



# Release Notes for Cisco Security Agent for Cisco Personal Assistant Release 1.0(1)

---

*Revised October 8, 2003*

These release notes provide download and installation instructions, and information on Cisco Security Agent for Cisco Personal Assistant Release 1.0.(1).

Cisco Security Agent for Cisco Personal Assistant software is available on the Cisco Personal Assistant Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/PA3des>.

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Determining the Software Version, page 3](#)
- [Downloading Cisco Security Agent for Cisco Personal Assistant 1.0\(1\), page 4](#)
- [Installing Cisco Security Agent for Cisco Personal Assistant 1.0.\(1\), page 4](#)
- [Notes on Using Cisco Security Agent for Cisco Personal Assistant, page 5](#)
- [Uninstalling Cisco Security Agent for Cisco Personal Assistant, page 6](#)
- [Cisco Personal Assistant Documentation, page 6](#)
- [Obtaining Documentation, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 9](#)



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Introduction

Cisco Security Agent for Cisco Personal Assistant provides intrusion prevention, malicious mobile code protection, operating system integrity assurance, and audit log consolidation. It is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with Cisco Personal Assistant servers that meet the system requirements specified in the “[System Requirements](#)” section on page 2.

Cisco Security Agent for Cisco Personal Assistant was created by using CiscoWorks Management Center for Cisco Security Agents and is based on the following Management Center for Cisco Security Agents version 4.0, build 119 policies:

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive MS IIS Module
- Server Module
- User Authentication Auditing Module
- Virus Scanner Module

Cisco Security Agent for Cisco Personal Assistant version 1.0.(1) also includes the PA Base Group Exceptions policy, which allows normal Personal Assistant operations that the other policies would not allow.

To add, change, delete, or view policies included in Cisco Security Agent for Cisco Personal Assistant, run CiscoWorks Management Center for Cisco Security Agents, and import the file CSA-for-Cisco-PA-1-4x-ver-1-0-1.export. The file is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/PA3des>.

For more information on CiscoWorks Management Center for Cisco Security Agents and on Cisco Security Agent, refer to <http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html>.

## System Requirements

- Cisco Personal Assistant version 1.4 or later.
- Microsoft Windows 2000 Server in English.



---

**Note** If you install Cisco Security Agent for Cisco Personal Assistant on a server running Windows in Japanese, the display of some non-ASCII characters will be corrupted.)

---

- If virus-scanning software is installed on the Personal Assistant server, McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 or later.
- Windows Automatic Update configured so that it does not automatically download updates to the Personal Assistant server.

# Determining the Software Version

This section contains procedures for determining the version in use for the following software:

- [Cisco Security Agent, page 3](#)
- [Policy for Cisco Security Agent for Cisco Personal Assistant, page 3](#)

## Cisco Security Agent

### To Determine the Cisco Security Agent Version in Use

**Step 1** Start Regedit.



**Caution**

Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

**Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

**Step 3** Expand the key  
HKEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc.\System Info\CSA Agent\Version.

**Step 4** Close Regedit.

## Policy for Cisco Security Agent for Cisco Personal Assistant

### To Determine the Policy Version in Use for Cisco Security Agent for Cisco Personal Assistant

**Step 1** Start Regedit.



**Caution**

Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

**Step 2** If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

**Step 3** Expand the key  
HKEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc.\System Info\PA-CSA Policy\Version.

**Step 4** Close Regedit.

# Downloading Cisco Security Agent for Cisco Personal Assistant 1.0(1)

## To Download Cisco Security Agent for Cisco Personal Assistant 1.0(1)

---

- Step 1** Confirm that the computer you are using has up to 20 MB of hard-disk space for the download file and the installed files.
  - Step 2** On a computer with a high-speed Internet connection, go to the Cisco Personal Assistant Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/PA3des>.
  - Step 3** Click **CiscoPA-CSA-4.0.0.119-1.0.1-Setup-K9.exe**.
  - Step 4** Follow the on-screen prompts to complete the download.
  - Step 5** If you plan to install Cisco Security Agent for Cisco Personal Assistant from a compact disc, burn the CD.
- 

# Installing Cisco Security Agent for Cisco Personal Assistant 1.0(1)

We recommend that you install Cisco Security Agent for Cisco Personal Assistant after regular business hours because the installation will affect Personal Assistant performance. In addition, when the installation completes, you must restart the Personal Assistant server for Cisco Security Agent for Cisco Personal Assistant to start working.

