WHITE PAPER

SECURITY BEST PRACTICES FOR CISCO PERSONAL ASSISTANT (1.4X)

INTRODUCTION

This document covers the recommended best practices for "hardening" a Cisco® Personal Assistant 1.4(x) server. The term "server hardening" is used to describe the process of making a server less susceptible to unwanted or unauthorized access and viruses.

SCOPE

This document should be used in conjunction with the *Cisco Personal Assistant Installation Guide* to harden the Cisco Personal Assistant server during installation and normal operations. The recommendations and configurations presented in this document will be evaluated and updated regularly.

The following sections in this document address the main security concerns for the Cisco Personal Assistant server:

- Securing the Cisco Personal Assistant Operating Environment - The Cisco Personal Assistant operating environment is made up of several third-party products. Each of these products should be secured by following the security guidelines published by the product manufacturer. These guidelines, along with specific recommendations for using each component with Cisco Personal Assistant, are summarized in this section, and can be used to harden the Cisco Personal Assistant operating environment during or after installation.

- Cisco Personal Assistant Security Policies - This section suggests the security policies that you can implement to further harden your server after installation is complete.

Finally, the "Error – Reference Source Not Found" section offers a list of Websites referenced in this document.

SECURING THE CISCO PERSONAL ASSISTANT OPERATING ENVIRONMENT

The Cisco Personal Assistant operating environment includes all the third-party components needed to service subscribers. These components consist mainly of Microsoft products, though other third-party products such as Nuance ASR and Real-Speak TTS are employed as well. The following Microsoft products are the required components of the Cisco Personal Assistant operating environment:

- Windows 2000 with Service Pack 4 and any current security patches
- Microsoft Internet Information Services (IIS) 5.0 and any current security patches
- Internet Explorer (IE) 6.0 with Service Pack 1 and any current security patches

For a detailed list of Cisco Personal Assistant operating environment components, refer to the Cisco *Personal Assistant Installation and Administration Guide*, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2026/prod_maintenance_guides_list.html. Each component in the Cisco Personal Assistant operating environment presents a security risk, because each may prevent Cisco Personal Assistant from running reliably and effectively if compromised. By default, however, most of these components are installed with minimum security, and thus can be reconfigured with increased security in mind.

As appropriate, use the guidelines presented in the following sections, in conjunction with the *Cisco Personal Assistant Installation and Administration Guide*, to harden the Cisco Personal Assistant operating environment during or after a new Cisco Personal Assistant installation.

Securing Windows

After it has started, IIS is vulnerable until the Windows 2000 installation on the Cisco Personal Assistant server is complete. One option is to disable IIS or wait to install it until after the Windows 2000 Service Pack 4 is applied. However, the most secure approach to installing Windows is to use the integrated method of burning a Windows 2000 CD with Service Pack 4. Detailed instructions are provided in the article, "Installing and Securing a New Windows 2000 System," available on the Microsoft Website. In addition, refer to the Microsoft Security home page for the most current hardening and security guide for Windows 2000 and IIS 5.0. To check an existing Windows 2000 installation for vulnerabilities, first confirm that Service Pack 4 is installed on the server. Then query the Microsoft TechNet Website for the latest information about securing an existing Windows 2000 system. A security policy can be applied to the Cisco Personal Assistant server, but it should not be applied until after the Cisco Personal Assistant installation is complete. For more information about security policies and how to apply them, refer to the Microsoft Website or Microsoft Windows 2000 online help.

Caution: Applying certain security templates can render Cisco Personal Assistant inoperable. If you apply security templates, make sure that they use the suggested security settings outlined in the Cisco Personal Assistant Server Security Policies section of this document. These settings enable the Cisco Personal Assistant server to remain fully functional.

Securing Internet Explorer

At a minimum, IE 6.0 with Service Pack 1 must be installed on the Cisco Personal Assistant server. As a best practice, use IE on the Cisco Personal Assistant server for Cisco Personal Assistant administration only—and for no other purpose. Perform the following steps to reduce the chance of exposure to a worm such as the recent Blaster and Nachi viruses. For additional information about preventing exposure to and recovering from the Blaster virus, refer to http://support.microsoft.com/default.aspx?scid=kb;en-us;826955.

To disable active scripting:

Microsoft recommends that you subscribe to the Security Notification Service. To do so, however, you must set IE to use less secure settings than those suggested in this procedure. Therefore, make sure that at least one computer at your site—other than a Cisco Personal Assistant server—is subscribed to the Security Notification Service, and perform the following procedure on remaining workstations. In this way, you can receive updates about the latest hot fixes and security issues without seriously compromising Cisco Personal Assistant security.

