# Release Notes for Cisco Cloud Web Security Connector, Release 3.0

**Last Updated: November 6, 2013**

This document includes the following sections:

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

# Introduction

These release notes are for the following releases:

- Cisco Cloud Web Security Connector 3.0.1.2
- Cisco Cloud Web Security Connector 3.0.1.1
- Cisco Cloud Web Security Connector 3.0.1.0
- Cisco Cloud Web Security Connector 3.0.0.3
- Cisco Cloud Web Security Connector 3.0.0.2
- Cisco Cloud Web Security Connector 3.0.0.1
- Cisco Cloud Web Security Connector 3.0.0.0

# Downloading the Latest Version of Cisco Cloud Web Security Connector

To download the latest version of Cisco Cloud Web Security Connector, you must be a registered user of Cisco Cloud Web Security.To obtain the Cisco Cloud Web Security Connector 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 the required version of **Connector** (Windows or Linux).

**Step 5** Follow the instructions in the *Connector Administrator Guide, Release 3.0* to install the package.

# New Features in Release 3.0.1.2

Cisco Cloud Web Security Connector 3.0.1.2 is a maintenance release that resolves the list of caveats in Table 1. This release is compatible with Red Hat Enterprise Linux / CentOS versions 5.4 and greater.

**Note** Connector 3.0.1.2 does not support 64-bit Java on 64-bit Linux. Customers who are using this configuration are advised to switch to 32-bit Java before upgrading to Connector 3.0.1.2.

When using Connector, the following actions are now supported.

- Download files greater than 4GB through Microsoft TMG 2010.
- Preemptive basic authentication.
- Forwarding traffic directly to the destination server either by default or as a failover if the proxy server is unavailable.
- User lookup by User Principal Name (UPN).

- Bind to a specific IP address before connecting to a Cloud Web Security proxy server.

Microsoft Sharepoint and applications that start NTLM handshake on non-persistent connections are now supported by Connector.

**Note** If you are using Microsoft Forefront TMG 2010, you must upgrade to Forefront TMG 2010 SP1 before upgrading to Cloud Web Security Connector 3.0.1.2.

# New Features in Release 3.0.1.1

Cisco Cloud Web Security Connector 3.0.1.1 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 3.0.1.0

Cisco Cloud Web Security Connector 3.0.1.0 is a maintenance release that resolves the list of caveats in Table 4. Connector 3.0.1.0 removes the limit of 250 concurrent SSL connections to the proxy server.

# New Features in Release 3.0.0.3

Cisco Cloud Web Security Connector 3.0.0.3 is a maintenance release that resolves the list of caveats in Table 6. This release does not introduce any new features.

# New Features in Release 3.0.0.2

Cisco Cloud Web Security Connector 3.0.0.2 is a maintenance release that resolves the list of caveats in Table 8. This release does not introduce any new features.

# New Features in Release 3.0.0.1

Cisco Cloud Web Security Connector 3.0.0.1 is a maintenance release that resolves the list of caveats in Table 10. This release does not introduce any new features.

# New Features in Release 3.0.0.0

Cisco Cloud Web Security Connector 3.0.0.0 resolves the list of caveats in Table 12. This release introduces support for NTLM pass-through.

# System Requirements

Cisco Cloud Web Security Connector is a lightweight server application that enables granular policy and reporting in Cisco Cloud Web Security. Connector can support up to 2,000 seats.

Cisco recommends deploying Cloud Web Security Connector on a Cisco UCS C210 M2 server. For further information see http://www.cisco.com/en/US/products/ps10889/index.html. If you are using a different server, it should have at least a dual core CPU with 4GB of RAM.

**Note** Cisco Cloud Web Security Connector is not supported in virtualized environments. Multiple instances of Connector on a single server are not supported.

The following sections show the supported Windows and Linux versions.

### Windows Versions

- Windows Server 2003 x86 (32-bit)
- Windows Server 2003 R2 x86 (32-bit)
- Windows Server 2008 x86 (32-bit) and x64 (64-bit)
- Windows Server 2008 R2 x64 (64-bit)

### Linux Versions

- Red Hat Enterprise Linux 6 x86 (32-bit) and x64 (64-bit).
- CentOS 6 x86 (32-bit) and x64 (64-bit).
- Red Hat Enterprise Linux 5 x86 (32-bit) and x64 (64-bit).
- CentOS 5 x86 (32-bit) and x64 (64-bit).

# Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

- Cisco Cloud Web Security Connector 3.0.1.2 Caveats
- Cisco Cloud Web Security Connector 3.0.1.1 Caveats
- Cisco Cloud Web Security Connector 3.0.1.0 Caveats
- Cisco Cloud Web Security Connector 3.0.0.3 Caveats
- Cisco Cloud Web Security Connector 3.0.0.2 Caveats
- Cisco Cloud Web Security Connector 3.0.0.1 Caveats
- Cisco Cloud Web Security Connector 3.0.0.0 Caveats

## Cisco Cloud Web Security Connector 3.0.1.2 Caveats

### Caveats Resolved by Release 3.0.1.2

Table 1 lists the caveats that Cisco Cloud Web Security Connector 3.0.1.2 resolves.

*Table 1 Caveats resolved by Cisco Cloud Web Security Connector 3.0.1.2*

| ID | Headline |
|---|---|
| BUG-2860 | Accept lack of boundary value for multipart Content-Type |
| EE-66 | Add support in Connector for Expect header and 100 (Continue) status code. |
| EE-132 | Option to use the Client IP from the X-Forwarded-For header if it exists in the HTTP request message. |
| EE-129 | NTLM settings are not retained in Connector Configuration Wizard. |
| EE-135 | log4j prints XML parsing warning message. |
| EE-137 | Connector requires periodic restart when primaryProyType=SSL |
| EE-143 | NTLM cache key causes frequent authentication against Active Directory. |

## Open Caveats in Release 3.0.1.2

There are no known unresolved caveats in Cisco Cloud Web Security Connector 3.0.1.2.

# Cisco Cloud Web Security Connector 3.0.1.1 Caveats

## Caveats Resolved by Release 3.0.1.1

Table 2 lists the caveats that Cisco Cloud Web Security Connector 3.0.1.1 resolves.

*Table 2 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.1.1*

| ID | Headline |
|---|---|
| EE-125 | Group Lookup Settings not populated in Connector installation Wizard |
| EE-115 | Add thread keepalive configuration property for the thread pool |
| EE-116 | Support NTLMv2 for user identification only |
| EE-122 | Add existing groupInclude property to the default agent.properties file |

## Open Caveats in Release 3.0.1.1

Table 3 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.1.1.

*Table 3 Caveats Open in Cisco Cloud Web Security Connector 3.0.1.x*

| ID | Headline |
|---|---|
| EE-66 | Add support in Connector for Expect header and 100 (Continue) status code. |

# Cisco Cloud Web Security Connector 3.0.1.0 Caveats

## Caveats Resolved by Release 3.0.1.0

Table 4 lists the caveats that Cisco Cloud Web Security Connector 3.0.1.0 resolves.

*Table 4 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.1.0*

| ID | Headline |
|---|---|
| BUG-2333 | Support downloading files larger than 4GB through Connector and TMG 2010. |
| BUG-2345 | Connector fails to start on new versions of Linux. |
| BUG-2352 | Support Preemptive Basic Authentication. |
| BUG-2428 | HTTP requests not handled properly when a user name is not provided during NTLM authentication. |
| BUG-2440 | Basic Authentication Pass-Through not supported. |
| BUG-2453 | AUP looping when persistent connections are enabled. |
| BUG-2523 | Enable Connector to forward all traffic directly to destination Web server either as default configuration or as failover if Scanning Proxy is unreachable. |
| BUG-2565 | Support user lookup by User Principal Name (UPN). |
| BUG-2688 | Authentication pop up with Citrix. |
| BUG-2712 | Add support in Connector for applications that start NTLM handshake on non-persistent connections, for example SharePoint. |
| BUG-2759 | Connector does not enable SO_REUSEADDR before attempting to bind the server socket to port 8080. |
| EE-73 | Do not forward an unexpected Proxy-Authorization header directly to an origin server. |
| EE-102 | Provide option to bind to a specific IP address before opening a connection to the proxy. |
| EE-118 | Remove 250 SSL Connection Limit |

## Open Caveats in Release 3.0.1.0

Table 5 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.1.0.

*Table 5 Caveats Open in Cisco Cloud Web Security Connector 3.0.1.0*

| ID | Headline |
|---|---|
| EE-66 | Add support in Connector for Expect header and 100 (Continue) status code. |

# Cisco Cloud Web Security Connector 3.0.0.3 Caveats

## Caveats Resolved by Release 3.0.0.3

Table 6 lists the caveats that Cisco Cloud Web Security Connector 3.0.0.3 resolves.

*Table 6 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.0.3*

| ID | Headline |
|---|---|
| BUG-2565 | Connector losing granularity after LDAP server being taken off line and comes back on line. |
| EE-86 | Provide full user granularity when the Connector is configured for persistent connections and basic auth using generic LDAP. |

## Open Caveats in Release 3.0.0.3

Table 7 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.0.3.

