Avaya Aura® 6.2 Feature Pack 4

System Manager Release 6.3.8 Security Guide

Release: 6.3.8
Issue: 0.2
June, 2014

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE

http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Contents

Avaya Aura® 6.2 Feature Pack 4 System Manager Release 6.3.8 Security Guide 1

Introduction 7

Product description 8

System Manager security overview 8

Responsibility for System Manager security 12

Software-only applications versus software-plus-hardware solutions 12

Responsibility for security updates 12

Complementing security guides of other Avaya products 12

Structure of this book 13

Platform security 14

Network layer security 17

System Manager firewall protection 19

HTTP/HTTPS DoS protection 20

Prevention of DoS Attacks 21

Protection against impact of viruses, worms, and other malicious code 21

File system security 22

Platform accounts 22

Web server security 23

Database security 24

Directory security 24

System integrity and monitoring 24

Application security 24

Application account and session management 24

Role-based Access Control 25

Application password or pin policy 29

Application session limits 30

Application-level authentication 30

Configuration for LDAP/AD 32
Backup and Restore 35
Backup 35
Restore 35
Audit trails and logs 36
Auditable events 37
Security-related events that are logged 37
Protection of audit records 38
Use of cryptography 38
Trust, Certificate, and Key Management or PKI 38
Updating Trusted Certificates of System Manager 39
Issuing a unique identity or server certificate to System Manager 41
Defining server trust relationships with Digital Certificates 42
System Manager to Avaya applications and servers 43
System Manager to third-party applications and servers 43
Default certificates and keys 43
Access to Avaya Services 44
Avaya Services Accounts, Authentication, and Authorization 44
References 45
Documents mentioned in this security guide 45
Security documents on the Avaya Support site 45
Appendix A: Avaya Security Advisories 46
Overview 46
Accessing Avaya Security Advisories 47
Interpreting an Avaya Security Advisory 48
Organization of an advisory 49
Overview 49
Avaya software-only products 49
Avaya system products 49
Recommended actions 49
Appendix B: Software and Firmware updates 51
Method that Avaya uses to delivers security updates 51

Validating a security update 52
Appendix C: Regulatory compliance 53
Considerations for customers who must comply with the Sarbanes-Oxley Act 53
Considerations for customers who must comply with the Graham-Leach-Bliley Act 54
Considerations for customers who must comply with CALEA 55
Considerations for customers who want to comply with ISO 17799 56
Considerations for customers who must comply with FISMA 57
Considerations for customers who must comply with HIPAA 58
Considerations for customers who must comply with PCI DSS 59
Considerations for non-US customers who must comply with regulations 60
Basel II 60
Common Criteria 60
Appendix D: DoS methods designed by Avaya 61
Appendix E: Product RPMs 64

Security design in System Manager 6.3.8

Introduction

This document provides an overview of security considerations, features, and solutions for System Manager Release 6.3.8. The goal is to equip Avaya partners, customers, and sales and system engineers with the information required to answer questions regarding data network and system security.

System security includes the security services that the platform offers and the security of the platform. This security guide describes the services that the platform offers to implement a secure solution. The guide also describes the security of the platform with regard to interception of the platform and the steps taken to harden the security-related settings of the platform.

This document describes the security services as well as the system security that is available in System Manager Release 6.3.8. This document does not discuss in detail the various security-related topics.

The reference section provides some sources of additional information. This document is also not the primary configuration guide for the various product security services. For detailed instructions, see the System Manager configuration manuals.

Information classifications and NDA requirements

This book provides security-related information according to the following information classifications:

Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Its unauthorized disclosure could have a severe adverse impact to Avaya or its customers, Business Partners, and/or suppliers.
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Its unauthorized disclosure could have significant adverse impact to Avaya or its customers, Business Partners, and/or suppliers. Information that some people would consider private is included in this classification.
Avaya Proprietary	This classification applies to all other information that does not clearly fit into the two classifications above and is considered sensitive only outside the Avaya. While disclosure might not have a serious adverse impact on Avaya or its customers, Business Partners, and/or suppliers, it is Avaya's information and unauthorized disclosure is against policy.
Public	This classification applies to information explicitly approved by Avaya management as non-sensitive information available for external release.

As this book is generally available, the information herein is considered public. While the book contains references to additional information sources, some sources disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

Disclaimer

Avaya has used reasonable commercial efforts to ensure that the information provided here under is accurate at this date. Avaya might change any underlying processes, architecture, product, description, or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the book, whether as a result of new information, future events, or otherwise. This document is provided "as is," and Avaya does not provide any warranty of any kind, express or implied.

Product description

Avaya Aura® System Manager provides centralized administration for multiple instances of Avaya Aura® Session Manager and Avaya Aura® Communication Manager today and is designed to manage all Avaya Aura® components in the future. Avaya Aura® System Manager provides a solution-level approach to network administration for IT departments to incorporate new components and applications under a common management umbrella over time, managing the elements of Avaya Aura® together as a system. Avaya Aura® System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing.

System Manager provides central administration of dial plans, network routing policy, and common user provisioning. Over time, Avaya Integrated Management features that have a centralized function will be migrated to Avaya Aura® System Manager, providing one place for managing users across all Avaya products as well as third-party applications that opt to leverage Avaya Aura® System Manager pluggable Service Oriented Architecture (SOA).

Using System Manager, IT and Telecom Operations of enterprises can manage the elements of Avaya Aura® as a system.

System Manager provides a common management framework that:

- Reduces complexity of operations for distributed multiple site networks with multiple control points inherent with SIP.
- Increases the value of convergence through integration with the enterprise IT infrastructure such as identity, security, Master Data, and ITIL processes.

System Manager security overview

This document describes the security-related considerations, features, and services for System Manager. As the Management Console for all Avaya products, System Manager must be resilient to attacks that might cause service disruption, malfunction, unauthorized access, or modification of data. System Manager as part of the Avaya Aura ® solution must be protected from security threats such as:

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks such as Cross-Site Scripting and Cross-Site Forgery.

System Manager has its own Authentication and Authorization (AA) framework, and all the requests to System Manager Services are routed through the AA framework. The AA framework prevents unauthenticated, unauthorized access to System Manager services and data.

The architecture is for the trusted communication framework infrastructure security layer and provides for the specification of trust relationships for:

- Administration
- Managed Elements

System Manager incorporates a hardened Linux operating system. This hardened operating system provides only the functions necessary to support the core applications, which is important for securing mission-critical call processing applications and protecting the customer from toll fraud and other malicious attacks.

The Linux operating system that Avaya has hardened limits the number of access ports, services, and executables. These limits protect the system from typical modes of attack. At the same time, the reduction of Linux functions reduces the attack surface which reduces the number of mandatory security patches needed.

The following figure shows the different interfaces through which you can gain access to System Manager. The direction of arrows depicts the direction in which the connection is initiated.

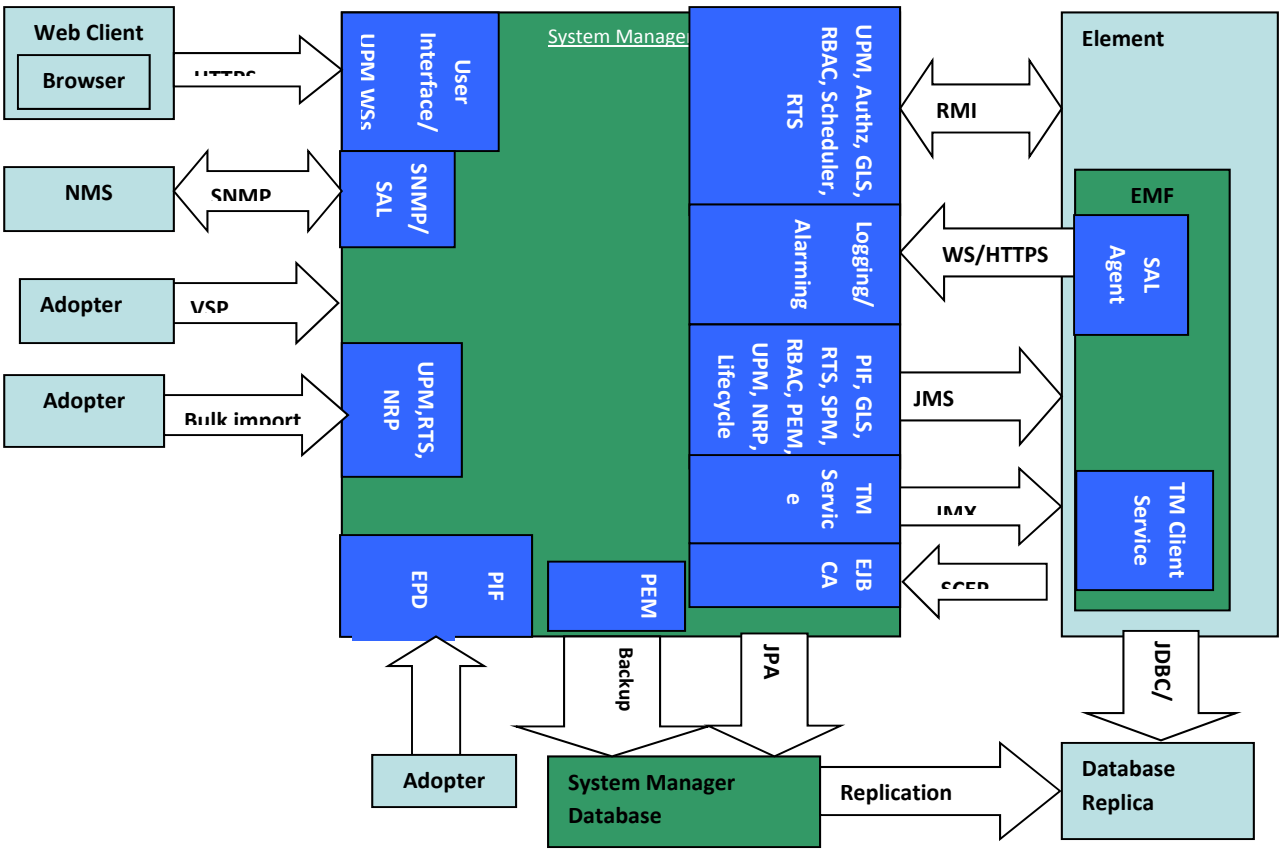


Figure 1 System Manager Software Interfaces

Terminology

NMS	Network Management System	SNMP	Simple Network Management Protocol
VSP	Virtual Service Provider	UPM	User Profile Management
RBAC	Role based Access control	SAL	Secure Access Link
RTS	Runtime Topology Service	NRP	Network Routing Policy Service
EPD	Extension Pack Definition. Used to define an extension point into which an extension pack can be plugged.	EJBCA	Enterprise JavaBeans Certification Authority
PEM	Panther Element Manager	GLS	Group and Lookup Service
Authz	Authorization	EMF	Element Management Framework
PIF	Plug-In Framework	NMS	
HTTPS	Hypertext Transfer Protocol Secure	Adopter	Product which integrates with System Manager
EP	Extension Pack	JPA	Java Persistence API
JDBC	Java Database Connectivity	WS	Web Service
SCEP	Simple Certificate Enrollment Protocol	SPM	Service Profile Management
TM	Trust Management		

The following table describes some of the interfaces provided by System Manager.

Interface	Description
HTTPS	Using the HTTPS interface, you can gain access to the System Manager user interface. System Manager secures this interface using SSL encryption, which enables encryption of data. Any attempts to gain access to port 80 or HTTP are automatically redirected to HTTPS.
SOAP/HTTPS	Using the SOAP/HTTPS (SOAP over HTTPS) interface, you can gain access to the System Manager secured Web Services. System Manager secures this interface using SSL authentication. The client accessing the Web Service must provide identity proof by performing a user name and password-based client authentication. System Manager uses this identity to authorize the client.
RMI	Using the RMI interface, elements can gain access to System Manager services such as EJBs. System Manager secures EJBs interface using Two-way (mutual) SSL authentication. Also, System Manager checks the identity of the user, a nonhuman identity, before providing access to the System Manager service.
Database Connections	All connections made by the System Manager services to database are secured using SSL authentication along with user name and password-based authentication. PostgreSQL Structured Query Language (pgsql) listens on the loopback interface for internal database connections, and database connections are also open for Secondary Server if Geographic redundancy is configured.
JMS	These JMS interfaces in System Manager are secured and require Two-way (mutual) SSL authentication to authenticate the element that is accessing the interface. System Manager also enforces a user name and password-based authentication in addition to the two-way SSL authentication of this interface. System Manager uses the authenticated identity to authorize the sender of the message.
SSH	You can gain access to the System Manager Command Line Interface (CLI) only through SSH. This interface is secured using a user name and password-based authentication. CLI sessions support Timeout. CLI administrative logging is done to the syslog files. System Manager also supports the Avaya Secure Gateway (ASG)-based authentication for certain system accounts used by Avaya Services.

