Understanding HP SIM security

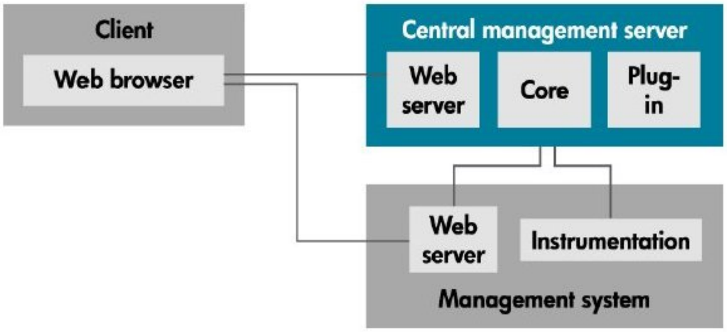
Overview

This document is provided as an overview of the security features available in the HP Systems Insight Manager framework. More detailed documentation can be found in the *HP Systems Insight Manager Technical Reference Guide*.

Architecture overview

HP Systems Insight Manager runs on a central management server (CMS) and communicates with managed systems using various protocols. The customer can browse to the CMS or directly to the managed system.

Figure 1. Architecture overview



Communication protocols

SNMP

SNMP v1 (Simple Network Management Protocol version 1) is one of the primary protocols used to gather data about systems. SNMP traps are used to notify HP Systems Insight Manager of status changes or other events on a system. SNMP is not a guaranteed protocol; there are no assurances that any request, response, or trap will reach its destination. SNMP security is limited to a clear-text community string included with the request, similar to a password. SNMP data is not encrypted, so the entire payload can be easily snooped on the network.

The operating system of the managed system may provide additional security capabilities for SNMP such as IP address restrictions for valid requests.

HTTP

HTTP (Hyper Text Transfer Protocol) is another primary protocol used to acquire data about managed systems during identification. HTTP is not a secure protocol and can be easily viewed on the network. The secure version of HTTP is called HTTPS and is described later.

WBEM

WBEM (Web-Based Enterprise Management) is another protocol used to acquire data about managed systems. It is primarily XML over HTTP or HTTPS.

DMI

DMI (Desktop Management Interface) is a legacy protocol for management data and has been largely superseded by WBEM. DMI is based on DCE/RPC (Distributed Computing Environment Remote Procedure Call) and is not secure.

RMI

Java™ RMI (Remote Method Invocation) is used within the CMS only for inter-process communication.

Remote Wake-Up

Remote Wake-Up refers to the ability to remotely turn on a system that is in a soft-off power state. Systems that support the Advanced Configuration and Power Interface (ACPI) should be awakened transparently by any network activity to the system. Alternatively, a system may support the Magic Packet technology. When a system is turned off, the Magic Packet–capable NIC is still powered on and monitoring traffic. If it receives the Magic Packet targeting it, the system will be powered on.

ICMP

ICMP (Internet Control Message Protocol) is used during automatic system discovery and prior to other requests to a system to ensure the system is responding. An ICMP echo request, also known as a *ping*, is sent to the system's IP address. Receipt of a proper reply indicates the system is up and responding.

IPX

The Service Advertising Protocol (SAP) is used to discover IPX systems. A SAP general service query for file server types is broadcast. Responses indicate the presence of one or more systems. A DiagRequest is used as a ping to IPX systems; a response indicates the system is up and responding.

Securing communication

Secure Sockets Layer (SSL)

SSL is an industry-standard protocol for securing communications across the Internet. It provides for encryption to prevent eavesdropping as well as data integrity to prevent modification, and it can also authenticate both the client and the server, leveraging public-key technology. All communications between the browser and the CMS are protected by SSL. HP Systems Insight Manager supports both SSL 3 and TLS 1.0 (Transport Layer Security).

Secure Shell (SSH)

SSH is an industry-standard protocol for securing communications. It provides for encryption to prevent eavesdropping plus data integrity to prevent modification, and it can also authenticate both the client and the server utilizing several mechanisms, including key-based authentication. HP Systems Insight Manager supports SSH 2.

HTTPS

HTTPS (Hyper Text Transfer Protocol Secure) refers to HTTP communications over SSL. All communications between the browser and HP Systems Insight Manager are carried out over HTTPS. HTTPS is also used for much of the communication between the CMS and the managed system.

