TARGETDIR=%INSTALLDIR%: The target directory for the installation. If not specified, the SecureSphere Agent will be installed in the default directory.

3. Register the SecureSphere Agent to the Gateway by executing the following command:

```
"<remote agent directory>\RemoteAgentCli.exe" --dcfg "<remote agent
directory>" --dtarget "<remote agent directory>" --dlog "<remote agent
directory>\logs\cli"          registration          advanced-register
registration-type=<Primary | Secondary>
is-db-agent=<true    |    false>    is-fam-agent=<false    |    true>
is-sp-agent=<false    |    true>    is-ad-agent=<false    |    true>
ragent-name=<remote agent name> site=mysite server-group="my server
group"     gw-ip=<gateway     IP     |     hostname>     gw-port=<443>
manual-settings-activation=<Automatic | Manual>
monitor-network-channels=<Both | Local> password=<secure>
```

The parameters are explained in the table at the end of the topic Silent Registration Parameter "Silent Registration Parameters" on page 135.

Alternatively, if you want to accept all the defaults, then execute the following command:

```
"<remote agent directory>\RemoteAgentCli.exe" [--dcfg "<remote agent
directory>" --dtarget "<remote agent directory>" --dlog "<remote agent
directory>\logs\cli"]   is-db-agent=<true   |   false>   registration
advanced-register ragent-name=<remote agent name> gw-ip=<gateway IP |
hostname>
```



Note: The parameters within the "[ ]" need to specified only if you installed the SecureSphere Agent in a directory different from the default directory.

If you want to change one of the other parameters, you can add it to the command (see the full command above). For example:

```
"<remote agent directory>\RemoteAgentCli.exe" [--dcfg "<remote agent
directory>" --dtarget "<remote agent directory>" --dlog "<remote agent
directory>\logs\cli"]   is-fam-agent=<true   |   false>   registration
advanced-register ragent-name=<remote agent name> gw-ip=<gateway IP |
hostname>
gw-port=<gateway management port>
```

4. Start the SecureSphere Agent by executing the following command:

```
sc start "SecureSphereRemoteAgent"
```

EXAMPLE: SILENTLY INSTALLING THE SECURESPHERE AGENT ON A WINDOWS SYSTEM

For example, the following commands install the SecureSphere Agent, silently register the SecureSphere Agent to the Gateway at IP address 10.10.10.10, and then start the SecureSphere Agent:

```
msiexec /i C:\Program Files\Imperva\RemoteAgent NOSCRIPT=true  /quiet
"C:\Program Files\Imperva\RemoteAgent\RemoteAgentCli.exe" --dcfg
"C:\Program Files\Imperva\RemoteAgent" --dtarget "C:\Program
Files\Imperva\RemoteAgent" --dlog "C:\Program
Files\Imperva\RemoteAgent\logs\cli" registration
advanced-register registration-type=Primary is-db-agent=true
is-fam-agent=false is-sp-agent=false ragent-name=MyAgent site=mysite
server-group="my server group" gw-ip=10.10.10.10 gw-port=443
manual-settings-activation=Automatic monitor-network-channels=Both
password=secure
sc start "SecureSphereRemoteAgent"
```

Installing the SecureSphere Agent Installation Manager on a Windows System Using the Standard Script

To install the SecureSphere Agent Installation Manager on a Windows system using the standard script:

1. Run the MSI installation file you downloaded as administrator.

   If you do not have administrator privileges, proceed as follows:

   - Open Windows Explorer and navigate to the MSI file (the installation file you saved in step 2 in Installing the SecureSphere Agent on a Windows System "Installing the SecureSphere Agent and Installation Manager on a Windows System" on page 131).
   - Shift-right-click the MSI file and select **Run as different user** from the menu.
   - In the **Run As** window, select **The Following User.**
   - Choose a user with administrator privileges.
   - Enter the password.
   - Click **OK**

   Otherwise, run the SecureSphere Agent Installation Manager installation file by executing the following command:

   ```
   msiexec /i "<agent installation manager full path\<package name.msi>"
   ```



Note: When you open a CLI, make sure that it is opened with administrator privileges.

Silent Registration Parameters

The following table lists and explains the parameters for silent registration.

Silent Agent Registration Parameters

Parameter	Description
Windows: `--dcfg "<remote agent directory>\RemoteAgent"`	`<remote agent directory>` is normally the same directory in which the SecureSphere Agent is installed.
non-Windows: `--dcfg <remote agent directory>/ragent/etc`	
Windows: `--dtarget "<remote agent directory>\RemoteAgent"`	
non-Windows: `--dtarget <remote agent directory>/ragent/etc`	
Windows: `--dlog "<remote agent directory>\RemoteAgent\logs\cli"`	
non-Windows: `--dlog <remote agent directory>/ragent/etc/logs/cli`	
`registration advanced-register`	Required.
`registration-type`	Specify "`Primary`" or "`Secondary`". See **Do you wish to register Remote Agent to a secondary gateway** as described in Registering the Remote Agent to a SecureSphere Gateway " Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141. **Default:** `Primary`
Windows, Solaris 10 and RHEL 5 only: `is-db-agent`	Specify `true` for database Remote Agents. **Default:** `true`
Windows, Solaris 10 and RHEL 5 only: `is-fam-agent`	Specify `true` for file Remote Agents. **Default:** `false`
Windows Only: `is-sp-agent`	Specify `true` for SharePoint Remote Agents. **Default:** `false`
Windows Only: `is-ad-agent`	Specify `true` for Active Directory SecureSphere Agents. **Default:** `false`

Parameter	Description
`ragent-name`	The name of the Remote AgentSecureSphere Agents, as it will appear in the SecureSphere GUI. See **Enter the SecureSphere Agent name** in Registering the Remote AgentSecureSphere Agent to a SecureSphere Gateway " Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141.
`site`	Specify the SecureSphere Agent's site in SecureSphere. If you specify `site`, then you must also specify `server group`. `site` is case-sensitive, embedded spaces are allowed (but you should then enclose the name in quotes, for example, "Big Site"), and leading and trailing spaces are not stripped out. **Default:** None
`server-group`	Specify the SecureSphere Agent's server group (within the site). If you specify `server-group`, then you must also specify `site`. `server-group` is case-sensitive, embedded spaces are allowed (but you should then enclose the name in quotes, for example, "Server Group A"), and leading and trailing spaces are not stripped out. You can enter the name of a non-existent server group, if you have configured SecureSphere appropriately. See Enabling Registration of an Agent with a Non-Existent Server Group on page 120. A server group with that name is created. **Default:** None
`gw-ip`	The IP address of the Gateway to which the SecureSphere Agents will be registered. See **Enter the Management Gateway listener IP address** in Registering the SecureSphere Agent to a SecureSphere Gateway

Parameter	Description
	" Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141.
`gw-port`	The management listener port number on the Gateway. See **Enter the Management Gateway listener port** in Registering the Remote AgentSecureSphere Agent to a SecureSphere Gateway " Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141. **Default:** `443`
`manual-settings-activation`	Specify `Manual` or `Automatic`. **Default:** `Automatic` See **Choose manual settings activation (configuration updates)** in Registering the Remote AgentSecureSphere Agent to a SecureSphere Gateway " Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141.
`password`	See **Enter the Gateway login password** in Registering the SecureSphere Agent to a SecureSphere Gateway " Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway" on page 141. **Default:** `secure`
`monitor-network-channels`	Specify `Local` or `Both`. The type of traffic to be monitored: • `Local` - local traffic only • `Both` - local and external traffic **Default:** `Both`
`tags`	This optional registration parameter applies only to

Parameter	Description
	SecureSphere Agent version 10.5 and later. Enter one or more existing tags to apply to the SecureSphere Agent. Separate multiple tags with commas. Do not insert spaces before or after commas. Add quotation marks (") before and after a tag name that includes spaces. For example, to apply a tag called *Backup exclusion,* enter: `tags="Backup exclusion"` To learn how to create a tag, see General Details Tab - Tags Section in the SecureSphere Agents chapter of the **SecureSphere User Guide.** An agent monitoring rule that applies to a tag that you enter will apply to the agent. To learn how to apply an agent monitoring rule to a tag, see Configuring SecureSphere Agent Monitoring Rules in the SecureSphere Agents chapter of the **SecureSphere User Guide**.

After Installing the SecureSphere Agent

This section presents issues related to post SecureSphere Agent installation and includes:

AIX Post Installation Information 139
Data Interface Discovery and Configuration 139

AIX Post Installation Information

If you have installed the SecureSphere Agent on a machine on which no SecureSphere Agent was previously installed, or if a version 8.5 or lower SecureSphere Agent was installed, then:

- If you want to monitor local DB2 shared memory traffic, you must restart all DB2 database instances after the first time you start the SecureSphere 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 SecureSphere Agent.

There is no need to reboot the machine.

Data Interface Discovery and Configuration

The Remote Agent does not automatically discover data interfaces for all OS/DB/interface type combinations, so in some cases you will have to manually configure the interfaces.

The table below lists the data interfaces automatically discovered by the Remote Agent, and those which the user must manually configure.

Automatic Data Interface Discovery

OS	Database	Interfaces
Automatic Discovery		
Unix-like	**Oracle**	TCP external
		TCP local
		IPC
		BEQ
	DB2	TCP external
		TCP Local
		shared memory
	Sybase	TCP external
		TCP local
Windows	**MSSQL**	TCP external
		TCP local
		MSSQL IPC (shared memory / named pipes)

OS	Database	Interfaces
Windows Itanium	**none**	none
Manually Configured		
Windows	**Oracle**	TCP external
		TCP local
		IPC
		BEQ
	DB2	TCP external
		TCP local
		shared memory Windows 2000/Itanium platforms not supported
	All Other Supported Databases	TCP external
		TCP local
Unix-like	**DB2**	TCP external
		TCP local
		shared memory
	All Other Supported Databases	TCP external
		TCP local

Contact your DBA for information about the data interfaces on your database server.

For more information on configuring data interfaces, see the **SecureSphere User Guide**.

First-Time Configuration Wizard

The configuration wizard guides you through the initial configuration of the Imperva agent. The configuration wizard starts automatically after the SecureSphere Agent finishes installing.

You should use the configuration wizard only for the first time configuration. You can later make changes to the configuration using the SecureSphere Agent Management Console. For more information, see SecureSphere Agent Management Console on page 148.

To run the configuration wizard again at another time:

1. Execute the following command:
   - **In non-Windows**: `<base dir>/ragent/bin/racli`

     The default `<base dir>` is `/opt/imperva`
   - **In Windows**: `<base dir>\RemoteAgent\StartCli.bat`

     The default `<base dir>` is `C:\Program Files\Imperva/`
2. Select option 1.

   The configuration wizard uses the following conventions:

Configuration Wizard Conventions

Convention	Meaning
<y>	confirm
<d>	discard and continue
<n>	continue
<s>	save
<q>	quit (discard un-saved settings)
<j>	jump to previous level
[value]	the default value to be used
<h>	help

The log file for the configuration wizard errors in non-Windows systems is:

SecureSphere Agent – `<base dir>/ragent/etc/logs/cli/cli.html`

SecureSphere Agent Installation Manager – `<base dir>/installer/etc/logs/cli/cli.html`

The default `<base dir>` is `/opt/imperva`

The log file for the configuration wizard errors in Windows systems is:

SecureSphere Agent – `<base dir>\RemoteAgent\logs\cli\cli.html`

SecureSphere Agent Installation Manager – `<base dir>\AgentInstallationManager\logs\cli\cli.html`

The default `<base dir>` is `C:\Program Files\Imperva\`

The configuration wizard will guide you through a series of questions in the order given below. If you are not certain about the configuration suggested by the configuration wizard, choose the default option. You can always reconfigure it later using the SecureSphere Agent management console. See SecureSphere Agent Management Console on page 148 for more information.

Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway

To complete the initial configuration wizard, you must register your agent to the SecureSphere Gateway.

Registration is the process by which the Remote Agent identifies itself to the Gateway. When registering the Remote Agent to the Gateway listener, the listener defines the listener port in the Remote Agent configuration file and knows from which Remote Agent to expect traffic.

You are given the choice of two registration options: quick (typical) registration, where most parameters are defined to their typical values, and advanced registration, where you must explicitly define each parameter.

If you decide to exit at this point, you can register later using the Remote Agent management console. See Remote Agent Management Console "SecureSphere Agent Management Console" on page 148 for more information.

Agent Registration Steps

Registration Step	Description
In a series of questions, you will be asked what type of traffic is to be monitored: • Database (DB) • File • SharePoint - Windows only • Active Directory (AD) - Windows only	The SecureSphere Agent is able to monitor all these kinds of traffic.
Enter the SecureSphere Agent name	Enter a name for the SecureSphere Agent. This name will be used in the SecureSphere GUI to identify the SecureSphere Agent. Enter alphanumeric characters.
Enter SecureSphere site name	Enter the name of the site to which to attach the SecureSphere Agent. Leave the site name empty if you are not sure of it at this point. You can always attach the SecureSphere Agent to a site later using the SecureSphere GUI. Note that the server group name is case-sensitive, embedded spaces are allowed, and leading and trailing spaces are not stripped out.
Enter the Remote Agent tags, separated by commas	This optional registration step applies only to SecureSphere Agent version 10.5 and later. This option is available only in advanced registration. Enter one or more existing tags to apply to the SecureSphere Agent. Separate multiple tags with commas. Do not insert spaces before or after commas. For example, to apply two tags called *Admin* and *Backup exclusion,* enter: `Admin,Backup exclusion` To learn how to create a tag, see General Details Tab - Tags Section in the SecureSphere Agents chapter of the **SecureSphere User Guide.** An agent monitoring rule that applies to a tag that you enter will apply to the agent. To learn how to apply an agent monitoring rule to a tag, see Configuring SecureSphere Agent Monitoring Rules in the SecureSphere Agents chapter of the **SecureSphere User Guide**.
Enter SecureSphere server group name	Enter the name of the server group (in the above site) to which to attach the SecureSphere Agent. Leave the server group name empty if you are not sure of it at this point or if you did not enter a site name. You can always attach the SecureSphere Agent to a server group later using the SecureSphere GUI. Note that the server group name is case-sensitive, embedded spaces are allowed, and leading and trailing spaces are not stripped out. You can enter the name of a non-existent server group, if you have configured SecureSphere appropriately. See Enabling Registration of an Agent with a Non-Existent Server Group on page 120. A server group with that name is created.

Registration Step	Description
Enter the Management Gateway listener IP address	Enter the Gateway management listener IP address, as defined in the SecureSphere Gateway listener configuration (see Managing SecureSphere Agents on page 79). This is the IP address with which the SecureSphere Agent registers, typically the SecureSphere Gateway's management IP address. You can enter the name of a non-existent server group, if you have configured SecureSphere appropriately. See Enabling Registration of an Agent with a Non-Existent Server Group on page 120. A server group with that name is created. **Note:** Bridge and sniffing interfaces cannot be defined as TCP listener interfaces.
Enter the Management Gateway listener port	The Gateway port used for registration. After successful registration, the listener configures the SecureSphere Agent configuration file with the high port used for the TCP tunnel, as defined on the Gateway when configuring the listener (see Managing SecureSphere Agents on page 79). Use 443 as the port, unless it has been changed through the Gateway configuration manager (`impcfg`).
Choose manual settings activation (configuration updates)	Manually activate the SecureSphere Agent settings. The following options are available: • **Manual**: The configuration changes performed using SecureSphere are manually approved by the user before they are applied to the Agent. • **Automatic**: All the configuration changes performed using SecureSphere are automatically applied to the SecureSphere Agent. **Default**: Automatic.
Monitor only local activity, or monitor both local activity and network traffic	**Note:** This parameter is relevant for database SecureSphere Agents only. If external traffic is monitored by a SecureSphere Gateway, the SecureSphere Agent should monitor only local traffic so as to prevent the SecureSphere Agent and the Gateway reporting the same traffic. The following options are available: • **Local**: Monitor only local traffic. • **Both**: Monitor both local and external traffic. When ignoring traffic on external data interfaces, SecureSphere automatically ignores new TCP data interfaces. This can be overridden manually in the **Settings** tab of the **Agent** window. For more information, see the **SecureSphere User Guide**.
Enter the Gateway login password	The password of the user "imperva" on the Gateway. Use "secure" as the password, unless this has been changed.
Do you wish to register the SecureSphere Agent to a secondary gateway	If you want to define a high availability configuration, then you must configure a secondary Gateway in addition to the primary Gateway. **Note:** The secondary Gateway must be in the same Gateway group as the primary Gateway. If it is not, the registration process will fail. To register the SecureSphere Agent to a secondary Gateway, you must go through this same configuration process on the secondary Gateway.

Registration Step	Description
Note: The next parameter are relevant only for the SecureSphere Agent Installation Manager, and you can later change them in the **Agent Installation Manager** tab in the **Agents** window.	
Download Directory	The directory to which the package distributed by Software Update will be downloaded.
Max Directory Size (MB)	The maximum size (in MB) allocated to **Download Directory**.
Bandwidth Limit (Kb/s)	The maximum bandwidth allocated to the installation package download process.

Upon successful registration, the following message appears: "The agent was successfully registered to Gateway."
If you receive an error message, see SecureSphere Agent Error Messages on page 155 for more information.

Uninstalling the SecureSphere Agent



Note: These instructions refer to uninstalling Version 10.0 and higher SecureSphere Agents. It does not include information about AS/400 and z/OS SecureSphere Agents.
For uninstalling a previous version, see the **SecureSphere User Guide** for that version.

This section includes:

Uninstalling the SecureSphere Agent on a non-Windows System 144
Uninstalling the SecureSphere Agent on a Windows System 145

Uninstalling the SecureSphere Agent on a non-Windows System



Note: Beginning with SecureSphere Agent version 10.0, it is not necessary to uninstall the SecureSphere Agent before installing a SecureSphere Agent. The only exception to this is when you want to re-install exactly the same version SecureSphere Agent that is already installed, in which case you must uninstall the SecureSphere Agent before installing it again.

To uninstall the SecureSphere Agent on non-Windows system:

1. Stop the SecureSphere Agent (see Starting and Stopping the SecureSphere Agent on page 146).
2. Execute: the following command:

   ```
   <base dir>/ragent/bin/uninstall
   ```

   where `<base dir>` is the directory in which the SecureSphere Agent is installed.
3. Follow the on-screen instructions.

To uninstall the SecureSphere Agent Installation Manager on non-Windows system:

1. Stop the SecureSphere Agent Installation Manager (see Starting and Stopping the SecureSphere Agent on page 146).
2. Execute: the following command:

   ```
   <base dir>/installer/bin/uninstall
   ```

   where `<base dir>` is the directory in which the SecureSphere Agent Installation Manager is installed.
3. Follow the on-screen instructions.

After Uninstalling the SecureSphere Agent on a non-Windows System

In general, you do not need to do anything after uninstalling the SecureSphere Agent, with the exceptions listed in the following paragraphs.

AIX

After Uninstalling a Version 9.0 or Higher SecureSphere Agent

You can re-install the same version without rebooting the database server. If you want to install a pre-version 9.0 SecureSphere Agent, you must reboot the database server.

After Uninstalling a Pre-version 9.0 SecureSphere Agent

The uninstall process will ask you to reboot the database server. If you plan to install version 9.0 or higher SecureSphere Agent, ignore the message. You do not have to reboot the database server.

EXAMPLE: AFTER UNINSTALLING A PRE-VERSION 9.0 SECURESPHERE AGENT

If you uninstall a version 8.5 SecureSphere Agent and plan to install a version 8.5 SecureSphere Agent, you must reboot the database server after the uninstall.

However, if you uninstall a version 8.5 SecureSphere Agent and plan to install a version 9.0 SecureSphere Agent, you do not have to reboot the database server, even though a message is displayed telling you that you must reboot.

Uninstalling the SecureSphere Agent on a Windows System

To uninstall the SecureSphere Agent on a Windows system:

1. Stop the SecureSphere Agent (see Starting and Stopping the SecureSphere Agent on page 146).
2. Using the Windows Add/Remove Program Control Panel applet, uninstall **Imperva SecureSphere SecureSphere Agent software**.

To silently uninstall the SecureSphere Agent on a Windows system:

1. Execute the following command:

```
msiexec /x SecureSphere Agent package full path>  /quiet
```



Note: When removing a SharePoint farm from being monitored by SecureSphere, after the uninstall process for all SharePoint agents, it is also recommended that you manually remove the Imperva web service (farm solution) from the SharePoint farm.

Upgrading the SecureSphere Agent

Beginning with version 10.0 SecureSphere Agents, to upgrade the SecureSphere Agent, install the new SecureSphere Agent. It is no longer necessary to uninstall any previous versions.

In Windows, you simply install the SecureSphere Agent, and if there is an existing SecureSphere Agent installed, it will be upgrade. In Unix, use the -u parameter in the installation command.

In both Windows and Unix, there is no need to re-register and upgraded SecureSphere Agent.



Note: For information regarding upgrading to a pre-version 10.0 SecureSphere Agent, see the **SecureSphere User Guide** for that version.

Starting and Stopping the SecureSphere Agent

This section reviews topics relating to the starting and stopping of the SecureSphere Agent.

After the initial configuration wizard completes successfully, you have the option of starting the SecureSphere Agent. If you wish to start the SecureSphere Agent at a different time, exit the configuration wizard and then start the SecureSphere Agent from either the SecureSphere Agent Management Console or from the command line.

For more information about the SecureSphere Agent Management Console, see SecureSphere Agent Management Console on page 148.



Note: The SecureSphere Agent cannot be started or stopped from the SecureSphere GUI, only from the SecureSphere Agent Management Console or from the OS command line.

This section reviews the following topics:

Starting and Stopping the SecureSphere Agent from the Management Console 146
Starting the non-Windows SecureSphere Agent from the Command Line 146
Stopping the non-Windows SecureSphere Agent from the Command Line 147
Starting the Windows SecureSphere Agent from the Command Line 147
Stopping the Windows SecureSphere Agent from the Command Line 147

Starting and Stopping the SecureSphere Agent from the Management Console

To stop, start or restart the SecureSphere Agent:

1. From the top level menu, select **Perform Actions (Start/Stop/Restart)**.
2. Choose one of the above options (**Start/Stop/Restart**).

Starting the non-Windows SecureSphere Agent from the Command Line

To start the SecureSphere Agent:

1. Execute one of the following commands:

```
<remote agent directory>/ragent/bin/rainit start
```

```
<remote agent directory>/ragent/bin/cli actions start
```

Stopping the non-Windows SecureSphere Agent from the Command Line

To stop the SecureSphere Agent:

1. Execute one of the following commands:

```
<remote agent directory>/ragent/bin/rainit stop
```

```
<remote agent directory>/ragent/bin/cli actions stop
```

Starting the Windows SecureSphere Agent from the Command Line

To start the SecureSphere Agent:

1. Execute the following command:

```
"<remote agent directory>\RemoteAgent\RemoteAgentCli.exe" actions start
```

To start the SecureSphere Agent Installation Manager:

1. Execute the following command:

```
"<remote agent directory>\AgentInstallationManager\RemoteAgentCli.exe" actions start
```

Stopping the Windows SecureSphere Agent from the Command Line

To stop the SecureSphere Agent:

1. Execute one of the following commands:

```
"<remote agent directory>\RemoteAgentCli.exe" actions stop
```

SecureSphere Agent Management Console

The SecureSphere Agent Management Console is a tool designed to help you perform additional actions relevant to the SecureSphere Agent, which are not available in the SecureSphere GUI.

From the menu it is possible to control the SecureSphere Agent (register/un-register, start, stop etc.), change agent settings and even troubleshoot.

This section describes how to use the SecureSphere Agent Management Console and includes the following information:

SecureSphere Agent Management Console Conventions 148
Starting the SecureSphere Agent Management Console 149
Registering the SecureSphere Agent to the Gateway 149
Activating Settings Manually 151
Agent Information Displayed in the Console 151
Agent Troubleshooting Using the Management Console 151

SecureSphere Agent Management Console Conventions

The SecureSphere Agent management console uses the following conventions:

<c>	confirm
<d>	discard and continue
<s>	save
<q>	quit (discard un-saved settings)
<j>	jump to previous level
<r>	jump to root menu (top level)
[value]	the default value to be used
A | D | C	this configuration item has been added (A), deleted (D) or changed (C)
Esc	exit command execution
<h>	help



Note:

- Configuration changes are not automatically saved. You must save them explicitly before exiting.
- Changes take effect only after the SecureSphere Agent is restarted.

non-Windows Agents

The log file for the SecureSphere Agent management console errors is:

`<base dir>/ragent/etc/logs/cli/cli.html`

The default `<base dir>` is `/opt/imperva`

Windows Agents

The log file for the SecureSphere Agent management console errors is:

<base dir>\RemoteAgent\logs\cli\cli.html

The default <base dir> is C:\Program Files\Imperva

Starting the SecureSphere Agent Management Console

To start the SecureSphere Agent Management console in a non-Windows system:

1. Run the following command:
   ./<base dir>/ragent/bin/racli
   The default <base dir> is /opt/imperva

To start the SecureSphere Agent Management console in Windows:

1. Run the following command:
   <base dir>\RemoteAgent\StartCli.bat
   The default <base dir> is C:\Program Files\Imperva
2. Choose 2 for Menu mode.

Registering the SecureSphere Agent to the Gateway

To register the Remote Agent to a listener on a SecureSphere Gateway:

1. Choose **Manage SecureSphere Agent Registration** from the top level menu.
2. Choose **Register the SecureSphere Agent to Gateway** and set the following parameters:

Parameter	Description
Choose the registration type	Select if the registration type is Primary or Secondary. When the connection with the primary Gateway is lost the Agent communicates with the secondary Gateway. If you choose secondary registration without doing primary registration first, then the registration fails immediately with an appropriate error message.
Enter the SecureSphere Agent name	Enter a descriptive name for the SecureSphere Agent. This is the name that will appear in the SecureSphere UI. Allowed values: alphanumeric characters, and the number of characters must be between 1 and 80.

Parameter	Description
Enter the SecureSphere Agent tags, separated by commas	This optional registration step applies only to SecureSphere Agent version 10.5 and later. This option is available only in advanced registration. Enter one or more existing tags to apply to the SecureSphere Agent. Separate multiple tags with commas. Do not insert spaces before or after commas. For example, to apply two tags called *Admin* and *Backup exclusion,* enter: `Admin,Backup exclusion` To learn how to create a tag, see General Details Tab - Tags Section in the SecureSphere Agents chapter of the **SecureSphere User Guide.** An agent monitoring rule that applies to a tag that you enter will apply to the agent. To learn how to apply an agent monitoring rule to a tag, see Configuring SecureSphere Agent Monitoring Rules in the SecureSphere Agents chapter of the **SecureSphere User Guide**.
Choose manual settings activation (configuration updates)	Enables manual activation of agent's settings. The following options are available: • **False**: All the configuration changes performed using SecureSphere are automatically applied to the Agent. • **True**: The configuration changes performed using SecureSphere are manually approved by the user before they are applied to the Agent. **Default**: False.
Choose to ignore external (TCP) interfaces	Enables ignoring the traffic that arrives from outside to the specific database in addition to the local traffic. In this case the Agent monitors all the traffic that is usually monitored by the Gateway. Here you need to decide if the default value is Enabled/Disabled.
Enter the Gateway listener IP address	Enter the Gateway listener IP address as defined in the SecureSphere Gateway listener configuration. This is the IP address that the SecureSphere Agent registers with. **Note:** Bridge and sniffing interfaces cannot be defined as listener interfaces.
Enter the Gateway listener port	This is the port used for registration. Upon successful registration, the Gateway configures the SecureSphere Agent with the listener high port used for the tunnel. Use port 443, unless this was changed on the Gateway (using the Gateway configuration manager).
Enter the Gateway login password	Use "secure" as password, unless this was changed on the Gateway (using the Gateway configuration manager). This is the password of user "imperva" on the Gateway.
Save pending changes	All changes must be confirmed and saved before registration continues. Note: All changes in the configuration take effect only after restarting the SecureSphere Agent.

At the end of this process, the SecureSphere Agent registers with the Gateway and the following message is displayed: **The Remote Agent was successfully registered to Gateway**.

If a different message appears see SecureSphere Agent Error Messages on page 155 for more information.

Upon successful registration, the Agent appears in the GUI, and further configuration can be done from there.



Note: If you remove a Gateway, then before you can re-register the agent to the Gateway, you must remove the secondary Gateway as well.

Activating Settings Manually

When the Manual Settings Activation option is enabled, see Registering the SecureSphere Agent to the Gateway on page 149, you need to activate manually the settings performed in the Agents window in the GUI. Once the configuration is done in the Agents window, you need to apply it manually in the Agent's console.

Before applying the settings, check if there are pending changes, see Agent Information Displayed in the Console on page 151.

To activate settings manually:

- From the top level menu, select **Activate Settings**.

Agent Information Displayed in the Console

The following information is displayed above the menus in the Console:

- **Release Number**: Agent's release number.
- **Registration Status**: Shows if the Agent is registered or not. The values are True - registered, False - not registered.
- **SecureSphere Agent Status**: The current status of the Agent, the values can be Stopped or Running.
- **Pending Configuration Update**: Indicates if there are configuration changes that should be manually activated, see Activating Settings Manually on page 151, the values are True/False.

Agent Troubleshooting Using the Management Console

The troubleshooting menu allows collecting logs, watching the full agent configuration and its counters.

To troubleshoot the SecureSphere Agent:

1. Choose "Troubleshooting" from the top menu.

The sub menu includes 4 options:

- Change Log Level
- Show Counters

Show Counters

This option displays the SecureSphere Agent user space counters, information which is useful for debugging, and is located in:

non-Windows

```
<base dir/ragent/etc/logs/ragent/ragent_log.htm.counter.html
```

Windows

```
<base dir>\RemoteAgent\logs\ragent\ragent_log.htm.counter.html
```

Counters include information on the SecureSphere Agent and OS activity. Example of such information: agent start time, OS CPU usage, agent user space cpu usage, number of packets that were received from interface and so on. Counter information is meaningful to the Imperva support team and should be printed if requested.

Working with High Availability

To work in the high availability mode, agents can be registered to two Gateways. This is the preferred option.



Note: In High Availability configurations, both Gateways must be in the same Gateway group.

If you are using an older version of agents, you can achieve high availability by having two Gateways configured with the same virtual IP address to which the Agent is reporting to. SecureSphere allows you to configure two listeners in high availability mode. Using the VRRP protocol, it is possible to configure the listeners to use one virtual IP, which is used as the TCP tunnel end point. One of the listener IP addresses acts as a master and processes the traffic, while the other IP address acts as backup. If the master fails, its role is then taken by the backup. This configuration ensures that the SecureSphere Agent traffic is always processed and reported to the Management Server.



Note: The SecureSphere Agent buffering feature ensures that traffic is not lost if the SecureSphere Agent cannot communicate with the Gateway listener.

To complete the configuration, perform the following tasks:

1. Configure the Gateway listeners to use VRRP (see Configuring the Gateways to Operate in the HA Mode with Agents on page 152).
2. Configure the SecureSphere Agent to register with both Gateways (see Configuring the SecureSphere Agent to Operate in the HA Mode on page 154).

Configuring the Gateways to Operate in the HA Mode with Agents

To configure the Gateways:

1. Configure a listener on the SecureSphere Gateway. See Configuring Listeners on page 122 for more information.
2. To the question "Do you want to use VRRP for this listener?", enter "y".
3. Answer the remaining the questions according to the table below:

Question	Description
Virtual instance name	The name of the VRRP circuit, which must be identical for both Gateways. Permitted characters are alphanumeric and underscore.
Virtual IP address	The virtual address for VRRP, which must be identical for both Gateways.
Virtual IP mask	The virtual IP mask, which must be identical for both Gateways.
Virtual router ID	The ID of the VRRP circuit, which must be identical for both Gateways. This must be a number between 1 and 255.
Virtual router mode	The virtual router mode MASTER or BACKUP. Only one of the Gateways is assigned the MASTER status.
Enable SSL	Set if the SecureSphere Agent will send its data encrypted. Possible value: y | n



Note: You must use the same listener port on both Gateways. See Configuring the SecureSphere Gateway Before Installation on page 122.

To define a VRRP agent related route on the Gateways:

1. SSH to the Gateway.
2. Login as user secure.
3. Select **Manage the SecureSphere gateway**.
4. Select **Manage remote agents**.
5. Select **Manage remote-agent related routes**.

Adding Routes

Option	Description
Will this be a virtual route, belonging to one of them?	Choose yes. The route will be associated with the Virtual IP. Possible value: y| n
Which virtual instance	Enter the virtual instance name to which the route will apply.
Type	Define whether this route is per subnet or specific to host. Possible value: net | host Enter "host" unless you want the route to be valid for the whole network.
Address	Available only when Type host is selected. Enter the IP address of the DB host.
Network	Available only when Type net is selected. The IP address of the network base on the network subnet. For example DB host IP address is 192.168.10.10 and its subnet mask 255.255.0.0, the net IP address will be 192.168.0.0.
Subnet mask	Available only when Type net is selected. The subnet mask of the network. Based on the example above net subnet mask will be 255.255.0.0
Gateway	Specify the default Gateway IP address which is used for the listener. The default Gateway IP must be from the listener subnet. If the listener IP address is the management IP address, you can choose a default Gateway from the management subnet.
Device	Specify specific Gateway physical interface to use or Enter for none. If none is selected, the best available interface is selected when routing.

Deleting Routes

Option	Description
Delete route	List of available routes is presented. Choose the route you wish to delete.

Agent routes are executed and added automatically when Gateway starts and are deleted automatically when Gateway is stopped. The routes are kept in the Gateway `bootstrap.xml` file.

Configuring the SecureSphere Agent to Operate in the HA Mode



Note: This section is relevant only for pre-version 7.0 SecureSphere Agents.

Configure the SecureSphere Agent according to the configuration guides outlined throughout this document. When done, register the SecureSphere Agent with both of the version 6.0 Gateways.

To configure the SecureSphere Agent:

1. Configure the SecureSphere Agent.
2. Save the configuration.

3. Register the SecureSphere Agent with primary Gateway private listener IP (see Registering the SecureSphere Agent to the Gateway on page 149).
4. Register the SecureSphere Agent again, now with secondary Gateway private listener IP (see Registering the SecureSphere Agent to the Gateway on page 149).
5. Start the SecureSphere Agent (see Starting and Stopping the SecureSphere Agent on page 146).
6. If the SecureSphere Agent registers with a listener that uses VRRP, the Gateway updates the SecureSphere Agent configuration file with the virtual IP address, as the TCP tunnel destination IP address.

Diagnostic Tools

This section includes the following information:

- SecureSphere Agent Logs on page 155
- SecureSphere Agent Error Messages on page 155
- Maintenance Tasks on page 156
- SecureSphere Agents in a Hypervisor (Virtualized) Environment on page 156

SecureSphere Agent Logs

The SecureSphere Agent maintains several logs.

non-Windows

The logs are located in directories under `<base dir>/ragent/etc/logs`.

The default `<base dir>` is `/opt/imperva`

Windows

The logs are located in directories under `<base dir>\ragent\etc\logs`.

The default `<base dir>` is `C:\Program Files\Imperva`

For further information on changing the log level and logger directory for each monitor individually, see Show Counters on page 151.

SecureSphere Agent Error Messages

If the remote SecureSphere Agent fails to register to the SecureSphere Gateway, the SecureSphere Agent management console displays one the error messages listed in the table below.

Additional information is available in the SecureSphere Agent Management Console log file (see SecureSphere Agent Logs on page 155)

Errors and Possible Causes

Error	Possible Cause
"Unregistration/Registration failed! - failed to initialize HTTP client."	This message indicates a failure to initialize an HTTP client on the db host.
"Unregistration/Registration failed! - failed to send/receive unregistration/registration data."	This message indicates that the SecureSphere Agent failed to send or receive the registration data to the SecureSphere Gateway. Check the connectivity between the DB host and the Gateway listener as follows: `telnet` to the listener IP address on port 443 (unless changed through the Gateway management console) and check if your listener accepts traffic on it (blank screen appear).

Error	Possible Cause
"Unregistration/Registration failed! - failed to send/receive authorized unregistration/registration data."	This message indicates failure to send/receive authorized data.
"Unregistration/Registration failed! - bad password."	The password for the "Imperva" user on the Gateway is incorrect. The default password is "secure". The user can change this password using the Gateway's configuration management.
"Unregistration/Registration failed! - missing registration/unregistration response data from the Gateway."	An empty response received from the Gateway.

Maintenance Tasks

As a rule the SecureSphere Agent does not require day-to-day maintenance. The SecureSphere Agent management console allows you to control buffered files storage size and directory through the global settings menu. For more information, see SecureSphere Agent Management Console on page 148.

SecureSphere Agents in a Hypervisor (Virtualized) Environment

This section describes the issues arising when the SecureSphere Agent is running in a hypervisor, for example, under VMware. The following issues are reviewed:

- If the MAC Address Changes on page 156

If the MAC Address Changes

You should configure the virtual NICs with fixed MAC addresses. However, if this is not feasible, then when the hypervisor changes the MAC address, you will have to re-register the SecureSphere Agent.

To re-register a SecureSphere Agent after its MAC address changes:

1. Unregister the SecureSphere Agent.
2. Delete the SecureSphere Agent from the workbench.
3. Re-register the SecureSphere Agent.

Prerequisite Tests for non-Windows Agents

The tests listed below are performed as part of the pre-install script. The installation script will not install the SecureSphere Agent if any of these tests fails.

The following section list the expected results of each of the tests for each platform.

Pre-Install Tests

Test ID	Test Name
1	OS compatibility
2	OS version
3	Platform compatibility
4	Kernel patch level
5	Kernel CPUs
6	Root volume
7	Disk space
8	Root permissions
9	Dependencies
10	Package instance
11	Executable instance
12	Driver instance
13	Temporary directory free space
14	Zone (Solaris)

It is possible to override these tests, that is, it is possible to ignore the results of a specific test. In this case, failure of the test will not prevent the SecureSphere Agent's installation.

For example, one of these tests determines whether the Imperva SecureSphere Agent is already running by searching for a process named `ragent`. If a process with that name, unrelated to Imperva, happens to be running, then the SecureSphere Agent will not be installed unless that test is overridden.

You should address the issues raised by the test by correcting the problem, for example, by providing the necessary disk space. If necessary, contact Imperva support.

Solaris Pre-Install

Test Name	Test | Test Result
OS compatibility	SunOS
OS version	5.8/5.9/5.10
Minimum kernel patch level	Solaris 8 –108528-23 (issued on July 28,2003) Solaris 9 –112233-12 (issued on April 21, 2004) Solaris 10 –112233-12 (issued on April 21, 2004) **Note:** To determine the installed patch level, execute the following command: `uname –a`
Platform compatibility	sparc or x86_64
Root volume	Check that root volume exists. For example, if the specified root directory is `/opt/imperva`, check that `/opt` exists.
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if the specified root directory is `/opt/imperva`, check free space in `/opt`.
Root permissions	The user who installs and runs and runs the SecureSphere Agent must belong to user group with root privileges.
Libraries Dependencies	not relevant
Executable instance	Check that there is no SecureSphere Agent running process or existing installed package.
Driver instance	Check there is no SecureSphere Agent module loaded in the kernel.
Temporary directory free space	Check that the `/var/tmp` directory free space is at least twice the size of the package (`bsx`) file.

Linux Pre-Install

Test Name	Test | Test Result
OS compatibility	'uname-s' == Linux
OS version	2.4/2.6
Kernel patch level	smp smp-hugemem smp-pae
Platform compatibility	x86_64 i386
Root volume	Check that root volume exists. For example, if specified root directory is `/opt/Imperva` check that `/opt` exists
32-bit libc libraries	The glibc.i686 library is required.

Test Name	Test | Test Result
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if specified root directory is `/opt/imperva` check free space in `/opt`

Root permissions	The user who installs and runs the SecureSphere Agent must belong to user group with root privileges. For example,
	`uid=1(other) gid=1(other)`
	`groups=1(other),0(root),2(bin),3(sys)`

Libraries Dependencies	With Redhat 6 only, checks RHEL 6 64-bit machines that glibc for 32-bit is installed.
Executable instance	Check that there is no SecureSphere Agent running process or existing installed package.
Driver instance	Check that the following command returns an empty string. `lsmod | grep krg`
Temporary directory free space	not relevant

HP-UX Pre-Install

est Name	Test | Test Result
OS compatibility	HP-UX
OS version	11.11/11.23/11.31
Kernel patch level	not relevant
Platform compatibility	PA-RISC/Itanium
Root volume	Check that root volume exists. For example, if the specified root directory is `/opt/imperva`, check that `/opt` exists.
Disk space	Check that the sum of package file sizes is smaller than root volume directory free space. For example, if the specified root directory is `/opt/imperva`, check the free space in `/opt`.
Root permissions	The user who installs and runs the SecureSphere Agent must belong to user group with root privileges.
Libraries Dependencies	For non- kernel based agents the `nettl` executable must exist. From release 6.0.2.36 all HP-UX agents are kernel based.
Executable instance	Check that there is no SecureSphere Agent running process or existing installed package.
Driver instance	Check that there is no SecureSphere Agent driver instance running.
Temporary directory free space	Check that the `/var/tmp` directory free space is greater than package size.

AIX Pre-Install

Test Name	Test | Test Result
OS compatibility	AIX

Test Name	Test | Test Result
OS version	5.2/5.3/6.1
Kernel patch level	The agent will not work with `bos.rte.libc` prior to 5.3.0.50, which is automatically installed by the 5300-05 kernel patch. To view the current value of `bos.rte.libc`, execute the following command: `lslpp -h bos.rte.libc`
Platform compatibility	powerpc32/64
Root volume	Check that root volume exists. For example, if the specified root directory is `/opt/Imperva`, check that `/opt` exists.
Disk space	Check that the sum of the package file sizes is smaller than root volume directory free space. For example, if the specified root directory is `/opt/imperva` check the free space in `/opt`
Root permissions	The user who installs and runs the SecureSphere Agent must belong to user group with root privileges.
Libraries Dependencies	The `libpthread` shared library must exist.
Executable instance	Check that there is no SecureSphere Agent running process or existing installed package.
Driver instance	Check that there is no SecureSphere Agent driver instance running.
Temporary directory free space	Check that the `/var/tmp` directory free space is greater than package size.

Supported Interfaces for the Gateway Listener

In typical installations, the listener is configured with the Gateway management IP address and uses the Gateway management physical interface. The listener can be configured on other interfaces as well.

For example, an organizational security policy does not allow DB hosts to communicate with the Gateway management IP / interface. The Gateway management IP is on the OOB network and connects only to the Management Server. It is required to use another physical interface for the listener. To comply with the requirement, you can use the LAN interface of the Gateway.

The table below provides detailed information about listener per physical interface combined with appliance mode.

Interfaces Supported in Listeners

GATEWAY MODE / INTERFACE	TCP
Bridge / data interfaces	X
Bridge / alternate management interface	V
Bridge / management interface	V
Sniffing / data interfaces	V – when data interface is not defined as sniffing.
Sniffing / alternate management interface	V – when not defined as sniffing interface.
Sniffing / management interface	V

Terminology:

Data interface – non on-board interface, also known as a Quad card or Silicom card.

Alternate management interface – also known as LAN interface. A secondary on-board interface which is not used as the management interface.

Management interface – on board interface used for management.

X – not supported

V – supported

Advanced Agent Configuration

This section includes the following information:

Working with a NATed Listener 161
Working with Multiple Oracle Instances 164
Monitoring Solaris Zones Using SecureSphere Agents 165
Monitoring MySQL Traffic 165
Working with DAC (Dedicated Administrator Connection) 165

Working with a NATed Listener

Depending on the topology, the configured Gateway listener IP address is sometimes NATed by a firewall (or other device) situated between the database server and the Gateway. When working with a NATed listener or when a firewall is present, some additional configuration is required.



Note: If the Gateway is NATed, then the agent's `bootstrap.xml` and `ctrl.xml` files are updated with the internal IP address.

Communication to and from the listener NAT must be allowed through the firewall. This includes the listener IP address, the listener high port and the listener registration port (usually 443).

Working with a NATed Listener in Non-Windows Environments

After registering the SecureSphere Agent with the Gateway, the Gateway configures the SecureSphere Agent configuration files `<base dir>/ragent/etc/bootstrap.xml` and `<base dir>/ragent/etc/ctrl.xml` with the IP address of the listener. If NAT is used for the listener IP address, this information must be edited with the NAT IP address as follows.

1. Successfully register the SecureSphere Agent with the Gateway (see Registering the SecureSphere Agent to the Gateway on page 149).
2. Backup (copy) the SecureSphere Agent configuration files `<base dir>/ragent/etc/bootstrap.xml` and `<base dir>/ragent/etc/ctrl.xml`.
3. Edit the SecureSphere Agent configuration files `<base dir>/ragent/etc/bootstrap.xml` and locate the tag `<data-tunnel>`. Below this tag search for `<gw-ip>`, which includes the listener real IP address.
4. Replace the IP address with the NAT IP address.
5. Make the same change in the `<base dir>/ragent/etc/ctrl.xml` file.

EXAMPLE:

Given the following information:

- The real listener IP address is 1.2.3.4
- The listener port is 5678
- The listener NAT IP address is 11.12.13.14

The configuration files `<base dir>/ragent/etc/ragent.xml` and `ctrl.xml` will at first look like this:

```
<data-tunnel>
    <gw-ip>1.2.3.4</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
    <registered>true</registered>
   </data-tunnel>
```

After the change, the configuration files will look like this (the changed portion is shown here in bold):

```
<data-tunnel>
    <gw-ip>11.12.13.14</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
    <registered>true</registered>
   </data-tunnel>
```

Working with a NATed Listener in Windows Environments

After registering the SecureSphere Agent with the Gateway, the Gateway configures the SecureSphere Agent configuration files `<base dir>\RemoteAgent\bootstrap.xml` and `<base dir>\RemoteAgent\ctrl.xml` with the IP address of the listener. If NAT is used for the listener IP address, this information must be edited with the NAT IP address as follows.

1. Successfully register the SecureSphere Agent with the Gateway (see Registering the SecureSphere Agent to the Gateway on page 149).
2. Backup (copy) the SecureSphere Agent configuration files `<base dir>\RemoteAgent\bootsrap.xml` and `<base dir>\RemoteAgent\ctrl.xml`.
3. Edit the SecureSphere Agent configuration file `<base dir>\RemoteAgent\bootstrap.xml` and locate the tag `<data-tunnel>`. Below this tag search for `<gw-ip>`, which includes the listener real IP address.
4. Replace the IP address with the NAT IP address.
5. Make the same change in the `ctrl.xml` file.

EXAMPLE:

Given the following information:

- The real listener IP address is 1.2.3.4
- The listener port is 5678
- The listener NAT IP address is 11.12.13.14

The configuration files `<base dir>\RemoteAgent\bootsrap.xml` and `<base dir>\RemoteAgent\ctrl.xml` will at first look like this:

```
<data-tunnel>
    <gw-ip>1.2.3.4</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
   </data-tunnel>
```

After the change, the configuration files will look like this (the changed portion is shown here in bold):

```
<data-tunnel>
    <gw-ip>11.12.13.14</gw-ip>
    <gw-port>5678</gw-port>
    <gw-ssl>true</gw-ssl>
    <protocol>TCP</protocol>
   </data-tunnel>
```

Working with Multiple Oracle Instances



Note: The SecureSphere Agent automatically discovers all the Oracle servers on a DB host and creates the required data interfaces. This section is relevant only if for some reason you want to configure a data interface.

A DB host configuration may include multiple Oracle servers installed. In such cases there will be multiple BEQ/IPC adapters, each with a unique path to the executable. You might want to only monitor specific adapters.

As an example, consider BEQ. For each of the databases installed there will be a BEQ adapter configured with each PROGRAM parameter pointing to a different full path to the Oracle executable. `$ORACLE_HOME` path is specific for each installation, but the executable name is the same - `Oracle`.



Note: When you configure the SecureSphere Agent to add a local Oracle monitor, you must enter the monitor service name. Service name in the SecureSphere Agent terminology is the BEQ PROGRAM parameter value, or if you configure IPC, its KEY parameter value. The SecureSphere Agent matches service name as a suffix.

If you would like the SecureSphere Agent to monitor all BEQ processes on the DB host, specify `Oracle` as the service name, which is also the value suggested by the SecureSphere Agent Management Console**.** However if you want to monitor only a specific BEQ adapter, then specify the full path or the suffix that makes it unique.

The same concept applies to IPC if its names are unique.

In some cases the `tnsnames.ora` file may not include the above information. This does not mean that no Bequeath adapter is configured. There is always a default Bequeath adapter configured pointing to the "oracle" executable. To find more details about the relevant instance you can examine the `listeners.ora` file under the `$ORACLE_HOME/network/admin/` directory.

EXAMPLE:

Below is a typical `tnsnames.ora` configuration file with TCP, BEQ and IPC configuration. The parameters relevant to the SecureSphere Agent configuration are in bold.

```
ORCL =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl)
    )
  )

IPC =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = orcl))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = orcl)
    )
  )
```

```
ORA920BEQ =
   (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL =
BEQ)(PROGRAM=/export/home/Oracle/OraHome1/bin/Oracle")
    (argv0=beq920)
      (args='(DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=BEQ)))')
      (envs='Oracle_HOME=/export/home/Oracle/OraHome1/,ORACLE_SID=orcl')
      )
     )
)
```

Monitoring Solaris Zones Using SecureSphere Agents

In the Solaris Zones architecture, all traffic passes through the global zone. When installing SecureSphere Agent in a Solaris zones configuration, it must be installed in the global zone only. From the global zone, the agent monitors access to databases in all zones.

When monitoring TCP traffic the zones are differentiated using the IP address. To monitor traffic from the specific zone, configure the correct IP address in the TCP data interface. For more information, see the **SecureSphere User Guide**.

When monitoring Oracle IPC or Oracle BEQ, the zone name should be added as a prefix to the Server Path parameter using the ':' separator.

For example: `zone1:/opt/oracle/product`.

Global zone should not be added as prefix, regardless if zones are enabled or not on the machine.

For discovered interfaces the relevant zone is reported as the property "Zone" (see Monitoring Solaris Zones Using SecureSphere Agents on page 165).

Monitoring MySQL Traffic

By default, the MySQL Unix clients connect to the MySQL database over a Unix domain socket. In order for the SecureSphere Agent to monitor this type of connection, this traffic must be redirected to the loopback interface.

To redirect MySQL traffic to the loopback interface:

1. Open the MySQL configuration file with a text editor.
   The default MySQL configuration file is `/etc/my.cnf`
2. In the `[client]` section, add the following line:

   ```
   protocol=TCP
   ```

3. Save the file.
4. Restart the MySQL server.

Working with DAC (Dedicated Administrator Connection)

When working with DAC, the MSSQL service listens locally on an additional port, by default locally only. Usually the service uses the port following the default MSSQL port, that is, 1433. If the port already in use, it will use a different port.



Note: To determine the additional local port on which the sql service is listening, use the following command:

```
netstat –anb
```

To support monitoring of DAC traffic:

1. Configure the DAC service port in the SecureSphere GUI under the service ports definitions (**Setup** > **Sites** > **Service** > **Definitions** tab > **Ports**.
2. Configure the agent to monitor the loopback interface.

Command Line Scripting Language



Note: This section is aimed at advanced users which know how to use SecureSphere Agent and scripting.

The Imperva SecureSphere Agent provides a scripting language to configure the SecureSphere Agent. This capability allows you to install and register agents using software distribution tools in large environments.

The SecureSphere Agent command line accepts input from a file with script commands to automatically configure the SecureSphere Agent.

This section includes the following information:

Conventions for Command Line Scripting 166
Syntax for Command Line Scripting 167

Conventions for Command Line Scripting

- You can see all the options using the tab key.
- Options are equivalent to the SecureSphere Agent Management Console menus.
- <TAB> lists all options and complete the command when the command prefix is typed.
- After completing the first word in the command, <TAB> will again show you all possible options.
- Save is perform automatically when completing a command, in contrast to the SecureSphere Agent management console mode (mode menu).
- Enter `exit` to exit the shell.

To start the command line in scripting shell, do one of the following:

non-Windows:

1. Execute the following command:

```
.<base dir>/ragent/bin/racli shell
```

The default `<base dir>` is `/opt/imperva`

Windows:

2. Execute the following command:

```
<base dir>\RemoteAgent\StartCli.bat
```

The default `<base dir>` is `C:\Program Files\Imperva\`

3. Choose option 3 Shell Mode.

4. Execute the following command:

```
RemoteAgentCli.exe -mode shell -dcfg  "C:\Program
Files\Imperva\RemoteAgent" -dlog "C:\Program
Files\Imperva\RemoteAgent\logs" -dtarget "C:\Program
Files\Imperva\RemoteAgent"
```

Syntax for Command Line Scripting

non-Windows

Command line shell options are equivalent to the SecureSphere Agent management console elements. This section discusses example configuration only. It does not list full menu of the available operations. Below you will find examples. See SecureSphere Agent Management Console on page 148 for details on the meanings of these elements.

Pressing <TAB> at the dbagent> shell prompt will display all available options:

```
dbagent>
  registration: Manage Agent Registration
  actions: Perform Actions (Start/Stop/Restart)
  trouble-shooting: Trouble Shooting
  shell-script: Read shell script from an input file.
```

Remember to register and start the SecureSphere Agent if needed.

If my file name and location is **/**tmp/myconfigurationscript, then the command is:

```
dbagent> shell-script directory=<The script file directory> file=<The
script file name>
dbagent>  shell-script directory=/tmp file=myconfigscript
```

To run it automatically from a script, use the following command:

```
<base dir>/ragent/bin/cli -mode <shell/menu/script> -dcfg <cfg-dir-path>
   -dlog <log-dir-path> -dtarget <target-dir-path> <params>
```

Option	Description
-dcfg	The path to the cli.xml file. When the default installation is used, the path is /opt/imperva/ragent/etc
-dlog	The log directory. When the default installation is used, the log directory is /opt/imperva/ragent/etc/logs
-dtarget	The target directory for the SecureSphere Agent configuration file ragent.xml When the default installation is used, the target directory is /opt/imperva/ragent/etc

```
.<base dir>/ragent/bin/cli -dcfg /opt/imperva/ragent/etc
    -dlog /opt/imperva/ragent/etc/logs
    -dtarget /opt/imperva/ragent/etc  shell-script directory=/tmp
    file=myconfigscript
```

Windows

Command line shell options are equivalent to the SecureSphere Agent management console elements. This section discusses an example configuration only. It does not list full menu of the available operations. See SecureSphere Agent Management Console on page 148 for details on the meanings of these elements.

Pressing <TAB> at the > shell prompt will display all available options:

```
>
  registration: Manage Agent Registration
  actions: Perform Actions (Start/Stop/Restart)
  trouble-shooting: Trouble Shooting
  shell-script: Read shell script from an input file
```

Remember to register and start the SecureSphere Agent if needed.

If `my file name and location` is `\temp\myconfigurationscript`, then the command is:

```
> shell-script directory=<The script file directory>
   file=<The script file name>
> shell-script directory=\temp file=myconfigscript
```



Note: Use the `ListPcapDevices.exe` tool, available from the Imperva FTP server under the agent installation directory, to get the names of the network interfaces.

If you would like to run it automatically from a script, use the following command:

```
<base dir>\RemoteAgentCli.exe -mode <shell | menu | script>
-dcfg <cfg-dir-path> -dlog <log-dir-path> -dtarget <target-dir-path>
<params>
```

Option	Description
`-dcfg`	The path to the `cli.xml` file. When the default installation is used, the path is `C:\Program Files\Imperva\RemoteAgent`
`-dlog`	The log directory. When the default installation is used, the log directory is `C:\Program Files\Imperva\RemoteAgent\logs`
`-dtarget`	The target directory for the SecureSphere Agent configuration file `bootsrap.xml` When the default installation is used, the target directory is `C:\Program Files\Imperva\RemoteAgent`

For example, if you have a script (see previous example) to run under the command line, execute:

```
<base dir>\RemoteAgentCli.exe -dcfg "C:\Program
Files\Imperva\RemoteAgent"
-dlog "C:\Program Files\Imperva\RemoteAgent\logs"
-dtarget "C:\Program Files\Imperva\RemoteAgent" shell-script
directory=\temp
file=myconfigscript
```



Note: The path used must be enclosed in double quotes.

CHAPTER 6

Gateways

This section describes configuration of SecureSphere Gateways, and includes the following:

Configuring Gateways and Gateway Groups 170
Gateway Groups 176
Exporting Technical Information from Gateway and Onebox 187

Configuring Gateways and Gateway Groups

SecureSphere Gateways monitor traffic, enforce policies and send events to the SecureSphere MX.

A Gateway's MX is defined during the Gateway's initial configuration, using `impcfg`.



Note: When a Gateway is registered to an MX, the Gateway sends the MX information about its network interfaces, and users may configure the Gateway on the basis of that information. If any of the Gateway network interfaces is deleted or removed, the MX's Gateway configuration based on the deleted interface becomes invalid. The user must then either restore the network interface on the Gateway or modify the Gateway configuration on the MX accordingly.

For more information, see Configuring a Gateway.

You can configure Gateways and Gateway groups, as follows:

Gateways

Creating a Gateway means creating a MX-Gateway relationship, that is, specifying that a Gateway is managed by this MX (the MX that the SecureSphere GUI is running on). This is done using `impcfg`.

For more information, see Configuring a Gateways and Gateway Groups "Configuring Gateways and Gateway Groups" on page 170.

To view a Gateway:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway. The Gateway's details are displayed in the **Gateway Details** tab.

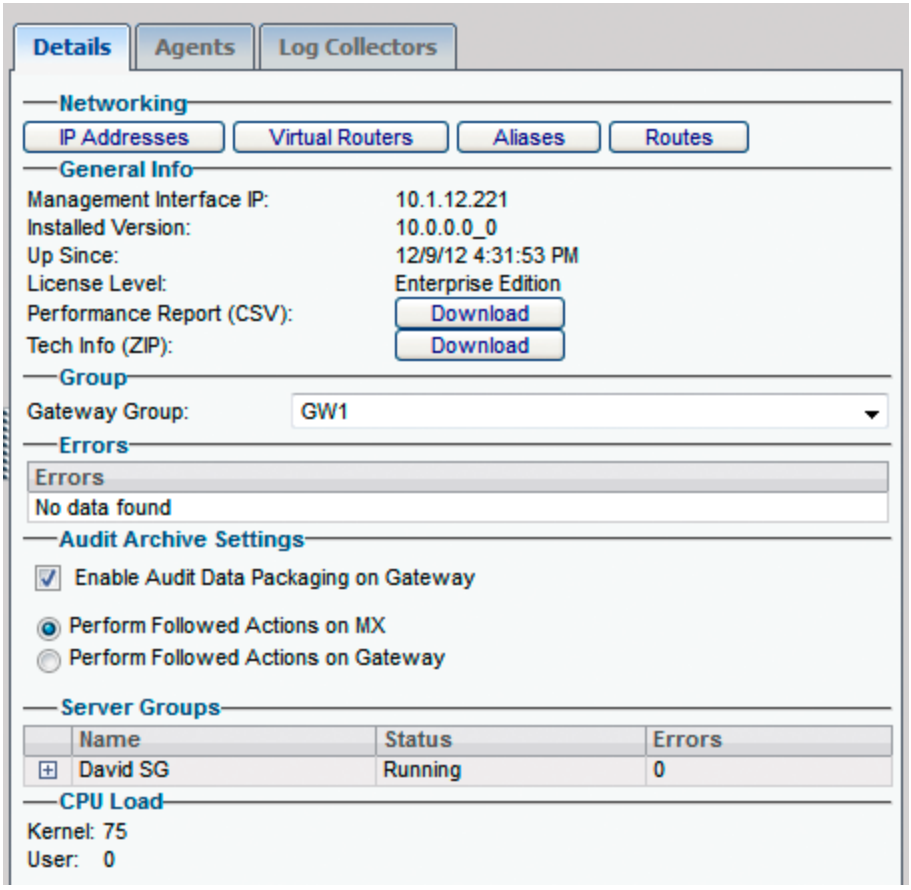


Figure 44: Gateway Details tab

Gateway Details

Details Tab - General Info

Field	Description
Management Interface IP	The IP address of the Gateway's management interface.
Installed Version	The version of SecureSPhere currently installed on this Gateway.
Up Since	The date and time since which the Gateway has been continuously running.
License Level	The Imperva license level (Enterprise).
Performance Report CSV	Click Download to export the Gateway's statistics to a CSV file.
Tech Info (ZIP)	Click Download to export Gateway or one-box get-tech-info to a zip file. For more information see Exporting Technical Information from Gateway and Onebox on page 187.

Details Tab - Group

Field	Description
Gateway Group	The name of the Gateway group to which this Gateway belongs. To move the Gateway to another group, select the group from the dropdown list. **Note:** When you move a Gateway from one Gateway group to another, the configurations of any DB Agents running on that Gateway will be lost and you will have to re-enter the configuration data (in **Main** > **Setup** > **Agents**).

The following section displays a read-only list of the errors reported for this Gateway.

Detail Tab - Errors

Field	Description
Errors	A description of the error, for example, "Minimum disk space reached, data is lost."

The following section displays options related to audit archive data generated on the Gateway.

Detail Tab -Audit Archive Settings

Option	Description
Enable Audit Data Packaging on Gateway	If this option is enabled, audit data is archived by the Gateway. For more information, see Configuring Archiving per Gateway on page 175. If this option is not enabled, audit data is archived by the MX.
Perform Followed Actions on MX	If the Enable Audit Data Packaging on Gateway option is enabled, a Followed Action defined for the archiving will be performed by the MX.
Perform Followed Actions on Gateway	If the Enable Audit Data Packaging on Gateway option is enabled, a Followed Action defined for the archiving will be performed by the Gateway. The only action interfaces that can be performed by the Gateway are the following: • SCP Archive • FTP Archive • Audit System Log • Gateway System Log • IP Block • User Block • Session Block If the Followed Action includes other action interfaces, they are performed by the MX.

The following table displays a read-only list of the server groups which this Gateway protects.

Detail Tab - Server Groups

Field	Description
Name	The name of the server group.
Status	The status of the server group (for example, "Running").
Errors	The number of errors for the server group. Expand the server group to display a list of the errors.

The following table the CPU load on the server.

Details Tab - CPU Load

Field	Description
kernel	The CPU load of the kernel mode module.
user	The CPU load of the user mode module.

SecureSphere Agent Details in the Gateways Window



Note: When you move a Gateway from one Gateway group to another (**Main** > **Setup** > **Gateways**), the configurations of any DB Agents running on that Gateway will be lost and you will have to re-enter the configuration data.

For each pre- version 7.0 SecureSphere Agent which sends events to the Gateway, the following data is displayed.

Agents Tab in the Gateways Window

Field	Description
Name	The name of the SecureSphere Agent.
Status	The status of the SecureSphere Agent (for example, "Running").
IP	The IP address of the database server on which the SecureSphere Agent is running.
Last Seen	The date and time of the last event received from the SecureSphere Agent.
Throughput	The SecureSphere Agent's throughput.
Conn / Sec	The number of connections per second handled by the SecureSphere Agent.

For information about SecureSphere Agent, see the SecureSphere Agents chapter in the **SecureSphere User Guide**.

Log Collectors Details in the Gateways Window

For each Log Collector that sends events to the Gateway, the following data is displayed.

Field	Description
Log Collector	The name of the Log Collector.
Status	The status of the Log Collector (for example, "Running").
Last Seen	The date and time of the last event received from the Log Collector.
Server Group	The name of the database server group.
Service	The name of the database service.
Events Since Up Time	The number of events since the connection to the Log Collector started.
Connections Since Up Time	The number of connections between the Gateway and the Log Collector.
Too Many Logs Count	The number of times the Gateway encountered too many logs (and was unable to handle all of them).
Invalid Events Count	The number of invalid events encountered in logs and discarded.
Invalid Logs Count	The number of logs which were completely invalid.
Failed Connection Count	The number of times the Gateway failed to connect to the Log Collector.
Errors Since Up Time	The number of errors since the connection to the Log Collector started.
Unexpected Collector Terminations	The number of times the connection to the Log Collector was unexpectedly terminated.
Up Since	The date and time of the connection to the Log Collector started.
Last Event Time	The date and time of the last event received by the Gateway.
Last Connection Time	The date and time of the last time the Gateway retrieved a log.

For information about Log Collectors, see Log Collector chapter **in the SecureSphere User Guide.**

Configuring Archiving per Gateway

For performance reasons, you may wish to send audit records directly from the Gateway to the archive location, rather than from the Gateway to the MX and from there to the archive.

To configuring archiving per Gateway:

1. If you will be using NFS for the archive directory, then in **Admin** > **System Definitions** > **Action Interfaces**, create an **NFS Archive** action interface and specify a **Destination Directory**.

   Alternatively, you can use SCP for the archive directory. In this cases, the appropriate action interface are already defined.

   For information on how to create an **NFS Archive** action interface, see "Creating and Configuring Action Interfaces" in the **SecureSphere User Guide**.
2. In **Main** > **Policies** > **Action Sets**, create an action set to be used by the archive action interface you will be using (whether NFS or SCP).

   Depending on how the action interface is configured, you may need to specify the **Destination Directory**.

   For information on how to do this, see "Creating Custom Action Sets" in the **SecureSphere User Guide**.
3. In **Main** > **Policies** > **Audit**, under **Archiving Action** (in the **Archiving** tab), select the action set.
4. In **Main** > **Setup** > **Gateways**, select **Archive audit data directly from Gateway**.

For SCP archives, no further configuration is necessary.

For NFS archives, you must mount the archive directory to the Gateway, as described in Mounting the Audit Archive Directory (NFS) on page 175.

Mounting the Audit Archive Directory (NFS)

This procedure describes how to mount the Audit Archive Directory (NFS).



Note: The mounted directory must be shared.

To mount a Windows directory:

1. SSH to the Gateway.
2. Execute the following command:

```
mount -t smbfs -o username=<win-user>,workgroup=IL
//<win-user>/<win-dir> /<unix-dir>
```

To mount a Linux directory:

1. Confirm that the NFS server is running on the remote machine.
2. Confirm that the directory is shared.
3. SSH to the Gateway.
4. Execute the following command:

```
mount host:/dir_to_mount //local_dir
```

To mount a CentOS5 directory:

1. SSH to the Gateway.
2. Execute the following command:

```
mount -t cifs -o username=<win-user>,workgroup=IL
//<win-user>/<win-dir> /<unix-dir>
```

Gateway Groups

You can view, create and edit Gateway groups.

To view a Gateway group:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Gateways** pane, click .
3. In the **Create New Gateway Group** window, enter the data in the table below.
4. Click **Create**.
5. Click **Save**.

Parameter	Options
Name	The name of the Gateway group.
Platform	Select a platform from the menu: • **Imperva** • **Imperva G2** • **Crossbeam** • **Other**
Gateway Mode	Select a mode from the menu: • **STP Bridge** • **IMPVHA Bridge** • **Sniffing** • **Reverse Proxy Apache** • **Reverse Proxy Kernel.** For more information about these modes, see Configuring a Gateway on page 68.
Fail Mode	Select a **Fail Mode**: • **Fail Open**: In the event the Gateway fails, it will continue to pass traffic without monitoring it. • **Fail Close**: In the event the Gateway fails, it will block all traffic. • **High Availability**: This gateway group is a High Availability cluster. This option is available only if Gateway Mode is **STP Bridge** or **KRP**. You must also toggle High Availability for each of the gateways in the group using `impcfg` (**Top** > **Gateway**> **Interfaces** > **Toggle HA on a bridge**).
Overload Policy	Select **Block on Overload** to specify that if the Gateway's throughput capacity is exceeded, all connections will be blocked until the throughput falls. A Gateway is considered overloaded when any of the following occurs: • CPU or memory utilization reach 100%. • Throughput exceeds the defined limit. • Resources are exhausted.

To view a Gateway group:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway group.

   The Gateway group's details are displayed in the **Gateway Group Details** pane.

To edit a Gateway group:

1. In the **Main** workspace, select **Setup** > **Gateways**.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway group.
4. In the **Gateway Group Details** pane, enter the following data:

Parameter	Description
General Info	
Name	The Gateway group's **Name** is displayed. You can change **Name** here.
Platform	The Gateway group's **Platform** is displayed.
Topology Configuration	
Mode	The Gateway group's **Mode** is displayed.
Fail Mode	Select a **Fail Mode**: • **Fail Open**: In the event the Gateway fails, it will continue to pass traffic without monitoring it. • **Fail Close**: In the event the Gateway fails, it will block all traffic. **Note: Fail Open** is not supported for 10G appliances.
Overload Policy	Select **Block on Overload** to specify that if the Gateway's throughput capacity is exceeded, all connections will be blocked until the throughput falls.
Reset untraceable user connections	FAM only - Select Reset untraceable user connections to specify that the SecureSphere Gateway should reset connections that were opened before the Gateway was started, so that the actual user will be identified in the audit file.
Allow Ambiguous Packets	
Allow IP bad checksum	Allow a packet through the Gateway even if it has a bad IP checksum.
Allow TCP bad checksum	Allow a packet through the Gateway even if it has a bad TCP checksum.
Allow TCP reset out-of-window	
Allow TCP sequence before ISN	Allow a packet through the Gateway even if its sequence number is less than the TCP session's ISN (Initial Sequence Number).
Allow TCP ack beyond sequence	
Allow TCP sequence out-of-window	
Allow UDP bad checksum	Allow a packet through the Gateway even if it has a bad UDP checksum.
External Logger	

Parameter	Description
Syslog transport	Select a transport protocol for issuing logs to syslog: • **UDP**: The connectionless UDP protocol is used. UDP carries less overhead but has the disadvantage that delivery is not guaranteed. • **TCP**: The TCP protocol is used. TCP carries a higher overhead than UDP but delivery is guaranteed. Some additional configuration may be necessary.
Primary Host	The IP address of the primary host to which syslogs will be sent.
Port	The port on the primary host to which syslogs will be sent.
Secondary Host	The IP address of the secondary host to which syslogs will be sent.
Port	The port on the secondary host to which syslogs will be sent.
Performance Profiling	
Enable	Check **Enable** to monitor the performance of this Gateway in the **System Performance** window (see Chapter 14, System Performance).
Gateways	
Gateway Name	A read-only list of the Gateways which are members of this group is displayed.
HTTP Connection	Expand this field to configure the Gateway group's connection to outside networks. **Allow Gateway to Connect with Outside Systems** - Allow the Gateway to connect to outside systems. **HTTP Proxy** - Specify the HTTP proxy the Gateway should use. Select from the list one of the HTTP proxies defined under **Main** > **Setup** > **Global Objects** > **Gateway HTTP Proxy**. **Validate Certificate** - Check this if you want the Gateway to validate the HTTP proxy's certificate.