Responsibility for System Manager security

Avaya is responsible for designing and testing Avaya-owned products for security. When Avaya sells a product as hardware or a software package, Avaya designs and tests the operating system and ensures that the operating system is up-to-date with security patches. In this case, Avaya might also modify the operating system, when necessary, for system operation or to resolve security vulnerability.

The customer is responsible for the appropriate security configurations on their data network. The customer is also responsible for using and configuring the security features available on System Manager. However, Avaya offers a service for assessing the customer network for performance as well as security issues. Avaya also offers configuration services for its products.

Software-only applications versus software-plus-hardware solutions

Avaya sells some communications applications as software-only products that must be installed on a customer-provided computer running an off-the-shelf operating system. For these products, the customer must ensure that the operating system and other third-party software are secure. Avaya sells other Avaya applications with Avaya-only hardware as well as software. For these applications, Avaya ensures that the operating system and any third-party software are secure. System Manager 6.3.8 is a software-plus-hardware solution.

Responsibility for security updates

When security-related applications or operating software updates become available, Avaya tests the updates, if applicable, before making them available to customers. In some cases, Avaya modifies the updated software before making updated software available to customers.

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to receive notification about Security Advisories by email. For more information, see What is an Avaya Security Advisory and How do I get Avaya Security Advisories?

When System Manager software security updates become available, the customer can install the updates or employ an installer from the customer services support group to install the updates. When Avaya installs the updates, the installer is responsible for following best security practices for server access, file transfers, and data backup and restore. For backups and restores of data, the customer is responsible for providing a secure backup and restore repository on the customer LAN.

Complementing security guides of other Avaya products

This document describes security-related issues and security features of System Manager. Avaya Aura® System Manager manages Avaya products that are part of the Avaya Aura® solution. This document complements the security guides that are available for all the managed elements in the Avaya Aura® solution. The security guides describe the potential security risks to Avaya products and the features that Avaya products offer to mitigate these security risks.

This document is a descriptive guide, not a procedural guide. Where appropriate, the guide references other product documentation for the actual procedures for configuring and using security features.

Some Avaya Security Guides available on the Support website are:

- Avaya Toll Fraud Security Guide
- Security Best Practices Checklist for Unified Communications Deployment
- Avaya and Vulnerability Scanning
- Mapping Common Vulnerability Exposure (CVE) numbers to Avaya Security Advisories (ASAs)

Structure of this book

Table 1 lists the sections and appendices contained in *Security Design for Avaya Aura® System Manager*.

Avaya Aura® System Manager Security guide

Chapter	Description
Introduction	Provides an introduction to the following topics: • Product System Manager Description • System Manager security philosophy overview • Avaya multilayer hardening strategy • Complementing security guides of other Avaya products
Platform Security	Describes the recommended security measures for securing the operating environment of the product for both turnkey and software-only solutions.
Application Security	Describes the application-specific security features and measures including application-specific accounts, authentication and authorization controls, security of APIs, and interfaces.
Account Management	Describes recommendations for maintaining and monitoring system accounts.
Audit Trails and Logs	Describes the audit trails and logging in the product.
Use of Cryptography	Describes the use of cryptography including the cryptographic algorithms, modes, and key lengths by the product.
Avaya Services Access	Describes the support and access provided to Avaya Services by the product including access technologies (SAL), Avaya Services accounts, and authentication technologies (ASG, passwords).

References	Lists the references.
Appendices	• Appendix A: Avaya Security Advisories • Appendix B: Software Updates • Appendix C: Regulatory Compliance • Appendix D: DoS Protections • Appendix E: RPM Information

Platform security

The following table lists the operating environment of System Manager.

Hardware	S8800 1U Server System Manager IBM x3550m2 and material code 700478589 R610 Server 2CPU MID2 Dell and material code 700501083 DL360G7 Server 2CPU MID4 HP and material code 700501093
Virtualization System	Avaya Aura® System Platform
Operating System	CentOS 5.6 64-bit

Avaya uses the open-source Linux operating system as a secure foundation for communications. System Manager uses CentOS 5.6 64-bit.

The open source foundation is beneficial because of the following reasons:

- Security experts worldwide review the source code for defects or vulnerabilities.
- Avaya works diligently to monitor both the enhancements and improvements created by the Linux community and to carefully review the changes before incorporating them into Avaya products.
- Linux-based Avaya servers and gateways protect against many DoS attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing, among others.

Avaya has modified or hardened the Linux operating system in the following ways to minimize vulnerabilities and to improve security:

- Minimal installation :RPMs removed

The Linux general distribution includes RPM Package Management (RPM) modules that install, uninstall, verify, query, and update software packages. System Manager has removed unused RPMs

from the general RPM distribution. For the list of RPMs required for the operation of System Manager, see Appendix E.

In addition to making the software file images smaller and more manageable, the operating system is more secure because attackers cannot compromise RPMs that are not present.

To determine which RPMs Avaya employs, use the rpm -qa command at the System Manager Server CLI to see the RPM list. See Product RPMs.

- Least privilege

System Manage supports a non-root installation. JBoss on System Manager runs as root. Also, the root SSH access on System Manager Server is disabled. You can establish SSH access using an admin account. To escalate access privileges, read the superuser permissions and restrictions by issuing the *su* command at the server command line interface.

CLI sessions support Timeout, and CLI administrative logging is performed for syslog files.

- Security function isolation

System Manager uses JBoss and Java cryptographic service provider architecture to isolate security functions from non-security functions to prevent compromise of the security function.

- Unnecessary IP ports closed

Many Linux modules like SSH or Apache or SSL and TLS (HTTPS) are applications that open Ingress network services. Avaya reduces the Ingress network services only to those that are necessary for telephony applications, thus minimizing exposure of the operating system to network-based attacks. By default, Avaya disables less secure network services such as TELNET (TELetype NETwork) and FTP. In System Manager, TELNET and FTP ports are Egress only.

By default, the following network services are disabled and only an administrator can re-enable the services:
Tftp, chargen, finger, http (gets redirected to https), X-windows, rlogin, rsh, rexec, netdump, rwhod, smb, yppasswd, ypserv, and Ypxfrd

In System Manager, nfs and portmap are installed and are required for the deployment manager. If you do not use the deployment manager, then you can stop nfs by running the following command:
/etc/init.d/nfs stop

- Secure connections

Avaya products protect authentication credentials and file transfers when sent across the network by using:

  - HTTPS

- Secure Shell (SSH)
- Secure Copy (SCP) or SFTP
- SNMP V3 which is the secure SNMP version
- SNMPV2 for listening and receiving Traps and SNMPV3 for listening to traps and exposing inventory information
- Secure LDAP
- Other protocols protected using a TLS or IPSEC connection
    - JMX over TLS: JMX authentication is a combination of certificate for the server side and password for the client side.
    - JMS over a TLS bisocket: Servers and clients generate private and public key pair and signed certificates and establish TLS connections for JMS traffic using the bisocket connection on the primary and secondary ports.
    - HTTPS: This protocol is a combination of Hypertext Transfer Protocol (HTTP) with SSL and TLS protocol which enables encrypted secure communication.

- Privilege escalation

  Avaya Linux-based products adopt the *privilege escalation* concept that requires lower-privileged accounts to log in at their normal level before login can escalate their privileges to perform more restrictive tasks, such as software replacement. Each privilege escalation requires a separate authentication and creates a log entry for monitoring.

  System Manager supports privilege escalation. Technicians who need higher privileges must log in using their normal service accounts and then escalate their privileges to perform more restrictive tasks, for example, software upgrades.

  To escalate access privileges, a technician uses su, a Linux/Unix escalation utility, that enables the user to log in to another account. The user must specify the account to log in to and respond to the authentication request for that account.

  You can read the superuser permissions and restrictions by issuing the su command at the server CLI. This command escalates the user permissions to the superuser level, and the output lists the commands that a superuser can and cannot run on the current host.

- No clear text passwords

  System Manager ensures that passwords are not stored, transmitted, displayed, or logged in the clear. Secure protocols (HTTPS, TLS, SSH) or encryption are used to secure password

transmission. Passwords stored in files, databases, or directory servers are stored as one-way hashed values.

System Manager does not provide for the restart of the operating system in the single-user mode. Unneeded accounts are removed. Accounts created by the operating system that are not required by the product are removed as part of the installation. System Manager has disabled shell access for system and service accounts. For example, an account used to run a service like Postgres does not have a shell defined.

The operating system is configured to limit the number of sessions and resources available to a given user.

- System Manager provides a customer a configurable warning banner for all interactive login sessions. On successful login, the system displays the date and time of the last successful login on the dashboard and then the number of failed login attempts since the last successful login in the logs. System Manager has disabled autocomplete on the login page and TCP timestamps.

Network layer security

Communication over the network poses the risk of interception by persons who might have unauthorized access to the network. This communication data might include:

- Translation data in transit or saved on a storage device including IP addresses and routing information from which an attacker can analyze traffic patterns.
- Application-specific traffic.
- Data exchanged during management and administration sessions.

This risk can be reduced by securing the communication data using digital encryption. The next section provides details about the encryption policy used by System Manager.

System Manager provides integrity verification by publishing a hash value using sha1 that can be verified for each file.

System Manager Encryption overview:

System Manager implements cryptographic algorithms and methodologies that are accepted in the INFOSEC community.

By default, System Manager does not use weak ciphers, < 128, SSLv2, and anonymous Diffie Hellman (DH). Server certificates use the SHA2. An external service does not support NULL certificates.

System Manager supports the encryptions in the following table:

Secure protocols	Available algorithms
SSH	3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour128, arc- four256, arcfour, blowfish-cbc, and cast128-cbc
HTTPS	SSL_DHE_DSS_WITH_RC4_128_SHA, SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, TLS_KRB5_WITH_RC4_128_MD5, TLS_KRB5_WITH_RC4_128_SHA, TLS_ECDH_ECDSA_WITH_RC4_128_SHA, TLS_ECDH_RSA_WITH_RC4_128_SHA, TLS_ECDHE_ECDSA_WITH_RC4_128_SHA, TLS_ECDHE_RSA_WITH_RC4_128_SHA, SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA, SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA, TLS_KRB5_WITH_3DES_EDE_CBC_MD5, TLS_KRB5_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,

	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
SNMP V3 with authentication and privacy	CFB-AES-128, CBC-DES

System Manager firewall protection

Firewall is a set of related programs, located at a network gateway server, that protect the resources of a private network from users from other networks. The term also implies the security policy that is used with the programs. An enterprise with an intranet that provides workers access to the wider Internet installs a firewall to prevent outsiders from gaining access to their own private data resources and for controlling what users of outside resources have access to. A firewall is a program or hardware device that filters information coming through an Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, the packet is not passed through.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

Packet filtering: A packet is a small chunk of data that the firewall analyzes against a set of **filters**. Packets that travel through the filters are sent to the requesting system and all others are discarded.

Proxy service: The firewall retrieves information from the Internet and then sends that information to the requesting system and vice versa.

Stateful inspection: This method is a newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is passed through. Otherwise, the packet is discarded.

The System Manager firewall implementation uses the Packet Filtering and Stateful Inspection techniques. The salient features of the firewall are:

- Supports unlimited access to loopback address, that is, **Packet filtering**.
- Drops all inbound packets barring the exceptions discussed further and processes all outbound packets and packets that are to be forwarded, that is, **Packet filtering**, by default.