Secure Task Execution and Single Login

Secure Task Execution (STE) is a mechanism for securely executing a command against a managed system using the Web agents. It provides authentication, authorization, privacy, and integrity in a single request. Single Login provides the same features but is performed when browsing a system. Secure Task Execution and Single Login are implemented in very similar ways. SSL is used for all communication during the STE and Single Login exchange. A single-use value is requested from the system prior to issuing the STE or Single Login request to help prevent against replay or delay intercept attacks. Afterwards, HP Systems Insight Manager issues the digitally signed Secure Task Execution or Single Login request. The managed system uses the digital signature to authenticate the HP Systems Insight Manager server. Note that the managed system must have a copy of the CMS SSL certificate imported into the Web agent and be configured to "trust by certificate" to validate the digital signature. SSL can optionally authenticate the system to HP Systems Insight Manager, using the system's certificate, to prevent HP Systems Insight Manager from inadvertently providing sensitive data to an unknown system.

NOTE to Insight Manager 7 users: Insight Manager 7 used the Automatic Device Authentication setting to control STE and Single Login access levels; these are replaced by tools in the new HP Systems Insight Manager authorization model. Any tool that requires STE access to the Web Agents includes it implicitly. For Single Login to Web Agents, the *Replicate Agent Settings* and *Install Software and Firmware* tools each provide administrator-level access to the Web Agents. *System Management Homepage As Administrator*, *System Management Homepage As Operator*, and *System Management Homepage As User* each provide Single Login access at the described level.

Distributed Task Facility

The Distributed Task Facility (DTF) is used for Custom Command tools and Multiple/Single-System Aware tools. Commands are issued securely to the managed system using SSH. Each managed system must have the CMS SSH public key in its trusted key store so that it can authenticate the CMS. Managed systems are also authenticated to the CMS by their SSH public key.

NOTE to HP Servicecontrol Manager Users: SSH replaces the existing signed RMI connections used by the DTF in HP Servicecontrol Manager. This adds a level of encryption and data integrity over signed RMI that was previously only available through the use of a secure network protocol such as IPSec.

WBEM

All WBEM access is over HTTPS for security. HP Systems Insight Manager is configured with a user name and password for WBEM agent access. Using SSL, HP Systems Insight Manager can optionally authenticate the managed system using its SSL certificate.

RMI

Java RMI is secured by requiring digitally signed requests using the CMS private key, which should only be available to the local system. All communications use localhost to prevent the communication from being visible on the network.

Certificate and key management

SSL certificates

Certificates generated by HP Systems Insight Manager and the Web Agents are by default self-signed. Public Key Infrastructure (PKI) support is provided so that certificates may be signed by an internal certificate server or a third-party Certificate Authority (CA).

Certificate sharing

HP Systems Insight Manager supports a mechanism whereby other components installed on the system can use the same certificate and private key, facilitating authentication of the system as a whole instead of each individual component. This is currently used by the Web Agents and the WBEM components on the CMS.

SSH keys

An SSH key-pair is generated during initial configuration. The CMS public key is copied to the managed system using the mxagentconfig tool. This key-pair is not the same as for SSL and requires a manual process to regenerate a new pair. Refer to the man pages or online documentation for mxagentconfig for more details.

Browser

SSL

All communication between the browser and the CMS or any managed server occurs using HTTPS over SSL. Any navigation using HTTP (not using SSL) is automatically redirected to HTTPS.

Cookies

Although cookies are required to maintain a logged in session, only a session identifier is maintained in the cookie. No confidential information is in the cookie. The cookie is marked as secure, so it is only transmitted over SSL.

Passwords

Any password fields displayed by HP Systems Insight Manager do not display the password. Passwords between the browser and the CMS are transmitted over SSL.

Browser warnings

There are several types of warnings that can be displayed by the browser or by the Java plug-in on the browser, most having to do with the SSL server certificate.

Untrusted system

This warning indicates the certificate was issued by an untrusted system. Since certificates are by default self-signed, this is likely if you have not already imported the certificate into your browser. In the case of CA-signed certificates, the signing root certificate must be imported. The certificate can be imported before browsing if you have obtained the certificate by some other secure method. The certificate can also be imported when you get the warning, but is susceptible to spoofing since the host system is not authenticated. Do this if you can independently confirm the authenticity of the certificate or you are comfortable that the system has not been compromised.

