# Release Notes for the Cisco Active Directory Agent, Release 1.0

**Revised: April 13, 2012, OL-25136-01**

## Contents

These release notes describe the role of the Cisco Active Directory Agent in an identity-based solution, its limitations and restrictions (caveats), and related information. These release notes supplement the Cisco Active Directory Agent documentation that is included with the software, and cover the following topics:



## Introduction

The Cisco Active Directory Agent (AD Agent) is a component that runs on a Windows machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP addresses and user identities in its database; and makes the latest mappings available to its client devices.

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

Client devices, such as the Cisco Adaptive Security Appliance (ASA) and the Cisco IronPort Web Security Appliance (WSA), interact with the AD Agent using the RADIUS protocol in order to obtain the latest set of IP-to-user-identity mappings, in any one of the following ways:

- On-Demand—The AD Agent can respond to an on-demand query from the client device for a specific mapping.
- Bulk Download—The AD Agent can respond to a request from the client device for the entire set of mappings currently in its cache.

The AD Agent interacts with the following components in a network:

- Client Devices
- Active Directory
- Syslog Servers

The AD Agent can support up to 100 client devices and 30 domain controller machines, and can internally cache up to 64,000 IP-to-user-identity mappings.

# Active Directory Agent Requirements

See the *Installation and Setup Guide for the Active Directory Agent, Release 1.0* for information on the Active Directory Agent Requirements.

# Active Directory Agent License Information

See the *Open Source Used in Cisco Active Directory Agent 1.0* document for the Active Directory Agent licence information,

# Important Notes

For the Active Directory Agent to function properly in an identity-based solution, you must ensure that:

- Hardware requirements are met. See http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html#wp1059852 for more information.
- Firewall exceptions, if required, must be configured on the AD Agent machine and the AD domain controller machines. See http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html#wp1060909 for more information.
- Ports listed in the Installation and Setup Guide for the Cisco Active Directory Agent, Release 1.0 must be open. See http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html#wp1062461 for more information.
- Active Directory requirements are met. See http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html#wp1060694 for more information.
- The Audit Policy configuration on AD domain controller machines allow successful logons to generate the necessary events in the Windows Security Log of that AD domain controller machine. See http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html#wp1058066 for more information.

# Installing the Active Directory Agent Software Release 1.0.0.32

See the *Installation and Setup Guide for the Active Directory Agent, Release 1.0* for information on how to install and configure the Active Directory Agent.

# Upgrading the Active Directory Agent Software Release 1.0.0.32 to Active Directory Agent Software Release 1.0.0.32.1

To upgrade the Active Directory Agent Software Release 1.0.0.32 (build 539) to Active Directory Agent Software Release 1.0.0.32.1 (build 598), complete the following steps:

**Step 1** Uninstall the existing Active Directory Agent Software Release 1.0.0.32 (build 539).

**Step 2** Install Active Directory Agent Software Release 1.0.0.32.1 (build 598).

**Note** After you uninstall AD Agent Software Release 1.0.0.32 (build 539) and install AD Agent Software Release 1.0.0.32.1 (build 598), all the configuration is lost in the process. You should make a note of all the existing configuration information such as AD Domain Controllers, consumer devices (ASAs), and so on and re-configure the newly installed AD Agent Software Release 1.0.0.32.1 (build 598) accordingly. See CSCtx26970 for more details.

See the *Installation and Setup Guide for the Active Directory Agent, Release 1.0* for information on how to install and configure the Active Directory Agent.

# Caveats

This section contains the lists of:



## Resolved Caveats in Cisco Active Directory Agent Release 1.0.0.32.1

*Table 1 Resolved Caveats in Active Directory Agent Release 1.0.0.32.1*

| Caveat | Description |
|---|---|
| CSCto69094 | DC name shown for the **adacfg cache list** command is not similar to the domain name given for the **adacfg dc create** command. |

*Table 1 Resolved Caveats in Active Directory Agent Release 1.0.0.32.1 (continued)*

| Caveat | Description |
|---|---|
| CSCtq45780 | When installing the AD Agent directly on domain controller, the AD Agent cannot monitor domain controllers in other trusted domains.<br><br>Due to the resolution of this bug, the following requirement mentioned in the Active Directory Requirements section of the *Installation and Setup Guide for the Active Directory Agent, Release 1.0*, is no more valid:<br><br>Before you configure even a single domain controller machine using the adacfg dc create command, ensure that the AD Agent machine is first joined to a domain (for example, domain J) that has a trust relationship with each and every domain (for example, domain D[i]) that it will monitor for user authentications (through the domain controller machines that you will be configuring on the AD Agent machine). |
| CSCtq54889 | AD agent crashs with two or more ASAs when requesting multiple requests. |
| CSCtr77801 | Support detection of mappings from DC running French 2008R2-SP1. |