*Table 7 Caveats Open in Cisco Cloud Web Security Connector 3.0.0.3*

| ID | Headline |
|---|---|
| BUG-2440 | Basic Authentication Pass-Through not supported. |
| BUG-2345 | Connector fails to start on new versions of Linux. |
| BUG-2523 | Requests sent to the wrong server when primaryProxy=DIRECT in agent.properties. |

# Cisco Cloud Web Security Connector 3.0.0.2 Caveats

## Caveats Resolved by Release 3.0.0.2

Table 8 lists the caveats that Cisco Cloud Web Security Connector 3.0.0.2 resolves.

*Table 8 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.0.2*

| ID | Headline |
|---|---|
| EE-67 | Provide full user granularity when the Connector is configured for persistent connections and NTLM. |

## Open Caveats in Release 3.0.0.2

Table 9 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.0.2.

*Table 9 Open Caveats in Cisco Cloud Web Security Connector 3.0.0.2*

| ID | Headline |
|---|---|
| BUG-2565 | Connector losing granularity after LDAP server being taken off line and comes back on line. |
| BUG-2440 | Basic Authentication Pass-through to Origin Server not working with Connector versions 3.0.0.0 and above. |
| BUG-2345 | Connector fails to start on RedHat / CentOS Linux versions greater than 5.4. |
| BUG-2523 | Connector should not send requests to the wrong server when filtering service is bypassed completely (by setting primaryProxy=Direct in agent.properties). |

# Cisco Cloud Web Security Connector 3.0.0.1 Caveats

## Caveats Resolved by Release 3.0.0.1

Table 10 lists the caveats that Cisco Cloud Web Security Connector 3.0.0.1 resolves.

*Table 10 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.0.1*

| ID | Headline |
|---|---|
| BUG-2464 | Fixed intermittent loss of granularity problem. |

## Open Caveats in Release 3.0.0.1

Table 11 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.0.1.

*Table 11 Caveats Open in Cisco Cloud Web Security Connector 3.0.0.1*

| ID | Headline |
|---|---|
| EE-67 | Provide full user granularity (not just internal IP) for all HTTP requests |
| BUG-2565 | Connector losing granularity after LDAP server being taken off line and comes back on line. |
| BUG-2440 | Basic Authentication Pass-through to Origin Server not working with Connector versions 3.0.0.0 and above. |
| BUG-2345 | Connector fails to start on RedHat / CentOS Linux versions greater than 5.4. |
| BUG-2523 | Connector should not send requests to the wrong server when filtering service is bypassed completely (by setting primaryProxy=Direct in agent.properties). |

# Cisco Cloud Web Security Connector 3.0.0.0 Caveats

## Caveats Resolved by Release 3.0.0.0

Table 12 lists the caveats that Cisco Cloud Web Security Connector 3.0.0.0 resolves.

*Table 12 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.0.0*

| ID | Headline |
|---|---|
| SS-13434 | NTLM Pass-through to Origin Server not working with Connector. |
| SS-13344 | Changed companyId property type from int to long. |
| BUG-2277 | Fixed failover to secondary proxy over an SSL connection. |
| BUG-2263 | Find security groups when CN and sAMAccountName do not match. |
| BUG-2331 | Gracefully recover when the Content-Length header is missing. |
| EE-7 | Added support for CIDR format IP address ranges in "ntlmIpExceptions" property. |
| EE-8 | Support wildcards in the "groupInclude" property. |
| EE-10 | Support connectorId configuration property that appears in the telemetry data. |

*Table 12 Caveats Resolved by Cisco Cloud Web Security Connector 3.0.0.0*

| ID | Headline |
|---|---|
| EE-37 | Flush output stream after each write. (Part of WebEx fix.) |
| EE-39 | Improve logging during startup to help troubleshoot issues. |
| EE-41 | Trim trailing white space from the license key property to avoid problems during startup. |

## Open Caveats in Release 3.0.0.0

Table 13 lists the caveats that are unresolved in Cisco Cloud Web Security Connector 3.0.0.0.

*Table 13 Caveats Open in Cisco Cloud Web Security Connector 3.0.0.0*

| ID | Headline |
|---|---|
| BUG-2464 | Intermittent loss of granularity problem. |
| EE-67 | Provide full user granularity (not just internal IP) for all HTTP requests |
| BUG-2565 | Connector losing granularity after LDAP server being taken off line and comes back on line. |
| BUG-2440 | Basic Authentication Pass-through to Origin Server not working with Connector versions 3.0.0.0 and above. |
| BUG-2345 | Connector fails to start on RedHat / CentOS Linux versions greater than 5.4. |
| BUG-2523 | Connector should not send requests to the wrong server when filtering service is bypassed completely (by setting primaryProxy=Direct in agent.properties). |

# Related Documentation

For more information, see the following documents:

- *ScanCenter Administrator Guide, Release 5.2*
- *Connector Administrator Guide, Release 3.0*

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.