Step 1: Start Internet Explorer.

Step 2: For each of the four security levels, perform the following actions:

- Click Tools > Internet Options.
- From the Internet Options dialog box, click the appropriate icon for the security level that you want to customize (Internet, Intranet, Trusted, Untrusted).
- Click Security > Custom Level.
- Under Scripting, check the Prompt field.

Step 3: Click OK.

Step 4: Click OK, and exit Internet Explorer.

Securing IIS

IIS is installed as part of Cisco Personal Assistant installation. Following are guidelines for securing the IIS 5.0 on the Cisco Personal Assistant server.

IIS Configuration Guidelines

Confirm that the most current cumulative update patch for IIS 5.0 is installed. If the operating system is installed or updated by using the method described in the "Securing Windows" section, then secure IIS 5.0 by removing the default settings. In addition, use the following guidelines to configure IIS on the Cisco Personal Assistant server.

Caution: Failure to follow the guidelines in this section may render the Cisco Personal Assistant Web server components inoperable.

- Remove sample files, folders, and Web applications.

Follow guidelines as specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Website.

- Secure Cisco Personal Assistant Web components.

Follow the guidelines specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Website.

- Disable all default IIS COM objects.

Follow guidelines as specified in the complete IIS 5.0 security checklist available on the Microsoft TechNet Website—except do not disable the "file system object" (FSO).

- Do not disable Parent Paths.

Do not follow the guidelines as specified in the complete IIS 5.0 security checklist on the Microsoft TechNet Website to disable Parent Paths. By default, this option is enabled, and should remain so on the Cisco Personal Assistant server.

Additional IIS Reference Information

The following security tools can be used after IIS is installed to expose any existing vulnerabilities.

Caution: Do not use these tools (or perform any procedures that are not referenced in this document) to alter the IIS configuration described in the previous section. If you do, you may render the Cisco Personal Assistant server inoperable.

- Use IIS Lockdown and URLScan tools.

You can use the Microsoft IIS Lockdown and URLScan tools to harden the IIS server. However, be careful not to disable support for active server pages (.asp) or the Scripts Virtual directory. Refer to the Security pages on the Microsoft TechNet Website for download instructions and details about how to use these tools. For information about configuring these tools in an Exchange environment, refer to article #Q309508 ("XCCC: IIS Lockdown and URLScan Configurations in an Exchange Environment") on the Microsoft Product Support Services Website.

- Follow Microsoft security checklists.

In addition to the complete checklist, Microsoft offers a baseline security checklist for IIS on its TechNet Website. Many of the checklist recommendations, such as subscribing to the Microsoft Security Notification Service, are necessary if you want to stay current with IIS security issues after installation.

Cisco Personal Assistant Server Security Policies

This section suggests some ways that you can further harden a default, "out-of-the-box" Cisco Personal Assistant server configuration. It is recommended that you implement the suggested changes in this section after you have completed the Cisco Personal Assistant installation.

For details about changing the settings presented in this section, search the Microsoft Website for the "Step-by-Step Guide to Using the Security Configuration Tool Set."

Changing Cisco Personal Assistant Server Security Settings

Use the hardening settings listed in Table 1 to restrict access to the Cisco Personal Assistant server. If your site already has a security policy in place, review the following policy settings to determine the additional settings necessary for securing the Cisco Personal Assistant server. These settings also can be made manually without applying a security template. It is important to turn on auditing in order to track how the Cisco Personal Assistant server is being accessed. Without using auditing, you cannot determine when someone has accessed your system.

Table 1. Local Policies: Audit Policies and User Rights Assignments

Setting	Default Value	Recommended Value
Audit account logon events	Success, Failure	Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Success, Failure	Failure
Audit logon events	Success, Failure	Failure
Audit object access	Success, Failure	No auditing
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Failure	Failure
Audit system events	No auditing	No auditing
Access this computer from the network	Backup operators, Power users, Users, Administrators, servername\IWAM, domainname\ISUR_servername, Everyone	Same as default, except do not include Everyone
Shut down the system	Backup operators, Power users, Administrators	Backup operators, Administrators

Using Strong Passwords

As part of a comprehensive security policy, you should use strong passwords, which can be enforced in Windows 2000. Strong passwords can be turned on by enabling Password Must Meet Complexity Requirements in the domain password policy settings.

Table 2 lists the settings that can be modified by using the Windows Local Security Policy utility on the Cisco Personal Assistant server.