Invalid certificate

If the certificate is invalid because it is not yet valid or it has expired, it could be a date/time problem, which could be resolved by correcting the system's date and time. If the certificate is invalid for some other reason, it may need to be regenerated.

Host name mismatch

If the name in the certificate does not match the name in the browser, you may get this warning. This can be resolved by browsing using the system's name as it appears in the certificate, for example, marketing1.ca.hp.com or marketing1. Refer to the System link format section below for information on changing the format of names created in links by HP Systems Insight Manager.

Signed applet

Previous versions of HP Systems Insight Manager use a Java plug-in that may additionally display a warning about trusting a signed applet. Those previous versions of HP Systems Insight Manager use an applet signed by Hewlett-Packard Company, whose certificate is signed by Verisign.

Browser session

By default, HP Systems Insight Manager does not time-out a user session while the browser is displaying the HP Systems Insight Manager banner. This is known as monitor mode, and allows a continuous monitoring of the managed systems without any user interaction. The session times-out after 20 minutes if the browser is closed or navigates to another site.

An active mode is also supported where the session times out after 20 minutes if the user does not interact with HP Systems Insight Manager, by clicking a menu item, link or button. You can enable active mode by editing the globalsettings.props file and setting EnableSessionKeepAlive to false.

Best security practices include care when visiting other web sites. You should use a new browser window when accessing other sites; when you are finished using HP Systems Insight Manager you should both log out and close the browser window.

System link format

To facilitate navigation to managed systems, HP Systems Insight Manager provides the System Link Configuration option to configure how links to managed systems are formed. Go to **Options→Security→System Link Configuration**.

Three options are available:

- Use the system name
- Use the system IP address
- Use the system full DNS name

If you need full DNS names to resolve the system on your network, keep in mind that the browser might display a warning if the name in the system's certificate does not match the name in the browser.

Operating-system dependencies

User accounts and authentication

HP Systems Insight Manager accounts are authenticated against the CMS host operating system. Any operating system features that affect user authentication will affect signing into HP Systems Insight

Manager. The operating system of the CMS can implement a lock-out policy to disable an account after a specified number of invalid sign in attempts. Additionally, an account can be manually disabled in the Microsoft® Windows® domain. Any account that cannot authenticate against the operating system prevents signing into HP Systems Insight Manager using that account.

NOTE: A user who is already signed into HP Systems Insight Manager is not re-authenticated against the operating system until the next sign in attempt and continues to remain signed into HP Systems Insight Manager, retaining all rights and privileges therein, until signing out of HP Systems Insight Manager.

IMPORTANT: If creating operating system accounts exclusively for HP Systems Insight Manager accounts, give users the most limited set of operating system privileges required. Any root or administrator accounts should be properly guarded. Configure any password restrictions, lock-out policies, and so on, in the operating system.

File system

Access to the file system should be restricted to protect the object code of HP Systems Insight Manager. Inadvertent modifications to the object code can adversely affect the operation of HP Systems Insight Manager. Malicious modification can allow for covert attacks, such as capturing sign in credentials or modifying commands to managed systems. Read-level access to the file system should also be controlled to protect sensitive data such as private keys and passwords, which are stored in a recoverable format on the file system. HP Systems Insight Manager does not store user account passwords for users signing into HP Systems Insight Manager.

IMPORTANT: HP Systems Insight Manager sets appropriate restrictions on the application files. These restrictions should not be changed because this could affect the operation of HP Systems Insight Manager or allow unintended access to the files.

Background processes

On Windows, HP Systems Insight Manager is installed and runs as a Windows service. By default, it runs using the administrator account used during product installation. On UNIX, HP Systems Insight Manager is installed and runs as daemons running as root.

Windows Cygwin

The version of Cygwin provided with the SSH server for Windows, for CMS and the managed systems, has been modified with security enhancements to restrict access to the shared memory segment. As a result, it does not interoperate with the generally available version of Cygwin. Only administrative users can connect to a system running the modified SSH server.

HP-UX/Linux

The device /dev/random is used, if available on the CMS, as a source for random numbers within HP Systems Insight Manager.

