Release Notes for Cisco Dynamic Content Adapter Release 2.01

January 29, 2003

Contents

This document includes the following information:

Introduction

These release notes contain late breaking information about the Cisco Collaboration Server Dynamic Content Adapter (DCA), version 2.01. Please review this document before installing and using the DCA. For all other information, including installation and configuration instructions, see the DCA documentation set. Descriptions and links to the complete DCA documentation set are provided in the getstart.htm file at the top level of the DCA CD.

CISCO SYSTEMS

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

Supported Platforms

This release of the DCA 2.01 supports the following platforms. For information on additional platform support, consult your Cisco representative or subsequent DCA documentation.

Server Platform

Server Type	OS	Web Server	Servlet Engine
Windows	Windows 2000, with service pack 3	Microsoft Internet Information Server (IIS) 5.0	Servlet Exec 4.1 ISAPI

Collaboration Server Versions

The DCA 2.01 supports Cisco Collaboration Server (CCS) version 5.0. Both multi-session agent and single-session agent configurations are supported. For information on DCA 2.01's compatibility with other CCS releases, consult your Cisco representative.

Collaboration Server Agent and Caller Browsers

The DCA 2.01 supports the following browser versions for agents and callers. These are identical to the browsers supported by CCS 5.0 with the following exceptions: Netscape 4.x browsers are not supported on Windows 98 and 2000 operating systems; Netscape 6.2.3 caller browsers are not supported:

Agent Desktop	IE: 5.01 sp2 to 6.0 NS: 4.76 **Note:** Netscape 4.x versions are not supported by Windows 98 or Windows 2000.
Caller Desktop	AOL: 6.0 and 7.0 IE: 4.01 sp2 to 6.0 sp1 NS: 4.76, 4.78 and 7.0 **Note:** Netscape 4.x versions are not supported by Windows 98 or Windows 2000.

Note: CCS and the DCA do not support Mac browsers for agents or callers.

New Features

The DCA 2.01 includes these new features:

- **Collaboration Toolbar**: The Collaboration Toolbar is a set of content sharing controls that integrates with the Cisco Collaboration Server Agent and Caller desktops. It significantly extends content sharing capability for both Single-Session and Multi-Session CCS users.
- **Popup Window Collaboration**: Popup Window Collaboration lets DCA users collaborate on the contents of popup windows opened through JavaScript. If desired, you can turn off popup window sharing, or target only specific popups.
- **Automatic Form Sharing**: Automatic Form Sharing allows DCA users to share information entered in online form fields as it is being entered.
- **Elimination of Security Warnings to Callers**: Standalone Collaboration Server requires users to download a Java applet in order to share complex Web content. By eliminating the need for the applet, the DCA 2.01 also eliminates the security warnings CCS callers receive as it downloads.
- **Configurable Parser**: The DCA 2.01 includes a customizable HTML parser, that allows complete control over the DCA's page parsing and modification process. Many SPLIT content Collaboration issues that in the past might have required modification to a Web site can now be remedied through parser configuration.
- **Localization and Multi-Byte Character Support**: The DCA Admin Tool and Collaboration Toolbar interfaces can be localized into any language. Out of the box, the DCA 2.01 includes Admin Tool and Collaboration Toolbar localization for English, French, Spanish, German, Korean, and Chinese (Simplified). The DCA 2.01 parser supports parsing of multi-byte character documents.
- **Integrated DCA/CCS Sessions:** In DCA 2.01, each DCA session is linked automatically with a specific CCS session ID. Multi-session chat agents can switch seamlessly back and forth between concurrent CCS/DCA sessions. Terminating a CCS session automatically terminates its corresponding DCA session.
- **Integrated DCA/CCS Reporting:** The DCA maintains a communication channel that allows tracking of DCA session activity (i.e., page shares) for inclusion in CCS reports.
- **Browser Mapping**: The DCA 2.01's browser mapping feature allows you to map different browsers to a single browser type/version that represents a highest common denominator for those browsers. This ensures that the Web content delivered during a session is compatible with all of the browsers in use by session participants.
- **Remote Monitoring**: The DCA 2.01 includes an API that can be used to send events (for example, exceptions, requests served) to a third-party monitoring tool. This can allow you to determine the health of the DCA and even provide troubleshooting and correction before users experience poor performance.