If you have made any changes in the **Gateway Group Details** pane, click **Save**.

Configuring a Kernel Reverse Proxy

Configuring a Kernel Reverse Proxy consists of the following:

- Configuring the Gateway appliance as a KRP using `impcfg` (see **Configuring a Gateway**)
- Configuring aliases and routing on the KRP, as described in this section
- Configuring KRP rules in the HTTP service's **Reverse Proxy** tab (see the "Reverse Proxies" chapter in the **SecureSphere User Guide**)

Aliases

An alias associates an inbound IP address and an outbound IP address for the KRP, enabling the SecureSphere administrator to "route" traffic from a specific inbound interface to a specific Web server. Since a network tends to be dynamic, IP address allocation may change from time to time. Aliases eliminate the need to configure changes in two places (on the Gateway and on the MX).

Beginning with SecureSphere version 10.0, aliases are defined in the SecureSphere GUI, so that administrators can centrally view and manage all KRP (Kernel Reverse Proxy) features: routing, interfaces and virtual routers (VRRP). In addition, configuration can also be accomplished importing a pre-prepared CSV file, simplifying the task of configuring multiple Gateways.



Note: When a Gateway is registered to an MX, the Gateway sends the MX information about its network interfaces, and users may configure the Gateway on the basis of that information. If any of the Gateway network interfaces is deleted or removed, the MX's Gateway configuration based on the deleted interface becomes invalid. The user must then either restore the network interface on the Gateway or modify the Gateway configuration on the MX accordingly.

Routing

If the KRP's IP addresses (usually outbound addresses) are not on the same network as the destination IP addresses, routing must be configured to enable connectivity. If the default route was changed, it is important to configure new routes (for example, SSH to the Gateway).



Note: If the backend server is not on the same network as the SecureSphere Gateway, make sure communication is allowed through any intervening firewalls.

A typical configuration is shown in the following figure.

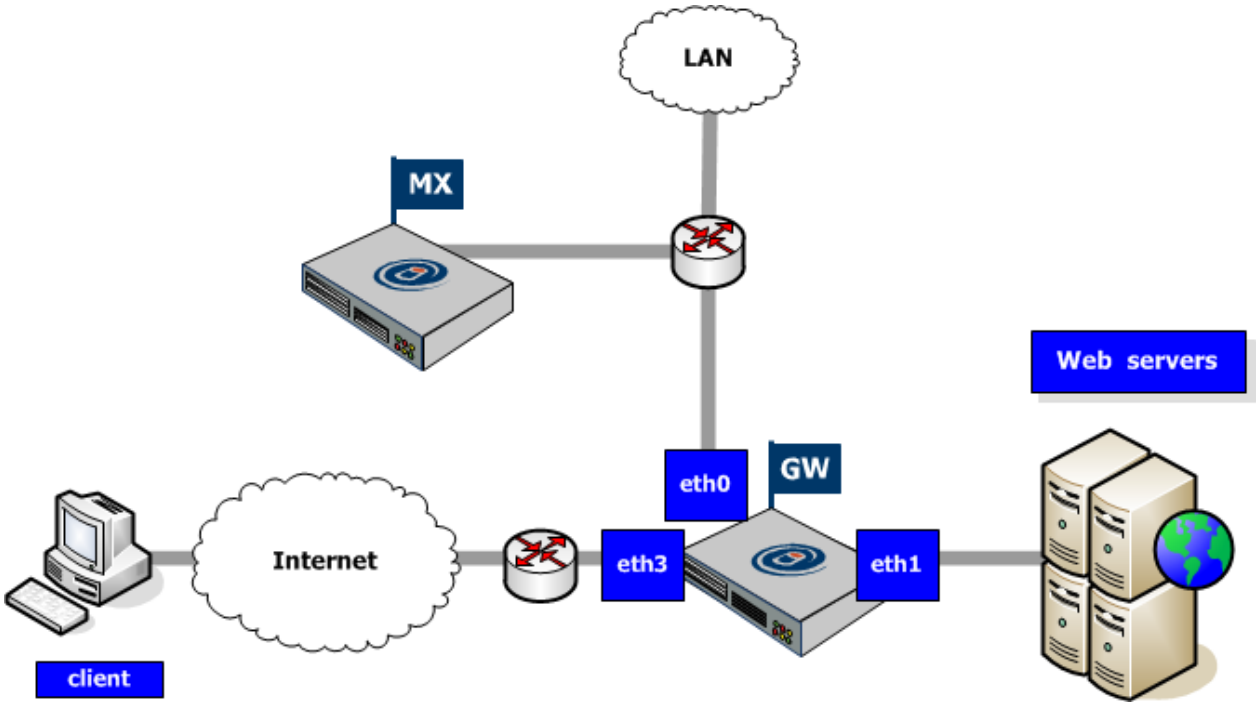


Figure 45: Typical Reverse Proxy Routing

There are two routes to be configured:

- **eth0**: to the SecureSphere MX
- **eth1**: to the Web server

All other traffic can be routed out through the Internet. The challenges here are to ensure that:

- The MX traffic is properly routed out through eth0
- Return traffic from the Web servers is routed out through eth3

Configuring Aliases

An alias associates an inbound IP address and an outbound IP address for the KRP, enabling the SecureSphere administrator to "route" traffic from a specific inbound interface to a specific Web server. To configure an alias, you must:

1. If you are using VRRP for High Availability, define an IP address for the Gateway.
2. If required, configure a virtual router.
3. Associate a pair of alias IP addresses with the network interfaces.

   You can associate multiple IP addresses with each network interface.

Defining an IP Address for the Gateway for VRRP

To define an IP address for the Gateway:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.

The Gateway's details are displayed in the **Gateway Details** tab.

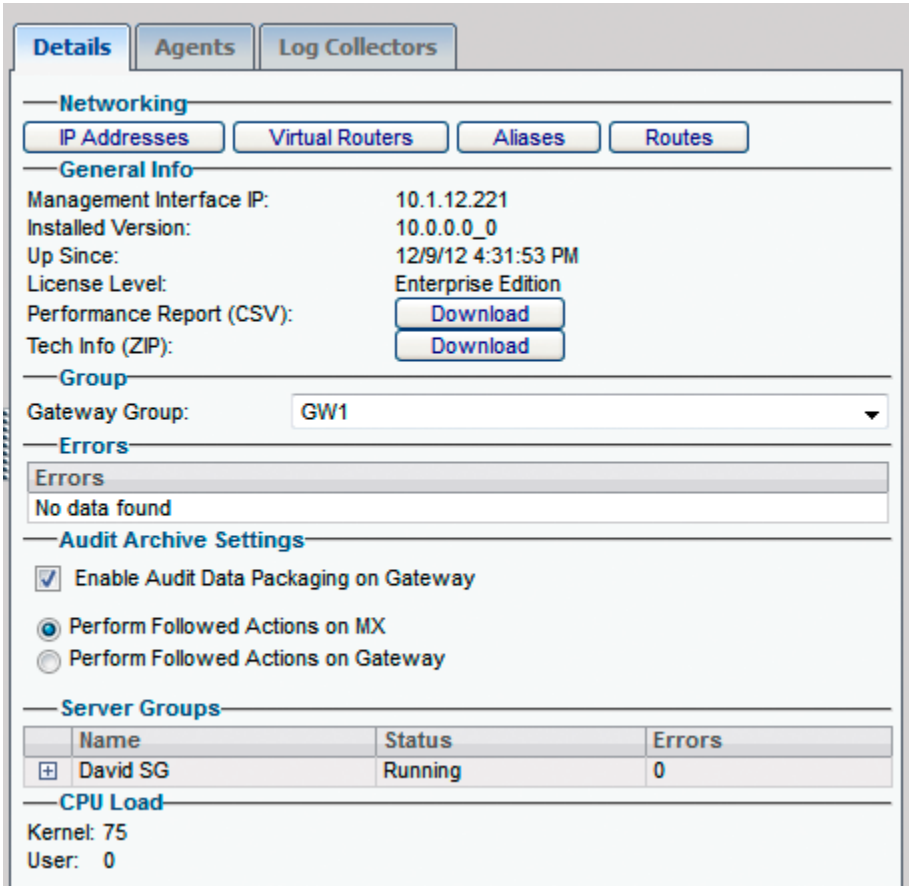


Figure 46: Gateway Details tab

If you are using VRRP to provide High Availability, you must define at least one IP address for the KRP Gateway, on which the two primary and secondary Gateways will communicate. To do this:

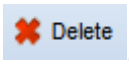
4. Under **Networking**, click **IP Addresses**.
5. In the **IP Addresses** window, click 

.
6. In the **IP Address** window, enter the data in the table **IP Address Window Parameters** below.
7. Click **OK** to save.
8. The IP address will be defined on the Gateway, exactly as if you had defined it in the Gateway's CLI. The required CLI commands are executed "behind the scenes."
9. Define additional IP addresses as required, or click **Close** in the **IP Addresses** window.

IP Address Window Parameters

Field	Description
Network Interface	From the dropdown menu, select the network interface to which the IP address will be assigned.
IP Address/Mask (CIDR)	Enter the IP address in CIDR notation.
Virtual	Check this box if the IP address is virtual, that is, an IP address that moves between the primary and secondary Gateways upon failover in the VRRP environment.
VR ID	If **Virtual** is checked, select the **VR ID** from the dropdown menu.
Next Hop	Specify the IP address to which to send outgoing traffic from this IP address. This field is used to route return traffic from the Web servers out from the KRP, for example, to ensure that traffic from a specific ISP is routed back to the same ISP.
Comment	Optional explanatory text.

To delete an IP address for the Gateway:

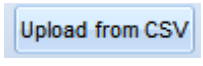
1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **IP Addresses**.
5. In the **IP Addresses** window, select an IP address.
6. Click 

.
7. Confirm the deletion.

Configuring a Virtual Router

This procedure describes how to configure a virtual router.

To define a virtual router:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Virtual Router**.
5. In the **Virtual Routers** window, do one of the following:
   - Click 

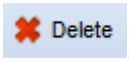
and browse to the CSV file containing the information (see Importing KRP Configuration From a CSV File on page 186), *or*
   - Click 

.
   - In the **Virtual Router** window, enter data in the table **Virtual Router Configuration Options** below.
   - Click **OK**.
   - Define additional virtual routers as required, or click **Close** in the **Virtual Routers** window.

Virtual Router Configuration Options

Field	Description
Network Interface	From the dropdown menu, select the network interface to which the virtual router will be assigned.
VR ID	Enter an identifier for the virtual router.
Primary IP Address	Enter the primary IP address for this virtual router. If you leave this empty, the VRRP protocol will assign an IP address. Optional: Enter the IP address to be used by the Virtual Router for multicast VRRP packets. If empty, VRRP will use the interface's primary IP address.
Default State	Choose **Primary** or **Secondary** from the dropdown menu.

To delete a virtual router:

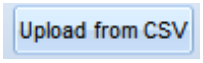
1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Virtual Routers**.
5. In the **Virtual Routers** window, select a virtual router.
6. Click 

.
7. Confirm the deletion.

Configuring an Alias

This procedure describes how to configure an alias.

To configure an alias:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Aliases**.
5. In the **Aliases** window, do one of the following:
   - Click 

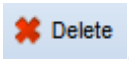
and browse to the CSV file contain the information (see Importing KRP Configuration From a CSV File on page 186), *or*
   - Click 

.
   - In the **Alias** window, enter the data in the table **Alias Configuration Options** below.
   - Click **OK**.
   - Define additional aliases as required, or click **Close** in the **Aliases** window.

Alias Configuration Options

Field	Description
Alias Name	Enter an alias name, or select one from the dropdown menu.
Enabled	Specify whether the alias is enabled.
External Address	Select an IP address from the dropdown menu.
Internal Address	Select an IP address from the dropdown menu.
Comment	Optional explanatory text.

To delete an alias:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Aliases**.
5. In the **Aliases** window, select an alias.
6. Click 

.
7. Confirm the deletion.

Configuring a Route

This procedure describes how to configure a route.

To configure a route:

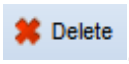
1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Routes**.
5. In the **Routes** window, click 

.
6. In the **Route** window, enter the data in the table **Route Configuration Options** below.
7. Click **OK**.
8. Define additional routes as required, or click **Close** in the **Routes** window.

Route Configuration Options

Field	Description
Type	From the dropdown menu, select **Network** or **Host**, specifying whether the route is per network or per a specific host.
Destination Address / Mask	If **Type** is Network, enter the IP address of the destination in CIDR notation. If **Type** is Host, enter the IP address of the destination (without CIDR).
Next Hop	Specify the IP address to which to all packets sent to **Destination Address** will be forwarded.
Virtual	Check this box if the IP address is virtual.
Network Interface	Optional: Select the network interface to use or leave blank. If left blank, the best available interface is selected when routing.
Virtual	If **Virtual** is checked, select the **VR ID** from the dropdown menu.
Metric	Optional: The metric to be used by the routing protocol to determine the route to be chosen when more than one route is available.

To delete a route:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Filter** pane, select **By Mode**, **By Platform** or **By Server Group**.
3. Select a Gateway.
4. Under **Networking**, click **Routes**.
5. In the **Routes** window, select a route.
6. Click 

.
7. Confirm the deletion.

Importing KRP Configuration From a CSV File

When configuring Virtual Routers (see Configuring a Virtual Router on page 183) or Aliases, (see Configuring an Alias on page 184), you have the option of importing the data from a CSV file you prepared in advance (possibly originally in the form of a spreadsheet).

Virtual Routers

The format of a CSV file for virtual routers is as follows:

Field Number	Field	Description
1	**VR ID**	The virtual router identifier.
2	**Network Interface**	for example, eth0, eth1, *etc.*
3	**Primary IP Address in CIDR Format**	
4	**Default State**	One of the following strings: • "Master" • "Backup"

Aliases

The format of a CSV file for aliases is as follows:

Field Number	Field	Description
1	**Alias Name**	
2	**Enabled**	0 or 1
3	**External IP Address in CIDR format**	
4	**External IP Address Interface**	for example, eth0, eth1, *etc.*
5	**External IP Address Next Hop**	
6	**External IP Address Virtual Flag**	0 or 1
7	**External IP Address VR ID**	
8	**Internal IP Address in CIDR format**	
9	**Internal IP Address Interface**	for example, eth0, eth1, *etc.*
10	**Internal IP Address Next Hop**	
11	**Comment**	



Note: When there is a request sent to the non existing page or the protected server is down, it returns blocking response and no alert is generated, as it is not an attack. For example, when the protected server is down, an error page is sent, but it does not indicate that the server is under attack.

Exporting Technical Information from Gateway and Onebox

On occasion, when encountering trouble with SecureSphere operation, Imperva support may request that you provide them with technical information that is automatically generated by SecureSphere, so they can analyze logs and other information. You can export this information from the SecureSphere Gateway using the GUI. This procedure describes how to export tech info for a SecureSphere Gateway from the GUI. For information on exporting tech info for SecureSphere MXs, see Exporting Technical Information from Management Servers on page 300.

To export technical information for a Gateway:

1. In the **Main** workspace, select Setup > Gateways.
2. In the **Gateways** pane, select the **Gateway** whose get tech info you want to export.



Note: The Gateway must be in the status Running.

3. In the **Details** pane, next to **Tech Info (zip)**, click **Download**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.



Note: When exporting technical information from a Onebox architecture, both Gateway and MX technical information is exported.

CHAPTER 7

Licenses

Imperva SecureSphere requires a license. This chapter describes the SecureSphere licensing process and reviews the following subjects:

License Overview 189
Uploading Licenses 190
Viewing Licenses 190
Managing Database Scanning and Assessment Licenses 192

License Overview

A license contains the following information:

- Product information - a list of the products enabled by the license, for example, Web, DB, File, etc.
- Gateway modules - the types of Gateway (for example, WAF, DMA/DBF, etc.) enabled by the license and counters for each module (specifying the number of modules enabled)
- Assessment counter - the number of scanned servers enabled
- File / URM - the number of users enabled
- Expiration date - for evaluation licenses only; non-evaluation licenses are not time-limited
- Maintenance period - specifying the period during which ADC content can be downloaded

When a license is renewed, it is replaced by a new license.

Licenses for a SecureSphere Management Server and all the Gateway it manages are installed on the Management Server.

Uploading Licenses

The procedure describes how to upload a license to SecureSphere.

To upload a license:

1. In the **Admin** workspace, click **Licensing**.
2. Click **Actions**.
3. From the menu, select **Upload License File**.
4. In the **Upload License File** window, click **Browse** and navigate to the license file.

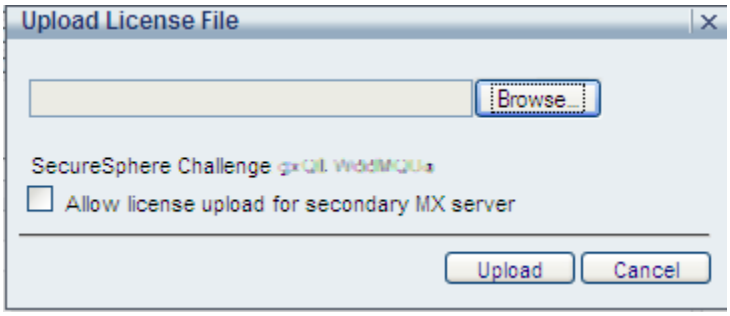


Figure 47: Upload License File Window

5. If this is an MX-HA deployment, enable **Allow license upload for secondary MX server**.
6. Click **Upload**.

Viewing Licenses

This procedure describes how to view licenses installed on SecureSphere.

To view all the installed licenses:

1. In the **Admin** workspace, click **Licensing**.

   A summary of the installed licenses is displayed in the **License** pane.

   Under **License Summary**, the following information is displayed:

   - **Level**: **Enterprise Edition**.
   - **Products**: A list of licensed products, for example, **WAF** (Web Access Firewall), **DAS** (Discovery and Assessment Server), Database Scanning and File Server Scanning and ThreatRadar.

   Under **License Summary (GW modules)**, the following information is displayed for each Gateway license:

   - **Module**: The Imperva product, for example DAS, DAM, *etc*.
   - **Quantity**: The number of modules included in the license.
   - **HW**: The Gateway hardware model, for example, **G4** or **G10**.
   - **File**: The name of the license file which contains this Gateway license.
   - **Expiration Date**: The date this Gateway license expires.

   Under **License Summary (Cross System modules)**, information is displayed about the Imperva Customer Service support license, including ADC content:

   - **Module**: For example, ADC Content, Maintenance, *etc*.
   - **Start Date**: The date from which the license is valid.
   - **Expiration Date**: The date the license expires.

   Under **License files**, the following information is displayed for each license file:

   - **File Name**: The name of the license file.
   - **License Type**: The type of license, for example, evaluation.

- **Issuing Date**: The date the license was issued.
- **Comments**: Other information.

2. Select a license file from among those displayed under **License files**.
   The details of the licenses contained in the selected file are displayed in the right pane, under **Details**.

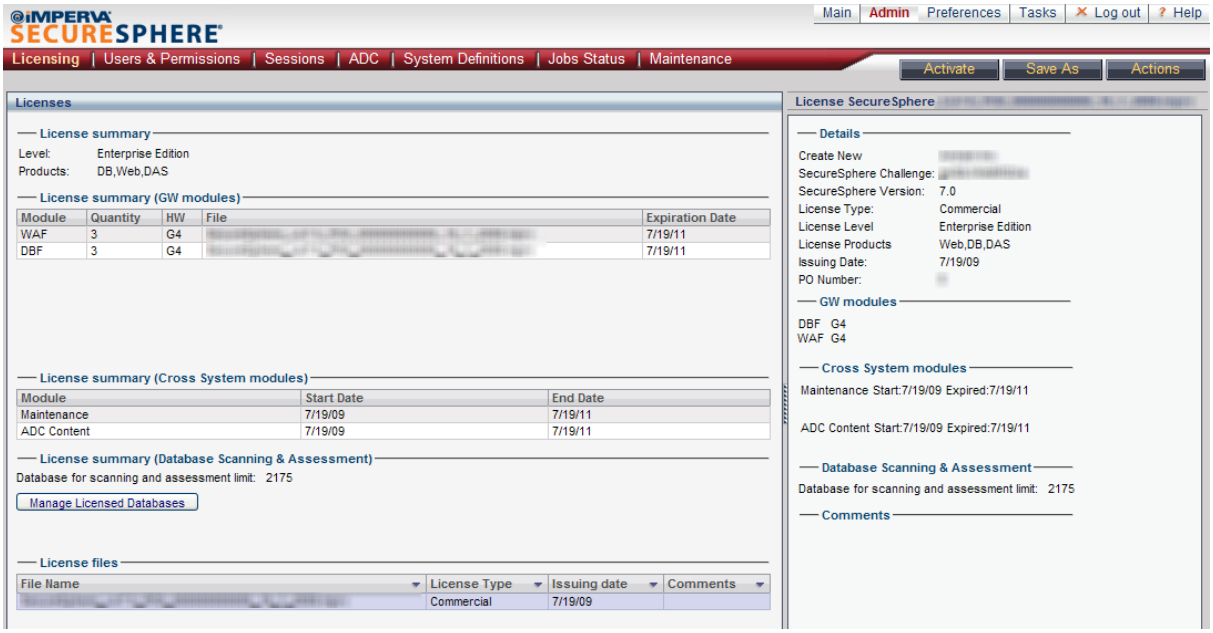


Figure 48: Licenses Window

Note: Some information about the license is displayed in the SecureSphere login screen.

Managing Database Scanning and Assessment Licenses

SecureSphere is licensed with a pre-defined number of assets that can be scanned and assessed based on Gateway modules. Once you start running assessments on assets, available licenses are automatically assigned. For every new asset, a new entry is added to the table in the Manage Licensed Databases window described below. This procedure describes how to manage these licenses after they have already been assigned.

To manage licenses for database scanning and assessment:

1. In the **Admin** workspace, click **Licensing**. Currently installed licenses are displayed.
2. In the **License Summary** (Database Scanning & Assessment) pane, click **Manage Licensed Databases**. The **Managed Licensed Database** window appears.
3. From the **Status** dropdown menu in the **Managed Licensed Databases** window, select the desired option:
   - **Licensed**: Assigns a license to the selected item.
   - **Unlicensed**: Removes a license from the selected item. The next time an assessment is run on this item, the SecureSphere Management Server will check if there is available license. If there is, it changes its status to "Licensed" and assesses the database. If there is no license available, it will remain unlicensed and any attempt of assessment results in an error.
   - **Ignore**: Ignores the selected item (doesn't attempt to assess it).
4. At the bottom of the Managed Licensed Databases window, click Save. Your changes have been saved.



Note: To remove an entry from the table and free up a license, select the item in the table and then click the Delete icon.

CHAPTER 8

Users and Permissions

SecureSphere provides a robust permissions model that enables you to create new users, assign them one or more roles that grant permissions to objects based on those roles, then grant users additional permissions to specific objects in SecureSphere.

This chapter describes how to manage SecureSphere users and contains the following sections:

Understanding Permissions 193
Permissions Workflow 197
Working with Roles 197
Working with Users 199

Understanding Permissions

This section provides information about the mechanism for managing users and permissions and the impact of granting or removing permissions. It reviews the following subjects:

Permission Models in SecureSphere 194
Roles and Users 194
Permission Types 195
Understanding the Permissions Window 195
Adding and Removing Permissions 196
Notes on Permission Behavior 196

Permission Models in SecureSphere

It is recommended that before you get started in creating roles and users you first determine how to best match your user model with your workflow. There are three primary models that are recommended to understand how to match SecureSphere users with your organization.

Based on:	
Role Based	In this model, users are assigned a specific role and receive permissions for fulfilling this role. For example, perhaps a user is designated specifically to monitor a certain type of traffic. You would assign them the role of Web or DB Administrator based on what kind of traffic they are responsible for.
Product Line Based	In this model, a user may be responsible for all aspects of a specific product line, either Web based or database based products. For example, they may be responsible for the configuration of security policies for that product, the monitoring of traffic, and the creation of reports. You would then create a user and assign them the various role for that product, or create a new role for this purpose and configure it as required.
Specific Access Based	In some cases you may want to give targeted permissions to an outside user. For example, if you are an ISP and want to give your customers the ability to only view the specific web service and monitor that service, you would create a user for this purpose, and only grant him permissions to view the specific objects related to the service. In some cases you may want to give targeted permissions to a user. In that case, you need to create a user for this purpose, and grant him only specific permissions.

Roles and Users

The permissions model in SecureSphere is based on the following primary types of permissions:

- **Roles**: Represents a role in an organization, such as a Web Security Administrator and includes a set of permissions specified for that role. SecureSphere comes with a set of pre-defined roles.
  For information on roles see Working with Roles on page 197
  For a list of predefined roles and their descriptions see PreDefined Roles on page 198
- **External Roles**: Represents a group of users defined in an external authorization system (currently Active Directory only). In SecureSphere these roles are mapped to the roles in external systems and can receive SecureSphere roles and permissions, similarly to SecureSphere users. For more information on external roles see the User Guide.
- **Users**: Represents an actual user in SecureSphere to whom permissions are granted. When users are created, they are assigned one or more roles, granting them the permissions associated with those roles, and can additionally be assigned permissions to specific users. For more information on users see Working with Users on page 199
- **External Users**: A user that is defined in the external authorization system (currently Active Directory only) and in SecureSphere this user is created automatically during user's first login. Such users cannot be deleted or assigned roles in SecureSphere, only in the external system. External users can receive SecureSphere permissions, granted explicitly by administrator, or automatically when it creates objects. For more information on external users see the **SecureSphere User Guide**.

Permission Types

There are three primary types of permissions that users can be granted to various SecureSphere components. These include the following:

Based on:	Description
View	Enables users to only view the specific object. Though users cannot edit their parameters nor create new objects. If a user doesn't have "view" permission to an object, they can still see the object's name.
Edit	Enables users to view a specific object, edit the details of an object (asset configuration, policy rules etc.), but not create new objects.
Create	Enables users to create objects (per category). These users then automatically receive edit and view permissions for this object. A category Subsystem on SOM controls all the permissions that SOM users are granted to work with MXs on that SOM.

In addition to the permissions mentioned above, all users can use all objects available in SecureSphere such as policies, global objects, action sets, etc., on assets they have permissions to. For example, if a user has edit permissions to a specific web service, they can apply any existing policy to that web server, even if they don't have view permissions on the policy.

Working with the Subsystem category objects on SOM:

- When you have **View** permissions, you can perform the following with MXs registered to that SOM:
- Viewing MXs in the **Registered MXs** window.
- Viewing MXs in the **Apply to MXs** pane that presents the items that can be downloaded to MXs.
- Viewing the statistical data from that MX in the **Dashboard**.
- When you have **Create** permission for MXs, you can create MXs.
- When you have **Edit** permissions, you can perform the following with MXs registered to that SOM:
- Editing MX properties.
- Registering an MX, deleting an MX and test connection to that MX.
- Drilldown to that MX.
- Downloading items to that MX.

Understanding the Permissions Window

This topic provides an overview of the Permissions window.

To access permissions:

1. From the **Admin** workspace, click **Users & Permissions**.

2. Select a user or group. For information on how to create users, see Creating a SecureSphere User on page 200.

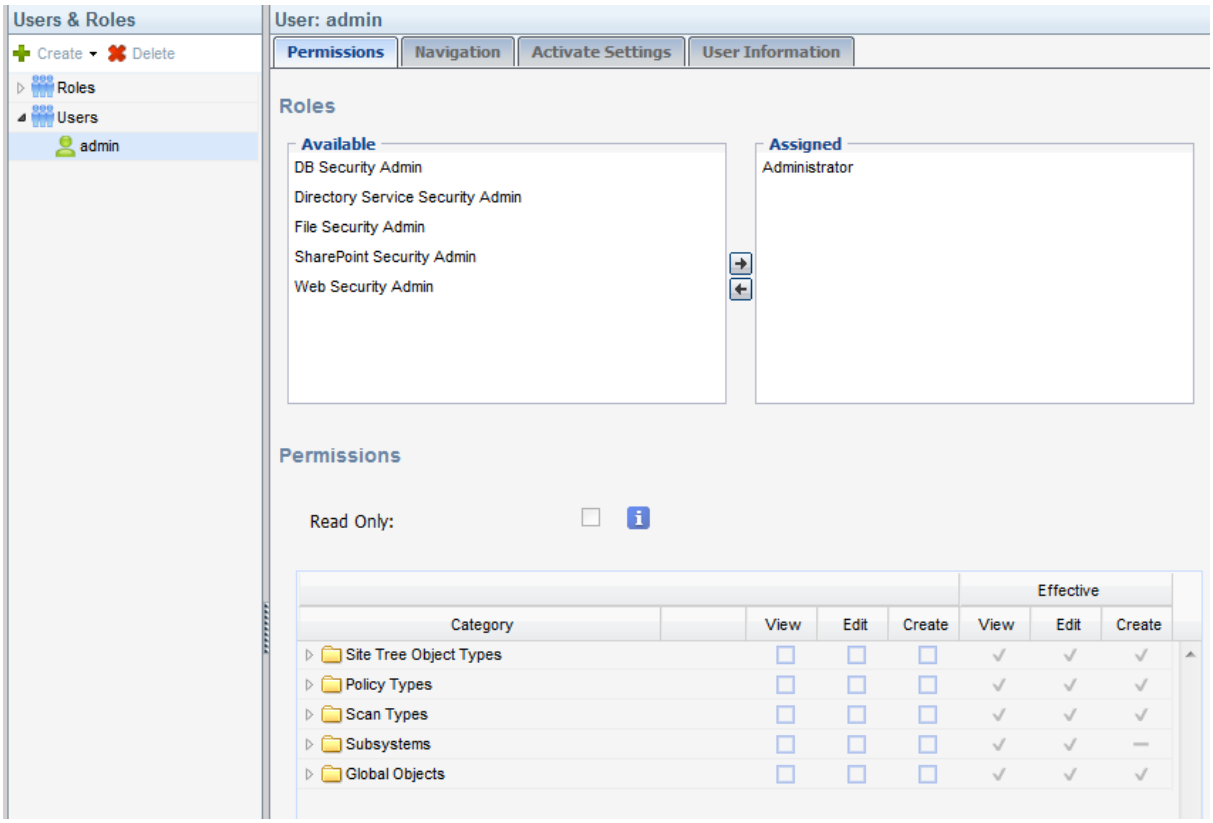


Figure 49: Remote Agent Permissions tab

Adding and Removing Permissions

Adding and removing permissions to objects in the permissions window is accomplished by selecting or deselecting the relevant checkbox then clicking Save. Permissions are granted to the specific object or category selected.



Note: When permissions are granted to categories, they automatically cascade to all objects in that category. The category object is selected, though the its objects appear disabled.

Notes on Permission Behavior

Granting or revoking permissions in SecureSphere affects various permission objects in different ways. The below provides some important information regarding permission behavior to assist in better understanding and managing permissions.

- The default user is "administrator". The Administrator user has create, view and edit permissions to the entire SecureSphere system
- Only Administrators or users assigned the **Administrator** role, have access to the **Admin** workspace
- A regular user has edit permission for any objects they create, except if an Administrator later revokes those permissions
- When enabling Edit permissions, uses are automatically granted view permissions

Permissions Workflow

The basic process of creating users and assigning permissions includes the following primary steps:

#	Action	Description	For more information, see...
1	**Create or customize roles as desired**	Customize existing roles or create new roles to match your organization's needs.	Working with Roles on page 197
2	**Create a new user**	Create a new user to represent a SecureSphere user that needs access.	Creating a SecureSphere User on page 200
3	**Assign roles to the user**	Assign the desired roles to the user that match that user's responsibilities.	Assigning Roles to Users on page 200
4	**Configure object specific permissions**	Configure any additional permissions for specific objects the user or role might require, if applicable.	Configuring Object or Category Level Permissions on page 201
5	**Configure navigation and activate settings permissions**	Configure permissions for access to views and activating settings.	Configuring Navigation Permissions and Activate Settings "Configuring Navigation Permissions" on page 202
6	**Configure user information**	Configure User information including phone, e-mail, department and more.	Configuring User Information on page 205



Note: In addition to the regular SecureSphere users, you can set permissions for the Active Directory users. For more information about integration with Active Directory, see **Configuring Integration with Active Directory** in the **SecureSphere User Guide**.

Working with Roles

Roles in SecureSphere reflect a role in your organization and contain a specific set of permissions required to perform that role. SecureSphere also contains a set of pre-defined roles which can be used.

Additionally, you can create new roles and customize them to match your company's workflow. The following subjects review various aspects of working with Roles:

PreDefined Roles 198

Custom Role Examples 198

Creating a Role 199

PreDefined Roles

SecureSphere comes with a set of pre-defined roles to assist you in easily configuring users with the level of permissions required to fulfill their roles.



Note: Predefined roles cannot be modified.

The following is a list of these pre-defined roles and a short description of each:

Pre-Defined Roles

Administrator	Main administrator user for SecureSphere. Assigned when first logging into SecureSphere. This user is responsible for managing SecureSphere and has permissions to all features and functionality.
Web/DB/File/SharePoint Security Admin	**Security Admins** are responsible for all the security aspects that deals with a specific product. For example, the Web Security Admin can create and edit services and applications, security policies and all global objects relevant to web products.

Custom Role Examples

The following are examples of custom roles that can be created to match a specific set of requirements.

Example 1: Managed Security Service Provider (MSSP)

MSSPs often offer third party solutions to their customers, and may want to provide some level of access to these products. In this case, you would want to provide view permissions to your customers for only those SecureSphere components that represent their specific services and applications, and provides under special permissions to the alerts screen. They would not obtain permissions to edit assets, policies, or global objects.

This can be done in different ways. For example, if you have 10 customers, each with only 1 user, you may want to create the user separately for each customer. Alternatively, you may want to create a role that would give navigation permissions to items such as monitoring, create individual users and include this role, then customize the user with permissions to view their specific assets.

Example 2: Web Services Engineer

If your organization utilizes a compartmentalized model such as a bank in which specific web services engineers should only have access to view details about specific services, you may want to:

- Create a new Role based the existing Web Security Admin
- Remove the Web Services and Applications that appear under Site Tree Object Type category
- Access each individual user, and under Web and Application Services (under site tree object types) click the edit button for these items, and select only those web services and applications you want the specific user to have access to.

Example 3: Audit Expert

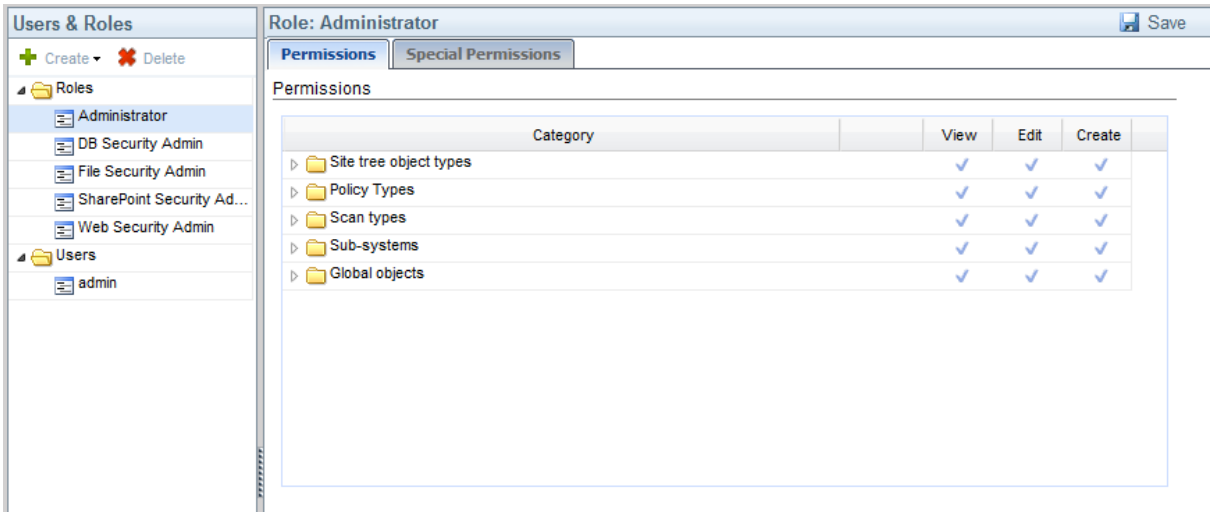
In some organizations there is a designated audit expert that creates audit policies, defines what data is audited, and how this data is handled. You may want to create a special Role for users who are responsible for creating these policies, but which prevent them from seeing actual audit data. In this case you could create a user (or role if there is more than one user with these responsibilities) which would only have create and edit permissions on audit policies. You may also want to provide them view permissions on a test database, which would enable them to test their policy as they are working on it, without exposing sensitive data.

Creating a Role

SecureSphere comes with a number of pre-defined roles. You can additionally create custom roles to better match your company's environment.

To create a Role:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, click , then **Create New Role**. The **Create New Role** window appears.
3. Type a **Name** for the role, then click **Create**. The new role is created and appears under **Roles** in the **Users and Roles** pane to the left-hand side of the window.



4. Configure this role with the desired permissions by selecting the role and defining permissions. When defining permissions in the **Permissions** pane, the same permissions are added to all the objects under that category.
5. To define different permissions for each object under the same category, click . The **Object Level Permissions** window appears.
6. Define the permissions that you want for each item in the **Object Level Permissions** list.

Working with Users

There are a number of aspects that are involved with working with users. They include the following:

Creating a SecureSphere User 200
Assigning Roles to Users 200
Configuring Object or Category Level Permissions 201
Configuring Navigation Permissions 202
Configuring the Authorization to Activate Settings 203
Granting Masking/Unmasking Capability to SecureSphere Roles and Users 204
Configuring User Information 205
Locking a User Account 206
Resetting a User Password 206
Read-Only User 208

Creating a SecureSphere User

Users in SecureSphere define a number of parameters that include roles to which a specific user is assigned, permissions to various SecureSphere objects ranging from site tree objects to global object, special permissions that provide access to views, and user information that define their full name, e-mail address, geographic location in the world, and more.

To create a SecureSphere User:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, click , then **Create New User**. The Create New User window appears.
3. Type a **Name** for the user.
4. In **Authenticator**, select **SecureSphere** or **External** as appropriate.
   - **SecureSphere**: The user is authenticated by SecureSphere using a password (entered in **Password** below).
   - **External**: The user is authenticated using an external service, such as LDAP.

     In this case, the **Enter Password** and **Re-Enter Password fields** are ignored by SecureSphere, and the user is required to provide the password defined in the LDAP server.

     The user's name in SecureSphere must be identical to the user's CN in LDAP. Case sensitivity is enforced, that is, "Mary" is not identical to "mary".

     For information about configuring SecureSphere to work with LDAP, see External Systems - LDAP.
5. If **Authenticator** is **SecureSphere**, enter the user's password in **Enter Password** and again in **Re-Enter Password**.
6. If **Authenticator** is **LDAP**, you can lookup the user in the LDAP database by clicking **Lookup User**.

   If **External Authorization** is not selected in the **Authentication & Authorization Configuration** window (see Authentication and Authorization Configuration on page 266), the user's SecureSphere password is used. If **External Authorization** is selected, you are prompted for the LDAP password.
7. Add one or more roles you want to assign the user by moving the desired roles to the Assigned pane. A role is a set of permissions to different objects. For more information on roles see Working with Roles on page 197
8. Click **Create**. The new user is created and appears under **Users** in the **Users and Roles** pane to the left-hand side of the window.

   You may now configure additional permissions for that user in addition to any permissions they are granted through roles. For more information see Configuring Object or Category Level Permissions on page 201.

Assigning Roles to Users

SecureSphere enables you to configure new users with roles and assign roles to existing users. By assigning roles to users you grant them the permissions that have been configured for the assigned roles.



Note: This procedure describes how to assign roles to existing users. Assigning roles to new users is part of the process of creating a new user. For information on assigning roles to new users, see Creating a SecureSphere User on page 200.

To assign a role to existing users:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you want to assign a new role. That users details are displayed in the details pane.
3. On the permissions tab, move the role you want to assign the user from the **Selected** pane to the **Assigned** pane.



Note: For information on creating new roles, see Creating a Role on page 199.

4. Click **Save**. Settings are saved and the user has now been granted the permissions available in the assigned role.

Configuring Object or Category Level Permissions

In addition to assigning users to a role, you have the option to assign them permissions to specific objects or categories of objects which may be relevant for their role or access model. For example, perhaps you are an ISP that provides SecureSphere as a paid service to your customers. And perhaps you'd like to give your customers only view access and only to their own web server. You could create a new user for each customer, and assign them additional (specific) view permissions for their web server.



Note: While you can add permissions on top of permissions provided through a predefined roles, you cannot revoke permissions that are part of these roles by default.

To configure additional permissions:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you want to assign additional permissions. That users details are displayed in the details pane.
3. In the **Permissions** pane, navigate to the category and object you want to grant permissions to. For example, if you want to assign additional permissions to a specific policy, next to the policy category, click **Edit** .
4. Select the desired object level permissions. The item is selected, and the item representing permissions is displayed. For more information on how permissions are represented in the **Permissions** tab, see Understanding How Permissions are Displayed on page 201.
5. In the **Object Level Permissions** window click **Save**.
6. In the **Users and Roles** window from the upper right-hand corner of the screen. Click **Save**.
7. Your changes have been saved and the additional permissions have been assigned.

Understanding How Permissions are Displayed

The way that permissions are displayed for a user depends on what permissions have been configured on a specific object. Permissions have three possible levels as displayed in the permission window.

Permission Levels

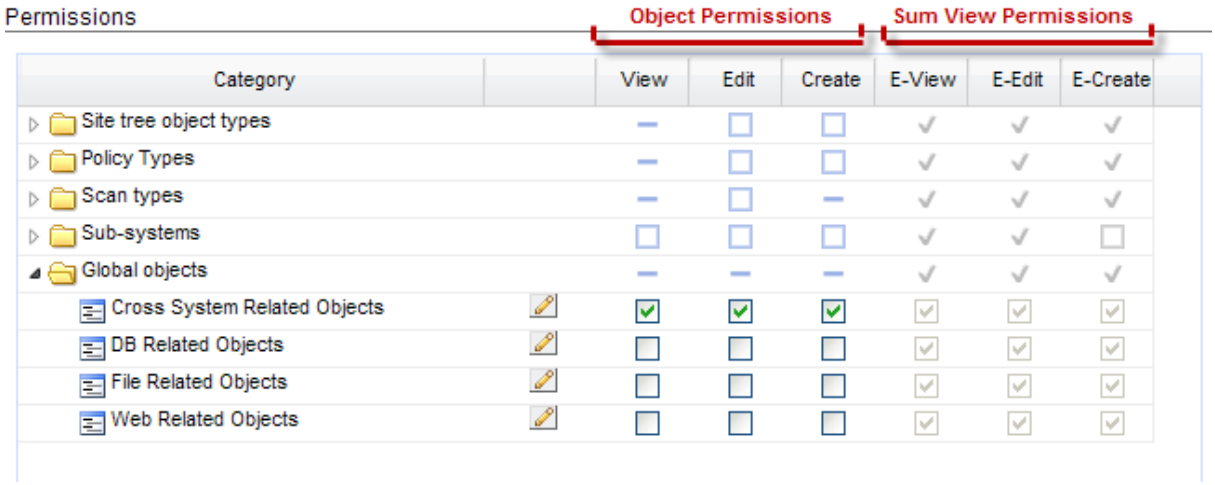
	Type	Description
☐	**None**	None of that category's object permissions have been assigned to the current user.
–	**Partial**	Some of the category's object permissions have been assigned to the current users.
✓	**Full**	All of the category's object permissions have been assigned to the current users.

Object View vs. Sum View

Permissions are displayed in SecureSphere on two levels:

- **Object View Permissions**: Displays permissions for the specific object only. For example, if a user has permissions to all Cross System Related Global objects as seen in the example below. Checkmarks are displayed for that category. Yet for the Global Objects category, you can see that hyphen symbols (partial) are displayed because this user does not have permissions to the other objects in that category.

- **Sum View Permissions**: Displays the sum of all permissions, both Object Level permissions, as well as permissions provided to users by roles they have been granted. So in the example below you can see that many of the objects the users have full permissions in Sum View, while under Object Permissions for the same items they only have partial permissions. This is due to the fact they have been granted additional permissions through their role which result in the user having all permissions for that object.



Configuring Navigation Permissions

In the Navigation tab you can define the navigation permissions to the enabled GUI windows.

For example, when you give a user permissions to access an agent, that user has access permissions to all data and all GUI windows pertinent to that agent - assuming no limitations have been placed on that user's navigation permissions. There are actions that the user can do on the agent's screen, like alter its configuration. However, the same agent appears in the software update screen thereby enabling the user to install the agent on a remote database or file server. This is an undesirable situation - you do not want the user with that permission to see the associated software update GUI window, and have access to all its functionality. By configuring the navigation permissions, you can define precisely which GUI windows can be seen by any user or role.



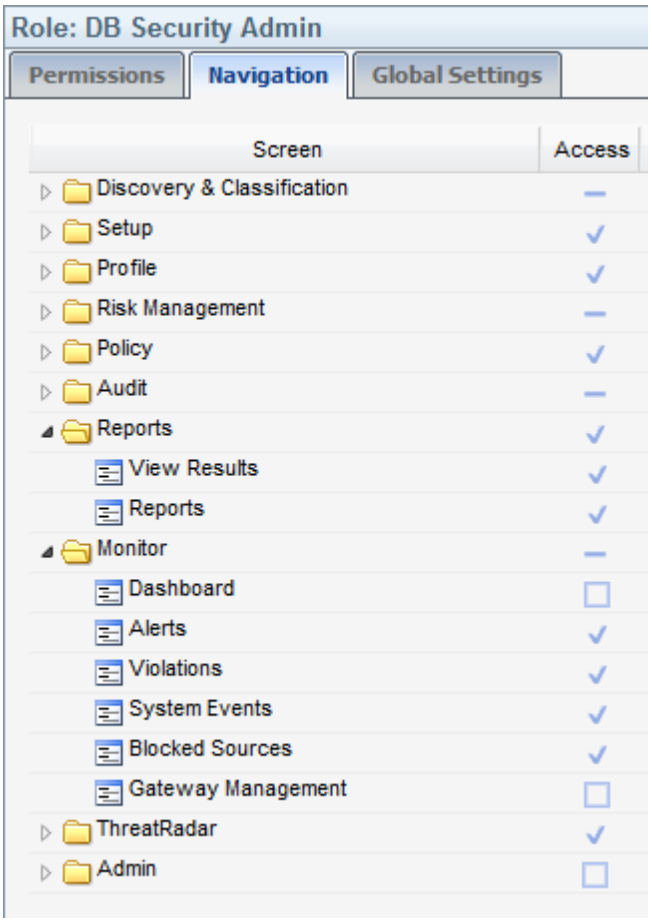
Note: An example of navigation permission might be that you want to allow a user to edit a certain database service but not see audit results. You would then give edit permissions on the service, but you wouldn't give navigation permissions on the audit screen.

A new user receives no navigation permissions by default. You must set navigation permissions either directly, or by assigning the user to a role that has navigation permissions.

To configure navigation permissions:

1. In the **Admin** workspace, select **Users and Permissions**.
2. In the **Users & Roles** pane, expand the **Users** category, then select the user or role to whom you want to assign navigation permissions. The users permissions of the selected user are displayed in the details pane. In the case of roles, only the **Access** column appears.

3. Click the **Navigation** tab. The relevant GUI windows categories and screens, together with their options, appear.



You can expand one or more categories to view the precise GUI windows of those categories.

Notes:

- The **Access** column is for adding permissions. The **Effective** column displays the default permissions, based on the role.
- A check mark signifies that the permission exists and cannot be removed. An empty check box signifies a non-existent permission that can be added. A dash mark appears only on categories and means that the windows in that category are a mixture of those with existing permissions, and those without.

4. To enable or disable permissions for any GUI window, check the appropriate options.
5. Click **Save**. Your settings are saved.

Configuring the Authorization to Activate Settings

A user for whom permission is given to use Activate Settings can modify the SecureSphere database by making the changes and clicking the Activate button. For any user, you can define under which conditions the Activate button will function, using the Activate Settings window.

To configure activate settings:

1. In the **Admin** workspace, select **Users & Permissions**.
2. In the **Users & Roles** pane, expand the **Users** category or the **Roles** category, then select the user or role for whom you want to configure activate settings.
3. In the **Global Settings** tab, select one of the **Activate Settings** options in the following table.

4. Click **Save**. Your settings are saved.

Activate Settings Options

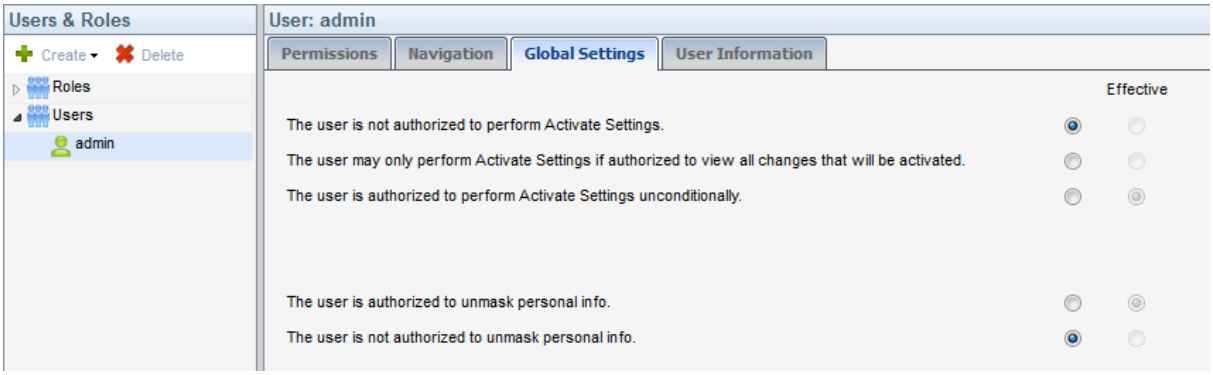
Parameter	Description
The user is not authorized to perform Activate Settings.	The user does not have permission to use Activate Settings.
The user may only perform Activate Settings if authorized to view all changes that will be activated.	The user is allowed to perform Activate Settings only if he has permission to view all the parameters whose settings will be changed when Activate Settings is performed.
The user is authorized to perform Activate Settings unconditionally.	There are no restrictions on the user in regard to the use of Activate Settings.

Granting Masking/Unmasking Capability to SecureSphere Roles and Users

The administrator can grant masking/unmasking capability to SecureSphere roles and users.

To grant masking/unmasking capability to SecureSphere roles and users:

1. Select **Admin > Users and Permissions**.
2. In the **Users & Roles** pane, navigate to the user or role of your choice.
3. Click the **Global Settings** tab.



4. Select the desired masking authorization state



Notes:

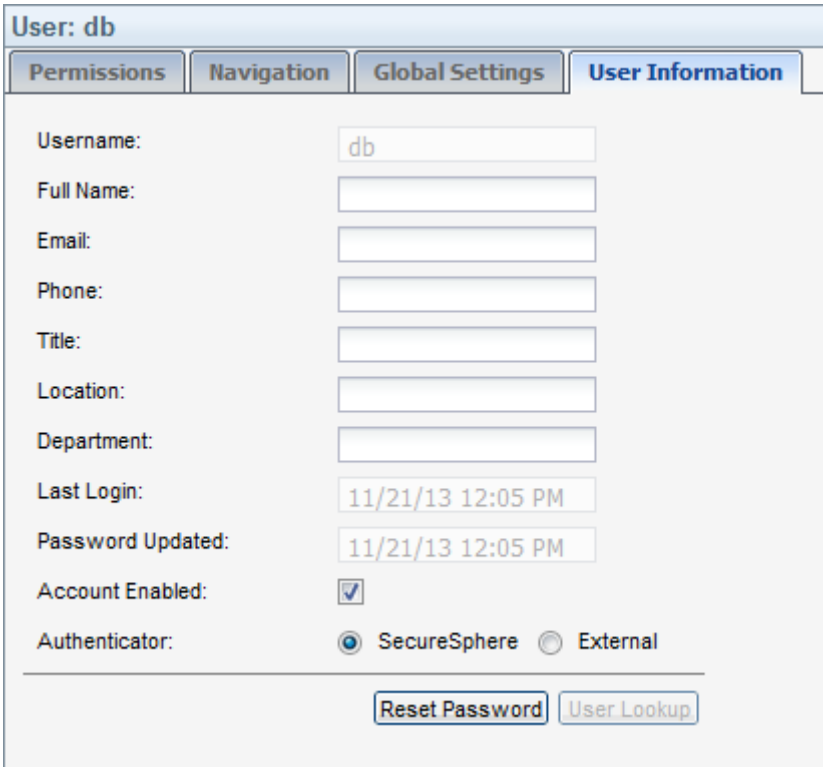
- The administrator always has the masking/unmasking capability.
- If permission is given to a user to configure followed actions, the user could circumvent masking by creating a followed action (e.g. mail, syslog message, etc..) which will include some of the sensitive fields. As a result the followed action data will display all the personal information in its unmasked state. It is recommended that permission to configure followed actions is granted only to those users for whom access to personal information is acceptable. See Action Interfaces on page 270.

Configuring User Information

When creating users it is recommended that you configure all the relevant details to identify that user. This can assist in communicating directly with a user, identifying to what department they belong, knowing their geographic location, and more.

To configure User Information:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, expand the **Users** category, then select the user you whose information you want to edit. That users permissions are displayed in the details pane.
3. Click the **User Information** tab. User Information is displayed.



The **Username**, **Last login**, **Password Updated** fields are informative and cannot be changed in this window. You can enter data into the other fields without restriction.

The following fields are displayed only when a user is not **admin**: **Account Enabled**, **Authenticator** (with **SecureSphere** and **External** options), and **User Lookup** (available when **Authenticator** is **External**). For more information on **Authenticator** and **User Lookup**, see Creating a SecureSphere User on page 200.

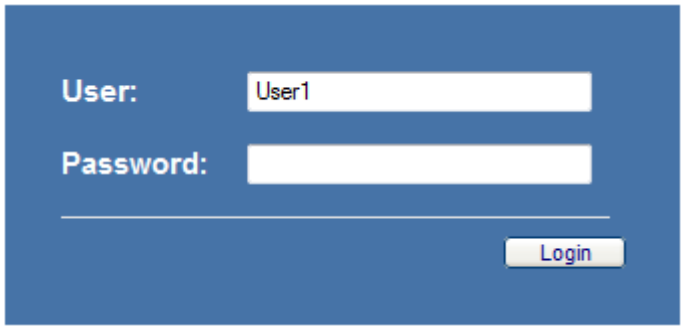


Note: Enable or disable a user's account by selecting or deselecting **Account Enabled**. This field is useful for temporarily disabling a user without having to delete and later re-create the user.

Locking a User Account

A user must type a user name and password to log into the SecureSphere GUI.

If a user types an incorrect password when trying to log in, the user name continues to be displayed and the password field is cleared. The user can try to type a password again.



If a user types an incorrect password 3 times within five minutes, SecureSphere locks the user account for 30 minutes. When the user account is locked, the user cannot log into SecureSphere even with the correct password.

Note: To modify the default values related to locking a user account, see User Lockout Settings on page 269.

To access a user account after it is locked:

- Thirty minutes after the user account was locked, the user must type the correct password.
- If the user forgot the password, the user must:
  - Ask the SecureSphere administrator to reset the password. See Resetting a User Password on page 206
  - Thirty minutes after the user account was locked, type the new password received from the SecureSphere administrator. See Using a Reset User Password on page 208

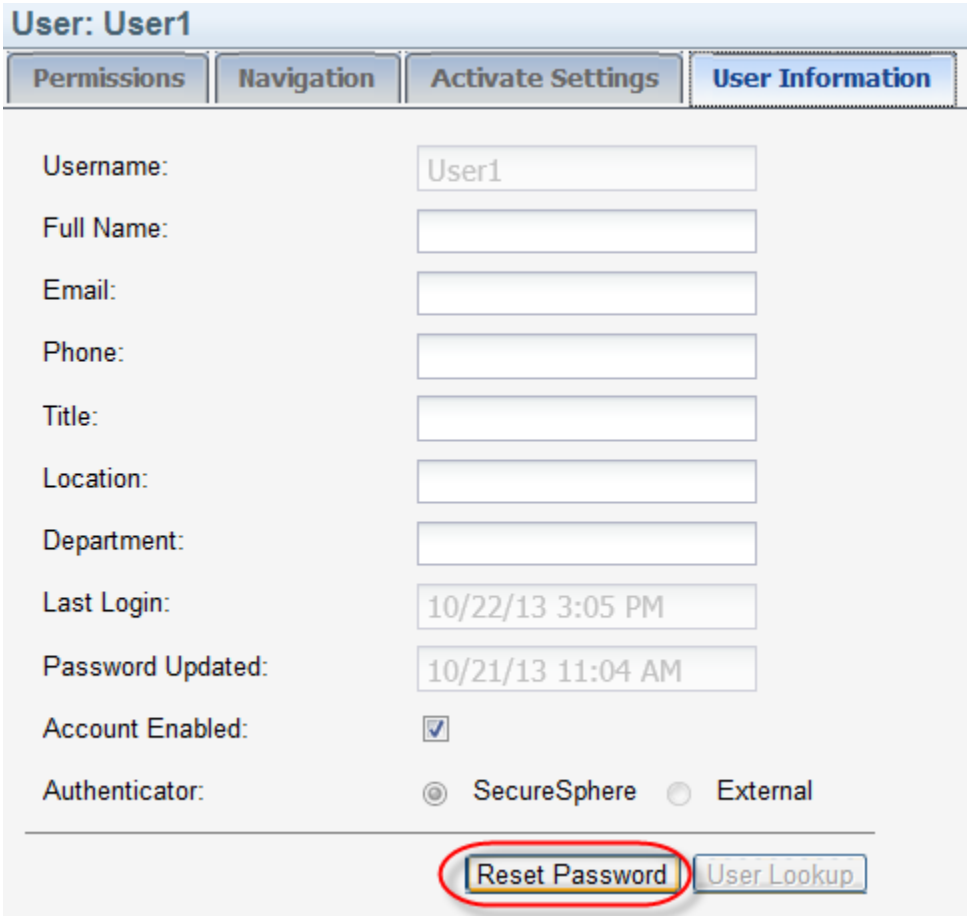
Resetting a User Password

An administrator can reset the password for a user account. This can assist users who forget their password.

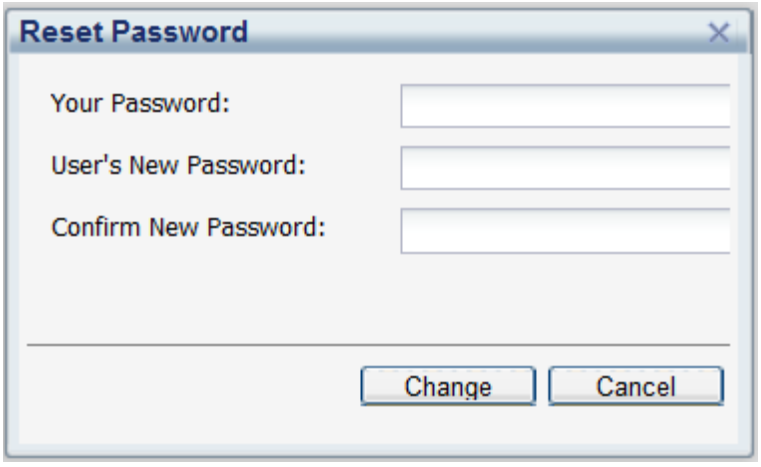
To reset a user password:

1. In the **Admin** workspace, select Users and Permissions.
2. In the **Users & Roles** pane, expand the **Users** category, and then select the user whose password you want to reset.

3. In the details pane, click the **User Information** tab and then click **Reset Password**.



The **Reset Password** window appears.



4. In the **Reset Password** window:
   - In the **Your Password** text box, type your SecureSphere administrator password.
   - In the **User's New Password** text box, type a new password for the user. The password must conform to the restrictions defined in Password Settings on page 268 regarding its length and allowed characters.
   - In the **Confirm New Password** text box, type the new user password again.
   - Click **Change** to save the new user password.

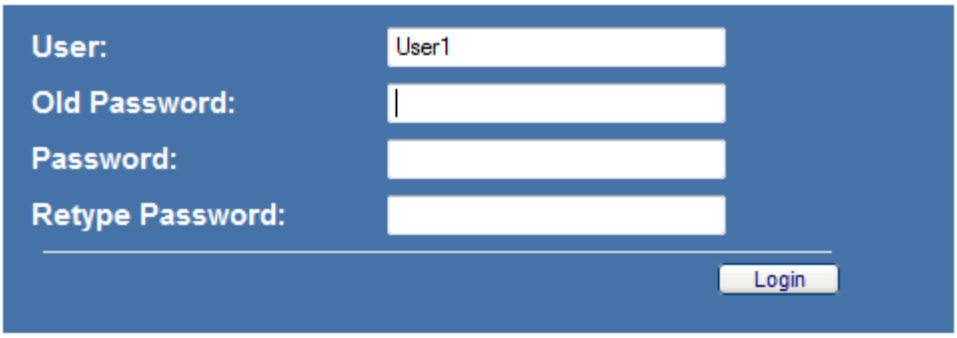
Note: When the user logs in using the reset password, the user must define a new password. See Using a Reset User Password on page 208.

Using a Reset User Password

The first time that a user logs into SecureSphere using a password that was reset by a SecureSphere Administrator, the user must replace the reset password with a new password.

To use a reset user password:

1. In the SecureSphere GUI login window, type the new password from the SecureSphere administrator and click **Login**. A window appears for defining a new password.



2. In the **Old Password** text box, type the password from the SecureSphere administrator.
3. In the **Password** text box, type a new password. The password must:
   - Contain a minimum of seven characters
   - Include at least one numeral
   - Include at least one lower-case letter
4. In the **Retype Password** text box, type the new password again.
5. Click **Login** to log into SecureSphere.

Read-Only User

Read-only user can use SecureSphere for viewing items only. This user cannot add or change anything in the system. You can manage read-only user's permissions by defining which items in the system this user can view.

The default system admin cannot be defined as read-only user. You can define additional admin user in the system and set this user to read-only. By that way you are able to easily add a new user with all the possible permissions and then by setting this user as read-only, you get a user that can view everything and cannot change anything.

You can define a SOM user as read-only. Such user cannot navigate to the Admin tab or drill down to MXs from any location in the SOM GUI. When a SOM read-only user enters MX, this user acts on MX as a read-only user as well.

Additional aspects of working with the read-only user:

- **Roles**: When assigning roles to read only users, these users inherit only the View permissions from these roles. You cannot set a role as read-only, only external roles, see Working with Roles on page 197.
- **Tasks**: Read-only user can open and edit tasks that this user is assigned to.
- **Preferences**: Read-only user can edit the preferences.
- **Save as**: A read-only user can save data as PDF or as CSV.
- **Reports**: A read-only user can run existing reports.



Note: The default system admin cannot be defined as read-only user. You can define additional admin users in the system and set this user to read-only. By that way you are able to easily add a new user with all the possible permissions and then by setting this user as read-only, you get a user that can view everything and cannot change anything.

SOM-MX Issues for Read-Only Users

You can define a SOM user as read-only. Such user cannot navigate to the Admin tab or drill down to any options under Admin. When a SOM read-only user enters MX, this user acts on MX as a read-only user as well.



Note: If a SOM read-only user tries to enter MX version 9.5, which does not have this capability, this user gets an error message.

CHAPTER 9

Sessions

This chapter describes the **Connected Users** window, which displays information about the users currently connected to the SecureSphere GUI, and includes the following:

Connected Users 210

Connected Users

The **Connected Users** pane displays information about the users currently connected to the SecureSphere GUI (that is, have open sessions).

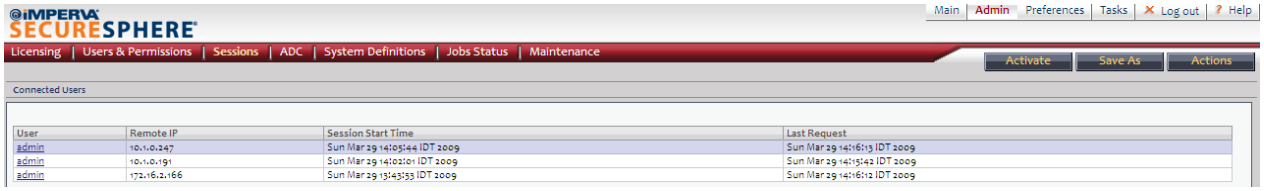


Figure 50: Session Window

For each user, the following information is displayed:

- **User**: The users name.
- **Remote IP**: The IP address from which the user is connected.
- **Session Start Time**: The date and time the session started.
- **Last Request**: The date and time of the last action performed by the user.
  The last action may be something as simple as displaying another tab in the GUI.

Sessions

Administrators can terminate (kill) sessions and disable users.

To kill a session:

1. In the **Admin** workspace, click **Sessions**.
2. In the **Connected Users** pane, select a user.
3. Click **Actions**.
4. From the menu, select **Kill User Session(s)**.

   All the user's sessions will be killed.



Note: An administrator cannot kill his own sessions or disable himself.

To disable a user and kill all of the user's sessions:

1. In the **Admin** workspace, click **Sessions**.
2. In the **Connected Users** pane, select a user.
3. Click **Actions**.
4. From the menu, select **Kill User Session(s) and Disable User**.

   All the user's sessions will be killed and the user will be logged off. The user will not be able to login again until he is enabled (see Working with Users on page 199).

CHAPTER 10

ADC

This chapter describes Imperva's Application Defense Center (ADC).

The Imperva Application Defense Center (ADC) is a premier research organization for security analysis, vulnerability discovery and compliance expertise. ADC research combines extensive lab work with hands-on testing in real world environments to ensure that Imperva's products, through advanced data security technology, deliver up-to-date threat protection and unparalleled compliance automation.

Having discovered dozens of commercial application vulnerabilities and having issued numerous security advisories, the ADC offers exceptional insight into both published and unpublished security threats.

ADC research not only provides an indispensable service to commercial application and database vendors and to security professionals, it also delivers the foundation for many Imperva SecureSphere features and services, including attack signature updates, database vulnerability assessments, and pre-defined compliance reports.

You can view and update ADC content, and view a history of ADC system events.

Viewing ADC Content and Status 213

Updating ADC Content 214

ADC History 215

Viewing ADC Content and Status

To view the status of ADC updates:

1. In the **Admin** workspace, click **ADC**.

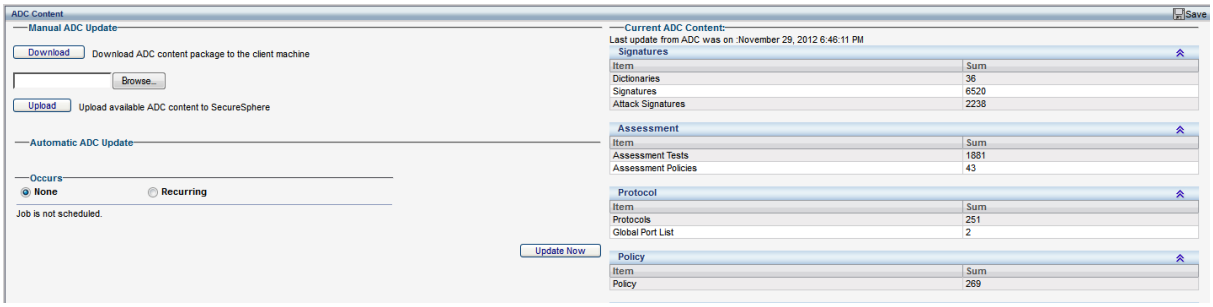


Figure 51: ADC Content window

2. In the **ADC Content** window, information about the ADC content last downloaded is displayed in the right half of the window, under **Current ADC Content**.

   The number of ADC Content items in each category is given under **Sum**.

   To hide the list of items in each category, click  (at the right end).

   To expand a hidden list, click .

   You can view the ADC content in the SecureSphere GUI**, as listed below.**

ADC content

Category	Item	Viewing the ADC Content for this category
Signatures	Dictionaries	In the **Main** workspace, select **Setup** > **Signatures**. The ADC dictionaries are listed under **Predefined Dictionaries** in the **Filter** pane.
	Signatures	In the **Main** workspace, select **Setup** > **Signatures**. Select a dictionary from those listed under **Predefined Dictionaries** in the **Filter** pane. The signatures belonging to the selected dictionary are displayed in the middle pane.
	Attack Signatures	
Assessment	Assessment Policies	In the **Main** workspace, click **Risk Management** > **DB Assessment Policies**. Assessment Policies are displayed.
	Assessment Tests	In the **Main** workspace, click **Risk Management** > **DB Assessment Policies**. Then select a policy from the **Assessment Policies** pane. The tests belonging to that policy are displayed in the **Test List** tab of the rightmost pane.
Protocol	Protocols	
	Global Port List	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **Port Names**. **Note:** The number given under **Sum** for **Global Port List** is the number of lists, not the total number of ports in the lists.

Category	Item	Viewing the ADC Content for this category
Policy	Policies	The various ADC policies can be viewed in several different GUI locations. For example, to view the SAP-related ADC security policies, select **Main** > **Policies** and click **SAP** in the **Filter** pane (under **By ADC Keywords**). The SAP-related ADC security policies are displayed in the **Policies** pane.
Report	Report	In the **Main** workspace, select **Reports** > **Manage Reports** and, in the **Filter** pane, select **ADC** under **Defined By**.
Stored Procedures	Stored Procedures	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **DB Related Objects** > **Stored Procedure Groups** > **Built In**.
Sql Table Groups	Table Groups	In the **Main** workspace, select **Setup** > **Global Objects**. Under **Scope Selection**, select **DB Related Objects** > **Database Table Groups**.
Sql Default Users	Default Users	

Updating ADC Content

ADC content can be updated manually or automatically, on a scheduled basis.