# Open Caveat in Cisco Active Directory Agent Release 1.0.0.32.1

*Table 2 Open Caveat in Active Directory Agent Release 1.0.0.32.1*

| Caveat | Description |
|---|---|
| CSCtx26970 | **Symptom** AD Agent has no mapping to update or replicate to consumer devices.<br><br>**Conditions** This issue occurs when you upgrade AD Agent, Release 1.0.0.32 with AD Agent, Release 1.0.0.32.1.<br><br>**Conditions** Uninstall AD Agent, Release 1.0.0.32 and install AD Agent, Release 1.0.0.32.1. |

# Open Caveats in Cisco Active Directory Agent Release 1.0.0.32

*Table 3 Open Caveats in Active Directory Agent Release 1.0.0.32*

| Caveat | Description |
|---|---|
| CSCti71996 | **Symptom** When a user logs into a machine, it may happen that two events are written to the controller's event log instead of a single event. As a result, two events are forwarded to the AD Agent. On rare occasions, the second event has a later timestamp (one second later) and the AD Agent sends two updates to the registered client devices regarding this login event.<br><br>**Workaround** None. This defect does not affect the functionality in any way. Two notifications are sent to the registered client devices instead of one. |

*Table 3 Open Caveats in Active Directory Agent Release 1.0.0.32 (continued)*

| Caveat | Description |
|---|---|
| CSCto34206 | **Symptom** On Windows 2008 R2 machines, some events are not written in their Security Log and are missing.<br><br>**Conditions** This issue occurs when the Active Directory (AD) server machine has one CPU, is under stress, writes events at an extremely high rate (1000/sec or more), and the number of written events is extremely high (over one million events).<br><br>**Workaround** None. The issue is with the AD server security event log. |
| CSCto86228 | **Symptom** The WMI Service on the domain controller machine halts operation, and the AD Agent reports the status of the domain controller machine as "down(no-retry)."<br><br>**Conditions** This issue might sometimes occur when you stop and start the AD Agent multiple times.<br><br>**Workaround** Restart the WMI Service on the domain controller machine, and then erase and create the domain controller machine in the AD-Agent (or restart the AD Agent). |
| CSCtq45780 | **Symptom** When installing the AD Agent directly on domain controller, the AD Agent cannot monitor domain controllers in other trusted domains.<br><br>**Conditions** This issue occurs in a multiple domain environment, only when installing the AD Agent directly on a domain controller. This issue does not exist on a single domain architecture.<br><br>**Workaround** If the client is monitoring more than one domain, the installation should be done on a member server (a machine that is not a domain controller) or install it on more than one domain. |

*Table 3 Open Caveats in Active Directory Agent Release 1.0.0.32 (continued)*

| Caveat | Description |
|---|---|
| CSCtr90042 | **Symptom** AD Agent does not accept domain names that do not contain the character "." (dot) in them.<br><br>**Conditions** This issue occurs when the domain name is a single word without a DNS domain. The domain name is not accepted and the following message is displayed:<br><br>`Error: Parameter '-domain' value 'wga' is not full DNS name of AD domain!`<br>`For further syntax information use: 'adacfg help dc'`<br><br>**Workaround** Micorsoft recommends to have domain names using the character "." (dot). This was not enforced prior to Windows OS 2008.<br><br>The following Microsoft links provide further information:<br>• Naming conventions in Active Directory<br>http://support.microsoft.com/kb/909264<br>• Information about configuring Active Directory domains by using single-label DNS names<br>http://support.microsoft.com/kb/300684 |

# Documentation Updates

*Table 4 Updates to Release Notes for the Cisco Active Directory Agent, Release 1.0*

| Date | Description |
|---|---|
| 4/9/2012 | Added the following sections:<br>• Upgrading the Active Directory Agent Software Release 1.0.0.32 to Active Directory Agent Software Release 1.0.0.32.1, page 3<br>• Resolved Caveats in Cisco Active Directory Agent Release 1.0.0.32.1, page 3<br>• Open Caveat in Cisco Active Directory Agent Release 1.0.0.32.1, page 4 |
| Sep 27, 2011 | Resolved CSCtr90042 |
| June 13, 2011 | Cisco Active Directory Agent, Release 1.0 |

# Related Documentation

## Release-Specific Documentation

Table 5 lists the product documentation available for the AD Agent, Release 1.0.

***Table 5 Product Documentation for the Active Directory Agent***

| Document Title | Location |
|---|---|
| Installation and Setup Guide for the Cisco Active Directory Agent, Release 1.0 | http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ad_agent_setup_guide.html |
| Release Notes for the Cisco Active Directory Agent, Release 1.0 | http://www.cisco.com/en/US/docs/security/ibf/release_notes/ibf10_rn.html |
| Open Source Used in Cisco Active Directory Agent 1.0 | http://www.cisco.com/en/US/docs/security/ibf/open_source_license_document/ipcentral.pdf |

## Other Related Documentation

Links to Adaptive Security Appliance (ASA) 5500 Series Release 8.4.2 documentation and Ironport Web Security Appliance (WSA) documentation are available on Cisco.com at the following locations:

- Cisco ASA 5500 Series Adaptive Security Appliances Page

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco Ironport Security Management Appliances Page

  http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.