Product Changes

The following DCA 1.0 features are discontinued in DCA 2.01:

- Customized Form code (used to automatically insert additional code after the last Form on a Web page)
- Snippets (used to automatically insert additional code into a Web page's source code)
- Agent link deadening (used to disable specific link types, for example, SUBMIT buttons, for agents in a DCA session)
- User patterns (used to define link parsing rules)

All of the behaviors available through these discontinued 1.0 features can be achieved in DCA 2.01 through parser configuration.

Known Caveats

This section contains up-to-date information on DCA 2.01 known issues and workarounds. Issues are arranged in the following categories:

Admin Tool Issues

NullPointerException appears in DCA Log

Symptom: Under a heavy load, a NullPointerException may appear in the DCA log file.

Conditions: This error is caused by an object in the DCA page tracking mechanism being cleaned up prematurely. The effect of this is to make a duplicate request for a page instead of serving it from the DCA's cache.

Workaround: None

Cisco Tracking Number: CSCma07185

Issues in the DCA Admin Tool UI

The following three issues exist in the DCA Admin Tool UI:

Symptom: The DCA Admin Tool does not include a Logout button. Workaround: Closing the browser window in which the Admin Tool is displayed will automatically log you out.

Symptom: The Admin Tool displays the wrong title ("Cisco UI Server") in its browser window title bar. Workaround: None

Symptom: By default, the Admin Tool displays a blank screen immediately after login. Workaround: None. Use the Admin Tool menu to navigate to the screen you want.

Cisco Tracking Numbers: CSCma10307; CSCma12644; CSCma12645

Cannot modify or delete entries in the RemoteMonitor.properties file through the Admin Tool

Symptom: When opened in the Admin Tool, you can add but not edit or delete entries in the RemoteMonitor.properties file.

Workaround: To modify or delete entries in RemoteMonitor.properties, open and edit the file in a text editor.

Cisco Tracking Number:CSCma13104

Unable to view log in the DCA Admin Tool if loaded in SSL mode

Symptom: Unable to view a log file through the DCA Admin Tool interface when using Internet Explorer with SSL.

Conditions: This occurs only when using SSL with Internet Explorer.

Workaround: Use another non-Internet Explorer browser or use regular HTTP to access the administration.

Cisco Tracking Number: CSCma18330

Netscape users must log back in after resizing their browser window

Symptom: When using the Admin Tool, Netscape users who resize their browser window are returned to the Admin Tool Login Page which displays the message: "You must specify a username."

Conditions: Occurs when Netscape users resize their browser window.

Workaround: None. Re-login to the Admin Tool.

Cisco Tracking Number: CSCma19811

Admin Tool may display incorrect number of session participants

Symptom: Under certain conditions, the DCA Admin Tool may display a larger number of participants than are actually in session.

Conditions: Occurs in integrated DCA-CCS when a user already in session reconnects to the DCA following a browser crash. While the old participant object (created before the browser crash) continues to persist, the DCA creates a new participant during the reconnect, thus causing a single user to appear as two participants in the Admin Tool.

Workaround: None. The superfluous participant will eventually time-out (based on the participant timeout setting) or be removed when the session ends.

Cisco Tracking Number: CSCma20084

Browser-Specific Issues

Internet Explorer 4.01 caller browser disappears after a page share

Symptom: For callers running IE 4.01, service pack 2, when a page is shared to them by an agent the caller browser disappears accompanied by a warning that the Active Desktop needs to be recovered after failing.

Conditions: The caller is using IE4.01 Service Pack 2, has Active Desktop turned on, and an agent attempts to share a page to the caller. This issue has been detected on NT and Windows 95. Note that CCS 4.0 supports IE 4.01 SP2 on callers only -- it is not supported on agents.

Workaround: Have caller turn off Active Desktop by right-clicking the desktop and unchecking the item labelled "View As Web Page."

Cisco Tracking Number: CSCma18728

Internet Explorer 5.01 client experiences intermittent crashes

Symptom: IE 5.01 experiences intermittent crashing when users reload the Collaboration Toolbar.

Conditions: Toolbar reloading is necessary if and when a DCA user closes the Collaboration Toolbar's browser window during a session. The source of this issue is related to IE 5.01's known issues with window handles of closed windows. Less frequent crashing of IE 5.01 during regular DCA use (unrelated to Toolbar reloading) has also been reported. Microsoft has ended support for IE 5.01.