Note: For information about using a proxy for ADC updates, see External HTTP Settings on page 276.

To manually update ADC content:

1. In the **Admin** workspace, click **ADC**.
2. Under **Manual ADC Update**, click **Download**.
3. Save the MPRV file that will be downloaded.
4. Browse to the downloaded file using the **Browse** button.
5. Click **Upload**.

   SecureSphere will be updated with the downloaded content.



Note: Some of the updates will not take effect until you Apply Settings.

To schedule automatic updating of ADC content:

1. In the **Admin** workspace, click **ADC**.
2. Under **Manual ADC Update**, select **Recurring**.
3. Define the schedule for automatic ADC updates.
4. To specify that Activate Settings be performed immediately after a successful automatic update of ADC content, select **Activate Settings**.
5. To update ADC content immediately, click **Update Now**.



Note: For ADC update to succeed, the Default Gateway and the DNS server must be set using `impcfg`.

ADC History

To view the history of ADC-related events:

1. In the **Main** workspace, click **Monitor** > **System Events**.
2. In the **Filter** pane, under **By SubSystem**, select **ADC**. ADC History is displayed.

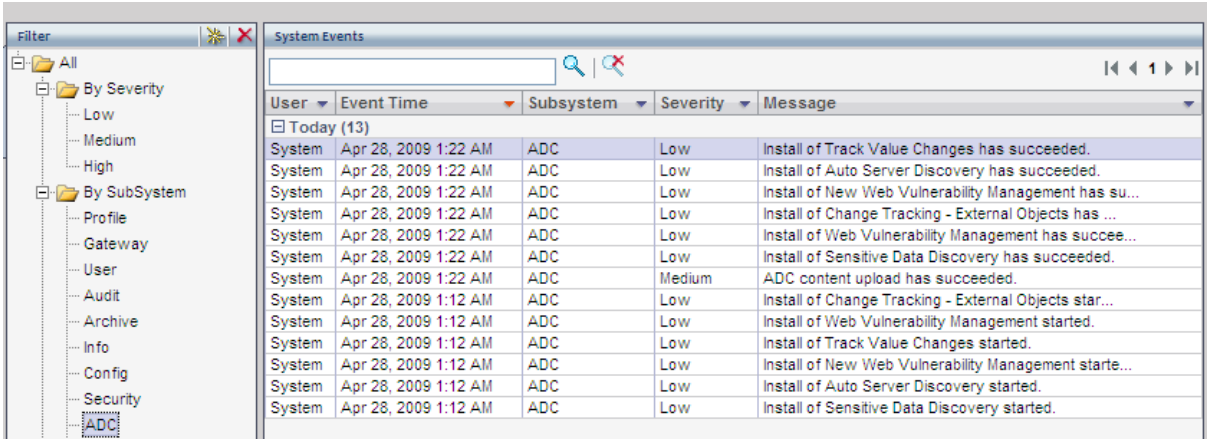


Figure 52: ADC History

CHAPTER 11

Job Status

This chapter describes the **Jobs Status** window, and includes the following:

Jobs Status 217
Displaying the Jobs Status Window 218
Editing a Job 218
Aborting a Job 219
Using the Log to Analyze Jobs 220
Miscellaneous Audit Data Operations 220

Jobs Status

The **Jobs Status** window displays information about jobs which were run, are currently running, or are scheduled to run.

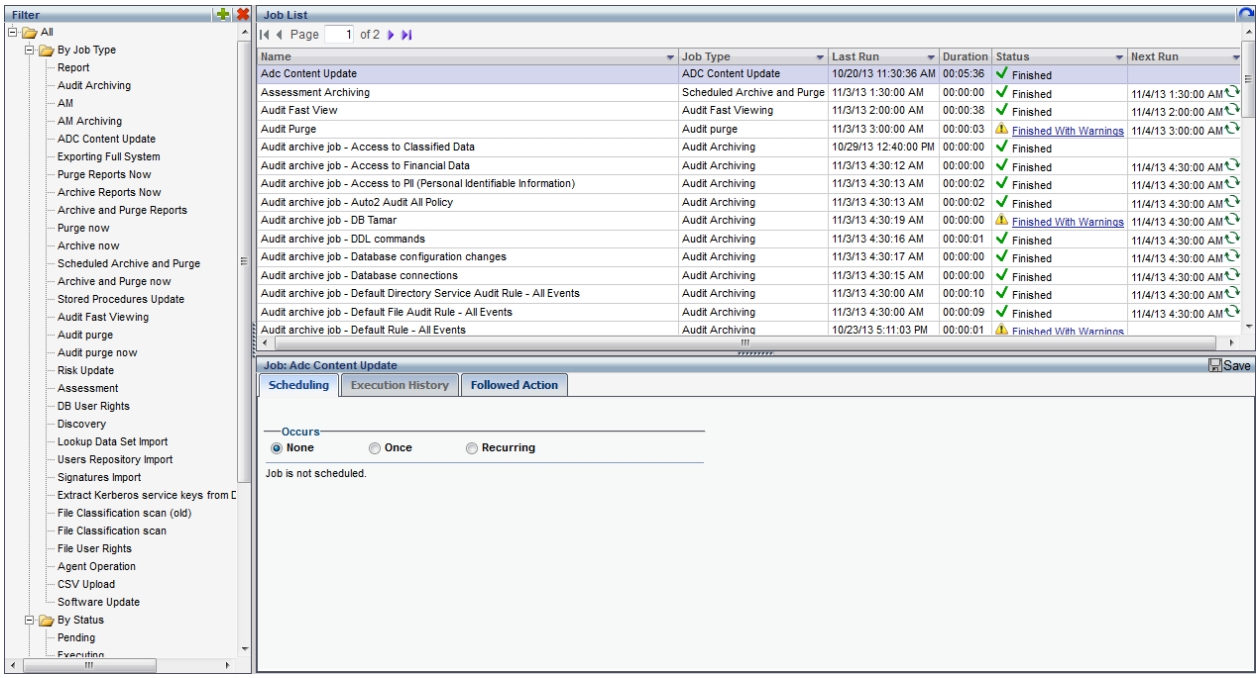


Figure 53: Job List Window

For each job, the following information is displayed:

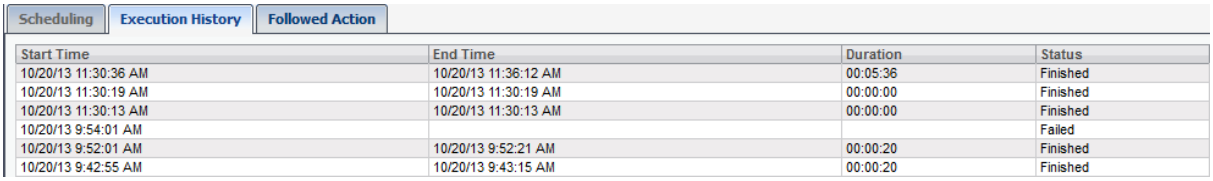
- **Name**: The job's name.
- **Job Type**: The job's type.
- **Last Run**: The date and time the job was last executed.
- **Duration**: If the job is complete, how long it took. If the job is running, how long it has taken thus far.
- **Status**: The status of the job's last execution. If the job's status is not "Finished", you can click on the status to display an explanation of the status.
  - **Finished**: The job was completed.
  - **Executing**: The job is running. The proportion of the job that has been completed (%) is displayed. You can abort an executing job, see Aborting a Job on page 219.
  - **Finished with Warnings**: The job was completed but errors occurred. Click on the link to view a window with details of the warnings.
  - **Failed**: The job failed to complete.
- **Next Run**: The date and time of the next scheduled run.

  The next run icon indicates that the job is recurring. Hover the mouse over the icon to display the schedule.

In the lower pane, there are three tabs which display information about the job currently selected in the **Job List** pane:

- **Scheduling**: This tab displays the schedule for running the job. You can reschedule the job from this tab. See Editing a Job on page 218.

- **Execution History**: A chronologically-ordered list of all executions of the job, with the last execution at the bottom of the list.



- **Followed Action**: This tab displays the job's followed action.

Displaying the Jobs Status Window

To display the Jobs Status **window:**

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, the last execution of jobs which have already run are displayed. You can refresh the list by clicking  in the upper-right corner of the **Job List** pane.

Editing a Job

You cannot change jobs which have already run, or have already started running, but you can change the scheduling and Followed Actions for future executions of a job.

Changing a job's scheduling enables you to ease system congestion if a lot of jobs are being run at the same time and causing load problems.

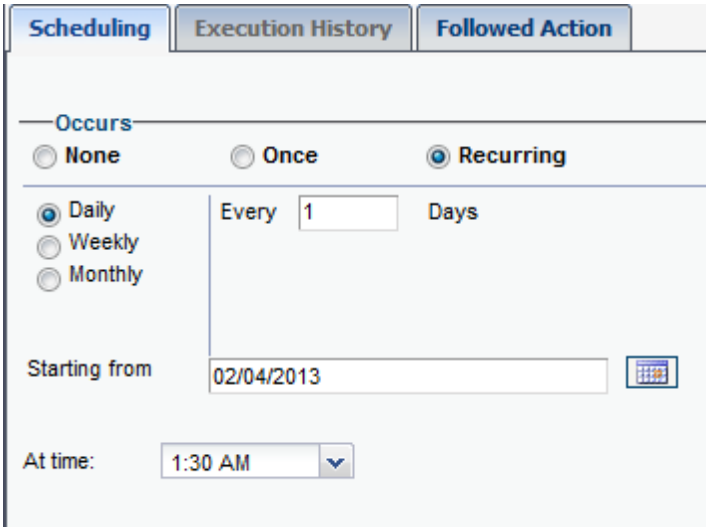


Note: SecureSphere saves a table of your jobs internally, so that in the event of excessive load or other problems, SecureSphere support can access your job schedules and records as a diagnostic aid.

To change a job's scheduling:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, select a job.
4. Click the **Scheduling** tab.
5. Under **Occurs**, select one of the following:
   - **None**: The job is never run.
   - **One Time**: The job is run on the date and time you specify.
   - **Recurring**: The job is run periodically, according to the schedule you define.

6. Configure the date and time you want the job to run, and in the case of a recurring job, the run schedule.



7. Click **Save**.

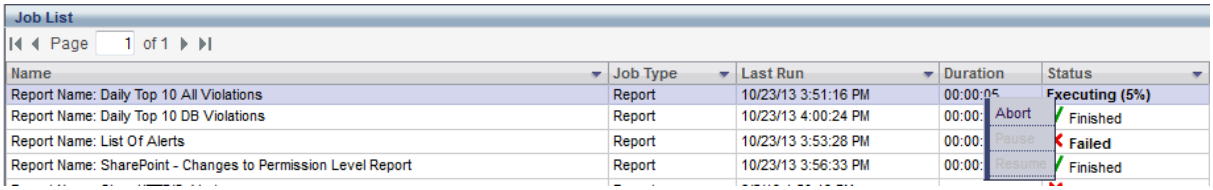
To change a job's followed action:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the **Filter** pane, you can define a filter on the jobs to be displayed in the **Job List** pane.
3. In the **Job List** pane, select a job.
4. Click the **Followed Action** tab.
5. Select a **Followed Action**. For information on creating followed actions, see **SecureSphere User Guide**.
6. Click **Save**.

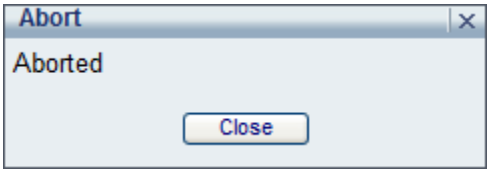
Aborting a Job

To abort a currently running job:

1. In the **Admin** workspace, click **Jobs Status**.
2. In the Job List pane, right-click a job that is executing and select **Abort** from the menu.



3. The **Abort** message appears.



4. Click **Close** to confirm. The job is aborted.



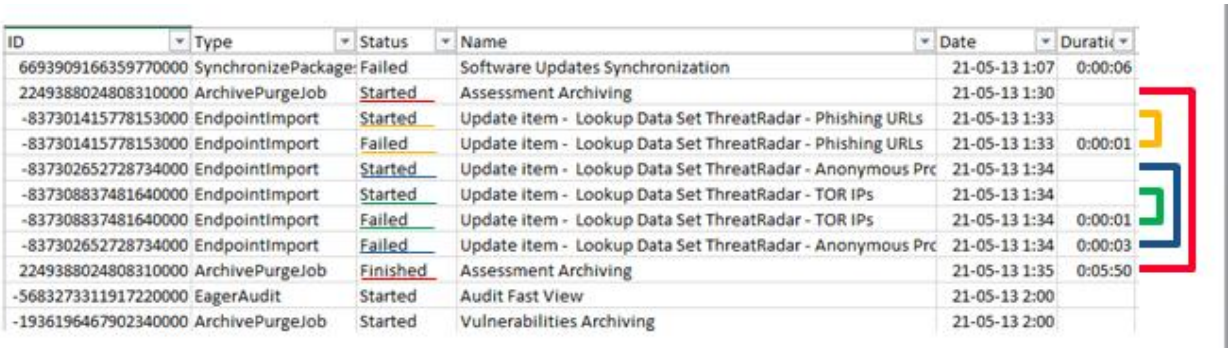
Note: Some jobs cannot be aborted.

Using the Log to Analyze Jobs

Whenever there is a change to the job status, a new line is added to a log file. The file is a .csv file with the following fields:

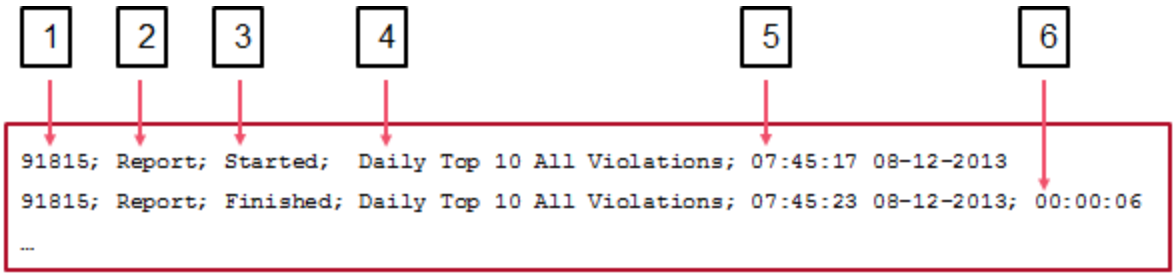
- IDType
- Status
- Name
- Date
- Duration

The image below shows when lines are added to the log file.



ID	Type	Status	Name	Date	Duratic
6693909166359770000	SynchronizePackage	Failed	Software Updates Synchronization	21-05-13 1:07	0:00:06
2249388024808310000	ArchivePurgeJob	Started	Assessment Archiving	21-05-13 1:30	
-837301415778153000	EndpointImport	Started	Update item - Lookup Data Set ThreatRadar - Phishing URLs	21-05-13 1:33	
-837301415778153000	EndpointImport	Failed	Update item - Lookup Data Set ThreatRadar - Phishing URLs	21-05-13 1:33	0:00:01
-837302652728734000	EndpointImport	Started	Update item - Lookup Data Set ThreatRadar - Anonymous Prc	21-05-13 1:34	
-837308837481640000	EndpointImport	Started	Update item - Lookup Data Set ThreatRadar - TOR IPs	21-05-13 1:34	
-837308837481640000	EndpointImport	Failed	Update item - Lookup Data Set ThreatRadar - TOR IPs	21-05-13 1:34	0:00:01
-837302652728734000	EndpointImport	Failed	Update item - Lookup Data Set ThreatRadar - Anonymous Prc	21-05-13 1:34	0:00:03
2249388024808310000	ArchivePurgeJob	Finished	Assessment Archiving	21-05-13 1:35	0:05:50
-5683273311917220000	EagerAudit	Started	Audit Fast View	21-05-13 2:00	
-1936196467902340000	ArchivePurgeJob	Started	Vulnerabilities Archiving	21-05-13 2:00	

An example of the log appears below:



Key:

- Execution ID
- Job type
- State
- Name
- Timestamp
- Duration

The log can be found at `/opt/SecureSphere/server/SecureSphereWork/logs/jobs/job_status.csv`.

Miscellaneous Audit Data Operations

The following procedures are used to configure various aspects of audit operations:

Changing the Audit Directory Path 221
Configuring Encryption 221

Changing the Audit Directory Path

The audit directory path in SecureSphere is configured by default under `var/SecureSphere/audit`. This path can be changed when wanting to store audit data in a different location than the default, including on an external volume.

To change the audit directory path:

1. SSH to the SecureSphere Gateway (or Onebox in Onebox configurations) using the credentials configured by the administrator during SecureSphere installation.
2. Create a mount point and mount the storage drive for the new location.
3. Navigate to the directory containing the `boostrap.xml` file by using the following command (default location):

```
cd /opt/SecureSphere/etc
```

4. Open the `bootstrap.xml` file using a text editor.
5. Modify the audit default settings whose location is indicated in the following:

```
<auditor-default-settings max-records-per-file="1000000"
max-file-size="512000000"                    max-saved-files="1095"
max-aggregated-records="10000" min-free-disk-space="2000000000"
min-free-disk-space-percent="10" low-free-disk-space="4000000000"
low-free-disk-space-percent="15"
audit-base-path="/var/SecureSphere"
use-audit-thread="true" max-records-per-time-slot="10000"/>
```

6. Save the changes and close the text editor.
7. Restart the Gateway. Changes only take effect once restart has been completed.
8. If you already have existing audit data on SecureSphere, you must do one of the following:
   - To keep existing data: Move all data including directories and files from the old directory to the new directory.
   - To purge existing data from the Management Server: Delete data from old directory, and cleanup Fast View data from the Management Server database by clicking **Apply** under **Alert Management Statistics** > **Management Server View** > **Apply**.

Configuring Encryption

You can configure SecureSphere to encrypt audit data located on the Gateway hard disk. Configuring encryption includes activating encryption on each Gateway, which will then manage encryption and decryption of all data on that Gateway, then restarting the Gateway in order for encryption to take effect. By default, encryption is turned off.



Notes:

- Turning encryption on and off does not cause loss of data already collected.
- Enabling encryption can impact system performance.
- Data that was already on the Gateway and not previously encrypted remains unencrypted even if encryption is enabled.

To configure encryption:

1. Login to the Management Server with the user: `root`
2. Execute the following command:

```
impctl gateway config --encryption=T
```



Note: To disable configuration, execute: impctl gateway config --encryption=F

3. Restart the Gateway by executing the following command:

```
impctl gateway restart
```

CHAPTER 12

Maintenance

This chapter describes various system maintenance tasks, and includes:

Audit Fast Viewing 223
Audit Purge 224
Assessment Results Archive 225
Discovery Results Archive 227
Exporting and Importing the Management Server 229
File Explorer Maintenance 236
Reports Archive 236
Risk Score Update 238
Kerberos Key Update 238
System Events Archive 240
Vulnerabilities Purge 241
Extracting Archives for Viewing 243
Audit Archive Conversion 244

Audit Fast Viewing

The **Audit Fast Viewing** window specifies the parameters for retrieving audit data for audit policies.

To define the parameters for audit fast view:

1. In the **Admin** workspace, click **Maintenance**.

2. In the **Maintenance** pane, click **Audit Fast Viewing**.

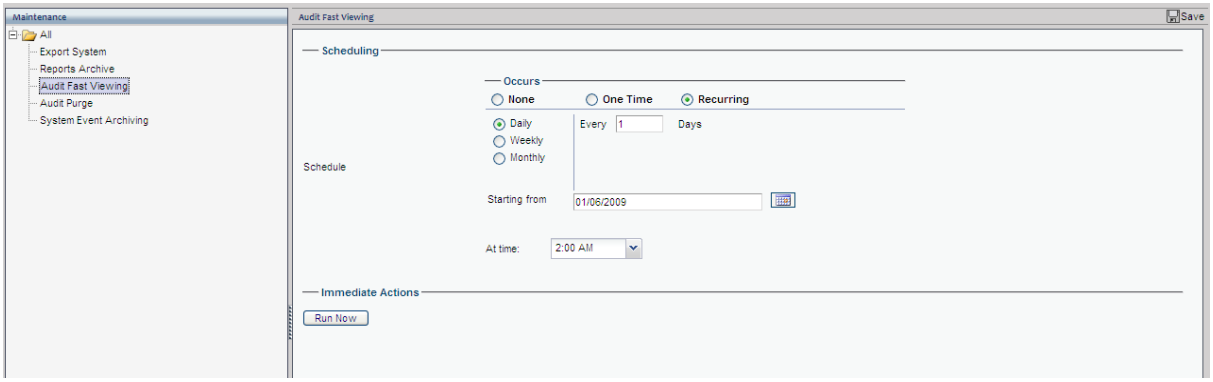


Figure 54: System Maintenance - Audit Fast Viewing

3. In the **Scheduling** section, under **Occurs**, select one of the options in the table **Audit Fast Viewing Scheduling Options** below.
4. Click **Run Now** to retrieve audit data immediately.
5. Click **Save**.

Note: The number of days of audit data retrieved in defined individually for each audit policy.

Audit Fast Viewing Scheduling Options

Parameter	Description
None	Audit data are not retrieved automatically. If this option is selected, the only way to retrieve audit data are to do so manually, by clicking **Run Now**.
Once	Audit data are retrieved automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are retrieved automatically according to the schedule you define.

Audit Purge

The **Audit Purge** window specifies the parameters for purging audit data for all Gateways being managed by SecureSphere.

To configure audit purge per audit policy, you need to configure **archiving** for Audit policies. For more information on configuring audit policies, see the **SecureSphere User Guide**.

To define the parameters for purging audit data:

1. In the **Admin** workspace, click **Maintenance**.

2. In the **Maintenance** pane, click **Audit Purge**.

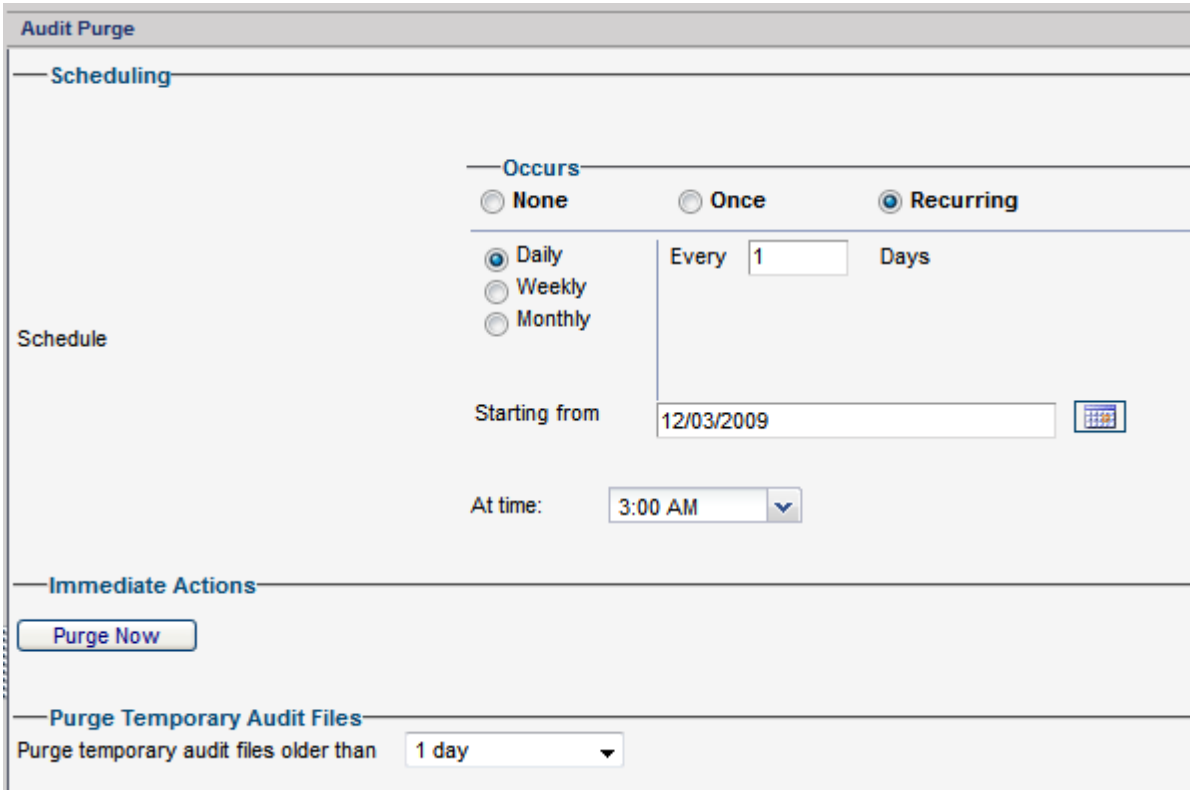


Figure 55: System Maintenance - Audit Purge

3. In the **Scheduling** section, under **Occurs**, select a scheduling option as describe in the table **Audit Purge Scheduling Options** below.
4. Click **Run Now** to purge audit data immediately.

   Before purging, make sure the audit data have been successfully archived.
5. In the **Purge Temporary Audit Files** section, specify how frequently temporary audit files are to be purged.

   Temporary audit files are audit data stored on the MX, either when running a fast view job (see Audit Fast Viewing on page 223) which collects audit data from Gateways on a scheduled basis, or when viewing audit files.
6. Click **Save**.

Audit Purge Scheduling Options

Parameter	Description
None	Audit data are not purged automatically. If this option is selected, the only way to retrieve purge data is to do so manually, by clicking **Run Now**.
Once	Audit data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are purged automatically according to the schedule you define.

Assessment Results Archive

The **Assessment Results Archive** window specifies the parameters for archiving assessment results.

To define the parameters for archiving of Assessment results:

1. In the **Admin** workspace, click **Maintenance**.

2. In the **Maintenance** pane, click **Assessment Results Archive.**

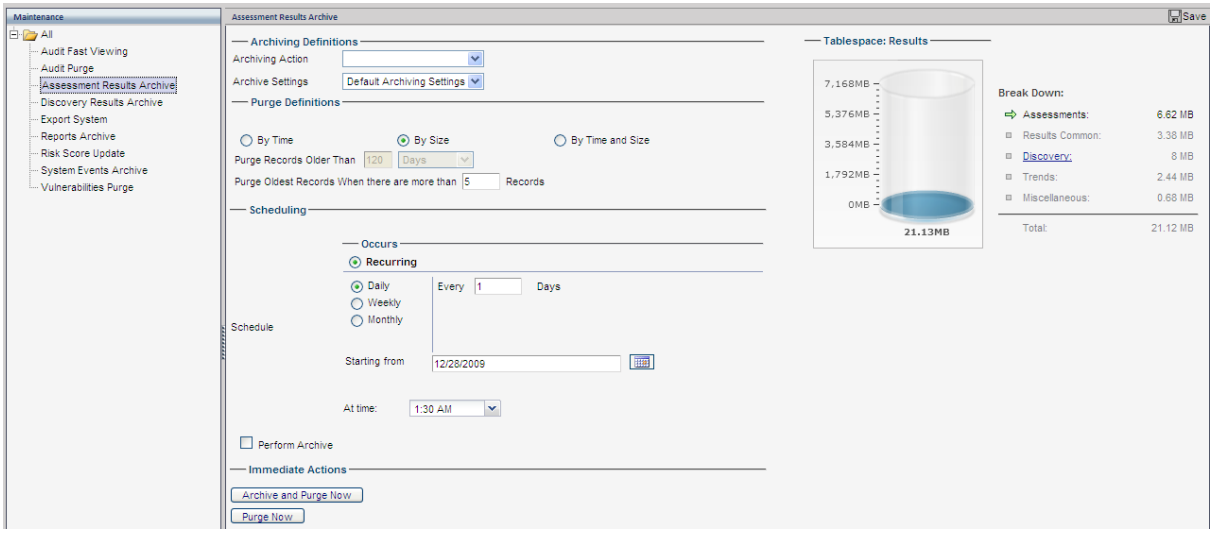


Figure 56: System Maintenance - Assessment Results Archive

3. In the **Archiving Definitions** section, set the parameters shown in the table **Assessment Results Archiving Definition Options** below.



Note: The Archive Setting menu item **Default Archive Settings** does not by default encrypt the archive file. To change these settings, in the **Main** workspace, select **Setup** > **Settings** and then select **Archive Settings** from the **Settings** pane, select **Default Archive Settings** and enter the encryption keys. Alternatively, you can define another archive setting in **Main** > **Setup** > **Settings** and use it here.

4. In the **Purge Definitions** section, select an option as shown in the table **Assessment Results Purge Definition Options** below.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 results are available.

5. In the **Scheduling** section, under **Occurs**, select a Scheduling Option as shown in the table **Assessment Results Purge Scheduling Options** below.
6. Select **Perform Archive** to archive the data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge results data immediately.
9. Click **Save**. For information on how to extract assessment or discovery result archives for viewing in its source format, see Extracting Archives for Viewing on page 243.

Assessment Results Archiving Definition Options

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving assessment results.
Archive Settings	From the menu, select the archive settings.

Assessment Results Purge Definition Options

Parameter	Description
By Time - Purge Records Older Than	Purge results older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of results exceeds the specified number, purge the oldest records.

Assessment Results Purge Scheduling Options

Parameter	Description
None	Results data are not purged automatically. If this option is selected, the only way to purge results data is to do so manually, by clicking **Run Now**.
Once	Results data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Results data are purged automatically according to the schedule youdefine.

Discovery Results Archive

The **Discovery Results Archive** window specifies the parameters for archiving assessment results.

To define the parameters for archiving of Discovery results:

1. In the **Admin** workspace, click **Maintenance**.

2. In the **Maintenance** pane, click **Discovery Results Archive.**

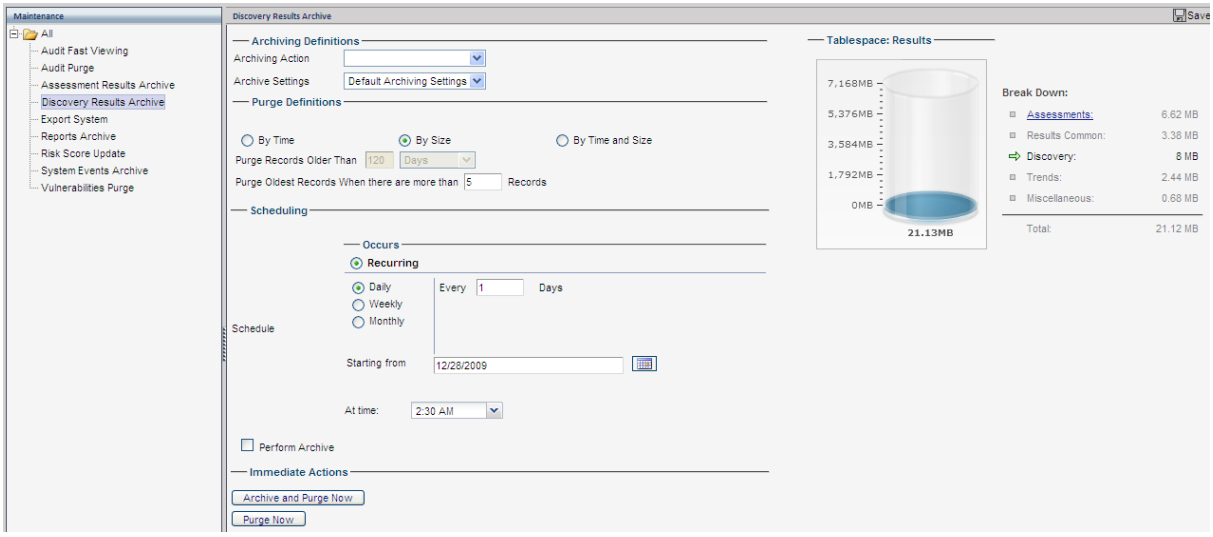


Figure 57: System Maintenance - Discovery Results Archive

3. In the **Archiving Definitions** section, set the parameters as described in the table **Discovery Results Archiving Definitions Parameters** below.



Note: The Archive Setting menu item **Default Archive Settings** does not by default encrypt the archive file. To change these settings, in the **Main** workspace, select **Setup** > **Settings** and then select **Archive Settings** from the **Settings** pane, select **Default Archive Settings** and enter the encryption keys. Alternatively, you can define another archive setting in **Main** > **Setup** > **Settings** and use it here.

4. In the **Purge Definitions** section, select an option as described in the table **Discovery Results Purge Definition Parameters** below.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 results are available.

5. In the **Scheduling** section, under **Occurs**, select a an option as described in the table **Discovery Results Scheduling Options** below.
6. Select **Perform Archive** to archive the data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge results data immediately.
9. Click **Save**. For information on how to extract assessment or discovery result archives for viewing in its source format, see Extracting Archives for Viewing on page 243.

Discovery Results Archiving Definitions Parameters

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving assessment results.
Archive Settings	From the menu, select the archive settings.

Discovery Results Purge Definition Parameters

Parameter	Description
By Time - Purge Records Older Than	Purge results older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of results exceeds the specified number, purge the oldest records.

Discovery Results Scheduling Options

Parameter	Description
None	Results data are not purged automatically. If this option is selected, the only way to purge results data is to do so manually, by clicking **Run Now**.
One Time	Results data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Results data are purged automatically according to the schedule you define.

Exporting and Importing the Management Server

You can export and import the SecureSphere data from the Management Server, including configuration files, the SecureSphere database, and (optionally) alerts data. Any data that arrives at the Management Server after the export operation begins is not included in the export file.

Exporting and importing are useful for the following purposes:

- Copying a database to another machine
- Backing up a database

You can perform these functions in any of the following ways:

- Export using the management interface
- Import and/or export using the interactive command line interface (CLI)
- Import and/or export using the non-interactive command line interface (CLI)



Note: You cannot use the SecureSphere GUI to import a SecureSphere database, because you must stop the SecureSphere Management Server during the import process.

Export Using the SecureSphere GUI

To export a SecureSphere database:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Export System**.

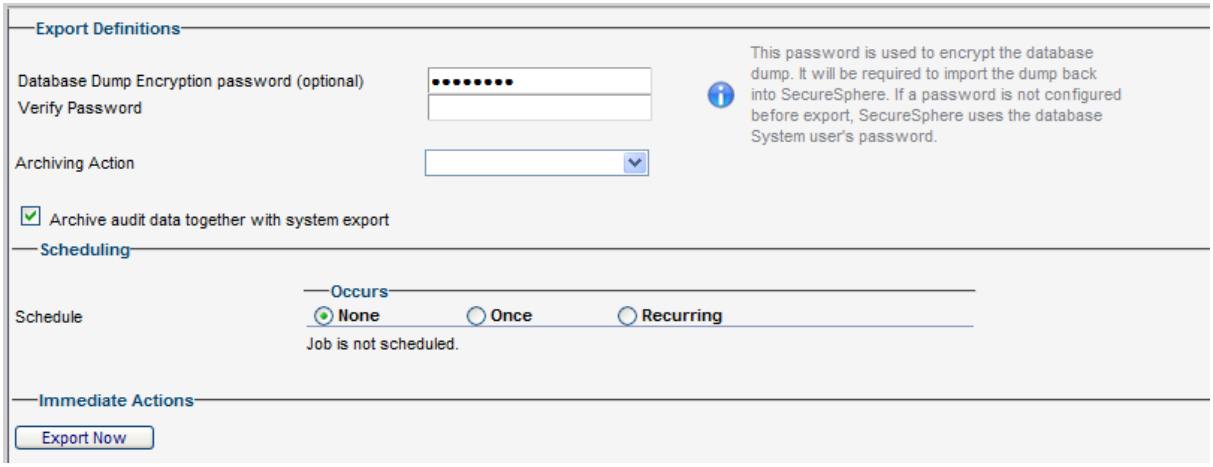


Figure 58: System Maintenance - Export System

3. In the **Export Settings** pane, in the **Export Definition** section, enter data as shown in the table **Export Definition Options** below.
4. Click **Save**.
5. Alternatively, you can perform the export immediately by clicking **Export Now**.

   The name of the export file is of the form: `/tmp/SecureSphere_<date>.dmp.gz`, where `<date>` is the current date in the format YYYYMMDD.
6. In the **Scheduling** section, under **Occurs**, select an option as described in the table Export Scheduling Options below.

Export Definition Options

Parameter	Description
Database Dump Encryption Password	The dump file is always encrypted. You can use the system password (the password of the DBA of the SecureSphere database) or specify another password. To specify another password, enter the password in Database Dump Encryption Password and re-enter the same password in Verify Password. If you do not enter an encryption password, the export file will be encrypted with the system password (the password of the DBA of the SecureSphere database). **Note:** You will not be able to import the encrypted dump file without the password. There is no workaround.
Verify Password	

Archiving Action	Select an Action Set from the dropdown list.
	Note: By default, only the **Default Archive Action Set** is available. To use a different Action Set:
	• Define an Action Interface of type NFS Archive (**Admin** > **System Definitions** > **Action Interfaces**).
	• Define an Action Set of type **Archiving** which uses the Action Interface you defined in the previous step (**Main** > **Policies** > **Action Sets**).
	• In the Action Interface's **Destination Directory**, specify the **Destination Directory** for the archive.
	• If the destination directory is not the default directory (/var/tmp), then you must also ensure that SecureSphere has the required permissions in that directory by executing the following OS commands:
	`chmod 777`
	`chown mxserver:mxserver`
	Select the Action Set you have just configured for **Archiving Action**.

Archive audit data together with system export	Select this option to also export the archive audit data temporarily stored on the MX. This does not export the audit data stored on the Gateways.

Export Scheduling Options

Parameter	Description
None	The export is never scheduled, but you can run it at any time by clicking **Export Now**.
One Time	The export is run on the date and time you specify in **At** and **At Time**.
Recurring	The export is run periodically according to the schedule you define.

Export / Import Manually Using the Interactive CLI



Note: There are at least four users defined on a Management Server:

- root: the OS superuser
- secure: a SecureSphere CLI user, with access only to `impcfg`
- system: the DBA of the SecureSphere database
- admin: a SecureSphere administrator with access to the SecureSphere GUI; any number of SecureSphere administrators and users can be defined



Note: Do not export while the ADC database is being updated, otherwise the exported file will be corrupted.

To export SecureSphere data using the interactive CLI:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command:

```
full_expimp.sh
```

3. Enter the following data when requested:
   - **operation**: Select `1` (export).
   - **system password**: Enter the system password (the password of the DBA of the SecureSphere database).
   - **export type**: Select `1` to export the alert data as well.
   - **export failed archive files:** Select `y` to include failed archive data (default is not to export).
   - **encryption password**: Enter a password for encrypting the dump file (the default is system password, that is, the password of the DBA of the SecureSphere database).
   - **export file**: Enter the name of the export file. The full name of the export file will be `<file_name>.dmp.gz`, where `<file_name>` is the name you enter here.
4. Enter `Y` to confirm the export.

To import SecureSphere data using the interactive CLI:

1. Login to the SecureSphere Management Server as `root`.
2. Stop the SecureSphere Management Server by executing the following command:
   `impctl server stop`
3. Execute the following command:
   `full_expimp.sh`
4. Enter the following data when requested:
   - **operation**: Select `2` (import).
   - **system password**: Enter the system password (the password of the DBA of the SecureSphere database).
   - **import type**: Select `1` to drop the target schema, that is, before starting the import operation, delete the schema on the machine to which the export file is being imported.

     This is the recommended option, since it ensures that the resulting data will consist only of the imported data.
   - **copy option**: Select 1 to copy the configuration files, that is, files not part of the SecureSphere database, for example:
     `SecureSphereWork/firsttime/firsttimeIds`,
     `SecureSphereWork/firsttime/mutableFirsttimeIds`,
     `SecureSphereWork/activated-configuration`

- **secure password**: The password of the SecureSphere CLI user.
- **import file**: Enter the fullpath name of the import file, that is, the previously exported file.

5. You will be asked whether the file is encrypted. If you answer `Y` (the default), then you will be asked to enter the encryption password.
6. Enter `Y` to confirm the import.
7. Start the SecureSphere Management Server by executing the following command:
   `impctl server start`
8. Review the import log for errors or warnings.

Export / Import Manually Using the Non-Interactive CLI

You can export and/or import the SecureSphere data using the `full_expimp.sh` command while specifying the options in the command line.

To export SecureSphere data using the non-interactive CLI:



Note: Do not export while the ADC database is being updated, otherwise the exported file will be corrupted.

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command, adding some or all the additional parameters listed in the following table:
   `full_expimp.sh --operation=1 --pwd=<password> --copyfiles=<copy_option> --logfile=<file_name>" --schema=<schema>`



Note:

- The exported file is always encrypted. The default password is the system password, that is, the password of the DBA of the SecureSphere database), although you can specify a different password using the `pwd` argument.
- The table below lists only the most frequently used import and export options. For a complete list of these options, enter the following command:
  `full_expimp.sh ?`

full_expimp.sh Export Parameters

Parameter	Description
`--dmpfile=<file>`	The destination file for the exported data. If not specified, the default is `/tmp/SecureSphere_<date>` where `<date>` is the current date in the format YYYYMMDD.
`--exptype=<n>`	Specifies whether the export will include alert data: • 1 - include the alert data • 2 - do not include alert data **default**: 1
`--schema=<name>`	Export only the `<name>` schema from the database. If not specified, the script will export the following database schemas: • SECURE • SECURE_DA • all ODM schemas

Parameter	Description
--copyfiles=<copy_option>	Specify 1 to copy the configuration files, that is, files not part of the SecureSphere database, for example: • SecureSphereWork/firsttime/firsttimeIds, SecureSphereWork/firsttime/mutableFirsttimeIds, SecureSphereWork/activated-configuration
--logfile=<file_name>	Specifies the location of the log file.



Note: The SecureSphere database comprises the following schemas:

- SECURE: The SecureSphere configuration and data
- SECURE_DA: Changes made to the SecureSphere configuration which have not yet been applied
- ODM: Active Module schemas

To import SecureSphere data using the non-interactive CLI:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command, adding some or all the additional parameters listed in the following table:
   `full_expimp.sh --operation=2 --pwd=<password> --dmpfile=<file>`



Note:

- The exported file is always encrypted. The default password is the system password, that is, the password of the DBA of the SecureSphere database), although you can specify a different password using the `pwd` argument.
- The table below lists only the most frequently used import and export options. For a complete list of these options, enter the following command:
  `full_expimp.sh ?`

full_expimp.sh Import Parameters

Parameter	Description
--imptype=<n>	Specifies whether the import will first delete imported schemas from the database: • 1 - delete imported schemas from the database • 2 - do not delete imported schemas from the database **default**: 1 If you specify 1 (delete imported schemas), then if the import file includes only one schema, only that schema is deleted from the database. If the import file includes all schemas, the following database schemas are deleted from the database: • SECURE • SECURE_DA • all ODM schemas
--copyfiles=<n>	Specifies whether to import configuration files (files not part of the SecureSphere database), for example: SecureSphereWork/firsttime/firsttimeIds, SecureSphereWork/firsttime/mutableFirsttimeIds, SecureSphereWork/activated-configuration. • 1 - import configuration files • 2 - do not import configuration files

Parameter	Description
`--src=<name>`	Specify this parameter to import only the `<name>` schema from the exported file.
`--dest=<name>`	If you have specified the `--src` parameter, the `--dest` parameter enables you to rename the imported schema in the target database. For example, if the exported file contains the SECURE schema, you can import it to SECURE_OLD by specifying: `--src=secure --dest=secure_old`
`--tbsname=<name>`	Import all the imported objects to the `<name>` tablespace instead of the tablespace they were in the source database.
`--tbsloc=<path>`	This option is set if you want to import the entire data of the imported objects to a specific tablespace instead of the tablespaces they were in the source database.

Listing the Contents of an Exported File

The procedure describes how to list the contents of an exported file.

To list the contents of an exported file:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command:
   `full_expimp.sh`
3. Enter the following data when requested:
   - **operation**: Select `3` (List dump file content).
   - **encryption password**: If the file is encrypted, enter a password (the default password is system password, that is, the password of the DBA of the SecureSphere database).
   - **Enter a file name for the operation**: Enter the fullpath name of a previously-exported file.
4. The output will be similar to the following:

```
full_expimp (version 2.0) started on Sun May  3 15:02:56 IDT 2009

Decompressing dump file
Dump file contains the following schemas:
SECURE
SECURE_DA

Dump contains SecureSphere version: 7.0.0.7014.Release
Dump was created using full_expimp version: 2.0

full_expimp completed successfully on Sun May  3 15:02:57 IDT 2009
```

Miscellaneous Maintenance Tasks

To list the contents of an exported file:

1. Login to the SecureSphere Management Server as `root`.
2. Execute the following command:
   `full_expimp.sh --operation=3 --dmpfile=<file>`

Note: If you import a system setup that was exported from a Onebox appliance to a different Onebox appliance, delete the Gateway from **Setup** > **Gateways** and then re-register the Gateway.

File Explorer Maintenance

When you delete data types and data owners in the **File Explorer**, the disk space used by the data is reclaimed on a daily basis. You can improve **File Explorer** performance by reclaiming the disk space manually.

To immediately reclaim disk space from unused File Explorer data:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **File Explorer Maintenance**.

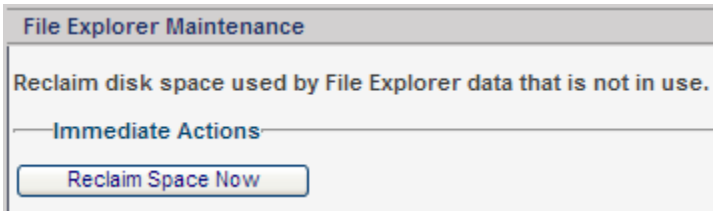


Figure 59: System Maintenance - File Explorer Maintenance

3. Click **Reclaim Space Now**.

Reports Archive

The **Reports Archive** window specifies the parameters for archiving reports.

To define the parameters for archiving reports:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Reports Archive.**

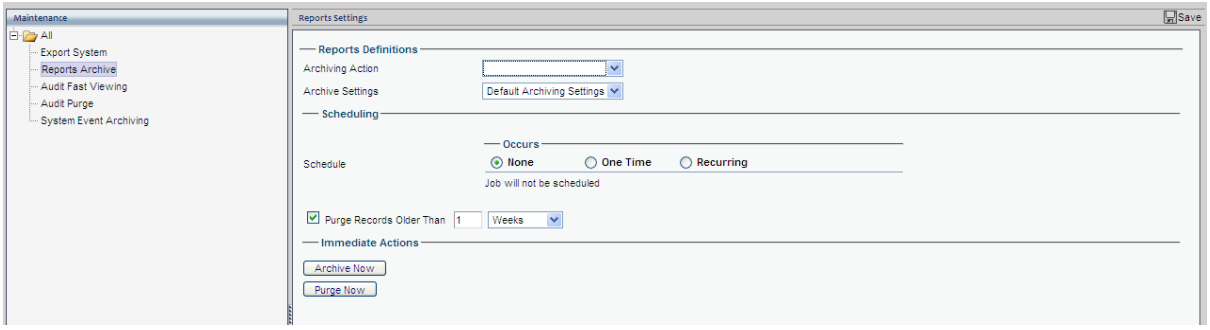


Figure 60: System Maintenance - Reports Archive

3. In the **Reports Definition** section, set the parameters as described in the table **Report Archive Settings** below.

Note: The Archive Setting menu item Default Archive Settings does not by default encrypt the archive file. To change these settings, in the Main workspace, select Setup > Settings and then select Archive Settings from the Settings pane, select Default Archive Settings and enter the encryption keys. Alternatively, you can define another archive setting in Main > Setup > Settings and use it here.

4. In the **Scheduling** section, under **Occurs**, select one of the options as describes in the table **Report Archive Scheduling** below.

5. Click **Archive Now** to archive reports.
6. Click **Purge Now** to purge report data.
   Before purging, make sure the reports have been successfully archived.
7. Click **Save**. Report archiving has been configured. For information on how to extract report archives for viewing in its source format, see Extracting Archives for Viewing on page 243.

Report Archive Settings

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving reports.
Archive Settings	From the menu, select the archive settings.

Report Archive Scheduling

Parameter	Description
None	Reports are not archived automatically. If this option is selected, the only way to archive reports is to do so manually, by clicking **Archive Now**.
One Time	Reports are archived automatically on the date and time you specify in **At** and **At Time**.
Recurring	Reports are archived automatically according to the schedule you define.

Risk Score Update

You can change the frequency of the risk score update.

To change the schedule of the risk score update:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Risk Score Update**.

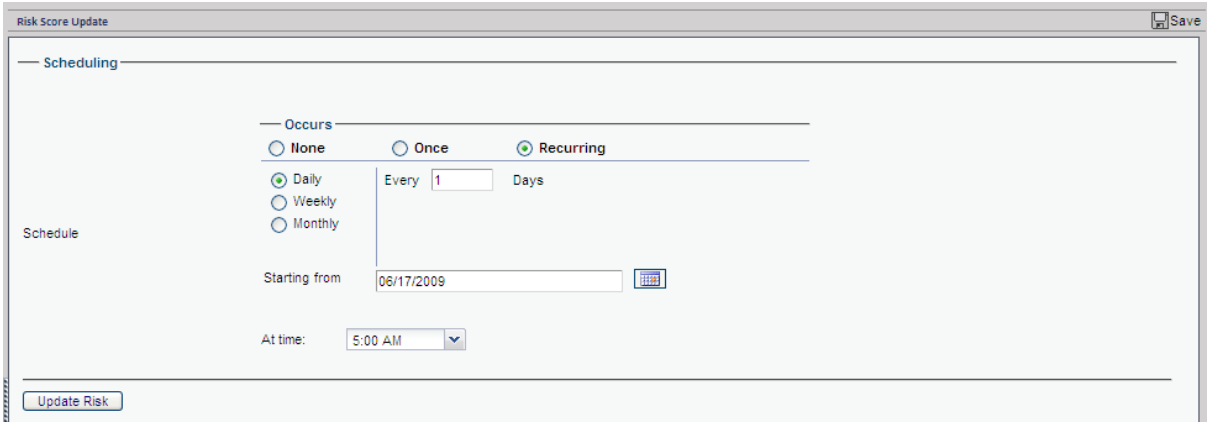


Figure 61: System Maintenance - Risk Score Update

3. In the **Scheduling** pane, under **Occurs**, select an option as described in the table **Risk Score Update Scheduling** below.
4. Click **Save**.
5. To update the risk score immediately, click **Update Now**.

Risk Score Update Scheduling

Parameter	Description
None	The risk score update is never scheduled, but you can update it at any time by clicking **Update Now**.
One Time	The risk score is updated on the date and time you specify in **At** and **At Time**.
Recurring	The risk score is updated periodically according to the schedule you define.

Kerberos Key Update

Kerberos is a protocol used to authenticate and encrypt traffic in client server architectures. When working in a Windows domain, you may need to configure Kerberos support in SecureSphere to decrypt traffic. Configuring Kerberos enables users to be identified and enables the correct display of user names in SecureSphere alerts, reports, and auditing information.



Note: Kerberos support is relevant to CIFS, SharePoint, and MSSQL services only.

You can manage Kerberos keys in the Kerberos Keys table, which you access in the **Main** workspace> **Setup > Global Objects**.

SecureSphere supports RC4, AES128, and AES256 Kerberos encryption types.

For more information, see *Configuring Kerberos Support* in the Imperva SecureSphere User Guides for File Security, Database Security, or SharePoint Security.

To define the parameters for updating Kerberos keys:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **Kerberos Key Update.**

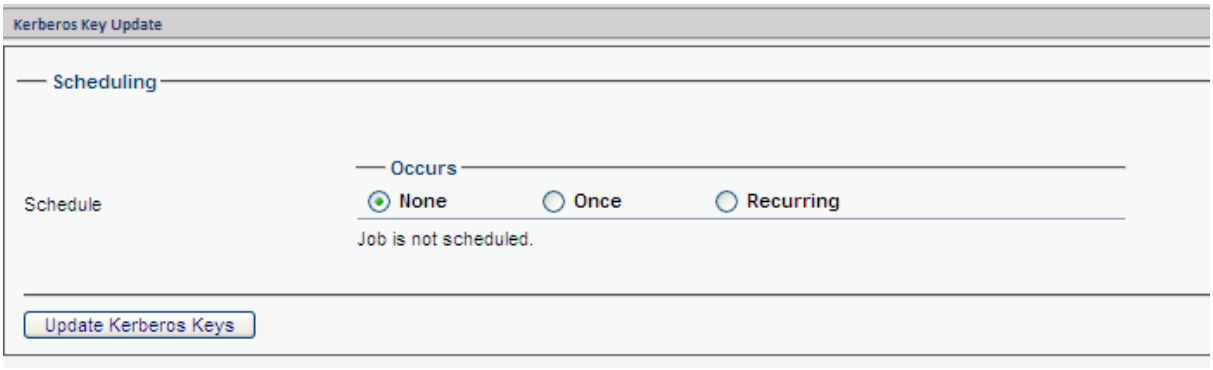


Figure 62: System Maintenance - Kerberos Key Update

3. In the **Scheduling** section, under **Occurs**, select one of the options described in the table **Kerberos Key Update Scheduling** below.
4. Click **Update Kerberos Keys** to update all Kerberos keys immediately.

Kerberos Key Update Scheduling

Parameter	Description
None	Kerberos keys are not updated automatically. If this option is selected, the only way to Kerberos keys is to do so manually, by clicking **Run Now**.
One Time	Kerberos keys are updated automatically on the date and time you specify in **At** and **At Time**.
Recurring	Kerberos keys are updated automatically according to the schedule you define.

System Events Archive

The **System Event Archive** window specifies the parameters for archiving system event data.

To define the parameters for archiving system event data:

1. In the **Admin** workspace, click **Maintenance**.
2. In the **Maintenance** pane, click **System Events Archive.**

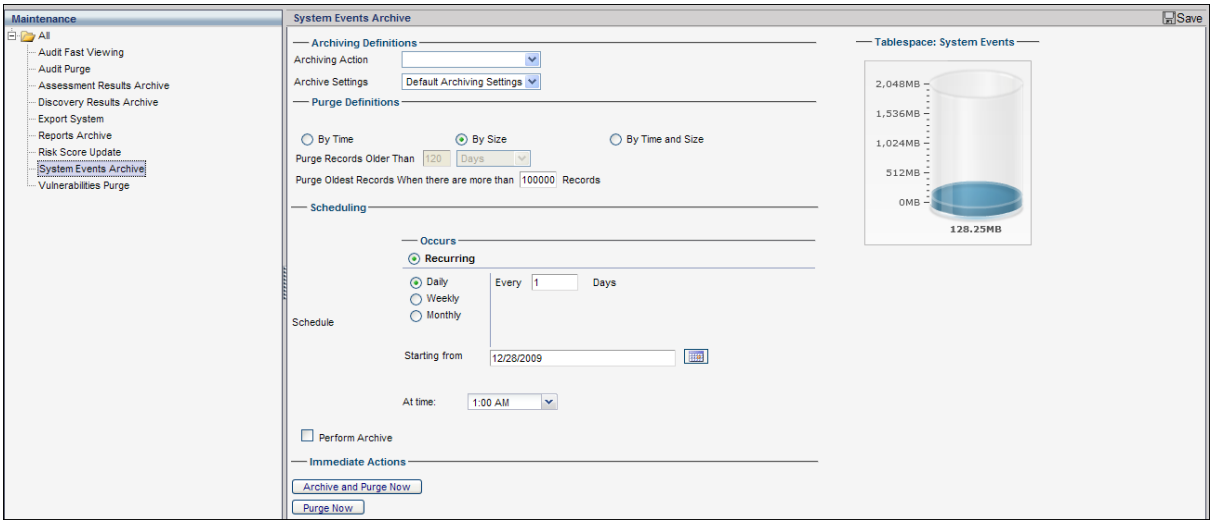


Figure 63: System Maintenance - System Events Archive

3. In the **Archiving Definitions** section, set the parameters described in the table **System Event Archive Settings** below.



Note: The Archive Setting menu item Default Archive Settings does not by default encrypt the archive file. To change these settings, in the Main workspace, select Setup > Settings and then select Archive Settings from the Settings pane, select Default Archive Settings and enter the encryption keys. Alternatively, you can define another archive setting in Main > Setup > Settings and use it here.

4. In the **Purge Definitions** section, select an option as described in the table **System Event Archive Purge Definition Parameters** below.



Note: The default is **By Size - Purge Oldest Records When there are more than Than 100,000 Records**, meaning that by default, no more than 100,000 system events are available.

5. In the **Scheduling** section, under **Occurs**, select an option as described in the table **System Event Archive Scheduling Options** below.
6. Select **Perform Archive** to archive the system event data before purging.
7. Click **Archive and Purge Now** to archive the data immediately then purge it from SecureSphere.
8. Click **Purge Now** to purge the system event data immediately.
9. Click **Save**. For information on how to extract system event archives for viewing in its source format, see Extracting Archives for Viewing on page 243.

System Event Archive Settings

Parameter	Description
Archiving Action	From the menu, select the Action Set to be performed after archiving system events.
Archive Settings	From the menu, select the archive settings.

System Event Archive Purge Definition Parameters

Parameter	Description
By Time - Purge Records Older Than	Purge system events older than the specified age.
By Size - Purge Oldest Records When there are more than Than ... Records	When the number of system events exceeds the specified number, purge the oldest records.

System Event Archive Scheduling Options

Parameter	Description
None	System event data are not purged automatically. If this option is selected, the only way to purge system event data is to do so manually, by clicking **Run Now**.
One Time	System event data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	System event data are purged automatically according to the schedule you define.

Vulnerabilities Purge

The **Vulnerabilities Purge** window specifies the parameters for purging vulnerability data for all Gateways being managed by SecureSphere.

To define the parameters for purging vulnerability data:

1. In the **Admin** workspace, click **Maintenance**.

2. In the **Maintenance** pane, click **Vulnerability Purge**.

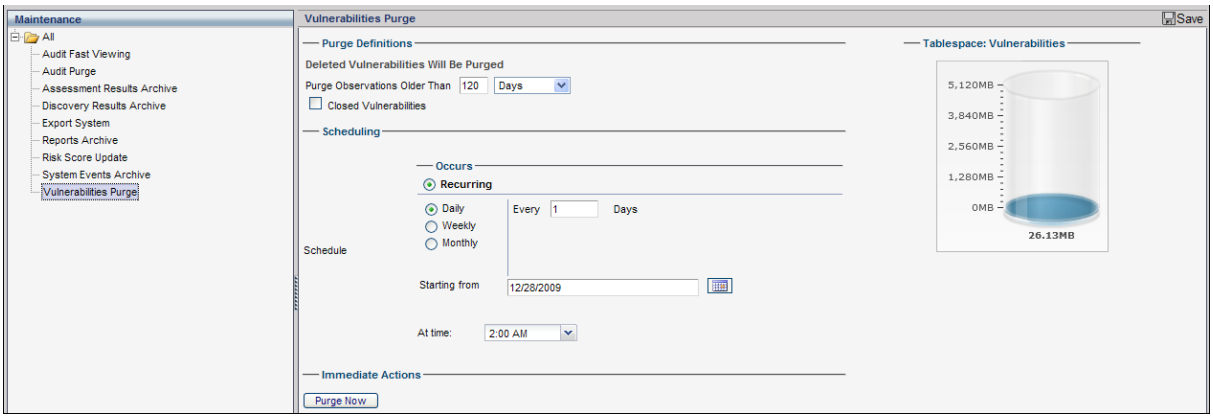


Figure 64: System Maintenance - Audit Purge

3. In the Purge Definitions section, configure the table **Vulnerability Purge Definitions** below.
4. In the **Scheduling** section, under **Occurs**, select an option as described in the table **Vulnerability Purge Schedule Settings** below.
5. Click **Run Now** to purge audit data immediately.

   Before purging, make sure the audit data have been successfully archived.
6. Click **Save**.

Vulnerability Purge Definitions

Parameter	Description
Purge Observations Older Than	Determines the period of time for which vulnerabilities should be purged from SecureSphere. You can enter a number, then a time period that includes days, months weeks and months. For example, you can configure SecureSphere to purge vulnerabilities that have been observed for the past 12 weeks.
Closed Vulnerabilities	When selected, purges all vulnerabilities in the SecureSphere server that have been closed.

Vulnerability Purge Schedule Settings

Parameter	Description
None	Audit data are not purged automatically. If this option is selected, the only way to retrieve purge data is to do so manually, by clicking **Run Now**.
One Time	Audit data are purged automatically on the date and time you specify in **At** and **At Time**.
Recurring	Audit data are purged automatically according to the schedule you define.

Extracting Archives for Viewing

While information that has been archived from SecureSphere cannot be imported back into SecureSphere, it can be extracted and viewed in its source format. This includes the following:

- Reports
- System Events
- Assessment Results
- Discovery Results

To extract and view data that have previously been exported from SecureSphere:

1. Copy the archive file to the SecureSphere server under the `\tmp` directory.
2. Run the following command:

```
java -jar ~mxserver/bin/packagertool.jar -unpack -target <target_dir>
-source <source_mprv_file> -keystore <server_kst_file>
-encAlias <encryption_alias> -sigAlias <signature_alias>
```

   where

   - **source**: The script's source can be either an mprv file to unpack, or a directory of audit files to pack back to an mprv file.
   - **target**: The script's target can be either an mprv file to pack to, or a directory of to unpack the mprv file to.
   - **keystore**: The new version keystore file. On the Server, the file is located at:
   - `/opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kst`
   - **newEncAlias**: New encryption key alias (optional)
   - **newSigAlias**: New signature alias (optional)
   - **encKey**: Old version encryption private key pem file (optional: use if archive is encrypted)
   - **encPass**: Old version encryption password (optional: use if archive is encrypted)
   - **sigKey**: Old version signature private key pem file (optional: use if archive is signed)
   - **sigPass**: Old version encryption password (optional: use if archive is signed)
3. Copy file(s) indicated in the message to your desktop, and rename by adding the extension `.tar`.
4. Extract the contents of the file. The reports contained in the archive are now available for viewing in original (PDF/CSV) format.



Notes:

- To use sigAlias and encAlias on Management Server, list the key's name without its path.
- Key names can be taken from **Setup** > **Archive Settings**.



Note: To repack the CSV files back to an MPRV file, execute:
java -jar ~mxserver\bin\packagertool.jar -pack -target <target_mprv_file> -source <source_dir> -keystore <server_kst_file> -encAlias <encryption_alias> -sigAlias <signature_alias>

EXAMPLE: EXTRACTING A FILE FOR VIEWING

java -jar ~mxserver/bin/packagertool.jar -unpack -target /tmp -source /tmp/archive-reports_20100502-141103_-9031273315142595961.mprv -keystore /opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/conf/securesphere.kst

Audit Archive Conversion

Audit archives can be converted using an action interface to CSV format, which can then be opened and analyzed with external tools such as those used for business intelligence. This section provides instructions on how to use the audit export tool to convert archives previously exported in standard SecureSphere MPRV format versions 6.2 and up. Both of these processes convert archives into CSV format packaged in a single TAR file.

The following procedures for converting and analyzing audit archives are available:

Exporting an Archive to TAR Format with CSV Values 244
Converting an MPRV file to TAR Format with CSV Values 245
Analyzing Converted Files 246

Exporting an Archive to TAR Format with CSV Values

This procedure describes how to configure a SecureSphere Run a Shell Command action interface to export audit files to CSV format and package them in a TAR file. Audit files then archived using this action interface can later be imported into a business intelligence tool and analyzed.

To configure a Run a Shell Command action interface for converting archive data:

1. Create directories in which to store both the unconverted mprv files and the converted CSV files, and change the owner of the directories to `mxserver`, by executing the following commands, substituting your own directory names:

```
mkdir <mprv files directory> <csv files directory>
chown mxserver <mprv files directory> <csv files directory>
```

2. In the SecureSphere **Main** workspace, select **Policies > Action Sets**. The **Action Sets** window appears.
3. In the **Action Sets** pane, click **New**. The **Action Set** dialog box appears.
4. Enter a name for the action set.
5. In the **Apply to** event type drop-down menu, select **Archiving**, then click **OK**. An action set is created.
6. Click the green arrow of the **OS Command** > **Run a Shell Command** action interface. The action interface is moved up to the **Selected Actions** pane.
7. Expand the action interface and configure its parameters as described in the table **Action Interface Parameters for Archive Export** below.
8. From the upper right-hand corner of the screen, click **Save**.

   When audit information is archived using this action interface, they will be packaged as CSV files in a TAR file and saved to the locations you configured in the arguments of the script.

   The log of the script is written to `/var/tmp/archive-convert-full.log and /var/tmp/archive-convert-error.log`

   Due to file size/archiving limits, a single TAR file from a single audit policy may contain multiple, similar values. Special care must be taken to guarantee that it contains only unique values. In order to achieve this you should perform a "select distinct".

   In case one of the files cannot be copied to the target location, it will be written to `/var/tmp/failed_delivery`
9. You should periodically delete the un-needed mprv and the TAR'ed CSV files to free disk space.

Action Interface Parameters for Archive Export

Parameter	Description
Name	Enter a name for the action interface.
Command	`/opt/SecureSphere/server/bin/processArchive.sh`

Arguments	`${Job.file} [OriginalArchiveLocation] [SCPtargetlocation] [OptionalEncryptionAlias] [OptionalSigningAlias]`
	Example:
	`${Job.file} root@10.1.1.21:/tmp/ root@10.1.1.21:/tmp/`
	See below for an explanation of the arguments.

Working Dir	`/opt/SecureSphere/server/bin`

Argument	Description
${Job.file}	A placeholder that indicates the location of the original archive.
[OriginalArchiveLocation]	The SCP location to which the **unconverted** archive should be copied. **Note:** This directory must already exist, and the owner must be set to "mxserver".
[SCPtargetlocation]	The SCP location to which the **converted** archive should be copied. **Note:** This directory must already exist and the owner must be set to "mxserver".
[OptionalEncryptionAlias]	Encryption alias, as used in the Archive Settings (optional)
[OptionalSigningAlias]	Signing alias, as used in the Archive Settings (optional)

Converting an MPRV file to TAR Format with CSV Values

This procedure describes how to use the audit archive tool to repackage MPRV archives previously exported using SecureSphere 6.2 and newer. This process processes binary information added as part of advanced audit archive creation and produces a TAR file containing audit data in CSV format.

To convert MPRV files 6.2 and newer to TAR with CSV:

1. Copy the archives you want to convert to the SecureSphere host.
2. Run the following commands on the desired files using the Command Line.



Note: If the archive is encrypted or signed, you will need to use the relevant keys. Audit files are located at /opt/SecureSphere/server/bin

- chmod +x ./convertAuditFiles.sh
- ./convertAuditFiles.sh

The files are converted to CSV and packaged into TAR format.



Note: Due to file size/archiving limits, a single TAR file from a single audit policy may contain multiple, similar values. Special care must be taken to guarantee it only contains unique values. In order to achieve this you should conduct a "select distinct".

Analyzing Converted Files

Once you have converted your audit archive files to CSV format, you can load them into the desired tool for analysis and run queries as desired.

To analyze converted files:

1. Load the CSV output from the extracted archives into your database.
   - In order to do so, you should understand the format of data and tables that are required. For more information, see Data Format on page 246
   - For an illustration of the relationship between tables see Relationship between Table "Relationship between Tables" on page 248
2. Run queries as required to match your needs, if required use join between the index and events. For a list of sample queries, see Sample Queries on page 248.

Data Format

This section reviews the types of information that are included in the audit archive (SecureSphere 6.2 and newer), after being converted to CSV files using the conversion tool. Use this information to load the CSV files into an external database and create appropriate links between the tables.



Note: When loading results into a non-Oracle database, an equivalent type should be used. For example VARCHAR2(4000 BYTE) should be some kind of string column of at least 4000 bytes. NUMBER(19,0) should be numeric column that supports numbers of 19 digits (decimal), etc.

1. **#.events CSV: table name in SecureSphere - AUDIT_EVENTS.**

   This file includes the following columns and their types (specified as a Oracle type):

   RESPONSE_INFO" VARCHAR2(4000 BYTE),
   "EVENT_ID" NUMBER(19,0),
   "EVENT_CREATION_TIME" DATE,
   "DEBUG_INFO" VARCHAR2(4000 BYTE),
   "STREAM_ID" NUMBER(19,0),
   "SOURCE_PORT" NUMBER(19,0),
   "DESTINATION_PORT" NUMBER(19,0),
   "ORIGINAL_USER_NAME" VARCHAR2(4000 BYTE),
   "RAW_QUERY" VARCHAR2(4000 BYTE),
   "PARSED_QUERY" VARCHAR2(4000 BYTE),
   "BIND_VARS" VARCHAR2(4000 BYTE),
   "URL" VARCHAR2(4000 BYTE),
   "SESSION_ID" NUMBER(19,0),
   "WEB_EVENT_ID" NUMBER(19,0),
   "WEB_SOURCE_IP" VARCHAR2(16 BYTE),
   "EXCEPTION_STRING" VARCHAR2(4000 BYTE),
   "RESPONSE_SIZE" NUMBER(19,0),
   "RESPONSE_TIME" NUMBER(19,0),

"AFFECTED_ROWS" NUMBER(19,0),
"AGENT" VARCHAR2(4000 BYTE),
"LOG_COLLECTOR_NAME" VARCHAR2(4000 BYTE),
"REAL_DATE_TIME" DATE,
"QUERY_GROUP" VARCHAR2(4000 BYTE),
"REPORT_COUNT" NUMBER(19,0),
"TICKET_ID" VARCHAR2(4000 BYTE),
"CUSTOM_TAGS" VARCHAR2(4000 BYTE)



Notes:

- **Delimiter**: The CSV file always includes an extra column (last) with value END. This can be used as a line delimiter ("END\n") for loaders which don't support newline characters inside data.

