HP Instant Support Enterprise Edition

Advanced Configuration

Security white paper

A.03.90

Executive overview 2
Security design 3
Security technology 3
ISEE architecture 4
Firewall requirements 4
Summary 6
For more information 6

Executive overview

Today's IT department plays a central role in meeting business objectives. Leveraging your IT infrastructure investments and improving overall system availability and utilization are crucial in today's business environment. HP Instant Support Enterprise Edition (ISEE) simplifies the management of highly diverse IT environments by providing a single remote monitoring and support solution for multiple operating systems and technologies, thereby reducing cost and complexity. HP ISEE provides features to manage diverse environments ranging from simple to complex, including mission-critical and multivendor IT environments.

HP ISEE is a support solution that enables the delivery of HP remote monitoring and support over the Internet. Today, many security-sensitive transactions—such as e-commerce, stock trades, and online banking—are executed securely over the Internet using the same industry-standard security technology utilized in ISEE by HP.

HP understands your company's security concerns and has leveraged its experience as a technology leader to create a secure remote support solution. To enhance the safety and integrity of your enterprise networks and support data, HP has incorporated a number of security technologies into the HP ISEE design. HP provides a multilevel, layered security structure through encryption, authentication, industry-standard security protocols, and best practices integrated at the physical, network, application, and operational levels. Transactions between HP and your enterprise network are restricted and tightly controlled through a single, secure access point. HP's remote monitoring and support capabilities, along with any support information collected, are used only to provide you with world-class HP support.

Support features

HP ISEE offers:

- **Remote hardware event management.** Diagnostic software monitors the status of your hardware and generates notification events when predetermined conditions are detected for supported servers, connected peripherals, and storage devices connected to supported systems[1]. Notification events are received by agent software installed on the monitored system at the customer site and then forwarded to HP for review and possible support action. This capability helps identify potentially critical problems before they occur and prevent them, increasing your system uptime.
- **Remote execution of diagnostic scripts.** A diagnostic engine installed on a monitored client is able to remotely execute support scripts that can diagnose problems on supported servers, connected peripherals, and storage devices, providing timely solutions to your problems. Additional system configuration information is collected for troubleshooting and faster resolution of problems on supported monitored servers running HP-UX; HP Netservers and HP ProLiant servers running Microsoft® Windows® or Red Hat Linux®; and HP Integrity servers. The execution of remote diagnostic and configuration scripts is controlled and scheduled by the customers.
- **Remote network access for HP support engineers.** (*Advanced Configuration only*) ISEE offers several options for establishing a secure connection between HP and your network, allowing an HP support engineer—with your authorization—to remotely access your monitored systems and devices. The HP support engineer can log in to your system, observing normal customer security procedures and permissions, in order to provide remote hardware or software support for faster resolution of problems. One connection option is a Virtual Private Network (VPN) terminated at an HP-provided VPN device deployed in the customer "demilitarized zone" (DMZ); another is a Secure Shell (SSH2) tunnel terminated at a customer-owned customer access server (CAS) deployed either in the customer DMZ or on a trusted network.

[1] Virtual array (VA) storage devices connected to systems with Intel® Itanium® 2 processors or running HP-UX 10.20 are not supported.

Security design

The HP ISEE security architecture design restricts access, authenticates users, authorizes appropriate use, and provides detailed logging, auditing, and activity reporting. A combination of security technology and operational policy controls reduces security risk.

The HP ISEE architecture adheres to security design principles in the following areas:

- Data privacy
- Data integrity
- User authentication
- Content authenticity and integrity
- Detailed logging and auditing
- Comprehensive operational security