Workaround: None.

Cisco Tracking Number: CSCma18239

Collaboration Toolbar does not properly reopen in Internet Explorer after a browser shutdown

Symptom: When logging an agent back into an existing CCS/DCA session after shutting down Internet Explorer, the DCA Collaboration Toolbar does not reopen properly.

Conditions: If, as the result of a browser crash or some other unspecified reason, a DCA user shuts down and reopens Internet Explorer, the following behaviors occur: 1) The Collaboration Toolbar opens in the CCS internal view, rather than the external view as it should; 2) the Toolbar does not automatically reload the Web page the user was viewing when IE was shut down. This behavior has been detected in IE 5.01, IE 5.5, and IE 6.0.

Workaround: After logging back in to CCS, the agent must 1) Click the CCS external View button to send the Collaboration Toolbar to the CCS external view window, and 2) click the Reload Toolbar button to reload the correct Web page in the Toolbar.

Cisco Tracking Number: CSCma18311

Netscape agents using SSL experience difficulty loading the Collaboration Toolbar

Symptom: When using SSL mode, Netscape agents are sometimes unable to load the Collaboration Toolbar.

Conditions: When a Netscape agent enters a CCS session, the Collaboration Toolbar should load automatically in the CCS external view. However, when utilizing SSL, the Collaboration Toolbar sometimes does not load properly. This is due to Netscape's default behavior by which it does not cache pages accessed over an SSL connection.

Workaround: Make the agent's Netscape browser cache pages over the SSL link. To do this, the following line must be added to the end of the prefs.js file located in the Users/default directory under the Netscape installation directory.

user_pref("browser.cache.disk_cache_ssl", true);

Cisco Tracking Number: CSCma18703

Virus scan causes the Collaboration Toolbar to run slowly on Netscape 4.x

Symptom: Virus Scan running on the client can cause the Collaboration Toolbar to run slowly on Netscape 4.x

Conditions: This is a common and known issue not specific to the DCA. It primarily affects Netscape 4.x. The problem stems from VirusScan blocking the download of files while it is scanning them repeatedly before the download is complete.

Workaround: None. If feasible, turn off virus scan.

Cisco Tracking Number: CSCma17968

Netscape client responds slowly to DCA events

Symptom: Netscape 4.x users may experience intermittent slow response to DCA events (for example, a page share).

Conditions: This is a common and known issue not specific to the DCA. It is most noticeable with Netscape running on Windows 2000 (an unsupported platform) but also occurs less frequently on the Windows 98 (unsupported) and NT. The behavior is the result of Netscape's underlying use of Windows' socket layer. It stems from a change in the Windows network implementation that causes HTTP POST transactions to not terminate properly, requiring the POST connection to timeout before completing. DCA clients use POST transactions frequently.

Workaround: None.

Cisco Tracking Number: CSCma18890

Netscape clients not receiving page shares through Netscape Proxy

Symptom: Netscape clients receiving content via a Netscape proxy do not receive page shares.

Conditions: This issue appears to result from the failure of DCA LongPoll events that normally pass between the DCA and client to negotiate the proxy. Internet Explorer clients appear to function properly and receive page shares through Netscape proxies.

Workaround: None.

Cisco Tracking Number: CSCma19131

Collaboration Toolbar Issues

Action Canceled page displays during download of unknown file type

Symptom: Downloading an unknown file type causes the page currently displayed in the Collaboration Toolbar to be replaced with a page displaying the message "Action Canceled." If the user downloading the file has automatic page sharing turned on, this Action Canceled page is also shared to other session participants.

Conditions: Examples of unknown file types may include exe, pdf, zip -- any file type that does not have a helper application or plugin associated with it on the client. Normal browser behavior is to prompt the user for download confirmation while leaving the current Web page loaded in the browser. Note that this issue does not prevent the file from downloading.

Workaround: Users can use the Back button on the Collaboration Toolbar to return to the previous page.

Cisco Tracking Number: CSCma18176

Multi-Session agents lose page history after switching sessions

Symptom: The Collaboration Toolbar's page history is cleared when multi-session agents switch between sessions. This prevents using the Forward and Back buttons to navigate between pages.

