HP Instant Support Corporate Edition

Security

invent

Overview

HP Instant Support Corporate Edition (ISCE) is a tool that offers a suite of web based trouble-shooting capabilities that identifies, diagnoses, and resolves computing problems. It is designed specifically for implementation within a company's distributed IT environment for business desktop support.

HP has placed significant investment into providing a secure HP ISCE architecture. HP understands your company's security concerns, and has leveraged its experience as a technology leader to make its support solution secure.

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

To address the safety of our support customer's networks and support data, [delete extra spacing]

HP incorporated a number of security technologies into the HP ISCE design. Encryption, authentication, and industry standard security protocols and best practices are integrated at the physical, network, application, and operational levels, providing a multi-level, layered security structure.

HP's support capabilities, and the support information collected, are utilized solely to provide you with world-class HP support. The HP ISCE architecture design protects both you and HP, while providing HP the capabilities necessary to quickly resolve your critical support issues.

Support Models

HP currently offers two implementation models with ISCE: The local model and the hosted model. In the hosted model, HP servers are used to host the ISCE server components, the backend database, and the content web pages. In the local model, all components are installed inside the company's network.

Self solve

Depending on the nature of the problem, end users can attempt to resolve their own issues by using the various suite of tools. These tools are designed to be very intuitive for an average end user to use.

Assisted solve

If the end user is unable to resolve a problem, the tool allows a seamless escalation to the next level of support. This is generally internal corporate support.

Collaborative support

If corporate support is having difficulty resolving the issue, they have the option to escalate via the tool to the next level of support. This next level of support could be HP, or a higher tier within their support structure. All information to date around the case is electronically sent to the next level. This includes the gathered system data, chat session, diagnostic results, etc. The helpdesk agent is now in a chat session with the next level of support on behalf of the end user to resolve the issue.

Remote control

The remote control feature provides call center agents access to the end-user desktop allowing them to share mouse, keyboard and the end-user display. Remote control capability is provided with a push installation of a host service to NT Server based systems. For other Microsoft operating systems like Windows 98 and NT Workstation, the end-user can download an application that will automatically run to share the desktop. The remote control offering is designed for low bandwidth (<128Kbps) network connections. No software will be required on the target system (other than a Microsoft OS, networking and Internet Explorer). No software is left on the end-user system when the remote control session is ended. For more details see Appendix B.

Security design

There are two types of users of ISCE: Call Agents and End Users. The HP ISCE architecture adheres to security design principles in the following areas:

Call agents

The HP ISCE security architecture has been designed to restrict access, authorize appropriate use, and provide detailed logging and auditing for call agents. Using a combination of security technology and operational policy controls, security risks are reduced.

End users

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

- Data Privacy – HP does not share any information collected from customers. Also, any data transferred between the end-user and call agents is encrypted using SSL.
- Data Integrity

Content Authenticity and Integrity

Security technology

HP ISCE utilizes the following industry standard encryption and authentication technology to provide a secure remote support solution:

- 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

A summary of the key security technologies utilized by ISCE is:

Security Technology	Addresses
RSA Asymmetric (public-key) Encryption	Confidentiality, Integrity and Authenticity of inter-host communications (ISCE Server components)
RSA RC4 Symmetric (private-key) Encryption	Confidentiality, Integrity and Authenticity of inter-host communications (ISCE Server components)
X.509v3 Digital Certificates	Authenticity of servers
Secure Sockets Layer (SSL)	Confidentiality, Integrity, Authenticity of web transactions

Table 1. Key security technologies

Appendix a

Privilege and feature matrix

Feature	Minimum privilege
Submit an Incident (local)	Guest
Submit an Incident (remote)	Admin on target machine
Find an Incident	Guest, but must have cookies enabled on browser
Knowledge, alerts	Guest
End user diagnostics	Admin on local machine
Agent diagnostics (remote)	Admin on target machine
Remote Control (push process)	Admin on target machine (to push software)
Remote Control (pull process)	Guest
Submit an Incident (local)	Guest

Table 2. Privilege and features

Appendix b

Remote control details

The remote control feature provides call center agents access to the end-user desktop allowing them to share mouse, keyboard and the end-user display. Remote control can be invoked as either a push to the end-user system or a pull download by the end-user. When the push process is initiated, the appropriate remote viewer will be launched automatically for the agent when the end-user system already has any of these services running: VNC host, Microsoft Terminal Server or MS Remote Desktop. In that case, any security issues unique to those pre-existing technologies would apply.

The call center agent initiates the pull process when an existing service is not available on the end-user system. The security features of the push process include:

1. Administrator privileges are required to push the RC host software to the target.

2. The RC host software only survives one use. The service immediately stops and un-registers itself when the client (agent) disconnects.

3. All of the host files are removed after the host has un-registered itself (only some dll's intermittently remain).

4. Logging of connection states to an SQL database on the Motive server by the push software is required.

The end-user may be directed to use the pull process by the call center agent based on their operating system type. The pull process requires the end-user to download and run the remote control host as a signed application. This host application opens a port to share the desktop with the call center agent. The host application and the open port only survive for one connection. Then, the port is closed and the remote control host application software is automatically removed.

In the case of either the push or pull process, no software (or additional security holes) will be left on the target system when the remote session is ended. The push process and the underlying remote control technologies are not configured to cross firewalls.

For more information

To learn more about HP Instant Support Corporate Edition, visit **www.hp.com/go/instantsupport**.

5982-3707EN, 10/2003