2. **Index (AKA Keys) - #.crc2key.csv, table name in SecureSphere - AUDIT_KEYS:**
   Includes the following:
   "CRC" NUMBER(19,0),
   "SERVER_GROUP_LC_ID" NUMBER(19,0),
   "SERVICE_LC_ID" NUMBER(19,0),
   "APPLICATION_LC_ID" NUMBER(19,0),
   "EVENT_SOURCE_TYPE" VARCHAR2(20 BYTE),
   "USER_TYPE" VARCHAR2(20 BYTE),
   "DB_USER" VARCHAR2(100 BYTE),
   "SQL_SOURCE_GROUP" VARCHAR2(4000 BYTE),
   "USER_AUTHENTICATED" NUMBER(1,0),
   "APPLICATION_USER_NAME" VARCHAR2(4000 BYTE),
   "SOURCE_IP" VARCHAR2(16 BYTE),
   "SOURCE_APP" VARCHAR2(4000 BYTE),
   "OS_USER" VARCHAR2(4000 BYTE),
   "HOST" VARCHAR2(4000 BYTE),
   "SERVICE_TYPE" VARCHAR2(20 BYTE),
   "DESTINATION_IP" VARCHAR2(16 BYTE),
   "EVENT_TYPE" VARCHAR2(20 BYTE),
   "OPERATION" VARCHAR2(4000 BYTE),
   "OPERATION_TYPE" VARCHAR2(4000 BYTE),
   "OPERATION_OBJECT" VARCHAR2(4000 BYTE),
   "OPERATION_OBJECT_TYPE" VARCHAR2(4000 BYTE),
   "SUBJECT" VARCHAR2(4000 BYTE),
   "DATABASE" VARCHAR2(4000 BYTE),
   "SCHEMA" VARCHAR2(4000 BYTE),
   "TABLE_GROUP" VARCHAR2(4000 BYTE),
   "SENSITIVE" NUMBER(1,0),
   "PRIVILEGED" NUMBER(1,0),
   "STORED_PROCEDURE" NUMBER(1,0),
   "EXCEPTION_OCCURRED" NUMBER(1,0),
   "QUERY_CRC" NUMBER(19,0),
   "RESPONSE_SIZE" VARCHAR2(20 BYTE),
   "AFFECTED_ROWS" VARCHAR2(20 BYTE),

"RESPONSE_TIME_BUCKET" VARCHAR2(20 BYTE),
"USER_DEFINED_TAG_1" VARCHAR2(4000 BYTE),
"USER_DEFINED_TAG_2" VARCHAR2(4000 BYTE),
"IS_TICKET" NUMBER(1,0),



Notes:

- **Delimiter**: The CSV file always includes an extra column (last) with value END. This can be used as a line delimiter ("END\n") for loaders which don't support newline characters inside data.
- **Server Group / Service / Application**: These columns include item ids and not names.

3. **Index to Events Mapping - #.crc2event.csv, table name in SecureSphere - AUDIT_EVENT_TO_KEY:**
   Includes the following:
   "EVENT_ID" NUMBER(19,0),
   "CRC" NUMBER(19,0),
4. **Responses - #.responses.csv, table name in SecureSphere - AUDIT_RESPONSES:**
   Includes the following:
   "EVENT_ID" NUMBER(19,0),
   "RESULT_SET_INDEX" NUMBER(10,0),
   "ROW_INDEX" NUMBER(19,0),
   "COL1" VARCHAR2(4000 BYTE),
   "COL2" VARCHAR2(4000 BYTE),
   "COL3" VARCHAR2(4000 BYTE),

Relationship between Tables

The above tables can be joined in order to query data based on both indexes and events for example, or on events and responses:

- Events table AUDIT_EVENTS column "EVENT_ID" and mapping table AUDIT_EVENT_TO_KEY column "EVENT_ID"
- Index table AUDIT_KEYS column "CRC" and mapping table AUDIT_EVENT_TO_KEY column "CRC"
- Events table AUDIT_EVENTS column "EVENT_ID" and responses table AUDIT_RESPONSES column "EVENT_ID"

Sample Queries

This section lists a number of examples to illustrate the different types of queries that can be used to extract information based on the type of information you wish to extract. The examples below work with the latest versions of Oracle and MSSQL databases, but may not be compatible with other DB types or with older Oracle/MSSQL versions.

In all examples below:

- Results include distinct rows (no duplicates)
- When events is accessed, duplicate event ids (EVENT_ID) are ignored by selecting the row with the highest REPORT_COUNT value

Example 1 (Index Only)

1. Get list of users (DB_USER), and tables/operations that they accessed (OPERATION_OBJECT / OPERATION), sort by user.

```
select distinct
    db_user,
    operation_object,
    operation
from audit_keys
order by db_user;
```

2. Get list of tables/operations that specific user "my_user" accessed (filter), sort by table.

```
select distinct
    operation_object,
    operation
from audit_keys
where db_user='MY_USER'
order by operation_object;
```

3. Get list of users and for each distinct count of the parsed queries (QUERY_CRC) that the user executed, sorted by count.

```
select
    db_user,
    count(distinct query_crc)
from audit_keys
group by db_user
order by count(distinct query_crc) desc;
```

Example 2 (Index + Events)

1. Get list of users and distinct parsed queries (PARSED_QUERY), sorted by user.

```
select distinct
    audit_keys.db_user,
    audit_events.parsed_query
from
    audit_keys,
    audit_events,
    audit_event_to_key
where
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id
order by db_user;
```

2. Get list of tables filtered by specific user "my_user", for each the sum of the following:

```
RESPONSE_SIZE / RESPONSE_TIME / AFFECTED_ROWS. Sorted by table
name.
select
    audit_keys.operation_object,
    sum(audit_events.response_size),
    sum(audit_events.response_time),
    sum(audit_events.affected_rows)
from
    audit_keys,
    (select
response_size,response_time,affected_rows,event_id,row_number(
) over (partition by event_id order by report_count desc) relevant
from audit_events) audit_events,
    audit_event_to_key
where
    audit_events.relevant=1 and
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id and
    audit_keys.db_user='MY_USER'
group by audit_keys.operation_object
order by operation_object;
```

3. Get list of users and full list raw queries (RAW_QUERY) that they executed, with event id (EVENT_ID) and time stamp (EVENT_CREATION_TIME).

```
select distinct
    audit_keys.db_user,
    audit_events.raw_query,
    audit_events.event_id,
    audit_events.event_creation_time
from
    audit_keys,
    (select
raw_query,event_creation_time,event_id,row_number()       over
(partition by event_id order by report_count desc) relevant from
audit_events) audit_events,
    audit_event_to_key
where
    audit_events.relevant=1 and
    audit_event_to_key.crc=audit_keys.crc and
    audit_event_to_key.event_id=audit_events.event_id
order by db_user;
```

Example 3 (Index + Events + Responses)

1. Get all responses (data) that specific user "my_user" retrieved from specific tables "my_table_1" or "my_table_2". This is done by finding events ids matching the filter, then getting all rows from the responses table with this event id.

```
select
    *
from
    audit_responses
where
    event_id in (select audit_events.event_id
                 from audit_keys,
                      audit_events,
                      audit_event_to_key
                 where
                      audit_event_to_key.crc=audit_keys.crc
and

audit_event_to_key.event_id=audit_events.event_id and
                      audit_keys.db_user='MY_USER' and
                      operation_object                      in
('MY_TABLE_1','MY_TABLE_2')
                );
```

CHAPTER 13

System Definitions

This chapter describes the parameters defined under **System Definitions** in the **Admin** workspace, and includes the items listed below:

Dynamic Profiling 252
Gateway Settings 262
Security and Authentication 266
Management Server Settings 270
User Interface Settings 296
ThreatRadar Settings 297

Dynamic Profiling

This section describes the windows related to profiling, and includes the following items:

Learning Exceptions 253
Profile Optimization 253
Profile Size Limits 253
Switching to Protect Mode Thresholds (SQL) 257
Switching to Protect Mode Thresholds (Web) 260

Learning Exceptions

These parameters define exceptions to the Web profile learning process.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Learning Exceptions Window Parameters

Parameter	Description
Don't learn requests that have no referer, unless the response code appears in this list:	As a rule, HTTP requests with no referer information are not learned, unless the target URL was already observed at least once. However, if the request's response codes appears in this comma-separated list, the request will be learned. Specify "none" to indicate no exclusions. **Default**: 200, 304
Don't learn requests with an unknown external host, unless the response code appears in this list:	As a rule, if an HTTP request has a host name which was not yet learned, and the request's referer is external (that is, it does not appear in the list of learned hosts), the request will not be learned. However, if the request's response codes is this comma-separated list, the request will be learned. Specify "none" to indicate no exclusions. **Default**: 200, 304

Profile Optimization

These parameters define exceptions to the profile optimization process.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Profile Optimization Window Parameters

Parameter	Description
Alert Occurrences	The number of times alerts need to take place within Alert Timeframe in Hours to generate an optimization issue.
Alert Timeframe in Hours	The period of time in which the number of alerts need to occur to generate an optimization issue.
Size Limit (%)	The percentage of the Profile Size Limit (see Profile Size Limits on page 253) which, when reached, generates an optimization issue.

Profile Size Limits

When one of these limits is exceeded, SecureSphere stops learning the application and issues a profile size violation system event.

You should not increase any of these values unless there is a compelling reason to believe that the limits will be exceeded, because a profile's size can impact both Gateway and MX performance. If you find yourself regularly exceeding these limits, then you should attempt to address the issue by using URL patterns, plugins or other methods before concluding that the limits must be increased.

The following table lists the parameters in the **Profile Size Limit** pane.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Profile Size Limits Window Parameters

Parameter	Description
Maximum allowed source applications per user	For DB profiles, the maximum number of applications allowed in a user's profile. When this number is exceeded, no additional applications are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any application for the relevant user. **Default**: 1000
Maximum allowed databases per user	For DB profiles, the maximum number of databases allowed in a user's profile. When this number is exceeded, no additional databases are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any database for the relevant user. **Default**: 1000
Maximum allowed source host names per user	For DB profiles, the maximum number of source host names allowed in a user's profile. When SecureSphere reaches this number, no additional host names are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any host for the relevant user. **Default**: 1000
Maximum allowed source IP addresses per user	For DB profiles, the maximum number of source IP addresses allowed in a user's profile. When SecureSphere reaches this number, no additional source IP addresses are added to the relevant profile and a warning message is written to the system log. If the profile reaches this limit, consider allowing any IP address for the relevant user. **Default**: 1000
Maximum allowed source OS users per user	For DB profiles, the maximum number of source operating-system user names allowed in a user's profile. When SecureSphere reaches this number, no additional OS user are added to the relevant profile and a warning message are written to the system log. If the profile reaches this limit, consider allowing any user for the relevant user. **Default**: 1000

Parameter	Description
Maximum allowed hosts per application	For DB profiles, the maximum number of hosts in a profile. When SecureSphere reaches this number, no additional hosts are added to the profile, and they also cannot be learned. **Default**: 4000
Maximum allowed URLs per directory	For Web profiles, the maximum number of URLs profiled in each directory. **Note:** The limit defined by this parameter is not enforced when URLs are added manually, only when they are learned. **Default**: 500
Maximum allowed queries per application	For DB profiles, the maximum number of queries allowed per profile. When SecureSphere reaches this number, no additional queries are added to the profile. **Default**: 3000
Maximum allowed parameters per URL	For Web profiles, the maximum number of different parameter names allowed per URL in the profile. When SecureSphere reaches this number, a certain percentage of the URL's parameters are deleted and a warning message is written to the system log. If these deletions occur repeatedly you should check whether some parameter names are dynamically generated by the application. In this case the profile will never stop growing and you should add a parameter prefix that matches all dynamic parameters. SecureSphere automatically generates parameter prefixes for parameters which start with letters and end with numbers. **Note:** The limit defined by this parameter is not enforced when parameters are added manually, only when they are learned. **Default**: 200
Maximum allowed parameters per application	For Web profiles, the maximum number of different parameter names allowed for each application in the profile. If these deletions occur repeatedly you should check whether some parameter names are dynamically generated by the application. In this case the profile will never stop growing and you should add a parameter prefix that matches all dynamic parameters. Note that SecureSphere automatically generates parameter prefixes for parameters which start with letters and end with numbers. Consult Imperva support before changing this value. **Note:** The limit defined by this parameter is not enforced when parameters are added manually, only when they are learned. **Default**: 3000
Maximum allowed URLs per application	For Web profiles, the maximum number of URLs in each profile. **Note:** The limit defined by this parameter is not enforced when URLs are added manually, only when they are learned. **Default**: 5000

Parameter	Description
Maximum allowed sub-directories per directory	For Web profiles, the maximum number of sub-directories allowed in a single directory in a server group's profile. When SecureSphere reaches this number, no additional sub-directories are added to the relevant directory and a warning message is written to the system log. Note that by default SecureSphere does not profile static URLs (such as image files) so only directories that include dynamic URL such as ASP and JSP files are counted. If the profile reaches this limit you should first check whether some directory names are dynamically generated by the application. In this case the profile will never stop growing and you should consider adding a URL pattern (prefix or suffix) which matches all dynamic directories. **Default**: 500
Maximum allowed parameters per SOAP action	For Web profiles, the maximum number of different parameter names allowed for each SOAP Action in the profile. When this limit is exceeded, no additional elements will be added to the relevant SOAP action and a warning message is written to the system log. **Default**: 100
Maximum allowed database users per application	For DB profiles, the maximum number of database users allowed per profile. **Default**: 100
Maximum database user groups per application	For DB profiles, the maximum number of database user groups allowed per profile. **Default**: 100
Maximum allowed queries per Query Group	For DB profiles, the maximum number of queries allowed per query group in a server group's profile. When SecureSphere reaches this number, no additional queries are added to the relevant query group and a warning message is written to the system log. By default SecureSphere switches query groups with many queries to Dynamic Protect and stops learning additional queries in these query groups. When the profile reaches this limit, check the recommended mode of this query group. If the recommended mode is Dynamic Protect and the query is in either Static Protect or Learning mode, consider manually switching it into Dynamic Protect. **Default**: 2000
Maximum allowed Query Groups per User	For DB profiles, the maximum number of query groups allowed in a user's profile. When SecureSphere reaches this number, no additional query groups are added to the relevant database user and a warning message is written to the system log. If the profile reaches this limit, check whether some query groups are dynamically generated by the application. In this case the profile will never stop growing and you should add an SQL Text Replacement rule which matches all dynamic SQLs. To define a Text Replacement rule, click **Main** > **Setup** > **Sites**, select a DB service, and click the **Operation** tab. You can define a new rule under **Text Replacement**. **Default**: 500

Parameter	Description
Maximum allowed SOAP actions per URL	For Web profiles, the maximum number of SOAP actions allowed for each URL in the profile. When this limit is exceeded, no additional SOAP actions are added to the relevant URL's profile and a warning message is written to the system log. **Default**: 100
Maximum allowed cookies per application	For Web profiles, the maximum number of cookies allowed for each profile. When this limit is exceeded, no additional cookies are added. If this limit is repeatedly exceeded, check whether some cookie names are dynamically generated by the application. In this case, the profile will never stop growing and you should consider adding a cookie prefix which matches all dynamic cookies. **Default**: 200
Maximum allowed action URLs per application	For Web profiles, the maximum number of action URLs allowed for each profile. **Default**: 200
Maximum allowed login URLs per application	For Web profiles, the maximum number of login URLs allowed for each profile. **Default**: 200

Switching to Protect Mode Thresholds (SQL)

The Protect mode thresholds determine when a DB profile's components are switched from Learning mode to Protect Mode.



Note: Do not change these values unless you are instructed to do so by Imperva support.

The table below describes the DB-related parameters in this window.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For further information, see the **SecureSphere User Guide.**

Protect Mode Thresholds (SQL) Window Parameters

parameter	Description
Duration (in hours) without new Query Groups required to close the query group list of a user	If SecureSphere sees no new query groups for a user during this time period, it assumes that it has learned all the query groups for this user and switches the user to Protect mode. You can manually close a users query group list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to test how the system closes the query group list. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 72.0
Duration (in hours) without new table operations required to close a user's operation list	If SecureSphere sees no new table/operations for a user during this time period, SecureSphere assumes that it has learned all the table/operations for this user and switches the user to Protect mode. New query groups which use existing table/operations continue to be learned. You can manually close a users table/operation list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to test how the system closes the tables & operations list. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 72.0
Duration (in hours) without change required to lock the allowed sources and Database-Schema pairs for a Database User	If SecureSphere sees no new item of a specific attribute for a user in Learning mode, the relevant list is locked. New items that belong to the locked list will generate violations (IP Addresses, Host Names, Source Applications, OS User Names and Databases). **Default**: 120.0
Learn individual queries for regular Query Groups	If not selected, new query groups will immediately be switched to protect mode. This is a global setting which applies to all users, but it can be overwritten for specific database profile user group as follows: in the **Main** workspace, click **Profiles** and select a database application in the **Sites** tree. In the **Users** pane, select a user group and, in the **Details** pane, click the **Learning Preferences** tab and under **Learn Individual queries for regular (DML) Query Groups**, select one of the parameters. **For more information, see SecureSphere User Guide.** **Note:** This feature applies to the profile and does not affect the audit mechanism.

parameter	Description
Number of queries required to switch the "stored procedures" Query Group into Dynamic Protect	When the number of queries in the "stored procedures and other operations" query group exceeds this number, the group is switched to Dynamic Protect mode. This number is by default identical with Maximum allowed queries per Query Group defined in the **Profile Size Limits** window; if you reduce Maximum allowed queries per Query Group, you should reduce this threshold accordingly. This is a global setting which applies to all users, but it can be overridden for specific database profile user group as follows: in the **Main** workspace, click **Profiles** and select a database application in the **Sites** tree. In the **Users** pane, select a user group and, in the **Details** pane, click the **Learning Preferences** tab and under **Number of queries required to switch the "stored procedures" Query Group to Dynamic Protect**, select one of the parameters. **For more information, see SecureSphere User Guide.** **Note:** This feature applies to the profile and does not affect the audit mechanism. **Default**: 2000
Number of queries required to switch a regular (DML) Query Group into Dynamic Protect	When the number of queries in a query group exceeds this number, the query group is switched to Dynamic Protect. The assumption is that this query group consists of dynamically generated queries. This parameter applies to all query groups except the "stored procedures and other operations" query group. **Default**: 200
Duration (in hours) without new Query Groups required to close the query group list of a user	The query group learning transition period is the number of hours during which there are no new query groups for a user in learning. After this time, the user's query group list is closed and the user enters protected mode. Once in protected mode, any query group not in the users list will generate a violation. The assumption is that after the learning transition period, the SecureSphere has learned all query groups for this user and can start protecting it. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 120 **Note:** You can manually close a users query group list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to effectively test how the system closes the query group list.

parameter	Description
Duration (in hours) without new Users required to close the users list	A Learning mode server group's user list is closed if no new users have been added to the group in this timeframe. The assumption is that SecureSphere has learned all users for this server group and can start protecting it. The minimum value of this parameter is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Default**: 168 **Note:** Any new query groups which use existing table/operation combinations can still be learned. You can manually close a users table/operation list, either completely or only for sensitive tables. For testing purposes (in a lab with low traffic levels) consider changing this limit to 24 to effectively test how the system closes the tables and operations list.

Switching to Protect Mode Thresholds (Web)

These thresholds determine when a Web profile's components are switched from Learning mode to Protect mode.



Note: Do not change these values unless you are instructed to do so by Imperva support.

The table below describes the Web-related parameters in this window.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For further information, see the **SecureSphere User Guide.**

Protect Mode Thresholds (Web) Window Parameters

Parameter	Description
Traceability Percentage required to switch a cookie into partial Protect mode **Traceability Percentage required to switch a cookie into full Protect mode** **Duration (in hours) required to switch all Cookies to protect or ignored mode** **Minimum occurrences required to switch a cookie into Protect mode**	These four parameters taken together determine when a cookie is switched from Learning mode. If the parameters **Duration (in hours) required to switch all Cookies to protect or ignored mode** and **Minimum occurrences required to switch a cookie into Protect mode** are both exceeded, then: • If the cookie was not changed during at least the number of sessions defined by **Traceability Percentage required to switch a cookie into partial Protect mode**, the cookie is switched to Protect mode without protection against injection. • If SecureSphere saw the SET cookie command for at least the number of sessions defined by **Traceability Percentage required to switch a cookie into full Protect mode**, and the cookie was not changed during at least the number of sessions defined by **Traceability Percentage required to switch a cookie into full Protect mode**, the cookie is switched to Protect mode with protection against injection. Note that **Traceability Percentage required to switch a cookie into partial Protect mode** and **Traceability Percentage required to switch a cookie into full Protect mode** are percentages, not absolute numbers, and relate to a percentage of the total sessions seen by SecureSphere. The minimum value of **Duration (in hours) required to switch all Cookies to protect or ignored mode** is 24 hours. If it is set to a smaller value, SecureSphere considers it as if it were set to 24 hours. **Defaults**: **Traceability Percentage required to switch a cookie into partial Protect mode**: 95.0 **Traceability Percentage required to switch a cookie into full Protect mode**: 95.0 **Duration (in hours) required to switch all Cookies to protect or ignored mode**: 240.0 **Minimum occurrences required to switch a cookie into Protect mode**: 10
Duration (in hours) required to switch all URLs to Protect mode	A URL is automatically switched to Protect mode based on the following factors: • the number of occurrences in the traffic • whether the URL has parameters • the time passed since it was first seen by SecureSphere The more frequently the URL occurs in traffic, the sooner it is switched to Protect mode. This parameter specifies the number of hours since the first time this URL was seen after which the URL is automatically switched to Protect mode, without regard to the number of its occurrences in the traffic or whether it has parameters. **Default**: 240.0

Parameter	Description
Success rate required to set a specific parameter as read-only	If a parameter has been seen **Number of occurrences required to determine if a parameter is read-only** times, it is set to read-only, if in Success rate required to set a specific parameter as read-only percent of the time it was successfully identified as read-only. If you are testing the system in a lab with a low amount of traffic, consider changing this parameter to 50, in order to be able to test the system and the way it sets parameters as read-only. The lower this number, the greater the chances of false positives and false negatives. **Default**: 99.9
Number of occurrences required to determine if a parameter is read-only	See the previous parameter. If you are testing the system in a lab with a low amount of traffic, consider changing this parameter to 6 in order to be able to test the system and the way it sets parameters as read-only. The lower this number, the greater the chances of false positives and false negatives. **Default**: 10

Gateway Settings

This section describes the windows related to Gateways, and the items below:

Audit Settings 263
Response Page Display in Alerts Settings 263
Web to Database User Tracking Settings 264
Configuring Traffic Distribution Analysis 264

Audit Settings

These parameters relate to auditing of responses and paths.

Audit Settings Window Parameters

Parameter	Description
Enable support for queries or full-paths larger than 4k	When enabled, the SecureSphere Gateway preserves the entire path or query regardless of size. If not enabled, only the first 4K of queries or paths are preserved.
Collect audit data from unapplied policies	When enabled, SecureSphere collects audit data from all Gateways, including Gateways on which the audit policy is not applied. This option is useful if the audit policy has been unapplied from some Gateways, in which case these Gateways may be holding relevant audit data even though the policy is no longer applied on them. When not enabled, SecureSphere collects audit data only from Gateways on which the audit policy is currently applied. This parameter affects the policies which are displayed in the following windows: • **Policy** in the **Scope** pane of **Main** > **Audit** > **<Product Name> Audit Data**. • **Policies** in the **Data Scope** tab of **Main** > **Reports** > **Manage Reports**.
File Audit Settings	You can move the listed audit fields between Phase 1 (**Aggregated Data**) and Phase 2 (**Event Data**) by checking the radio button next to the name of each field. The setting takes effect immediately for audit data generated in the future. Existing audit files are not affected by changes to these parameters.
SharePoint Audit Settings	You can move the listed audit fields between Phase 1 (**Aggregated Data**) and Phase 2 (**Event Data**) by checking the radio button next to the name of each field. The setting takes effect immediately for audit data generated in the future. Existing audit files are not affected by changes to these parameters.

Response Page Display in Alerts Settings

These parameters relate to the display of response pages.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Response Page Display in Alerts Settings Window Parameters

Parameter	Description
Maximal disk space on gateway for responses	Maximum disk space on Gateway that will be allocated for responses (in MB). When this disk space fills up, new response pages will overwrite old ones. **Default**: 5000 MB
Maximal response page size	The maximum response page size (in KB.) **Default**: 1000 KB

Web to Database User Tracking Settings

These parameters define the web to database user tracking functionality. You should consult with Imperva support before changing any of these parameters.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Web to Database User Tracking Settings Window Parameters

Parameter	Description
Learning Mode	This parameter defines a balance between the speed of learning and its accuracy. Choose one of the following options: • **Quick**: Learn quickly but with a loss of accuracy. This is the default. • **Refined**: Monitor activity over a greater length of time in order to improve accuracy. The correlation requires more repeated confirmations before it is learned. The learning process is slower, but it is more accurate.
Maximum Pending Request Time (seconds)	Web to Database User Tracking matches the start of an HTTP request to the data returned (ultimately from SQL statements) in response to the request. This parameter defines the maximum time SecureSphere will wait before concluding that there was no response to the request. The default value (10 seconds) is very "patient", which allows for delayed topology options such as using a SecureSphere SecureSphere Agent in Global Mode to send correlation packets to the SecureSphere Gateway.
Pending HTTP Request End At	This parameter defines the event at which the request ends. Choose one of the following options: • **Response Headers** • **Response Data Start** • **Response Complete**
Pending HTTP Request Start At	This parameter defines the event at which the response begins. Choose one of the following options: • **Request Complete** • **Request Headers**

Configuring Traffic Distribution Analysis

The traffic distribution analysis feature provides information about the database traffic processed by SecureSphere Agents which can assist administrators in configuring SecureSphere Agent Monitoring Rules Overview to reduce the amount of data processed by SecureSphere Agents and sent to the Gateway.

In this window (**Admin** > **System Definitions** > **Traffic Distribution Analysis**) you can configure the parameters for the traffic distribution analysis feature.

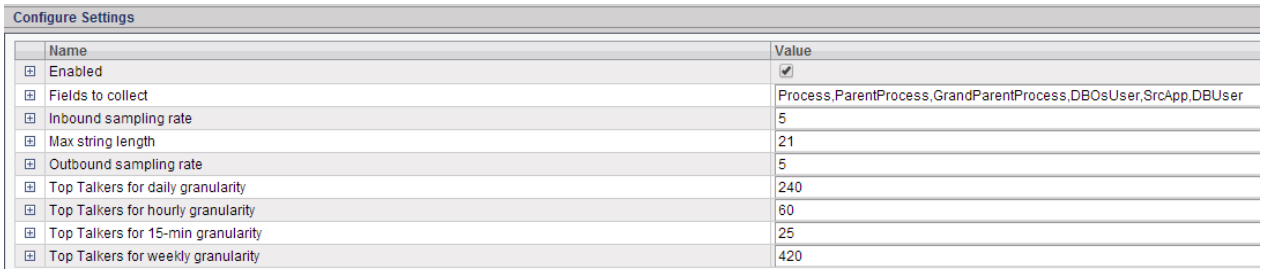


Figure 65: Traffic-Distribution-Analysis

Name	Description
Enabled	Check this option to enable the traffic distribution analysis feature. The feature will be enabled for the first 100 SecureSphere Agents defined on the MX.
Fields to collect	A comma-separated list of the fields to be collected. The available field names are: • Process - the process from which the traffic originated • ParentProcess - the parent of Process • GrandParentProcess - the parent of Parent Process • DBOsUser - The OS user name of the user who originated the traffic. • SrcApp - The source application which originated the traffic. • DBUser - The DB user name of the user who originated the traffic. For fields that are not collected, records that differ only by those fields are aggregated to the same record. In addition to the fields selected here, the following fields are also collected: • SecureSphere Agent ID • interface • source IP address • destination IP address • destination port These fields are also taken into account in calculating the "top talkers" (see below).
Inbound sampling rate	Sample only every *n*th packet and ignore the rest. For example, 5 means sample only every fifth packet, thus ignoring 4 out of 5 packets.
Max string length	Only the first *n* characters of every string will be collected.
Outbound sampling rate	Sample only every *n*th packet and ignore the rest. For example, 5 means sample only every fifth packet, thus ignoring 4 out of 5 packets.
Top Talkers for daily granularity	On a daily basis, SecureSphere aggregates traffic for each SecureSphere Agent only for the first *n* unique combinations of **Fields to collect** with the most traffic (the "top talkers"), where "traffic" includes inbound and outbound traffic, both handled and ignored.

Name	Description
Top Talkers for hourly granularity	For each 2 hour period, SecureSphere aggregates traffic for each SecureSphere Agent only for the first *n* unique combinations of **Fields to collect** with the most traffic (the "top talkers"), where "traffic" includes inbound and outbound traffic, both handled and ignored.
Top Talkers for 15-min granularity	For each 15 minute period, SecureSphere aggregates traffic for each SecureSphere Agent only for the first *n* unique combinations of **Fields to collect** with the most traffic (the "top talkers"), where "traffic" includes inbound and outbound traffic, both handled and ignored.
Top Talkers for weekly granularity	For each weekly period, SecureSphere aggregates traffic for each SecureSphere Agent only for the first *n* unique combinations of **Fields to collect** with the most traffic (the "top talkers"), where "traffic" includes inbound and outbound traffic, both handled and ignored.

Security and Authentication

This section describes the windows related to security and authentication, and includes the following:

Authentication and Authorization Configuration 266
FIPS Settings 267
Password Settings 268
SSL Certificate Expiration Monitoring 269
User Lockout Settings 269

Authentication and Authorization Configuration

The **Authentication and Authorization** configuration includes the following two parts:

- In the **Authentication** section, add username and password to identify the user.
- In the **Authorization** section, define the process of granting roles and permissions for SecureSphere/external system users.

To configure user authentication:

1. In the **Admin** workspace, select **System Definitions** > **Authentication & Authorization Configuration**. The **Authentication & Authorization Configuration** pane appears.
2. For **User Authentication**, select one of the following options:
   - **SecureSphere**: Allows authenticating using the internal SecureSphere database only.
   - **External**: Allows authenticating using external authentication systems. If you select this option, you must select the external system from the **External Authentication System** dropdown list. The external systems that you can choose from are defined in the **External Systems** pane, see External Systems on page 277.
   - **User Specific**: Allows authenticating using SecureSphere database or external authentication systems. If you select this option, you must select the external system from the **External Authentication System** dropdown list. The external systems that you can choose from are defined in the **External Systems** pane, External Systems on page 277.
3. To enable managing SecureSphere users in LDAP, select **External Authorization**. The LDAP group permissions are reflected in the SecureSphere external role permissions. For **External Authorization System**, select an external system from the dropdown list.

   For information about external systems, see External Systems on page 277.

4. Click **Save**.



Notes:

- When de-selecting the External Authorization option, all the external users are moved to the regular users section in the **Users & Permissions** window. They maintain their external system authentication, but lose their external role assignment.
- When selecting the **External Authorization** option, all Users with external system authentication become externally authorized: they are moved to the External Users section in the Users & Permissions window, and their permissions are based on their External Roles.

FIPS Settings

This parameter relates to FIPS (Federal Information Processing Standard) 140-2.

For more information about SecureSphere FIPS 140-2 compliance, see Appendix F, FIPS 140 Compliance.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

FIPS Settings Window Parameters

Parameter	Description
FIPS Mode	If enabled, the Management Server and the Gateways will communicate in a manner compliant with the FIPS 140-2 standard. For more information about FIPS 140 standard, see Appendix F, FIPS 140 Compliance. **Default**: not selected

Password Settings

These parameters define requirements for passwords of SecureSphere users and administrators.

These settings apply only to internal SecureSphere users and administrators, that is, the ones defined in the SecureSphere GUI. For more information, see Understanding Permissions on page 193.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Password Settings Window Parameters

Parameter	Description
Password validity period (in days): Passwords expire at the end of this period	The number of days after which a password expires. At the end of this period, the user or administrator is required to change the password. The new password must be different from all of the four (4) previous passwords. **Default**: 100 days
Password length: Minimum required number of characters in a password	The minimum length of a password (in characters). **Note:** The longer the password, the more difficult it is to guess. **Default**: 7 characters
A password must be significantly different from last password used	Specifies whether a new password must be significantly different from the password it replaces. **Note:** If a new password is significantly different from the password it replaces, knowledge of the previous password does not confer an advantage on attackers. **Default**: not selected
A password must include capital letters	Specifies whether a password must include at least one upper-case character. **Default**: not selected
A password must include numbers	Specifies whether a password must include at least one numeric character. **Default**: selected
A password must include lower case letters	Specifies whether a password must include at least one lower-case character. **Default**: selected
A password must include non alpha-numeric characters	Specifies whether a password must include one of the following characters: ! @ # $ % ^ & * ( ) < > ? . _ + = - [ ] { } \ | : ; , / ` ~ **Default**: not selected



Note: The longer a password and the greater the variety of its required characters, the more difficult it is to guess and the greater the security it confers.

For more information about user permissions, see Understanding Permissions on page 193.

SSL Certificate Expiration Monitoring

Every night at 23:00 SecureSphere scans the SSL keys and identifies those keys about to expire and those which have already expired (including an optional grace period). The parameters below define the deletion process.

In the **SSL Settings** pane, configure the options.

SSL Settings Pane Parameters

Parameter	Description
Number of days before SSL key expiration to issue system event warning	The number of days before an SSL key's expiration date on which to issue a low-severity system event warning. If empty, no warnings are issued. **Default**: None
Expired SSL key deletion grace period	The number of days after an SSL key's expiration date on which to delete the key. If **Expired SSL key deletion grace period** is not empty: • Expired keys are deleted after the grace period has passed. • A system event is issued for keys that expire on the date of the scan. If **Expired SSL key deletion grace period** is empty, no keys are deleted and no systems events are issued. **Default**: None

If both fields are empty, the scan is not run.

User Lockout Settings

These parameters define the values related to a locked user account. For more information, see Locking a User Account on page 206.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Lockout Settings Window Parameters

Parameter	Description
Login failed attempts period	The period (in minutes) in which entering an incorrect password multiple times (defined by the **Number of failed login attempts** parameter) locks an account. **Default**: 5 minutes
Number of failed login attempts	The number of times that entering an incorrect password (within the period defined by the **Login failed attempts period** parameter) locks an account. **Default**: 3 times
Lock duration	The period (in minutes) that an account remains locked. **Default**: 30 minutes

Management Server Settings

This section describes the windows related to Management Servers, and includes:

Action Interfaces 270
Agents 273
Alert Aggregation Configuration 273
Application Groups Settings 274
Assessments 274
CSV Upload Default Settings 274
Data Owner Settings 275
External HTTP Settings 276
External Systems 277
Remote DB Connectivity 287
File URM 289
Keywords Settings 289
Log Collectors 291
Lookup Data 293
Policy Settings 293
Report Settings 293
Server Definitions 294
Software Update Settings 295
Stored Procedures Settings 295
System Events Notifications 295

Action Interfaces

Parameters of the following Action Interfaces are defined in the **Action Interfaces** window:

- Archive to an FTP Location
- Archive to an SCP Location
- Assign as Task
- Block a User
- Block an HTTP Session
- Block an IP (Address)
- Create a Review Task
- Log DAM audit events to System Log (Gateway syslog) using the CEF standard
- Log FAM audit events to System Log (Gateway syslog) using the CEF standard
- Log SharePoint audit events to System Log (Gateway syslog) using the CEF standard
- Log audit events to System Log (Gateway syslog)
- Log custom security event to System Log (syslog) using the CEF standard
- Log network security event to System Log (syslog) using the CEF standard
- Log security event to RSA enVision
- Log security event to System Log (syslog) using the CEF standard
- Log system event to RSA enVision

- Log system event to System Log (syslog) using the CEF standard
- Log to System Log (syslog)
- Monitor a User
- Monitor an HTTP Session
- Monitor an IP (Address)
- Remedy Create Incident
- Run a Shell Command
- SNMP Trap
- Send an Email
- Terminate Session

The parameters in all these windows are explained in Working with Action Sets and Followed Actions **in the SecureSphere User Guide.**

The windows here (**Admin** > **System Definitions** > **Action Interfaces**) enable an administrator to:

- Define Action Interfaces
- Pre-define a value for an Action Interfaces parameter used in Action Sets by deselecting **User-Configured** for that parameter, so that when a user includes the Action Interface in an Action Set (**Main** > **Policies** > **Action Sets**), the values of these parameters are pre-defined in the Action Interface and the user cannot change them.

For example, if the Action Interface **Send an Email** is defined, then when the user defines an Action Set which includes it, the **SMTP Server Address** is pre-defined and the user cannot change its value.

This is illustrated in the following figures.

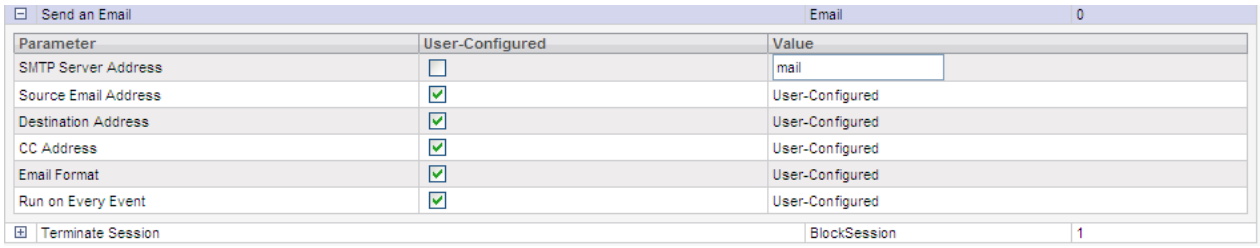


Figure 66: Send Email Action Interface

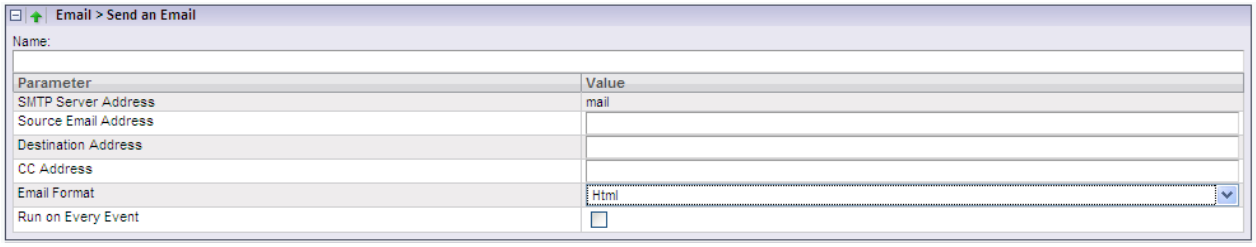


Figure 67: Send an Email used in an Action Set

In the Interfaces pane:

- The **Type** column specifies in which types of objects the Action Interface can be used.
- The **Usage Counter** column specifies the number of Action Sets in which the Action Interface is used.

Note: For most Types, there are pre-defined Action Interfaces. For the Types HTTP Archive, HTTPS Archive and NFS Archive, no Action Interfaces are pre-defined, but administrators can create new Action Interfaces of these Types.

Creating and Configuring Action Interfaces

You can create a new Action Interface, or edit and delete an existing one.

To create a new Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, click .
4. Enter the Action Interface's **Name**.

   Name should be meaningful, because the Action Interface will be used in Action Sets.
5. Select the Action Interface's **Type** from the drop-down list.

   An Action Interface's **Type** determines the Action Set event types in which it can be used.

   For more information, see "Working with Action Sets and Followed Actions" in the **SecureSphere User Guide**.
6. Click **Create**.
7. When the new Action Interface is displayed in the list, expand it by clicking on the plus-sign to the left of its name.
8. Edit the Action Interface's parameters.

   To pre-define a value for one of the Action Interface's parameters, deselect **User-Defined** for that parameter and enter a value. If you select **User-Defined**, the user will have to specify a value for the parameter when defining an Action Set that uses this Action Interface.

   See Working with Action Sets and Followed Actions in the **SecureSphere User Guide**.
9. Click **Save**. Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To edit an existing Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, select an Action Interface from the list.
4. Expand the Action Interface by clicking on the plus-sign to the left of its name.
5. Edit the Action Interface's parameters.

   To pre-define a value for one of the Action Interface's parameters, deselect **User-Defined** for that parameter and enter a value. If you select **User-Defined**, the user will have to specify a value for the parameter when defining an Action Set that uses this Action Interface.

   For more information, see Working with Action Sets and Followed Actions in the **SecureSphere User Guide**.
6. Click **Save**. Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

To delete an existing Action Interface:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Action Interfaces**.
3. In the **Interfaces** pane, select an Action Interface from the list.
4. Click .
5. Click **Save**. Settings are saved. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Agents

This parameter relates to SecureSphere Agent.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Agents Window Parameters

Parameter	Description
Apply default services to new agents according to protected IPs	If enabled, a newly-defined SecureSphere Agent will monitor the database service previously defined as protected by the SecureSphere Gateway, provided that exactly one database service is defined for the Gateway (group). **Default**: enabled
Deletion interval for automatically discovered installed certificates	Automatically discovered installed certificates will be deleted after the specified number of days after the first time the SecureSphere Agent does not discover them. **Default**: 90 days

Alert Aggregation Configuration

These parameters define how alerts are aggregated.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Alert Aggregation Configuration Window Parameters

Parameter	Description
Alert aggregation mechanism is active	Enable this parameter in order to activate the alert aggregation mechanism. **Warning**: Disabling this parameter will cause SecureSphere to produce large number of alerts of the same type. **Default**: enabled
Maximal no. of regular alerts that can be aggregated into a single alert	When an aggregated regular (non-monitoring) alert reaches this limit, no new alerts will be aggregated to it. **Default**: -1 (meaning there is no limit)
Maximal no. of monitoring alerts that can be aggregated into a single alert	When an aggregated monitoring alert reaches this limit, no new alerts will be aggregated to it. **Default**: -1 (meaning there is no limit)
Maximal no. of detailed alerts kept per aggregated alert	When alerts are aggregated, SecureSphere stores, in addition to the aggregated alert information, a certain number of unaggregated alerts, which you can see in the alert viewer when browsing the aggregated alert. This parameter limits the number of raw alerts kept per aggregated alerts. Increase this value with caution, as large values may result in a very quick growth of the database, and will cause the system to discard old alerts more frequently in order to make room for new alerts. **Default**: 30

Application Groups Settings

This parameter relates to whether the Sites hierarchy or the Application Group hierarchy is used to apply policies.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Applications Groups Settings Window Parameters

Parameter	Description
Apply application-level policy objects using application group hierarchy	Use the Application Group hierarchy rather than the Sites hierarchy. **Default**: not selected **Note:** A site can be organized either based on a server group hierarchy (**Main** > **Setup** > **Sites**) or on an application hierarchy (**Main** > **Setup** > **Applications**), but not both. Once the decision has been made, the organization cannot be changed, that is, the site cannot be migrated from one hierarchy to the other.

Assessments

This parameter relates to whether legacy assessment tests are enabled. For more information, see Pre-Defined Assessment Policies.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Assessments Window Parameters

Parameter	Description
Assessment Record Results Limit	This value indicates the maximum number of results returned for a vulnerability scan. If more results are detected, they will not be displayed. **Default**: 1000
Legacy Assessment Tests	Select to enable legacy assessment tests. **Default**: not selected

CSV Upload Default Settings

This parameter relates to the CSV Upload Settings when uploading IP Groups and Protected IP Addresses.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Assessments Window Parameters

Parameter	Description
Case Sensitive	Specifies whether the data in the CSV file are case sensitive, so if existing data match the data in the CSV file, they are not considered duplicates.
Encoding	Select either **ASCII** or **UTF8**.
Format	Select **UNIX** or **Windows**.
Use First Line As Header	Specifies whether the first line of the CSV file contains data to be imported or column headings.
Override Existing Entries	If the data in the CSV file matches existing data, then the data in the CSV file will overwrite the exiting data.

Data Owner Settings

Data Usage Settings

Data Usage Settings parameters relate to the Data Usage feature. If this feature is enabled, FAM collects usage statistics and suggests data owners for folders and files based on the frequency with which specific users access the folders and files. These suggestions can be accepted or rejected by the SecureSphere administrator. The collected usage statistics are used for URM audit enrichment.

Data Usage Window Parameters

Parameter	Description
Disable Data Owners usage statistics calculation (Audit Fast View)	If selected, SecureSphere will not collect audit statistics and will not suggest data owners for files and folders. This setting also affects the URM audit enrichment functionality.
Save Data Usage for Folders Only	If selected, FAM will suggest owners only for folders but not files. This reduces the amount of data processed.
Tree Depth	If specified, FAM will suggest data owners for folders (and files, if **Save Data Usage for Folders Only** is not selected) only to the specified folder hierarchy depth.

Data Owner Portal Settings

Data Owner Portal Settings are used to customize the operation of Data Owner Review in SecureSphere, and subsequently the Data Owner Portal, which is a logical entity separate from SecureSphere, though accessed on the same server.

The following options are available:

Data Owner Portal Parameters

Parameter	Description
Review Mode: Defines how permissions can be reviewed, as follows:	

Parameter	Description
Review Inherited Permissions	If selected, enables the review of permissions that were inherited in addition to having been directly granted. By default users only need to review permissions that have been directly granted. This is useful when data owners are required to review permissions that were granted on a top level folder that is not in the scope of their review, but the permissions are inherited by files and folders that the data owner needs to review.
Allow non-recursive operations	If selected, allows approving or rejecting permissions on a parent folder, without approving permissions to its sub-folders and files. Inherited permissions cannot be reviewed by default. For example, a data owner such as a VP R&D wants to approve permissions on a top level folder without approving it for sub-folders, because he wants to delegate review for permissions in the sub-folders. Enabling this option adds a checkbox to the Permissions Pane of the Data Owner Portal.
Incremental Review: When users configure a new review, there is an option called **Last Review Data** which when enabled, only requires review of new permissions added since last review, and hides permissions that were previously approved or rejected. The following feature impacts how review is conducted when the **Last Review Data** checkbox is selected.	
Include new files with inherited permissions only	New files that weren't directly granted permissions will not need to be reviewed unless this checkbox is selected. Note that when enabling this checkbox, the Review Inherited Permissions option mentioned above is automatically enabled and added to the Data Owner Portal Permissions pane.

External HTTP Settings

To perform various updates SecureSphere needs to establish an Internet connection. The External HTTP Settings capability is used to establish the Internet connection using a proxy. The following updates can be performed:

- ADC content updates
- Web scanners updates
- ThreatRadar updates
- Software Updates
- Community Defense updates
- Key Exchange updates

To configure an Internet connection using HTTP proxy:

1. In the **Admin** workspace, click **System Definitions**.
2. From the **System Definitions** pane, select **External HTTP Settings**. The **External HTTP Settings** pane appears on the right.
3. Enter the parameters as described below.
4. Click **Save**.

Parameter	Description
Ignore HTTP Certificate	Specify whether to ignore the HTTP certificate.
HTTP Proxy Configuration	Select to enable the following parameters.
IP	Enter the proxy's IP address.
Port	Enter the proxy's port, for example, 80 for HTTP or 443 for HTTPS.
Authentication Policy	Select an authentication protocol from the dropdown list.
User/Password/ Verify Password	Enter the username and the password defined for SecureSphere user account on the proxy server.
Domain	When the NTLM is selected as the Authentication policy, you must specify the domain.

External Systems

These parameters specify how to connect to the lookup dataset and also define external systems that can be used in the SecureSphere login process to use the external system, it must be enabled in the External Systems pane.

For information about lookup datasets, see the Advanced Configuration chapter in **SecureSphere User Guide**. For information about the authentication configuration see Authentication and Authorization Configuration on page 266.

If you change these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Defining External Systems

You can create a new External System, or edit and delete an existing one.

To create a new External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, click . The **External Systems** window appears.
4. In the **Name** text box, enter the name for the external system.
5. From the **Type** drop-down list, select one of the options described in the table below.
6. If you change any of these parameters, click **Save**.

   If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Option	Description
Active Direction Collection	Describes how to configure Domain Forests, known as Active Directory Collections in SecureSphere. For more information see External Systems - Active Directory Collection (Forest) on page 278.
Kerberos Authentication	Describes how to configure SecureSphere to connect to the Kerberos domain account and authenticate users so users do not need to login with a user and password. For more information see External Systems - Kerberos Authentication on page 279.
LDAP	For more information, see External Systems - LDAP on page 282.
LDAP Authentication & Authorization	For more information, see External System - LDAP Authentication and Authorization on page 282.
RADIUS Authentication	For more information, see External System - RADIUS Authentication on page 285.
SQL	For more information, see External System - SQL on page 286.
SSL Proxy	For more information, see External System - SSH Proxy on page 286.

To edit an existing External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, select an External System from the list.
4. Expand the External System by clicking on the plus-sign to the left of its name.
5. Edit the External System's parameters. See External Systems - LDAP on page 282 for an explanation of External System parameters.
6. If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To delete an existing External System:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **External Systems**.
3. In the **External System** pane, select an External System from the list.
4. Click .
5. Click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

External Systems - Active Directory Collection (Forest)

SecureSphere supports the use of Domain Forests. In SecureSphere, this feature is known as Active Directory Collections. By configuring an Active Directory Collection you enable the system to integrate user information across various Active Directory domains. Members of the collection can be from different forests as long as they have two way trust.

For information on creating and managing an Active Directory Collection external system, see Defining External Systems on page 277.

Active Directory Collection Configuration Parameters

Parameter	Description
Available LDAP System	Lists the various LDAP systems that have been configured in SecureSphere.
Collection Members	Lists those LDAP systems you have selected to participate in the LDAP Collection (members of the forest). **Note:** Using the Test Connection button, you can test connections to all enabled members after saving.

External Systems - Kerberos Authentication

SecureSphere enables you to configure connectivity with your Kerberos Domain account to enable Windows users to be automatically logged into SecureSphere through Kerberos and subsequently eliminate the need for them to enter a username and password.

This procedure describes how to configure the required components in order to support this form of authentication. Kerberos involves the following primary steps:

Configuring Automatic Kerberos Authentication

	Action	Description	For more information, see...
1	**Setup the Domain Controller**	Configure the Service Principal on the domain controller and generate a keytab file for import into SecureSphere.	See your Windows server documentation for assistance.
2	**Add Hostnames and IP addresses to Domain Controller**	Configure your Domain Controller with host names and IP addresses.	See your Domain Controller documentation for assistance.
3	**Configure Browsers**	Configure the browser you want to use to access SecureSphere.	Configuring the Browser for Kerberos Authentication on page 280
4	**Configure SecureSphere**	Configure SecureSphere Admin definitions required to support authentication.	Configuring SecureSphere for Automatic Kerberos Authentication on page 281

Supported Components

Kerberos Authentication is supported with the following components:

Components	Supported Versions
Servers	Win2003, Win2008
Clients	WinXP, Win7, Vista, Win2000
Browsers	Internet Explorer versions 6,7,8 and 9 Firefox versions 3, 3.6 and 4 Chrome (latest) Safari (latest)

Configuring the Browser for Kerberos Authentication

The first step in configuring kerberos authentication and enabling users to access SecureSphere and be automatically authenticated using Kerberos (and not need to enter a username and password), involves making some minor changes in the browser.



Notes:

- When logging in, users must navigate to the host name of the SecureSphere server. Navigating to the IP address will not enable them to automatically log in and they will be asked for credentials.
- Clients must be in the same domain of the Domain Controller, or in a domain with a trust or sub-domain.
- When users are in a domain with trust, they need to navigate using the SecureSphere server hostname + full domain. For example, https://MX_hostname.domain.com:8083/

Currently, Kerberos authentication requires configuring the browser:

- **Windows IE**: see Configuring Windows Internet Explorer (IE) for Kerberos Authentication on page 280
- **Firefox**: see Configuring Firefox for Kerberos Authentication on page 280

Configuring Windows Internet Explorer (IE) for Kerberos Authentication

This procedure describes how to configure Windows IE to support Kerberos authentication to SecureSphere. For instructions on how to configure Firefox, see Configuring Firefox for Kerberos Authentication on page 280.

To configure Windows IE:

1. In **Windows IE**, from the **Tools** menu, click **Internet Options**. The **Internet Options** window opens.
2. Click the **Security** tab.
3. Select the **Local Intranet** zone, then click the **Sites** button. The **Local Intranet** window opens.
4. Click **Advanced**, advanced settings are displayed.
5. Type the fully qualified URL for the website that is to be authenticated using Kerberos.
   For example: `http://mywebsite.mycompany.com`
6. Click **OK**.
7. Configure SecureSphere settings as described in Configuring SecureSphere for Automatic Kerberos Authentication on page 281.

Configuring Firefox for Kerberos Authentication

This procedure describes how to configure Firefox to support Kerberos authentication to SecureSphere. For instructions on how to configure Windows IE, see Configuring Windows Internet Explorer (IE) for Kerberos Authentication on page 280.

To configure Firefox:

1. Open **Firefox**.
2. In the **Address** bar, type **About:Config**. A warning message is displayed. Click **I'll be careful, I promise**. Configuration settings are displayed.
3. Find the Preference Name **network.negotiate-auth.trusted-uris** and double-click it. The **Enter String Value** window opens.
4. Type the Domain for the website that is to be authenticated using Kerberos.
   For example: `il.imperva.com`
5. Click **OK**. Settings have been changed.
6. Configure SecureSphere settings as described in Configuring SecureSphere for Automatic Kerberos Authentication on page 281.

Configuring SecureSphere for Automatic Kerberos Authentication

To support Kerberos authentication of SecureSphere users, you need to configure settings in the Admin workspace of SecureSphere.



Note: Time needs to be synced between clients, the SecureSphere Server, and the Domain Controller using the same timeserver.

To configure SecureSphere Kerberos Admin settings:

1. In the **Admin** workspace, click **System Definitions > External Systems**. External Systems are displayed.
2. In the **External System** pane, click **New**. The **New External System** window opens.
3. Type a **Name** for the External System, select **Kerberos Authentication** from the dropdown menu, and click **Create**. A new **External System** is added to the **Details** pane.
4. Expand the **External System** by clicking the plus sign to the left of its name.
5. Click **Upload Kerberos Details**. Then do the following:
   - In the **Service Principal** field, type the **Service Principal Key** you configured in the Domain Controller. The syntax of a Service Principal is username@mycompany.com.
   - Under **File**, click **Browse** and navigate to the location of your **Keytab file**.
   - Click **Upload**.

   Note: For instructions on obtaining a Service Principal name or generating a Keytab file, see your Domain Controller documentation or refer to the Imperva Support Knowledge Base.
6. Under **Username Type,** select a **Username Type**. This option represents how user names are formatted in SecureSphere. Select one of the following:
   - **Username with domain**: Select this option when SecureSphere usernames are required to have domain names attached. For example, if your user name is JamesT and your company name is Company, users must enter: JamesT@Company.com
   - **Username without domain**: Select this option when using internally when no domain is required as part of the username. Using the above example, your user would type in JamesT.

   Note: If there is the possibility that you have two users from different domains with the same username, be sure your system is configured to use Usernames with domains.
7. Click **Save**.
8. Enable the external system by selecting the **Enabled** checkbox.
9. Click **Save**.
10. In the **System Definitions** tree in the left-hand side of the window, click **Authentication Configuration**.
11. In the **Details** pane, click one of the following:
    - **External**: Authenticating with an external system such as Radius, LDAP and Kerberos
    - **User Specific**: Takes the settings as configured in the Authenticator field of the User Information Tab under **Users and Permissions**.
12. Select the **External System** you configured in step 2. above.
13. Click **Save**.

    You can now create users in the Users and Permissions section of the Admin workspace. These users need to match the ones you created on your Domain Controller.

External Systems - LDAP

You can define the LDAP external system.

The connection can be established once this external system is enabled.

LDAP configuration Parameters

Parameter	Description
Name	The external system's name.
Primary Server	The IPv4 or IPv6 address or the host name of the primary external system.
Secondary Server	The IPv4 or IPv6 address or the host name of the secondary external system.
Use SSL	Specifies whether to connect to the external system using SSL.
Port	The port number on the external system.
Account Name DN	The account name or DN (Distinguished Name) under which to connect to the external system.
Password	The password to use when connecting to the external system.
Verify Password	Re-enter the password.
Base DN	The Base Distinguished Name is the domain account name in the LDAP server's navigation tree.
Follow Referrals	Select this option to tell/direct the LDAP system to follow referrals.
LDAP Custom Fields	In the **Custom Field** text box, type the LDAP name of the custom field, to receive data from a specific Active Directory field. For example, "physicalDeliveryOfficeName" instead of "Office".

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - LDAP Authentication and Authorization

You can set the parameters related to LDAP authentication and authorization of SecureSphere users.

SecureSphere supports LDAP Authentication and Authorization with the following Windows platforms: 2003, 2003 R2, 2008, 2008 R2, 2012, and 2012 R2.

The connection can be established once this external system is enabled.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.



Note:

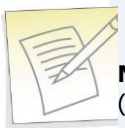
- The admin user cannot be authenticated using LDAP, but is always authenticated by SecureSphere.
- When configuring the external system using a hostname, and not an IP address: In order to use LDAP to authenticate SecureSphere users, a DNS client must be enabled on the Management Server using the `impcfg` command. For more information, see Name Resolution (DNS client).

LDAP Authentication Window Parameters

Parameter	Description
Connection Settings	
Name	The external system's name.
Primary LDAP Server Host	The IP address or the host name of the primary LDAP server.
Port	The port number of the LDAP service on the primary LDAP server.
Secondary LDAP Server Host	The IP address or the host name of the secondary LDAP server.
Port	The port number of the LDAP service on the secondary LDAP server.
Use SSL	Select to specify that communication with LDAP servers is encrypted. If this option is selected, ensure that the port number is changed accordingly.
Validate Certificate	You can authenticate the LDAP server using its certificate. **Validate Certificate** is enabled only if **Use SSL** is checked. If you check **Validate Certificate**, then you must upload the LDAP server's certificate to the MX by clicking **Upload Certificate**. The MX will then validate the certificate according to the settings in the **SOM to MX Communication Settings** window. For more information, see Setting Up SSL with Certificate Authentication on MX.
Upload Certificate	Upload the LDAP server's certificate to the MX. Click **Upload Certificate** and in the **Upload Certificate** window, browse to a .cer certificate file and click **Upload**. After uploading the certificate, you can view it under **Trusted Certificates** in the **SOM to MX Communication Settings** window. For more information, see Setting Up SSL with Certificate Authentication on MX.
Access Mode These parameters specify whether access to the LDAP server is anonymous or conducted under a specific user. Select one of the following:	
Anonymous	Use the "guest" account on the LDAP server, if it is configured.
User Account	If **User Account** is selected, then the following parameters must be defined: • **Account DN**: The Distinguished Name of the domain account under which the LDAP server is to be accessed. • **Password**: The domain account's password. • **Verify Password**: Re-enter the password.

Parameter	Description
Search Settings The following parameters define how to locate a user in LDAP.	
Identifier Field	Enter the unique identifier that SecureSphere uses to identify the external LDAP users. If **Identifier Field** is empty, the user name in SecureSphere is the same as on the LDAP server. **Note:** Case-Sensitivity: Depending on the LDAP server, the login process (authentication by sam-name/email, etc.) may or may not be case-sensitive. However regarding **Identifier Field** vs. name, the comparison in SecureSphere is case-sensitive (this is a cross-system behavior). For example if the user CN in LDAP is "John Smith", you must set the SecureSphere user name to "John Smith" not "john smith". Default: CN.
Base Path for Users	The domain path in the authentication server's navigation tree where the LDAP users are stored. **Note:** You can set this parameter only when the External Authentication parameter is enabled, see step 3. on page 6-222.
Search Filter	The search criteria for the unique identifier. **Note:** If you change the search filter in your authentication server's account (for example, from username to email) users will then have to use a different login name.
Users Search Scope	Select one of the following: • **One Level**: Limits the search to the base path only. • **Subtree:** Allow searching subtree branches.
Authorization Settings	
Enable	Enables reflecting LDAP permission group structure in SecureSphere, where LDAP groups are mapped to SecureSphere external roles.
Base Path for LDAP Groups	The domain path in the authentication server's navigation tree where the LDAP groups are stored. **Note:** You can set this parameter only when the External Authentication parameter is enabled, see step 3 in Authentication and Authorization Configuration on page 266.
Groups Search Scope	Select one of the following: • **One Level**: Limits the search to the base path only. • **Subtree:** Allow searching subtree branches.

Click **Test Connection** to verify that the connection to the LDAP servers is functioning properly.



Note: To point SecureSphere to the Active Directory Global Catalog, set **Base Path** to the domain root (for example, DC=corpmain,DC=com) and **Port** to 3268.

To define, view, or modify the LDAP authentication configuration for individual users:

- For a new user, see Creating a SecureSphere User on page 200.
- For an existing user, see Configuring User Information on page 205.

Third-Party Authentication Task Flow:

1. Obtain the enterprise account details (server's IP addresses, domain account name to be used for authentication, its password, etc.) from your Domain Administrator.
2. Configure the system for third-party authentication. See Authentication and Authorization Configuration on page 266.
3. Configure the users who are to be authenticated via third-party authentication.
   - For a new user, see Creating a SecureSphere User on page 200.
   - For an existing user, see Configuring User Information on page 205.

External System - RADIUS Authentication

You can define the RADIUS external system to connect to the RADIUS server.

The connection can be established once this external system is enabled.

RADIUS Authentication Parameters

Parameter	Description
Name	The external system's name.
Primary Server	The IP address or the host name of the primary external system.
Secondary Server	The IP address or the host name of the secondary external system.
Primary/Secondary Server Port	The port number on the external system used by primary/secondary server. Default: 1812.
Shared Secret	The shared password to use when connecting to the RADIUS server.
Verify Shared Secret	Re-enter the password.
Authentication Protocol	The authentication method that is used to establish the connection with the RADIUS server.
Additional Attributes	Provide the RADIUS attributes which should be specified to communicate with the RADIUS server. For each attribute, provide the following: • **Id**: The attribute Id refers to the numerical value of the "RADIUS attribute Type" as defined by RADIUS RFC 286, section 5 (http://tools.ietf.org/html/rfc2865). For example, the Id of Attribute "NAS-IP-Address" is 4, the id of attribute "Service-Type" is 6 and so on. • **Value**: When providing values for the attributes which have a fixed set of predefined values (for example: "Service Type"), please provide the numeric ID of the value (as defined in the RFC286 for each attribute). For example: If you wish to set Attribute "Service-Type" with value of "Framed", you would provide this attribute with the value of 6 (see: http://tools.ietf.org/html/rfc2865#section-5.6)

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - SQL

You can define the SQL external System to connect to the SQL server.

The connection can be established once this external system is enabled.

SQL External System Parameters

Parameter	Description
Name	The external system's name.
Database Type	The database type.
Server IP	The IP address of the SQL server.
Port	The port number of the SQL service on the SQL server.
Server Name/Domain	Enables you to specify a specific domain name.
Database Name	Name of the Database.
User Name	The name of the user as it appears on the SQL server.
Password	The password to use when connecting to the SQL server.
Verify Password	Re-enter the password.

Click **Test Connection** to verify that the connection to the external system is functioning properly.

External System - SSH Proxy

If the network topology is such that the MX does not have access to the servers which it needs to scan, you can define an SSH Proxy through which the scans will be run. The MX will open an SSH session to the SSH proxy and access the scanned servers through the proxy.

The SSH proxy can be any machine, including a SecureSphere Gateway, which:

- has access to the servers to be scanned, *and*
- which the MX can access via SSH.

Once you have defined an SSH proxy, it will appear as a choice in the **Scan Proxy** dropdown menu (**Servers** tab in **Main** > **Sites** > **Server Group**).

If you want to use a SecureSphere Gateway as an SSH proxy, you still must define it here, otherwise it will not appear as one of the choices under **Scan Proxy**.

SSH Proxy External System Parameters

Parameter	Description
Enabled	Check **Enabled** if you will be running scans using this proxy.
Name	The SSH proxy's name. This name will appear in the **Scan Proxy** dropdown menu. It does not have to be the same as the proxy's hostname.
Server IP	The IP address of the SSH proxy.
User Name	The name of the user under whose account the SSH session on the proxy will be opened.
Password	The user's password.
Verify Password	Re-enter the password.

After entering the above parameters and clicking **Save**, you can test the connection by clicking **Test Connection**.

Remote DB Connectivity

Remote DB Connectivity enables centralized driver management, allowing connection to a variety of databases.

SecureSphere connects to DBs to perform various actions, such as assessment tests, lookup data sets updates, retrieving stored procedures and so on. When establishing connection between SecureSphere and a DB, MX needs to connect directly to DBs and execute SQL, which is done using drivers.

SecureSphere works with JDBC drivers only. Some drivers are installed on SecureSphere by default. In some cases you need to install additional drivers and not only use default SecureSphere drivers. For example, MySQL and Progress databases are not provided with drivers because of the license issues.

In addition to driver, you need a Connection String to connect to a DB. A Connection String is a text string that provides the following:

- Information to which DB to connect
- The parameters that are required to define the connection details
- How to connect
- Additional parameters related to security and other issues.

Using Connection String allows you to be in full control over the driver connection process. With Remote DB Connectivity you can install any drivers and connection strings that you want and you can yourself define combinations between them.

First you define a driver and then the Connection String. You can define the Connection String that you want or let SecureSphere to find for this driver the First Working Connection, meaning that SecureSphere tries all the Connection Strings related to this DB until it finds the one that works.

For more information on defining the driver for a MySQL database, see MySQL Users on page 42.

Working with Drivers

All the drivers installed on SecureSphere are presented in the Remote DB Connectivity pane in the following two groups:

- Predefined Drivers "Setting Up Predefined Drivers" on page 288: Predefined Drivers are drivers delivered with SecureSphere. All the driver definitions are read-only. Predefined drivers can use predefined connections and user defined connections. Predefined connections are also read-only. You can set the user defined connections.
- User Defined Drivers "Setting up User Defined Driver" on page 288: In addition to the drivers installed by default, you can add user defined drivers. For user defined drivers you need to create user defined connections only. You can delete a user defined driver only when it is not used by a DB service.

Setting Up Predefined Drivers

This procedure describes how to set up predefined or user defined drivers.

To set up user defined connections (predefined/user defined drivers):

1. In the **Admin** workspace, select **System Definitions** > **Remote DB Connectivity**. The **Remote DB Connectivity** pane appears.
2. Click + next to the driver for which you want to define connection. The driver definition parameters pane expands.
3. In the **User Defined Connections** area click 

.
4. Type the **Name** and the **Connection String** required in order to communicate with the DB and click **Save**. The new connection is saved and the **Test Connection** button appears.
5. Click **Test Connection**. The **Test Connection** dialog box appears. Set the Test Connection Parameters table below.
6. Click **Test**. The **Test Connection** progress bar appears presenting the progress and the status of the connection with the DB.

Test Connection Parameters

Parameters	Description
IP	The IP of the computer on which the DB is installed.
User Name	User Name for connecting to the DB
Password	The password required for the connection to the DB.
Database Name	The name of the DB to which you want to connect.
Port	The communication port used by the DB.
Server Name	The name of the server on which the DB is installed.



Note: A user defined driver or connection string cannot be deleted if it is used by a DB service. If you try to delete such driver/connection string, an error message will appear. In the case of a connection string, the error message will only show up after you click Save.

Setting up User Defined Driver

The procedure describes how to set up a user defined driver.

To add a new driver (user defined drivers only):

1. In the **Admin** workspace, select **System Definitions** > **Remote DB Connectivity**. The **Remote DB Connectivity** pane appears.
2. In the **User Defined Drivers** area, click 

. The **New DB Driver** dialog box appears with the settings in the **DB Driver Settings** table below.
3. Click **Create**. The New DB Driver dialog box closes and the new driver appears in the **User Defined Drivers** table.
4. Click + next to the new driver. The driver pane expands presenting all the driver settings.
5. In the **Driver Jar Files**, click 

. The **Upload Jar Files** dialog box appears.
6. In the **Upload Jar Files** dialog box, click **Browse** and locate the required jar file.

7. Click **Upload**. The progress bar presents the status of the upload process.
8. Once the jar file has been upload successfully, a new jar file appears in the **Driver Jar Files** table.

DB Drivers Settings

Setting	Description
Driver Name	Type the name that you want for the new driver.
DB Type	Select the DB to which you want to connect using the new driver.
Driver Class Name	Type the driver class name.

File URM

These parameters relate to File User Rights Management, specifically to viewing URM results.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

File URM Window Parameters

Parameter	Description
Server Request Time Limit	When viewing URM results, the number of seconds after which a query to the server will be considered as having timed out. If this happens, the user will be asked to filter the data in order to reduce the amount of data returned. **Default**: 40 seconds

Keywords Settings

These parameters allow administrators to define keywords to be used in filtering reports.

The following procedures can be used to manage keywords:

- Defining a New Keyword on page 290
- Deleting a Keyword on page 291
- Associating a User-defined Keyword with a Report on page 291

The ADC keywords in the following table are ADC pre-defined.

Keywords Settings Window Parameters

Key Name	Description
Basel II	Indicates that a report is a Basel II report. **Defaults**: **Filter Enabled** and **ADC**: selected
EBS	Indicates that a report is an EBS report. **Defaults**: **Filter Enabled** and **ADC**: selected
GLBA	Indicates that a report is a GLBA report. **Defaults**: **Filter Enabled** and **ADC**: selected
HIPAA	Indicates that a report is a HIPAA report. **Defaults**: **Filter Enabled** and **ADC**: selected
ISO 27001	Indicates that a report is an ISO 27001 report. **Defaults**: **Filter Enabled** and **ADC**: selected
PCI	Indicates that a report is a PCI report. **Defaults**: **Filter Enabled** and **ADC**: selected
PeopleSoft	Indicates that a report is a PeopleSoft report. **Defaults**: **Filter Enabled** and **ADC**: selected
Privacy	Indicates that a report is a Privacy report. **Defaults**: **Filter Enabled** and **ADC**: selected
SAP	Indicates that a report is a SAP report. **Defaults**: **Filter Enabled** and **ADC**: selected
SOX	Indicates that a report is a SOX report. **Defaults**: **Filter Enabled** and **ADC**: selected
SharePoint	Indicates that a report is a SharePoint report. **Defaults**: **Filter Enabled** and **ADC**: selected

Defining a New Keyword

This procedure describes how to define a new keyword. For more information on Keyword settings, see Keyword Settings "Keywords Settings" on page 289.

To define a new keyword:

1. Click .
2. Enter the keyword's **Name**.
3. If you want to able to filter the list of reports based on this keyword, select **Filter Enabled**.

   If **Filter Enabled** is not selected, then you cannot filter the list of reports by this keyword, but you can still associate the keyword with a report.