- For TCP packets, checks for various combinations of the TCP flags to ascertain whether a packet is valid or not. The standard rules for identifying valid TCP packets are incorporated into the System Manager firewall , that is, **Packet filtering**.
- Supports Stateful inspection of packets wherein state checks are performed on all inbound and outbound packets to ascertain that packets are in proper state for secure communication. For inbound packets, the state MUST be either ESTABLISHED or RELATED, and for outbound, the state MUST be either NEW, ESTABLISHED, or RELATED, that is, **Stateful inspection.**
- Disables ICMP timestamp responses as the responses provide an attacker knowledge of the date that is set on your machine. This feature might help defeat all time-based authentication protocols **[Packet filtering]**.
- Provides inbound communication on ports that are reflected as part of the System Manager 6.3.8 port matrix document **[Packet filtering]**.

The firewall rules are captured in the file *$MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh*. To configure and enable the firewall, run the following command:
#sh $MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh

To query the firewall status, run the following command: *service iptables status*.
To start or enable the firewall, run the following command: *service iptables start*.
To stop and disable the firewall, run the following command: *service iptables stop*

To modify System Manager firewall rules, edit the $MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh file and append the rule at the appropriate location in the rule chain. You require root access to edit the firewall rules.

Note: The firewall rules are applied on a packet in top-down fashion. So ensure that any additional rule appears at the proper position in the firewall rule chain.

System Manager default firewall settings

System Manager 6.3.8 Port Matrix lists all the ports and protocols that System Manager uses. This document is available to Avaya Direct, Business Partners, and Customers at the following support site http://support.avaya.com/security

On this page, select the **Avaya Product Port Matrix Documents** link, and then scroll down the System Manager 6.3.8 Port Matrix document. You can gain access to this document only after logging into the Avaya Support site using valid support site credentials.

HTTP/HTTPS DoS protection

System Manager provides the following default security for HTTP/HTTPS connections:

- Connection limit

System Manager limits the database connection by defining a database connection pool size. Also, System Manager limits the number of active sessions for a user. This feature helps in DoS protection. The database connection pool size reduces connection churn overhead and also makes the database service available to valid users by denying unlimited or large number of database connections. In System Manager, the database connection pool size is set to 50.

- Inactivity Timeout

This feature provides resource optimization in System Manager by closing a connection that is no longer in use or inactive. By default, a connection closes in 30 minutes, and you can configure this from the user interface.

Prevention of DoS Attacks

A denial-of-service (DoS) attack is an incident causing denial of access to a resource. Regardless of the method, the net effect of DoS attacks is to deny legitimate access to a server or an application.

System Manager is designed to survive the DoS attacks as listed in the following table, without rebooting, restarting, or reloading, and automatically recovers full service after the DoS attack has subsided. For more details, see Appendix D - DoS methods Avaya has designed against

Protection against impact of viruses, worms, and other malicious code

Most viruses and worms, often called ***malware***, have the effect of

- Disrupting or delaying normal functionality
- Changing configurations by rewriting code
- Retrieving sensitive data

Although similar in their effects, viruses and worms differ in their functionality. A virus needs a host such as an application, an email, or a file and a user action, such as, opening an email attachment to propagate. A worm does not need a host or any user action. Viruses and worms are commonly delivered through email, visiting infected websites, or sharing file systems.

For information on loading virus software on Avaya servers, see https://downloads.avaya.com/css/appmanager/css/P8Secure/documents/100156571.

Security impacts of viruses and worms

Security implementation	Security impact
Natural immunity	Avaya Linux-based servers do not support: • Incoming or forwarding email • User Web browsing
Performance degradation	Avaya has tested third-party, host-based antivirus products on Linux-based servers and uncovered

Security implementation	Security impact
	significant performance degradation attributable to the third-party software. Do not install such products on Linux-based servers.

File system security

The following are implemented to secure the file system on the System Manager server:

- Default file creation mode on System Manager server umask setting:
  The default **umask 0002** is set for normal user. With this mask, default directory permissions are 775 and default file permissions are 664. The default **umask for the root user is set as 0022** which results in default directory permissions as 755 and default file permissions as 644. With an umask of **0022**, only you can write data, but anyone can read data.

- The system files are not open for casual editing by users and groups who must not perform such system maintenance. Key files such as keystore and password files are not open for casual editing by users and groups.

Platform accounts

System Manager Local Operating System accounts

The root SSH access on System Manager Server is disabled. At the time of installation, the following accounts are created by default:

Account	Remarks
Admin	A nonroot user account
craft , inads, init, sroot, rasaccess	ASG user accounts: Avaya Service technicians can use these accounts.
nortel	A user account that uses a public key-based authentication. A dedicated system account used for file replication between System Manager and CS1000.
Postgres	A login created by the installation of the System Manager software Postgres SQL database system. Access to the system using this login is disabled.

Avaya Service technicians can establish a remote SSH session to the System Manager server by using any of the ASG logins.

Account administration recommendations

For login account management, remember the following recommendations and constraints:

- Administer at least one local operating system account in all servers so that access is possible even if you cannot reach external AAA servers.
- Be cautious in enabling password aging for accounts authenticated through external servers, for example RADIUS accounts, that do not support the user changing a password through the application server.
- Because system access by Avaya Services is infrequent yet often required to maintain maximum uptime, do not enable password aging for Avaya Services accounts.
- Simple Authentication and Security Layer (SASL) authentication is not supported.

Administrators can establish SSH access using an admin account. To escalate access privileges, provide the *"su"* command at the server command line interface and read the superuser permissions and restrictions.

Credentials management

- System Manager Trust Management enables SSL support in System Manager JBoss container services.
- Credentials configured for an external AAA server such as RADIUS or LDAP are stored on the external server, not within the application.

Privilege escalation

For details, see section **Privilege escalation** .

Web server security

The following measures make the System Manager Web server secure:

- System Manager does not display the Web server version information.
- System Manager does not have files outside of the document root directory.
- System Manager has disabled directory browsing and the ability to follow symbolic links.
- System Manager has disabled unnecessary modules, HTTP Trace, and unnecessary methods.
- System Manager limits large requests and the maximum number of clients, requests, and threads.
- System Manager has lower timeout values to prevent DoS.
- System Manager provides trust and authentication.
- System Manager Web server specifies no-cache, no-store to prevent client side caching of Web pages to prevent the storing of sensitive information.
- System Manager Login pages cannot be placed inside frames, preventing the system against an attack known as ClickJacking.

Database security

System Manager secures database by enforcing encryption and authentication for all new connections to the database.

System Manager ensures that the database server is not compromised by:

- Denying remote access to the System Manager database. The System Manager database can only be accessed locally.
- Ensuring that communication between the database and System Manager application is done over a mutually authenticated TLS/SSL secure connection.
- Writing System Manager applications that prevent SQL injection attacks.
- Encrypting sensitive data such as passwords in the database.
- For supporting geographic redundancy, System Manager allows only peer System Manager server from a specific IP Address to connect to database.

To further harden the postgre database, the login shell for the postgres user is disabled. The postgres database user password is changed and is referred to as an environment variable for the root user saved in /root/.bash_profile. Postgres passwords are encrypted.

Directory security

System Manager uses an LDAP server and runs the *slapd* service the System Manager server to facilitate CS1000 or CallPilot administration.

System integrity and monitoring

System Manager has a system monitoring tool. This tool runs as a service and raises an alarm if the usage of any of the system resources such as a disk crosses the threshold limit.

For more details on the Health monitoring service, see **Administering Avaya Aura® System Manager**.The document is posted on **Avaya Support Site** for product **Avaya Aura® System Manager** Release **6.3.x** in the Downloads and Documents **section.**

Application security

This section describes the application-specific security measures provided by the product including data input validation, application layer authentication, and authorization controls.

Application account and session management

System Manager Installation creates the following accounts:

1. system: The user that authorizes global user data. For example, to define permissions for shared address or public contacts, you must define permissions as a *system* user.

2. admin: The user created at the time of installation. This user has a blanket access to System Manager including element managers.

You can create additional users through the System Manager common console.

Role-based Access Control

Role based access control (RBAC) provides organizations the ability to assign server, gateway, and application access permissions based on the job function or role of a user. RBAC within System Manager consists of two services for customers:

- RBAC management service: To configure and assign roles and permissions.
- Authorization service: To enforce the authorization based on the roles and permissions defined in System Manager.

All System Manager users can perform the operations that users are authorized to perform. System Manager provides the creation and assignment of roles to users.

The Role Based Access Control (RBAC) in System Manager supports two types of roles:

- Built-in
- Custom

Using these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are the default roles that System Manager provides. You can assign these roles to users, but you cannot delete these roles or change the permission mappings in the built-in roles. Built-in roles provide authorization to users for performing common administrative tasks.

System Manager supports the following default roles created at the time of installation.

Role name	Role permissions
Auditor	Provides read-only access to observe the system. You gain access to logs, configuration information, and audit files, but you cannot run any command.
System Administrator	Provides read-write access to system parameters such as IP addresses, upgrade software, and the ability to modify, assign, or define other roles and read-write access to create and modify logins and all other functionalities. You obtain read-write access to all System Manager resources.
Avaya Services Administrator	This role is equivalent to the System Administrator role. The role is assigned to the service personnel based on the access level set on the External Authentication page in the **Etoken authentication** section.
Avaya Services Maintenance and Support	Provides read-only access to maintenance logs and the ability to run diagnostics and view the output of diagnostics tools. You cannot run any

	command that might provide access to another host. The role is assigned to the service personnel based on the access level set on the External Authentication page in the **Etoken authentication** section.
Backup Administrator	Provides access to perform backups and restores.
Cloud Service Provider Administrator **Note**: This is a template role - This template can be used to create customized cloud service provider role using the clone roles mechanism.	Has permissions to: • Configure the solution • Manage the organization hierarchy of tenants. For example, site, department, and team. • Assign elements and resource permissions to the site • Manage end users for the tenant • Manage Tenant Administrators and Site Administrators
Tenant Administrator **Note**: This is a template role - This template can be used to create customized tenant administrator role using the clone roles mechanism.	Has permissions to: • Manage end users for the tenant • Gain access to Communication Manager Web pages
Communication Manager Admin	Provides permission to perform any action within the System Manager Communication Manager capabilities with access to all the related functions and tasks. You can perform any action related to Communication Manager devices, such as adding an endpoint, editing an endpoint, and more. You do not gain access to the scheduler.
Discovery Admin	Provides permission to configure discovery parameters such as SNMP version, SNMP credentials, the subnets, and the devices that you want to discover. You also have the rights to schedule and run a discovery operation.
End-user	Prevents log in to System Manager.
Messaging System Admin	Provides access to and permission for all activities related to messaging or mailbox. You cannot perform any task related to Communication Manager as a Messaging Administrator.
Presence Admin	Provides read-write access to the Presence configuration.
Presence Auditor	Provides read-only access to logs, configuration information, and audit files. You cannot run any command that might enable you to access another host.
Security Administrator	Provides read-write access to create other logins and create, modify, or assign roles. You can also install ASG keys, licenses, PKI certificates, and keys.