Database

Access to the database server should be restricted to protect HP Systems Insight Manager data. Specify appropriate non-blank passwords for all database accounts, including the system administrator (sa) account for SQL Server. Changes to the operating data, such as authorizations, tasks, and collection information, can affect the operation of HP Systems Insight Manager. System data contains detailed information about the managed systems, some of which might be considered restricted including asset information, configuration, and so on. Task data might contain extremely sensitive data, such as user names and passwords.

SQL Server/MSDE

HP Systems Insight Manager uses only Windows authentication with SQL Server and MSDE. The installation of MSDE creates a random password for the sa account, though it is not used for HP Systems Insight Manager.

Remote SQL Server

SQL Server 2000 supports advanced security features, including SSL encryption during sign in and data communication. More information can be found in SQL Server documentation and the *Microsoft SQL Server 2000 Security White Paper*, available from the Microsoft website.

PostgreSQL

PostgreSQL uses a password that is randomly generated when HP Systems Insight Manager is installed. This password can be changed through the command line. Refer to the mxpassword reference for more information.

Oracle

The Oracle database administrator must create a user (preferably with a non-blank password) for HP Systems Insight Manager to use when connecting to Oracle. The Oracle user must have, at the minimum, the Connect and DBA roles, which allow HP Systems Insight Manager to have the correct privileges to create and delete HP Systems Insight Manager tables and views, along with read/write access to the HP Systems Insight Manager tables. Changes to the operating data, such as authorizations, tasks, and collection information, can affect the operation of HP Systems Insight Manager. System data contains detailed information about the managed systems, some of which might be considered restricted, including asset information, configuration, and so on. Task data can contain extremely sensitive data, such as user names and passwords.

Auditing

The HP Systems Insight Manager audit log contains entries for important system activities, such as executed tasks, authorization modifications, user sign in and sign out, and so on. Tools by default are configured so that results are logged to the audit log, but their tool definition files can be modified so that this is not the case.

Command-line interface

Much of HP Systems Insight Manager's functionality can be accessed through the command line. To access the command-line interface, you must be logged on to the CMS using an operating system that is a valid HP Systems Insight Manager user account. That account's authorizations and privileges within HP Systems Insight Manager apply to the command line interface as well.

NOTE: On a Windows system, the operating system account must have administrator-level access on the CMS for all of the commands to work properly.

How-to: configuration checklist

General

- Configure firewalls to allow desired ports/protocols.
- Review lockdown versus ease of use.
- After configuring the CMS and managed systems, run discovery on the CMS.

Configure CMS

- Inspect SSL server certificate and update if desired.
- Configure WBEM passwords and SNMP community strings in global protocol settings. Refer to the Configure CMS for managed systems section below.
- Configure user accounts, based on operating system accounts that will access HP Systems Insight Manager.
- Review and configure toolboxes if defaults are not appropriate.
- Review and configure authorizations for users.
- Configure system link configuration format.
- Review audit log.

Strong security

NOTE: see How-to: lockdown versus ease of use for more details)

- Enable Require Trusted Certificates, inspect and import desired system SSL certificates or root signing certificates.
- Require only known SSH keys, inspect and import desired system SSH public keys.

Configure managed systems

- Configure SNMP community strings, which are required at the CMS.
- For WBEM on HP-UX and Linux, configure the WBEM password. This password is required at the CMS. For the highest level of security, a different user name and password can be used for each managed system; each user name and password pair must be entered into the CMS to enable access.
- The CMS requires a user name and password to access WMI data on Windows systems. By default, a domain administrator account can be used for this, but you should use an account with limited privileges for WMI access. You can configure the accounts accepted by each Windows managed system by using the Computer Management tool:
  1. First select the WMI Control item
  2. Right-click **WMI Control** and select **Properties**
  3. Select the **Security** tab, select **Root namespace**, and click **Security.**
  4. Add a user to access WMI data along with their access rights. The enable account and remote enable permissions must be enabled for correct operation of HP Systems Insight Manager.
  5. The user name and password specified here must be configured in the CMS.
- Set up user accounts for Insight Web Agents.
- Add CMS SSH public key to the system's trusted key store by running mxagentconfig on the CMS.
- Configure trust relationship option for Insight Web Agents; import CMS SSL certificate if set to trust by certificate.