   For user-defined keywords, **ADC** is by default not selected, and this cannot be changed.
4. Click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Deleting a Keyword

This procedure describes how to delete an existing keyword. For more information on Keyword settings, see Keyword Settings "Keywords Settings" on page 289.

To delete a keyword:

1. Select the keyword.
2. Click . Click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Associating a User-defined Keyword with a Report

This procedure describes how to associate a user-defined keyword with a report. For more information on Keyword settings, see Keyword Settings "Keywords Settings" on page 289.

To associate a user-defined keyword with a report:

1. In the **Main** workspace, click **Reports** > **Manage Reports**.
2. Select a report.
3. In the **General Details** tab, move the user-defined keyword from **User Defined Keywords** to **Report Keywords**.
4. Click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Log Collectors

These parameters relate to Log Collectors. Note that Log Collectors and instances of Log Collectors are defined in different parts of the SecureSphere GUI.

- Log Collectors are defined, edited and deleted in the **System Definitions** window.
- Instances of Log Collectors are defined for specific database services on specific database servers or server groups in the **Main** workspace, under **Sites**.

The following types of Log Collectors are available:

- DB2 over AS400
- Teradata (versions prior to 13.0)

Defining Log Collectors

You can create a new Log Collector, or edit and delete an existing one.

To create a new Log Collector:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, click .
4. Enter the Log Collector's **Name**.
5. In the **Create Collector Definitions** window, enter the parameters.
6. Edit the Log Collector's parameters.

   See Log Collector Parameters on page 292 for an explanation of Log Collector parameters.
7. If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To edit an existing Log Collector:

1. In the **Admin** workspace, click **System Definitions**.

2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, select an Log Collector from the list.
4. Expand the Log Collector by clicking on the plus-sign to the left of its name.
5. Edit the Log Collector's parameters.
   See Log Collector Parameters on page 292 for an explanation of Log Collector parameters.
6. If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

To delete an existing Log Collector:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **Log Collectors**.
3. In the **Collector Definitions** pane, select an Log Collector from the list.
4. Click .
5. Click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Log Collector Parameters

The following table list log collector parameters.

Log Collector Parameters

Parameter	Description
Name	The Log Collector's name.
Executable	The name of the Log Collector executable file.
Supported Services	The database service's supported by the Log Collector.
Supported Protocols	The protocols supported by the Log Collector.
User	The user name with which the Log Collector logs on to the database.
Password	The password.
Location	Additional information required to specify the location of the logs on the Host. For example, directory (for FTP and SCP), or the URL (for HTTP and HTTPS) or the database schema.
Delete Log	Enable **Delete Processed Log** to delete logs (on the database server) which have been converted to CSV format and sent to the SecureSphere Gateway process.
Additional Configuration	Additional parameters defining the Log Collector. Contact Imperva support before changing these.
Additional Configuration Template	The name of a file containing additional configuration information. Click **Upload File** to obtain this file.
Additional Configuration XML Validation	The name of a file containing additional configuration information relating to XML validation. Click **Upload File** to obtain this file.

Lookup Data

These parameters are related to lookup data. For more information, see Protecting and Auditing Custom Information with Lookup Data.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Lookup Data Window Parameters

Parameter	Description
Query Timeout	Determines the period of time after which no response is received that the query shall time out. **Default: 15 minutes**
Maximal Lookup Data Set Size	Maximum Lookup Dataset size, that is, the maximum number of results returned from the query. Lookup Dataset size is defined in **Main** > **Setup** > **Global Objects**. **Default**: 10000

Policy Settings

These parameters relate to Security Policies.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Policy Settings Window Parameters

Parameter	Description
Enable comments for policy changes	If enabled, users are able to add comments when modifying a Security Policy. **Default**: Disabled

Report Settings

These parameters are related to reports.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Report Settings Window Parameters

Parameter	Description
Maximal number of rows in a report in CSV format	The maximum number of rows in a CSV format report. Additional data beyond this number of rows will not be included in the report. **Default**: 10000
Enable the downloading of additional fonts when working with different languages.	If checked, SecureSphere assumes that all PDF reports include East Asian fonts, and requires that the user install these fonts before viewing PDF reports. If not checked, SecureSphere assumes that PDF reports do not include East Asian fonts, so if a report does include these fonts it will be incorrectly displayed.
Maximal number of pages in a report in PDF format	The maximum number of pages in a PDF format report. Additional data beyond this number of pages will not be included in the report. **Default**: 500
Template for results files	A sequence of placeholders which defines the report's file name. **Default**: ${reportName}_${username}_${date}
Include report sent by e-mail followed action as link instead of attachment	Include a direct link to a report when an e-mail followed action is used. When disabled, the report is sent as an attachment. **Default**: Disabled.
URL for reports and tasks links	The URL of SecureSphere which hosts reports, for example https://10.3.250.103:8083. SecureSphere then appends the URL so that it directs users to the specific report.

Server Definitions

These parameters relate to the MX server.

Server Definition Window Parameters

Parameter	Description
Server Name	You can assign a name to the Management Server. This name will be displayed in the title of the SecureSphere GUI window. This name can be different from the MX appliance's hostname. **Default**: none

Software Update Settings

These parameters relate to the Software Update feature.

Software Update Window Parameters

Parameter	Description
Enable direct software update notifications from Imperva Update Server	If checked, the SecureSphere MX will periodically contact the Imperva Software Update Server and compare the installed SecureSphere components with the available software patches and upgrades. The MX requires an open internet connection to perform this synchronization. If not checked, synchronization must be performed in an off-line procedure, as described in the "Software Updates" chapter of the **SecureSphere User Guide**.

Stored Procedures Settings

These parameters define how name conflicts are resolved and empty stored procedures saved when importing stored procedures.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Stored Procedures Settings Window Parameters

Parameter	Description
Override existing built in stored procedure data	If selected, imported built-in stored procedures replace existing built-in stored procedures with the same name. **Default**: selected
Override existing user defined stored procedure data	If selected, imported user-defined stored procedures replace existing user-defined stored procedures with the same name. **Default**: selected
Save empty built in stored procedures	Empty built-in stored procedures are saved in the SecureSphere database. **Default**: not selected
Save empty user defined stored procedures	Empty user-defined stored procedures imported from the database are saved in the SecureSphere database. **Default**: not selected



Note: Built-in stored procedures are those provided by the database vendor.

System Events Notifications

These parameters relate to system event notifications.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

System Events Notifications Settings Window Parameters

Parameter	Description
Gaps in minutes between consecutive gateway overload messages	When a Gateway cannot process all the traffic, a system event is generated as a warning. Another system event is created if the Gateway is still overloaded after this interval. **Default**: 15 minutes
Gap in minutes between consecutive ambiguous packets messages	Generate an ambiguous packet message only if this interval has passed since the last such message. **Default**: 5 minutes
Issue a system event when a gateway blocks more than the following number of ambiguous packets per minute	Generate a system event if the Gateway blocks more than this number of packets in one minute. **Default**: 60 packets
Issue a system event when the following CPU utilization percentage is exceeded	Generate a system event if CPU utilization exceeds this percentage. **Default**: 90 percent
Gap in minutes between consecutive CPU utilization messages	Generate a CPU utilization system event only if this interval has passed since the last CPU utilization system event was generated. **Default**: 60 minutes
Gap in minutes between consecutive gateway throughput messages	Generate a Gateway throughput system event only if this interval has passed since the last Gateway throughput system event was generated. **Default**: 60 minutes
Issue a system event when the following throughput is exceeded	Generate a system event if the Gateway throughput exceeds this rate. **Default**: 90 MBs / second
Issue a system event when the ADC content has not been updated for the following number of days	Generate a system event if this interval has passed since ADC content was updated. **Default**: 30 days

User Interface Settings

This section describes the windows related to the user interface (GUI), and includes the following:

Display Limits 296
Language Settings 297

Display Limits

These parameters relate to the display of items in the SecureSphere GUI.

If you change any of these parameters, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide**.

Display Limits Window Parameters

Parameter	Description
Maximum options in pushdown menu	The maximum number of items displayed in drop-down menus. If the list includes more items, they are not displayed and are not available for selection. **Default**: 500 items
Maximum rows in table	The maximum number of items displayed in tables. If the list includes more items, they are not displayed and are not available for editing. **Default**: 500 item

Language Settings

These parameters define the language used in the SecureSphere GUI.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

Language Settings Window Parameters

Parameter	Description
Select Display Language	The language in which GUI elements will be displayed. **Default**: English
Change language without affecting the database	If enabled, texts in the SecureSphere database, for example, policy names, will not be translated into the **Display Language** when displayed in the GUI. **Default**: Enabled

ThreatRadar Settings

This section describes the windows related to ThreatRadar, and includes the following:

General ThreatRadar Settings on page 297

General ThreatRadar Settings

This parameter enables you to enable or disable ThreatRadar.

If you change this parameter, click **Save**. If you are in delayed activation mode, you must activate these settings before they take effect. For more information, see the **SecureSphere User Guide.**

General Settings Window Parameters

Parameter	Description
ThreatRadar is Enabled	If enabled, SecureSphere ThreatRadar is enabled. **Default**: not selected

CHAPTER 14

System Performance

This section describes the **System Performance** window, which displays performance data about Management Servers, Gateways and SecureSphere Agents. It includes the following:

Management Server 298
Exporting Technical Information from Management Servers 300
Gateways and Agents 300
Troubleshooting Performance 302

Management Server

The **Management Server** window displays real-time information about the Management Server.

To display real-time information about the Management Server:

1. In the **Admin** workspace, click **System Performance**.

2. In the **System Performance** pane on the left, click **Management Server.**



Figure 68: System Maintenance - Management Server

If the Management Server is in an MX-HA configuration, the IP address of the active server is displayed at the top of the window.

The graphs display the following information:

Graph	Displays
CPU Load Percentage Over Time By Component	The CPU load attributable to each of the Management Server's functions. Each line is differently colored and represents a different function, according to the color-coded list of functions alongside the graph. **Note:** The **Jobs** graph displays only jobs whose CPU usage is greater than 10%.
Machine Load Over Time	The overall machine load over time, as returned by the Linux "top" command.

- You can change the time period displayed in the graphs by selecting **View Last Hour** or **View Last Day**.
- To output the data in the graphs to a CSV file:
  - Click  (to the left of the words **Management Server** at the top of the window).

- Alternatively, you can click **Save As** (in the upper right corner) and select **Save as CSV**.



- To move the generation of the CSV file to a background process, click **Move to Background** in the **Export CSV window**.

The data in the CSV file is the same data displayed in the graphs.

Note: The exported data relate to the previous 24 hours.

Exporting Technical Information from Management Servers

On occasion, when encountering trouble with SecureSphere operation, Imperva support may request that you provide them with technical information that is automatically generated by SecureSphere, so they can analyze logs and other information. You can export this information from the SecureSphere Management Server using the GUI. This procedure describes how to export technical information for a SecureSphere Management Server from the GUI. For information on exporting technical information from SecureSphere Gateways or Onebox architectures, see Exporting Technical Information from Gateway and Onebox on page 187.

To export technical information from Management Servers:

1. In the **Admin** workspace, select System Performance > Management Server.
2. From the top of the **Details** pane, click **MX Tech Info**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.

Note: When exporting technical information from a Onebox architecture, both Gateway and Management Server technical information is exported.

Gateways and Agents

The **Gateways and Agents** window displays real-time information about the Gateways and DB Agents.

To display real-time information about Gateways and DB Agents:

1. In the **Admin** workspace, click **System Performance**.
2. In the **System Performance** pane on the left, click **Gateways & Agents.**

Note: data are displayed only for those Gateways for which **Enable** is checked under **Performance Profiling** in the **Gateway Group Details** window (see Gateway Groups on page 176).

3. Select a time period:
   - **Last 24 hours**:

- **Last Hour**:
- **Custom**: If you choose **Custom**, you will be asked to define a custom time frame (between **From Date and Time** and **To Date and Time**) and to click **Set**.

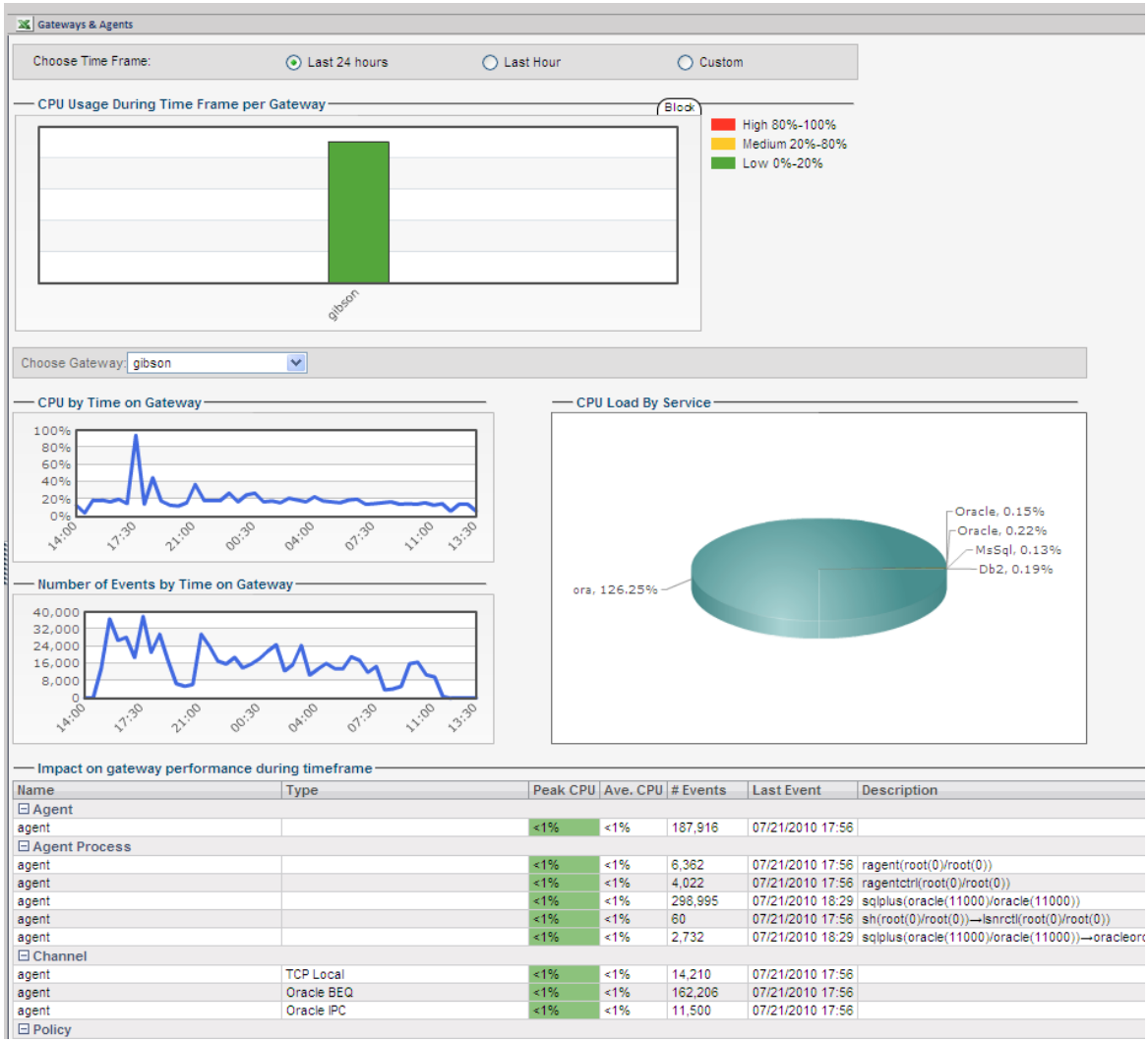


Figure 69: System Maintenance - Gateways and DB Agents

This window is divided into several sections, and displays the following information about the selected time period:

- **CPU Usage During Timeframe per Gateway** - The CPU usage for each Gateway during the selected time period.

4. **Choose Gateway** - Select a Gateway from the list.



Note: An event occurs when SecureSphere "hooks into" the traffic stream, for example, to parse it.

Information about the selected Gateway is displayed, as shown in the table **Gateway Information** below.

5. You can change the time period displayed in the graphs by selecting **Last 24 Hours** or **Last Hour** or **Custom**.
6. To output the data in the graphs to a CSV file:

- Click  (to the left of the words **Gateways & Agents** at the top of the window).

- Alternatively, you can click **Save As** (in the upper right corner) and select **Save as CSV**.



- To move the generation of the CSV file to a background process, click **Move to Background** in the **Export CSV window**.

Note: The exported data relate to the previous 72 hours.

Gateway Information

Section	Displays
CPU / # of Events by Time on Gateway	The graph at the top displays the percentage of CPU use by events. The bottom graph displays the number of events over time.
CPU Load By Service	This pie chart shows the distribution of events by site-server group-service.
Impact on gateway performance during timeframe	The events table groups events of the last 72 hours by time and displays the resources used by each type of event. You can expand the event types to view sub-groups of events. **Notes** • Agent process details refer to the process on the server monitored by the DB Agent. • The top ten objects only are presented.

Troubleshooting Performance

By periodically reviewing the **System Performance** data, you can identify bottlenecks and other problems in your SecureSphere deployment. This section provides some guidelines to assist in troubleshooting, and includes the following:

Management Server 302
Gateways and Agents 303

Management Server

If your Management Server's performance seems excessive over a long time frame, identify the components that use the most CPU resources. Peaks in CPU usage are common and are to be expected, so you should investigate only consistent and prolonged high CPU usage.

Bear in mind that high CPU usage indicate nothing more than high traffic, so review the CPU usage at irregular intervals to determine whether there really is a problem or not.

Component showing consistently high CPU usage	
GUI	It may be that too many users are connected to the GUI at the same time.
Monitoring	You should tune alerts.
Learning	Implement gradual learning.
Audit	It may be that you are trying to view too much audit data at the same time. Consider creating custom time frames that implement the fast view capabilities.
Jobs	These include reports, assessments, scans, archive, Active Modules, Lookup Data sets imports and purges. Consider scheduling these jobs to distribute the load evenly during the day/week. Alternatively, review the jobs to confirm that they are running on relevant data.
Gateway Updates	It may be that one or more of the Gateways is repeatedly requesting configuration. Look for errors in **Setup** > **Gateways**.
Followed Actions	These include emails, syslog actions, archive storage, SNMP and OS commands. Some of these may be CPU intensive because of file size or errors. Review the followed actions and identify these problems.

The values on the vertical scale of the **Machine Load Over Time** graph are the "processes" values returned by the Linux "top" command, defined as follows:

The total number of processes running at the time of the last update. This is also broken down into the number of tasks which are running, sleeping, stopped, or undead. The processes and states display may be toggled by the t interactive command.

Gateways and Agents

This Gateways and Agents window summarizes the resource usage of various SecureSphere components on a specific Gateway. This section review subjects regarding the Gateways and Agents window and includes the following:

System Performance - CPU Load 303
System Performance - Policies 304
System Performance - Signature and Dictionaries 304
System Performance - SSL 304
System Performance - Agents 304

System Performance - CPU Load

If the CPU usage for a specific Gateway seems excessive over a long time frame, identify peak periods of CPU usage, narrowing the time frame.

In the **CPU Load By Service** graph, you can identify the services that incur the highest CPU loads. For each of these services, review the policies, signatures and dictionaries associated with the service to determine which of these might be responsible.

You may find, after investigation, that you need an additional Gateway, or that the Gateway needs to be upgraded to a more powerful model.

System Performance - Policies

For each service with a high CPU load, review the following:

- Identify the alerts that match the policy and rule of this service. If these are false positives, fine tune the policy or unapply it from the application(s), service(s) or server group(s) where the false positives occurred.

  Consider also the possibility that the policy is not required.
- If an audit policy uses too much CPU, it may be too complex. The problem may also be that the relevant signatures and dictionaries are CPU-intensive (see System Performance - Signature and Dictionaries on page 304 below).
- Alternatively, edit the policy by changing some of the criteria or unapply it from some services.

System Performance - Signature and Dictionaries

For each service with a high CPU load, review the following:

Component	Description
Security Signatures	Review the signature (**Main** > **Setup** > **Signatures**) and determine whether it can be safely disabled (ADC signatures) or modified (custom signatures).
SQL Dictionaries (including Stored Procedures & Privileged Operations)	In **Main** > **Setup** > **Global Objects**, review stored procedures and privileged operations and disable those which are not required.
Generic Dictionaries (including Sensitive Data Dictionaries)	Identify the policies using the dictionary, and edit or unapply them accordingly.
SQL injection / XSS	In **Monitor** > **Alerts**, review the most frequently-occurring SSL injection and XSS alerts, and create exceptions for those which are false positives.

System Performance - SSL

If SSL operations are consuming significant CPU resources, consider installing an SSL accelerator.

Alternatively, configure the Web server to reuse SSL sessions.

System Performance - Agents

DB agents run on the DB server and communicate with a SecureSphere Gateway, so they use resources on both machines.

On the DB Server

In **Main** > **Setup** > **Agents**, you can see the CPU usage and other statistics for each agent in the **General Details** tab. If an agent's CPU usage is excessive, then use OS platform commands to determine which agent process is responsible. Sometimes excessive CPU usage is reflected in the Gateway's statistics (see **On the Gateway** below).

Review the relevant audit policies. It may be that it is not necessary to audit all of the database traffic, in which case you should create appropriate exclusions.

Otherwise, you may be able to reduce the CPU load by reconfiguring the deployment.

On the Gateway

In the **Impact on gateway performance during timeframe** table, you can see the CPU resources consumed by each DB Agent communicating with the Gateway. Excessive CPU usage on the Gateway may indicate a problem with the DB Agent, for example, if the DB Agent is monitoring a backup process. In this case you should create an exclusion on the DB Agent.

Installing SecureSphere Agent for z/OS

This chapter describes how to install and configure SecureSphere Agent Agent for z/OS.



Note: For information on configuring SecureSphere Agent for z/OS in SecureSphere, see the "SecureSphere Agents" chapter in the **SecureSphere User Guide**.

It reviews the following subjects:

Installing SecureSphere Agent for z/OS - Version 3.1 305
Installing SecureSphere Agent for z/OS - Version 2.1 323

Installing SecureSphere Agent for z/OS - Version 3.1

This section contains the following information:

Upgrading from Previous Versions to Version 3.1 305
Configuring SecureSphere Agent Agent for z/OS Tasks 306
Before Installing and Configuring SecureSphere Agent for z/OS 306
Downloading and Installing SecureSphere Agent for z/OS 310
Configuring SecureSphere Agent for z/OS (on z/OS) 313
Starting, Managing, and Stopping SecureSphere Agent for z/OS 322

Upgrading from Previous Versions to Version 3.1

SecureSphere Agent for z/OS version 2.1 and version 3.1 can run at the same time on z/OS.

To enable IMS monitoring support, you must install version 3.1. Installing version 3.1 does not override existing versions.

If you want your existing installed version to continue monitoring DB2 while using version 3.1 only for monitoring IMS, continue with the next section - *Configuring SecureSphere Agent for z/OS Tasks* "*Configuring SecureSphere Agent Agent for z/OS Tasks*" on page 306.

If you want version 3.1 to monitor DB2 and IMS, continue with the following procedure.

To disable an existing SecureSphere Agent for z/OS (version 2.1):

1. Stop the previous version using the following command:

```
/P process_name
```

   For example,

```
/P NSUPROC
```

2. In the SecureSphere GUI, delete the SecureSphere Agent for z/OS that you just stopped.
3. Install SecureSphere Agent for z/OS version 3.1.
4. Install the latest maintenance.



Note: If you want to restore a previous SecureSphere Agent for z/OS, follow the above procedure, that is, stop the agent, delete it from the GUI and install the other version and its maintenance.

Configuring SecureSphere Agent Agent for z/OS Tasks

The SecureSphere administrator must perform the tasks described below.

	Task Overview	For more information, see...
	Make the necessary preparations for installing SecureSphere Agent for z/OS.	Before Installing and Configuring SecureSphere Agent for z/OS on page 324
	Download and install the SecureSphere Agent for z/OS.	Downloading and Installing SecureSphere Agent for z/OS on page 328
	Configure the SecureSphere Agent for z/OS license.	Specifying the License Key on page 331
	Using `impcfg`, configure the data and configuration channels on which SecureSphere Agent for z/OS communicate with the SecureSphere **Gateway**. Note: A SecureSphere Agent listener and a SecureSphere Agent for z/OS listener cannot be defined on the same port.	Adding a SecureSphere Agent for DB2 z/OS Listener on page 83

Before Installing and Configuring SecureSphere Agent for z/OS

There are a number of items you should verify and understand before beginning to install and configure SecureSphere agent for z/OS. This includes:

Information You Must Have Before You Begin 307
Terminology Used In This Guide 307
Roles and Assignments for the Installation and Configuration 307
Mainframe Software Requirements 309
Security Requirements 309
TCP/IP Requirements 309
Optimizing Performance 309
Supported Facilities 310

Information You Must Have Before You Begin

Verify that you have the following items:

Item	Additional Information
Credentials to access the Imperva FTP site	You use the credentials to access the FTP site and to download and install SecureSphere Agent for z/OS files.
License key for the SecureSphere Agent for z/OS	You must specify the license key when you install the SecureSphere Agent for z/OS on the z/OS host.

Terminology Used In This Guide

The product includes the following components.

- A component referred to as SecureSphere Agent for z/OS, that runs as a started task and gathers data about the DB2 and IMS subsystems being audited.
- A component referred to as the SecureSphere Gateway, that receives all the information gathered by SecureSphere Agent for z/OS.
- A component referred to as SecureSphere Management Server, that provides the collection rules to SecureSphere Agent for z/OS.

Roles and Assignments for the Installation and Configuration

Depending on the size and complexity of your IT organization, several people might contribute to the SecureSphere Agent for z/OS installation and configuration process. In most cases, these are the roles and their specific skills or knowledge.

- DB2 DBA or System Administrator
- Network Administrator
- Security Administrator
- System Programmer

The matrix shows:

- In order, the tasks that you perform during the installation and configuration (The tasks in the table are covered in the topics that follow.)
- In most cases, who in the organization will be involved in completing those tasks

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Before you install SecureSphere Agent for z/OS	Authorize any required TCP/IP connections and provide information that the System Programmer uses during product customization.		X		
	Define mainframe TCP/IP authority.			X	
Downloading and installing SecureSphere Agent for z/OS	Install the product by downloading a job that allocates the data sets and then copies the product libraries to z/OS.				X
Configuring SecureSphere Agent for z/OS	Specify the license key and product libraries on z/OS.				X
	Application Program Facility (APF) authorize the LOAD library and make the authorization permanent following an IPL. (You do not have to IPL the system to install the product.)				X
	Specify the customization parameters specific to DB2 or IMS (such as the load libraries for the versions of DB2).	X			X
	Specify the customization parameters specific to TCP/IP (such as the port numbers for the data receiver and plan provider). **Note:** For more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 84**.**		X		X
Completing the configuration for the started task	Bind the DB2 packages for the product.	X			
	Authorize the started task for the product so that it can access the required resources.			X	
	Grant DB2 privileges to the user ID for the started task so that it can access the DB2 Catalog for any DB2 instance being audited.	X		X	
	Initialize and secure the rules data sets for the product so that it can only be modified by the started task.			X	X
	Specify a priority for the started task in Workload Manager (WLM).				X
	Modify the started task procedure and copy the procedure to the SYSPROC library,				X
Starting, managing, and stopping SecureSphere Agent for z/OS	Start the started task.				X

Mainframe Software Requirements

Before unloading and installing SecureSphere Agent for z/OS, verify that you have the following software installed and operational on your z/OS system.

- IBM z/OS version 1.8 or later (64 bit mode required)
- DB2 for z/OS version 8, 9 or 10
- IBM TCP/IP version 3.1 or later

Security Requirements

The table lists the security requirements for SecureSphere Agent for z/OS.

Element	Security Requirement
DB2	You must authorize the started task-user ID so that it can access the DB2 Catalog for any DB2 instance being audited.
Rules data sets	You must protect the rules data sets for SecureSphere Agent for z/OS so that it can only be modified by the started task. You will specify the rules data sets using the Local Rules Dataset Name customizable parameter when you configure SecureSphere Agent for z/OS.
Started task	For the product to run successfully, you must provide SecureSphere Agent for z/OS with adequate authority to operating system and database resources. Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task for the product uses TCP to communicate with the Imperva. If you are using RACF, the started tasks for the product must have an OMVS segment defined in RACF.

TCP/IP Requirements

You must have TCP/IP network connections between the LPAR where auditing is performed and the SecureSphere Gateway and SecureSphere Management Server.

Before installing the product, you will need the:

- TCPIP.DATA data set name
- TCP/IP port numbers for the data receiver and plan provider (for more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83)
- Host name for the data receiver and plan provider
- You will also need to define mainframe TCP/IP authority.

Optimizing Performance

The product is designed for optimal performance so that auditing activities never impact normal business transaction processing. Key performance features include:

- When available, use of zIIP processors
- No reliance on slow, resource-intensive database trace utilities
- Off loads audit data from mainframe so that analysis, reporting, and data storage expenses are not incurred on the mainframe

Supported Facilities

The product supports the following local attach facilities for DB2 on z/OS:

- Call Attach (CAF)
- Resource Recover Services (RRSAF)
- CICS
- TSO
- IMS

The product also supports DRDA for distributed connections.

Downloading and Installing SecureSphere Agent for z/OS

This topic contains information about how to download and install SecureSphere Agent for z/OS. It includes:

Downloading and Installing the Product 310
APF Authorizing the LOAD Library 311
Creating the ADMIN Library 312

Downloading and Installing the Product

The section describes the prerequisites and procedures required for downloading and installing SecureSphere Agent for z/OS and includes:

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance 310
Procedure for Downloading and Installing the Product 310
Procedure for Downloading and Installing the Cumulative Maintenance 311

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance

To unterse the files, you must have installed TRSMAIN V4 or AMATERSE.



Note: AMATERSE is an enhanced replacement for TRSMAIN and it is strongly recommended that you upgrade from TRSMAIN V4 to AMATERSE.

For information about installing or upgrading to AMATERSE, see http://techsupport.services.ibm.com/390/trsmain.html.

Procedure for Downloading and Installing the Product

This section contains the procedures you follow to download and install the product for the first time or upgrade the product to a new version or release.



Note: When you download and install the product, also be sure to download and apply any cumulative maintenance included in the FTP directory. Skipping this step may cause the product to behave incorrectly.

If you have already installed the product and only need to install cumulative maintenance, see Procedure for Downloading and Installing the Cumulative Maintenance "Procedure for Downloading and Installing the Product" **on page 328.**

To download and install the product files:

1. From the FTP site, download the file `readme.txt`**.** This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the install file, from the FTP site, download the file `unpack.jcl`, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed product file to your mainframe system. The install process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.
4. Follow the instructions in the RECVBASE member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command to create the product datasets from the remaining members contained within the untersed dataset.

Procedure for Downloading and Installing the Cumulative Maintenance

This section contains the procedures you follow to download and install the cumulative maintenance.

To download and install the maintenance files for an existing installation:

1. From the FTP site, download the file `readme.txt`**.** This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the cumulative maintenance file, from the FTP site, download the file `unpack.jcl`, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed cumulative maintenance file to your mainframe system. The maintenance process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.
4. Follow the instructions in the RECVFIXS member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command and update your product libraries from the remaining members contained within the untersed dataset.

APF Authorizing the LOAD Library

The product uses dataspaces, cross memory services, and other functions that require APF authorization. These are common and necessary requirements of system level software. The library that contains SecureSphere Agent for z/OS LOAD modules (*?tomiumhlq***.**LOAD) must be APF authorized.

You must also ensure that the authorization is permanent to prevent losing authorization at your next IPL.

To APF authorize the LOAD library, your system programmer must issue an APF command. The table shows examples of the commands.

Status of the Data Set for the LOAD Library	Example Command
Managed by the IBM System Management Service (SMS)	SETPROG APF,ADD,DSNAME**=***?tomiumhlq*.LOAD,SMS
Not managed by SMS	SETPROG APF,ADD,DSNAME**=***?tomiumhlq*.LOAD,VOLUME=volume

Once the LOAD library has been APF authorized, updates or changes made to the configuration using the Product Customization Facility must be done by someone with authority to update an APF authorized library. (This person is typically not a DBA.)

Creating the ADMIN Library

The product uses an administration (ADMIN) library to manage and maintain product keys and the associated product libraries. You must allocate and catalog this ADMIN library.



Note: You must create the ADMIN library only if you are installing the product for the first time.

Follow this process.

1. Locate the ALLOCATE member in the *?tomiumhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job to allocate the library.

   Result: The job allocates a data set with the format shown in the following table:

Item	Value
Data set format	Partitioned data set (PDS)
Record format	Fixed block (FB), 80-character logical records LRECL=80, RECFM=FB,blksize Where blksize is your site standard block size.
Allocated space	Two tracks and 10 directory blocks

Including the Product Libraries in Your Disaster Recovery Plan

The product includes the data sets listed in the table below. These resources should also be included in your backup and disaster recovery plan.

Data Set Name	Description
?tomiumhlq.ADMIN	This library contains product keys.
?tomiumhlq.CNTL	This library contains the control members for SecureSphere Agent for z/OS, including sample JCL.
?tomiumhlq.DBRMLIB	This library contains the DB2 definitions for SecureSphere Agent for z/OS.
?tomiumhlq.EXEC	This library contains the REXX executables needed to configure SecureSphere Agent for z/OS.
?tomiumhlq.LOAD	This library contains the executable LOAD modules needed to execute SecureSphere Agent for z/OS.
?tomiumhlq.MESSAGES	This library contains descriptions for product messages.
?tomiumhlq.MLIB	This library contains messages issued by the ISPF interface.
?tomiumhlq.MSG	This library contains the message modules used by SecureSphere Agent for z/OS.
?tomiumhlq.PLIB	This library contains ISPF panels used by SecureSphere Agent for z/OS.

Configuring SecureSphere Agent for z/OS (on z/OS)

This topic contains information about using the Product Customization Facility to configure SecureSphere Agent for z/OS and includes:

Accessing the Product Customization Facility 313
Specifying the License Key 313
Specifying the Product Libraries 314
Specifying the Customizable Parameters 315
Detailed Information About the Customization Parameters 317
Completing the Configuration 319

Accessing the Product Customization Facility

Follow this process to access the Product Customization Facility. You must access the Tomium Product Customization Facility if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

1. At the TSO prompt (option 6), specify the following command.

   `EX '?tomiumhlq.EXEC(TOMMCONF)' '?tomiumhlq'`

   Where *?tomiumhlq* is the high-level qualifier for SecureSphere Agent for z/OS LOAD library that you specified when you installed SecureSphere Agent for z/OS.

   Result: The product displays the Product Customization Facility menu.

```
                  Tomium Product Customization          Row n to n of n
Command ===> _____________________________________ Scroll ===> CSR

   Product load library. . . ?tomiumhlq.LOAD

Type S to select a product for customization, B to BROWSE the $README member

   Product Name / Description                              Version
 _ License Management                                      nn.nn.nn
```

Specifying the License Key

You received a license key for SecureSphere Agent for z/OS when you purchased SecureSphere Agent for z/OS. This license key is required to run SecureSphere Agent for z/OS and protects the software from unauthorized use. You must specify the license key if you are:

- installing the product for the first time
- adding new keys or removing old keys

If the proper product keys are not present SecureSphere Agent for z/OS will fail. Follow this process to specify the license key.

1. Type **S** next to License Management.
2. Press **Enter**.

3. On the Tomium Enterprise Software Product Key Update panel, specify:
4. **Y** in the Manage Product Keys field
5. **Y** in the Manage Product Libraries field
6. Press **Enter**.

   Result: The panel redisplays with the values in the table License Key Values below.
7. Type **End** on the command line and press **Enter** or press the appropriate function key.

   Result: The Product Customization Facility displays the next Enterprise Software Product Key Update panel in the series.

License Key Values

Field	Description
Product Name	Name of the family of products for this key
CPU Id	Processor id for which this key is valid
Expires	Expiration date for this key
Features	All feature codes in the key

Specifying the Product Libraries

You must specify the product libraries if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

This step ensures that there is a locator module in SecureSphere Agent for z/OS LOAD library. (The locator module indicates where the license keys are stored.) Without this module SecureSphere Agent for z/OS will not be able to perform product key validation and SecureSphere Agent for z/OS will fail. Follow this procedure to specify SecureSphere Agent for z/OS libraries.

1. On the Tomium Enterprise Software Product Key Update panel, specify:
   - The fully qualified data set name of the ADMIN library that you allocated in the Tomium Administration Library field (Do not specify quotes around the name.)
   - Your license key in the Product Key field
2. Press Enter.
3. Verify that the Status column displays Locator correct.
4. Type End on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility redisplays the Product Customization Facility menu.

   The below table describes the remaining fields on the panel.

Field	Description
LC	Use this field to update (U) or delete (D) libraries.
Product Library	Lists the Tomium Enterprise Software product LOAD libraries contained in the ADMIN data set library. Each library contains a locator module, which identifies the location of the ADMIN library.
Status	Describes the status of the locator module

Specifying the Customizable Parameters

You must specify the customizable parameters if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

If you are upgrading and you want to use the existing values for the customization parameters, you can save the existing values by accessing the panel and pressing END to save and exit the panel.



Note: You must perform this step if you are installing or upgrading the product. Saving and exiting the panel activates the NSUUOPT module that contains the customizable parameters. If you are upgrading, saving and exiting the panel upgrades the module so that it is at the same version and release level as the product.

Follow this procedure.

1. On the Product Customization Facility menu, type **S** next to SecureSphere Agent for z/OS and press Enter.

   Result: The Product Customization Facility displays the SecureSphere Agent for z/OS **Customization Options** panel.

```
 ---------- Tomium Activity Monitor Customization Options Vnn.nn.nn -----------
Command ===>

    Product Load Library . . TOMIUM.V3R1.LOAD
    Options Module Name. . . TSAUOPT
    Note: These are your current parameters.

 General Operating Options:
  Message Level. . . . . . . . . . 2                  1 - 3  ( 3 = Verbose )
  Max Dataspace Size . . . . . . . 100                1 to 2047 Megabytes
  Local Rules Dataset Name . . . .
  Monitored Subsystems . . . . . .


 Communication Parameters:
  Inactivity Disconnect Timeout. . 300                0 to 6000 Seconds
  Data Receiver Port Number. . . . 17670              1 to 65535
  Data Receiver Host Name. . . . .
  17670
  Plan Provider Port Number. . . . 17670              1 to 65535
  Plan Provider Host Name. . . . .


 DB2 Operating Parameters:
  Resolve Group Attach Name. . . . Y                  Y-Yes  N-No
  Package Collection ID  . . . . . TSAD310            DB2 Collection Name
  DB2 Version 9 Load Library . . .
  DB2 Version 10 Load Library. . .


 Press ENTER to update END to save and exit
       CANCEL to exit ignoring any changes made since the last update
```

Tomium Activity Monitor Customization Options



Note: For more information about configuring `Data Receiver Port Number` and `Plan Provider Port Number` in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.

2. Specify the values for the parameters. (You can reset all the parameters to SecureSphere Agent for z/OS defaults at any time by typing **DEFAULT** on the command line and pressing Enter.)
3. Press Enter.
4. Type **End** on the command line and press Enter or press the appropriate function key.

   If you will be running multiple SecureSphere Agent for z/OSs on different LPARs, you can override the Product Load Library and the Options Module Name so that you can specify or change the customization parameters without leaving the panel.

Value You Want to Change on the Panel	Action to Take
Product Load Library	Specify the following command on the command line. NEWLIB ?tomiumhlq.LOAD Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new library name in the Product Load Library field.
Options Module Name	Specify the following command on the command line. NEWOPT ?name Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new module name in the Options Module Name field.

Detailed Information About the Customization Parameters

The table provides detailed information about the customization parameters.

Parameter	Description	Default Value
Message Level	The detail level for messages issued by SecureSphere Agent for z/OS Specify a numeric value between 1 and 3. 1—Least verbose. Only severe messages are displayed. 2—Verbose. Severe and warning messages are displayed. 3—Most verbose. All messages are displayed.	2
Max Dataspace Size	1 to 2047 Megabytes	100
Local Rules Dataset Name	The fully qualified name of the data set used for the local copy of the rules (each SecureSphere Agent for z/OS started task has its own local copy of the rules data sets). Specify any valid dataset name that complies with your site naming requirements. It is recommended that the LPAR is included as a node in the dataset name.	There is no default value.
Monitored Subsystems		
Inactivity Disconnect Timeout	Specifies a communications timeout value in seconds for the collector If this length of time is reached without any interaction with the SecureSphere Gateway, the connection will be dropped and retried. The value that you specify should be set to a multiple of the heartbeat values used by the SecureSphere Gateway. If the value is set to 0, the timeout is disabled. Specify a numeric value between 0 and 6000.	300
Data Receiver Port Number	The port number that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same port number using impcfg. For more information, see SecureSphere Administration Guide. Specify a value from 1 to 65535. **Note**: For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.	17670
Data Receiver Host Name	The domain name or the IP address that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same IP address using impcfg. For more information, see SecureSphere Administration Guide.	17670
Plan Provider Port Number	The port number of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for z/OS. **Note**: SecureSphere Agent for z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for z/OS from the SecureSphere Gateway (see **SecureSphere User Guide**). Specify a value from 1 to 65535. **Note**: For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.	17670

Parameter	Description	Default Value
Plan Provider Host Name	The domain name or the IP address of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for z/OS. Note: SecureSphere Agent for z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for z/OS from the SecureSphere Gateway (see **SecureSphere User Guide**).	There is no default value.
Resolve Group Attach Name	For the DB2 subsystems that you specify with the DB2 Subsystems Selected for Audit parameter, specifies whether or not group attach names should automatically resolve to all members of the data sharing group. Y - Resolve group attach names to all members. N - Use N if a data sharing member subsystem name is the same as the group attach name. The group is not audited.	Y
Package Collection ID	The collection ID All packages required for the audit extractor should be bound using the same collection ID. Specify a collection ID for the bound that is from 1 to 8 alphanumeric characters in length. This ID must be unique to the agent instance. Make a note of this field because you will need it again later in the configuration process.	TSAD310
DB2 Version 9 LOAD Library	Data set name for the DB2 version 9 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
DB2 Version 10 LOAD Library	Data set name for the DB2 version 10 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.

Completing the Configuration

This topic contains information about the tasks you must complete to finish configuring SecureSphere Agent for z/OS outside of the Product Customization Facility. It reviews the following topics:

Binding Packages for the Product 319
Determining the Remaining Tasks to Complete for the Started Task 320
Authorizing the Started Task for the Product 320
Granting DB2 Privileges 320
Initializing and Securing the Rules Data Set 321
Specifying the Priority Using WLM 321
Modifying the Started Task Procedure 321

Binding Packages for the Product

The product requires that you perform a DB2 bind on those packages it uses during the audit process. You must perform a DB2 bind if you are:

- installing the product for the first time
- upgrading to a new version or release of the product
- installing maintenance and one or more of the packages have changed

Follow this process to bind the packages.

1. Locate the NSU1000 member in the ?hlq.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job.
4. Verify that the job competed successfully and that all the return codes were zero.

Determining the Remaining Tasks to Complete for the Started Task

The remaining information in this topic covers the tasks that you must complete for the started task. You must complete all the remaining tasks in this topic if you are:

- Installing the product for the first time
- Upgrading to a new version or release of the product and you want to use a new started task (You do not have to complete these if you want to use the existing started task.)

Authorizing the Started Task for the Product

Before you can start the product, you must authorize:

- The user ID for the started task so that it can access the necessary data sets (such as the rules data set, the APF authorized LOAD library, and any of the remaining product libraries)
- The started task so that is can access the TCP/IP stack on z/OS

Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task uses TCP/IP to communicate with the data receiver. If you are using RACF, the started tasks must have an OMVS segment defined in RACF.

Granting DB2 Privileges

The started task must be granted EXECUTE authority on the NSU packages in the NSU collection. This must be done for each non-data sharing DB2 subsystem ID and for at least one member in any data sharing group. If a data sharing group has had privileges granted on a different LPAR setup, it does not need to be repeated at this stage.

1. Locate the NSU2000 member in the *?tomiumhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. If multiple non-data sharing subsystems will be supported on the LPAR, you must duplicate the GRANT step in the job for each subsystem. The table **Variable Descriptions** below provides the descriptions for the variables in the jobs and indicates the action you take for the value in the duplicated GRANT step.
4. Submit the job.
5. Verify that the job competed successfully and that all the return codes were zero.

Variable Descriptions

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*ssid*	ID of the DB2 subsystem or name of the data sharing group	Specify a GRANT step and ?ssid for each non-sharing DB2 subsystem.
?*db2exit*	Name of the library for the DB2 exit library	If the DB2 subsystem uses a different library, specify the name of the library in the GRANT step.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*db2load*	Name of the DB2 LOAD library	If the DB2 subsystem uses a different LOAD library, specify the name of the library in the GRANT step.
?*dsntiad*	The name of the plan associated with the LMOD DSNTIAD For a default installation, it is DSNTIAxx where xx is the version (such as 81 or 91).	No change required.
?*dsnrunlb*	The name of the library where DSNTIAD resides The library must be APF authorized.	No changed required.
?*db2coll*	The name of the collection ID for NSU packages Specify the same value that you specified for the Package Collection ID customizable parameter.	No change required.
?*stcuser*	PUBLIC or to the name of the started task for SecureSphere Agent for z/OS	If you duplicate the GRANT step, do not change this value.

Initializing and Securing the Rules Data Set

The product uses a rules processing engine to isolate transactions to be reported from other, routine transactions. For each SecureSphere Agent for z/OS started task, the rules data set must be initialized before you can start SecureSphere Agent for z/OS or customize the rules data set.

You specified the rules data set using the Local Rules Dataset Name customizable parameter when you configured the product. Follow this procedure to initialize and secure the rules data set.

1. Locate the NSU3000 member in the `?tomiumhlq`.CNTL data set.
2. Modify the sample JCL using the instructions included in the member. The data set name for `?rulesdsn` must match the value specified for the Local Rules Dataset Name customizable parameter (see **SecureSphere User Guide**) and should include the LPAR as a node in the name.
3. Submit the job.
4. Use your security administration product (such as RACF) to protect the rules data set so that only its owning started task can update it.
5. Verify that the job competed successfully and that all the return codes were zero.

Specifying the Priority Using WLM

To further optimize performance, set the Workload Manager (WLM) goal and importance of the started task equal to or higher than that of the DB2 subsystems being audited. With this priority, SecureSphere Agent for z/OS will run faster and more reliably.

Modifying the Started Task Procedure

Follow this procedure to modify the started task procedure and to copy the procedure to the SYSPROC library.

1. Locate the NSUPROC member in the ?hlq.CNTL library.
2. Modify the sample JCL using the instructions included in the member.

3. If you are using CA Detector for DB2 for z/OS, specify the COLL=2 parameter on the EXEC statement. (The COLL parameter is optional. The default is COLL=1.)
4. Copy the JCL to your SYSPROC library.

Starting, Managing, and Stopping SecureSphere Agent for z/OS

This topic contains information about starting and managing SecureSphere Agent for z/OS and includes:

Requirements and Restrictions for Starting SecureSphere Agent for z/OS 322
Modifying the Started Task Procedure and Starting the Started Task 322
Using Operator Commands to Stop and Manage the Product 322

Requirements and Restrictions for Starting SecureSphere Agent for z/OS

SecureSphere Agent for z/OS has these requirements and restrictions.

- If you are using other DB2 monitoring or auditing products at your site, you must start SecureSphere Agent for z/OS before you start the other monitoring or auditing products.
- Do not start more than one SecureSphere Agent for z/OS to audit the same DB2 subsystem or member of a data sharing group.

Modifying the Started Task Procedure and Starting the Started Task

Follow this procedure to start the started tasks.

1. Locate the TAMPROC member in the *?tomiumhlq*.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLLID=2 parameter on the EXEC statement.
   The COLLID parameter is optional. The default is COLLID=1.
4. Copy the JCL to your SYSPROC library.
5. Perform the appropriate action. If you want to use:
   - SDSF, specify /`s taskname`
   - An MVS operator command, specify `S taskname` or `START taskname`

Using Operator Commands to Stop and Manage the Product

The table below describes the MVS operator commands that you can specify from a console to manage SecureSphere Agent for z/OS. In the command example, replace `taskname` with job name assigned by MVS to the started task address space. The table shows the tasks, the commands to specify, and an example using NSUPROC as the `taskname`.

Task You Want to Perform	Command to Specify	Example
Delete the dataspace associated with the collection process for a DB2 subsystem	/F taskname,MAINT,DELDSP, db2id where db2id is the ID of the DB2 subsystem. **Note**: Before you can delete the dataspace, you must terminate collection of the audit data using the TERM command shown below in this table.	/F NSUPROC,MAINT, DELDSP,DB2A
Resize the dataspace associated with the collection process for a DB2 subsystem (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F taskname,MAINT,RSZDSP, db2id,nnnn Where: db2id is the ID of the DB2 subsystem nnnn is a number between 1 and 2047	/F NSUPROC,MAINT, RSZDSP,DB2A,500
Resize the dataspace associated with the collection process for all DB2 subsystems (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F taskname,MAINT,RSZDSP, ALL,nnnn Where nnnn is a number between 1 and 2047.	/F NSUPROC,MAINT, RSZDSP,ALL,500
Set the verbosity level (n) of the messages that appear in //NSUPRINT	/F taskname,MSGLVL,n Where n is 1, 2, or 3 with 1 providing the least and 3 providing the most information.	/F NSUPROC,MSGLVL,1
Start the address space for SecureSphere Agent for z/OS	/S taskname	/S NSUPROC
Terminate collection of audit data for a single DB2 subsystem	/F taskname,TERM,db2id Where db2id is the specific DB2 SSID. You cannot specify a data sharing group attach name.	/F NSUPROC,TERM,DB2A
Terminate collection of audit data in all the DB2 subsystems and stop the address space for SecureSphere Agent for z/OS	/P taskname	/P NSUPROC
Terminate collection of audit data in all the DB2 subsystems	/F taskname, TERM,ALL	/F NSUPPROC, TERM,ALL

Installing SecureSphere Agent for z/OS - Version 2.1

This section contains the following information:

Configuring SecureSphere Agent for z/OS Tasks 324

Before Installing and Configuring SecureSphere Agent for z/OS 324
Downloading and Installing SecureSphere Agent for z/OS 328
Configuring SecureSphere Agent for z/OS (on z/OS) 331
Starting, Managing, and Stopping SecureSphere Agent for z/OS 341

Configuring SecureSphere Agent for z/OS Tasks

The SecureSphere administrator must perform the tasks described below.

	Task Overview	For more information, see...
	Make the necessary preparations for installing SecureSphere Agent for z/OS.	Before Installing and Configuring SecureSphere Agent for z/OS on page 324
	Download and install the SecureSphere Agent for z/OS.	Downloading and Installing SecureSphere Agent for z/OS on page 328
	Configure the SecureSphere Agent for z/OS license.	Specifying the License Key on page 331
	Using impcfg, configure the data and configuration channels on which SecureSphere Agent for z/OS communicate with the SecureSphere Gateway. **Note**: A SecureSphere Agent listener and a SecureSphere Agent for z/OS listener cannot be defined on the same port.	Adding a SecureSphere Agent for DB2 z/OS Listener "Adding a SecureSphere Agent for DB2 z/OS Listener" on page 83

Before Installing and Configuring SecureSphere Agent for z/OS

There are a number of items you should verify and understand before beginning to install and configure SecureSphere agent for z/OS. This includes:

Information You Must Have Before You Begin 324
Terminology Used In This Guide 325
Roles and Assignments for the Installation and Configuration 325
Mainframe Software Requirements 326
Security Requirements 327
TCP/IP Requirements 327
Optimizing Performance 327
Supported Facilities 327

Information You Must Have Before You Begin

Verify that you have the following items:

Item	Additional Information
Credentials to access the Imperva FTP site	You use the credentials to access the FTP site and to download and install SecureSphere Agent for z/OS files.
License key for the SecureSphere Agent for z/OS	You must specify the license key when you install the SecureSphere Agent for z/OS on the z/OS host.

Terminology Used In This Guide

The product includes the following components.

- A component referred to as SecureSphere Agent for z/OS, that runs as a started task and gathers data about the DB2 subsystems being audited.
- A component referred to as the SecureSphere Gateway, that receives all the information gathered by SecureSphere Agent for z/OS.
- A component referred to as SecureSphere Management Server, that provides the collection rules to SecureSphere Agent for z/OS.

Roles and Assignments for the Installation and Configuration

Depending on the size and complexity of your IT organization, several people might contribute to the SecureSphere Agent for z/OS installation and configuration process. In most cases, these are the roles and their specific skills or knowledge.

- DB2 DBA or System Administrator
- Network Administrator
- Security Administrator
- System Programmer

The matrix shows:

- In order, the tasks that you perform during the installation and configuration (The tasks in the table are covered in the topics that follow.)
- In most cases, who in the organization will be involved in completing those tasks

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Before you install SecureSphere Agent for z/OS	Authorize any required TCP/IP connections and provide information that the System Programmer uses during product customization.		X		
	Define mainframe TCP/IP authority.			X	

Location in the Process	Installation and Configuration Task	Role			
		DB2 DBA	Network Administrator	Security Administrator	System Programmer
Downloading and installing SecureSphere Agent for z/OS	Install the product by downloading a job that allocates the data sets and then copies the product libraries to z/OS.				X
Configuring SecureSphere Agent for z/OS	Specify the license key and product libraries on z/OS.				X
	Application Program Facility (APF) authorize the LOAD library and make the authorization permanent following an IPL. (You do not have to IPL the system to install the product.)				X
	Specify the customization parameters specific to DB2 (such as the load libraries for the versions of DB2).	X			X
	Specify the customization parameters specific to TCP/IP (such as the port numbers for the data receiver and plan provider). **Note:** For more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.		X		X
Completing the configuration for the started task	Bind the DB2 packages for the product.	X			
	Authorize the started task for the product so that it can access the required resources.			X	
	Grant DB2 privileges to the user ID for the started task so that it can access the DB2 Catalog for any DB2 instance being audited.	X		X	
	Initialize and secure the rules data sets for the product so that it can only be modified by the started task.			X	X
	Specify a priority for the started task in Workload Manager (WLM).				X
	Modify the started task procedure and copy the procedure to the SYSPROC library,				**X**
Starting, managing, and stopping SecureSphere Agent for z/OS	Start the started task.				X

Mainframe Software Requirements

Before unloading and installing SecureSphere Agent for z/OS, verify that you have the following software installed and operational on your z/OS system.

- IBM z/OS version 1.8 or later (64 bit mode required)
- DB2 for z/OS version 8, 9 or 10
- IBM TCP/IP version 3.1 or later

Security Requirements

The table lists the security requirements for SecureSphere Agent for z/OS.

Element	Security Requirement
DB2	You must authorize the started task-user ID so that it can access the DB2 Catalog for any DB2 instance being audited.
Rules data sets	You must protect the rules data sets for SecureSphere Agent for z/OS so that it can only be modified by the started task. You will specify the rules data sets using the Local Rules Dataset Name customizable parameter when you configure SecureSphere Agent for z/OS.
Started task	For the product to run successfully, you must provide SecureSphere Agent for z/OS with adequate authority to operating system and database resources. Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task for the product uses TCP to communicate with the Imperva. If you are using RACF, the started tasks for the product must have an OMVS segment defined in RACF.

TCP/IP Requirements

You must have TCP/IP network connections between the LPAR where auditing is performed and the SecureSphere Gateway and SecureSphere Management Server.

Before installing the product, you will need the:

- TCPIP.DATA data set name
- TCP/IP port numbers for the data receiver and plan provider (for more information, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83)
- Host name for the data receiver and plan provider
- You will also need to define mainframe TCP/IP authority.

Optimizing Performance

The product is designed for optimal performance so that auditing activities never impact normal business transaction processing. Key performance features include:

- When available, use of zIIP processors
- No reliance on slow, resource-intensive database trace utilities
- Off loads audit data from mainframe so that analysis, reporting, and data storage expenses are not incurred on the mainframe

Supported Facilities

The product supports the following local attach facilities for DB2 on z/OS:

- Call Attach (CAF)

- Resource Recover Services (RRSAF)
- CICS
- TSO
- IMS

The product also supports DRDA for distributed connections.

Downloading and Installing SecureSphere Agent for z/OS

This topic contains information about how to download and install SecureSphere Agent for z/OS. It includes:

Downloading and Installing the Product 328
APF Authorizing the LOAD Library 329
Creating the ADMIN Library 330

Downloading and Installing the Product

The section describes the prerequisites and procedures required for downloading and installing SecureSphere Agent for z/OS and includes:

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance 328
Procedure for Downloading and Installing the Product 328
Procedure for Downloading and Installing the Cumulative Maintenance 329

Prerequisite for Downloading and Installing the Product or Cumulative Maintenance

To unterse the files, you must have installed TRSMAIN V4 or AMATERSE.



Note: AMATERSE is an enhanced replacement for TRSMAIN and it is strongly recommended that you upgrade from TRSMAIN V4 to AMATERSE.

For information about installing or upgrading to AMATERSE, see http://techsupport.services.ibm.com/390/trsmain.html.

Procedure for Downloading and Installing the Product

This section contains the procedures you follow to download and install the product for the first time or upgrade the product to a new version or release.



Note: When you download and install the product, also be sure to download and apply any cumulative maintenance included in the FTP directory. Skipping this step may cause the product to behave incorrectly.

If you have already installed the product and only need to install cumulative maintenance, see Procedure for Downloading and Installing the Cumulative Maintenance **"Procedure for Downloading and Installing the Product" on page 328.**

To download and install the product files:

1. From the FTP site, download the file readme.txt. This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the install file, from the FTP site, download the file unpack.jcl, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed product file to your mainframe system. The install process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.
4. Follow the instructions in the RECVBASE member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command to create the product datasets from the remaining members contained within the untersed dataset.

Procedure for Downloading and Installing the Cumulative Maintenance

This section contains the procedures you follow to download and install the cumulative maintenance.

To download and install the maintenance files for an existing installation:

1. From the FTP site, download the file readme.txt. This file describes the datasets contained within the directory. Additionally, it may contain special instructions regarding the download process that are not included in this document.
2. If JCL is needed to unterse the cumulative maintenance file, from the FTP site, download the file **unpack.jcl**, a JCL file that contains sample JCL using TRSMAIN or AMATERSE.
3. Transfer the tersed cumulative maintenance file to your mainframe system. The maintenance process is started by untersing a single dataset. This dataset is described in the readme.txt file. This dataset may be downloaded directly to your mainframe system if the mainframe system has an internet connection, or it may be downloaded to an interim system first and then uploaded to the mainframe.
4. Follow the instructions in the RECVFIXS member of the resulting untersed file. When submitted, this job will execute the TSO RECEIVE command and update your product libraries from the remaining members contained within the untersed dataset.

APF Authorizing the LOAD Library

The product uses dataspaces, cross memory services, and other functions that require APF authorization. These are common and necessary requirements of system level software. The library that contains SecureSphere Agent for z/OS LOAD modules (`?tomiumhlq`.LOAD) must be APF authorized.

You must also ensure that the authorization is permanent to prevent losing authorization at your next IPL.

To APF authorize the LOAD library, your system programmer must issue an APF command. The table shows examples of the commands.

Status of the Data Set for the LOAD Library	Example Command
Managed by the IBM System Management Service (SMS)	SETPROG APF,ADD,DSNAME=*?tomiumhlq*.LOAD,SMS
Not managed by SMS	SETPROG APF,ADD,DSNAME=*?tomiumhlq*.LOAD,VOLUME=volume

Once the LOAD library has been APF authorized, updates or changes made to the configuration using the Product Customization Facility must be done by someone with authority to update an APF authorized library. (This person is typically not a DBA.)

Creating the ADMIN Library

The product uses an administration (ADMIN) library to manage and maintain product keys and the associated product libraries. You must allocate and catalog this ADMIN library.



Note: You must create the ADMIN library only if you are installing the product for the first time.

Follow this process.

1. Locate the ALLOCATE member in the *?tomiumhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.
3. Submit the job to allocate the library.
   Result: The job allocates a data set with the format shown in the following table Data Set Details below.

Data Set Details

Item	Value
Data set format	Partitioned data set (PDS)
Record format	Fixed block (FB), 80-character logical records LRECL=80, RECFM=FB,blksize Where blksize is your site standard block size.
Allocated space	Two tracks and 10 directory blocks

Including the Product Libraries in Your Disaster Recovery Plan

The product includes the data sets listed in the table below. These resources should also be included in your backup and disaster recovery plan.

Data Set Name	Description
?tomiumhlq.ADMIN	This library contains product keys.
?tomiumhlq.CNTL	This library contains the control members for SecureSphere Agent for z/OS, including sample JCL.
?tomiumhlq.DBRMLIB	This library contains the DB2 definitions for SecureSphere Agent for z/OS.
?tomiumhlq.EXEC	This library contains the REXX executables needed to configure SecureSphere Agent for z/OS.
?tomiumhlq.LOAD	This library contains the executable LOAD modules needed to execute SecureSphere Agent for z/OS.
?tomiumhlq.MESSAGES	This library contains descriptions for product messages.
?tomiumhlq.MLIB	This library contains messages issued by the ISPF interface.
?tomiumhlq.MSG	This library contains the message modules used by SecureSphere Agent for z/OS.
?tomiumhlq.PLIB	This library contains ISPF panels used by SecureSphere Agent for z/OS.

Configuring SecureSphere Agent for z/OS (on z/OS)

This topic contains information about using the Product Customization Facility to configure SecureSphere Agent for z/OS and includes:

Accessing the Product Customization Facility 331
Specifying the License Key 331
Specifying the Product Libraries 332
Specifying the Customizable Parameters 332
Detailed Information About the Customization Parameters 335
Completing the Configuration 338

Accessing the Product Customization Facility

Follow this process to access the Product Customization Facility. You must access the Tomium Product Customization Facility if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

1. At the TSO prompt (option 6), specify the following command.

   `EX '?tomiumhlq.EXEC(TOMMCONF)' '?tomiumhlq'`

   Where ?tomiumhlq is the high-level qualifier for SecureSphere Agent for z/OS LOAD library that you specified when you installed SecureSphere Agent for z/OS.

   Result: The product displays the Product Customization Facility menu.

```
                 Tomium Product Customization          Row n to n of n
Command ===> _____________________________________ Scroll ===> CSR

   Product load library. . . ?tomiumhlq.LOAD

Type S to select a product for customization, B to BROWSE the $README member

   Product Name / Description                              Version
 _ License Management                                      nn.nn.nn
```

Specifying the License Key

You received a license key for SecureSphere Agent for z/OS when you purchased SecureSphere Agent for z/OS. This license key is required to run SecureSphere Agent for z/OS and protects the software from unauthorized use. You must specify the license key if you are:

- installing the product for the first time
- adding new keys or removing old keys

If the proper product keys are not present SecureSphere Agent for z/OS will fail.Follow this process to specify the license key.

1. Type **S** next to License Management.
2. Press Enter.
3. On the Tomium Enterprise Software Product Key Update panel, specify:

4. **Y** in the Manage Product Keys field
5. **Y** in the Manage Product Libraries field
6. Press Enter.

   Result: The panel redisplays with these values:
7. Type End on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility displays the next Enterprise Software Product Key Update panel in the series.

License Values

Field	Description
Product Name	Name of the family of products for this key
CPU Id	Processor id for which this key is valid
Expires	Expiration date for this key
Features	All feature codes in the key

Specifying the Product Libraries

You must specify the product libraries if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

This step ensures that there is a locator module in SecureSphere Agent for z/OS LOAD library. (The locator module indicates where the license keys are stored.) Without this module SecureSphere Agent for z/OS will not be able to perform product key validation and SecureSphere Agent for z/OS will fail. Follow this procedure to specify SecureSphere Agent for z/OS libraries.

1. On the Tomium Enterprise Software Product Key Update panel, specify:
   - The fully qualified data set name of the ADMIN library that you allocated in the Tomium Administration Library field (Do not specify quotes around the name.)
   - Your license key in the Product Key field
2. Press Enter.
3. Verify that the Status column displays Locator correct.
4. Type **End** on the command line and press Enter or press the appropriate function key.

   Result: The Product Customization Facility redisplays the Product Customization Facility menu.

   The table **Panel Field Descriptions** describes the remaining fields on the panel.

Panel Field Descriptions

Field	Description
LC	Use this field to update (U) or delete (D) libraries.
Product Library	Lists the Tomium Enterprise Software product LOAD libraries contained in the ADMIN data set library. Each library contains a locator module, which identifies the location of the ADMIN library.
Status	Describes the status of the locator module

Specifying the Customizable Parameters

You must specify the customizable parameters if you are:

- installing the product for the first time
- upgrading to a new version or release of the product

If you are upgrading and you want to use the existing values for the customization parameters, you can save the existing values by accessing the panel and pressing END to save and exit the panel.



Note: You must perform this step if you are installing or upgrading the product. Saving and exiting the panel activates the NSUUOPT module that contains the customizable parameters. If you are upgrading, saving and exiting the panel upgrades the module so that it is at the same version and release level as the product.

Follow this procedure.

1. On the Product Customization Facility menu, type S next to SecureSphere Agent for z/OS and press Enter.
   Result: The Product Customization Facility displays the SecureSphere Agent for z/OS Customization Options panel.

```
-------- Tomium Database Activity Monitor Customization Options Vnn.nn.nn ------
Command ===>
                                                                      More:    - +

    Product Load Library . . ?tomiumhlq.LOAD
    Options Module Name. . . NSUUOPT
    Note: Parameters Initialized to Tomium Recommended Values

SecureSphere Agent for z/OS  Database Activity Monitor Message Log Parameters:
 Message Data Set Name. . . . . --------
 Message Language . . . . . ENU                  ENU
 Message Set. . . . . NSU01                  NUS01
 Sysout (NSUPRINT) Message Level  2                  1 - 3  ( 3 = Verbose )

SQL Related Parameters:
 Package Collection ID  . . . . . NSUD210            DB2 Collection Name
 SQL Retry Delay. . . . . 1                  0 - 9999 Seconds
 Number of SQL Retries. . . . . 5                  0 - 9999 Attempts
 -DISPLAY LOCKS for -913 Retries. N                  N - Never
                                                     R - For Every retry
                                                     F - Only for Failure

Communication Parameters:
 Inactivity Disconnect Timeout  . 300                1 to 6000 Seconds
 Data Receiver Port Number. . . .                    1 to 65535
 Data Receiver Host Name. . . . .
 Plan Provider Port Number. . . .                    1 to 65535
 Plan Provider Host Name. . . . .


General Operating Options:
 Max Dataspace Size . . . . . 100                1 to 2047 Megabytes
 Local Rules Dataset Name . . . .

DB2 Environment Information:
```

```
   DB2 Version 8 Load Library . . .
   DB2 Version 9 Load Library . . .
   DB2 Version 10 Load Library . . .
   Resolve Group Attach Name. . . . N                    Y-Yes  N-No
   DB2 Subsystems Selected for Audit


 Press ENTER to update END to save and exit
       CANCEL to exit ignoring any changes made since the last update
```

Tomium Database Activity Monitor Customization Options



Note: For more information about configuring `Data Receiver Port Number and Plan Provider Port Number in SecureSphere`, see Adding a SecureSphere Agent for DB2 z/OS Listener **on page 83**.

2. Specify the values for the parameters. (You can reset all the parameters to SecureSphere Agent for z/OS defaults at any time by typing **DEFAULT** on the command line and pressing Enter.)
3. Press Enter.
4. Type **End** on the command line and press Enter or press the appropriate function key.

If you will be running multiple SecureSphere Agent for z/OSs on different LPARs, you can override the Product Load Library and the Options Module Name so that you can specify or change the customization parameters without leaving the panel.

Changing Customizable Parameters

Value You Want to Change on the Panel	Action to Take
Product Load Library	Specify the following command on the command line. NEWLIB *?tomiumhlq*.LOAD Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new library name in the Product Load Library field.
Options Module Name	Specify the following command on the command line. NEWOPT ?name Press Enter Result: The Product Customization Facility displays a confirmation dialog. Press Enter again. Result: The Product Customization Facility redisplays the panel with the new module name in the Options Module Name field.

Detailed Information About the Customization Parameters

The table provides detailed information about the customization parameters.

Parameter	Description	Default Value
Message Data Set Name	The name of the data set that contains SecureSphere Agent for z/OS message descriptions.	*?tomiumhlq*.**MSG**
Message Language	The language for the messages ENU (U.S. English) is the only valid value for this version of SecureSphere Agent for z/OS.	ENU
Message Set	The name of the message set to be used by SecureSphere Agent for z/OS NSU01 is the only valid value for this version of SecureSphere Agent for z/OS.	NSU01
Sysout (NSUPRINT) Message Level	The detail level for messages issued by SecureSphere Agent for z/OS Specify a numeric value between 1 and 3. 1—Least verbose. Only severe messages are displayed. 2—Verbose. Severe and warning messages are displayed. 3—Most verbose. All messages are displayed.	2
Package Collection ID	The collection ID All packages required for the audit extractor should be bound using the same collection ID. Specify a collection ID for the bound that is from 1 to 8 alphanumeric characters in length. This ID must be unique to the agent instance. **Note**: Make a note of this field because you will need it again later in the configuration process.	NSUD210
SQL Retry Delay	Indicates the number of seconds that any component of SecureSphere Agent for z/OS should wait before retrying the operation if it encounters a time out condition. Specify a numeric value between 0 and 9999.	1
Number of SQL Retries	The number of times that any component of SecureSphere Agent for z/OS will retry an SQL operation before failing. Specify a numeric value between 0 and 9999	5
-DISPLAY LOCKS for -913 Retries	Indicates the action SecureSphere Gateway takes for locks for -911 and -913 retries. If a time out condition occurs, the extractor can issue a -DISPLAY LOCKS command to DB2. The output from the command appears in NSUPRINT. Specify either: N—Never display locks. R—Display locks at each retry. F—Display locks only when the operation fails.	N
Inactivity Disconnect Timeout	Specifies a communications timeout value in seconds for the collector If this length of time is reached without any interaction with the SecureSphere Gateway, the connection will be dropped and retried. The value that you specify should be set to a multiple of the heartbeat values used by the SecureSphere Gateway. If the value is set to 0, the timeout is disabled. Specify a numeric value between 1 and 6000.	300

Parameter	Description	Default Value
Data Receiver Port Number	The port number that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same port number using `impcfg`. For more information, see **SecureSphere Administration Guide**. Specify a value from 1 to 65535. **Note**: For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener on page 83.	17671
Data Receiver Host Name	The domain name or the IP address that the SecureSphere Gateway uses to receive the audit data from the collector. You must define the same IP address using `impcfg`. For more information, see **SecureSphere Administration Guide**.	There is no default value.
Plan Provider Port Number	The port number of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for z/OS. **Note**: SecureSphere Agent for z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for z/OS from the SecureSphere Gateway (see **SecureSphere User Guide**). Specify a value from 1 to 65535. **Note**: For more information about how to configure this in SecureSphere, see Adding a SecureSphere Agent for DB2 z/OS Listener **on page 83.**	17670
Plan Provider Host Name	The domain name or the IP address of the SecureSphere Gateway that provides the collection rules to SecureSphere Agent for z/OS. **Note**: SecureSphere Agent for z/OS policies are defined on the SecureSphere Management Server, but they are sent to SecureSphere Agent for z/OS from the SecureSphere Gateway (see **SecureSphere User Guide**).	There is no default value.
Max Dataspace Size	The maximum size allocation, in megabytes, for the data collection dataspace. Specify a numeric value between 1 and 2047.	100
Local Rules Dataset Name	The fully qualified name of the data set used for the local copy of the rules (each SecureSphere Agent for z/OS started task has its own local copy of the rules data sets). Specify any valid dataset name that complies with your site naming requirements. It is recommended that the LPAR is included as a node in the dataset name.	There is no default value.
DB2 Version 8 LOAD Library	Data set name for the DB2 version 8 LOAD library. This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
DB2 Version 9 LOAD Library	Data set name for the DB2 version 9 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.