Conditions: The DCA does not track history on a per-session basis. Therefore, this is expected behavior, necessary to prevent visited pages from concurrent sessions becoming part of the same history

Workaround: Preclude the need for Forward-Back button navigation for MS agents through use of links in CCS ScriptBuilder. Agents should also use navigation controls provided by the content they are sharing rather than browse history.

Cisco Tracking Number: CSCma18729

Multi-Session agents lose Form Share and FollowMe state after switching sessions

Symptom: Form Sharing and FollowMe are automatically turned off when a Multi-Session agent switches sessions.

Conditions: This is expected behavior. If Form Sharing and FollowMe were not turned off, they would automatically trigger a page share when the agent switched back into session, potentially overwriting data a caller had entered in a form in the interim.

Workaround: None

Cisco Tracking Number: CSCma18749

DCA callers can receive the agent Collaboration Toolbar configuration

Symptom: Callers may mistakenly receive the Collaboration Toolbar configuration intended for agents (agents are typically given access to a fuller control set).

Conditions: This can occur if a caller logs into the same CCS server as agent using a different server/domain name (for example, the agent accesses the CCS server using http://ccsserver, while the caller accesses the server using http://ccsserver.mydomain.com.

Workaround: Ensure that both callers and agents access the CCS server using the same server/domain name.

Cisco Tracking Number: CSCma18889

Using Remote Control commands disables agents' Back/Next buttons

Symptom: The Back and Next buttons on the agents Collaboration Toolbar are automatically disabled when an agent uses any Remote Control command (Page Share, FormShare, Follow Me). These buttons will be re-enabled after subsequent navigation; however, any navigation history accumulated in the period prior to Remote Control use will be lost.

Conditions: Normal use.

Workaround: None. Train agents accordingly.

Cisco Tracking Number: CSCma19663

At start of new session, Toolbar displays last shared page from previous session

Symptom: If an agent alternates between Single and Multi CCS sessions, the DCA Collaboration Toolbar may display the last shared page from a previous session at the start of a new session.

Conditions: Occurs when a Single-Session agent logs out of CCS, and then logs back in as a Multi-Session agent without first closing all open browser windows.

Workaround: Have Single-Session agents close all browser windows before logging back into CCS as Multi-Session agents.

Cisco Tracking Number: CSCma18350

Using Follow ME command causes agent to lose form data

Symptom: In a scenario in which an agent and caller are alternately completing fields in a form, using the Follow Me or Remote Control Follow Me command may cause the agent to lose form data.

Conditions: Occurs under the following conditions. Steps must be recreated exactly to trigger the error:

Scenario 1:

1. Agent modifies a form and uses Form Share to share the data to a caller.

2. Caller modifies the form. Agent uses Remote Control Form Share to get the caller data.

3.Agent modifies a form and uses Form Share to share the new data back to the caller.

4. Agent clicks Remote Control Follow Me command (it does not matter whether or not the caller has modified the form immediately prior to this).

The error occurs when step 4 is performed. The form data on the Agent Desktop is rolled back to what is was at the conclusion of step 2.

Conditions: Occurs under the following conditions. Steps must be recreated exactly to trigger the error:

Scenario 2:

1. Caller modifies a form. Agent uses Remote Control Form Share to get the caller data.

2. Agent modifies the form and uses Form Share to share the data to the caller.

3. Caller modifies the form. Agent uses Remote Control Form Share to get the new caller data.

4. Agent clicks Follow Me command (it does not matter whether or not the agent has modified the form immediately prior to this).

The error occurs when step 4 is performed. The form data on the Agent Desktop is rolled back to what is was at the conclusion of step 2.

Workaround: In a scenario in which an agent and caller are alternately completing fields on a form, agent should avoid using the Follow Me/Remote Control Follow Me commands. Instead, use only the Form Share/Remote Control Form Share Commands to pass the data back and forth.

Cisco Tracking Number: CSCma20222

Last disconnected caller appears to persist in session

Symptom: After disconnecting the last caller from a session, that caller's name continues to appear in the Collaboration Toolbar's Remote Control user list. Additionally, the last page shared during the session continues to be displayed, and the Collaboration Toolbar's sharing buttons remain active.

Conditions: Occurs in Multi-Session Agent desktop configurations after an agent has ended a session. While the Agent Desktop correctly shows that the session has ended, the caller's name continues to appear in the user list, and the last shared page continues to display.