Configure CMS for managed systems

The CMS must be configured with the user name and password used for WBEM and WMI access, and for the SNMP community names. These can be set using the Global Protocol Settings page if a common user name and password or community name is used across all the systems in the network, or individually for systems using the System Protocol Settings page. Both of these are accessible from the **Options→Protocol Settings** menu. The command line tool mxnodesecurity can also be used to configure these settings. Refer to the man page or online documentation for details.

IMPORTANT: Any passwords specified in the Global Protocol Settings page are used during system identification. Sensitive passwords, such as root or domain administrator passwords, should not be specified here if there is a risk of sending these to untrustworthy systems.

How-to: lockdown versus ease of use

Moderate

The Insight Management Agents should be configured to trust by certificate. This requires distributing the HP Systems Insight Manager certificate, which includes the public key, to all the managed systems. Once the systems have been configured to trust the HP Systems Insight Manager system, they will accept secure commands from that particular system only.

This certificate can be distributed in a number of different ways including:

1. Use the Web-based interface in an individual Insight Management Agent to specify the HP Systems Insight Manager system to trust. This causes the agents to pull the digital certificate from the HP Systems Insight Manager system immediately, enables you to verify it, and then sets up the trust relationship. While this option does have some limited vulnerability, it would be possible to spoof the HP Systems Insight Manager system at the time the certificate is pulled and thus set up an unexpected trust relationship. However, it is reasonably secure for most networks.
2. Import the HP Systems Insight Manager certificate during initial installation of the Insight Management Agents. This can be done manually during an attended installation or through the configuration file in an unattended one. This method is more secure because there is little opportunity for the spoofing attack described above.
3. If you have already deployed the Insight Management Agents, you can distribute the security settings file and the HP Systems Insight Manager certificate directly to the managed systems using OS security.

IMPORTANT: When using the Trust by certificate option, the HP Systems Insight Manager SSL certificate must be redistributed if a new SSL certificate is generated for the CMS. SSH on the managed system normally operates in a mode similar to trust by certificate in that it requires the SSH public key from the CMS. Note that the SSH public key is not the same as the SSL certificate. The command mxagentconfig is used on the CMS to copy the key to the managed system. This must be done for each user account that is to be used on the managed system since the root or Administrator account is used by default.

IMPORTANT: The HP Systems Insight Manager SSH public key must be redistributed if the SSH key-pair is regenerated.

Strong

The strong security option lets you take advantage of every security feature. This option provides the highest level of security available within the HP Systems Insight Manager security framework, but there are some additional procedural steps you must make in your server operations. Also, this option is facilitated by using your own PKI that includes a certificate authority and certificate server.

1. First, you must generate certificates from your certificate server for each managed system and the HP Systems Insight Manager system. To do this, first generate a certificate signing request (CSR) from the various systems. This generates a PKCS#7 file. This file should then be taken to the certificate server and signed, and then the resulting file (generally a PKCS#10 response) should be imported into the each managed system and the HP Systems Insight Manager system.

   IMPORTANT: To maximize security, it is important that none of these steps be done over a network unless all communications are already protected by some other mechanism.

   Thus, in the case of the Insight Management Agents, a floppy disk should be taken directly to the managed system, have the PKCS#7 file placed on it, and hand-carried to a secure system with access to the certificate server. The PKCS#10 response file should similarly be placed on the floppy disk and returned to the managed system to be imported into the Insight Management Agents.

2. Take the root certificate (just the certificate, not the private key) of your certificate server and import that into the HP Systems Insight Manager trusted certificate list. This allows HP Systems Insight Manager to trust all the managed systems because they were signed with this root certificate.
3. Take the certificate from the HP Systems Insight Manager system and import it into the Insight Management Agents of each system. This allows the managed systems to trust the HP Systems Insight Manager system. This certificate can be distributed using any of the methods available to distribute the HP Systems Insight Manager certificate. However, the option to pull the certificate directly from the HP Systems Insight Manager system over the network must be avoided due to the potential *man-in-the-middle* attack.
4. Once these steps have been completed, you can turn on the option in HP Systems Insight Manager to enable Require Trusted Certificates. Select **Options→Security→Certificates→Trusted Certificate**. The warnings presented around this option make it clear that any managed system that does not have a certificate signed by your certificate server will not be sent secure commands from the HP Systems Insight Manager system, although it will be monitored for hardware status.