SIP AS Auditor	Provides read-only access to all the SIP Foundation server management functionality.
SIP AS Security Administrator	Provides access to the security features provided by the SIP Foundation server. For example, Security Extension.
SIP AS Administrator	Provides read-write access to all the SIP Foundation server management functionality.
CS1000_Admin1	Provides unrestricted OAM access to most administrative functions except security and account administration and provisioning for all customers on all call servers and related elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, and SNMP management for CS1000 systems. You can use all roles on all UCM elements with all permissions. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: SNMP Manager As this role gives permissions to all elements of type Linux Base, this role is not meant for users who only require authorization to manage CS1000 systems. The administrator must create a custom role for these users.
CS1000_Admin2	Provides unrestricted OAM access including security and account administration and provisioning for all customers on all call server elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, SNMP, IPsec, and SFTP management for CS1000 systems. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: SNMP Manager As this role provides permissions to all elements of type Linux Base, this role is not meant for users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users.
CS1000_CLI_Registrar	Provides permission to register and unregister individual CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI. The

	role has a single permission value to allow or deny a user to register or unregister an element. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Linux Base Users assigned to this role do not have CS1000 security or network level security privileges. This role is intended specifically for installation and repair technicians.
CS1000_PDT2	Provides full diagnostic and operating system access to all call servers. You cannot gain access to administrative functions and customer provisioning data unless combined with another role. You have access to the all elements of type: CS1000
MemberRegistrar	Provides limited access. You can register new members to the primary server. You have access to the following elements: • All elements of type: IPSec Manager • All elements of type: LinuxBase The following hidden permissions are granted to the MemberRegistrar role and cannot be copied to another role. PERM_PkiAdmin: Permission to perform PKI administration operations.
NetworkAdministrator	Note: The NetworkAdministrator role has been removed from System Manager 6.3.8 release. During Upgrades and Data Migration, care will be taken to assign all users from NetworkAdministrator role to System Administrator role. Similarly, all child roles of NetworkAdministrator role will be assigned to System Administrator role.
Patcher	Provides access to software maintenance functions such as patching and maintenance. You obtain access to the following elements: • All elements of type: Linux Base • All elements of type: Patching Manager
Service Technician	The system assigns the role to the service personnel when the service personnel connect to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.

On the Roles Web page you can create a custom role that maps to specific elements of different type and specify customized permissions for those elements. You can create custom roles for any user whose role is not authorized on one or more individual elements of any element type.

You can assign the roles that you created to users to perform specific tasks on an element.

For example, a custom role that you create for a single element can only perform specific tasks on that element. There is a specific permissions set that defines what this role allows you to do on that element.

You can also define roles that apply to how elements and element types are hierarchically arranged under user-defined groups. When you map permission to a selected group, the system takes that group into account when determining user permissions.

All roles need to be created in a hierarchical fashion i.e. you have to always select a parent role in order to create a new role which essentially then becomes the child of the selected parent. When a role gets deleted, all the child roles under it will also be deleted.

Role Management can be added as a custom privilege into a role.

Application password or pin policy

Password policy is the set of rules or laws that govern the creation and lifecycle of a password. The policy includes the combination of characters that form a password, the life expectancy of a valid password before a new one must be created, and the lockout period for invalid login attempts. The password policies apply only to administrators, not to externally authenticated users governed by an external authentication system.

The following table specifies the configurable password rules that System Manager provides:

Password policy rule	Default setting
Minimum password length	Passwords must have at least eight characters.
Minimum digits	Passwords must have at least one numeric character.
Minimum upper-case	Passwords must have at least one upper-case character.
Minimum lower-case	Passwords must have at least one lower-case character.
Minimum special characters	Passwords must have at least one special character.
Type of characters	Password characters that you can use are: a-z A-Z 0-9 {}|()<>,/.=[]^_@!$%&-+":?`\; You cannot use the previous six passwords.
Maximum invalid consecutive logins before an account is locked	Five
Lockout duration after reaching the maximum invalid logins	Accounts are locked for two minutes if five consecutive failed login attempts occur within 10 minutes.
Maximum number of days a password can be used	Passwords expire in 90 days after the last change.
Minimum number of days between password changes	Passwords cannot be changed in one day after the last change.
Number of days warning given before a password expires	Show password expiration warning during login 7 days before passwords expire. Expired password can be changed.
Number of days after an inactive account is locked	Not applicable.

Application session limits

Active sessions

System Manager enables the administrator to manage the global properties of user sessions including the maximum session time and the maximum idle time.

The end user can:

• Specify a number for the maximum session time in minutes from 0 to 1440 (24 Hours) in the **Maximum Session Time** field. The default value set for this attribute is 120 minutes.

•Specify a number for the maximum idle time in minutes from 0 to 1440 (24 Hours) in the **Maximum Idle Time** field. The default value set for this attribute is 30 minutes.

The total number of active sessions and sessions for each user or time of day is unlimited.

Application inactivity timeouts

Inactivity timeouts are implemented for users logged into a Linux shell through SSH or into the System Manager Management Web interface. The following table summarizes the inactivity timeouts for these connections.

Service	Session Inactivity timeout (Enabled Y/N, default timeout)	Configurable by the customer
SSH	Enabled, 4 hours	Yes
Web	Enabled , 30 minutes	Yes

Application-level authentication

In the current release, System Manager by default supports database-based authentication. You can configure System Manager to authenticate administrative users using other external authentication services such as Enterprise Directory or a RADIUS server.

Avaya Aura® System Manager supports external authentication services and supports:

- Centralized control of enterprise logins and passwords
- Enforcement of password aging, complexity, minimum length, and reuse requirements
- Avaya product adherence to the enterprise corporate security standards regarding logins and passwords

External authentication services	Required external servers	Authentication information
LDAP-based authentication	Requires an LDAP Version 3.0 directory	Configure System Manager to authenticate the enterprise LDAP for administrator authentication.

	server. Servers tested with System Manager are: ☑ Microsoft Active Directory (AD 2000 and AD 2003) ☑ openLDAP ☑ SUN LDAP 5.2	These users must still be provisioned in the System Manager database as System Manager requires that authorization information to provide privilege-based access.
RADIUS-based authentication	Requires a RADIUS server. This release of System Manager has been tested to interoperate with ☑ Free Radius	Authenticate administrative users for a RADIUS server. This setup also supports token-based authentication mechanisms such as SecurID. But like LDAP authentication, you must provision the users in the System Manager database for authorized access.
Token-based authentication • RSA SecurID	Requires a RADIUS server integrated with: ☑ RSA SecurID server	Use this authentication for a RADIUS server.
Kerberos server	Requires a Kerberos Server version 5.0	Use this authentication that is a Windows 2003 server with an Active Directory (AD) installed on the server.
SAML	System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4	Use this authentication for enterprise-level Single Sign On.

System Manager supports up to three authentication authorities in the authentication chaining:

- Local users
- External RADIUS users
- External LDAP users

The authentication scheme policy determines and uses the three authentication authorities in the following order:

- Local users (default)
- External RADIUS users and then local users
- External LDAP users and then local users
- External LDAP users, followed by external RADIUS users, and then local users
- External RADIUS users, followed by external LDAP users, and then local users
- External KERBEROS server

The authentication server policy controls the settings for the external LDAP, RADIUS, and KERBEROS servers**.**

Configuration for Radius

Specify the following configuration parameters to securely integrate System Manager into a customer network.

Parameter	Description	Expected values	Examples
IP or DNS	The hostname or IP address of the RADIUS server that will be used as the primary RADIUS server for authentication.	IP address such as 192.168.111.23 or "hostname.rnd.avaya.com"	192.168.111.23
UDP PORT	The port number that the primary RADIUS Server uses to receive RADIUS authentication requests.	An integer	1812
SHARED SECRET	The secret key that is used to sign RADIUS data packets to ensure data packets originate from a trusted source. Ensure that the client configuration of the RADIUS server is associated with this shared secret.	A string	Abv234key

Configuration for LDAP/AD

Specify the following configuration parameters for integration into the customer network.

Parameter	Description	Expected values	Examples
IP or DNS	The IP address or DNS name of the LDAP server.	IP address such as 192.168.111.23 or hostname.rnd.avaya.com	192.168.111.23
TCP Port	The TC port number of the LDAP/AD server.	An integer	26982
Base Distinguished Name	The base DN value which is going to be used. The complete DN used for the authentication is LDAP_USERNAME_PREFIX+ "=" + name entered by user + "," + LDAP_BASE_DN.	A string	dc=testdomain, dc=avaya, dc=com
SSL/TLS Mode	The mode to be used if TLS/SSL connection is required between IAM module and the primary LDAP server. Set this value TRUE. Note: See for the following description for how to use SSL.	Boolean	TRUE or FALSE
Is Active Directory	The parameter to use if active directory does not support anonymous binding.	Boolean	TRUE or FALSE
Supports Anonymous Binding	Select if supported. Active directory does not support Anonymous Binding.	Boolean	TRUE or FALSE
Distinguished Name for Root Binding	Type the distinguished name for the root binding.	STRING	cn=root
Password for Root Binding	Type the password for the root binding.	STRING	

Using SSL with LDAP:

With System Manager Configuration, you can use SSL when you connect to the LDAP servers. To use SSL, perform the following additional configuration:

1. Check SSL/TLS Mode as TRUE.
2. Ensure that the **server is configured for SSL**.
3. Ensure that the port number mentioned above TCP Port is the SSL port.

The LDAP External Authentication process uses the System Manager default certificate. To configure SSL with LDAP:

1. Import the External Authentication Server certificate as a trusted certificate in the System Manager Trust store using one of the following methods:
   - Import from existing
   - Import from file
   - Import as PEM Certificate
   - Import using TLS
2. Configure the external authentication server. For information, see LDAP configuration section. Edit Authentication Scheme to External LDAP Users, then local users.
3. Set the System Manager default certificate as a client certificate. If the external authentication server requires client side authentication, then add the System Manager certificate as a client in the external authentication server.

   - Navigate to **Services > Security > Certificates > Authority**.
   - Under CA Functions, select **Download pem file** and save the certificate to a file.
   - Export the certificate to the external authentication server.

Configuration for Kerberos:

Specify the following configuration parameters to securely integrate System Manager into a customer network.

Parameter	Description	Expected values	Examples
DC Host Name (FQDN)	To specify the FQDN of the Kerberos Server.		Format: machineName.domainName.com/net/
DC Computer Domain	To specify the domain name of the Kerberos server.		Format: global.avaya.com

Keytab File	To specify the encrypted Kerberos server key.		File extension keytab file

Note: When you log on to the Kerberos server using Single Sign-on (SSO), you cannot exit from System Manager using the Logout link because in this context, SSO automatically authenticates you inside the Domain Controller (DC) domain. You must manually close the browser to exit the application.

Configuration for SAML:

Parameter	Description	Expected values	Examples
Metadata Type	Specifies the method to query the metadata for Remote Identity Provider. The values are: • URL. A valid HTTP URL. • File. A valid XML file.		Format: URL/FILE
Metadata Url	Specifies the valid HTTP URL for the metadata of Remote Identity Provider.		
Metadata File	Specifies the valid XML file for the metadata of Remote Identity Provider.		
Choose File	Selects an XML file that contains the metadata for Remote Identity Provider.		

Backup and Restore

To perform Backup and Restore functions, use the System Manager console.

Backup

The backup operation from the System Manager console creates a backup image of the System Manager database. Customers are responsible for the security of their backup data.

System Manager backup operation supports integrity check by verifying the signature of the files. This will avoid the restore of corrupted or tampered backups on the System Manager. The key length used is 2048 and the algorithms used are DSA and ELG-E.

Restore

The restore operation is initiated from the System Manager console. The restore operation restores the System Manager database with the configuration data contained in the backup data.

For more information about Backup and Restore operations, see *Administering Avaya Aura® System Manager*.

The document is posted on Avaya Support Site for product **Avaya Aura® System Manager Release 6.3.x** in the **Downloads and Documents section.**

The System Manager PEM backup zip contains pg_dump and is not in a readable format. Some parts of the backup archive must be encrypted. System Manager 6.3.4 onwards does support integrity checking of backup files. System Manager 6.3.4 onwards does provide a mechanism or capability to verify that the contents of backup archive files have not been changed in an unauthorized manner.

Audit trails and logs

An audit trail or log is a chronological sequence of records showing who has accessed a computer system and what operations a user performed during a given period of time. Audit trails are recorded in reference to two basic areas: Linux-based shell commands and any application management-based changes. CLI administrative logging is done to the syslog files.

To ensure compliance with enterprise security policies, System Manager provides capabilities to monitor configuration changes and other security events through the logging and alarming infrastructure.

System Manager Application contains agents that collect logging and alarming events. System Manager communicates with these agents to retrieve, process, and centralize the administration of events.

The logging and alarm event displays show such details as event timestamp, severity, description, and originating host or application. Log messages follow the Avaya Common Logging Format. You can administer alarms, that is, clear, acknowledge, and export alarms to a spreadsheet.

Configuration options include defining the severity level at which the events of an application must be collected, the log file sizes and locations, and event data retention policy.