Workaround: The caller's name will be removed automatically when the agent enters a new session. Optionally, agents can also refresh the Toolbar display by clicking the External View button on the Agent Desktop.

Cisco Tracking Number: CSCma20202

Resizing NS 4.x window during Form Sharing causes form to be reset

Symptom: When a Netscape 4.x user in the act of receiving a Form Share resizes his browser window, the form is reset and any form data received prior to that point is lost.

Conditions: Occurs in Netscape 4.x browsers running on Windows 2000.

Workaround: In the case of a Netscape 4.x caller receiving a Form Share from an agent, the agent should turn Form Share off and then back on again. This will trigger a resend of the entire page along with any form data.

In the case of a Netscape 4.x agent receiving a Form Share from a caller, (via Remote Control Form Sharing) the agent should turn Remote Control Form Share off and then back on again.

Cisco Tracking Number: CSCma22242

"Hidden" CCS sharing controls appear the first time a new SS agent logs into CCS

Symptom: In some instances, the very first time a a Single-Session agent logs into CCS, sharing controls on the CCS Agent Desktop that are normally overridden and hidden by the DCA (for example, the Page Share button) are visible.

Conditions: Occurs the first time a new Single-Session agent logs into CCS from any PC. Frequency is sporadic -- does not happen for all new SS agents.

Workaround: Have the agent log out and back into CCS. After the initial login, the issue does not reoccur.

Cisco Tracking Number: CSCma22300

Second agent in session unable to receive page shares from first agent

Symptom: In some instances, when an additional Single-Session agent joins an existing CCS session, the additional agent is unable to receive page shares from other agents in the session (the new agent CAN receive and share pages with the caller).

Conditions: Occurs infrequently. In those instances where it occurs, the problem is noticeable immediately upon the first page share.

Workaround: Have the new agent log out and back into CCS.

Cisco Tracking Number: CSCma22389

Reload Toolbar command crashes IE 4.01, IE 5.01 sp2, and NS 7.0 caller browsers

Symptom: When an agent clicks the Reload Toolbar button (located on the CCS Agent Desktop Caller Info page), it crashes the Collaboration Toolbar browser window for callers using Internet Explorer 4.01, IE 5.01sp2, or Netscape 7.0.

Conditions: Occurs regularly with callers on Internet Explorer 4.01, IE 5.01sp2, or Netscape 7.0 when an agent clicks the Reload Toolbar button AND the Collaboration Toolbar browser window is open on the caller side. Note that the agent is not affected.

Workaround: The purpose of the Reload Toolbar button is specifically to reload the Collaboration Toolbar browser window for callers after a crash. Therefore, it is unlikely that agents will click this button when that window is open on the caller side. Nonetheless, when in session with callers using Internet Explorer 4.01, IE 5.01sp2, or Netscape 7.0, agents should verify that the callers' Collaboration Toolbar browser window i closed before using the Reload Toolbar command.

Cisco Tracking Number: CSCma23472 (NS 7.0), CSCma23484 (IE 4.01), and CSCma23556 (IE 5.01sp2)

Reload Toolbar does not display for Multi-Session agents running NS 4.x

Symptom: The Reload Toolbar button does not display for Multi-Session chat agents using Netscape 4.x (this button normally displays on the Caller Info page in the CCS Agent Desktop).

Conditions: Occurs for Multi-Session agents running Netscape 4.x. Occurs because the HTML that specifies this button does not include it within a FORM tag (Netscape 4.x can only render buttons that are wrapped in a FORM tag).

Workaround: Modify line 261 in the \pub\html\multichatui\callerinfo.jhtml file from this:

```
<INPUT type=button value="Reload Toolbar" onClick=reloadconsole()>
```

To this:

```
<FORM><INPUT type=button value="Reload Toolbar"
onClick=reloadconsole()></FORM>
```

Cisco Tracking Number: CSCma23573

Installation-Uninstallation Issues

Servlet Exec is incompatible with other servlet engines

Symptom: ServletExec is incompatible with other servlet engines and may not install properly if another servlet engine is installed on your DCA Server.

Workaround 1: Cisco recommends installing the DCA on a "clean" machine. If another servlet engine was previously installed on the server on which you are installing the DCA, it must be completely removed before the DCA can be installed. For more information, consult the ServletExec Installation Guide.