   IMPORTANT: As in the Moderate option, you need to redistribute the HP Systems Insight Manager SSL certificate to the managed systems whenever a new HP Systems Insight Manager SSL certificate is generated.

5. For SSH, turn on the option to accept SSH connections only from specified systems. Select **Options→Security→SSH Keys** and enable the option **The central management server will accept an SSH connection only if the key is in list below**. Afterwards, you must manually import each managed system's public SSH key into the list of keys in HP Systems Insight Manager.

   NOTE: To configure this in previous version of HP Systems Insight Manager, add or modify the following line in mx.properties:

   ```
   MX_SSH_ADD_UNKNOWN_HOSTS=false
   ```

and then restart HP Systems Insight Manager.

Afterwards, you must manually import each managed system's public SSH key into the list of keys in HP Systems Insight Manager.

Port listing

The following ports and protocols are used by the HP Systems Insight Manager solution.

CMS		**Managed System**		**Port**	**Protocol**	**Description**
In[2]	Out	In	Out		ICMP[1]	Ping
	Y	Y		22	SSH	SSH server (for DTF)
	Y	Y		161	SNMP	SNMP Agent
Y			Y	162	SNMP Trap	Trap listener
	Y[4]	Y		80	HTTP	Management processor and other devices; standard Web server
Y	Y[4]	Y		280	HTTP	Web server for HP Systems Insight Manager; Web agent auto-start port
	Y[4]	Y		443	HTTPS	Management processor and other devices; standard Web server
	Y			1443		Microsoft SQL Server database
	Y	Y		2301	HTTP	Web agent Web server
Y[3]				2367	RMI	HP Systems Insight Manager RMI connection
	Y	Y		2381	HTTPS	Web agent Web server
	Y			5432		ProstgreSQL Server database
	Y	Y		5988	HTTP	WBEM service
	Y	Y		5989	HTTPS	WBEM service
Y				50000	HTTPS	HP Systems Insight Manager Web server
Y				50001	HTTPS	HP Systems Insight Manager SOAP (configurable[6])
Y				50002	HTTPS	HP Systems Insight Manager SOAP with client certificate authentication (configurable[7])
Y				50003	HTTP	HP Systems Insight Manager SOAP (configurable[8])
Y			Y	50004	HTTPS/HTTP	WBEM event receiver (configurable)
Y				50005	WBEM	WBEM Events
Y				50006	PostgreSQL	PostgreSQL
Y				50008	SIM JMS	JMS port
Y				50009	SIM JNDI	JNDI port

	Y	Y		50010	DMI[5]	DMI
				50013	RMI	Web Services RMI Loader
				50014	JRMP	JRMP Invoker
				50015	Pooled invoker	Pooled invoker
	Y[4]	Y		411	HTTP	IBM Director agent
	Y[4]	Y		1311	HTTPS	Server administrator
	Y[4]			2069	HTTP	OSEM
	Y[4]	Y		3202	HTTPS	StorageWorks NAS
	Y[4]	Y		3257	HTTPS	Rack & Power Manager
	Y[4]	Y		4095	HTTP	CommandView ESL
	Y[4]	Y		4096	HTTP	CommandView SDM
	Y[4]	Y		8000	HTTP	HP Web letAdmin
	Y[4]	Y		8008	HTTP	Default home page
	Y[4]	Y		8443	HTTPS	HP Web JetAdmin

NOTES:

[1] All ports are for TCP and UDP (except ICMP).

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

[3] RMI port is used within the CMS for inter-process communication. Connections from outside the CMS are not accepted, and firewalls may block this port.

[4] Many CMS outgoing ports are used for discovery.

[5] The exact UDP/TCP ports used by DMI are dynamic and vary from system to system, but they tend to be around 32,780 and higher.

[6] Port number is configurable in mx.properties using MX_SOAP_PORT.

[7] Port number is configurable in mx.properties using MX_SOAP_SSO_PORT.

[8] Port number is configurable in mx.properties using MX_SOAP_HTTP_PORT; port can be enabled/disabled in globalsettings.props using HTTP_SOAP_PORT_ENABLE with “true” or “false.”