Parameter	Description	Default Value
DB2 Version 10 LOAD Library	Data set name for the DB2 version 10 LOAD library This data set name is obtained from the DB2 started task. Provide an appropriate LOAD library for each DB2 version used for audited subsystems.	There is no default value.
Resolve Group Attach Name	For the DB2 subsystems that you specify with the DB2 Subsystems Selected for Audit parameter, specifies whether or not group attach names should automatically resolve to all members of the data sharing group. Y - Resolve group attach names to all members. N - Use N if a data sharing member subsystem name is the same as the group attach name. The group is not audited.	Y
DB2 Subsystems Selected for Audit	One or more DB2 subsystem IDs (or data sharing group attach names) to be audited Separate multiple subsystem IDs by commas. Do not use spaces between subsystem IDs and commas. A space terminates the comma-delimited subsystem list. You can specify that SecureSphere Agent for z/OS gathers data for a maximum of 250 DB2 subsystems or members of a data sharing group. If you have more than 250, you can start another SecureSphere Agent for z/OS but you must also be sure that each DB2 subsystem is specified for only one of SecureSphere Agent for z/OSs.	There is no default value.

Completing the Configuration

This topic contains information about the tasks you must complete to finish configuring SecureSphere Agent for z/OS outside of the Product Customization Facility. It reviews the following topics:

Binding Packages for the Product 338
Determining the Remaining Tasks to Complete for the Started Task 339
Authorizing the Started Task for the Product 339
Granting DB2 Privileges 339
Initializing and Securing the Rules Data Set 340
Specifying the Priority Using WLM 340
Modifying the Started Task Procedure 340

Binding Packages for the Product

The product requires that you perform a DB2 bind on those packages it uses during the audit process. You must perform a DB2 bind if you are:

- installing the product for the first time
- upgrading to a new version or release of the product
- installing maintenance and one or more of the packages have changed

Follow this process to bind the packages.

1. Locate the NSU1000 member in the ?hlq.CNTL data set.
2. Modify the sample JCL using the instructions included in the member.

3. Submit the job.
4. Verify that the job competed successfully and that all the return codes were zero.

Determining the Remaining Tasks to Complete for the Started Task

The remaining information in this topic covers the tasks that you must complete for the started task. You must complete all the remaining tasks in this topic if you are:

Installing the product for the first time

Upgrading to a new version or release of the product and you want to use a new started task (You do not have to complete these if you want to use the existing started task.)

Authorizing the Started Task for the Product

Before you can start the product, you must authorize:

- The user ID for the started task so that it can access the necessary data sets (such as the rules data set, the APF authorized LOAD library, and any of the remaining product libraries)
- The started task so that is can access the TCP/IP stack on z/OS

Using your security administration product (such as RACF), you should establish application profiles for the started task. For example, the started task uses TCP/IP to communicate with the data receiver. If you are using RACF, the started tasks must have an OMVS segment defined in RACF.

Granting DB2 Privileges

The started task must be granted EXECUTE authority on the NSU packages in the NSU collection. This must be done for each non-data sharing DB2 subsystem ID and for at least one member in any data sharing group. If a data sharing group has had privileges granted on a different LPAR setup, it does not need to be repeated at this stage.

1. Locate the NSU2000 member in the *?tomiumhlq*.CNTL data set**.**
2. Modify the sample JCL using the instructions included in the member.
3. If multiple non-data sharing subsystems will be supported on the LPAR, you must duplicate the GRANT step in the job for each subsystem. The table **Variable Descriptions** below provides the descriptions for the variables in the jobs and indicates the action you take for the value in the duplicated GRANT step.
4. Submit the job.
5. Verify that the job competed successfully and that all the return codes were zero.

Variable Descriptions

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*ssid*	ID of the DB2 subsystem or name of the data sharing group	Specify a GRANT step and ?ssid for each non-sharing DB2 subsystem.
?*db2exit*	Name of the library for the DB2 exit library	If the DB2 subsystem uses a different library, specify the name of the library in the GRANT step.
?*db2load*	Name of the DB2 LOAD library	If the DB2 subsystem uses a different LOAD library, specify the name of the library in the GRANT step.
?*dsntiad*	The name of the plan associated with the LMOD DSNTIAD For a default installation, it is DSNTIAxx where xx is the version (such as 81 or 91).	No change required.

Variable	Value to Specify	Action to Take in the Duplicated GRANT Step
?*dsnrunlb*	The name of the library where DSNTIAD resides The library must be APF authorized.	No changed required.
?*db2coll*	The name of the collection ID for NSU packages Specify the same value that you specified for the Package Collection ID customizable parameter.	No change required.
?*stcuser*	PUBLIC or to the name of the started task for SecureSphere Agent for z/OS	If you duplicate the GRANT step, do not change this value.

Initializing and Securing the Rules Data Set

The product uses a rules processing engine to isolate transactions to be reported from other, routine transactions. For each SecureSphere Agent for z/OS started task, the rules data set must be initialized before you can start SecureSphere Agent for z/OS or customize the rules data set.

You specified the rules data set using the Local Rules Dataset Name customizable parameter when you configured the product. Follow this procedure to initialize and secure the rules data set.

1. Locate the NSU3000 member in the *?tomiumhlq*.CNTL data set.
2. Modify the sample JCL using the instructions included in the member. The data set name for `?rulesdsn` must match the value specified for the Local Rules Dataset Name customizable parameter (see **SecureSphere User Guide**) and should include the LPAR as a node in the name.
3. Submit the job.
4. Use your security administration product (such as RACF) to protect the rules data set so that only its owning started task can update it.
5. Verify that the job competed successfully and that all the return codes were zero.

Specifying the Priority Using WLM

To further optimize performance, set the Workload Manager (WLM) goal and importance of the started task equal to or higher than that of the DB2 subsystems being audited. With this priority, SecureSphere Agent for z/OS will run faster and more reliably.

Modifying the Started Task Procedure

Follow this procedure to modify the started task procedure and to copy the procedure to the SYSPROC library.

1. Locate the NSUPROC member in the ?hlq.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLL=2 parameter on the EXEC statement. (The COLL parameter is optional. The default is COLL=1.)
4. Copy the JCL to your SYSPROC library.

Starting, Managing, and Stopping SecureSphere Agent for z/OS

This topic contains information about starting and managing SecureSphere Agent for z/OS and includes:

Requirements and Restrictions for Starting SecureSphere Agent for z/OS 341
Modifying the Started Task Procedure and Starting the Started Task 341
Using Operator Commands to Stop and Manage the Product 341

Requirements and Restrictions for Starting SecureSphere Agent for z/OS

SecureSphere Agent for z/OS has these requirements and restrictions.

- If you are using other DB2 monitoring or auditing products at your site, you must start SecureSphere Agent for z/OS before you start the other monitoring or auditing products.
- Do not start more than one SecureSphere Agent for z/OS to audit the same DB2 subsystem or member of a data sharing group.

Modifying the Started Task Procedure and Starting the Started Task

Follow this procedure to start the started tasks.

1. Locate the NSUPROC member in the *?tomiumhlq*.CNTL library.
2. Modify the sample JCL using the instructions included in the member.
3. If you are using CA Detector for DB2 for z/OS, specify the COLLID=2 parameter on the EXEC statement. The COLLID parameter is optional. The default is COLLID=1.
4. Copy the JCL to your SYSPROC library.
5. Perform the appropriate action. If you want to use:
   - SDSF, specify /`s taskname`
   - An MVS operator command, specify `S taskname` or `START taskname`

Using Operator Commands to Stop and Manage the Product

The table below describes the MVS operator commands that you can specify from a console to manage SecureSphere Agent for z/OS. In the command example, replace `taskname` with job name assigned by MVS to the started task address space. The table shows the tasks, the commands to specify, and an example using NSUPROC as the `taskname`.

Task You Want to Perform	Command to Specify	Example
Delete the dataspace associated with the collection process for a DB2 subsystem	/F `taskname`,MAINT,DELDSP, `db2id` where `db2id` is the ID of the DB2 subsystem. **Note**: Before you can delete the dataspace, you must terminate collection of the audit data using the TERM command shown below in this table.	/F NSUPROC,MAINT, DELDSP,DB2A

Task You Want to Perform	Command to Specify	Example
Resize the dataspace associated with the collection process for a DB2 subsystem (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F **taskname**,MAINT,RSZDSP, **db2id**,**nnnn** Where: **db2id** is the ID of the DB2 subsystem **nnnn** is a number between 1 and 2047	/F NSUPROC,MAINT, RSZDSP,DB2A,500
Resize the dataspace associated with the collection process for all DB2 subsystems (If the change is permanent, you must update the Max Dataspace Size customization parameter using the Product Customization Facility.)	/F `taskname`,MAINT,RSZDSP, ALL,`nnnn` Where `nnnn` is a number between 1 and 2047.	/F NSUPROC,MAINT, RSZDSP,ALL,500
Set the verbosity level (n) of the messages that appear in //NSUPRINT	/F `taskname`,MSGLVL,`n` Where `n` is 1, 2, or 3 with 1 providing the least and 3 providing the most information.	/F NSUPROC,MSGLVL,1
Start the address space for SecureSphere Agent for z/OS	/S `taskname`	/S NSUPROC
Terminate collection of audit data for a single DB2 subsystem	/F `taskname`,TERM,`db2id` Where `db2id` is the specific DB2 SSID. You cannot specify a data sharing group attach name.	/F NSUPROC,TERM,DB2A
Terminate collection of audit data in all the DB2 subsystems and stop the address space for SecureSphere Agent for z/OS	/P `taskname`	/P NSUPROC
Terminate collection of audit data in all the DB2 subsystems	/F *taskname*, TERM,ALL	/F NSUPPROC, TERM,ALL

CHAPTER 15

Gateway High Availability

The term "High Availability" refers to SecureSphere's ability to maintain connectivity and monitoring even when a SecureSphere appliance fails.



Note: Two Gateways in a High Availability deployment must be configured identically (same policies, objects, *etc.*)

This chapter describes the High Availability options for deploying SecureSphere, and includes:

Layer 2 High Availability Deployments 343
Layer 3 (Proxy) High Availability Deployments 347
Other High Availability Deployments 349

Layer 2 High Availability Deployments

It is possible to deploy High Availability at layer 2 as follows:

At the Network Level 343
At the SecureSphere Level 344

At the Network Level

Examples of layer 2 High Availability deployments at the network level include:

- Link Aggregation (Etherchannel) on page 344
- RSTP (Rapid Spanning Tree Protocol)

Link Aggregation (Etherchannel)

One or more SecureSphere Gateways can support link aggregation. For example, two interfaces on a SecureSphere Gateway can be connected to two interfaces on a network load balancer. Traffic can pass through both connections. For example, uplink traffic can travel through the first interface card while downlink traffic goes through the second interface card.

In bridge mode, each SecureSphere Gateway includes four network interfaces dedicated to application security. So it is possible to aggregate traffic through two connections. If the load balancer has 100Mbps Fast Ethernet interfaces, then aggregating links can also increase total throughput. Even if the traffic is split between the two segments, SecureSphere can accurately inspect all traffic and block attacks.

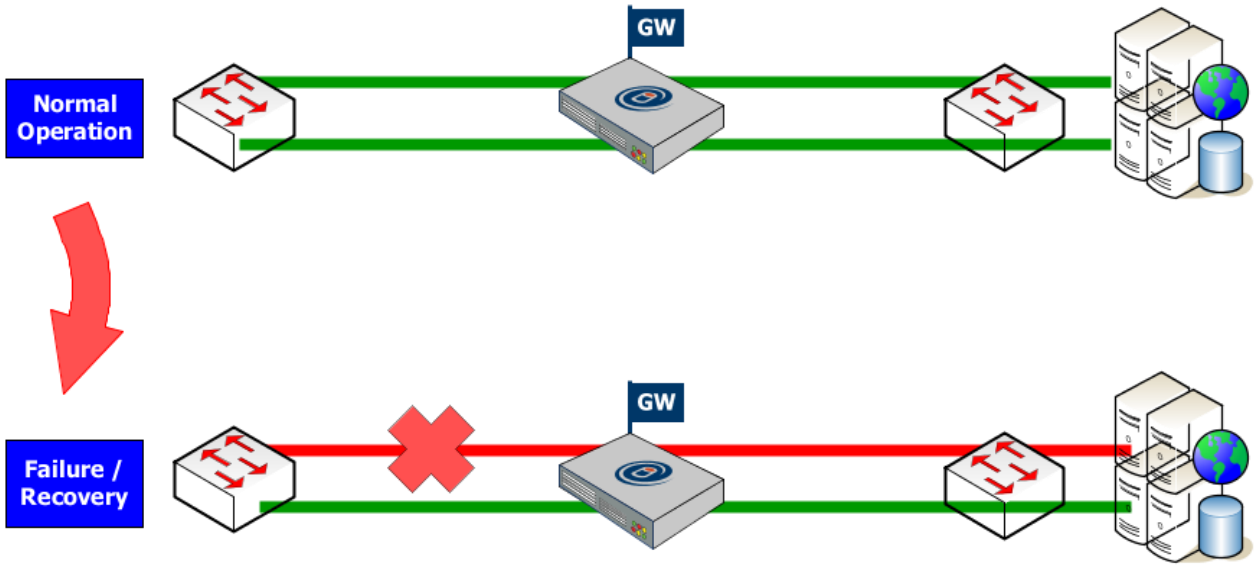


Figure 70: Link Aggregation

If an Ethernet cable is disconnected or a network interface fails, then traffic will continue to be forwarded through the active link on the SecureSphere Gateway.

At the SecureSphere Level

Examples of layer 2 High Availability deployments at the SecureSphere level include:

- IMPVHA Protocol — Active-Passive and Active-Active Failover on page 344
- Bridge STP on page 345

IMPVHA Protocol — Active-Passive and Active-Active Failover

IMPVHA is a proprietary redundancy protocol developed by Imperva for environments which do not have a redundant network architecture and STP cannot be implemented. For some environments, STP convergence times may be unacceptably long or STP may conflict with existing protocols, such as RSTP. In these situations, the Imperva High Availability (IMPVHA) protocol is the ideal solution.

With IMPVHA, two SecureSphere Gateways can be configured as layer 2 bridges in either active-passive or active-active mode. The configuration and failover mechanism is similar to VRRP, except that when a failover occurs, the backup device informs connected devices to redirect traffic via ARP requests rather than assuming the primary device's IP address. When an IMPVHA pair is deployed, the backup Gateway sends periodic loopcheck broadcast messages. If no response is received within the configurable failover time (default is 0.5 seconds), the backup Gateway becomes active.

Since a SecureSphere Gateway supports two bridges through its four network interface cards, it is possible to configure one bridge as the IMPVHA primary for one network and the second bridge as a backup for another network. In this configuration, two SecureSphere Gateways can support an active-active failover configuration.

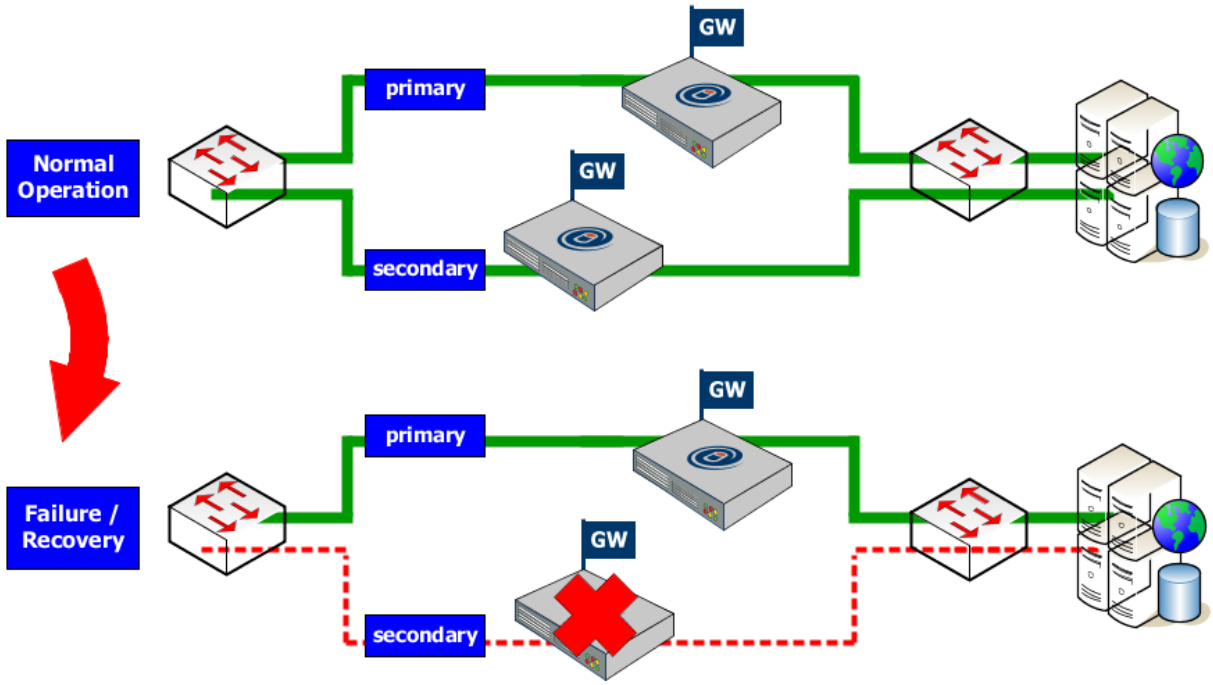


Figure 71: IMPVHA

IMPVHA — Configuration

IMPVHA is configured for each SecureSphere Gateway using the `impcfg` command line utility. Configure each Gateway as Bridge IMPVHA with IMPVHA on.

For more information, see Configuring a Gateway as a Bridge on page 72.

Bridge STP

SecureSphere can be deployed in bridge mode in existing high-availability deployments, for example, STP. One of the SecureSphere Gateways is designated as the master and the other as its backup. Initially, the network directs traffic destined for the server to the master.

If the master Gateway fails, the failure appears to the network as a failure of a switch port. Connected devices automatically recognize that the failed Gateway is no longer reachable and then redirect traffic to the backup Gateway, which becomes the new master Gateway.

If the previous master is restarted, it becomes the backup.

Because the two SecureSphere Gateways are deployed as bridges (that is, they have the same policies and the SecureSphere Management Server sees them as two active Gateways), TCP connections are negotiated directly between the client and the back-end server. A failover event does not disrupt TCP connections or affect user sessions.

For more information, see Configuring SecureSphere on page 46.

Bridge STP — Active-Passive Failover

In this deployment, only the SecureSphere Gateway configured as the master is active. The backup SecureSphere Gateway is in standby mode, waiting to take over if the first SecureSphere Gateway fails.

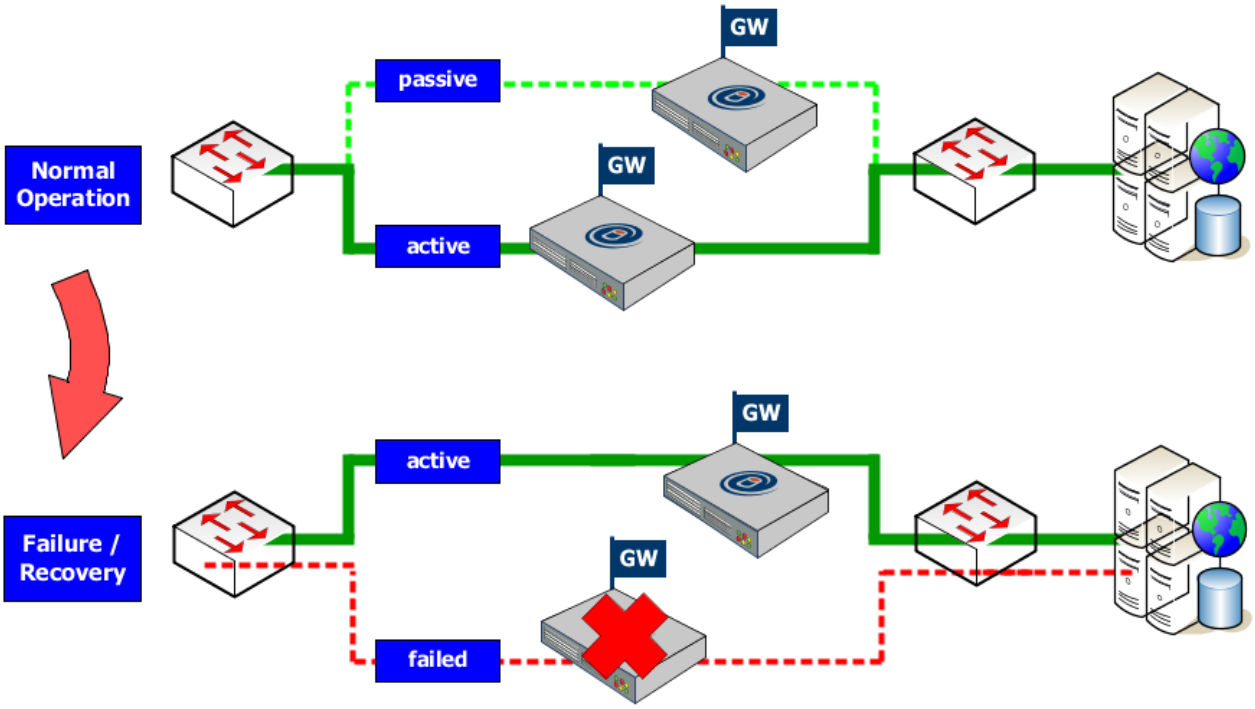


Figure 72: Active Passive Failover

This deployment is somewhat inefficient because at any given time, one of the SecureSphere Gateways is idle — it is functioning properly but is not processing any traffic.

This deployment can also be used with both transparent and non-transparent reverse proxies.

Bridge STP — Active-Active Failover

This deployment is the same as the previous one, except that both SecureSphere Gateways are active and monitor traffic simultaneously. If one of them fails, all traffic flows through the other Gateway. Total network capacity is reduced until the failure is corrected.

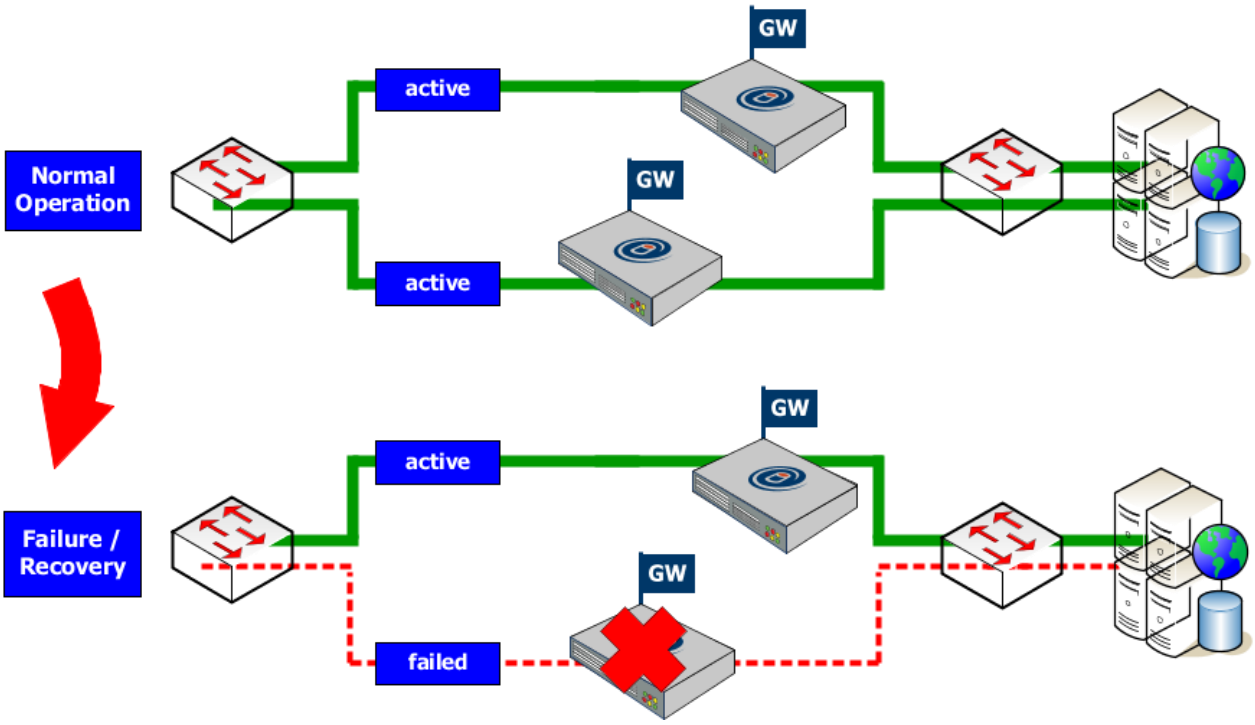


Figure 73: Active-Active Failover

This deployment supports load sharing if sessions are sticky, that is, the same session always passes through the same Gateway.

When configuring such a solution, ensure that each Gateway is able to handle the bandwidth of both Gateways, should one of them fail.

Redundant Architecture (STP) — Configuration

If STP or a similar capability is available in the network, configure the Gateways (with `impcfg`) as either:

- Bridge IMPVHA with IMPVHA off
- Bridge STP with STP on

For more information, see Configuring SecureSphere on page 46.

Layer 3 (Proxy) High Availability Deployments

It is possible to deploy High Availability at layer 3 as follows:

- At the Network Level on page 348
- At the SecureSphere Level on page 349



Note: Proxy deployments are relevant for Web traffic only. For more information, see Topologies and Deployment on page 23.

At the Network Level

SecureSphere is often deployed as a direct replacement for legacy reverse proxy appliances. In many cases, administrators choose to configure SecureSphere as a bridge because it fits into the existing architecture and reduces the operational burden associated with Web proxies. However, in some cases, administrators deploy SecureSphere as in proxy mode to meet architectural requirements or for content modification.

The SecureSphere Web Application Firewall supports both reverse proxy and transparent proxy configurations. Both proxy configurations offer content modification, including cookie signing and URL rewriting. Transparent proxy mode enables transparent deployment without network or DNS changes.

Examples of layer 3 High Availability deployments at the network level include:

Load Balancer Integration on page 348

Load Balancer Integration

In proxy mode, one or more SecureSphere Gateways are deployed as either a Reverse Proxy or a Transparent Reverse Proxy. A load balancer balances the traffic between the Gateways and the Gateways forward the traffic to the Web servers. It is possible to configure load balancer to work in active-active or active-passive modes.

In this mode, the IP address of the Web site resolves to the SecureSphere Gateway's IP address. If SSL is used, then the Gateway should be configured to terminate the SSL connection. Note that in proxy mode, SecureSphere establishes a new connection to the Web server on behalf of the client.

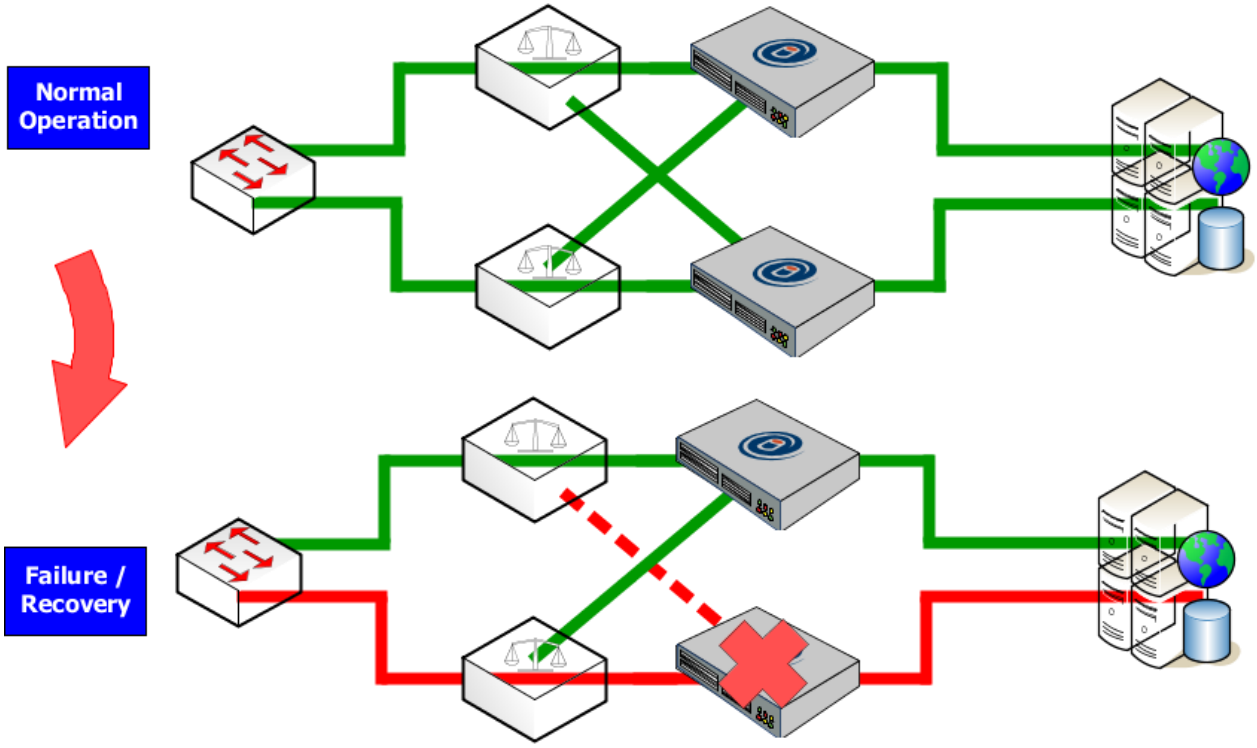


Figure 74: Load Balancer Integration

At the SecureSphere Level

Examples of layer 3 High Availability deployments at the SecureSphere level include:

- Redundant Architecture (VRRP) — Configuration on page 349

Redundant Architecture (VRRP) — Configuration

VRRP is suitable for a deployment where the SecureSphere Gateway has an IP address, that is, it is not configured as a bridge or as a transparent reverse proxy, but as one of the following:

- a non-transparent reverse proxy
- a listener for DB Agents

To configure a SecureSphere Gateway for VRRP, configure the aliases as virtual. For more information, see Configuring Aliases on page 181.

Other High Availability Deployments

Other High Availability deployments include:

- Fail-Open Bridge on page 350
- Sniffing Gateway High Availability on page 350

Fail-Open Bridge

Fail-open configuration preserves uptime without the cost or management effort of building and maintaining a redundant architecture. In the event of an appliance failure, SecureSphere's specialized network interface card detects the failure and physically completes the connection through the SecureSphere Gateway. The NIC card will fail open in milliseconds, minimizing network downtime.

Though connectivity is maintained, application servers will not be monitored or protected from attacks until the SecureSphere Gateway resumes operations.

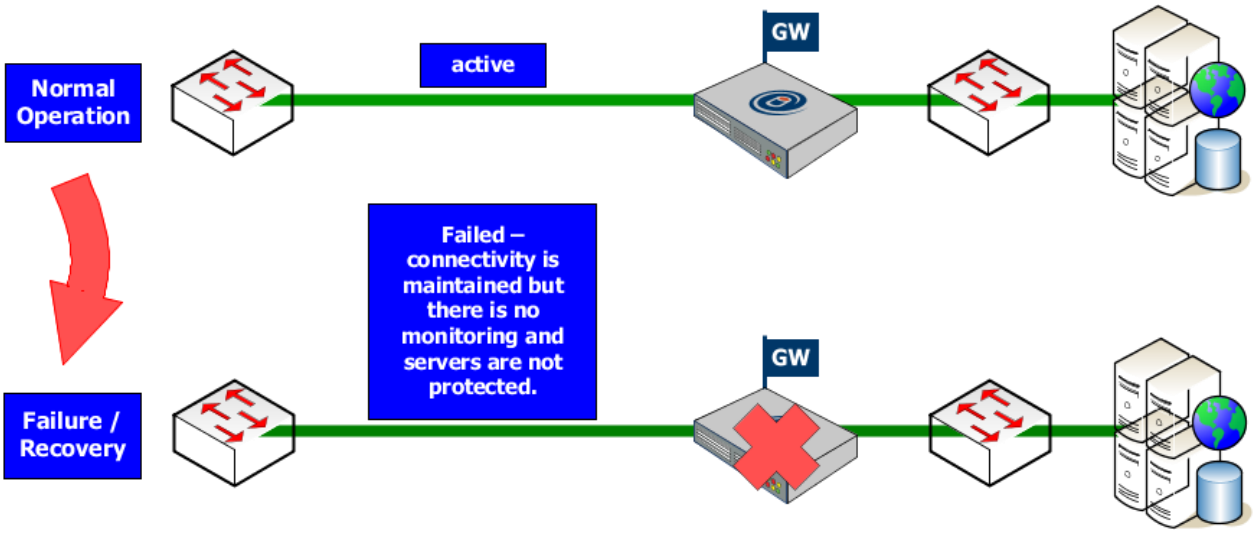


Figure 75: Fail Open

Note: A SecureSphere Gateway deployed in sniffing mode provides a similar level of connectivity continuity in the event of failure: traffic continues to flow through the network but it is not monitored.

Fail Open — Configuration

The Gateway appliance is configured as fail open by default. When you first connect the Gateway appliance to the network, no sites or server groups are defined, so no policies are implemented, nothing is monitored or blocked, and all traffic is passed through the appliance.

You can change the mode using the `impctl` command line utility. For more information, see Configuring SecureSphere on page 46.

Sniffing Gateway High Availability

Configuring SecureSphere as a sniffing Gateway enables organizations to protect critical servers without introducing a new point of failure. It is a lower price alternative to deploying two or more redundant SecureSphere Gateways.

To deploy SecureSphere as a sniffing Gateway, connect it to an open SPAN port or a network TAP to observe traffic. A second connection to an active port on the switch allows SecureSphere to block malicious connections by sending TCP resets to the server.

In the event of a SecureSphere Gateway failure, network traffic is unaffected, but it will not be monitored or protected until the SecureSphere Gateway becomes operational again.

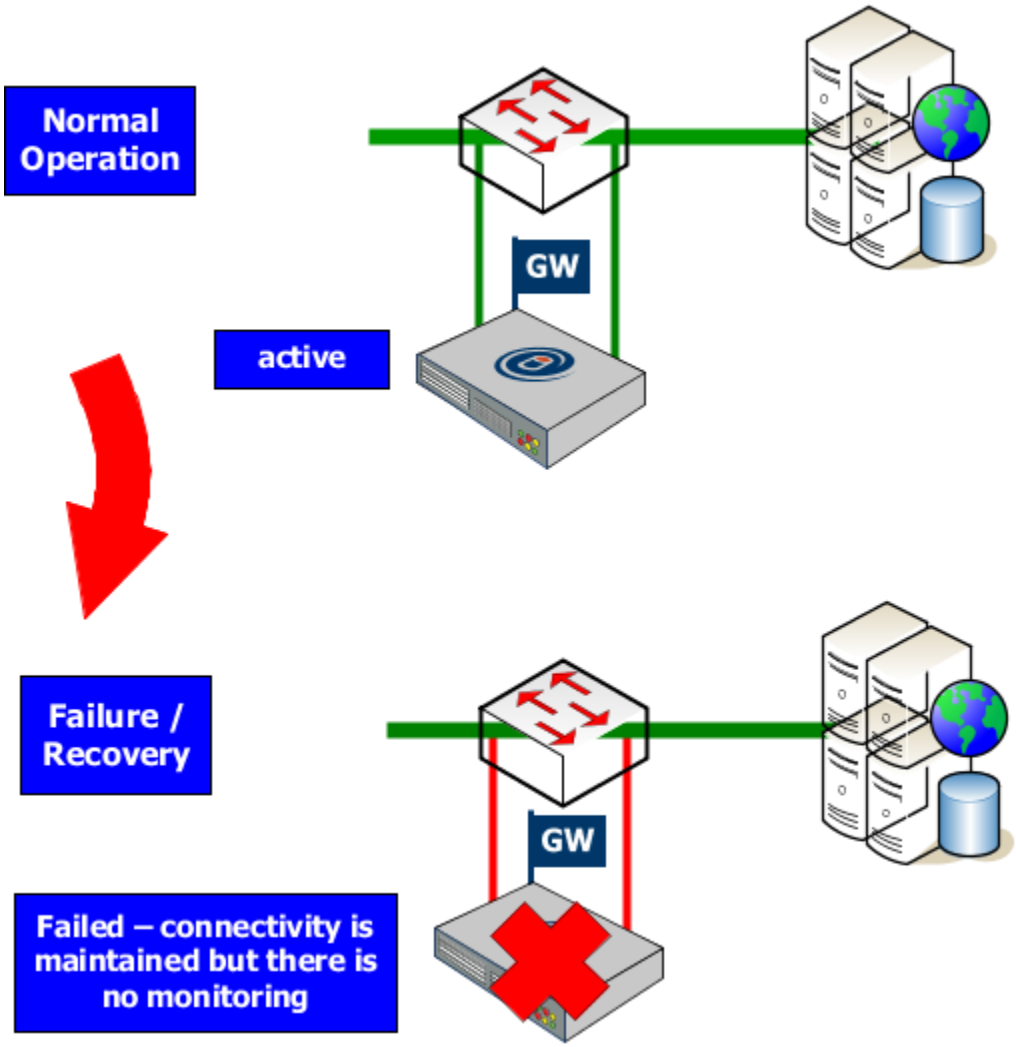


Figure 76: Network Monitor - No HA

For some organizations, it may be imperative to monitor and audit all Web or database traffic without disruption. These organizations can deploy multiple SecureSphere Gateways in non-inline mode. If one of the Gateways fail, the other Gateway will continue to monitor and record traffic.

In this configuration, each Gateway should be managed by a separate Management Server or by using the integrated software management option (Onebox).

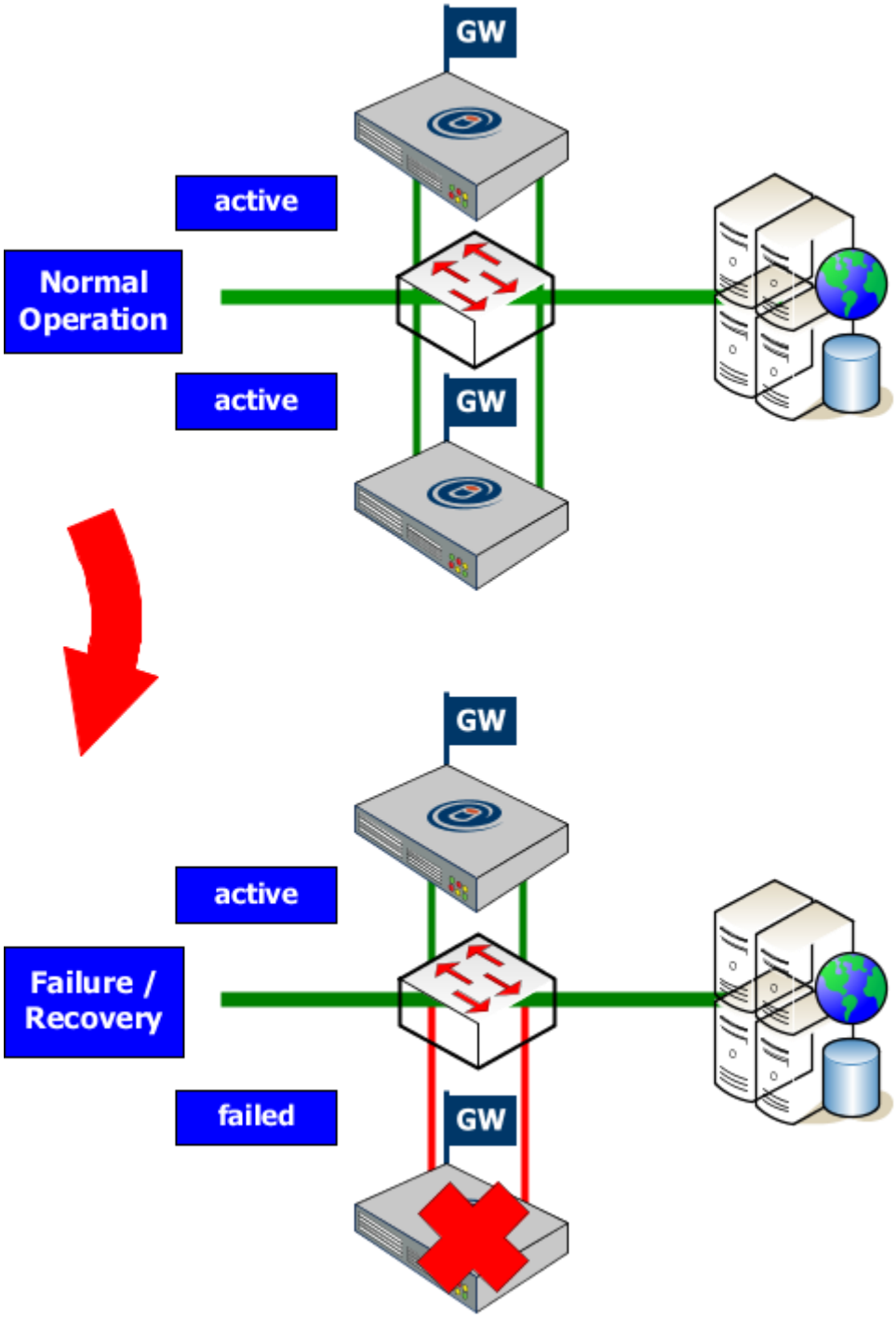


Figure 77: Sniffing - Redundant Gateways

CHAPTER 16

Management Server High Availability (MX-HA)

This chapter describes High Availability options for SecureSphere Management Servers (MXs), and includes:

Management Service-High Availability(MX-HA) Overview 353
Management Server-High Availability(MX-HA) Implementation 354
Management Server High Availability (MX-HA) Components 354
Before Installing Management Server High Availability (MX-HA) 355
Installing Management Server High Availability (MX-HA) 361
After Installing Management Server High Availability (MX-HA) 365
Monitoring Management Server High Availability (MX-HA) 368

Management Service-High Availability(MX-HA) Overview

The SecureSphere system comprises two main components, the Gateway and the Management Server (MX). Real time protection is the primary task of the Gateway, whereas the MX's main roles are to configure the system, collect events from the Gateway, analyze them and display resulting alerts.

The SecureSphere Gateway is a mission-critical component — if a Gateway fails, the Web and database servers behind the Gateway are no longer protected. On the other hand, if a SecureSphere MX fails, protection is not interrupted.

A MX failure which continues for an extended period of time will impact the level of protection which the SecureSphere Gateways provide, for the following reasons:

- **Profiling**: Application Profiling is performed by the MX based on data collected from the Gateways.
- **Policies and Profiles**: No changes can be made to existing profiles or policies.
- **Alerts**: The Gateway passes events to the MX, which stores and analyzes them and displays alerts derived from the events. If connectivity to the MX is down, the Gateway saves events locally for later transmission, but the Gateway will eventually overwrite older events as available disk space is reduced. When connectivity to the MX is restored and the Gateway transmits its store of accumulated events to the MX, the MX will have incomplete data. Also, alerts normally pushed to predefined recipients via email now remain unnoticed.
- **Auditing**: This uses huge amounts of storage. These data are stored on the Gateway, but unless archived regularly (a MX task) the newest auditing data are lost.



Note: In an MX-HA environment, there are many configuration changes which cannot be performed using the command line tools `impcfg` and `impctl`. For more information, see Command Line Tools and MX-HA on page 58.

Management Server-High Availability(MX-HA) Implementation

The MX-High Availability capability uses redundant MXs in a fully-automatic active/standby failover implementation, requiring no user interaction. The system senses the loss of the active server, and the failover mechanism begins. In the field the typical failover time period (which depends on the size of the system, and time elapsed since the last scheduled database synchronization) has been under measured as under 10 minutes, and the maximum time encountered was 30 minutes.

- The HA configuration comprises two MXs in the active/standby mode. Although only one server is active (i.e., managing the SecureSphere system), both servers are running to allow database synchronization (using a standard Oracle process).
- Database synchronization is a scheduled process, the frequency and timing of which is decided by the system administrators. This means that whenever the active MX fails, there is always some data on its disk that is not mirrored on the standby MX.
- A heartbeat function (Linux) enables close monitoring of the active MX. During a server or network failure, the heartbeat function triggers the failover process and dispatches system logs (syslogs) to warn users that the active server requires attention.



Note: In the hosts files on each of the MX-HA servers, the host's name must appear **exactly** once.

Management Server High Availability (MX-HA) Components

The following components are included in the Management Server-High Availability solution:

Linux Heartbeat 355
Oracle Standby Database (Data Guard) 355
SecureSphere Server 355
HA Health Check 355
Imperva Watchdog 355

Linux Heartbeat

Linux heartbeat is a Linux utility which enables implementing active-passive clusters. The heartbeat is the heart of MX-HA that is responsible for the database and MX and where they run.

The heartbeat configuration includes the following resources:

- Virtual IP address (VIP)
- Database server
- SecureSphere server

Once the heartbeat is started, all the resources are allocated to a specific server.

The heartbeat checks the status of the resources every minute. If one of the resources fails to run on the server, all resources are moved to the other server.

Oracle Standby Database (Data Guard)

Database synchronization is based on Oracle standby database (or Data Guard). Once MX-HA is installed, the database on the primary server is configured to support Oracle standby database. The database on the secondary server is deleted and copied from the primary server as a standby database.

After the installation, the standby database is constantly synchronized with the primary database using Oracle solution.

If the standby database fails to synchronize with the primary, it is recreated from the primary database.

SecureSphere Server

SecureSphere server is one of the resources in the heartbeat, but it is not modified during the MX-HA installation. The only change performed on the SecureSphere server is how it is started.

HA Health Check

In order to verify that everything is up and running, there is a health check mechanism that checks both servers. The heart of this mechanism is the `healthCheck.sh` script.

Imperva Watchdog

The Imperva watchdog script checks the heartbeat status, and if it is invalid, it restarts the heartbeat. The watchdog checks the heartbeat only after a successful start of the MX-HA using `impctl`. If MX-HA is stopped manually, it is removed from the watchdog's watch list.

Before Installing Management Server High Availability (MX-HA)

This section reviews items that need to be taken before installing the Management SErver in High Availability (MX-HA) mode, and includes the following:

Hardware and Software Requirements 356

Pre-Installation Tasks 356

Hardware and Software Requirements

In MX-HA, the private network that links the two MX servers is used to constantly copy incremental database and file changes. Additionally, during installation and occasionally at other times, all database data will need to be transferred on that network. While there is no minimum required bandwidth, it is recommended that the network connection between the two be reliable and quick, and fast enough to handle the required amount of traffic for your deployment.

Management Server High Availability (MX-HA) requires a specific hardware and software configuration that includes:

- Two MXs

  MX-High Availability cannot be installed on Gateways or Onebox configurations.
- You must have licenses for both servers.
- Both servers must have the same amount of memory (RAM).
- It is recommended that both servers have the same amount of disk space, otherwise failover to a server with less disk space will negatively impact performance and can in some circumstances even fail (for example, when the server needs more space than the failover machine can allocate).
- Both servers must have the same version of SecureSphere installed.

  MX-HA is supported in SecureSphere versions 6.0.5.6238 and later.
- Each server must have the following two network interfaces:
  - An interface for public network.
  - An interface for interconnect (using cross-link cable or other connection) to the other server. This interface is used by Linux heartbeat and by Oracle to synchronize the standby database.
- SSH trust between the servers for both `root` and `oracle` users.
- Well-defined and unique host names on both servers.

Pre-Installation Tasks

This section lists the pre-installation tasks that need to be conducted before installing the Management Server in High Availability Mode and includes the items listed below.



Note: The public IP addresses of both MX servers must be on the same subnet. If the servers are located at different sites, there must be a VLAN between the sites with the same subnet.

Install the Latest Patch 356
Configure the Interconnected Interfaces 357
Test the Interconnected Interfaces 357
Download the RPMs and Prepare the Servers 357
Set Up Hostnames 358
Configure SSH Trust for User Root 359
Configure SSH Trust for User Oracle 360

Install the Latest Patch

1. Install the latest patch to your version of SecureSphere on **both** MXs.

2. Reboot both MXs.

For information about downloading and installing patches, see the Imperva support site.

Configure the Interconnected Interfaces

The interconnected network must be defined during the first-time login procedure on the MX by setting up the LAN interfaces. If this was not done during the first-time login, the LAN interfaces can be configured now using `impcfg`.

To configure the interconnected interfaces on the MX:



Note: Both interconnected interfaces must be on the same subnet.

1. Perform the following on both MXs:
   a) Start `impcfg`.
   b) In the **Top** Screen, select **3) Manage platform**.
   c) In the **Platform Management** Screen, select **1) Manage network**.
   d) In the **Network Management** Screen, select **2) LAN interface**.
   e) Configure all three options:
      - **Change device**
      - **Change IP address**
      - **Change IP netmask**
   f) Return to the **Top** screen by selecting option **t**.
   g) Apply the settings by selecting option **A**.
   h) Confirm the new settings by selecting option **C**.

Test the Interconnected Interfaces

To test the interconnected interfaces:

1. Ping from the first MX to the second MX on its internal interface.
   The ping will fail, because the MX blocks ICMP by default.
2. Immediately after the ping, execute `arp -a` and locate the arp entry of the other server.
   If the arp entry has a valid MAC address for the other server, the interconnect was successfully configured.

Download the RPMs and Prepare the Servers

On both servers, perform the following:

1. Login as user `root`.
2. Execute the following command:

```
mkdir /var/tmp/mxha
cd /var/tmp/mxha
```

3. Navigate to the appropriate `MX-HA` directory on the Imperva FTP site (`ftp-us.imperva.com`).
   The directory names are listed in the table **HA RPM Directories** below.
4. Download both of the files in the `MX-HA` directory to the `/var/tmp/mxha` directory.
   The names of the files to download are listed in the table **HA RPM Files** below.
5. Execute the following command:

```
impctl server ha preparerpm
```

HA RPM Directories

	Directory Name
32 bit	/Downloads/SecureSphere_Setup/v10.0/32Bit/MX-HA/
64 bit	/Downloads/SecureSphere_Setup/v10.0/64Bit/MX-HA/

HA RPM Files

	File Names
32 bit	oracle-EE-11.2.0.3.2.i386.rpm oracle-EE-bin-11.2.0.3.2.i386.rpm
64 bit	oracle-EE-11.2.0.3.2.x86_64.rpm oracle-EE-bin-11.2.0.3.2.x86_64.rpm

Set Up Hostnames

To define hostnames:

1. On both MXs, edit the /etc/hosts file and add the hostnames and public IP addresses of both MXs.

```
127.0.0.1       localhost.localdomain localhost node1
10.1.12.111     node1
10.1.12.134     node2
```

Figure 78: /etc/hosts File

2. Verify that there are no duplicate names in the file.



Note:

- There is no need to add the private or the virtual IP address.
- In the hosts files on each of the MX-HA machines, the host's name must appear **exactly** once.

3. On both MXs, execute the following commands:

```
impctl hardening config --root-source-ip-exception=<vip>
impctl hardening config --root-source-ip-exception=<other_MX private interconnect>
impctl hardening config --root-source-ip-exception=<other_MX physical>
```

where:

- <vip> is the floating IP address, that is, the IP address shared by both MXs.
- <other_MX private interconnect> is the IP address of the interconnect on the other MX; for example when you are running this command on the primary MX, specify the IP address of the interconnect on the secondary MX.
- <other_MX physical> is the public IP address of the other MX; for example, when you are running this command on the primary MX, specify the public IP address of the secondary MX.

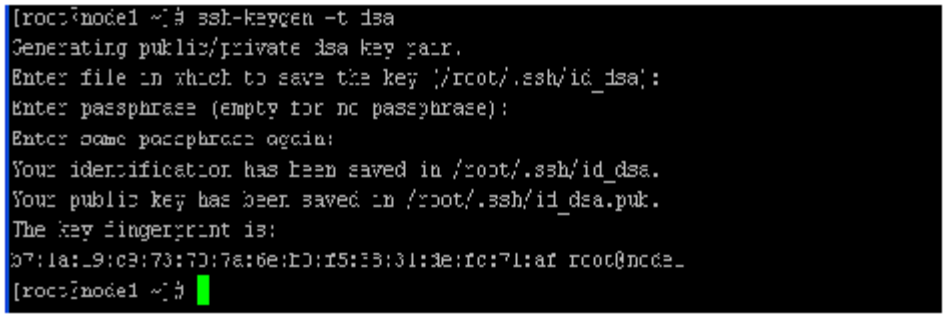
Configure SSH Trust for User Root

To configure SSH trust for user root:

1. Connect to an MX using SSH as user `root`.

   Note: To connect as user root over SSH, you must connect as a CLI user other than `root` and `secure` and use the `admin` command. For more information, see CLI Users on page 55.

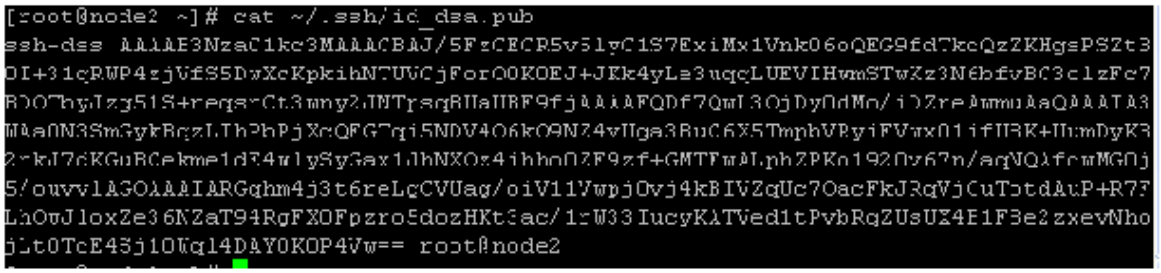
2. Execute the following command:
   ```
   ssh-keygen -t dsa
   ```
3. In response to each of the prompts, press Enter.



4. Execute the following command:
   ```
   cp ~/.ssh/id_dsa.pub ~/.ssh/authorized_keys
   ```
5. Perform steps 1. through 4. on the second MX.
6. Edit the `~/.ssh/authorized_keys` file on both MXs, so that the files on both MXs contain the keys of both MXs, as follows:

   Warning: Read all these instructions before executing the first one, and then execute each step carefully and exactly as written.

   a) On the first MX, execute the following command:
   ```
   cat ~/.ssh/id_dsa.pub
   ```



   b) Copy the output to the clipboard.
   Make sure you select only the output, without the trailing new line.
   c) In the other MX terminal session, enter the **echo** command but **do not press Enter**.
   d) Paste to the data that was copied earlier to the clipboard into the other MX terminal session.
   e) Add the following text at the end of the command you are putting together:
   ```
   >> ~/.ssh/authorized_keys
   ```
   You have now constructed a command from three elements (see the screen shot below):
   - the word "echo"

- the clipboard data
- the >> redirection



f) Press **Enter**.

7. Perform the previous step (6.1-6) on the second MX as well.
8. On both MXs, check the SSH connection using the following command:
   `ssh <other-server-hostname> date`
   The command should run without asking for a password.

Configure SSH Trust for User Oracle

To configure SSH trust for user oracle:

1. Connect to a MX using SSH as user `root`.



Note: To connect as user root over SSH, you must connect as a CLI user other than `root` and `secure` and use the `admin` command. For more information, see CLI Users on page 55.

2. Execute the following command:
   `su - oracle`
3. Execute the following command:
   `ssh-keygen -t dsa`
4. In response to each of the prompts, press Enter.
5. Execute the following command:
   `cp ~/.ssh/id_dsa.pub ~/.ssh/authorized_keys`



6. Perform steps **1** through **5** on the second MX.
7. Edit the `~/.ssh/authorized_keys` file on both MXs, so that the files on both MXs contain the keys of both MXs, as follows:

Warning: Read all these instructions before executing the first one, and then execute each step carefully and exactly as written.

a) On the first MX, execute the following command:

```
cat ~/.ssh/id_dsa.pub
```



b) Copy the output to the clipboard.

Make sure you select only the output, without the trailing new line.

c) In the other MX terminal session, enter the **echo** command but **do not press Enter**.

d) Paste to the data that was copied earlier to the clipboard into the other MX terminal session.

e) Add the following text at the end of the command you are putting together:

```
>> ~/.ssh/authorized_keys
```

You have now constructed a command from three elements (see the screen shot below):

- the word "echo"
- the clipboard data
- the >> redirection



Figure 79: The Constructed Command

f) Press **Enter**.

8. On both MXs, check the SSH connection using the following command:

```
ssh <other-server-hostname> date
```

The command should run without asking for a password.

Installing Management Server High Availability (MX-HA)

MX-HA is installed on an already functioning Management Server (MX). You should have two MXs, one of which you designate as primary and the other as secondary.

To install MX-HA:

1. Perform the pre-installation tasks (see Pre-Installation Tasks on page 356).

2. Upload licenses for both the primary MX and the secondary MX to the primary MX.

   Alternatively, you can upload only the primary MX license, install MX-HA on the primary server and install the secondary license (on the primary MX) at a later time. This alternative is not recommended, because it temporarily leaves the configuration without a license for the secondary MX, but it can be done.

3. Login to the primary MX as user `root`.



Note: The installation is performed only on the primary server. The secondary server is installed as part of the installation of the primary server, and any data on the secondary server is deleted.

4. On the primary server, execute the following command, entering parameters as listed in the table **Installation Parameters** below.

```
impctl server ha install
```

Installation Parameters

Parameter	Description	Default Value
Installation Directory	The directory in which MX-HA will be installed.	`/opt/secsph-ha`
Directory for temporary data	The directory in which temporary files will be written during the installation process.	`/var/tmp/secsph-ha`
Keep alive IP address (pingable server)	This IP address is used to check the network status. You can use any IP address on your network as long as it remains constant, active and pingable. If the keep alive address does not respond to the ping, a fail over occurs.	
Secondary server public IP address	The public address of the secondary MX.	
Virtual server IP address	The IP address used to access the MX-HA servers.	
Heartbeat interface name	The interface which is the direct connection between the two MXs.	
Public interface name	The management interface name.	
sys user password	The password for the sys user in the database. This password must be entered a second time for verification. **Note:** The password can contain any combination of lowercase letters, uppercase letters, numbers and the following special characters: * ( ) - + = | # % ^ : / ~ . , [_	

The screen shots below show a typical installation.



Note: You have the option of exporting the database before the installation. You can export the database before installing MX-HA, or optionally, during the MX-HA installation (see the figure **MX-HA Installation - Part 1** below).



Figure 80: MX-HA Installation - Part 1



Figure 81: MX-HA Installation - Part 2

After Installing Management Server High Availability (MX-HA)

This section reviews what can be done after Management Server High Availability has been installed and includes the following:

Verify the Primary Server is Active 365
Register the Gateway 365

Verify the Primary Server is Active

Once the installation is completed, verify that the primary server is active and running.

To verify that the primary server is active and running:

1. Execute the following command on both the primary and secondary servers:

```
impctl server ha status
```

The following output should appear:

```
started,ip-on-node1,db-on-node1,server-on-node1,running
```

status Command Output Explanation

	Explanation
`started`	heartbeat status
`ip-on-node`	the host that owns the active Virtual IP address (VIP)
`db-on-node1`	the host that owns the active database
`server-on-node1`	the host that owns the active MX
`running`	status of the active host

Register the Gateway

After installing MX-HA, the Gateway must be (re)registered with MX-HA.

To register the Gateway:

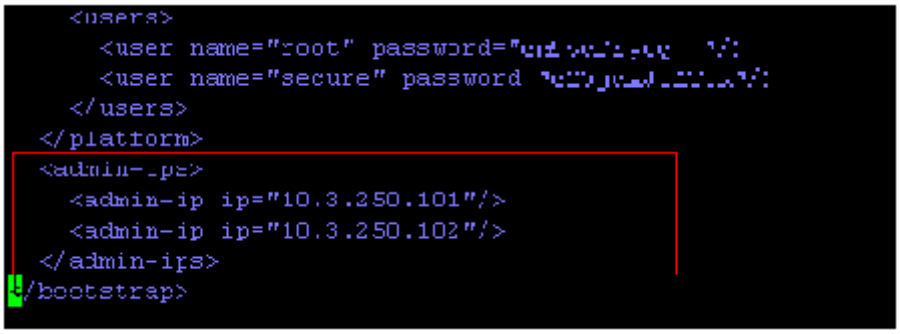
1. Configure `admin-ips` in the `bootstrap.xml` file.
2. Re-register the Gateway using the virtual IP address (VIP) of the MXs.

admin-ips

1. Add the following xml part to the `bootstrap.xml` file on each of the Gateways (`/opt/SecureSphere/etc/bootstrap.xml`):

```
<admin-ips>
 <admin-ip ip="server-real-ip1"/>
 <admin-ip ip="server-real-ip2"/>
</admin-ips>
```

Substitute the servers' real IP addresses (inside double quotes) for `server-real-ip1` and `server-real-ip2`s.



Re-registration

After the installation process has successfully finished, re-register the Gateway using the MX-HA virtual IP address.

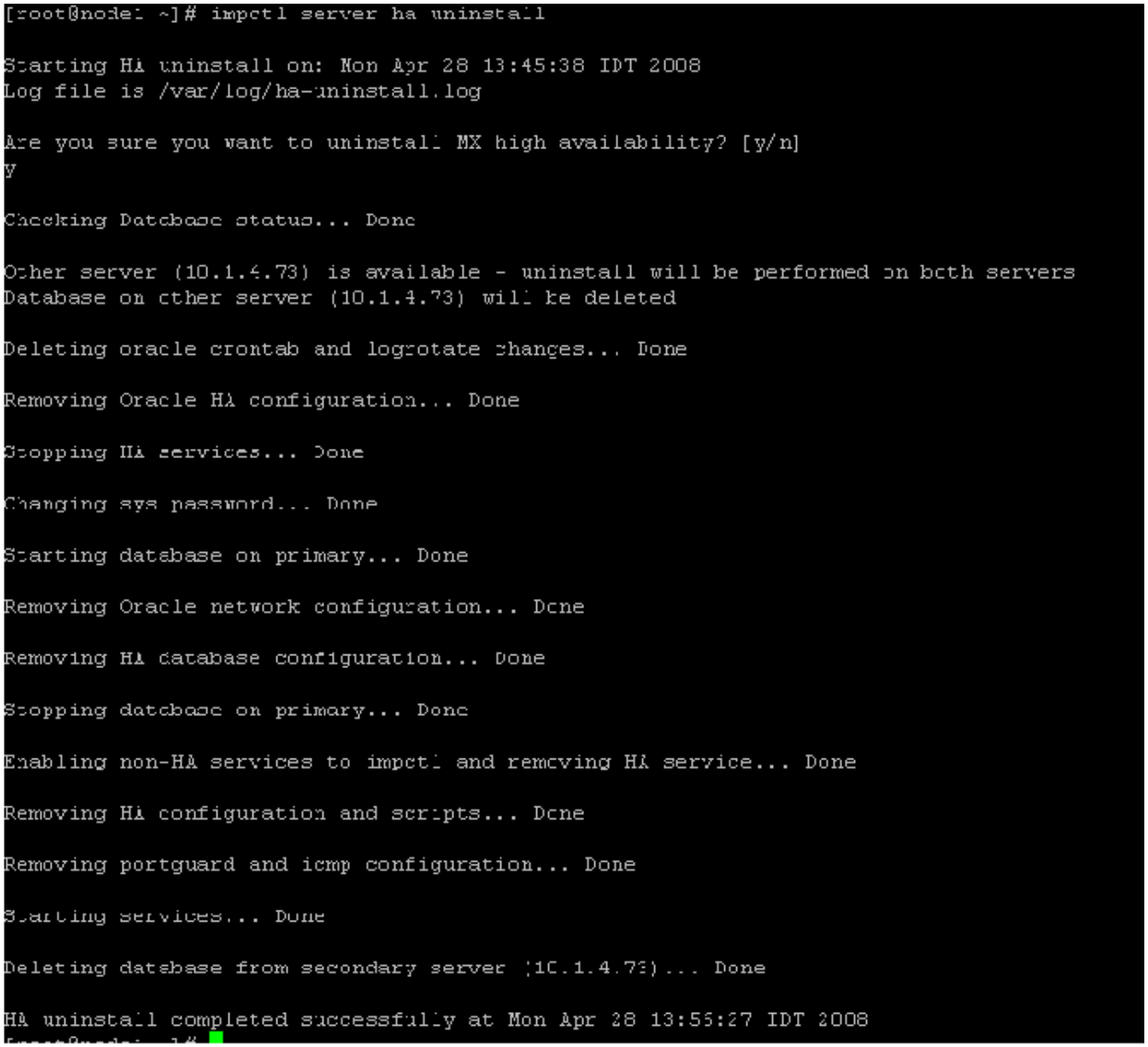
Uninstalling MX-HA

To uninstall MX-HA solution, the primary server must be available, otherwise, there is no guarantee that the uninstall process will successfully complete.

To uninstall MX-HA:

1. Login to the primary MX server as user `root`.
2. **Execute the following** command:

```
impctl server ha uninstall
```



Once the uninstall process is complete, the primary server functions normally as a single server. The secondary server is unusable, and its database must be recreated using the following command:

```
impctl db create
```

Changing Database and/or System Passwords

To change the system (database) and/or secure (system) password on the primary MX, use the following command:

```
impctl server ha password
--set-database-password=NEW_SYSTEM_PASS
--set-server-password=NEW_SECURE_PASS
```

Monitoring Management Server High Availability (MX-HA)

This section includes the following:

MX-HA Status 368
Confirming that MX-HA is Correctly Configured 369
MX-HA Logs 370
Heartbeat Behavior 372
Known Issues 372
File List 373

MX-HA Status

impctl server ha status Command

The **impctl** command displays the status of MX-HA. The command syntax is as follows:

```
impctl server ha status
```

This command returns information about whether the MX-HA is started and on which server the resources are running. The output of this command returns the server that holds each resource (IP, database and server) even if only some resources are up.



Note: When you run this command on a secondary MX, it shows the status of the primary MX.

impctl server ha status Output

The output of the `impctl ha status` command will be similar to one of the following:

- If the secondary MX is synchronized:

```
started,ip-on-mxha1,db-on-mxha1(secondary-synchronized),server-on-mxha1,running
```

- If the secondary MX database is down or inaccessible:

```
started,ip-on-mxha1,db-on-mxha1(secondary-status-unknown),server-on-mxha1,running
```

- If the secondary MX is not synchronized:

```
started,ip-on-mxha1,db-on-mxha1(secondary-synchronization-lag:9m-26s),server-on-mxha1,running
```

- If the secondary MX is down:

```
started,ip-on-mxha1,db-on-mxha1(secondary-unavailable),server-on-mxha1,running
```

Confirming that MX-HA is Correctly Configured

After configuring MX-HA, you may wish to confirm that the configuration is correct rather than to wait for the primary MX to fail. This section describes the following:

Initiating a Failover in an MX-HA Environment 369
Confirming That the MX-HA Servers are Synchronized 370

Initiating a Failover in an MX-HA Environment

This section describes how to perform a safe and successful failover in MX-HA. A failover is sometimes required for testing.

To initiate a failover:

1. Execute the following command on both MXs:

```
impctl server ha status
```

   If HA is running on both MXs, the output on each MX should resemble the following:

```
started,ip-on-mxha1,db-on-mxha1(secondary-synchronized),server-on-mx
ha1,running
```

2. Confirm that the MXs are synchronized (see Confirming That the MX-HA Servers are Synchronized on page 370).
3. Initiate a failover by performing one of the following:
   a) On the primary MX, stop the primary MX by executing the following command:

```
impctl server ha stop
```

   b) or,
   c) On the secondary MX, perform a failover by executing the following command:

```
impctl server ha failover
```

4. Wait until the secondary MX becomes active (that is, it has become the primary MX). You can determine whether it is active by using the following command:

```
impctl server ha status
```

   - If the secondary MX is now the primary MX, that is, if failover has successfully occurred, the output should resemble the following:

```
started,ip-on-mxha1,db-on-mxha1(secondary-synchronized),server-on-mx
ha1,running
```

   At this point, the MXs have switched roles:

   - The MX that was formerly the secondary MX is now the primary MX, and its GUI is now usable.
   - The MX that was formerly the primary MX is now the secondary MX.

5. If you initiated the failover with the `impctl server ha stop` command (as in step a), then in order to restore the HA functionality, proceed as follows:
   a) Start the new secondary MX (the MX that was previously the primary one) by executing the following command:

```
impctl server ha start
```

6. If you initiated the failover with the `impctl server ha failover` command (as in step b), then the secondary MX will automatically be started and HA functionality restored. There is nothing you need do.

