



Release Notes for Cisco Cloud Web Security Passive Identity Management, Release 1.2

Last Updated: October 3, 2013

This document includes the following sections:

- [Introduction, page 2](#)
- [Downloading the Latest Version of Cisco Cloud Web Security Passive Identity Management, page 2](#)
- [System Requirements, page 3](#)
- [Caveats, page 3](#)
- [Related Documentation, page 5](#)



Introduction

These release notes are for the following releases:

- Cisco Cloud Web Security Passive Identity Management 1.2.3.9
- Cisco Cloud Web Security Passive Identity Management 1.2.3.8
- Cisco Cloud Web Security Passive Identity Management 1.2.3.7
- Cisco Cloud Web Security Passive Identity Management 1.2.3.6

Downloading the Latest Version of Cisco Cloud Web Security Passive Identity Management

To download the latest version of Cisco Cloud Web Security Passive Identity Management, you must be a registered user of Cisco Cloud Web Security. To obtain the Cisco Cloud Web Security Passive Identity Management software, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Follow this link to the Cisco ScanCenter login page:
https://scancenter.scansafe.com/portal/admin/login.jsp |
| Step 2 | Enter your Cisco Cloud Web Security credentials. |
| Step 3 | Click the Admin tab. |
| Step 4 | In the Downloads menu, click Connector . |
| Step 5 | Click Download to download Cisco Cloud Web Security Passive Identity Manager. |
| Step 6 | Follow the instructions in the <i>Passive Identity Management Administrator Guide, Release 1.2</i> to deploy the package. |
-

New Features in Release 1.2.3.9

Cisco Cloud Web Security Passive Identity Management 1.2.3.9 is a maintenance release that resolves the list of caveats in [Table 1](#). This release introduces support for Microsoft Windows 8 and Internet Explorer 10.

New Features in Release 1.2.3.8

Cisco Cloud Web Security Passive Identity Management 1.2.3.8 is a maintenance release that resolves the list of caveats in [Table 2](#). This release does not introduce any new features.

New Features in Release 1.2.3.7

Cisco Cloud Web Security Passive Identity Management 1.2.3.7 is a maintenance release that resolves the list of caveats in [Table 3](#). This release does not introduce any new features.

New Features in Release 1.2.3.6

Cisco Cloud Web Security Passive Identity Management is a maintenance release that resolves the list of caveats in [Table 5](#). This release introduces support for Microsoft Internet Explorer 9 and Mozilla Firefox 4.

System Requirements

Cisco Cloud Web Security Passive Identity Management is a small Microsoft Windows application, typically executed via a logon script to obtain user or group information. This information is passed out-of-band via an HTTPS request and a user identifier is embedded in the browser user-agent request header for all subsequent requests.

The following sections show the supported Windows versions and Browser versions.

Windows Versions

- Windows 8 x86 (32-bit) and x64 (64-bit).
- Windows 7 x86 (32-bit) and x64 (64-bit).
- Windows Vista x86 (32-bit) and x64 (64-bit).
- Windows XP SP3 x86 (32-bit) and x64 (64-bit).

Browser Versions

- Microsoft Internet Explorer version 7 to 10.
- Mozilla Firefox (current and previous release only).

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

The following sections list caveats with Severity 1-3:

- [Cisco Cloud Web Security Passive Identity Management 1.2.3.9 Caveats](#)
- [Cisco Cloud Web Security Passive Identity Management 1.2.3.8 Caveats](#)
- [Cisco Cloud Web Security Passive Identity Management 1.2.3.7 Caveats](#)
- [Cisco Cloud Web Security Passive Identity Management 1.2.3.6 Caveats](#)

Cisco Cloud Web Security Passive Identity Management 1.2.3.9 Caveats

Caveats Resolved by Release 1.2.3.9

[Table 1](#) lists the caveats that Cisco Cloud Web Security Passive Identity Management 1.2.3.9 resolves.

Table 1 *Caveats Resolved by Cisco Cloud Web Security Passive Identity Management 1.2.3.9*

ID	Headline
BUG-2906	PIM 1.2.3.8 changes the Firefox version in the user agent from the actual version to 4.

Open Caveats in Release 1.2.3.9

There are no known caveats that are unresolved in Cisco Cloud Web Security Passive Identity Management 1.2.3.9.

Cisco Cloud Web Security Passive Identity Management 1.2.3.8 Caveats

Caveats Resolved by Release 1.2.3.8

[Table 2](#) lists the caveats that Cisco Cloud Web Security Passive Identity Management 1.2.3.8 resolves.

Table 2 *Caveats Resolved by Cisco Cloud Web Security Passive Identity Management 1.2.3.8*

ID	Headline
BUG-2655	Cannot run PIM with user levels other than administrator.
BB-780	PIM does not provide user granularity for Firefox 10.
BUG-2199	PIM 1.2.3.5 malforms useragent string, triggers WebKnight block

Open Caveats in Release 1.2.3.8

There are no known caveats that are unresolved in Cisco Cloud Web Security Passive Identity Management 1.2.3.8.

Cisco Cloud Web Security Passive Identity Management 1.2.3.7 Caveats

Caveats Resolved by Release 1.2.3.7

[Table 3](#) lists the caveats that Cisco Cloud Web Security Passive Identity Management 1.2.3.7 resolves.

Table 3 *Caveats Resolved by Cisco Cloud Web Security Passive Identity Management 1.2.3.7*

Id	Headline
EE-43	PIM on <= IE8 shouldn't use IE9 specific registry location for the User Agent

Open Caveats in Release 1.2.3.7

[Table 4](#) lists the caveats that are unresolved in Cisco Cloud Web Security Passive Identity Management 1.2.3.7.

Table 4 *Caveats Open in Cisco Cloud Web Security Passive Identity Management 1.2.3.7*

Id	Headline
BUG-2199	PIM 1.2.3.5 malforms useragent string, triggers WebKnight block

Cisco Cloud Web Security Passive Identity Management 1.2.3.6 Caveats

Caveats Resolved by Release 1.2.3.6

[Table 5](#) lists the caveats that Cisco Cloud Web Security Passive Identity Management 1.2.3.6 resolves.

Table 5 *Caveats Resolved by Cisco Cloud Web Security Passive Identity Management 1.2.3.6*

Id	Headline
SS-13406	Make PIM work with IE9 first and then later with FF4 (if this is at all possible)
BUG-2207	PIM user issues accessing gotomeeting.com

Open Caveats in Release 1.2.3.6

[Table 6](#) lists the caveats that are unresolved in Cisco Cloud Web Security Passive Identity Management 1.2.3.6.

Table 6 *Caveats Open in Cisco Cloud Web Security Passive Identity Management 1.2.3.6*

Id	Headline
BUG-2199	PIM 1.2.3.5 malforms useragent string, triggers WebKnight block

Related Documentation

For more information, see the following documents:

- [ScanCenter Administrator Guide, Release 5.2](#)
- [Passive Identity Management Administrator Guide, Release 1.2](#)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009-2012 Cisco Systems, Inc. All rights reserved.