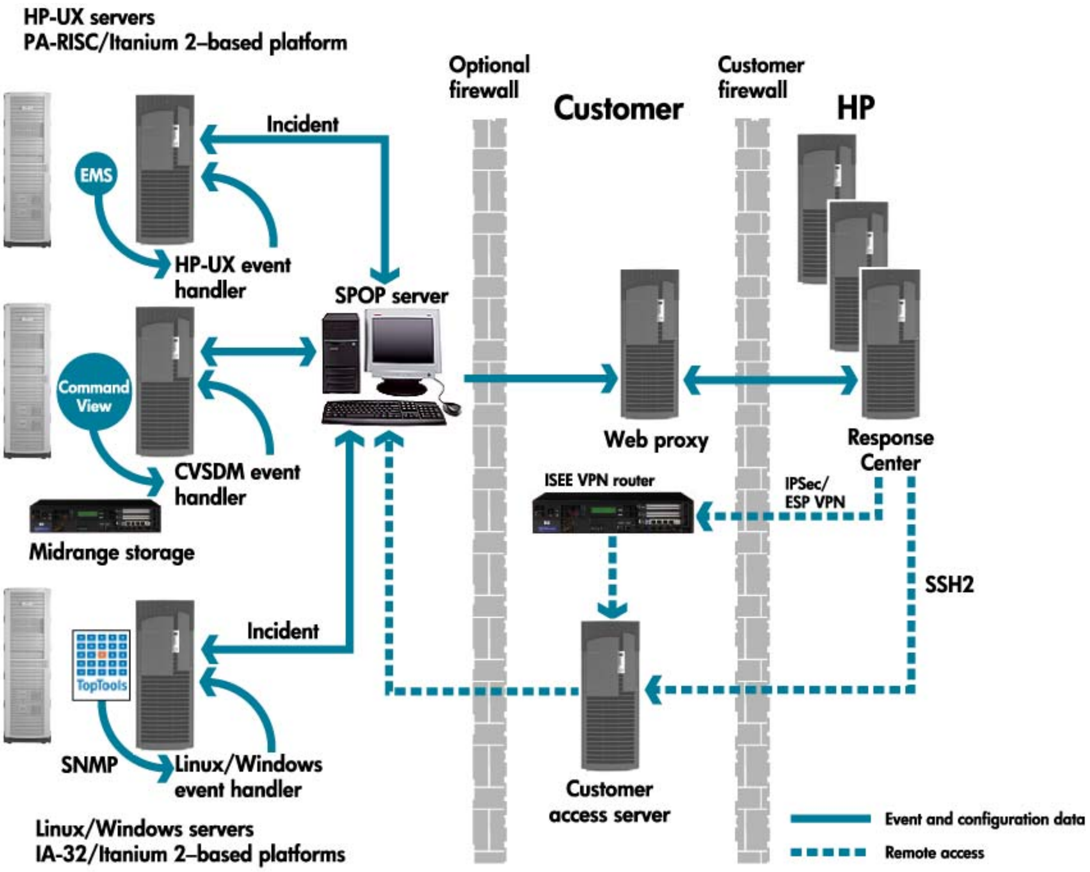
Security technology

HP ISEE Advanced Configuration utilizes the following industry-standard encryption and authentication technologies:

- Secure Sockets Layer 3.0 (HTTPS/SSL)
- X.509 Digital Certificate Standard
- MD5 Message Digest
- RC4 128-bit private-key encryption
- RSA 2048-bit public-key encryption
- Secure Shell (SSH2) with 3DES encryption
- IPSec Virtual Private Network
- RADIUS Authentication

ISEE Advanced Configuration architecture

Figure 1. The following diagram depicts the ISEE Advanced Configuration architecture. Not all supported platforms or remote access technologies are depicted.



Firewall requirements

The following tables reflect the ISEE firewall port requirements for each supported ISEE configuration. Depending on the configuration selected by the customer, these port requirements may be at the customer's Internet firewall or at both Internet and internal firewalls, if a DMZ configuration is selected.

All transmission control protocols (TCPs) assume return communication is permitted for "established" network connections. Specific IP address information for HP support servers will be provided to assist with configuring the firewall rules.

The enterprise SPOP (support point of presence) configuration is the *recommended* model for full ISEE support functionality. This configuration utilizes an SPOP server installed within the customer's enterprise (internal) network. The SPOP server is an HP-provided, Intel-based HP ProLiant workstation running the Windows 2000 Advanced Server operating system. The platform is security hardened using various security tools, such as ISS Lockdown, Microsoft Baseline Security Analyzer (MBSA), and Norton Antivirus, as well as all current operating-system platform security patches and hotfixes. The SPOP configuration enables centralized collection and administration of hardware events that are transmitted to HP, and it provides a central repository of HP support tools for use in the delivery of remote HP support services in the customer's environment.