Any configuration changes using the System Manager is logged. As part of the logging process, the logs contain the login name of the individual making the change, the date and time of the change, the IP address of the connecting system, and a synopsis of the before and after data changes.

All log files are configured to roll over at a specific interval to prevent the log files from using up the entire disk space. In regards to the ability to modify a log file, an administrator with root access to the server console can make changes to a log file. With administrator access through the System Manager Management console, you can view or download log files. By keeping the root password private and restricting access to the console, this item should not be a major concern.

System Manager Log management is an approach to dealing with large volumes of applications-generated log messages, for example, audit records, audit trails, and event logs. Log management also includes log collection, centralized aggregation, long-term retention and purging, log forwarding in real-time and in bulk after storage, log analysis, and log search and reporting. Log management is driven by

reasons of security, system, applications, and net work operations, such as system or network administration and configurations.

System Manager provides two ways for handling log messages of the products that it manages.

- Real-time log management
  Real-time log management is only applicable to logs that are in Avaya common logging format. The System Manager console provides the Graphical User Interface (Logging UI) for viewing and searching Log information. Functionalities available through Logging UI module are:
    - Listing logs
    - Searching logs using Boolean Advanced search
    - Filtering logs
    - Viewing log details

  To purge logs, use the System Manager Data retention UI.

- Log pulling on demand through System Manager log harvester
  Use log harvesting to collect log files from multiple hosts on demand. Unlike real-time log forwarding, log harvesting is independent of the format of logs. Serviceability Agent co-locates the products that can be configured to harvest the log files generated by the applications for debugging an application remotely. The advantages of this feature are:
    - No network traffic unless the admin asks to see the log
    - Easy debugging
    - Scaling
    - Log format independent approach
    - Enhancing overall performance

System Manager provides the Graphical User Interface (Log Harvesting) for archiving, browsing, searching, and downloading of logs. The functionalities available through the log harvesting module are:

- Creating new harvest profiles
- Archiving requests for a profile
- Viewing log files in a log browser
- Searching in the logs
- Downloading the selected file or archive

Auditable events

Security-related events that are logged

Security events related to the following actions or activities are logged:

- Attempted login or logoff, whether successful or not
- Establishment of a new administrative access session regardless of port of entry
- Assignment of a user profile to an administrative session
- Display, list, change, addition, or deletion of a user profile
- Any administrative access to local user accounts, for example, to view, add, change, or delete
- Failed attempt to access an object or execute an action to which the user does not have access

- Trust management activities, as in certificate administration

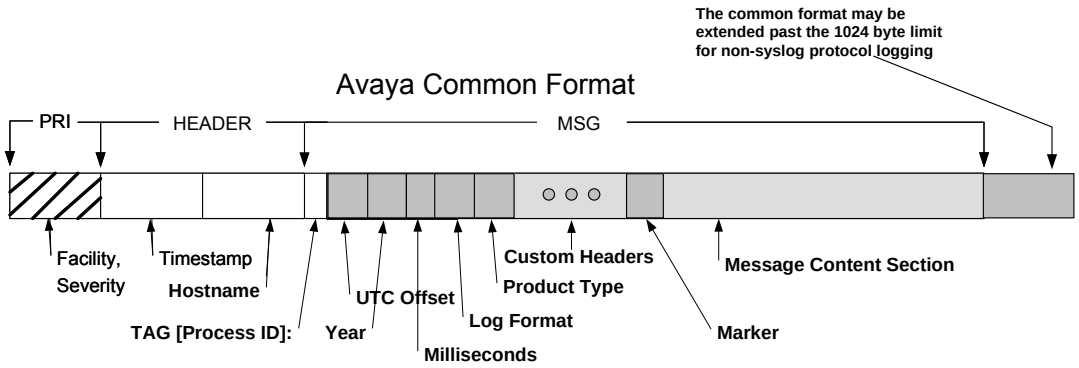
RBAC logs the security logs if the user is not authorized to create, edit, and delete the role.

System Manager provides no special facility reserved for security-related events.

Security information is logged in or notified through:

- Syslog security log
- Miscellaneous logs that track security-related information, such as:
  - Linux access security log
  - Platform command history log
  - HTTP or Web access log
  - IP events
- System Manager central log

Avaya Common Logging Format



Protection of audit records

Maintaining logs on remote machines is a technique that discourages attack because with the method, an attacker must gain access to multiple systems to remove their activities from log files. For a system that is not running on a server or desktop OS, such as Windows, Unix, and Linux, remote logging to at least one remote log server is important for a central security information management. Logging is done following RFC 3164 (SYSLOG protocol) at a minimum. Preference is given to using RFC 3195 (Reliable Delivery for syslog) in lieu of RFC3164. Client devices that do not support user or administrative login are exempt from this requirement.

Use of cryptography

Trust, Certificate, and Key Management or PKI

In cryptography, a **digital certificate** is an electronic document that uses a digital signature to bind a public key with an identity. The identity includes information such as the name of a person or an

organization, their address, and more. The certificate is a means to verify that a public key belongs to an individual.

Digital certificates certify that a public key belongs to its reputed owner. To ensure greater trust, a trusted party can sign the public key and the information about its owner, creating a public-key certificate, usually called a certificate. Similar to a driving license, a certificate guarantees the identity of its bearer.

A trusted party that issues digital certificates is called a certification authority (CA), similar to a governmental agency that issues driving licenses. A CA can be an external certification service provider or even a government, or the CA can belong to the same organization as the entities that the CA serves. CAs can also issue certificates to other sub-CAs, which creates a tree-like certification hierarchy called a public-key infrastructure (PKI).

In the context of System Manager, the certificate that System Manager uses to assert its identity to the far end is called its Identity Certificate. The issuer or CA certificates that System Manager uses to verify or validate the identity of the far end is referred to as Trusted Certificates.

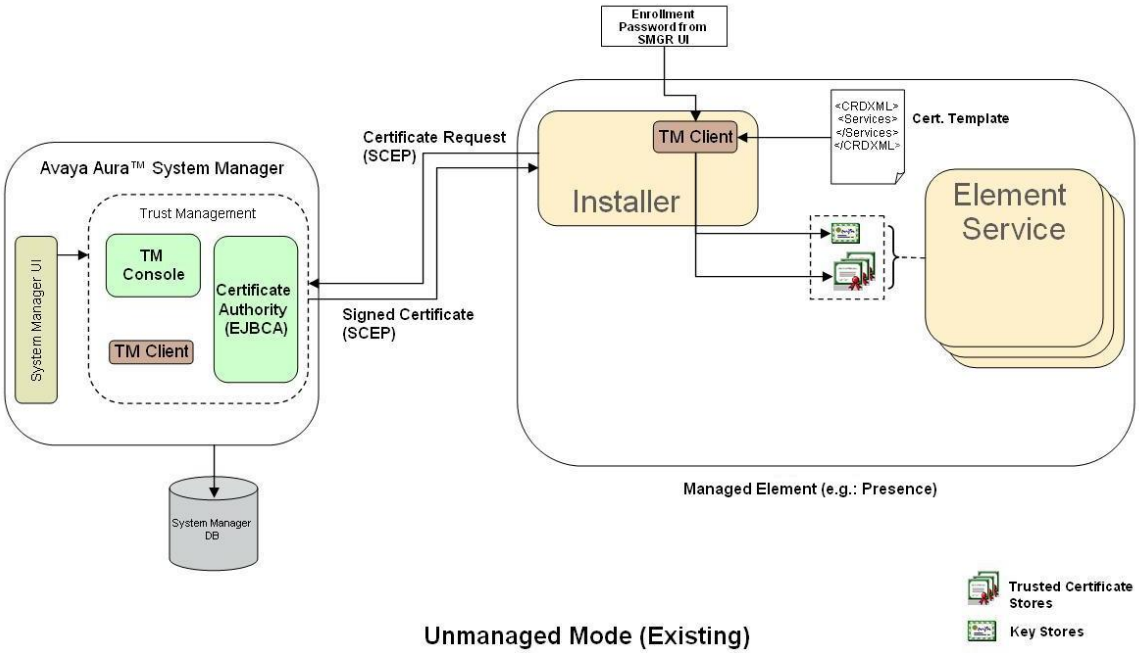
Updating Trusted Certificates of System Manager

System Manager Trust Management provisions and manages certificates of various applications, such as servers and devices, enabling the applications to have secure interelement communication. System Manager provides Identity (Server) and Trusted (Root/CA) certificates that the applications can use to establish mutually authenticated TLS sessions.

System Manager supports two modes of trust management for its managed elements: Unmanaged and Managed.

Unmanaged mode of trust management

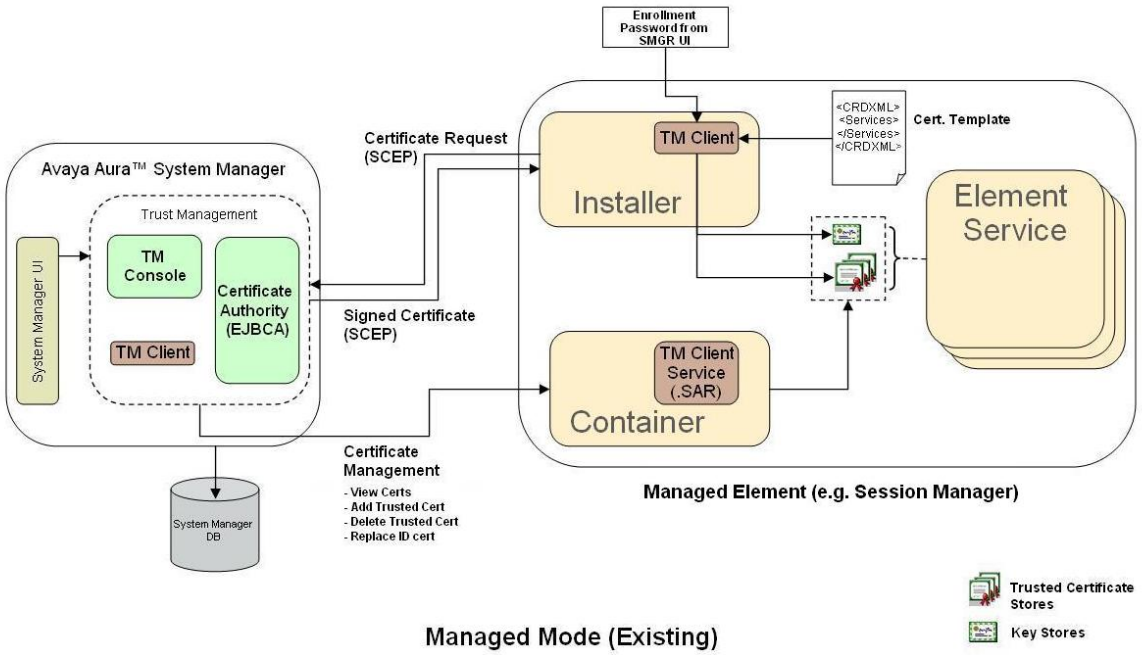
The following diagram shows the unmanaged mode of trust management. Here, the application uses the TM client to request the System Manager to issue certificates based on the certificate template, named Certificate Requirement Document (CRD) and provided by the application. This mode is always client initiated. System Manager has no knowledge of the certificates present on the remote managed element and cannot manage the certificates.



Unmanaged Mode (Existing)

Managed mode of trust management

The following diagram shows the managed mode of trust management. Here, the application hosts the TM client service in a container. In this mode, System Manager is responsible for managing the applications certificates. The managed element performs the installation or initialization in the same manner as in the unmanaged mode. The applications register as an element in System Manager and their certificates can now be managed from the System Manager console.



Managed Mode (Existing)

The Trust Management service of System Manager is deployed with the certificate authority software, Enterprise Java Beans Certificate Authority (EJBCA), which is configured to be a root CA by default. However, System Manager supports third-party certificates.

From System Manager 6.3.4 release, Trust Management supports one Certificate Authority and one user interface for Certificate Authority.

In System Manager, element installation sets up the trust between System Manager and its managed elements.

From System Manager 6.3.4 release, you can manage certificates through one user interface. To manage certificates for System Manager and its Managed Elements, go to **Elements** > **Inventory** on the System Manager home page.