NOTE: It is not recommended that you enable management protocols such as SNMP or DMI on systems outside your firewall or directly connected to the Internet.

Vulnerability and Patch Management Pack firewall ports

HP SIM Server

The following ports must be open on the HP SIM server.

Port	Protocol	Description
280	TCP	HP SIM HTTP port
50000	TCP	HP SIM HTTPS port
5989	TCP	HP SIM Web-Based Enterprise Management (WBEM)/WMI Mapper Secure Port
22	TCP	HP SIM SSH port
50001	TCP	HP SIM secure Simple Object Access Protocol (SOAP) port
161	TCP/UDP	SNMP
162	TCP/UDP	SNMP traps

VPM Server

The following ports must be open on the VPM server.

NOTE: The following ports are applicable to the CMS only.

MSDE

Port	Protocol	Description
445	TCP	MSDE Named Pipes Communications
1434	UDP	MSDE Shared Instance Support
variable	TCP	MSDE TCP/IP Communications

VPM must be able to access the following websites through your firewall:

- http://www.microsoft.com
- https://ftp.hp.com
- http://support.microsoft.com
- http://rhn.redhat.com
- http://www.cve.mitre.org
- http://www.itrc.hp.com
- http://www.msus.windowsupdate.com
- http://download.microsoft.com/
- https://www.hp.com/
- http://managementsoftware.hp.com

For more information, refer to the following sources:

- http://www.microsoft.com/sql/techinfo/administration/2000/security/winxpsp2faq.asp
- http://support.microsoft.com/default.aspx?kbid=839980

Harris STAT® Scanner Engine

Port	Protocol	Description
443	TCP	HTTPS port
80	TCP	HTTP port
135, 137, 138, 139, 445	TCP and UDP	File and Printer Sharing for Microsoft Networks

Radia Patch Manager

Port	Protocol	Description
3464	TCP	Configuration Server
3466	TCP	Radia Management Portal

Target nodes

The following ports must be open on the target nodes.

Scanner Access (Target Nodes)

Port	Protocol	Description
135, 137, 138, 139, 445	TCP and UDP	File and Printer Sharing for Microsoft Networks
135, 137, 138, 139, 445	TCP and UDP	Remote Registry service
	IPC$, ADMIN$, C$	Default admin shares must be enabled

HP Systems Insight Manager

Port	Protocol	Description
161	TCP/UDP	SNMP
162	TCP/UDP	SNMP traps
2301, 2381, 49400	TCP	HP Proliant Agents

Radia Patch Manager

Port	Protocol	Description
3465	TCP	Radia Agent
3463 (remote exec)	TCP	Agent deployment

Virtual Machine Management Pack ports

The Virtual Machine Management Pack uses the following ports:

Port	Protocol	Description
1124	TCP and UDP	HP VMM Control **Note:** This port is applicable to CMS only.
1125	TCP and UDP	HP VMM Agent **Note:** This port is applicable to CMS and managed systems.
1126	TCP and UDP	HP VMM Agent **Note:** This port is applicable to CMS and managed systems.

NOTE:

- Communication between browsers and the VMM Web Service uses HTTPS over port 50010.
- Communication between the VMM Web Service and the VMM Service (both on the HP SIM CMS) uses SSL over port 1124.
- Communication between the VMM Service and VMM agent (on virtual machine hosts) uses SSL over ports 1125 and 1126.
- Communication between the VMM agent during a virtual machine move or copy operation uses SSL over port 1126.

Integrated Lights-Out (iLO) ports

The following ports are used by iLO. Disabling certain features of iLO will affect the list of ports actually opened by iLO. Refer to the *Integrated Lights-Out Security* technology brief located at: http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf

Port	Protocol	Description
22	SSH	iLO text / CLI
23	Telnet	Remote console; virtual serial port
80	HTTP	HTTP interface
161	SNMP	SNMP GET/SET
162 (out)	SNMP	SNMP trap
443	HTTP/SSL	HTTPS interface; encrypted XML access
636 (out)	LDAP/SSL	Secure LDAP to directory server
3389	Terminal Service	Terminal Services session (software-based remote console using Windows)
17988	Virtual Media	Virtual Media

5982-3225EN, 05/2006