Listed firewall port openings are required at the customer's *Internet*-facing firewall. No additional firewall restrictions prevent communication between the SPOP server and the Internet for listed ports:

Enterprise SPOP configuration **Customer Internet firewall**				
Service	Protocol	Port	Direction	Feature
https *	tcp	443	outbound **	Transport of hardware events to HP, synchronization of hardware event status from HP to SPOP server, synchronization of diagnostic script execution requests from HP to SPOP server, synchronization of diagnostic script execution results from SPOP server to HP

* Encrypted prior to transport with 128-bit RSA RC4 using SSL protocol

** Can utilize customer Web proxy

Remote access VPN **Customer Internet firewall**				
IPSec IKE	udp	500	bi-directional	VPN Internet Key Exchange (establish shared security parameters and authentication keys for remote access VPN)
IPSec ESP	50	none	bi-directional	VPN Security (provide confidentiality, data integrity, and authentication of IP packets for remote access VPN)

Remote access Secure Shell (SSH2) **Customer Internet firewall**				
SSH	tcp	22	inbound *	Secure Shell (provide confidentiality, data integrity, and authentication of IP packets)

* Specific IP address information for HP servers will be provided to assist with firewall rules

The DMZ SPOP configuration is an *exception-based option* for customers with heightened security concerns and no requirements for certain ISEE enterprise management and monitoring features[2]. This model utilizes an SPOP server installed within the customer's DMZ network. While the recommended configuration consists of the SPOP system in the enterprise and the VPN hardware in the DMZ, should customer security requirements mandate that the SPOP server be deployed in the DMZ, this option will be evaluated based on customer needs and may potentially be deployed on an exception basis. However, certain enterprise management and monitoring features cannot be supported on a DMZ SPOP server without additional firewall port requirements[2].

[2] HP Services customers who require the following HP support services must choose the enterprise SPOP configuration or open additional firewall ports to enable full functionality: Network Assessments, Network Availability Monitoring (NAM), Network Environment Services (NES), SANScan (Configuration Gathering for SANs), SANmaster (event management for SANs and Brocade switches), Storage Managed Services (storage backup services), Unreachable Device Notification (UDN), and HP ProLiant Server support.

DMZ SPOP configuration requires that all firewall ports listed in the Enterprise SPOP table be opened at the customer's Internet-facing firewall and that the following additional ports be opened at the customer's *internal* firewall:

DMZ SPOP configuration **Customer internal firewall**				
Service	**Protocol**	**Port**	**Direction**	**Feature**
http *	tcp	80	outbound **	Hardware event transport from monitored clients in the enterprise to SPOP server in the DMZ

Optional functionality				
ssh	tcp	22	inbound	Remote support using Secure Shell, Secure File Transfer from SPOP server in DMZ to supported clients in the enterprise *(requires customer-installed SSH server)*
rdp	tcp	3389	outbound	Centralized enterprise view of hardware events on SPOP server *(using Terminal Services from customer desktop to SPOP server in DMZ)*
smtp	tcp	25	inbound	Customer approval of diagnostic script execution requests by HP *(not required when customer has an SMTP mail server in DMZ)*

* Encrypted with 128-bit RC4 by HP client software prior to transport

** Can utilize customer Web proxy

Summary

Utilizing proven security technology, the ISEE architecture is a secure e-business infrastructure that leverages your company's Internet connectivity to provide a high-bandwidth, secure HP remote support solution.

For more information

For more information on HP Instant Support Enterprise Edition, visit us at:
www.hp.com/go/instantsupport

The list of supported products can be found in the ISEE Getting Started Guide at:
www.hp.com/learn/isee

For more information on HP Services, contact your local HP Account Support Team or any of our worldwide sales offices, or visit us at:
www.hp.com/go/services

5982-8918EN, 10/2004