System Manager 6.3.8 now supports generation of certificates by using SHA2 as the signing algorithm and 2048 as the default key size. All new certificates will be signed using this algorithm and use 2048 as the default key size unless explicitly overridden by the requesting client.

Issuing a unique identity or server certificate to System Manager

EJBCA is a third-party open source application that System Manager uses to issue identity and trusted certificates to applications through SCEP.

During installation, the application uses the System Manager Trust management service to request for a unique identity certificate. For this, the application must provide location information and the enrollment password.

You can add a third-party identity certificate for System Manager instead of using the internal CA signed certificate, which is the default certificate from Avaya CA. See Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.1 - Issue 0.1 at https://downloads.avaya.com/css/P8/documents/100144833.

You can also set up System Manager CA as a sub-CA. For information about how to set System Manager Certificate Authority (EJBCA) as SUB-CA, see *Administering Avaya Aura® System Manager*.

System Manager uses the certificate profile, ID_CLIENT_SERVER, for SIP Communications. The following table lists the related details:

Profile attributes	**Default value**	**Description**
Validity (Days)	730	The validity determines the validity in days of certificates from the time the certificate is issued.
Allow validity override	False	If you enable extension override, X509 certificate extensions featured in *certificate requests* are honored. Otherwise, X509 certificate extensions are ignored.
Allow extension override	False	If you enable subject DN override, the X509 subject DN extension created in a certificate can come directly from the request sent by the users.
Use Basic Constraints	True	
Basic Constraints Critical	True	
Use Path Length Constraint	False	
Path Length Constraint		
Use Key Usage	True	
Key Usage Critical	True	
Use Subject Key ID	True	
Use Authority Key Id	True	
Use Subject Alternative Name	True	
Subject Alternate Name Critical	False	

Defining server trust relationships with Digital Certificates

To establish mutually authenticated TLS connections between System Manager and any other Avaya or third-party application or server, either end must be able to establish the identity of the other party during the initial TLS handshake and establish the relationship back to a known trusted third party. To enable this exchange and establish this trust relationship, both parties must provide their chain of trust. System Manager supports third-party certificates. See Application notes for supporting third-party certificate in Avaya Aura® System Manager.

System Manager to Avaya applications and servers

To prevent eavesdropping and maintain privacy, the management traffic between System Manager and other Avaya applications or servers is secured using TLS. For System Manager to be able to trust the certificate that a component presents, System Manager and the component must both be enrolled in the same PKI hierarchy.

For System Manager to manage trust after the initial enrollment has taken place, System Manager enables each component to enroll *itself* into the PKI domain using the component installer. Enrollment into the PKI hierarchy is restricted through the use of a challenge password. The CA knows the password and manually communicates the password to the local administrator, who provides the password to the component at installation time.

System Manager to third-party applications and servers

Use only unique, nondefault identity or server certificates within System Manager when interoperating with third-party applications or servers.

Default certificates and keys

System Manager uses its own Certificate Authority (CA) to issue its default certificates. To view and manage these default certificates, use the System Manager User Interface.

To see the certificate management interface for the default certificates of System Manager, go to **Home > Elements > Inventory > Manage Elements > System Manager > More Actions**.

The following are the details of the validations for TLS connections:

1) **Mutual TLS Authentication:** During a TLS handshake, mutual TLS authentication is performed. The identity certificate of the third-party entity is validated against the trusted CA certificate repository in the System Manager for TLS. If this verification fails, System Manager does not accept the connection.
2) **Additional Validation on Entity Identity Certificate:** If the mutual TLS authentication is successful, further validation is performed on the Entity Identity Certificate for the credential name or the far end IP address.
    a. If the Common Name string is empty, the connection is accepted.
    b. If the Common Name string is not empty, the system searches the Common Name and the IP address of the entity at following places in the identity certificate provided by the Entity.
        i. CN value from the subject.
        ii. subjectAltName.dNSName
        iii. subjectAltName.uniformResourceIdentifier
        For IP Address comparison, the IP address string is converted to :W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Case insensitive search is also performed in this case.

Access to Avaya Services

Data transmission to and from Avaya Services in support of customer equipment is protected through nonsecure data networks such as the Internet, over modems, and through SNMP notifications. For more information, contact Avaya Services.

Avaya Services can reach System Manager residing in a customer network for maintenance and services without needing to request access from customers. Avaya Services gain access to the System Manager server through the SAL gateway. The authentication and authorization of the technician is accomplished by way of their PKI user certificate. Also, each login is traceable.

The Avaya Technician can log in to System Manager with any of the following three accesses:

- Read-Write Access (Avaya Services Administrator)
- Read and Diagnostic Access (Avaya Services Maintenance and Support)
- No Access

The Read-Write Access is the default access that the System Manager administrator provides to an authenticated technician. This access is assigned to the Avaya Services Administrator role. System Manager has the option to change the default role from the System Manager console.

If the System Manager administrator sets the No Access option, the Avaya Technician sees an error message after authentication to informing that authorization to access the resource (System Manager) is not available.

Access to the remote cut-through is restricted for the technician. As the technician only has access to the System Manager box through the SAL gateway and no other machine present in that network, any links pointing to any other box in the customer network do not work. So, even if access to System Manager is compromised, the other machines in the network are not affected.

The technician can reach System Manager over HTTPS through the Axeda enterprise. The Axeda enterprise currently allows only a single HTTPS connection to be established with a device or system managed by System Manager. Hence, only a single technician can access System Manager when accessed from the Axeda enterprise. This limitation is to avoid a DoS attack.

Avaya Services Accounts, Authentication, and Authorization

Management and maintenance of System Manager is done through the System Manager console. However, maintenance and troubleshooting often require operating system-level access to the System Manager server. The following sections describe administrative accounts in System Manager.

Avaya Services Accounts

System Manager supports Access Security Gateway (ASG) so that Avaya services can securely access customer systems. ASG is configured by an Authentication file (AF) that contains the customer-specific Product ID (AFID) and the key to validate the challenge and response credential. Avaya technicians can then log in on a customer machine using a credential composed by a challenge and response. The following table provides the services login details:

Account	Service level	Privileges
sroot	Root	Services Root, same as _root. Protected by the Password Change System authentication of Avaya.
craft	susers	craft cannot perform login administration or change customer services.
init	susers	Same as craft.
inads	susers	Same as craft.
rasaccess	susers	rasaccess cannot stop Session Manager.

References

You can find the following documents at the Avaya Support website at: http://support.avaya.com/

Documents mentioned in this security guide

Document title	Document number
Administering Avaya Aura® System Manager 6.3.8	
Installing the Avaya S8510 Server Family and its Components	03-602918

Security documents on the Avaya Support site

Document title	Link
Avaya Enterprise Services Platform Security Overview	Requires non-disclosure agreement.
Avaya's Security Vulnerability	http://support.avaya.com/elmodocs2/security/sec

Document title	Link
Classification	urity_vulnerability_classification.pdf
Security Best Practices Checklist for Unified Communications Deployment	This document is available at: https://support.avaya.com/security
Avaya Toll Fraud Security Guide	
Avaya and Vulnerability Scanning	
Mapping Common Vulnerability Exposure (CVE) numbers to Avaya Security Advisories (ASAs)	

For other security documents, visit https://support.avaya.com/security.

Appendix A: Avaya Security Advisories

Overview

Avaya Product Security Support Team (PSST) performs the following functions:

- Manages Avaya product vulnerabilities and threats.
- Maintains information posted at http://support.avaya.com/security.
- Performs security testing and auditing of the core products of Avaya.
- Resolves security-related field problems in support of Avaya Global Services.
- Manages the security at the alerts@avaya.com mailbox.

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

When security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: High, Medium, Low, and None (see **Interpreting an Avaya Security Advisory**). Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and its risk level, the advisory might include a recommended mitigation action, a recommendation regarding the use of a third-party-provided patch, a planned Avaya software patch or upgrade, or additional guidance regarding the vulnerability or more.

Accessing Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support web site at http://support.avaya.com/security. Customers can register at Avaya Support web site to receive email notifications of Avaya security advisories. The time frame of distributing advisories is indicated in the following table:

Vulnerability classification of Avaya	Target intervals between assessment and notification
High	Within 24 hours
Medium	Within 2 weeks
Low	Within 30 days
None	At the discretion of Avaya

To sign up to receive advisories by email on the Avaya Security Support website:

1. Browse to http://support.avaya.com.
2. If you do not have an account, go to http://sso.avaya.com and click **Register Now**. Follow the instructions. To register, you need an Avaya SSO login and a Sold To number.
3. After you set up an SSO user ID and password, enroll for the e-notifications you want to receive.
4. To enroll, click on the **My E-Notifications** link from the home page of the website (http://support.avaya.com). You can also select the **My E-Notifications** link under Online Service Manager.
5. To enroll for additional e-notifications of your choice, click **Add New E-Notifications**.
6. If you select one of the five buttons on the top of the page, you will receive email notifications when new content is added or revised for all Avaya products related to the following content areas:

    - Product Correction Notices
    - Security Advisories
    - Product Support Notices – High Priority
    - End of Sale Notices
    - Services Support Notices

7. To receive an email notification for a particular product, select **Choose from the Product list** and then select the product for which you want to receive notifications. At the prompt, select the release and content types from the available release and content type combinations for the selected product.

If you have any questions about enrolling for My E-Notifications on the Avaya Customer Self Service website, send an email message to support@avaya.com.

Interpreting an Avaya Security Advisory

The precise definitions that PSST follows in classifying vulnerabilities relative to their potential threat to Avaya products is available in the Security Vulnerability Classification document at https://support.avaya.com/css/P8/documents/100066674

The following table summarizes the three main categories.

The security vulnerability classification of Avaya

Vulnerability classification	Criteria for classification
High	The product is vulnerable to: • Attacks from a remote unauthenticated user who can easily access high-level administrative control of a system or critical application without interaction with a user of the product beyond standard operating procedures. • Attacks from remote unauthenticated user who can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. For example, see the advisory at http://support.avaya.com/css/P8/documents/100062710
Medium	The product does not meet the criteria for high vulnerability but is vulnerable to: • Attack from a user who can gain access to a user account. Access does not directly require the privileges of a high-level administrative account. • The system or critical application or both shutting down, rebooting, or becoming unusable. An existing administrative or local account is used for this attack. • Attack from a user who can gain access to a local user account from which higher-level privileges are available. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064239

Low	The product does not meet criteria for medium or high vulnerability but is vulnerable to: • Compromise of the confidentiality, integrity, or availability of resources, although any compromise is difficult or unlikely without nonstandard direct user interaction. • Noncritical applications shutting down, rebooting, or becoming unusable. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064944
None	A related third-party product has vulnerability but the affected software packages, modules, or configurations are not used on an Avaya product and there is therefore no vulnerability. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064240

Organization of an advisory

Overview

The overview provides a description of the vulnerability. For operating system or third-party software, a link is also provided for quick access to a website for more information. The linked information provides:

- A description of the risk
- Instructions on how to correct the problem, which might include:
  - Installing an update
  - Revising the administration of the product
- A description of what additional security fixes, if any, are included in the update.

Avaya software-only products

For Avaya software-only products, the advisory lists specific Avaya products that use, but are not bundled with, operating system software that might be vulnerable. Information includes:

- The product version affected
- Possible actions to take to reduce or eliminate the risk

Avaya system products

For Avaya system or turnkey products, the advisory lists the specific Avaya products that are vulnerable or are bundled with operating system software that might be vulnerable. Information includes:

- The level of risk
- The product version affected
- Possible actions to take to reduce or eliminate the risk

Recommended actions

The advisory provides a list and description of steps to take to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade.

For operating system and third-party software, the recommended actions are normally identified in detail through website links in the security advisory.

Appendix B: Software and Firmware updates

Method that Avaya uses to delivers security updates

Generally, Avaya makes security updates available on or through the Avaya Security website at http://support.avaya.com/security. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals:

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update with a 30-day maximum delivery time. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update with a one-year maximum delivery time. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update with a one-year maximum delivery time. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.