Cisco Tracking Number: none

Uninstalling the DCA-CCS updater does not remove the DCA directory

Symptom: Uninstalling the DCA does not remove the DCA directory. The uninstall procedure does not alert you to this fact.

Conditions: Occurs when you uninstall the DCA.

Workaround: After uninstalling the DCA, manually delete the DCA install directory.

Cisco Tracking Number: CSCma00451

Uninstalling the DCA-CCS updater does not remove agent UI settings written to the CCS database

Symptom: After uninstalling DCA-CCS updater, clicking the External View button in the Single-Session Agent desktop causes the external view window to close and reopen (rather than toggling the window between internal and external view as it should).

Conditions: This results from the fact that after a login, Single-Session agent UI preference settings are written to the CCS database. Uninstalling the DCA-CCS updater does not delete these database entries.

Workaround: Using any SQL tool (for example, Query Analyzer for MSSQL Server or PL/SQL for Oracle Server) access the CCS database, and execute the following SQL command:

(for Query Analyzer)

```
Delete AGENT_ROLE_OVERRIDE_PROPERTY
```

(for PL/SQL)

```
Delete from AGENT_ROLE_OVERRIDE_PROPERTY;
```

This will delete all information contained in the AGENT_ROLE_OVERRIDE_PROPERTY. Once the CCS server has been restarted, when agents log in, they will use the properties set in agent.properties (on the server).

Cisco Tracking Number: CSCma21326

Parsing Issues

Some Web content may not parse correctly with the DCA's default parser configuration

Symptom: Some content served through the DCA does not work properly or does not display correctly.

Conditions: Some content may be created in such a way that URLs embedded in the content are not parsed and reformatted correctly by the DCA parser. This type of problem is frequently seen when links are processed in JavaScript. Similar problems may occur with JavaScript content, where the DCA does not parse the script content correctly, resulting in a script that has errors or no longer functions as intended.

Workaround: The DCA parser can be customized to address problems with specific content.

Cisco Tracking Number: CSCma1851 and CSCma22149

Applets and Flash Movies not displaying

Symptom: Some applets and Flash objects do not download correctly -- appearing instead as gray boxes on Web pages viewed through the DCA.

Conditions: This is a parsing issue related to applets that do not have a codebase attribute defined for them (applets that have codebase attributes display correctly).

Workaround: Parser customization, or define the codebase attribute for affected files.

Cisco Tracking Number: CSCma18638

JavaScript links that render HTML directly are not parsed

Symptom: JavaScript links that render HTML directly, bypassing document.write () will not be parsed and may result in the browser not sharing the resulting page.

Conditions: Links formed using the protocol "javascript:" in the HREF portion of a link tag automatically replace the target of the link (which is normally the page the link resides in) with the results of whatever the JavaScript returns. In the case of function that return nothing, it does not change the page location and just executes the code. The link can be forced to behave like that even when the function call returns a value by adding "void(0);" to the end of the link. That function call always returns

nothing, preventing the unload of your content. DCA can't catch the text rendered by the JavaScript function before it loads into the page, and therefor cannot support this method of writing out documents. This is an relatively rare usage of JavaScript, and there are web sites devoted to urging content designers to stop using it altogether.

Workaround: Use standard document.write() or document.writeln() calls in conjunction with void(0); these result in the DCA client side parser handling the text generated into the page and the correct links being generated.

Cisco Tracking Number: CSCma19892Popup Window Issues

IE 6.x browsers support only limited popup window sharing functionality

Symptom: Internet Explorer 6.x users (both agents and callers) cannot share updates to the contents of popup windows (by using Page Share, Form Share, Follow Me). Additionally, IE 6.x users can receive, but not originate shares of popup window open events. The following behaviors occur:

- IE 6.x users cannot share out updates to the contents of popup windows. Other session participants, regardless of their browser type/version will not receive the shared data. For example, if an IE 6.x agent completes a form in a popup window and clicks Form Share, callers, regardless of their browser type/version, will not receive the updated contents of the form.

- Similarly, IE 6.x users cannot receive shares of updates to the contents of popup windows from other participants, regardless of the others participants' browser type/version. For example, if a caller using NS 7.0 completes a form in a popup window and clicks Form Share, an IE 6.x agent will not receive the updated contents of the form.