Table 2. Local Policies: Security Options

Setting	Default Value	Recommended Value
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares	Do not allow enumeration of SAM accounts and shares
Allow system to be shut down without having to log on	Disabled	Disabled
Audit use of Backup and Restore privilege	Disabled	Disabled
Clear virtual memory pagefile when system shuts down	Disabled	Disabled
Digitally sign client communication (always)	Disabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled
Digitally sign server communication (when possible)	Disabled	Enabled
Disable Ctrl-Alt-Del requirement for login	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Enabled
LAN manager authentication level	Send LM and NTLM responses	Send NTLM response only
Message text for users attempting to log on	(blank)	Customer-specific information indicating that the system is for authorized use only; this information is important as legal protection if unauthorized access occurs
Message title for users attempting to log on	(blank)	Customer-specific information indicating that the system is for authorized use only; this information is important as legal protection if unauthorized access occurs

Number of previous logons to cache (in case domain controller is not available)	10 logons	5 logons
Prevent system maintenance of computer account password	Disabled	Enabled
Prompt user to change password before expiration	14 days	7 days
Rename administrator account	Not defined	Not defined
Restrict CD-ROM access to locally logged-on users only	Disabled	Enabled
Restrict floppy access to locally logged-on users only	Disabled	Enabled
Secure Channel: Digitally encrypt or sign secure channel data (always)	Disabled	Enabled
Secure Channel: Require strong (Windows 2000 or later) session key	Disabled	Enabled
Send unencrypted password to connect to third-party SMB [small and medium-sized business] servers	Disabled	Disabled
Smart card removal behavior	No Action	Lock workstation
Unsigned driver installation behavior	Warn but allow installation	Do not allow installation
Unsigned non-driver installation behavior	Silently succeed	Silently succeed / Warn but allow installation

Table 3 gives the settings that can be modified by using the Windows Local Security Policy utility on the Cisco Personal Assistant server.

Table 3. Event Log Settings

Setting	Default Value	Recommended Value
Maximum application log size	10240 kilobytes	10240 kilobytes
Maximum security log size	10240 kilobytes	10240 kilobytes
Maximum system log size	10240 kilobytes	10240 kilobytes

Restrict guest access to application log	Disabled	Enabled
Restrict guest access to security log	Disabled	Enabled
Restrict guest access to system log	Disabled	Enabled
Retain system log	As needed	As needed
Retention method for application log	As needed	As needed
Retention method for security log	As needed	As needed

Table 4 lists the services settings that should be employed on the Cisco Personal Assistant server. You can administer these recommended services settings by accessing the Service Control Panel in the Administration Tools folder.

Table 4. Services Settings

Setting	Default Value	Recommended Value
Alerter	Automatic	Disabled
Application Management	Disabled	Disabled
Automatic Updates	Disabled	Disabled
Background Intelligent Transfer Service	Disabled	Disabled
Cisco Security Agent	Automatic	Automatic (must be disabled during installation of Personal Assistant)
Clipbook	Manual	Disabled
COM+ Event System	Automatic	Manual
Computer Browser	Automatic	Disabled
DHCP Client	Automatic	Disabled
Distributed File System	Automatic	Disabled
Distributed Link Tracking Client	Automatic	Disabled
Distributed Link Tracking Server	Manual	Disabled
Distributed Transaction Coordinator	Automatic	Disabled

DNS Client	Automatic	Automatic
DNS Server	Disabled	Disabled
Event Log	Automatic	Automatic
Fax Service	Manual	Disabled
File Replication Service	Disabled	Disabled
IIS Admin Service	Automatic	Automatic
Indexing Service	Disabled	Disabled
Internet Connection Sharing	Manual	Disabled
Intersite Messaging	Disabled	Disabled
IPSec Policy Agent	Automatic	Automatic
Kerberos Key Distribution Center	Disabled	Disabled
License Logging Service	Disabled	Disabled
Logical Disk Manager	Automatic	Automatic
Logical Disk Manager Administrative Service	Manual	Manual
Messenger	Automatic	Disabled
Net Logon	Automatic	Automatic
NetMeeting Remote Desktop Sharing	Manual	Disabled
Network Connections	Manual	Manual
Network DDE	Disabled	Disabled
Network DSDM DDE	Manual	Manual
NT LM Security Support Provider	Manual	Manual
Performance Logs and Alerts	Manual	Manual
Plug and Play	Automatic	Automatic
Print Spooler	Automatic	Disabled
Protected Storage	Automatic	Automatic
QoS RSVP	Manual	Manual
Remote Access Auto Connection Manager	Manual	Disabled
Remote Access Connection Manager	Manual	Disabled