Avaya product development staff incorporates a third-party update into its software in one of three ways:

- Avaya simply bundles the specific update or the new release of the affected software with the Avaya Session Manager software so that the security-related updates are automatically incorporated into the Avaya product operation.
- Avaya modifies the Session Manager software so that the specific update or the new release of the affected software is appropriately incorporated into the Session Manager operation.
- Avaya modifies the specific update or the new release of the affected software so that the security-related updates are automatically incorporated into the Session Manager operation.

When Avaya incorporates one or more security fixes into its software, Avaya delivers the fixes in one of three forms:

- A security update: Includes operating system or third-party software security fixes or both.
- An Avaya software update: Includes software security fixes to the Avaya application software.
- An Avaya full release of software: Includes all software for the Avaya product, including software security fixes to the Avaya application software or security fixes for the operating system and third-party fixes or both.

Validating a security update

When Avaya determines that a third-party security update applies to one or more of its products, Avaya product development tests the update on the affected current products to ensure there are no adverse effects to the published functionality of the products. In addition, when third-party updates are included in new software releases, the products are thoroughly tested.

Avaya-generated security updates are likewise tested on all affected products prior to release. Avaya security updates are likewise tested before incorporation into subsequent releases. Testing meets requirements of internal Avaya testing standards, including testing for the following:

- Denial of Service
- Encryption standards
- Certificate management
- Audits and logging
- Access control

Appendix C: Regulatory compliance

System Manager supports regulatory compliance: Sarbanes-Oxley Act, Graham-Leach-Bliley Act, CALEA, ISO 17799, FISMA, HIPAA, and PCI.

Considerations for customers who must comply with the Sarbanes-Oxley Act

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the requirements of the act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Sarbanes-Oxley Act of 2002 is a federal law enacted in response to a number of accounting scandals involving major U.S. corporations. A key requirement of the act is that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting. One major area of internal control consists of information technology controls. As a result, the Sarbanes-Oxley Act holds chief information officers responsible for the security, accuracy, and reliability of the systems that manage and report financial data.

To the extent that a company uses data collected or transmitted by System Manager as part of its overall cost or revenue reporting and financial management, the company can use its security-related features to secure the data. Use of these features can further demonstrate the good faith data management and reporting of the company.

System Manager Security features also help prevent unauthorized access to the customer network, in general.

Features related to data security and documented in more detail in other sections of this document are:

Feature	Mapping to Sarbanes-Oxley	Reference
Encryption	Protects transmitted data from packet-sniffing and eavesdropping.	See System Manager Encryption Overview on page 17.
Access control	Protects access to data from unauthorized personnel.	See Role-Based Access Control on page 25.
Authentication	Restricts access to the system by use of login and password.	See Administrative Accounts on page 43.
Logging	Logs security-related events.	See Audit Trails and Logs on

Feature	Mapping to Sarbanes-Oxley	Reference
		page 35.
Backup of data	Data saved on backup media or backup server.	See Backup and Restore on page 35.

Considerations for customers who must comply with the Graham-Leach-Bliley Act

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the requirements of the act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Graham-Leach-Bliley Act (GLB) requires financial institutions to disclose privacy policies regarding customer data. This disclosure must describe the ways the institution might use and disclose private information.

Where indicated in their policy, financial institutions must protect the privacy of their customers, including the nonpublic, personal information of the customer. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical, and physical safeguards.

System Manager data to which the Graham-Leach-Bliley Act might apply includes customer names and telephone numbers, called and calling number data, and abbreviated dial lists.

Use of the following key features can protect customer privacy and demonstrate compliance with the interagency guidelines supporting the Graham-Leach-Bliley Act.

Feature	Mapping to Graham-Leach Bliley Act	Reference
Encryption	Protects transmitted and stored data from unauthorized individuals.	See System Manager Encryption Overview on page 17.
System access control	Protects access to data from unauthorized personnel.	See Role-Based Access Control on page 25.
Authentication	Restricts access to the system by using login and password.	See Administrative Accounts on page 43.

Feature	Mapping to Graham-Leach Bliley Act	Reference
Backup of data	Protects against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures by using encryption and key.	See Backup and Restore on page 35.

Considerations for customers who must comply with CALEA

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the requirements of the act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In response to concerns that emerging technologies such as digital and wireless communications are increasing the difficulty for law enforcement agencies to execute authorized surveillance, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) in 1994. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that the systems support the necessary surveillance capabilities of law enforcement agencies.

In an order effective September 23, 2005, the FCC concluded that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. To the extent that CALEA applies to Avaya offerings, such offerings have achieved compliance with the applicable CALEA requirements. In the event that an Avaya customer is subject to CALEA requirements, there are various third-party products, including Session Border Controller products, which claim to provide or facilitate CALEA compliance. Examples of these products are:

- NexTone
- AcmePacket

In addition, System Manager Characteristics that can aid in CALEA compliance are the following:

- Standard architectures. For example:
  - Uses Open Systems Interconnection (OSI) standards for network communications. Therefore, transmissions are interceptable for surveillance tools established to work with the OSI standards.
  - Calls are always divided into call control signaling and voice or bearer signaling. This trait simplifies the task of determining what data to observe.
- Authenticity and integrity assurance of the calls under surveillance through its encryption and authentication capabilities.

- Call Detail Records that records called numbers and other call data that might be useful to law enforcement.

Considerations for customers who want to comply with ISO 17799

ISO 17799 of the International Standards Organization, "Information technology - Security techniques - Code of practice for information security management," is an internationally accepted standard of good practice for information security. ISO 17799 suggests a well-structured set of controls to address information security risks, covering confidentiality, integrity, and availability aspects. None of the suggested controls is mandatory. However, an organization wishing to be in compliance should show a security strategy that explains the decision not to implement key controls.

ISO 17799 addresses the following broad categories of data security management:

ISO 17799 Security Guidelines	Security features and processes
Ensure that applications process information correctly.	
Use validation checks to control processing.	Use the System Log and Maintenance Alarm and Event logs. See **Audit Trails and Logs** on page 35.
Validate data input into your applications.	See **Administering Avaya Aura® System Manager**.The document is posted on **Avaya Support Site** for product **Avaya Aura® System Manager** Release **6.3.x** in the **Downloads and Documents** section.
Protect message integrity and authenticity.	See System Manager Encryption Overview on page 17.
Validate the output data of your applications.	Use audits and status reports to verify output. See Audit Trails and Logs.
Use cryptographic controls to protect your information	See System Manager Encryption Overview on page 17.
Protect and control the system files of your organization.	
Control the installation of operational software.	System Manager requires the appropriate access control to install software. See *System Manager Installation and Administration Guide*.
Control the use of system data for testing.	Avaya uses internal ISO-certified testing processes for software.

ISO 17799 Security Guidelines	Security features and processes
Control access to program source code.	System Manager source code is not accessible outside of Avaya. The Red Hat Linux operating system is also restricted. See Appendix E.
Control development and support processes.	
Establish formal change control procedures.	Avaya uses internal ISO-certified change control processes for software.
Review applications after operating system changes.	Avaya uses internal ISO-certified test procedures after operating system changes.
Restrict changes to software packages.	Avaya includes only the Linux software packages that Avaya needs. Avaya software is proprietary, and Linux software cannot be changed on an installed system. Standard program binaries are normally installed with write-only permissions to the super-user (root) and cannot be modified.
Prevent information leakage.	System Manager does not have antivirus, antiworm, or antitrojan software. Avaya does not recommend using third-party antivirus software. For more information, see **Protection against impact of viruses, worms and other malicious code**
Control outsourced software development.	Avaya software, if outsourced, is developed according to ISO-certified processes of Avaya.
Control your technical system vulnerabilities.	System Manager offers many features and processes to protect the customer communications network.

Considerations for customers who must comply with FISMA

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the requirements of the act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Federal Information Security Management Act of 2002 provides for development and maintenance of minimum controls required to protect federal information and information systems.

Telecommunications systems and commercially developed information security systems are included in the systems referenced under this act.

As a result, in most cases, government agencies can use the security-related features of Avaya to secure telecommunications data. System Manager Security features can also help prevent unauthorized access to the customer network, in general.

Features related to system security and documented in more detail in other sections of this document are:

Feature	Mapping to FISMA	Reference
Encryption	Protects transmitted data from packet-sniffing and eavesdropping and other unauthorized access.	See System Manager Encryption Overview on page 17.
System access control	Protects access to data from unauthorized personnel.	See Role-Based Access Control on page 25.
Authentication	Restricts access to the system by login and password.	See Administrative Accounts on page 43.
Logging	Logs security-related events.	See Audit Trails and Logs on page 35.
Firewall	Protects access to the network.	See Firewall.
Backup of data	Saves data on backup media or backup server. Protected by encryption and key.	See Backup and Restore on page 35.

Considerations for customers who must comply with HIPAA

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the requirements of the act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to disclose to health care recipients the ways in which the institution might use and disclose private information. HIPAA also requires health care providers to protect the privacy of certain individually identifiable health data for health care recipients.

System Manager Data to which HIPAA might apply includes customer names and telephone numbers, and called and calling number data.

Use of the following key features can protect patient privacy and demonstrate the health care provider's compliance with HIPAA.

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	See System Manager Encryption Overview on page 17.
System access control	Implement technical policies and procedures for electronic information systems that maintain electronically-protected health information to allow access only to those persons or software programs that have been granted access rights.	See Role-Based Access Control on page 25.
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	See Administrative Accounts on page 43.
Backup of data	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronically-protected health information.	See Backup and Restore on page 35.

Considerations for customers who must comply with PCI DSS

Note: This applies to standard global merchants and card processing service providers. Customers should rely on appropriate legal counsel and requirements of their card issuers for interpretation of the standards requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The PCI Data Security Standard (DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment card brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International, to help facilitate the broad adoption of consistent

data security measures on a global basis. This comprehensive standard is intended to help organizations proactively protect customer account data.

PCI does not apply to System Manager Data.

Considerations for non-US customers who must comply with regulations

Any specific country might have unique regulations that raise compliance issues for Avaya products. For example, countries such as Switzerland and Liechtenstein have Banking Secrecy laws that require a financial organization to inform a customer when the customer identity has been revealed or information that might reveal customer identity has been released. Such revelations can have negative effect on the business of a bank. Therefore, the communications services of a bank must be secure to prevent unauthorized access to data such as names, telephone numbers, and account codes. To that end, System Manager, through its authentication processes, access control, and encryption methods, can protect call detail records, as well as the calls to customers. In this way, Avaya can help a customer comply with banking secrecy laws and protect the integrity of its business. Avaya also offers these security features to protect administered data that might reveal customer identity, as might be the case, for example, if a customer IP address or phone number is contained within the firewall rules established for the product.

Basel II

Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework is a comprehensive set of banking standards compiled by the Basel Committee on Banking Supervision. The national banking overseers in many European countries seek to implement country-specific laws and procedures to meet the Basel II standards. To measure risk levels for a banking standards, Basel II mandates tracking of loss event data, which includes hacking of financial systems, theft of data, and impersonation. To this end, Avaya systems offer a number of security features, such as those described in the previous paragraph, to minimize loss event data, and therefore, risk level measurements.

For any country in which System Manager is sold, there might be a need to inform customers about System Manager Support for governmental regulations. In this case, the sales engineer or account executive should engage an Avaya legal officer, security specialist, or a compliance specialist to determine the specific ways in which System Manager might help the customer comply with regulations.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

The security properties of products are evaluated by competent and independent licensed laboratories to determine their assurance.

Supporting documents that are used within the Common Criteria certification process define how the criteria and evaluation methods are applied when certifying specific technologies.

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.

All the signatories of the CCRA recognize these certificates.

The CC Web portal (http://www.commoncriteriaportal.org/index.html) reports the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news, and events.

Appendix D: DoS methods designed by Avaya

A denial-of-service (DoS) attack occurs when the attacker attempts to make some resource too busy to answer legitimate requests or to deny legitimate users access to the system. Regardless of the method, the net effect of DoS attacks is to shut down a server or an application.

System Manager is resilient to the DoS attacks listed in the following table without rebooting or restarting, and without reloading. System Manager automatically recovers to full service after the DoS attack.