In either case, the secondary MX must perform a full synchronization with the primary MX, and will not be ready for another failover until the synchronization is complete.

To determine when the standby MX has re-synchronized and is ready for failover, follow the instructions in Confirming That the MX-HA Servers are Synchronized on page 370 below.

Confirming That the MX-HA Servers are Synchronized

This procedure describes how to verify the status of an MX HA server.

To verify the status of an MX-HA server:

1. Login as root to the secondary MX.
2. Check the last entries in `server_ha_debug.log`, usually located in `/opt/SecureSphere/server-ha/log/ VICE /opt/secsph-ha/` and confirm that:
   - the date and time of the entries are recent
   - the status is "`Database is standby`"
   - lag is `0`

   For example, in `server_ha.log`, the output might be:

```
[12/11/12 14:58:06 healthCheck] - Secondary database is fully synchronized
```

MX-HA Logs

This section reviews MX-HA logs and includes the following:

MX-HA Components Writing to the Logs 370
Logs in the /opt/securesphere/server-ha/log Directory 371
alert_secsph.log 371
Heartbeat Statuses 371
Resource Status 371
Server Status 371
impctl watchdog 371

MX-HA Components Writing to the Logs

The following are the main components that write to the logs:

- `ha-dbora` is responsible for managing the database. `Ha-dbora` writes to the log when the heartbeat is requesting to stop, start or get status of the database server. This component runs only on the primary server.
- `ha-secsph` is responsible for managing the SecureSphere server. `Ha-secsph` writes to the log when heartbeat is requesting to stop, start or get status of the SecureSphere MX. This component runs only on the primary server.
- `healthCheck` is responsible for the database health on both servers. This component checks if the server is the primary or secondary, and according to the answer verifies that the database is in the correct status. If needed, this component runs other components to recreate and standby database or changing the standby database to primary.
- `syncDirs` is responsible for synchronization of directories and files from the primary server to the secondary server, this is done using `rsync` utility and according the `rsync.conf` file. This component runs only on the secondary server.

- watchdog: every time the watchdog checks the heartbeat status, it writes information to the log file about the current status and whether it is going to restart the heartbeat or not.

Logs in the /opt/securesphere/server-ha/log Directory

- The server_ha.log file contains overview information, mostly changes in status.
- The server_ha_debug.log file contains detailed information file about the heartbeat, cluster, resources and transitions between the servers.
  Information from ha-dbora, ha-secsph and the watchdog is also written to this file.

alert_secsph.log

This file is the Oracle database log, and contains information from Oracle database, including information relevant to the standby solution. The log is located under the /opt/oracle/admin/secsph/bdump directory, assuming that /opt/oracle is the Oracle installation directory.

Heartbeat Statuses

MX-HA uses the Linux heartbeat solution. Part of the heartbeat is the Cluster Resource Manager (CRM), which takes care for the group of resources and handles starting, stopping and moving them between the servers.

MX-HA uses /usr/lib/heartbeat/crmadmin to determine where the resources are running and the status of each server.

Resource Status

To determine where a resource is running, MX-HA uses crmadmin -W <resource>, where <resource> is one of the following:

- **PrimaryGroup:ip_resource**, **PrimaryGroup:OracleDB**
- **PrimaryGroup:SecureSphere**

The output of this command is the server name that holds the resource, or a message if the resource is not running or nothing if the heartbeat is down.

The impctl server ha status command uses the crmadmin to list the owners of the resources.

The healthCheck script uses crmadmin in order to decide which server is the primary, that is, the server that holds the IP resource.

Server Status

To determine the server status, MX-HA uses the crmadmin -S <hostname> command. The output of this command is the current status of the server.

The two most important statuses are S_IDLE and S_NOT_DC. Both statuses mean that the server is idle, either primary or secondary. Other statuses, such as S_ELECTION, S_TRANSITION_ENGINE, S_STARTING and so on, meaning that the server is performing a task, such as starting, stopping, change status from primary to secondary and so on.

impctl watchdog

The watchdog is responsible for health checking of the management components. In a regular management configuration, the watchdog verifies that the database and the SecureSphere server are working properly.

Under MX-HA configuration, the `watchdog` command does not check the database or the server. It checks only the heartbeat.

Every time the `watchdog` runs, it checks the heartbeat status and the owner of the IP resource. If the status is not idle or if `crmadmin` returned nothing, it means that everything is functioning properly.

The `watchdog` restarts the heartbeat, if the heartbeat is idle and but the IP address is not running on both nodes.

Heartbeat Behavior

This section reviews heartbeat behavior and includes the following:

Failover Sequence 372
Standby Recreation 372

Failover Sequence

The heartbeat uses the internal scripts `ha-dbora` and `ha-secsph` to verify the status of the IP address, database and SecureSphere server. If one of the resources has an invalid status, the heartbeat stops higher resources. If IP address is down, both database and SecureSphere server are stopped. If the database is down, only the SecureSphere server is stopped.

Then, the heartbeat tries to start the failed resource again. If the start is successful, heartbeat continues to start all other dependent resources. If the start operation fails, heartbeat performs failover and moves all the resources to the other server.

During a failover, the heartbeat stops all the resources on the primary server (server A) and starts them on the other server (server B). At this time, server A is in the TRANSITION status. When server B finishes starting all the resources, server A status becomes `S_IDLE`, and since the database on server A is not standby, it is recreated.

When the process completes, server A is still in the `S_IDLE` status, which is invalid for the secondary server. At this time, the watchdog restarts the heartbeat on server A and the entire environment is valid again.

If during the failover from server A to server B, one of the resources could not start on server B, the heartbeat stops everything on both servers. At this point, the `watchdog` command restarts the heartbeat on both servers.

In addition, failover occurs when the primary server reboots or the `server-ha` service is stopped.

Standby Recreation

The standby database is constantly being synchronized with the primary database. There are several situations in which the standby database is recreated. This means that the database is deleted, and is copied from the primary database, as follows:

- The standby database has a lag higher than a certain level. The level is configured in the `bootstrap.xml` file, and its value is 10 redo logs by default.
- The healthcheck process cannot check the synchronization level.
- The database is not a valid standby. For example, after a failover, the new secondary server contains a primary database and not a standby database. In this case, the database on the new secondary server is recreated.

The standby database can be recreated only if the primary database and server are running. Otherwise, the standby writes a message to the `healthCheck.log` and is not recreated.

Known Issues

This section reviews MX-HA known issues and includes the following:

MX-HA Installation Failure 373
Failure While Building the Standby Database 373
Management Server (MX) Replacement 373

MX-HA Installation Failure

A failure of the MX-HA installation procedure does not invoke an uninstall process. Before proceeding, you must "clean up" the unsuccessful installation on the primary server and re-initialize the database on the secondary server.

1. On the primary server, execute the following command:

```
impctl server ha uninstall
```

2. On the secondary server, execute the following command:

```
impctl db start
```

Failure While Building the Standby Database

In very rare cases, the standby database needs to be recreated. The creation process can take some time, and during this time the standby database is not operational and cannot become the primary database. If there is an unrecoverable failure on the primary server while the standby is recreated, MX-HA cannot overcome this failure. In some cases, a manual intervention can solve the problem, but in other cases there is no solution.

For example, if the database files are deleted from the primary server during the standby recreation, there is no valid database to use, and MX-HA or manual operations cannot start the system.

If this occurs, contact Imperva support.

Management Server (MX) Replacement

Currently, there is no supported option to install only a secondary server in the MX-HA solution. If the secondary server crashes and needs to be replaced, replace it using the following procedure:

1. Uninstall MX-HA from the primary MX.
2. Connect and configure the new secondary MX, including all prerequisites.
3. Reinstall MX-HA from the primary MX.

File List

The following files are installed when the MX-HA is installed:

MX-HA File List

File Name	Description
cib.xml	This file is the heartbeat configuration file. This file contains the heartbeat resource configuration including the operations, timeouts and scripts.
ha-dbora	This file is located under `/etc/init.d` and handles the operations that heartbeat can do on the database, including start, stop and status. Currently, this script also checks ping to the Gateway to verify that the network is available.
ha-secsph	This script is located under `/etc/init.d` and handles the operations that heartbeat can perform, including start, stop and status.
creConfig.sh	This script creates data guard configuration after creating a standby database.
deconfigNet.sh	This script removes the Oracle net configuration, and is used when uninstalling MX-HA.
deconfigPrimary.sh	This script changes the primary database back to stand-alone database, and is used when uninstalling MX-HA.
failover.sh	This script performs data guard failover to change a standby database to the primary database.
getInfo.sh	This script is used to get information about the database. The information is the database role (primary or standby) and database status (down, started, mounted or open).
getSeq.sh	This script is used to get the current redo log sequence of the local or remote database.
healthCheck.sh	This is the main script.
healthcheckmasterDB.sh	This script checks the status of the database and performs ping to the Gateway in order to verify that the network and database are healthy. If something is not valid, the script returns an error and the heartbeat identifies that the resource is down.
healthcheckmasterJAVA.sh	This script is similar to `healthcheckmasterDB`**.sh**, but checks SecureSphere server.
instPrimary.sh	This script changes a stand-alone database to the primary database in an MX-HA configuration. This script is executed during the MX-HA installation process.
instStandby.sh	This script recreates the standby database from the primary database.
modnet.sh	This script is for setting up the Oracle network. This script is executed only once, during the MX-HA installation process.
resync_standby.sh	This script is used when the standby is not valid. This script deletes the data guard configuration, recreates the standby database and creates the data guard configuration using the relevant scripts.
rmArch.sh	This script handles deletion of archived redo logs from both primary and secondary servers. This script is executed by the **crontab**.
rmDGConfig.sh	This script removes the Oracle Data Guard configuration, and is used before recreating the standby database.

File Name	Description
rsync.conf	This file contains all the files and directories that need to be synchronized from the primary server to the secondary server.
shutDB.sh	This script is used to shutdown the database.
standby.conf	This file is a general configuration file that contains extraction of information from the `bootstrap.xml` file and general functions that are used by other scripts.
startDB.sh	This script is used to start the database.
syncDirs.sh	This script synchronizes files and directories from the primary server to the secondary server according to the `rsync.conf` file. This script is executed by `ha-dbora` every time heartbeat requests database status.

CHAPTER 17

Network High Availability

In addition to high availability provided by both the Management Server and the Gateway, the network itself can also be used to provide high availability This option relies on a mechanism which detects when an opposing network interface is down, and subsequently takes the operating interface on the opposite side of the network link offline to prevent data from being sent to an inoperative interface.

Once the problematic network interface becomes available, the SecureSphere appliance gives the operating interface (which was manually taken down) a period of time to come up and stabilize. If it does not succeed, then the original interface is taken back offline. This is in order to prevent a situation in which the interfaces get involved in an ongoing pattern of going up and down. The amount of time given for the interface to come back up is configurable by editing a supporting file.



Note: This chapter describes how to achieve high availability through the network. It detects link status and enables HA only if it is network related. It does not facilitate HA when an issue is software related. For information on how to provide HA in these cases, see Management Server High Availability (MX-HA) on page 353 or Gateway High Availability on page 343.

This chapter includes the following:

Network High Availability Support 376
Configuring Network High Availability 377

Network High Availability Support

Network high availability is supported in bridge mode (STP / Impvha). It is not available in Kernel Reverse Proxy or sniffing modes. The following table lists the interface types and their support for network high availability.

Interface Support for Network High Availability

Interface Type	G-Series	X-Series
Copper	Supported	Supported
1 G	Not Supported	Supported
10 G	Not Supported	Not Supported
10 G with Bypass Support	Not Supported	Supported

Configuring Network High Availability

You can configure the amount of retries, and subsequently the period of time that is provided for the operating interface to come back up.



Note: This procedure should only be conducted after consulting with a member from the Imperva support team.

To modify the number of retries for an interface:

1. Navigate to the following location on the SecureSphere appliance:
   `opt/SecureSphere/etc`
2. Access the following file:
   `hades.cfg`
3. Modify the following parameter:
   `bridge_relief_count_[#]`
   where [#] is the value for the number retries you want SecureSphere to attempt before it manually takes the interface offline.

Default: 5 retries (10 seconds)

Please note that each retry is made after 2 seconds. So the overall amount of time an interface is given to come back up is the number of retries multiplied by 2.

EXAMPLE:

If you set the parameter to: **bridge_relief_value_1**

It attempts 1 retry after two seconds, or give the interface 2 seconds to come online until the original interface is taken down again.

If you set the parameter to: **bridge_relief_value_6**

It attempts 6 retries two seconds apart, or give the interface 12 seconds to come online the original interface is taken down again.

APPENDIX A

Network Services

This appendix describes various network configuration issues related to deploying SecureSphere, and includes:

SecureSphere Component Communication 378
Configuring Firewall Ports 379
Serial Console Access to SecureSphere 380

SecureSphere Component Communication

The table **SecureSphere Component Communication** below lists the protocols through which the various SecureSphere components communicate with each other.

SecureSphere Component Communication

Source	Destination	Protocol	Destination Port	Remarks
Gateway	MX	HTTP	TCP 8083	If the Gateway and MX server have a dedicated network (either with a cross cable or through a dedicated switch) then there is no need to open these ports on the firewall.
MX	Gateway	SSH	TCP 22	
MX	Gateway	HTTPS	TCP 443	
MX	www.imperva.com	HTTP	TCP 80	automatic signature update
Gateway	syslog server	syslog	UDP 514	if audit is configured
MX	syslog server	syslog	UDP 514	
desktop	MX	HTTPS	TCP 8083	

Source	Destination	Protocol	Destination Port	Remarks
desktop	MX	SSH	TCP 22	
Gateway	DNS server	DNS	TCP 53 UDP 53	DNS is required to resolve host names defined in SecureSphere policies.
Gateway	NTP server	NTP	UDP 123	NTP is needed to guarantee accuracy of timestamps.

Configuring Firewall Ports

The SecureSphere allows a great deal of flexibility in its deployment modes. Firewalls can be placed wherever they are required.

The Figure **Firewall Port Configuration** below shows that ports that need to be open to enable different functions required by SecureSphere to communicate through the deployed firewalls.

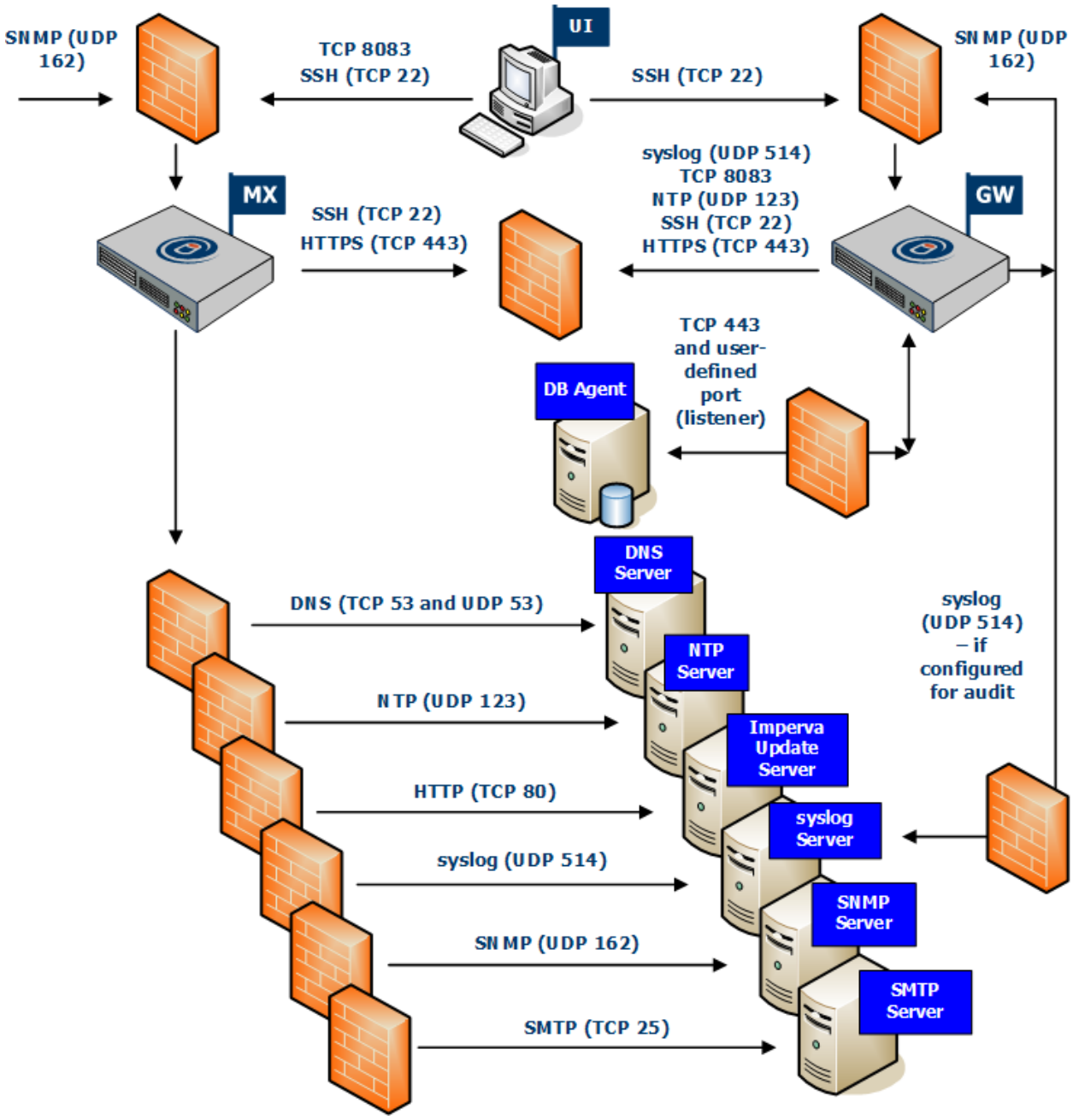


Figure 82: Firewall Port Configuration

Serial Console Access to SecureSphere

This section describes the steps administrators need to take in order interact with SecureSphere's Command Line Interfaces (CLIs) through a serial console, rather than a VGA and PS2 keyboard and review the following:

Supported Versions and Upgrades 381
Supported Serial Console Settings 381

Before You Begin: Checking OS Layer Serial Console Access 383
Configuring BIOS Settings for Serial Console 383
Editing the GRUB Configuration File 383

Supported Versions and Upgrades

This section describes supported versions and upgrades and reviews the following:

Hardware 381
Software 381
Upgrades 381

Hardware

The steps described in this document are supported only on the FTL versions of G4, G8, G16 and MX appliances, with BIOS versions 74 and 85.

Software

The minimum SecureSphere software version required is 6.0.6.6302. Prior versions are not supported.

Upgrades

The changes described in this document will survive an upgrade from SecureSphere release 6.0.6.6302 to 6.2.0.6442. Other upgrades have not been tested. Furthermore, whenever SecureSphere is reinstalled, administrators must reapply the `grub.conf` changes described in Editing the GRUB Configuration File on page 383.

Supported Serial Console Settings

Throughout this document, the serial console settings administrators should use are as follows:

Serial Console Settings

Setting	Value
baud rate	38400
data bits	8
parity	none
stop bits	1
flow control	none
terminal emulation	VT 100+

VT 100 Escape Sequences

VT 100 key	Escape sequence sent
HOME	<ESC> h
END	<ESC> k
INSERT	<ESC> +
DELETE	<ESC> -
PAGE UP	<ESC> ?
PAGE DOWN	<ESC> /
ALT	<ESC> ^A
CONTROL	<ESC> ^C
F1	<ESC> 1
F2	<ESC> 2
F3	<ESC> 3
F4	<ESC> 4
F5	<ESC> 5
F6	<ESC> 6
F7	<ESC> 7
F8	<ESC> 8
F9	<ESC> 9
F10	<ESC> 0
F11	<ESC> !
F12	<ESC> @

Before You Begin: Checking OS Layer Serial Console Access

In its default configuration, SecureSphere supports OS layer access via a serial console. It is highly recommended to first confirm that they you such access as follows:

1. Set the connections parameters on the console client (for example, using `putty`) to those defined in the table Serial Console Settings found in Supported Serial Console Settings on page 381.
2. Connect to the SecureSphere appliance via its DB9 serial port.
3. Initialize the connection and confirm that you get a Linux prompt and are able to log in, for example, with the "secure" user credentials.



Note: If serial console access only at the OS layer is sufficient for your needs, then no configuration changes are needed.

Configuring BIOS Settings for Serial Console

After making the changes described below and rebooting the machine, you will be able interact with the BIOS UI though both the VGA and the serial console.

Use your existing VGA port and PS2 keyboard to make the following changes:

1. Power on the SecureSphere appliance.
2. Press F2 to enter BIO configuration
3. Set Server Management-> Console Redirection-> Console Redirection to one of the following:
   - [Serial Port A] (DB9)
   - [Serial Port B] (Rj45)
4. Set Flow Control to [None].
5. Set Baud Rate to [38.4K].
6. Set Terminal Type to [VT100+].
7. Set Legacy OS Redirection to [Enable].
8. Save & Exit using "F10".

At this stage the Keyboard and VGA are no loner required.

Editing the GRUB Configuration File

Changing the settings below will allow you to interact with the bootloader and see the messages it prints to the console as modules are loaded.



Warning: Once these settings take effect, boot time messages will only be available through the serial console and not through the VGA console. Only BIOS and OS access will still be available through the VGA and PS2 keyboard.

1. Edit the `/boot/grub/grub.conf` file.
2. Add the following text at the end of each line that start with the word "kernel":
   `onsole=ttyS0,38400`
3. Save the file and exit.

The `/boot/grub/grub.conf` file should now look like this (the added text is highlighted):

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sysvg/root.vol
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
serial --unit=0 --speed=38400
terminal --timeout=5 serial console
title CentOS (2.6.18-53.1.4.el5.imp40smp)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-53.1.4.el5.imp40smp ro
root=/dev/sysvg/root.vol rhgb quiet panic=10 console=ttyS0,38400
        initrd /initrd-2.6.18-53.1.4.el5.imp40smp.img
title CentOS (2.6.18-53.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-53.el5 ro root=/dev/sysvg/root.vol rhgb
quiet panic=10 console=ttyS0,38400
        initrd /initrd-2.6.18-53.el5.img
```

APPENDIX B

Add-Ons

This appendix describes various network configuration issues related to configuring add-on hardware in conjunction with SecureSphere, and includes:

Hardware Security Modules (HSM) 385
Storage Area Networks (SAN) 397
SSL Accelerator 408
LOM (Lights Out Management) 408

Hardware Security Modules (HSM)

Hardware Security Module devices (HSMs) store private encryption keys in specialized key storage devices. These devices protect the key information by making it impossible to gain access to the keys, even if the device is stolen.

A network HSM (Hardware Security Module) device is a central key Management Server which stores private keys. The network HSM provides a service to other devices on the network for performing operations with the secret keys.

Imperva SecureSphere supports the use of the following HSMs:

- nCipher card: nCipher Card on page 386
- nCipher netHSM: nCipher netHSM on page 393



Note: Beginning with SecureSphere version 10.0, SafeNet LunaSA is no longer supported.

All these solutions provide:

- secure storage of up to 256 private keys

- SSL acceleration

nCipher Card

The nCipher card is installed inside the SecureSphere appliance.

Installing the nCipher Card

The nCipher card is installed in an available PCI slot in the appliance.

To install the nCipher Card:

1. Shut down the appliance.
2. Power down the appliance.
3. Remove the appliance cover.
4. Insert the nCipher card into the PCI slot and verify that it is firmly in place.
5. Replace the cover.
6. Power on the appliance.

Installing the nCipher Card Driver

To install the nCipher card driver:

1. Execute the following command:

```
/opt/nfast/sbin/install
```

Verifying the Installation

To verify the nCipher card installation:

1. Execute the following command:

```
/opt/nfast/bin/enquiry
```

The output should resemble the following:

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        EFEB-96AB-EBE3
 mode                 operational
 version              2.32.14
 speed index          4240
 rec. queue           390..590
 level one flags      Hardware HasTokens
 version string       2.32.14cam6, 2.22.43cam8 built on Oct 13 2006 16:16:12
 checked in           0000000046dee54e Wed Sep  5 20:20:14 2007
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level  four  flags        OrderlyClearUnit  HasRTC  HasNVRAM  HasNSOPermsCmd
```

```
  ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable
  HasFileOp  HasPCIPush  HasKernelInterface  HasLongJobs  ServerHasLongJobs
  AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
   module type code     0
   product name         nFast server
   device name
   EnquirySix version   4
   impath kx groups
   feature ctrl flags   none
   features enabled     none
   version serial       0
   remote server port   9004
  Module #1:
   enquiry reply flags  Failed
   enquiry reply level  Six
   serial number        EFEB-96AB-EBE3
   mode                 operational
   version              2.22.43
   speed index          4240
   rec. queue           35..152
   level one flags      Hardware HasTokens
   version string       2.22.43cam8 built on Oct 13 2006 16:16:12
   checked in           00000000452f6a4d Fri Oct 13 12:28:29 2006
   level two flags      none
   max. write size      8192
   level three flags    KeyStorage
   level four flags        OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd
  ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable
  HasFileOp  HasPCIPush  HasKernelInterface  HasLongJobs  ServerHasLongJobs
  AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
   module type code     7
   product name         nC1003P/nC3023P/nC3033P
   device name          #1 nFast PCI device, bus 13, slot 1.
   EnquirySix version   5
   impath kx groups     DHPrime1024
   feature ctrl flags   LongTerm
   features enabled     StandardKM ModexpSpeedRating
   version serial       24
   rec. LongJobs queue  34
   SEE machine type     PowerPCSXF
```

nCipher enquiry command sample output

From the above sample output, you can see the following:

- The nfast server is up and its mode is operational ("`mode`" is "`operational`").
- Module 1 is the hardware card.
- The HSM mode is operational.

Security World Initialization

The nCipher security world must be initialized whenever one or more of the following conditions is true:

- The HSM is newly installed, so it does not yet have a security world.
- An existing security world is discarded.
- Whenever the appliance is reinstalled.

To initialize the security world:

1. On the card's bracket, move the switch to the **I** position (initialization).

On G series appliances, the bracket is accessible from the rear.

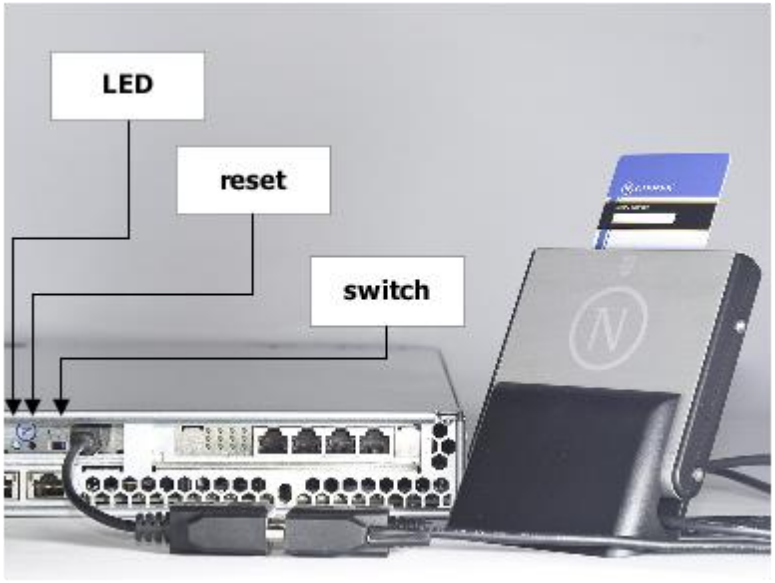


Figure 83: HSM Card Bracket and Reader - G Series Appliances

On X series appliances, the bracket is accessible from the front.

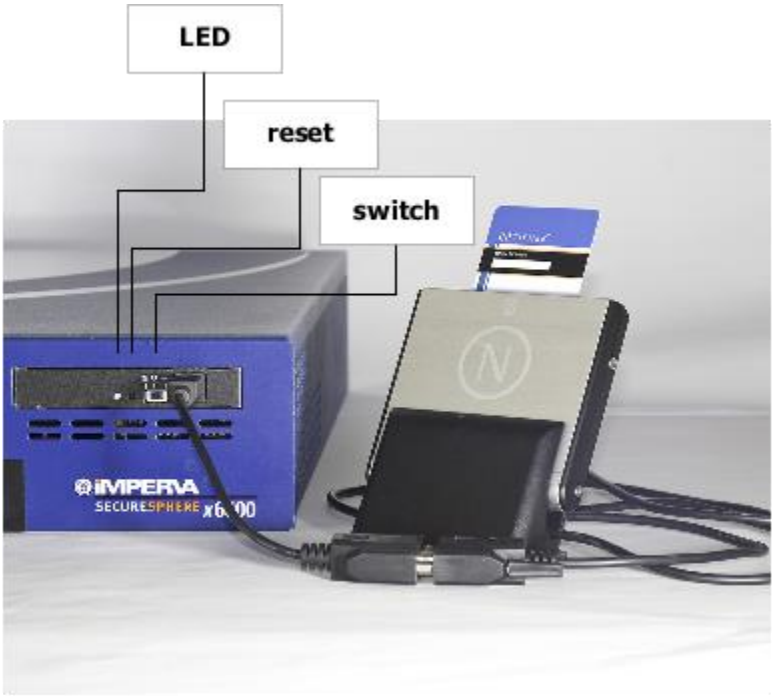


Figure 84: HSM Card Bracket and Reader - X Series Appliances

2. Press the RESET button (use a paper clip).
   The LED will blink for a few seconds.
3. When the LED stops blinking, use the nCipher `enquiry` command to confirm that the card is in the pre-initialization mode (see the output example in Verifying the Installation on page 386), that is, that "`mode`" is "`pre-initialization`".
4. Execute the following command:

```
/opt/nfast/bin/new-world -i -Q 1/1
```

5. When you are asked to do so, insert the SmartCard into the nCipher reader.
6. When you are asked for a passphrase, press <Enter>.

   The output should resemble the following:

```
[root@Nigiri bin]# /opt/nfast/bin/new-world -i -Q 1/1
11:43:11 WARNING: Module #1: preemptively erasing module to see its
slots!
Create Security World:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: unknown card
 Module 1 slot 0:- no passphrase specified - overwriting card
Card writing complete.
security world generated on module #0; hknso =
b9d79789b3386f58e0c150f7f3f0657a976e036c
```

7. When the LED stops blinking, use the nCipher `enquiry` command to confirm that the card is now in the initialization mode (see the output example in Verifying the Installation on page 386), that is, that "`mode`" is "`initialization`".
8. On the card's bracket, move the switch to the **O** position (operational).
9. Press the RESET button (use a paper clip).

   The LED will blink for a few seconds and then will remain mostly on, that is, it will blink only every few seconds.
10. At this point, use the nCipher `enquiry` command to confirm that the card is in the operational mode (see the output example in Verifying the Installation on page 386), that is, that "`mode`" is "`operational`".
11. Execute the following command:

```
/opt/nfast/bin/cryptest
```

    The card will run some internal tests.
12. Confirm that the internal tests were successful by reviewing the output.

    At the end of the output, a message summarizes the number of tests run and their results. For example:

```
...
...
...
16 key types OK, 6 types and 1 mechanisms skipped, 54 mechanisms
successfully tested
```

13. At this point, you can remove the SmartCard from the card reader.

Importing Keys

This section provides an overview of the process. For detailed information on how to do this, see the nCipher documentation.

This procedure will import one or more keys into the HSM.

1. Obtain the protected server's certificate as a `<name>.pfx` file.

   For example, assume the server uses `newkey.pfx`. This file contains both the server's private key and its certificate.

   You will:

   - Extract the key and certificate into two separate files.

- Import the key into the HSM and make a "fake" key.
- Upload the fake key and certificate to the SecureSphere Management Server.

2. The private key imported into HSM must be unencrypted. To create a file containing the key and certificate without the passphrase, execute the following command:

```
openssl pkcs12 -in newkey.pfx -out newkey-combined.pem -nodes
```

For example:

```
[root]# openssl pkcs12 -in newkey.pfx -out newkey-combined.pem
-nodes
Enter Import Password:  **********
MAC verified OK
```

3. You now have a text file named `newkey-combined.pem` (in the above example), which includes two keys. Next, you will create other two text files from this file:
   - **one for the key**
   - **one for the certificate**

   a) Execute the following command to create an RSA private key in *.pem format:

```
openssl rsa -in newkey-combined.pem -out newkey-private.pem
```

   b) Save `newkey-private.pem`.

   c) Execute the following command to create an RSA cert key in *.pem format:

```
cp newkey-combined.pem newkey-cert.pem
```

   d) Using a text editor such as `vi`, delete from `newkey-cert.pem` all the lines except for the following:

```
-----BEGIN CERTIFICATE-----
……
……
-----END CERTIFICATE-----
```

   `newkey-cert.pem` now contains only the certificate.

   e) Save `newkey-cert.pem`.

4. Execute the following command:

```
/opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=<full path name of the private-key PEM file> \
embedsavefile=<name of the PEM file to which to write the key> \
plainname=<full path name of the new-key PEM file> \
nvram=no
```

For example:

```
[root]# /opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=/tmp/newkey-private.pem
embedsavefile=fake_new_private.pem \
plainname=/tmp/fake_new_private.pem nvram=no
operation      Operation to perform         import
application    Application                  embed
verify         Verify security of key       yes
type           Key type                     RSA
pemreadfile    PEM file containing RSA key  /tmp/newkey-private.pem
embedsavefile  Filename to write key to     fake-newkey-private.pem
plainname                                          Key        name
/tmp/fake_new_private.pem
nvram          Blob in NVRAM (needs ACS)    no
Key successfully imported.
Path                              to                              key:
/opt/nfast/kmdata/local/key_embed_1d15d8797231860dced8ee5b97e6b3f322
301e2c
```

5. Using a disk-on-key or some other media, carry the following files (created in the previous step) to the computer from which you run the SecureSphere GUI (the file names from the example above are given here):
   - `newkey-cert.pem`
   - `fake_newkey_private.pem`



Warning: These files contain the server's private key in unencrypted form. You must erase this extremely sensitive information in accordance with your site's procedures.

Update the Gateway HSM

1. On the SecureSphere Gateway, start `impcfg`.
2. Select **Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)** > **Enable nCipher HSM**.
3. **Apply** and **Confirm** the operation.

Update the Server with the Certificate Key

This section provides an overview of the process. For detailed information on how to do this, see the **SecureSphere User Guide**.

1. Start the SecureSphere GUI.
2. Got to **Setup** > **Sites**, select (or create) an HTTP service.
3. In the HTTP service's **Definitions** tab, under **Encryption Support**, click .
4. In the **Add SSL Keys** window:
   a) Enter a **Name**.
   b) Check **HSM**.
   c) Select **PEM file format**.

d) In **Private Key**, browse to the `fake-newkey-private.pem` file.

e) In **Public Key**, browse to the `newkey-cert.pem` file.

f) Click **Upload**.

nCipher netHSM

This section includes the following:

High Level Functional Description 393
Components Taking Part in the Integration 393
High Level Installation Process 393
nCipher HSM Installation 394
Setting Up the Integration 395
Basic netHSM Configuration 396

High Level Functional Description

This section describes the integration with the network HSM provided by the nCipher company, netHSM.

- SecureSphere supports storing keys on the netHSM and accessing the keys in real-time in order to decrypt SSL web traffic. The following options are supported:
- Accessing multiple keys from multiple SecureSphere Gateways.
- Accessing the same key from multiple SecureSphere Gateways, including the case of Gateways that are in high availability mode.
- Working with a mix of keys, where some keys are stored in an HSM device while other keys are stored in SecureSphere.



Note:

- When generating command state, do not use passphrase.
- If the key is already in nCipher, then you must create a fake key using the `generate -r embed` command.

Components Taking Part in the Integration

The following components are involved in the integration:

- The nCipher netHSM – the server that holds the secret keys (referred to in this document as the netHSM).
- The nCipher RFS Server – the remote file system server (referred to in this document as the RFS Server).
- The SecureSphere Gateway – performs the traffic decryption and receives key services from the netHSM. The SecureSphere Gateway will be referred to in this document as the Gateway.
- The SecureSphere MX Server – holds the security policy instructing which keys should be applied to the encrypted traffic. The SecureSphere MX Server will be referred to in this document as the MX Server.

High Level Installation Process

To integrate SecureSphere to the netHSM, proceed as follows:

1. Register the Gateway to the netHSM.
2. Register the Gateway to the RFS Server.

3. Enable nCipher support on the SecureSphere Gateway.
4. Synchronize between the Gateway and the RFS server.
5. Define the security policy on the MX Server.

The following figure shows the relationship between the components which comprise an nCipher HSM configuration.

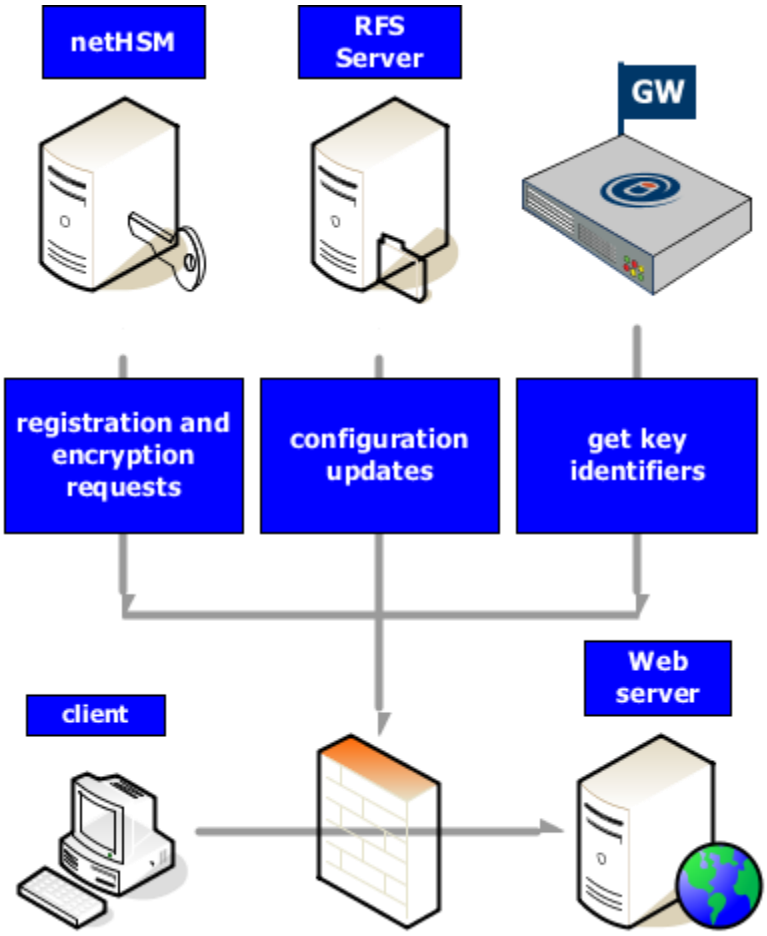


Figure 85: netHSM Components

nCipher HSM Installation

This section review aspects of nCipher HSM installation including the following:

Assumptions 394
Installing the nfast Software Package 395

Assumptions

This section outlines the process of integrating SecureSphere with a netHSM. It is assumed that the netHSM is already functional, so what remains to be done is to integrate SecureSphere to the device.

Consult with your netHSM administrator to confirm that the following prerequisites have been met.

1. netHSM is operational, and that the security world of the HSM device is appropriately initialized.

2. The correct version of SecureSphere is already installed and has successfully gone through the setup process.

   netHSM integration is enabled in SecureSphere version 6.0.6 patch 5 and above.
3. Keys are loaded to the netHSM: the keys are already stored in the netHSM, and for each stored key you have the matching fake key and certificate. If you need to do this yourself, see Basic netHSM Configuration on page 396 for instructions.
4. The RFS server is already installed and you know its IP address.

   Any Gateway using netHSM should have network access to the RFS through its management interface.
5. All connections between the Gateway and the netHSM and the RFS server pass through the Gateway's management interface.

   It is assumed that you have network connectivity between the Gateway and the RFS Server and the netHSM.
6. Confirm that you have access to the RFS Server and the netHSM.

   The RFS Server and the netHSM are separate devices (see the figure in High Level Installation Process on page 393) under the responsibility of the netHSM administrator. Several steps in this procedure are performed on the nCipher machines. If you do not have access to these machines, please contact the nCipher administrator to obtain access.

Installing the nfast Software Package

To install the nCipher application:

1. Execute the following commands:

```
/opt/nfast/sbin/install
```

Setting Up the Integration

Per-installation Checklist

Before setting up the integration procedure between SecureSphere and the netHSM, review the following checklist:

DB Pre-installation checklist

Step	✓	Action
1		netHSM is operational
2		RFS server is operational
3		SecureSphere is operational
4		You have the netHSM IP address
5		You have the RFS Server IP address
6		nfast RPM is installed on the Gateway

To integrate between SecureSphere and the netHSM:

1. Ensure that the SecureSphere Gateway accesses the netHSM and to the RFS Server through the appliance's management interface.

   Do this in `impcfg` (**Manage Platform** > **Manage Networks** > **Static Routes**).
2. Define the Gateway as a client to netHSM.

   On the netHSM, select **Menu** > **System** > **System configuration** > **Client config** > **New/Edit client** from the menu, and enter the Gateway's management IP address.
3. On the SecureSphere Gateway, get the netHSM's electronic serial number and key-hash (which will be used in subsequent commands) by executing the following command:

```
/opt/nfast/bin/anonkneti <netHSM-IP-address>
```

You will get the following output: ESN KEY-HASH.

4. Register the Gateway as a client to netHSM by executing the following command:

```
/opt/nfast/bin/nethsmenroll <netHSM-IP-address> <ESN> <KEY-HASH>
```

where <ESN> and <HASH> are the values obtained in the previous step.

5. Synchronize the Gateway with the RFS Server as follows:
   a) Add the Gateway as a permitted entity on the RFS server by executing the following command on the RFS Server for each Gateway:

```
/opt/nfast/bin/rfs-setup --gang-client --write-noauth
<Gateway-IP-Address>
```

   b) Bond and synchronize each Gateway with the RFS Server by executing the following command on the Gateway:

```
/opt/nfast/bin/rfs-sync --setup --no-authenticate <RFS-IP-address>
```

   c) Update the secure world and certificates files by running the following command:

```
/opt/nfast/bin/rfs-sync --update
```

6. Enable nCipher support on the SecureSphere Gateway as follows:
   a) Run `impcfg` and enable HSM (**Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)**).
   b) In `impcfg`, apply the configuration.
   c) Confirm that the private keys are already loaded to the netHSM.

   It is assumed that the private keys are already loaded to the netHSM, and you have the appropriate fake keys, and matching certificates. If you still need to do this yourself, see Basic netHSM Configuration on page 396.
7. Configure the keys on the SecureSphere Management Server by editing the web service and adding the appropriate fake keys and matching certificate files.
8. Sign these keys as HSM keys by selecting **HSM** for these keys.

Once the Gateway is updated, you can start decrypting traffic using your netHSM device.

Terminating the Integration

To terminate the integration between the netHSM and SecureSphere:

1. Remove the keys from the MX by deleting all the keys marked as HSM, and replacing them with the real keys as appropriate.
2. Disable the nCipher HSM by disabling HSM (**Manage SecureSphere Gateway** > **Manage hardware security modules (HSM)**)
3. On the Gateway, remove the RPM by executing the following command:

```
#rpm –e nfast
```

Basic netHSM Configuration

You must import one or more keys into the netHSM.

1. Obtain the protected server's certificate as a <name>.pfx file.

   For example, assuming the server name is Lizard, the file name would be `lizard.pfx`. This file contains both the server's private key and its certificate.
2. Open the server's certificate file (for `lizard.pfx`) and extract the key and certificate (to a file named `lizard-combined.pem`) by running the following command:

```
openssl pkcs12 -in lizard.pfx -out lizard-combined.pem –nodes
```

3. Using a text editor such as `vi`, open the `lizard-combined.pem` file.
4. Separate the key and certificate out of the `lizard-combined.pem` file. into two separate files – one for the private key and the other for the certificate.
5. Save the lines between:

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

into a file named `lizard_private.pem`.

6. Save the lines between:

```
-----BEGIN CERTIFICATE-----
```

...

```
-----END CERTIFICATE-----
```

into a file named `lizard_cert.pem`.

7. Import the key into the HSM and produce a fake key by executing the following command:

```
/opt/nfast/bin/generatekey --import embed protect=module \
pemreadfile=lizard_private.pem embedsavefile=fake_lizard_private.pem
\ plainname=lizard nvram=no
```

where:

- `pemreadfile` is the real private key to be stored in the netHSM.
- `embedsavefile` is the output fake key to be loaded on the MX Server.

8. Transfer the files `lizard_cert.pem` and `fake_lizard_private.pem` to the SecureSphere Management Server and import them.

   Make sure the **HSM** checkbox is checked.

9. After adding the key to the netHSM, synch it to the Gateway by running the following command on the SecureSphere Gateway:

```
/opt/nfast/bin/rfs-sync –update
```



Note: You must run the update command on the Gateway every time you add or remove a key on the netHSM to be used on the Gateway.

Storage Area Networks (SAN)

This section describes how to integrate SecureSphere with Storage Area Networks, and includes:

SAN Overview 398
Supported SAN Hardware 398
Configuring SecureSphere for SAN 399
Disabling the SAN 408

SAN Overview

SAN connectivity enables SecureSphere to store data on centrally managed storage, providing the following benefits:

- better allocation and use of resources
- storage redundancy for higher availability
- central storage security management
- central backup/restore strategies

SecureSphere supports the following usage scenarios for a Storage Area Network (SAN):

- On a Gateway, you can use the SAN to store audit data collected by the Gateway.
- On a management server (MX), you can use the SAN to store configuration, event, audit and report archives.
- On a Onebox, you can use the SAN to store audit data, configuration, event, audit and report archives.

The section describes how to connect and define and connect SecureSphere to the Storage Area Network, and how to configure SecureSphere to use the SAN.

Supported SAN Hardware

Supported SAN Hardware includes the following:

Host Bus Adapters 398
Cabling 398

Host Bus Adapters

SecureSphere supports the following Emulex Host Bus Adapters:

- For PCI-X single channel: LP10000
- For PCI-X dual channel: LP10000DC
- For PCI-E single channel: LPe11000
- For PCI-E dual channel: LPe11002

These PCI-X HBA cards provide one 2GB Fibre Channel link with automatic 1GB downward compatibility. The PCI-E HBA cards provide one 4GB Fibre Channel link with automatic 1GB downward compatibility.

Other HBAs are not currently supported.

Cabling

The HBA provides one or two Fiber Channel port via an LC type optical connector. A suitable optical FC cable must be provided by the SecureSphere user. The type of the cable depends of the equipment to which it will be attached (RAID or a FC switch).

Configuring SecureSphere for SAN

This section reviews how to configure SecureSphere for SAN.



Note:

- On a SecureSphere Gateway, SAN is used only for the audit data. The path of the audit directory is defined in the `audit-base-path` attribute in the `bootstrap.xml` file.
- On a SecureSphere MX, SAN is used for archiving. The path of the archive directory is defined in the SecureSphere GUI.

SAN Configuration Task Overview

This section reviews the main tasks involved with configuring SAN.

SAN Configuration Tasks

Step		Action	For more information, see
1.		Determine your storage requirements.	Determine Storage Requirements on page 400
2.		Make a note of the original SCSI configuration. **Note:** This step is to be performed **only** by authorized Imperva personnel.	Make a Note of the Original SCSI Configuration on page 400
3.		Add the HBA to the SecureSphere appliance. **Note:** This step is to be performed **only** by authorized Imperva personnel.	Add the HBA to the SecureSphere Appliance on page 401
4.		Check that the HBA card is functioning properly.	Check the HBA Card on page 401
5.		Request that the Storage Manager add a Logical Volume.	Request that the Storage Manager Add a Logical Volume on page 402
6.		Physically connect to the SAN.	Physically Connect to the SAN on page 403
7.		Scan the Fiber Channel (FC).	Scan the Fibre Channel on page 403
8.		Update `/etc/modprobe.conf`.	Update /etc/modprobe.conf on page 404
9.		Create a file system on the SCSI target.	Create a File System on the SCSI Target on page 405
10.		Mount the new file system.	Mount the New File System on page 405
11.		Test the new file system.	Test the New File System on page 405
12.		Create a startup file.	Create a Startup File on page 405
13.		Reboot the SecureSphere appliance.	Reboot the Machine on page 407

Step		Action	For more information, see
14.		Configure SecureSphere to use the SAN.	Configure SecureSphere to Use the SAN on page 407

Each of these steps is explained in detail in the following sections.

Determine Storage Requirements

1. Determine the storage requirements, taking into account the following considerations.
   Accurately planning storage requirements requires some analysis. Some issues that influence the decision include:
   - special requirements of the SecureSphere site
   - capacity of the SAN storage device(s)
   - amount of traffic audited by the SecureSphere Gateways and archived by the MX
   - accumulated experience with historical storage requirements at this site
   - projections of future storage requirements

   Note: The Storage Manager must allocate a separate Logical Volume for each SecureSphere appliance which accesses external storage.

Make a Note of the Original SCSI Configuration

Warning: This step is to be performed **only** by authorized Imperva personnel.

The appliance may already have SCSI devices, specifically internal SCSI disks. You must take a note of the SCSI devices which have been recognized before you add the Fibre Channel adapter. This will allow you to know what SCSI devices will be added by the FC connection.

1. To see the list of SCSI devices, examine the `/proc/partitions` file.
   On a machine with local SCSI disks, the `/proc/partitions` file will be similar to the following:

```
[root@localhost ~]# cat /proc/partitions
major minor  #blocks  name

   8     0  244008960 sda
   8     1      56196 sda1
   8     2  243947025 sda2
 253     0   29360128 dm-0
 253     1  142802944 dm-1
 253     2   68616192 dm-2
 253     3    3145728 dm-3
```

   In this example, there are partitions on the `sda` SCSI drive (`sda` stands for SCSI disk `a`), indicating that the machine currently has only one SCSI disk.
   Make a note of **all** the SCSI disks (everything that starts with `sd`).

Add the HBA to the SecureSphere Appliance



Warning:

- This step is relevant **only** for G-series appliances. For X-series appliances, a SAN card can only be installed in the factory, and not at the customer site.
- If the HBA card has been installed by the appliance manufacturer, it is not necessary to perform this step.
- This step is to be performed **only** by authorized Imperva personnel.

1. Shut down the appliance and power it off.



Warning: Make sure you are properly grounded before handling the HBA card and the open appliance box.

2. Remove the cover.
3. Locate an empty PCI slot.
4. Insert the HBA card into the empty PCI slot and secure it in place.
5. Close the cover and secure it.
6. Power the appliance on.

Check the HBA Card

1. Log in as `root`.
2. Manually load the Emulex device driver by executing the following command:
   ```
   # modprobe lpfc
   ```
3. Obtain the adapter's WWN by executing the following command:
   ```
   # systool -a -v -c fc_host
   ```
   The following is an example output:

```
Class = "fc_host"
Class Device = "host4"
Class Device path = "/sys/class/fc_host/host4"
active_fc4s = "0x00 0x00 0x01 0x00 0x00 0x00 0x00 0x01
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 "
fabric_name = "0x20000000c963a4ad"
issue_lip = <store method only>
maxframe_size = "2048 bytes"
node_name = "0x20000000c963a4ad"
port_id = "0x000000"
port_name = "0x10000000c963a4ad"
port_state = "Linkdown"
port_type = "Unknown"
speed = "unknown"
supported_classes = "Class 3"
supported_fc4s = "0x00 0x00 0x01 0x00 0x00 0x00 0x00 0x01
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 "
supported_speeds = "1 Gbit, 2 Gbit"
symbolic_name = "Emulex LP10000DC-M2 FV1.91A5 DV8.1.10.9"
tgtid_bind_type = "wwpn (World Wide Port Name)"
uevent = <store method only>
Device = "host4"
Device path =
"/sys/devices/pci0000:00/0000:00:06.0/0000:0b:00.2/0000:0d:01.1/host
4"
uevent = <store method only>
```

If the driver does not load successfully, there will be no output from the `systool` command.

If the driver does load successfully, a green LED on the adapter will blink until a link is established.

Request that the Storage Manager Add a Logical Volume

1. At this point, ask the local Storage Manager to allocate a Logical Volume on the storage device (using the Storage Manager tools) and configure the partitioning and/or zoning to allow the appliance to access it.

   The information you must provide is:

   - the amount of storage needed, as determined in the first part of this procedure
   - the HBA's WWN, which you obtained in the previous step

     In the example above the number is "`0x10000000c963a4ad`" (see the `port_name` parameter).
   - the type of the operating system, in this case, Linux

   This step may take some time due to maintenance schedules, allocation decisions, *etc.*, so you should perform it as soon as possible.



Note: The zoning should be configured so that the SecureSphere appliance sees only the SCSI target it is supposed to use as a file system.

Physically Connect to the SAN

1. Insert the optical cable connector into the Adapter.

   Pay attention to the Receive/Transmit sides. The other end of the cable should be connected to the appropriate storage device or Fibre Channel switch.

   After a short while the green LED on the adapter should stop blinking. This indicates that a link has been negotiated and established. If this does not happen ask the Storage Manager for help.

Scan the Fibre Channel

At this stage, the driver scans the Fibre Channel for SCSI targets. This operation is performed by the FC device driver, when it is initiated.

1. Unload the driver by executing the following command:

   ```
   # rmmod lpfc
   ```

2. If you are not using multipath go to step 1.
3. If you are using multipath, then perform the following steps:

   a) Open the `/etc/multipath.conf` file with a text editor.

   Note: The `/etc/multipath.conf` file is installed by default when you install the `device-mapper-multipath`.

   b) Insert a "#" character to comment-out the lines that blacklist all devices by default.

   So the following lines:

   ```
   blacklist {
           devnode "*"
   }
   ```

   become:

   ```
   #blacklist {
   #         devnode "*"
   #}
   ```

   c) Remove the "#" character to un-comment the lines that enable the `devnode` blacklist.

   So the following lines:

   ```
   #blacklist {
   #       wwid 26353900f02796769
   #         devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
   #         devnode "^hd[a-z]"
   #}
   ```

   become:

```
blacklist {
        wwid 26353900f02796769
         devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
         devnode "^hd[a-z]"
}
```

d) Perform a dry run and evaluate the setup by executing the following command:

```
# multipath -v2 -d
```

The output should look like this:

```
mpath1 (3600601602d401e0083e32ef66638de11) dm-4 DGC,RAID 5
[size=100G][features=1 queue_if_no_path][hwhandler=1 emc] \_ round-robin 0
[prio=1][active]   \_ 1:0:0:0 sdb 8:16   [active][ready] \_ round-robin 0
[prio=0][enabled]  \_ 2:0:0:0 sdd 8:48   [active][ready]
```

e) Start the required multipath processes by executing the following command:

```
# /etc/init.d/multipathd start
```

f) Execute the multipath command:

```
# multipath -v2
```

g) To get a listing of the current setup, execute the following command:

```
# multipath -ll
```

h) Integrate the startup of the appropriate daemons in the boot sequence by executing the following commands:

```
# chkconfig --add multipathd
# chkconfig multipathd on
```



Note: Additional documentation is available in the directory `/usr/share/doc/device-mapper-multipath-x.x.x/`

Update /etc/modprobe.conf

1. Add the following line to the `/etc/modprobe.conf` file:

   ```
   alias scsi_hostadapter lpfc options scsi_mod max_scsi_luns=256
   ```

   Note: If the file already contains `alias scsi_hostadapter`, you must use a different name, for example, `alias scsi_hostadapter1`.

2. Execute the following command:

   ```
   # modprobe lpfc
   ```

3. Examine the `/proc/partitions` file by executing the following command:

   ```
   # cat /proc/partitions
   ```

4. Compare the contents of the `/proc/partitions` file with what you recorded in the Make a Note of the Original SCSI Configuration on page 400.

   If your appliance previously had an sda disk and now has an sdb disk as well, then sdb is the disk that has been detected on the Fibre Channel. You will use this information in the following sections, wherever you encounter the sdX notation.



Note: If you are using multipath, the partition is named dm-X, where X is a number.

If you have successfully completed all the steps above, you can proceed to add the newly accessed storage to the Linux operating system.

Create a File System on the SCSI Target

1. Execute the following the command:
   ```
   # mkfs.ext3 /dev/sdX
   ```
   This will create an ext3 file system on the SCSI target at `/dev/sdX`.



Note: There is no need to create a partition for the `/dev/dm-X` devices. You need only format them using the `mkfs.ext3 /dev/dm-X` command, where X is a digit.

Mount the New File System

1. Create a mount point and mount the file system by executing the following command:
   ```
   # mkdir -p /mnt/external-storage
   # mount /dev/sdX /mnt/external-storage
   ```



Note: If you are using multipath, the device is named `/dev/dm-X` , where X is a digit.

Test the New File System

1. Create a file in the new file system.
2. Remove the file you created in the previous step.

Create a Startup File

You will be creating a startup file that will load the FC module and attach the external storage at boot time, **before** SecureSphere starts.

1. Create a startup file named `/etc/init.d/external-storage` which consists of the following code:

```
#!/bin/bash
# chkconfig: 35 84 98
# description: Loads the Emulex FC driver
mount_point=/mnt/external-storage
device=""
```

```
DRIVERS="lpfc"
disks=$(cat /proc/partitions | awk '$4 ~ "^sd" {print $4}')
for disk in ${disks}; do
    if [[ -a /dev/${disk} ]]; then
        success="$(udevadm info -a -p $(udevadm info -q path -n /dev/${disk}) | grep $DRIVERS | wc -l)"
        if [[ "${success}" -gt 0 ]]; then
            device="/dev/"${disk}
            break
        fi
    fi
done
module=lpfc
prog=$( basename ${0} )
prog=${prog#[SK]??}
function start() {
        if [ "$(lspci -d 10df:fa00 -n)" ] || [ "$(lspci -d 10df:fe00 -n)" ]; then
        modprobe ${module}
            if ! grep -qw ${module} /proc/modules; then
                echo "${prog}: could not load module \"${module}\""
            exit 1
        fi
     fi
    if [[ ! -z "$device" ]];then
        declare dev=$( basename ${device} )
        #
        # Probe for LP10000-E or LP11e002. If found, load lpfc.
        #
        if ! grep -wq ${dev} /proc/partitions; then
            echo "${prog}: cannot find \"${dev}\" in /proc/partitions"
            exit 1
        fi
        mkdir -p -m 777 ${mount_point}
        mount ${device} ${mount_point}
        if ! grep -wq ${mount_point} /proc/mounts; then
            echo "${prog}: cannot mount \"${device}\" on \"${mount_point}\""
                exit 1
            fi
    fi
}

function stop() {
     if [[ ! -z "$device" ]];then
        umount -f ${mount_point}
     fi
     rmmod ${module}
}
```

```
case "${1}" in
start)
      start
      ;;
stop)
      stop
      ;;
restart)
     stop
     start
     ;;
esac
```

2. Link the startup file to the boot/shutdown sequence by executing the following commands:

```
# chmod 755 /etc/init.d/external-storage
# chkconfig --add external-storage
# chkconfig external-storage on
```

Reboot the Machine

1. Reboot the SecureSphere appliance to verify that the required processes automatically start.
   When the machine comes up the new file system should be accessible via the `/mnt/external-storage` mount point.

Configure SecureSphere to Use the SAN

You must configure the SecureSphere appliance to use SAN.

- On a Gateway, you can use the SAN to store audit data.
- On a management server (MX), you can use the SAN to store you can use the SAN to store configuration, event, audit and report archives.
- On a Onebox, you can use the SAN to store both audit data, you can use the SAN to store configuration, event, audit and report archives.

To use the SAN to store audit data:

If you are using the SAN to store the Gateway's audit data, configure the SecureSphere Gateway or Onebox as follows:

1. Open the `/opt/SecureSphere/etc/bootstrap.xml` file using a text editor.
2. If you are using SecureSphere version 6.2 or higher, change the path of the `audit-base-path` attribute to point to the SAN.
3. If you are using SecureSphere version 6.0.6.X, change the path of the `var-dir` attribute to point to the SAN.
4. Restart the Gateway.

To use the SAN to store archive data:

If you are using the SAN to store archive data, configure the SecureSphere MX or Onebox as follows:

1. Start the SecureSphere GUI.
2. In the **Admin** worskpace, click **System Definitions**.
3. In the **System Definitions** pane, select **Action Interfaces**.
4. In the **Interfaces** pane, click .
5. Create a new interface of **Type** NFS Archive.

6. In the **Main** worskpace, click **Policies** > **Action Sets**.
7. Create a new Action Set of type **Archiving**.
8. In the **NFS > Archive** parameter, define the `/mnt/external-storage` mount point.
9. Use the new Action Set as the **Archive Action** (in the **Archiving** tab) in a policy, for example, in an Audit policy.

Disabling the SAN

This section reviews displaying the SAN and includes the following topics:

On the Management Server 408
On the Gateway 408

On the Management Server

Reconfigure archiving actions so that they do not archive to the SAN location.

On the Gateway

To disable SAN on the Gateway, you must:

- disable SAN in SecureSphere
- reconfigure the appliance so that it no longer accesses the SAN

To disable SAN on a SecureSphere Gateway:

1. Open the `bootstrap.xml` file with a text editor.
2. Restore the `audit-base-path` attribute in the first element to its previous value.
   The default value for Imperva platforms is `/var/SecureSphere`.
3. Restart the Gateway.

To reconfigure the appliance so that it no longer accesses the SAN:

1. Login to the appliance as `root`.
2. Execute the following command:un the command:
   `# chkconfig external-storage off`
3. Reboot the appliance.
   You must reboot the appliance in order to cleanly shut down any applications that currently use external storage.

SSL Accelerator

SSL accelerator cards are used to speed SSL processing in SecureSphere appliances. The cards are available for all SecureSphere appliances.

SecureSphere SSL accelerator cards support keys of length 1024 bits and higher.

For more information on SecureSphere SSL accelerator cards, see the Imperva Customer Support Portal (CSP) at www.imperva.com.

LOM (Lights Out Management)

This section reviews lights out management and includes the following:

Overview 409
Connecting to the LOM 409
Managing the LOM 410

Overview

The LOM (Lights Out Management) add-on is available as a factory installed option for the selected appliances, and enables the following functions to be performed remotely

- power on
- power off
- reboot (reset)

Connecting to the LOM

To connect to the LOM card:

1. Point your browser to https://<IP address of LOM card>

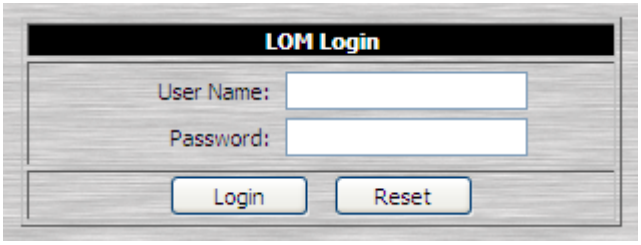


Figure 86: LOM Login Window

The default **IP Address** for LOM card configuration is **http://192.168.0.60**.

2. Enter the **User Name** and the **Password**.
   The default is administrator and the default **Password** is password.
3. Click **Login**.
   The **LOM Management** window is displayed.

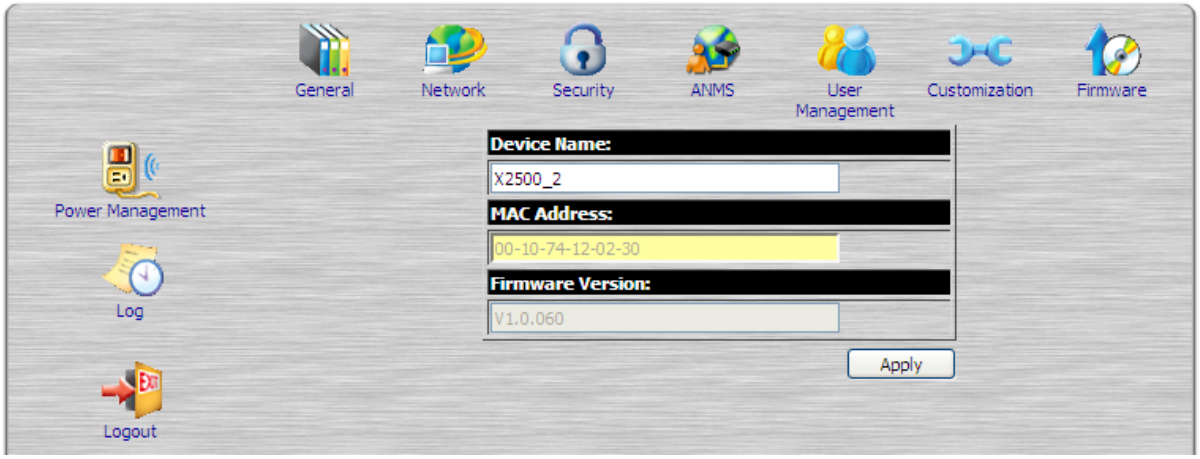


Figure 87: LOM General Window

4. Select one of the options by clicking on it.

Managing the LOM

The **LOM Management** window offers the following options:

General 410
Network 411
Security 413
ANMS (RADIUS Settings) 414
User Management 415
Customization 417
Firmware 418
Power Management 419
Log 420
Logout 421

General

This topic reviews General settings.



Figure 88: LOM General Window

The **General** window displays the following parameters:

General Window Parameters

Parameter	Description
Device Name	Enter the LOM card's device name. The name can be up to 16 characters long.
MAC Address	**Read only**: The LOM card's MAC address.
Firmware Version	**Read only**: The version number of the LOM card's firmware.

If the LOM card's IP address is assigned by a DHCP, the address is displayed at the bottom of the window.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Network

This topic reviews Networking.

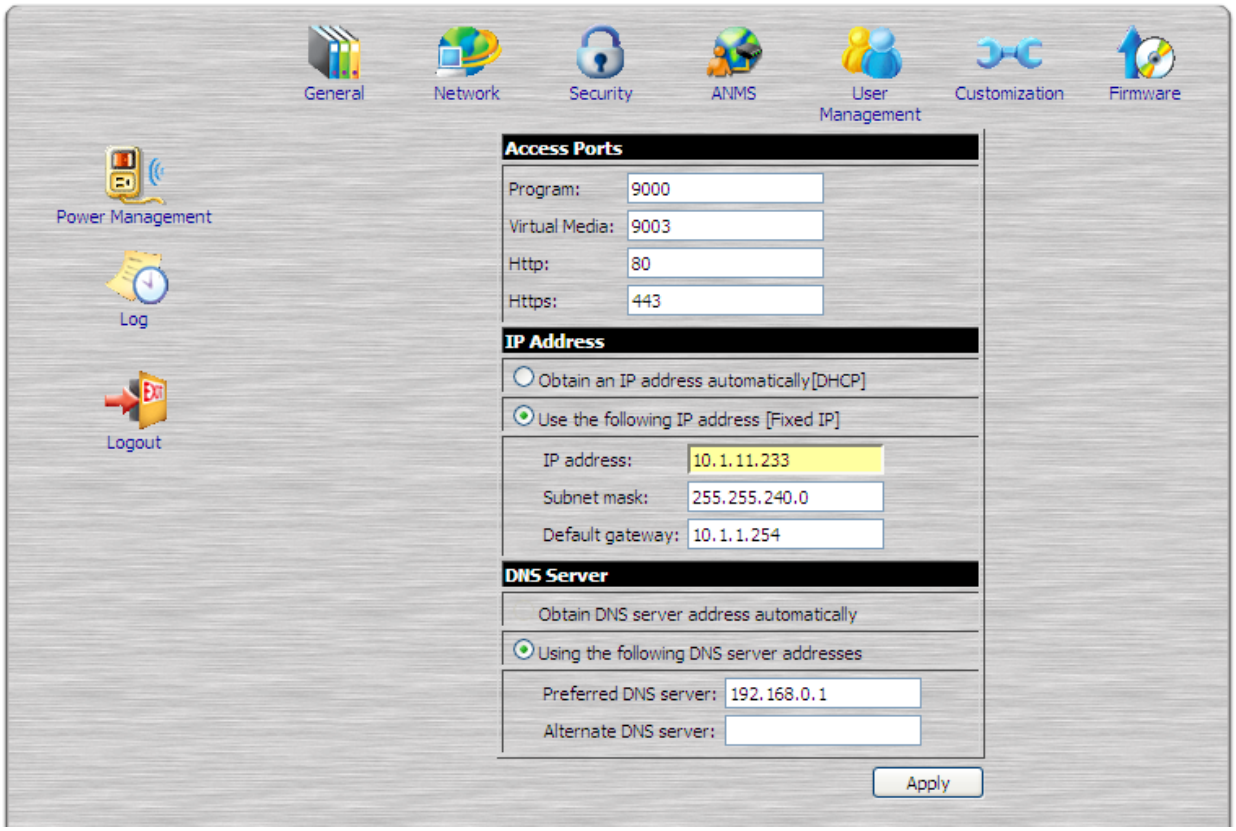


Figure 89: Network Window

The **Network** window displays the following parameters:

Network Window Parameters

Parameter	Description
Access Ports	
Programs	The port number used for keyboard, video, mouse and message data transfers. Valid entries are 1024-65536. The default is 9000.
Virtual media	The port number used for data transfer using the virtual media feature. Valid entries are 1024-65536. The default is 9003.
Http	The port number for browser login. Valid entries are 1-65536. The default is 80.
Https	The port number for browser login. Valid entries are 1-65536. The default is 443.
IP Address **Note:** If you change the IP address, then you must check **Reset on Exit** on the **Customization** window (see Customization on page 417) so that the change will take effect.	
Obtain an IP Address Automatically (DHCP)	Obtain a dynamically-assigned IP address using DHCP.
Use the Following IP Address (Fixed IP)	The device has a fixed IP address.
IP Address	Enter the device's fixed IP address.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default Gateway.
DNS Server	
Obtain DNS Server address automatically	Select this item to specify that the DNS server's IP address is obtained automatically.
Use the following DNS Server address	Select this item to specify that you will enter the DNS server's IP address in Preferred DNS Server. Selecting this option enables the next two items.
Preferred DNS Server	Enter the IP address of the primary DNS server.
Alternate DNS Server	Optionally, enter the IP address of the secondary DNS server.



Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Security

This topic reviews Security.

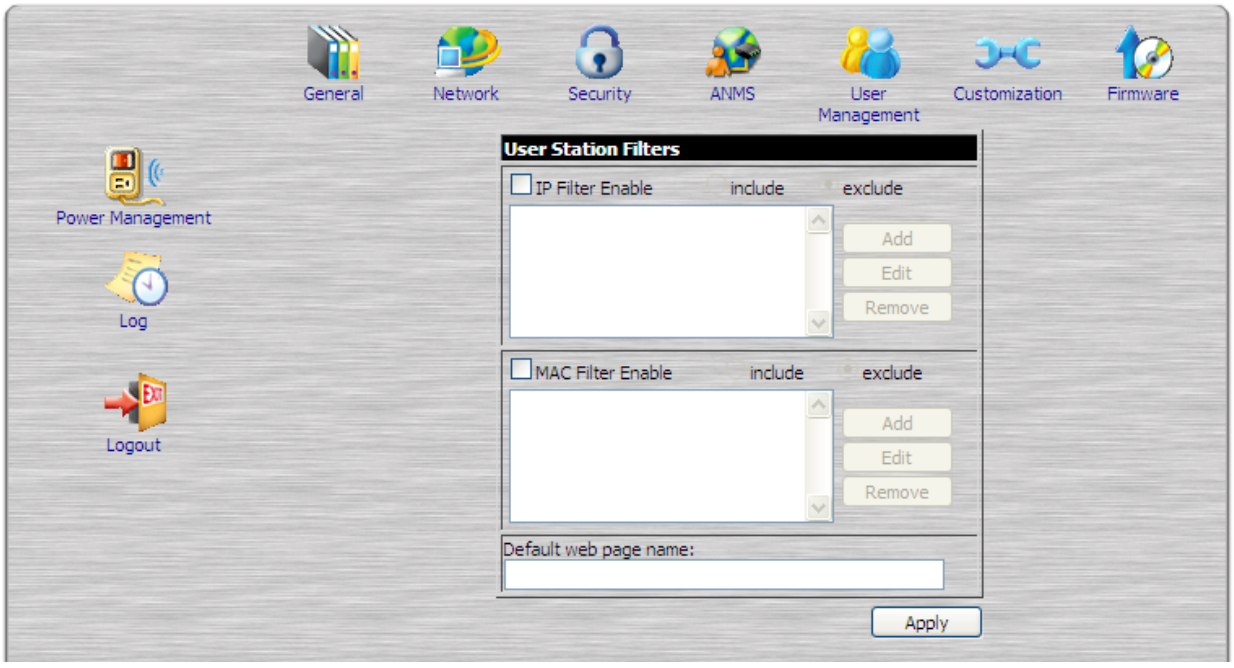


Figure 90: Security Window

You can filter access to the LOM card by specifying the IP addresses and/or MAC addresses of devices which are allowed or not allowed to access the LOM card.

To define a filter based on the IP address of the device accessing the LOM card:

1. Select **IP Filter Enable**.
2. Click **Add**.
3. In the first dialog box, enter a starting IP address and click **OK**.
4. In the first dialog box, enter an end IP address and click **OK**.

   Up to 100 IP address ranges can be specified.
5. Select **include** or **exclude** as appropriate.

To define a filter based on the MAC address of the device accessing the LOM card:

1. Select **MAC Filter Enable**.
2. Click **Add**.
3. Enter a MAC address.
4. Select **include** or **exclude** as appropriate.

Defining a Required Login String for Web Browser Access

Default Web page name enables administrators to specify a login string, in addition to the URL, which must be entered when accessing the LOM device using a browser. For example:

```
192.168.0.2/abcdefg
```

Users must include the forward slash and the string when accessing the LOM card.

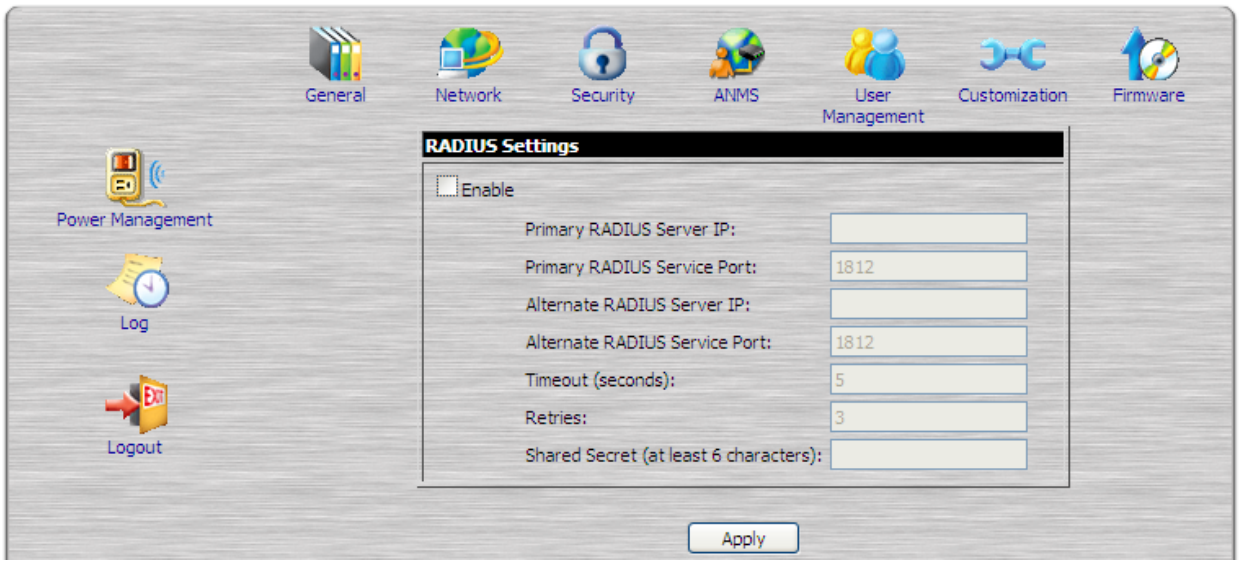


Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

ANMS (RADIUS Settings)

This topic reviews ANMS (RADIUS) settings.

Equation 1: ANMS (RADIUS Settings) Window



The **ANMS (RADIUS Settings)** window displays the following parameters:

ANMS (RADIUS Settings) Window Parameters

Parameter	Description
Primary RADIUS Server IP	The IP address of the primary RADIUS server.
Primary RADIUS Server Port	The port number of the RADIUS service on that server.
Secondary RADIUS Server IP	The IP address of the secondary RADIUS server.
Secondary RADIUS Server Port	The port number of the RADIUS service on that server.
Timeout (seconds)	The number of seconds after which a timeout condition is raised while attempting to connect to a RADIUS server.
Retries	The number of times to try to establish the connection to the RADIUS server.
Shared Secret (at least 6 characters)	The shared secret, for authentication with the RADIUS server.

On the RADIUS server, grant users access according to the following table:

RADIUS Permissions

Access Code	Description
C	Grants the user administrator privileges, allowing him or her to configure the LOM card.
W	Allows the user to access the LOM card using the Windows client.
J	Allows the user to access the LOM card using Java.
P	Allows thew user to power on, power off and reset the SecureSphere appliance in which the LOM card is installed.
L	Allows the user to access log information using a browser.
V	Limits to the viewer's access to viewing the video display.

Note:

- The access codes are not case-sensitive.
- A user can be assignee more than one code, separated by commas.
- Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

User Management

This topic reviews User Management.

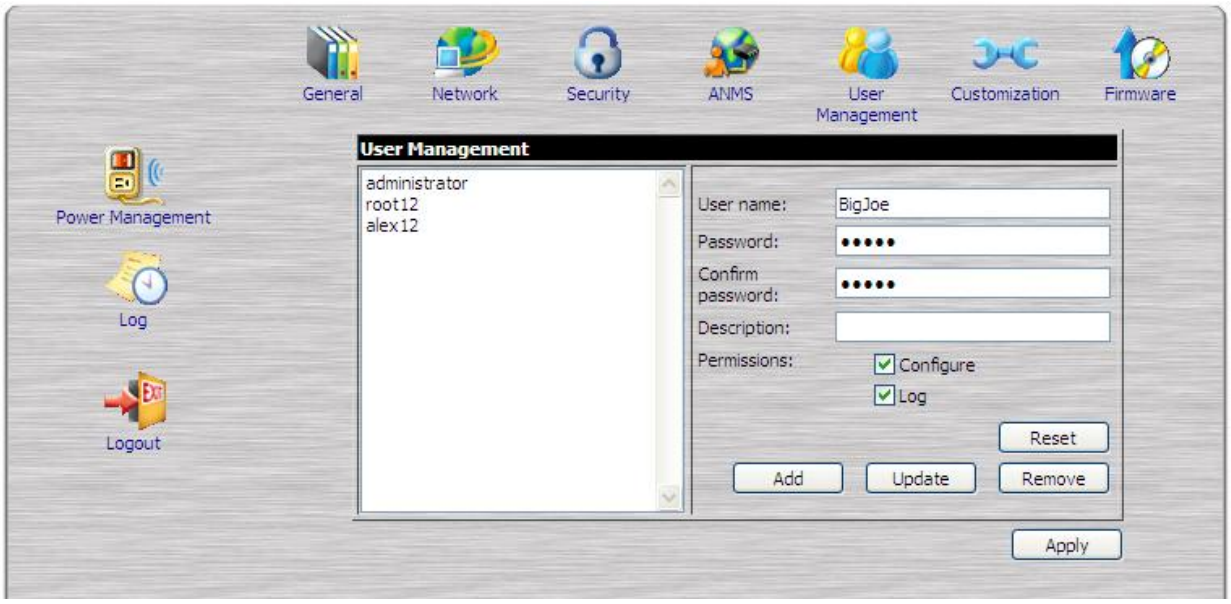


Figure 91: User Management Window

The **User Management** window displays the list of users authorized to connect to the LOM card, and enables you to add, edit or delete users.

To add a user:

1. Enter the parameters from the table **User Management Window Parameters** below for the user.
2. Click **Add**.

User Management Window Parameters

Parameter	Description
User Name	The user's name (between 6 and 16 characters).
Password	The user's password (between 6 and 16 characters).
Confirm Password	Enter the password a second time, to confirm it.
Description	**Optional**: information about the user.
Permissions	Define the user's permissions by selecting one or both of **Configure** or **Log**.

To edit a user:

1. Select the user from the list on the left.
2. Change the user's parameters, as required.
3. Click **Update**.

To delete a user:

1. Select the user from the list on the left.
2. Click **Remove**.



Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Customization

This topic reviews Customization .

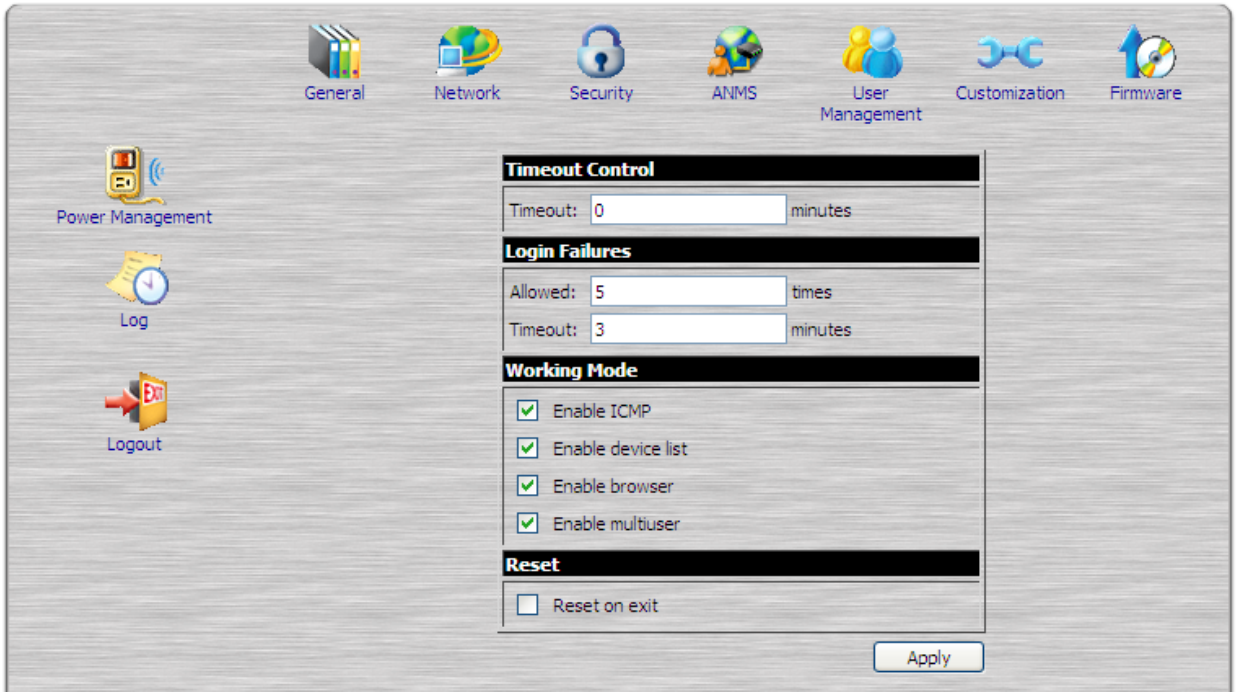


Figure 92: Customization Window

The **Customization** window displays the following parameters:

Customization Window Parameters

Parameter	Description
Timeout Control	
Timeout	The session will be ended if there is no input from the connected device for a period of **Timeout** minutes.
Login Failures	
Allowed	The number of failed login attempts a user is allowed, before he is locked out for **Timeout** minutes.
Timeout	The number of minutes a locked out user is prevented from logging in.
Working Mode	
Enable ICMP	If enabled, the LOM card can be PINGed.
Enable Device List	If enabled, the LOM card will be listed among the available devices.
Enable browser	If enabled, the LOM card can be accessed using a browser.
Enable multiuser	If enabled, up to 32 users can access the LOM card simultaneously.
Reset	
Reset on exit	Reset the LOM card when exiting this application.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Firmware

This topic reviews Firmware.

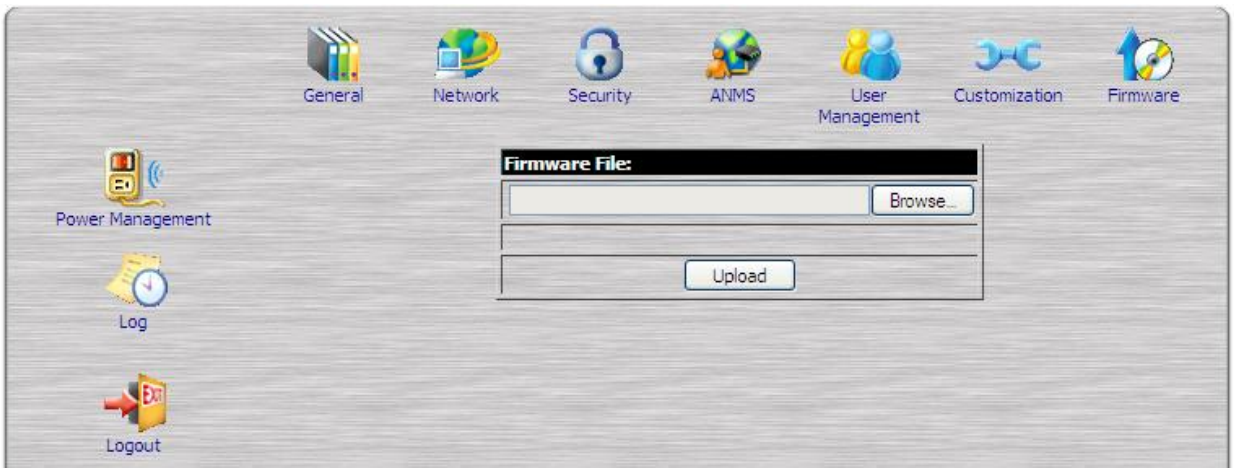


Figure 93: Firmware Window

The **Firmware** window enables you to upgrade the LOM card's firmware from a file you have previously downloaded.

To upgrade the firmware:

1. Browse to the file containing the firmware.
2. Click **Upload**.

Note: The firmware will be updated after you restart the appliance.

Power Management

This topic reviews Power Management.



Figure 94: Power Management Window

The **Power Management** window displays the following parameters:

Power Management Window Parameters

Parameter	Description
Server Power	Indicates whether the SecureSphere appliance is on or off.
Power On/Off	Click to power the SecureSphere appliance on or off, as appropriate.
Reset	Click to reset the SecureSphere appliance.

Note: Click **Apply** to apply any changes you have made. The changes will not be applied immediately, but only after you logout.

Log

This topic reviews the Log.

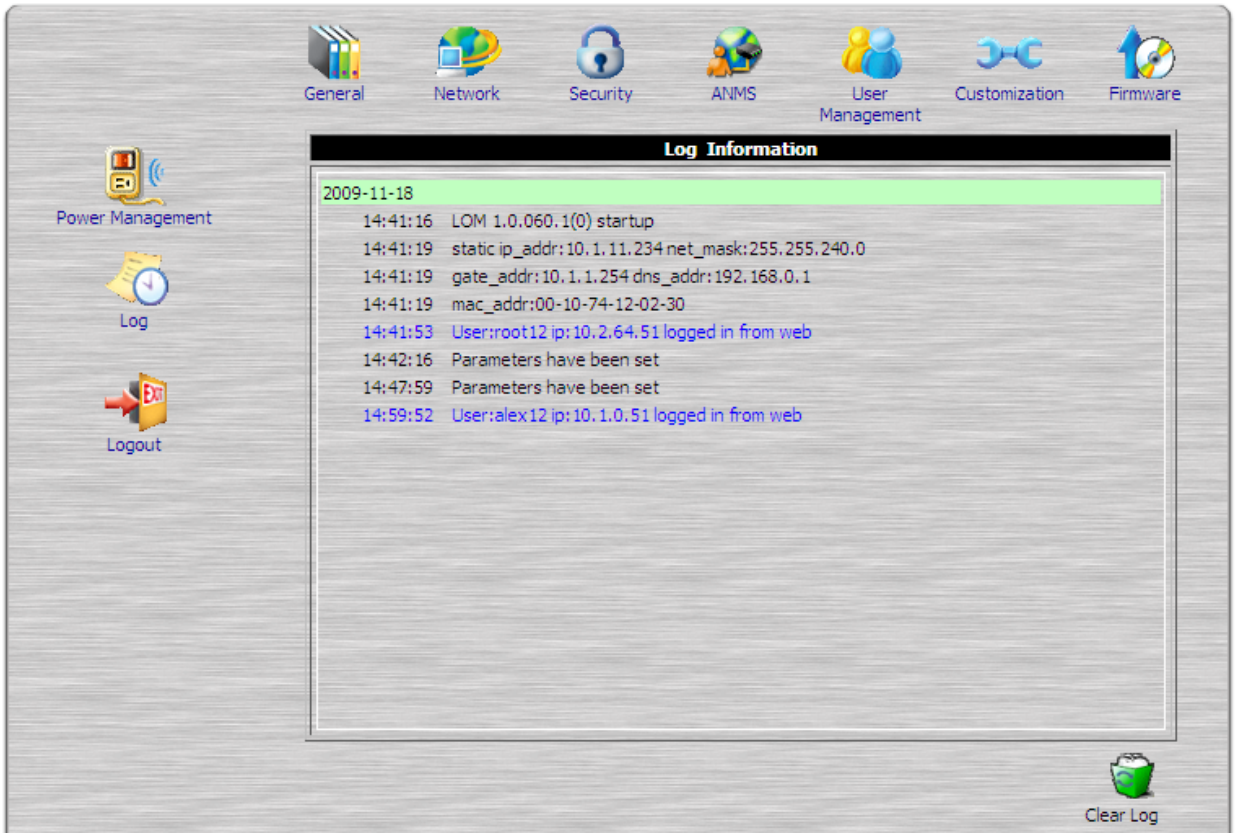


Figure 95: Log Window

The **Log** window displays the events log.

To clear the events log, click the **Clear Log** icon.

Logout

This topic reviews Logging Out.

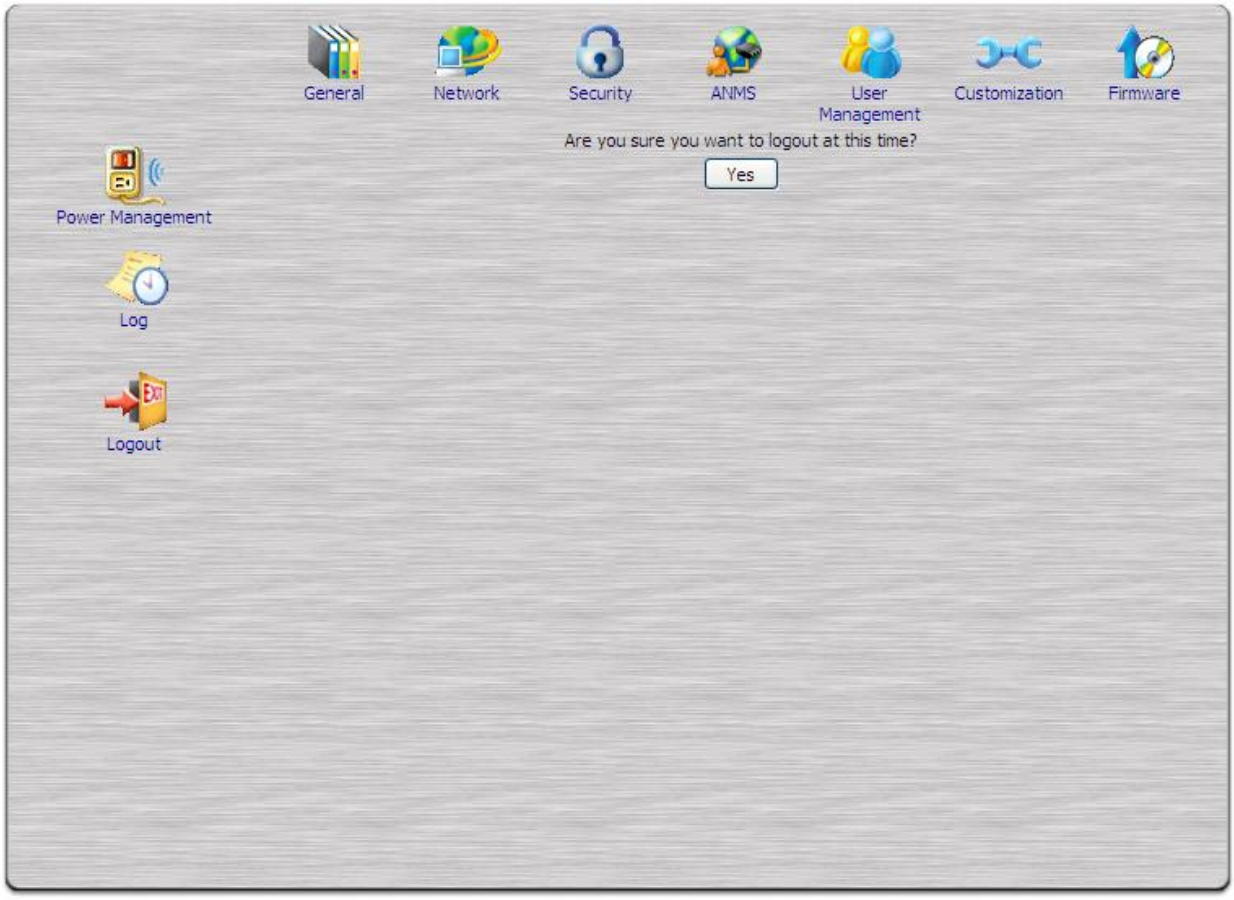


Figure 96: Logout Window

If there are pending changes that have not yet been applied, a message will be displayed to that effect. The changes will be applied after you logout.

To logout, click **Yes**.

APPENDIX C

Command Line Interface

This chapter is a reference to the SecureSphere command line tools and reviews the following topics:

impcfg 422
impctl 426
Miscellaneous Commands 430

impcfg

This section describes the impcfg command and reviews the following:

impcfg Functionality Map 422

impcfg Functionality Map

The table **impcfg Functionality Map** below shows the complete `impcfg` functionality.



Note: (I) means immediate activation, that is, the command is executed and, if relevant, the SecureSphere database is updated immediately.

impcfg Functionality Map

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
Manage SecureSphere Server	Deactivate server			Configuring a Management Server on page 67
	Restart server (I)			
	Stop server (I)			
	Change management password			
	Change database password			
	Deactivate server			
Manage SecureSphere Gateway	Perform actions (start, stop, etc.)	Unregister gateway **(I)**		Configuring a Gateway on page 68
		Soft gateway restart **(I)**		
		Hard gateway restart (teardown/prepare resources) **(I)**		
		Stop gateway **(I)**		
		Refresh gateway status **(I)**		
Manage SecureSphere Gateway *(continued)*	Change gateway name			
	Change server address /password			
	Change operation mode	Sniffing		Configuring a Gateway as a Sniffing Gateway on page 74 **Note:** The management server must be running when you execute this command.
		Bridge STP		Configuring a Gateway as a Bridge on page 72
		Bridge IMPVHA		

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
		Reverse Proxy Apache		Configuring Apache Reverse Proxy on page 109
		Reverse Proxy Kernel		Configuring Kernel Reverse Proxy "Configuring a Kernel Reverse Proxy" on page 180
	Manage hardware security modules (HSM)	enable nCipher HSM		Hardware Security Modules (HSM) on page 385
		enable SafeNet HSM		
	Manage remote agents	Add a legacy (pre 7.0) agent		Managing Remote Agents "Managing SecureSphere Agents" on page 79
		Modify a legacy (pre 7.0) agent		
		Delete a legacy (pre 7.0) agent		
		Add agent listener		
		Delete agent listener		
		Add z/OS agent listener(s)		
		Delete z/OS agent listener		
		Manage remote agent routes		
Manage SecureSphere Gateway *(continued)*	Manage interfaces and routes *(for a bridge)*	Create bridge		Configuring a Gateway as a Bridge on page 72
		Delete bridge		
		Toggle STP on a bridge		
		Toggle High Availability on a Bridge		
	Manage interfaces and routes *(for a sniffing gateway)*	Set sniffing interface(s)		Configuring a Gateway as a Sniffing Gateway on page 74
		Set blocking interface		

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
		Add/modify blocking mask		
		Delete blocking mask		
	Manage interfaces and routes *(for an Apache Reverse Proxy)*	Add alias		Configuring Apache Reverse Proxy on page 109
		Modify Alias		
		Delete Alias		
		Enable high availability		
		Manage reverse proxy (kernel) routes		
	Change Cluster Configuration	Add/Modify Cluster Configuration		SecureSphere Database Security User Guide
		Delete Cluster		
		Change IPv4 address		
		Change Device		
		Change Port		
Manage SecureSphere DAS	Deactivate server			Configuring a Data Assessment Server (DAS) on page 85
	Restart server (I)			
	Stop server (I)			
	Change management password			
	Change database password			
	Deactivate server			
Manage platform	Manage network	Management interface	Change device	Management Interface on page 93
			Change IP address	
			Change netmask	
			Locate device **(I)**	
		LAN interface	Change device	LAN Interface on page 94
			Change IP address	
			Change netmask	
			Locate device **(I)**	

Top Screen Menu	Level 1 menu	Level 2 menu	Level 3 menu	For more information, see
		Default gateway		Default Gateway on page 96
		Static routes	Add route	Static Routes on page 96
			Delete route	
		Name Resolution (DNS client)	Enable DNS client	Name Resolution (DNS client) on page 97
			Set domain	
			Set search list	
			Set name servers	
		Locate network devices		Locate Network Devices on page 98
	Manage time	Add time server		Time Servers on page 100
		Delete time server		
	Manage users			Users Management on page 100
	Manage hostname			Hostname Management on page 105
	Manage bootloader password			Bootloader Password Management on page 106
	Reboot the appliance **(I)**			Configuring the Platform on page 89
	Shutdown the appliance **(I)**			Configuring the Platform on page 89
Upgrade / updates				This option is reserved for future use.

impctl

`impctl` is a lower level configuration tool that runs on the appliances. `impcfg` runs `impctl` on the appliance to deploy the configuration that the administrator defines in `impcfg`.



Warning: `impctl` is for highly experienced administrators only. Inexperienced users can seriously damage the appliance's configuration, requiring reinstallation from scratch, and they should therefore use `impcfg` instead

"Safe" impctl Commands

The table below lists the commonly used "safe" `impctl` commands.

impctl - Selected "Safe" Functionality

impctl command	Description
`impctl show commands --verbose`	List `impctl` commands and their arguments.
`impctl status`	Display the status of the appliance.
`impctl server start`	Start the MX server.
`impctl server stop`	Stop the MX server.
`impctl server restart`	Stop and then start the MX server.
`impctl server ha password --set-database-password=NEW_SYSTEM_PASS --set-server-password=NEW_SECURE_PASS`	Change system (database) and/or secure (system) password on HA-MX server. For more information about SecureSphere users and passwords, see The Different SecureSphere Users on page 54.
`impctl gateway start`	Start the Gateway.
`impctl gateway stop`	Stop the Gateway.
`impctl gateway restart`	Stop and then start the Gateway.
`impctl gateway register`	Register the Gateway to its MX server.
`impctl gateway unregister`	Unregister the Gateway from its MX server.
`impctl gateway config --encryption=yes`	Encrypt database audit files stored on the Gateway.
`impctl hardening config --root-source-ip-exception=<IP address>`	Specify an IP address from which user root is allowed to login over SSH.

Stopping and Starting the MX in an MX-HA Environment

The correct way start and stop the MX in an MX-HA environment is by using the following commands:

```
impctl server ha start
impctl server ha stop
```



Warning: Do not use `impcfg` or `impctl` to start and stop the MX as you would in a non-MX-HA environment (as described in Configuring a Management Server on page 67). Use only the above commands.

Miscellaneous impctl Commands

Disk Maintenance

Use the following command on MX appliances with mirrored disks to determine if a disk has failed.

```
impctl platform storage raid adaptec arcconf getconfig 1
```

The status of the appliance's disk drives is displayed.

Below is an example of a portion of the command's output. Note that in this example, "Device 0" has failed (its State is given as "Failed").

```
-------------------------------------------------------------------------
Physical Device information
-------------------------------------------------------------------------
      Device #0
         Device is a Hard drive
         State                          : Failed
         Supported                      : Yes
         Transfer Speed                 : Failed
         Reported Channel,Device        : 0,0
         Reported Location              : Connector 0, Device 0
         Vendor                         : WDC
         Model                          : WD1002FBYS-02A6B
         Firmware                       : 03.00C06
         Serial number                  : WD-WMATV1847734
         Size                           : 0 MB
         Write Cache                    : Unknown
         FRU                            : None
         S.M.A.R.T.                     : No
      Device #1
         Device is a Hard drive
         State                          : Online
         Supported                      : Yes
         Transfer Speed                 : SATA 3.0 Gb/s
         Reported Channel,Device        : 0,1
         Reported Location              : Connector 0, Device 1
         Vendor                         : WDC
         Model                          : WD1002FBYS-02A6B
         Firmware                       : 03.00C06
         Serial number                  : WD-WMATV1847454
         Size                           : 953869 MB
         Write Cache                    : Enabled (write-back)
         FRU                            : None
         S.M.A.R.T.                     : No
```

To determine which disk is "Device 1", use the following command:

```
impctl platform storage raid adaptec arcconf IDENTIFY 1 DEVICE 0 1
```

To determine which disk is "Device 0", use the following command:

```
impctl platform storage raid adaptec arcconf IDENTIFY 1 DEVICE 0 0
```

If this command is successful, the LED of the device lights up. If the device has failed, the command may not succeed, that is, the LED may not light up, depending on the nature of the failure.

Miscellaneous Commands

Powering Down the Appliance



Note: This section relates only to the NG (X series and M series) appliances.

Both of the following OS commands power down the appliance:

- `poweroff`
- `shutdown -P now`

After using either of these commands to power down the appliance, you must remove the power cord and re-insert it before powering up the appliance again.

For appliances with only one power supply, you can alternatively wait two minutes before powering up the appliance again.



Warning: These commands are the only correct, supported ways to power down the appliance.

Changing the Password for Management Server - Gateway Communication

Communication between a Management Server and its Gateways (including Gateway registration to the Management Server) is secured by a password. The default password is "secure".

To change the Password for Management Server - Gateway Communication:

1. Open a browser and go to the Gateway's port 443 using HTTPS, for example:
   `https://10.1.1.10:443/`
2. Enter the user "`imperva`" and the current password.
   The default password is "`secure`".
3. From the menu, click **Change the Gateway's login password**.
4. In the **Change SecureSphere Gateway login password** screen, enter the following information:
   - **Old password**
   - **New password**
   - **Confirm new password**
5. Click **Submit**.

APPENDIX D

FIPS 140 Compliance

This chapter describes SecureSphere FIPS (Federal Information Processing Standard) 140-2 compliance, and includes:

2.1 Encrypted Communications 431
2.2 MX Encrypted Communications 431
2.3 SecureSphere Gateway and Platform Communications 433
2.4 HSM solution 433
2.5 SecureSphere WAF in FIPS Mode 433
Limitations 433
Activating FIPS Mode 434

2.1 Encrypted Communications

SecureSphere uses FIPS-certified encryption modules to perform cryptographic operations within the cryptographic boundary. The cryptographic modules used by SecureSphere are compiled and operated in FIPS mode and perform the appropriate self tests at initialization.

2.2 MX Encrypted Communications

SecureSphere's Management Server operates under Java JRE version 1.6. As part of its operation it performs cryptographic operations such as archiving, communications to clients, and communications with the Gateways it manages. All of these operations are performed by the RSA Crypto-J version 4.0 FIPS package which is certified at FIPS level 1.

The NIST certificate number is 1048 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#1048 http://www.).

2.2.1 FIPS-Approved Algorithms

The following algorithms are applied when using Crypto-J in FIPS mode:

- AES (Cert. #669)
- DSA (Cert. #251)
- ECDSA (Cert. #72)
- HMAC (Cert. #353);
- RNG (Cert. #389 and vendor affirmed: SP 800-90)
- RSA (Cert. #311)
- SHS (Cert. #702)
- Triple-DES (Cert. #614)

2.2.2 FIPS-Non-Approved Algorithms

The following algorithms are **not** approved when using Crypto-J in FIPS mode:

- AES-GCM (non-compliant)
- DES
- Diffie-Hellman
- DESX
- ECAES
- EC Diffie-Hellman
- ECIES
- RNG (X9.31 non-compliant, MD5 and SHA1)
- RC5
- RSA OAEP (for key transport)
- RSA Keypair Generation MultiPrime
- RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength);
- HMAC-MD5
- Raw RSA
- RC4
- RC2
- ECDHC
- MD2
- MD5
- PBE (SHA1 and Triple-DES)
- RIPEMD 160

2.3 SecureSphere Gateway and Platform Communications

SecureSphere Gateway and platform communications are accomplished using OpenSSL version FIPS 1.1.2. This OpenSSL version is used for all incoming and outgoing connections related to the SecureSphere daemon.

OpenSSL FIPS 1.1.2 is FIPS-certified with overall level 1 with certificate number 918 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt918.pdf http://www.).

2.3.1 FIPS-Approved Algorithms

The following algorithms are applied when using OpenSSL in FIPS mode:

- Triple-DES (Cert. #613)
- AES (Cert. #668)
- SHS (Cert. #701)
- HMAC (Cert. #352)
- RSA (Cert. #310)
- RNG (Cert. #387)

2.3.2 FIPS-Non-Approved Algorithms

The following algorithms are **not** approved when using OpenSSL in FIPS mode:

- DES
- Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength);
- RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength);
- DSA (Cert. #250; non-compliant)

2.4 HSM solution

SecureSphere can be integrated with nCipher's netHSM which is FIPS level 2 (or 3, depending on configuration) certified, which provides FIPS-certified key storage solutions. For more information, see Imperva's support site for solution number 903.

2.5 SecureSphere WAF in FIPS Mode

In order to decrypt web traffic in FIPS mode, SecureSphere uses the FIPS-certified NSS cryptographic module. The module is both level 1 and 2 certified. SecureSphere uses it in level 1 with NIST certificate #815 (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2007.htm#815 http://www.).

In order to decrypt in FIPS mode you need to configure the server group address to be the internal address of the web server and decrypt the traffic using SecureSphere reverse proxy Apache mode, while keeping the server side traffic clear (or vice versa).

Limitations

The following features are **not** supported in FIPS mode:

- Assessment – all tests that are categorized as "OS Level"
- Assessment – all tests that are categorized as "Track Changes"
- Action Sets – Archive to SCP Location Action Interface
- Web KRP (Kernel Reverse Proxy) when the KRP encrypts/decrypts data
- Web TRP (Transparent Kernel Reverse Proxy) when the TRP encrypts/decrypts data
- RSA keys shorter than 1024 bits

Activating FIPS Mode

To activate FIPS mode:

1. In the **Admin** workspace, click **System Definitions**.
2. In the **System Definitions** pane, select **FIPS Settings**.
3. Enable **FIPS Mode**.
4. Click **Save**.

   If you are in delayed activation mode, you need to activate this settings. For further information, see the **SecureSphere User Guide**.

APPENDIX E

Disaster Recovery

This appendix details disaster recovery procedures for the SecureSphere Management Server.



Note: The features described in this appendix are available in SecureSphere versions 7.5 Patch 6 and later.

Disaster Recovery 435

Disaster Recovery

In the event that a Management Server becomes unusable, it is possible to transfer its data to another machine on which the SecureSphere Management Server has been installed.

For information on exporting and importing Management Server data, see Exporting and Importing the Management Server on page 229.

Preparing for Disaster Recovery

To prepare for disaster recovery:

1. Prepare a standby server in another location.
2. On the active Management Server, install two licenses, one for the active server and one for the standby server.
   For information on installing licenses, see Licenses on page 189.

3. Whenever you upgrade the active Management Server to a new version of SecureSphere, upgrade the standby server to the same version.
4. On a scheduled basis, export the Management Server data and store the exported data off-site.



Note: The exported data include SSL keys and licenses.

Recovery

To configure the standby Management Server:

1. Confirm that the standby Management Server is running the same version of SecureSphere (including patches) that was running on the primary Management Server.
2. Import the exported data to the standby Management Server.
3. Re-register the SecureSphere Gateways to the standby Management Server (see Configuring a Gateway on page 68) by running the script in the next section (Automatically Re-registering the Gateways on page 436).



Note: The secondary Management Server must be up and running when you perform this step.

Automatically Re-registering the Gateways

You can simplify the Gateway registration process by automatically re-registering the Gateways to the Management Server.

To automatically re-register the Gateways:

1. On the Management Server, execute the following command:

```
impctl force-remote-registration --mx-ip=10.1.5.117
--mx-password='secure12'
[--gateway-password='different_password']
```

force-remote-registration Parameters

Parameter	Description
`--mx-ip`	The IP address of the standby Management Server.
`--mx-password`	The secure user password for the Gateway. For more information, see SecureSphere Users on page 54.
`--gateway-password`	**Optional** : The password for Gateway-MX SSL. If this parameter is not specified, then the default password is used. If the password is not the same for all Gateways or is not correct, you will prompted for each password.

The first two parameters are required.

Error messages are output to the Management Server's `impctl` log and to `stderr`.

If one Gateway cannot be registered, the script will continue to try to register the other Gateways.

You can also see the registration in the Gateway's log by executing the following command on the Gateway:

```
impctl show log --verbose
```

The `--verbose` parameter adds the date and time to each output line.

APPENDIX F

PCI Compliance

This appendix describes PCI compliance, and includes:

PCI Data Security Standard 438
PCI Compliance 439

PCI Data Security Standard

PCI DSS requirements apply to all system components that are included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including network components, servers and applications.

- Network components may include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types may include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- Applications may include but not limited to all purchased and custom applications, including internal and external (Internet) applications.

SecureSphere and PCI DSS

SecureSphere can assist administrators in achieving PCI compliance for their systems by tracking, monitoring and, if necessary, blocking access to cardholder data. At the same time, SecureSphere Management Servers, Gateways and SecureSphere Agents are considered network components in the cardholder data environment, and are thus themselves subject to the PCI DSS.

The requirements relevant to SecureSphere fall into the following areas:

- Protecting the SecureSphere appliance itself, for example, through the use of firewalls. For more information, see Protecting the SecureSphere Appliance on page 439.
- Protecting cardholder data stored by SecureSphere or in transit between protected systems and the SecureSphere appliance. For more information, see Protecting Cardholder Data on page 439.

PCI Compliance

This section reviews the following topics:

Protecting the SecureSphere Appliance 439
Protecting Cardholder Data 439

Protecting the SecureSphere Appliance

The default SecureSphere configuration provides protection for the SecureSphere appliance as follows:

1. Root and secure user access (see SecureSphere Users on page 54) to the appliance OS is available only locally, and not over SSH. SSH access to the appliance OS is available only for users other than `root` and `secure` (see CLI Users on page 55), and these users can execute only a limited set of OS commands.
2. Passwords for all SecureSphere administrators and users must be at least 7 characters long, and contain at least 1 alphabetic and at least 1 numeric character, in conformance with PCI requirements.
3. The default SecureSphere administrator is required to change his password logging in to SecureSphere for the first time.
4. All SecureSphere administrators and users must change their passwords at least once every 90 days (configurable in **Admin** > **System Definitions** > **Security and Authentication** > **Password Settings**). The new password cannot be the same as any of the previous four passwords.
5. All SecureSphere administrators and users are locked out after 3 consecutive failed authentication attempts.
6. GUI and CLI sessions are terminated automatically after 15 minutes of inactivity.
7. SecureSphere log files are accessible only by authorized administrators.
8. SecureSphere logs all administrator access (logins) to SecureSphere appliances and to the SecureSphere GUI.
9. SecureSphere uses SSH to secure administrative access to the SecureSphere Management Server, and SSL/TLS to secure connections between the SecureSphere Management Server and SecureSphere Gateways.

In addition, administrators should restrict the physical access to the SecureSphere appliance to authorized personnel only.

Protecting Cardholder Data

To protect cardholder data, the SecureSphere administrator should configure SecureSphere as follows:

1. Configure the SecureSphere Gateway to mask cardholder data before storing audit data locally. The audit data transmitted to the SecureSphere Management Server to be stored there will then be in masked form.

   For information on masking sensitive data, see the "Configuring Data Masking Options" section in Chapter 2 of **SecureSphere User Guide**.
2. Encrypt audit data stored on the SecureSphere Gateway, which remain encrypted when transmitted from the Gateway to the Management Server and stored there.

   For information on how to configure this option, see the "Configuring Encryption" section in the Maintenance chapter of the **SecureSphere Administration Guide**.
3. Encrypt audit archives. For information on encrypting archives, see the "Managing Archive and Key Settings" section in the "Advanced SecureSphere Configuration" chapter of the **SecureSphere User Guide**.

4. Encrypt the data channel between the SecureSphere Gateway and the SecureSphere SecureSphere Agents installed on the database server, so that data transmitted over this channel (which will be masked only on the Gateway) are not exposed.

   In `impcfg`, configure the SecureSphere Agent data channel to use SSL. For more information, see the "Managing SecureSphere Agents" section in the "Configuring SecureSphere" chapter of the **SecureSphere Administration Guide**.

Index

2

2.1 Encrypted Communications • 433

2.2 MX Encrypted Communications • 433

2.2.1 FIPS-Approved Algorithms • 434

2.2.2 FIPS-Non-Approved Algorithms • 434

2.3 SecureSphere Gateway and Platform Communications • 435

2.3.1 FIPS-Approved Algorithms • 435

2.3.2 FIPS-Non-Approved Algorithms • 435

2.4 HSM solution • 435

2.5 SecureSphere WAF in FIPS Mode • 435

A

Aborting a Job • 217, 219

Accessing the Product Customization Facility • 313, 331

Action Interfaces • 204, 270

Activating FIPS Mode • 436

Activating Settings Manually • 151

ADC • 20, 22, 212

ADC History • 215

Add the HBA to the SecureSphere Appliance • 400, 402

Adding a Legacy (pre-version 7.0) SecureSphere Agent • 81

Adding a SecureSphere Agent for DB2 z/OS Listener • 81, 83, 306, 309, 316, 318, 324, 326, 327, 335, 337

Adding a SecureSphere Agent Listener • 81, 82

Adding and Removing Permissions • 196

Add-Ons • 21, 386

admin-ips • 366

Advanced Agent Configuration • 161

After Installing Management Server High Availability (MX-HA) • 366

After Installing the SecureSphere Agent • 139

After Uninstalling a Pre-version 9.0 SecureSphere Agent • 145

After Uninstalling a Version 9.0 or Higher SecureSphere Agent • 145

After Uninstalling the SecureSphere Agent on a non-Windows System • 145

Agent Information Displayed in the Console • 151

Agent Troubleshooting Using the Management Console • 151

Agents • 273

AIX • 145

AIX Post Installation Information • 139

Alert Aggregation Configuration • 273

alert_secsph.log • 372

Aliases • 180, 187

Analyzing Converted Files • 246

ANMS (RADIUS Settings) • 416

Apache and Kernel Reverse Proxy on the Same Gateway • 24, 30, 111

Apache Reverse Proxy (ARP) • 24, 30

APF Authorizing the LOAD Library • 311, 329

Appliance OS • 55

Application Groups Settings • 274

Assessment Results Archive • 225

Assessments • 274

Assigning Roles to Users • 197, 200

Associating a User-defined Keyword with a Report • 289, 291

Assumptions • 395

At the Network Level • 343, 347, 348

At the SecureSphere Level • 344, 347, 349

Audit Archive Conversion • 244

Audit Fast Viewing • 223, 225

Audit Purge • 224

Audit Settings • 263

Authentication and Authorization Configuration • 92, 98, 200, 266, 277, 284, 285

Authentication Failure • 56

Authorizing the Started Task for the Product • 320, 339
Automatically Re-registering the Gateways • 438
Automating First Time Login • 47
Automating the Registration of an Agent • 120

B

Basic netHSM Configuration • 396, 397
Before Installing and Configuring SecureSphere Agent for z/OS • 306, 324
Before Installing Management Server High Availability (MX-HA) • 356
Before You Begin
    Checking OS Layer Serial Console Access • 384
Binding Packages for the Product • 319, 338
Bootloader Password Management • 66, 90, 106, 428
Bridge Deployments • 25
Bridge STP • 344, 345
Bridge STP — Active-Active Failover • 347
Bridge STP — Active-Passive Failover • 346

C

Cabling • 399
Change Root User Password • 101, 102
Changing Database and/or System Passwords • 368
Changing MX Properties in an MX-HA Environment • 58
Changing the Audit Directory Path • 221
Changing the Gateway's Mode to ARP • 109
Changing the MX of a Gateway • 112
Changing the Password for Management Server - Gateway Communication • 432
Check the HBA Card • 400, 402
Choosing a Deployment • 23
CIDR Notation • 51, 58, 70
CLI Users • 47, 55, 359, 360, 441
Command Line Interface • 21, 58, 424
Command Line Scripting Language • 166
Command Line Tools and MX-HA • 58, 354
Common Arguments • 50
Completing the Configuration • 319, 338
Components Taking Part in the Integration • 394
Configure RADIUS Authentication • 101, 102, 104
Configure SecureSphere to Use the SAN • 401, 408
Configure SSH Trust for User Oracle • 360
Configure SSH Trust for User Root • 359
Configure the Interconnected Interfaces • 357
Configuring a Data Assessment Server (DAS) • 61, 65, 85, 427
Configuring a Gateway • 45, 55, 57, 58, 61, 63, 68, 72, 73, 74, 76, 80, 109, 177, 425, 438
Configuring a Gateway as a Bridge • 63, 64, 70, 72, 74, 109, 345, 425, 426
Configuring a Gateway as a Sniffing Gateway • 63, 64, 70, 74, 425, 426
Configuring a Gateway for a Cluster • 71, 75
Configuring a Gateway for a Cluster - Gateway Already Registered • 77
Configuring a Gateway for a Cluster as Part of First Time Login • 70, 75
Configuring a Gateway Registered in a Cluster • 78
Configuring a Kernel Reverse Proxy • 70, 71, 107, 180, 426
Configuring a Management Server • 55, 59, 61, 62, 67, 425, 430
Configuring a Route • 185
Configuring a Virtual Router • 183, 186
Configuring Aliases • 181, 349
Configuring an Alias • 109, 184, 186
Configuring Apache Reverse Proxy • 63, 64, 70, 107, 109, 111, 426, 427
Configuring Archiving per Gateway • 173, 175
Configuring ARP • 109
Configuring BIOS Settings for Serial Console • 384

Configuring Encryption • 221
Configuring Firefox for Kerberos Authentication • 280
Configuring Firewall Ports • 35, 57, 380
Configuring Gateways and Gateway Groups • 170, 171
Configuring Kernel Reverse Proxy • 63, 107, 109, 111
Configuring Kernel Reverse Proxy and Apache Reverse Proxy on the Same Gateway • 31, 109, 111
Configuring Listeners • 45, 122, 152
Configuring Navigation Permissions • 197, 202
Configuring Network High Availability • 378
Configuring Object or Category Level Permissions • 197, 200, 201
Configuring SecureSphere • 20, 24, 46, 345, 347, 350
Configuring SecureSphere Agent Agent for z/OS Tasks • 305, 306
Configuring SecureSphere Agent for z/OS (on z/OS) • 313, 331
Configuring SecureSphere Agent for z/OS Tasks • 324
Configuring SecureSphere Agent Routes • 107
Configuring SecureSphere for Automatic Kerberos Authentication • 279, 280, 281
Configuring SecureSphere for SAN • 400
Configuring SecureSphere Routes • 107
Configuring SecureSphere Using the Command Line Tools • 57, 58
Configuring the Authorization to Activate Settings • 203
Configuring the Browser for Kerberos Authentication • 279, 280
Configuring the Gateways to Operate in the HA Mode with Agents • 152
Configuring the Management Server for High Availability • 109
Configuring the Platform • 55, 62, 66, 89, 91, 99, 101, 106, 428
Configuring the SecureSphere Agent to Operate in the HA Mode • 152, 154
Configuring the SecureSphere Gateway Before Installation • 116, 122, 153
Configuring Traffic Distribution Analysis • 264
Configuring Transparent Reverse Proxy • 28, 108
Configuring User Information • 197, 205, 284, 285
Configuring Windows Internet Explorer (IE) for Kerberos Authentication • 280
Confirming that MX-HA is Correctly Configured • 370
Confirming That the MX-HA Servers are Synchronized • 370, 371
Connected Users • 210
Connecting to a X or M Series Appliance Using a Serial Console • 39
Connecting to the G Series Appliance Using a Serial Console • 35, 37, 43
Connecting to the G2 or G2-2 Appliance Using a Serial Console • 36, 38, 39
Connecting to the LOM • 410
Connecting to the Management Server • 41
Conventions for Command Line Scripting • 166
Converting an MPRV file to TAR Format with CSV Values • 245
Copyright Notice • 2
CPU Affinity • 24
Create a File System on the SCSI Target • 400, 406
Create a Startup File • 400, 406
Create New User • 101, 102, 104
Creating a Bootable USB Device Containing the Installation Image • 40
Creating a Role • 199, 201
Creating a SecureSphere User • 196, 197, 200, 205, 284, 285
Creating and Configuring Action Interfaces • 272
Creating the ADMIN Library • 312, 330
CSV Upload Default Settings • 274

Custom Role Examples • 198
Customization • 414, 419

D

Data Format • 246
Data Interface Discovery and Configuration • 139
Data Owner Settings • 275
Date Changes • 57
Default Gateway • 65, 92, 96, 428
Defining a New Keyword • 289, 290
Defining a Required Login String for Web Browser Access • 415
Defining an IP Address for the Gateway for VRRP • 181
Defining External Systems • 277, 278
Defining Log Collectors • 291
Deleting a Keyword • 289, 291
Deleting a Legacy (pre-version 7.0) SecureSphere Agent • 81, 82
Deleting a SecureSphere Agent for DB2 z/OS Listener • 81, 84
Deleting a SecureSphere Agent Listener • 81, 83
Detailed Information About the Customization Parameters • 317, 335
Determine Storage Requirements • 400, 401
Determining the Remaining Tasks to Complete for the Started Task • 320, 339
Diagnostic Tools • 155
Disabling the SAN • 409
Disaster Recovery • 21, 437
Discovery Results Archive • 227
Disk Maintenance • 430
Display Limits • 296
Displaying the Jobs Status Window • 218
Document Conventions • 22
Download the RPMs and Prepare the Servers • 357
Downloading and Installing SecureSphere Agent for z/OS • 306, 310, 324, 328
Downloading and Installing the Product • 310, 328
Dynamic Profiling • 252

E

Edit External Authentication Configuration • 101, 104, 105
Editing a Job • 217, 218
Editing the GRUB Configuration File • 382, 384
Enable / Disable RADIUS • 104, 105
Enabling Automatic Creation of a Service for a Discovered Data Interface • 121
Enabling Registration of an Agent with a Non-Existent Server Group • 120, 136, 142, 143
Encryption (SSL) • 111
End User License and Services Agreement • 3
Example 1 (Index Only) • 248
Example 2 (Index + Events) • 249
Example 3 (Index + Events + Responses) • 250
Exceptions • 53
Export / Import Manually Using the Interactive CLI • 232
Export / Import Manually Using the Non-Interactive CLI • 233
Export Using the SecureSphere GUI • 230
Exporting an Archive to TAR Format with CSV Values • 244
Exporting and Importing the Management Server • 229, 437
Exporting Technical Information from Gateway and Onebox • 172, 188, 300
Exporting Technical Information from Management Servers • 188, 300
External HTTP Settings • 214, 276
External System - LDAP Authentication and Authorization • 278, 282
External System - RADIUS Authentication • 278, 285
External System - SQL • 278, 286
External System - SSH Proxy • 278, 286
External Systems • 50, 53, 266, 277

External Systems - Active Directory Collection (Forest) • 278
External Systems - Kerberos Authentication • 278, 279
External Systems - LDAP • 278, 282
Extracting Archives for Viewing • 226, 228, 237, 240, 243

F

Fail Open — Configuration • 350
Fail Safe and Fail Open Modes • 26
Fail-Open Bridge • 349, 350
Failover Sequence • 373
Failure While Building the Standby Database • 374
Features Available in the Each Deployment Mode • 32
File Explorer Maintenance • 236
File List • 374
File URM • 289
FIPS 140 Compliance • 21, 433
FIPS Settings • 267
Firmware • 420
First-Time Configuration Wizard • 140
First-Time Login (Configuration) • 57
Forward Compatibility • 34
From a Gateway to a Onebox • 112
From a Onebox to a Gateway • 112

G

G Series Appliances (Except G2 and G2-2) • 35
G2 and G2-2 Appliances • 37
Gateway Actions • 71
Gateway Details • 172
Gateway Groups • 176, 300
Gateway High Availability • 20, 24, 29, 73, 343, 377
Gateway Settings • 262
Gateway/Management Server Appliance Initial Configuration • 57
Gateways • 20, 170
Gateways and Agents • 300, 303
General • 412
General Optional Arguments • 49
General ThreatRadar Settings • 297
Granting DB2 Privileges • 320, 339
Granting Masking/Unmasking Capability to SecureSphere Roles and Users • 204

H

HA Health Check • 355
Hardware • 382
Hardware and Software Requirements • 356
Hardware Security Modules (HSM) • 70, 386, 426
Heartbeat Behavior • 373
Heartbeat Statuses • 372
High Level Functional Description • 394
High Level Installation Process • 394, 396
Host Bus Adapters • 399
Hostname Management • 66, 90, 105, 428
Hostnames • 52

I

If the MAC Address Changes • 156
impcfg • 59, 424
impcfg Functionality Map • 62, 424
impctl • 428
impctl server ha status Command • 369
impctl server ha status Output • 369
impctl watchdog • 373
Imperva Watchdog • 355
Importing Keys • 391
Importing KRP Configuration From a CSV File • 183, 184, 186
IMPVHA — Configuration • 345
IMPVHA Protocol — Active-Passive and Active-Active Failover • 344
Including the Product Libraries in Your Disaster Recovery Plan • 312, 330
Information You Must Have Before You Begin • 307, 324
Initial Configuration • 35, 47, 75
Initializing and Securing the Rules Data Set • 321, 340

Initiating a Failover in an MX-HA Environment • 370
Inline Gateways • 25
Install the Latest Patch • 357
Installation Monitoring for G Series • 35
Installation Monitoring for G2 and G2-2 Appliances • 37
Installing a New SecureSphere Agent as part of Software Update • 114
Installing G Series Appliances From USB • 35
Installing G2 and G2-2 Appliances from USB • 38
Installing Management Server High Availability (MX-HA) • 362
Installing SecureSphere Agent for z/OS • 20, 305
Installing SecureSphere Agent for z/OS - Version 2.1 • 323
Installing SecureSphere Agent for z/OS - Version 3.1 • 305
Installing SecureSphere Agents • 20, 113
Installing the nCipher Card • 387
Installing the nCipher Card Driver • 387
Installing the nfast Software Package • 396
Installing the SecureSphere Agent • 117
Installing the SecureSphere Agent and Installation Manager • 116, 124
Installing the SecureSphere Agent and Installation Manager on a non-Windows System • 124, 130
Installing the SecureSphere Agent and Installation Manager on a Windows System • 131, 132, 134
Installing the SecureSphere Agent Installation Manager on a Windows System Using the Standard Script • 131, 134
Installing the SecureSphere Agent on a Non-Windows System Using the Standard Script • 125, 126
Installing the SecureSphere Agent on a Windows System Using the Standard Script • 131, 132
Installing the SecureSphere Software • 35
Installing X and M Series Appliances From USB • 40
Intended Audience • 19
Introduction to the SecureSphere Administration Guide • 19, 20
IPv4 / IPv6 Dual Stack • 51
IPv6 • 50
IPV6 Address Formats • 51
IPv6 in impcfg and impctl • 52

J

Job Status • 20, 22, 216
Jobs Status • 217

K

Kerberos Key Update • 238
Kernel Reverse Proxy (• 30
Kernel Reverse Proxy (KRP) • 24, 29
Keywords Settings • 289, 290, 291
Known Issues • 374

L

LAN Interface • 65, 92, 94, 427
Language Settings • 297
Layer 2 High Availability Deployments • 343
Layer 3 (Proxy) High Availability Deployments • 347
Learning Exceptions • 253
License Overview • 189
Licenses • 20, 22, 189, 437
Limitations • 435
Link Aggregation (Etherchannel) • 344
Linux Heartbeat • 355
Listing the Contents of an Exported File • 235
Load Balancer Integration • 348
Locate Network Devices • 66, 92, 98, 428
Locking a User Account • 206, 269
Log • 422
Log Collector Parameters • 291, 292
Log Collectors • 291
Log Collectors Details in the Gateways Window • 174

Logout • 423
Logs in the /opt/securesphere/server-ha/log Directory • 372
LOM (Lights Out Management) • 410
Lookup Data • 293

M

Mainframe Software Requirements • 309, 326
Maintenance • 20, 22, 223
Maintenance Tasks • 155, 156
Make a Note of the Original SCSI Configuration • 400, 401, 405
Manage SecureSphere Agent Related Routes • 122, 123
Manage User • 56, 101, 103
Management Interface • 65, 92, 93, 427
Management Server • 298, 302
Management Server (MX) Replacement • 374
Management Server High Availability (MX-HA) • 20, 58, 68, 109, 353, 377
Management Server High Availability (MX-HA) Components • 354
Management Server Settings • 270
Management Server-High Availability(MX-HA) Implementation • 354
Management Service-High Availability(MX-HA) Overview • 353
Managing Database Scanning and Assessment Licenses • 192
Managing SecureSphere Agent Related Routes • 81, 85
Managing SecureSphere Agents • 64, 70, 79, 143, 426
Managing the LOM • 411
Mandatory Arguments • 48
Miscellaneous Audit Data Operations • 220
Miscellaneous Commands • 432
Miscellaneous impctl Commands • 430
Miscellaneous Maintenance Tasks • 236
Modifying a Legacy (pre-version 7.0) SecureSphere Agent • 82
Modifying the Started Task Procedure • 321, 340
Modifying the Started Task Procedure and Starting the Started Task • 322, 341
Monitoring Management Server High Availability (MX-HA) • 369
Monitoring MySQL Traffic • 165
Monitoring Solaris Zones Using SecureSphere Agents • 165
Mount the New File System • 400, 406
Mounting the Audit Archive Directory (NFS) • 175
MX-HA Components Writing to the Logs • 371
MX-HA Installation Failure • 374
MX-HA Logs • 371
MX-HA Status • 369
MySQL Users • 42, 287

N

Name Resolution (DNS client) • 65, 92, 97, 428
nCipher Card • 386, 387
nCipher HSM Installation • 395
nCipher netHSM • 386, 394
Network • 413
Network High Availability • 21, 377
Network High Availability Support • 377
Network Management • 90, 91, 93, 95, 96, 97, 98
Network Services • 21, 379
Non-Transparent Reverse Proxy Overview • 28
Notes on Permission Behavior • 196

O

Obtaining the Latest Version of the SecureSphere Agent • 117, 125, 131
On the Gateway • 409
On the Management Server • 409
Optimizing Performance • 309, 327
Optional Cluster Arguments • 49
Optional Listener Arguments • 49
Optional Sniffing Arguments • 50

Oracle Standby Database (Data Guard) • 355
Other High Availability Deployments • 349
Overview • 50, 112, 410

P

Password Settings • 207, 268
Passwords • 56
PCI Compliance • 21, 440, 441
PCI Data Security Standard • 440
Per-installation Checklist • 396
Permission Models in SecureSphere • 194
Permission Types • 195
Permissions Workflow • 197
Physically Connect to the SAN • 400, 404
Platforms and Installation • 20, 34
Policy Settings • 293
Power Management • 421
Powering Down the Appliance • 432
PreDefined Roles • 194, 198
Pre-Installation Tasks • 356, 362
Preparing for Disaster Recovery • 437
Preparing for Installation • 116, 117
Preparing the Appliance • 35
Preparing the Database • 116, 117, 120
Prerequisite for Downloading and Installing the Product or Cumulative Maintenance • 310, 328
Prerequisite Tests for non-Windows Agents • 118, 157
Procedure for Downloading and Installing the Cumulative Maintenance • 311, 329
Procedure for Downloading and Installing the Product • 310, 311, 328
Profile Optimization • 253
Profile Size Limits • 253
Protecting Cardholder Data • 441
Protecting the SecureSphere Appliance • 441

R

Read-Only User • 208
Reboot the Machine • 400, 408
Reconfiguring the DAS as a Onebox • 62, 88
Recovery • 438
Redundant Architecture (STP) — Configuration • 347
Redundant Architecture (VRRP) — Configuration • 349
Register the Gateway • 366
Registering a Gateway • 57
Registering the SecureSphere Agent and the SecureSphere Agent Installation Manager to a SecureSphere Gateway • 135, 136, 137, 141
Registering the SecureSphere Agent to the Gateway • 149, 151, 155, 162, 163
Relationship between Tables • 246, 248
Remote DB Connectivity • 287
Removing Cluster Configuration from a Gateway • 79
Replacing a Faulty Gateway • 43
Replacing a Faulty Gateway Using an Already-Configured Gateway • 44
Replacing Gateways • 43
Report Settings • 293
Reports Archive • 236
Request that the Storage Manager Add a Logical Volume • 400, 403
Requirements and Restrictions for Starting SecureSphere Agent for z/OS • 322, 341
Re-registration • 367
Resetting a User Password • 206
Resource Status • 372
Response Page Display in Alerts Settings • 263
Reverse Proxy Deployments • 23, 26
Reverse Proxy Mode Advantages • 27
Reverse Proxy Overview • 26
Reverse Proxy with Load Balancer • 24, 31
Risk Score Update • 238
Roles and Assignments for the Installation and Configuration • 307, 325
Roles and Users • 194
Routing • 180

S

Sample Queries • 246, 248
SAN Configuration Task Overview • 400
SAN Overview • 399
Scan the Fibre Channel • 400, 404
SecureSphere Agent Configuration Tasks • 116
SecureSphere Agent Details in the Gateways Window • 173
SecureSphere Agent Error Messages • 144, 151, 155
SecureSphere Agent Logs • 155
SecureSphere Agent Management Console • 116, 140, 141, 146, 148, 156, 167, 168
SecureSphere Agent Management Console Conventions • 148
SecureSphere Agents in a Hypervisor (Virtualized) Environment • 155, 156
SecureSphere and PCI DSS • 440
SecureSphere Component Communication • 379
SecureSphere Features Which Support IPv6 • 50
SecureSphere MX and Gateway • 52
SecureSphere Server • 355
SecureSphere Users • 54, 58, 68, 87, 438, 441
Security • 415
Security and Authentication • 266
Security Requirements • 309, 327
Security World Initialization • 389
Serial Console Access to SecureSphere • 381
Server Definitions • 294
Server Status • 372
Sessions • 20, 22, 210, 211
Set Up Hostnames • 358
Setting Up Predefined Drivers • 287, 288
Setting Up the Integration • 396
Setting up User Defined Driver • 287, 288
SharePoint • 117
Show Counters • 151, 155
Silent Registration Parameters • 133, 135
Silently Installing the SecureSphere Agent Installation Manager on a non-Windows System • 126, 128
Silently Installing the SecureSphere Agent on a non-Windows System • 125, 126
Silently Installing the SecureSphere Agent on a Windows System • 131, 132
Sniffing Gateway High Availability • 349, 350
Sniffing Mode • 24
Software • 382
Software Update Settings • 295
SOM-MX Issues for Read-Only Users • 209
Special Considerations for SUSE and OEL UEK Platforms • 119, 125, 126, 127, 130
Specifying the Customizable Parameters • 315, 332
Specifying the License Key • 306, 313, 324, 331
Specifying the Priority Using WLM • 321, 340
Specifying the Product Libraries • 314, 332
SSL Accelerator • 409
SSL Certificate Expiration Monitoring • 269
Standby Recreation • 373
Starting and Stopping the SecureSphere Agent • 144, 145, 146, 155
Starting and Stopping the SecureSphere Agent from the Management Console • 146
Starting the non-Windows SecureSphere Agent from the Command Line • 146
Starting the SecureSphere Agent Management Console • 149
Starting the Windows SecureSphere Agent from the Command Line • 147
Starting, Managing, and Stopping SecureSphere Agent for z/OS • 322, 341
Static Routes • 65, 92, 96, 107, 428
Stopping and Starting the MX in an MX-HA Environment • 59, 429
Stopping the non-Windows SecureSphere Agent from the Command Line • 147

Stopping the Windows SecureSphere Agent from the Command Line • 147
Storage Area Networks (SAN) • 398
Stored Procedures Settings • 295
Supported Components • 279
Supported Facilities • 310, 327
Supported Interfaces for the Gateway Listener • 123, 160
Supported SAN Hardware • 399
Supported Serial Console Settings • 382, 384
Supported Versions and Upgrades • 382
Switching Deployments • 112
Switching to Protect Mode Thresholds (SQL) • 257
Switching to Protect Mode Thresholds (Web) • 260
Syntax for Command Line Scripting • 167
System Definitions • 20, 22, 252
System Events Archive • 240
System Events Notifications • 295
System Performance • 20, 22, 298
System Performance - Agents • 304
System Performance - CPU Load • 303
System Performance - Policies • 304
System Performance - Signature and Dictionaries • 304
System Performance - SSL • 304

T

TCP/IP Requirements • 309, 327
Terminating the Integration • 397
Terminology Used In This Guide • 307, 325
Test the Interconnected Interfaces • 357
Test the New File System • 400, 406
The Admin Workspace • 21
The Different SecureSphere Users • 54, 429
ThreatRadar Settings • 297
Time Management • 90, 98, 100
Time Servers • 66, 99, 100, 428
Timeout • 56
Top Screen • 60
Topologies • 24, 25
Topologies and Deployment • 20, 23, 70, 73, 348
Transparent Reverse Proxy • 27
Transparent Reverse Proxy - Selected Web Servers • 24, 28
Transparent Reverse Proxy Overview • 27
Troubleshooting Performance • 302

U

Understanding How Permissions are Displayed • 201
Understanding Permissions • 193, 268
Understanding the Permissions Window • 195
Uninstalling MX-HA • 367
Uninstalling the SecureSphere Agent • 144
Uninstalling the SecureSphere Agent on a non-Windows System • 144
Uninstalling the SecureSphere Agent on a Windows System • 145
Update /etc/modprobe.conf • 400, 405
Update the Gateway HSM • 393
Update the Server with the Certificate Key • 393
Updating ADC Content • 214
Upgrades • 382
Upgrading from Previous Versions to Version 3.1 • 305
Upgrading the SecureSphere Agent • 113, 127, 129, 146
Uploading Licenses • 190
User Interface Settings • 296
User Lockout Settings • 206, 269
User Management • 417
Users and Permissions • 20, 22, 55, 193
Users Management • 66, 90, 100, 428
Using a Reset User Password • 206, 208
Using Operator Commands to Stop and Manage the Product • 322, 341
Using the Log to Analyze Jobs • 220

V

Verify the Primary Server is Active • 366

Verifying Prerequisites • 117, 118
Verifying Prerequisites for non-Windows Agents • 118
Verifying Prerequisites for Windows Agents • 118, 119
Verifying the Installation • 387, 390, 391
Viewing ADC Content and Status • 213
Viewing Licenses • 190
Virtual Routers • 186
Vulnerabilities Purge • 241

W

Web to Database User Tracking Settings • 264
What this Publication is About • 20
When Installing a SUSE or OEL UEK SecureSphere Agent • 130
When Starting a SUSE or OEL UEK SecureSphere Agent • 130
Working with a NATed Listener • 123, 161
Working with a NATed Listener in Non-Windows Environments • 162
Working with a NATed Listener in Windows Environments • 163
Working with DAC (Dedicated Administrator Connection) • 165
Working with Drivers • 287
Working with High Availability • 123, 124, 152
Working with Management Servers After the Installation • 35, 41
Working with Multiple Oracle Instances • 164
Working with Roles • 194, 197, 200, 208
Working with Users • 194, 199, 211

X

X and M Series Appliances • 39