Do not install Cisco Security Agent for Cisco Personal Assistant by using Windows Terminal Services.

## To Install Cisco Security Agent for Cisco Personal Assistant 1.0(1)

---

- Step 1** If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.
  - Step 2** In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Personal Assistant file, and double-click **CiscoPA-CSA-4.0.0.119-1.0.1-Setup-K9.exe**.
  - Step 3** Follow the on-screen prompts.
  - Step 4** When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.  
Cisco Security Agent for Cisco Personal Assistant begins to work as soon as you restart the Personal Assistant server. You do not need to configure the application.
-

# Notes on Using Cisco Security Agent for Cisco Personal Assistant

The following sections contain information on using Cisco Security Agent for Cisco Unity Bridge:

- [Cisco Security Agent Task Bar Icon Available Only for First Windows Logon, page 5](#)
- [Locations in Which Cisco Security Agent Logs Events, page 5](#)
- [Disabling and Re-enabling the Cisco Security Agent Service, page 5](#)

## Cisco Security Agent Task Bar Icon Available Only for First Windows Logon

If two people log on to Windows on the Personal Assistant server—one at the server and the other by using Windows Terminal Services, or both by using Terminal Services—only the first person to log on will have access to the Cisco Security Agent icon.

## Locations in Which Cisco Security Agent Logs Events

Cisco Security Agent logs events in the following three locations:

<b>Windows application event log</b>	Events that are generated by Cisco Security Agent have an event source of CSAgent.
<b>Securitylog.txt</b>	Cisco Security Agent logs one event per line. We recommend that each administrator who logs on to the Personal Assistant server add a shortcut for Securitylog.txt to the Windows desktop. The file is located in the <InstallDirectory>\Cisco\CSAgent\Log directory.
<b>CSA Control Panel</b>	To display the CSA Control Panel, double-click the Cisco Security Agent task bar icon, and click the Messages tab. Only events that have occurred since you logged on to Windows appear in the CSA Control Panel.

## Disabling and Re-enabling the Cisco Security Agent Service

Disable the Cisco Security Agent service in the following situations:

- Before you install any software on the Personal Assistant server.
- Before you upgrade any software, including Personal Assistant, on the Personal Assistant server. This also applies to automatic upgrades.
- Before you add, change, or delete values in the Windows registry.
- Before you change Windows system or boot files.



### Caution

When you disable the Cisco Security Agent service, you must re-enable it before it starts monitoring the Personal Assistant server again.

---

**To Disable the Cisco Security Agent Service**

---

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the right pane, double-click **Cisco Security Agent**.
  - Step 3** On the General tab, in the Startup Type list, click **Disabled**.
  - Step 4** Click **Stop**.
  - Step 5** Click **OK** to close the Cisco Security Agent Properties dialog box.
  - Step 6** Close **Services**.
- 

---

**To Re-enable the Cisco Security Agent Service**

---

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the right pane, double-click **Cisco Security Agent**.
  - Step 3** On the General tab, in the Startup Type list, click **Automatic**.
  - Step 4** Click **Start**.
  - Step 5** Click **OK** to close the Cisco Security Agent Properties dialog box.
  - Step 6** Close **Services**.
- 

## Uninstalling Cisco Security Agent for Cisco Personal Assistant

---

**To Uninstall Cisco Security Agent for Cisco Personal Assistant**

---

- Step 1** Right-click the **Cisco Security Agent** icon in the Windows task bar, and click **Suspend Security**.  
If the icon does not appear in the task bar, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the Cisco Security Agent service.
  - Step 2** On the Windows Start menu, click **Programs > Cisco Systems > Uninstall Cisco Security Agent**.
  - Step 3** Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Personal Assistant.
  - Step 4** Click **Yes** again to restart the Personal Assistant server.
- 

## Cisco Personal Assistant Documentation

For descriptions and URLs of Personal Assistant documentation on Cisco.com, refer to *About Cisco Personal Assistant Documentation*. The document is shipped with Personal Assistant and is available at

[http://www.cisco.com/en/US/products/sw/voicesw/ps2026/prod\\_pre\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2026/prod_pre_installation_guides_list.html).

# Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
 Attn: Customer Document Ordering  
 170 West Tasman Drive  
 San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

### Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

### Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.