- IE 6.x users can receive but not originate shares of popup window open events. For example, if a caller using NS 7.0 opens a popup window and clicks Page Share, the popup WILL open for an IE 6.x agent. However, if the IE 6.x agent opens a popup and clicks Page Share, the popup will not open for the caller, regardless of the caller's browser type/version.

- Note: IE 6.x agents CAN get updated contents of non-IE 6.x caller popup windows by using sharing commands in the Remote Control tool set. For example, if a caller using NS 7.0 completes a form in a popup window, an IE 6.x agent can click Form Share in the Remote Control tool set to get the updated contents of the form.

Conditions: Affects Internet Explorer 6.x on all platforms. The problem is related to IE 6's handling of popups whereby each new window acts as a new browser in terms of COM objects and prevents JavaScript access to the window.

Workaround: If popup window sharing is required for your site, do not deploy IE 6.x browsers to agents. Train agents to examine callers' browser type/version (on the CCS Caller Information page), and to use only basic popup window sharing with IE 6.x callers. Train IE 6.x agents to use Remote Control to get updates to the contents of non-IE 6.x caller popups.

Cisco Tracking Number: CSCma22029

Users receive a JavaScript error when closing popup windows

Symptom: Users intermittently receive an "Unspecified" JavaScript error when closing a popup window. "Object not found" messages also accompany the event.

Conditions: This typically results from a race issue occurring on pages that contain interdependent scripts and which are unloaded before JavaScript has had time to complete loading. The error is often in the content itself and results from miscommunication between frames and/or scripts when all or some of the content failed to load.

Workaround 1: Sites that do not require the sharing of content in popup windows can disable automatic popup window sharing. Note however, that once this is done, popup window sharing will not occur.

To disable automatic popup window sharing:

1. Open the `proxy_rules_include_text.xml` file located at: `<DCArootdirectory>\webapp\WEB-INF\Cisco\properties`
2. Uncomment the following line of code in the file:

   // groupStr+="var _DCA_stopSharingPopups=true;";
3. Restart the DCA.

Workaround 2: Sites that want to share popups and are willing to modify their Web content, can modify the JavaScript use to call specific popups they wish to share.

To do this:

1. Disable automatic popup window sharing as described in Workaround #1, above.
2. For popup windows whose content you want to share though the DCA, replace the JavaScript "window.open()" call normally used to open the window with the following:

   ```
   if(typeof _DCA_windowOpen!="undefined")_DCA_windowOpen(arguments);
   else window.open();
   ```

   Note that any popup window opened during a DCA session by methods other than this code will not be sharable. This code will not adversely affect the normal behavior of windows in which it is inserted. Its syntax ensures that windows it calls will open normally in non-DCA contexts.

Cisco Tracking Number: CSCma19130

Popup windows unable to load content in SSL

Symptom: In SSL mode, popup windows opened using window.open(this.href) may be unable to load content.

Conditions: Using window.open(this.href) to open a popup results in a URL that is parsed twice by the DCA, therefore containing a duplicate DCA thread. For example, a popup called using:

<a href="http://www.somesite.com" OnClick="window.open(this.href); return false;">

will result in a URL formatted as:

http://mydcaserver.mydomain.com/DCA/http/mydcaserver.mydomain.com/DCA/http/www.somesite.com).

In non-SSL mode this URL, while not desirable, will nevertheless function correctly. However, in SSL mode, because the duplicate thread causes the DCA to attempt to access itself, the URL will fail to load in the window.

Workaround: Do not use (this.href) to specify URLs in window.open calls. Specify an actual URL instead.

Cisco Tracking Number: CSCma19569

IE 5.01 and IE 6.0 callers receive a JavaScript error when sharing identically named popup windows

Symptom: Timing related JavaScript errors may occur in the caller browser during popup window sharing. The error message the caller receives can vary, determined in part by whether the browser's "Disable script debugging" option is selected. The error messages may consist of:

- "A null reference was passed to the stub." (IE 6.0)
- "Unspecified Error" (most common)
- "Object Expected"
- "Error in Unknown Source"

Conditions: Affects Internet Explorer 5.01 and 6.0 caller browsers. Occurs when an agent attempts to share a popup window that has the same name but a different location of an earlier popup window that was closed on the agent desktop but remains open on the caller side. The current popup window binds to the original window handle in the caller causing a JavaScript error.