Remote Procedure Call (RPC)	Automatic	Automatic
Remote Procedure Call (RPC) Locator	Disabled	Disabled
Remote Registry Service	Automatic	Disabled*
Removable Storage	Disabled	Disabled
Routing and Remote Access	Disabled	Disabled
RunAs Service	Disabled	Disabled
Security Accounts Manager	Automatic	Automatic
Server	Automatic	Automatic
Simple Mail Transport Protocol (SMTP)	Automatic	Automatic (If installed)
Smart Card	Disabled	Disabled
Smart Card Helper	Disabled	Disabled
Simple Network Management Protocol (SNMP) Service	Manual	Automatic (if PA has to be managed using any SNMP monitoring agent)
System Event Notification	Automatic	Automatic
Task Scheduler	Disabled	Disabled
TCP/IP NetBIOS Helper Service	Automatic	Automatic
Telephony	Manual	Manual
Telnet	Disabled	Disabled
Terminal Services	Automatic	Automatic
Uninterruptible Power Supply	Manual	Manual
Utility Manager	Disabled	Disabled
Windows Installer	Manual	Manual
Windows Management Instrumentation	Automatic	Automatic
Windows Management Instrumentation Driver Extensions	Manual	Manual
Windows Time	Automatic	Automatic
Workstation	Automatic	Automatic

World Wide Web Publishing Service	Automatic	Automatic

* The Remote Registry Service must be enabled to install Cisco Personal Assistant and to configure failover. As soon as Cisco Personal Assistant is installed or failover is configured, the service should be disabled again.

Securing Remote Access

Telnet access should not be allowed on the Cisco Personal Assistant server. In addition, although a modem is required by the Cisco Technical Assistance Center (TAC) to support a Cisco Personal Assistant server, as a best practice turn it off or disconnect it when not in use.

Securing the Physical Unit

You can find best practices for securing a physical unit from unwanted access on the CERT Coordination Center (CERT/CC) Website. Refer to the “Practices About Hardening and Securing Systems” section in the Security Improvement Modules on the CERT site.

Protecting Cisco Personal Assistant from Virus Attacks

To minimize the risk of virus attacks, install an antivirus software package on the Cisco Personal Assistant server. Before doing so, however, you should address the following issues:

- Disable antivirus software during installation of Cisco Personal Assistant.

It is best to install antivirus software only after Cisco Personal Assistant is installed. If it already is installed prior to installing the Cisco Personal Assistant application, disable it before proceeding. Note that in some cases you may need to completely remove the antivirus software, and reinstall it after you have completed the Cisco Personal Assistant installation.

- Use caution when employing message scanning.

Consider the impact that scanning has on the performance of the Cisco Personal Assistant server prior to scanning for viruses in a certain way. For instance, performing a complete file I/O scan may have a negative impact on Cisco Personal Assistant server performance. Do not employ any message scanning that could drastically impact the performance of the Cisco Personal Assistant server.

Protecting Cisco Personal Assistant from Hacker Attacks

Follow Microsoft recommendations on securing the server from unwanted or unauthorized access. You can obtain vulnerability scanners (such as Cisco Scanner, Nessus, and SAINT) that identify security vulnerabilities on your network. As a best practice, do not install the scanner on the Cisco Personal Assistant server.

Additionally, a Cisco Security Agent specifically configured to protect Cisco Personal Assistant is available on Cisco.com. The Cisco Security Agent provides threat protection for server and desktop computing systems. It aggregates multiple security functions, combining host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation. It is highly recommended that you install a Cisco Security Agent on the Cisco Personal Assistant server.

FOR MORE INFORMATION

For more information about topics referenced in this document, refer to the following sites.

Cisco Personal Assistant Documentation

• Official Cisco Personal Assistant 4.0 product documentation is available on Cisco.com at:
http://www.cisco.com/en/US/products/sw/voicesw/ps2026/tsd_products_support_series_home.html

CERT/CC Website

- The CERT/CC Website follows: http://www.cert.org/.

IETF Website

- • The IETF Website follows: http://www.ietf.org

Microsoft Websites

- The Microsoft home page follows: http://www.microsoft.com/.
- The Microsoft Security home page follows: http://www.microsoft.com/security/default.mspx
- The Microsoft TechNet home page follows: http://technet.microsoft.com/en-us/default.aspx

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA