



Release Notes for Cisco Support Tools' Release 2.4(1)

July 2009

Contents

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 6](#)
- [Caveats, page 8](#)
- [Documentation Updates, page 9](#)

Introduction

These release notes contains information about the Cisco Support Tools, 2.4(1). Review this document before installing and using Support Tools. For all other information, including hardware and software requirements, compatibility, installation and configuration instructions, see the *Support Tools 2.4(1) User Guide* (http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html). You can access the Support Tools documentation from the `getstart.htm` (located at the top level of your Support Tools Installation CD).

Cisco Support Tools 2.4(1) is a suite of utilities that allow you to manage and troubleshoot the ICM Nodes which process call load, routing, and reporting. Through Support Tools, you can troubleshoot configuration and performance problems on these systems from a single machine in your network - the Support Tools Server.



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

Copyright © 2009 Cisco Systems, Inc. All rights reserved.

Access to utilities in the Support Tools suite is through a browser-based interface--the Support Tools Dashboard--installed on the Support Tools Server. Different levels of security are used to control Dashboard access and tools access, during low bandwidth situation (for example, via dialup access) or when web browsing is otherwise impractical. Additionally, most Support Tools utilities can be accessed and run through the command line.

System Requirements

This section contains the following:

- [Cisco Unified Platform Compatibility, page 2](#)
- [Support Tools Installation Platforms, page 2](#)
- [Support Tools Dashboard Browser Support, page 3](#)
- [Support Tools Server Requirements, page 3](#)

Cisco Unified Platform Compatibility

See the *Support Tools 2.4(1) User Guide* (http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html) for information on Support Tools 2.4(1) compatibility with Cisco Unified Communications Products including Unified Contact Center (Cisco Unified ICM, Cisco Unified Contact Center Express (Unified CCX) and Cisco Unified Customer Voice Portal (Unified CVP).



Note

The Support Tools Server Release 2.4 should be used when connecting to Nodes post Unified CVP 7.0(2) release in order to achieve full feature functionality.

Support Tools Installation Platforms

Support Tools Server Platform

The Support Tools Server must be installed either on a standalone Server (i.e., one on which no Cisco Unified Communications products are installed), or it can be collocated on an existing Unified ICM Client Database Server in your Unified ICM network or on an existing Unified Customer Voice Portal Operations Console (also referred as CVP OAMP Server) in your Unified CVP network.



Caution

Excluding the Unified ICM Administration and Database Server or the Cisco Unified Customer Voice Portal Operations Console. DO NOT collocate the Support Tools Server on any machine running Cisco Unified Software. Otherwise, you may observe performance issues.

See the *Support Tools 2.4(1) User Guide* (http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html) for information on Support Tools Server platform requirements.

Support Tools Node Platform

You can install the Support Tools Node on any of the following supported Cisco Unified Communications Nodes:

- Cisco Unified ICM Administration and Data Server
- Cisco Unified ICM CallRouter
- Cisco Unified ICM Peripheral Gateways (PGs)
- Cisco Unified ICM Logger
- Unified CCX
- CTI Object Server (CTIOS)
- Cisco Agent Desktop (CAD)
- Unified CVP
- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Web Interaction Manager (Unified WIM)
- Cisco Unified E-Mail Interaction Manager (Unified EIM)
- Cisco Media Blender (CMB)

The Support Tools 2.4(1) Node installer is bundled with the Cisco Unified ICM 7.2(7) and Cisco Unified ICM 7.5(3).



Note

Installation of Support Tools Node on a Unified CM Server and Unified CCX Server, hosted on a Linux platform is not supported.

Support Tools Dashboard Browser Support

See the *Support Tools 2.4(1) User Guide*

(http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html) for information on Support Tools Dashboard supported browsers.

Support Tools Server Requirements

Support Tools Server OS Requirements

Prior to installing the Support Tools Server, one of the following operating systems must be installed and properly configured:

- Microsoft Windows XP Professional with Service Pack 1
- Microsoft Windows Server 2000 with Service Pack 4
- Microsoft Windows Server 2003 Standard Edition with Service Pack 2

Support Tools Node Agent OS Requirements

Following are the Support Tools Node Agent OS Requirements:

- Microsoft Windows XP Professional (no SP requirements)
- Microsoft Windows Server 2000 (no SP requirements)
- Microsoft Windows Server 2003 Standard Edition (no SP requirements)

New Features

- **Improved log collection on Unified CM Servers:** The log collection Algorithm of the Support Tools has been improved to reduce the CPU and I/O usage when collecting logs from CUCM Servers. With this enhancement, the log collection in the CUCM Node will be much faster and less I/O intensive as compared to the earlier releases of Support Tools.

- **Capture files collection:** Some components in Unified ICM like the Peripheral Interface Manager (PIM), and Open Peripheral Controller (OPC) now support an advanced debugging mechanism called Capture files, which gives the support engineer more information about the component.

Support Tools Release 2.4(1) has been enhanced to collect the capture files generated by different PIM and OPC components of the Unified ICM Nodes. This helps you to collect the relevant capture files along with the rest of the log files and send it to the support team.

- **Support Tools Server and Cisco Unified Customer Voice Portal Operations Console (CVP OAMP Server) Co-Residency on a single machine:** This enhancement enables the Support Tools Server and Unified C VP Operations Console to co-exist on a single computer.

Prior to this release, the Support Tools Server and Unified CVP Operations Console could not co-exist on the same server. This restriction required users to add an additional server dedicated to Support Tools Server. This enhancement will allow Support Tools Server to be installed over an existing Unified CVP Operations Console.



Note

- You must restart the Unified CVP Resource Manager Service after installing the Support Tools Server over an existing Unified CVP Operations Console.
- You cannot install the Unified CVP Operations Console on a server having the Support Tools Server. The Unified CVP Operations Console must be installed first, followed by the Support Tools Server.
- Co-residency of the Support Tools Server and the Unified CVP Operations Console is not supported if any other ICM component is installed on the CVP Server.

For additional information on the enhancements refer the *Support Tools 2.4(1) User Guide* (http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html).

Limitations and Restrictions

This section describes significant functioning-as-designed limitations of this product, and limitations imposed by third-party products.

- **The Support Tools Server installed on Windows XP does not support IPSec.**

When you install the Support Tools Server on Windows XP, IPSec is not configured. However, when the Support Tools Node is installed as part of an Enterprise application Servers (for example, Unified ICM or Unified CVP), it is installed on Windows Server 2003 and thus IPSec is enabled.

Furthermore, IPsec is enabled in such a way that it **requires** and allows communication from Support Tools Servers that has the same IPsec key. Since the IPsec is not supported for Windows XP, the Support Tools Server cannot provide this authentication, therefore the connection between the two is prevented.

Workaround:

- Disable the IPsec on the Support Tools Node. You may need to do this for every Node that you want to communicate with.

Or

- You may opt to install the Support Tools Server on a Windows Server 2003 which provides an option to enable IPsec.

- **Performance Monitor tool is not supported on Releases preceding 2.2.(1) release.**

For example, If you have a 2.2 (1) Server and if you are trying to run the Performance Monitor tool on a 2.1(1) Node agent, then you will not see the expected result.

- **Log Collector Tool imposes a maximum number of systems per log group and logs per system.**

By default, the Log Collector allows a maximum of:

- 10 systems per log group
- 10 logs for each system for each request

These default values are determined by the registry settings to ensure optimal performance.



Caution

Do not modify these settings without consulting your Cisco support representative.

- **You may observe performance issues when you run the Cisco Web utility from a command line on a Node.**

Cisco Web utilities are executed and run on the Support Tools Server. However, when initiating these utilities from the command-line, you need to specify the tool to be executed on a particular Support Tools Node. For more information on the command-line, refer the *Support Tools 2.4(1) User Guide* (http://www.cisco.com/en/US/products/ps5905/products_user_guide_list.html).

As registry comparisons and merged logs collections tend to be resource-intensive, it is suggested that these actions not be executed from a Node due to possible performance impact to that system.

- **Browsers configured to use web proxy for local addresses prevent local login to the Dashboard on the Support Tools Server.**

You cannot access the Support Tools Dashboard through your local login on the Support Tools Server. Your login will fail because your web browser is configured to use a proxy for local addresses. The browser returns an error stating that the proxy is unable to find the requested page.

To avoid a log-in failure, ensure that the browser on the Support Tools Server does not use a proxy for local addresses. For example, in Internet Explorer 6.0, this setting is located at: *Tools > Internet Options > Connections > LAN Settings > Bypass proxy for local addresses*.

- **Unix utilities support US-ASCII characters only.**

The set of Unix-style utilities included with Support Tools 2.4(1) (for example, `chmod`, `diff`, `grep`) supports US-ASCII characters only. If desired, you can replace the US-ASCII releases of these tools with localized releases. Unix utilities are installed on the Support Tools Server at `<support_tools_root>\Unix Tools`.

- **Using command redirection to save output on Latin-1 systems may result in files that display incorrect characters in the Windows text editors.**

When you use the Cisco web utilities from a command-line on the Latin-1 systems, your saved output (through the command redirection) may result in files that display incorrect characters. (When you view the results in a Windows-based text editor such as Notepad.)

This occurs because the OEM character set (used to render text in a command window) is different than the ANSI character set (used to render text in Windows text editors) on Latin-1 systems. Your output may display correctly when initially viewed in a DOS window. Files saved via command redirection may display incorrect characters when later viewed in a Windows text editor.

Workaround:

- To avoid this limitation, on Latin-1 systems, avoid using the following command redirection to save output to a file: `>registry /list > my_file.txt`

- **No CLI support for new Web Tool functionality introduced in Support Tools 2.2(1).**

New functionality introduced in the Web Tools utility (i.e., Trace and Log, System Interrogate, Registry Compare) in Support Tools release 2.2.(1) is not supported through a command line interface. To use the new Support Tools release 2.2(1) functionality, you must access and use the Web Tools through the Support Tools Dashboard. This is applicable to all versions starting from Support Tools release 2.2(1).

Important Notes

The following sections contain important information that may have been unavailable upon the initial release of documentation for Release 2.4(1):

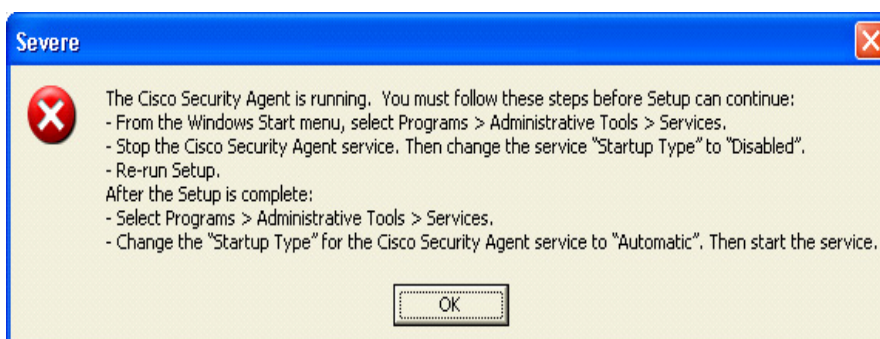
- [Check for WMI Service Started/Automatic, page 6](#)
- [Cisco Security Agent Warning Message, page 6](#)
- [Internet Explorer security warning message, page 7](#)
- [Uninstalling the Unified CVP Operations Console when the Support Tools Server has been co-installed on the same machine., page 7](#)

Check for WMI Service Started/Automatic

If you choose to disable WMI, the System Interrogate tools do not return OS, hardware, Web Server, or SQL Server information for the interrogation report. Enabling the WMI service using one of the service control options restores full functionality to the System Interrogation tool.

Cisco Security Agent Warning Message

If CSA is running when you attempt to run the Support Tools setup, you will see the following warning message:



Follow the steps in the dialog to resolve this issue.

Internet Explorer security warning message

If the below popup appears when the dashboard is opened, it indicates JRE (Java Runtime Environment) not available to Internet Explorer on the system. Installation of JRE on the system will resolve the issue.



Uninstalling the Unified CVP Operations Console when the Support Tools Server has been co-installed on the same machine.

In the co-resident mode, both the Support Tools Server and the Unified CVP Operations Console are installed on the same Server/machine. If you choose to uninstall the Unified CVP Operations Console in the co-resident mode, you must first uninstall the Support Tools Server. Otherwise, you may encounter un-installation errors.

Caveats

Using the Bug Toolkit

If you are a registered Cisco.com user, you can find the latest information about resolved, open, and closed caveats for Support Tools by using the Bug Toolkit, an online tool that allows you to query caveats according to your own needs. By using Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides.

To access Bug Toolkit, you need:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

-
- Step 1** To access the Bug Toolkit, go to <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>
- Step 2** Log on with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the “Search for Bug ID” field then, click Go. Alternatively, under “Select Product Category”, choose Voice and Unified Communications; or, under “Select Products” choose Cisco Unified Intelligent Contact Management Enterprise and then choose the “Software Version” you are interested in.

For information about how to search for bugs, create saved searches, create bug groups, and so on, click Help in the Bug Toolkit window. .

Open Caveats in This Release

This section contains a list of defects that are currently pending in Support Tools Release 2.4(1). Defects are listed by component and then by identifier.

-
- Step 1** If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Identifier	Headline
CSCsv01103	Registry not updated properly on un-installation of Support Tools Server on win2k3R2.
CSCsv07037	Trace group not displayed in Trace Group field on Support Tools Server Dashboard.

Resolved Caveats in This Release

Resolved caveats are no longer listed in these Release Notes. Instead, you can find the latest resolved caveat information through the Bug Toolkit. The Bug Toolkit is an online tool that is available for the customers to query defects according to their own needs.



Tip

You need an account with Cisco.com to use the Bug Toolkit to find open and resolved caveats of any severity for any release. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Documentation Updates

This section provides documentation changes that were unavailable when Release 2.4(1) was released.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Documentation Feedback

You can provide comments about this document by sending email to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