Attack type	Description
SYN flood (TCP SYN)	Phony TCP SYN packets from random IP addresses at a rapid rate fill up the connection queue and deny TCP services to legitimate users.
Land and LaTierra	The Land attack combines IP spoofing with opening a TCP connection. The Land attack sends a request to open a TCP connection (SYN flag in the header is on) but changes the IP address so that both the source and destination IP addresses are the same as the destination host IP address. When the destination host receives the packet, that host sets a SYN, ACK to itself because the destination and source IP addresses are the same with the same sequence number. The system expects a different sequence number related to the SYN, ACK packet from the other host, so the system keeps sending the ACK packet back expecting an updated sequence number. This process puts the host into an ACK loop. The LaTierra attack is similar to the Land attack but sends TCP packets to multiple ports at once.

Smurf / Pong	A large numbers of ICMP echo (ping) messages sent with the forged address of the intended victim, and Layer 2 devices issue an echo reply (pong), multiplying the traffic by the number of responding hosts.
Fraggle	Like Smurf, Fraggle is a UDP flood that uses an IP broadcast address of the victim (IP spoofing) that results in an infinite loop of echo and reply messages.
Jolt1 and Jolt 2	The Jolt2 attack raises the CPU utilization to 100% causing instability in the system until the Jolt2 attack stops. Most instances of this attack are from illegally fragmented packets: • If no port number is passed as an argument then Jolt2 sends illegally fragmented ICMP ECHO (pings) packets to the specified port. • If a port number is provided, then Jolt2 sends illegally fragmented UDP packets to the specified port. In both cases, Jolt2 sends a continuous stream of same fragmented packet in which • The fragment offset is 65520. • The TTL is set to 255. • The IP MF flag is set to zero. Due to these settings, the IP checksum of the last fragment equals zero, which is illegal. Jolt2 then sends 9 bytes of IP data including the IP header 20 bytes (total of 29 bytes) but sets the total length to 68 bytes. The offset and the packet length (65520 + 68) exceeds the maximum size of an IP datagram imposed by the 16-bit total packet length field in the IP header (maximum allowed packet size is 65563 bytes). This packet should fail the integrity check and discarded right away. However, some systems do not perform the integrity check and continue buffering these fragments. This process can utilize 100% of the CPU, and in some cases, the system crashes.
Packet replay attack	Packet replay refers to the recording and retransmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences because an intruder can replay legitimate authentication sequence messages to gain access to a system. An attacker can replay the same packet at different rates, and the system attempts processing duplicate packets causing

	• Total resource depletion • Termination of existing connections • Chaos or confusion or both in the internal buffers of the running applications • System crashes in some cases
Gratuitous ARPs	Most systems send out an Address Resolution Protocol (ARP) request for its own IP address to check for a duplicate IP address on the network. Some systems update their own ARP cache when systems receive a gratuitous ARP packet. The attacker uses this vulnerability to change the ARP table with the MAC address of the host router, so all the packets start to flow either through their system or with a invalid MAC address for a router or important server.
Teardrop, overlap, or fragmented packets	The teardrop and associated attacks exploit the packet reassembly code that breaks packets into smaller pieces (fragments) based on the maximum transmission unit (MTU) of the network. When reassembled, packets are often misaligned. The next fragment does not begin where the last fragment ended but inside the previous fragment memory allocation. This process causes memory allocation failures and the system crashes.
PING flood	Because so many ping utilities support ICMP echo requests and an attacker does not need much knowledge, sending a huge number of PING requests can overload network links.
Finger of death	The attacker sends finger requests to a specific computer every minute but never disconnects. Failure to terminate the connection can quickly overload the server process tables. The finger listen port number is 79 (see RFC 742).
Chargen packet storm	The attacker can spoof the chargen service port (19) from one service on one computer to another service on another computer causing an infinite loop and causing loss of performance or total shutdown of the affected network segments.
Malformed or oversized packets	Malformed packets attack attempt to deny service by causing protocol handlers to cease operation due to the difficulty the handlers have in processing odd formations of a protocol or the packets sent as part of the protocol. Oversized attacks place data in an order that is out of specifications, or create packets that are larger than the maximum

	allowed size.
OOB nuke	Continuous transmission of out-of-band packets with the TCP URGENT flag but without subsequent data to the most commonly attacked port (135-Netbios Session Service). Other ports are also possible targets.
SPANK	The target responds to TCP packets sent from a multicast address causing a DoS flood on the target network.
SNMP PROTOS	Utilizing the Protos SNMP tool to test SNMP code, an attacker can generate thousands of valid SNMP packets with strange and anomalous values that cause error conditions. See http://www.ee.oulu.fi

Appendix E: Product RPMs

The following table describes the list of RPMs required for the operation of System Manager.

basesystem	expat
glib2	python
libSM	dbus
libtermcap	compat-gnutls
ncurses	libXdmcp
sed	xorg-x11-filesystem
bzip2-libs	perl-IO-Tty
libcap	ntp
iptables	perl-XML-SAX
zip	libfontenc
gzip	fontconfig
libIDL	gamin-python
lm_sensors	db
ttmkfdir	openssh-askpass
gpm	openssh-server
ethtool	tmquantum-pki-service-installer
libFS	perl-IPC-Run
redhat-menus	libusb
xorg-x11-font-utils	postgresql92-libs
perl-Digest-HMAC	postgresql92-contrib
perl-HTML-Parser	kernel
centos-release-notes	glibc-common

perl-Net-DNS	mlocate
crash	vim-enhanced
perl-DBI	libselinux
libsoup	cairo
cyrus-sasl-plain	e2fsprogs-libs
unzip	libgssapi
file	pam
dos2unix	pam_krb
hdparm	cyrus-sasl-md5
liboil	parted
perl-Archive-Tar	libhugetlbfs
perl-XML-NamespaceSupport	libutempter
glib2	sgml-common
libgcc	htmlview
libart_lgpl	python-iniparse
libsepol	trousers
libcap	syslinux
audit-libs	vte
libacl	poppler
libsysfs	system-config-services
lm_sensors	system-config-language
gmp	perl-IO-Socket-SSL
hesiod	libgcj
cyrus-sasl-plain	vte
findutils	opensp
e2fsprogs	policycoreutils
cracklib	fipscheck-lib
pygobject	libnotify
logrotate	mkinitrd
tar	hwdata
device-mapper-multipath	gjdoc
pycairo	dmraid-events
audit-libs-python	man
libselinux-python	libbonobo
mtools	fipscheck-lib
udev	selinux-policy
wget	system-config-users
net-tools	hal
microcode	libbonoboui
tmpwatch	libgsf
xterm	kudzu

pyxf86config	oddjob-libs
audit	yum
cyrus-sasl-md5	yum-fastestmirror
libuser	gucharmap
cryptsetup-luks	firstboot-tui
alchemist	libbonoboui
pygtk	libgsf
libgcj	gucharmap
opensp	NetworkManager
gtk2-engines	NetworkManager-glib
python-urlgrabber	system-config-network
xsri	NetworkManager
zenity	xorg-x11-xfs
system-config-rootpassword	libXrender
trousers	unixODBC
libwnck	ftp
dmraid	xorg-x11-fonts-Type
pciutils	lua-devel
notify-python	perl-Config-Properties
libnotify	tcl
mkbootdisk	expect
oddjob	libksba
system-config-network-tui	pinentry
hal	password-sync-rpm
NetworkManager-glib	rrdtool
librsync	lua-rrdtool
python-libs	bash
dbus-libs	openssl
csync	libxml
libXau	nspr
perl-Net-OpenSSH	libX11
asgtools	nss
fontconfig	initscripts
groff	libXext
gamin	gdbm
libXdmcp	perl
openssh	mesa-libGL
perl-XML-Parser-EasyTree	bind-libs
ABG	libxml2-python
lua	mesa-libGLU
expect	foomatic

pth	libXft
net-snmp	gtk
perl-rrdtool	libxslt
uuid	dbus-glib
postgresql92-server	libicu
glibc	gnupg
popt	quota
openldap	krb5-workstation
util-linux	sudo
freetype	sos
ruby-libs	glibc
curl	openssl
ruby	libxml
pango	popt
libwpd	avahi
libvorbis	mesa-libGL
vixie-cron	gtk
rsync	libwpd
krb5-libs	gnutls
nspr	openldap
libpng	dbus-glib
avahi-glib	libexif
bind-libs	rsync
freetype	rpm
rpm-libs	rpm-libs
pango	setup
libgcc	chkconfig
filesystem	libstdc++
cracklib-dicts	audit-libs
termcap	libacl
zlib	tcp_wrappers
atk	dmidecode
mktemp	procps
libICE	iproute
libart_lgpl	libdaemon
info	bzip2
libsepol	shared-mime-info
readline	pcre
gawk	perl-Digest
libgpg-error	hmaccalc
cyrus-sasl-lib	cpio

libattr	iputils
elfutils-libelf	libevent
diffutils	perl-Net-IP
db4	crontabs
keyutils-libs	rmt
libsysfs	giflib
perl-Compress-Zlib	perl-XML-LibXML-Common
keyutils	sysfsutils
less	ed
binutils	time
grep	eject
ORBit	mkisofs
libvolume_id	libaio
perl-Socket	hesiod
iptables-ipv6	perl-IO-Socket-INET
vim-common	man-pages
libgomp	libICE
mingetty	readline
sgpio	libtermcap
libdrm	libdaemon
checkpolicy	ORBit
startup-notification	elfutils-libelf
perl-URI	libdmx
bitstream-vera-fonts	libsoup
perl-IO-Zlib	libcroco
perl-HTML-Tagset	gpm
perl-libwww-perl	libaio
nash	libselinux
centos-release	device-mapper
perl-XML-Parser	rhpl
libdmx	newt
bc	libgssapi
libtheora	libsemanage
perl-BSD-Resource	libuser
psutils	libselinux-utils
iptstate	usermode
pilot-link	ntsysv
attr	python-numeric
udftools	python-sqlite
libidn	lvm
mgetty	which

libcroco	mcstrans
mcelog	sysklogd
gmp	prelink
libgtop	at
traceroute	alchemist
pkgconfig	gettext
pax	parted
setserial	lsof
symlinks	device-mapper
dump	cracklib
grub	nfs-utils-lib
perl-Convert-ASN1	gettext
rootfiles	libpcap
zlib	pygtk2-libglade
atk	bitmap-fonts
libstdc++	libwnck
libSM	system-config-securitylevel
libgpg-error	poppler
ncurses	gtk2-engines
bzip2-libs	libbonobo
keyutils-libs	dbus-python
libattr	notification-daemon
libIDL	wpa_supplicant
libgomp	module-init-tools
libdrm	antlr
libX11	setools
startup-notification	selinux-policy-targeted
cyrus-sasl-lib	pm-utils
libvolume_id	pirut
libtheora	sqlite-devel
giflib	perl-Text-ASCIITable
pilot-link	dbus-libs
pcre	perl-Net-SFTP-Foreign
libgtop	perl-XML-LibXML
libevent	chkfontpath
libFS	libXrender
libidn	unixODBC
tcp_wrappers	yum-updatesd
liboil	openssh-clients
e2fsprogs-libs	perl-XML-Writer
shadow-utils	mkisofs

coreutils	libdbi
cairo	tcl
cryptsetup-luks	smem
libutempter	postgresql92
kpartx	tzdata
pam	krb5-libs
SysVinit	libgcrypt
libpcap	avahi
psmisc	libpng
ppp	gnutls
system-config-securitylevel-tui	wireshark
passwd	libXfont
authconfig	avahi-glib
nfs-utils-lib	libexif
m2crypto	bind-utils
yum-metadata-parser	nfs-utils
pyorbit	xinetd
python-elementtree	libgcrypt
tcsh	nss
device-mapper-event	mesa-libGLU
MAKEDEV	libxslt
iscsi-initiator-utils	ruby-libs
libsmi	libicu
perl-Net-SSLeay	rpm-python
dnsmasq	libhugetlbfs
portmap	PyXML
kbd	python-ldap
vim-minimal	readahead
irqbalance	psacct
rng-utils	gpg-pubkey
wdaemon	ecryptfs-utils
pam_krb5	ecryptfs-utils
sox	libtasn
sqlite	