The error is caused by a browser timing issue when the code executes to examine the existing window's content. The browser attempts to deliver and execute code in a partially loaded window with invalid content and fails with error codes in the browser's internal JavaScript server.

Workaround: Use unique window names in popup window open commands, OR have callers close popup windows in unison with agents, OR have agents leave popup windows open during a session, OR disable popup window sharing (see "Users receive a JavaScript Error when closing popup windows" CSCma19130).

Cisco Tracking Number: CSCma19572

AOL 6.0 callers on Windows 95 callers receive JavaScript errors when sharing popup windows with unspecified locations

Symptoms: Popup windows launched without an initial location specified in their window.open JavaScript call typically (90% of the time) result in errors. The error may manifest itself as a blank window and/or a JavaScript error message. Error messages can appear at any time: when the window opens, when it is in use, or as it is being closed. DCA page sharing functionality will continue to function correctly once the caller has acknowledged thee error messages.

Conditions: Occurs on AOL 6.0/Windows 95 platforms. This results from a timing issue in the AOL 6.0/Windows 95 platform that leaves the window blank and stops the execution of JavaScript calls in the newly opened window. This problem applies equally to shared content being applied as it does to the user actively clicking a link to open the window. Errors may occur at any stage (opening or closing the window) because of the timing problem.

Workaround: Always specify a location (URL) in window.open events OR avoid sharing popups with callers using AOL 6./Windows 95 OR share only specific popups which specify the desired URL in the window.open() calls OR disable popup window sharing in general. (See "Users receive a JavaScript Error when closing popup windows" CSCma19130 for more.)

Cisco Tracking Number: CSCma19666

Session-Related Issues

New DCA session created when both agent and caller(s) exit and log back in to CCS

Symptom: If both the agent and caller(s) in a CCS MeetMe session are forced to re-login to CCS (for example, due to concurrent browser crashes or if both closed their CCS Desktop browser windows) they are automatically entered into a new DCA session (with a new session ID), rather than the existing one. The last shared page is not automatically restored and any state information accumulated during the last session is lost.

Conditions: Only occurs when both agent AND caller(s) are forced to log back in to CCS.

Workaround: None

Cisco Tracking Number: CSCma19974

Incorrect PC clock setting can cause the DCA participant cookie to expire prematurely

Symptom: DCA participant cookies expire based on a configurable timeout. If a user's PC clock setting is too fast, or if the user's time zone setting is incorrect, the cookie may expire prematurely. In turn, this can result in a new DCA session being created each time the user makes a subsequent request to the DCA.

Workaround: You can adjust the cookie timeout period by editing the ParticipantTimeout property in the Proxy.properties file.

Cisco Tracking Number: None

Other Issues

Users' browsers are not mapped until they request content through the DCA

Symptom: Browser mapping may not reflect the browsers of all users in session.

Conditions: Until a user makes an initial request for content to the DCA, that user's browser is not considered by the DCA for the purposes of browser mapping. The initial request can include: clicking a link on a parsed page; receiving a page share from another user; entering a URL in the Collaboration Toolbar Address Bar. Note however that the first Web page automatically displayed to users at the start of the DCA session DOES NOT constitute a request to the DCA.

Workaround: Have users request content from the DCA to have them included in the browser map. Any pages that depend on browser mapping should be requested only after first making sure all session participants browsers have been mapped.

Cisco Tracking Number: CSCma16694

Without Browser Mapping, participants may receive inappropriate browser-specific content

Symptom: When collaborating on sites that deliver browser-dependant content based on a server-side determination of a requester's browser, some participants in a session may receive content inappropriate for their browser. For example, if an agent, using IE 5.5 requests content, IE 5.5-specific content may be returned, cached by the DCA, and then shared to callers whose browser type and/or version may be different than the agent's.

Conditions: Occurs when DCA Browser Mapping is not used and a Web site delivers browser-dependant content based on a server-side determination of a requester's browser. Note that if the browser determination is made on the client-side, the content participants receive will be appropriate for their browser, but may then vary from participant to participant.

Workaround: Use the DCA's Browser Mapping feature to ensure that all users receive similar browser-dependant content based on the lowest-common-denominator of browsers used in the session.

Cisco Tracking Number: CSCma20698

Broken HTTP server can result in caching of incorrect user credentials

Symptom: In some circumstances, when a user presents the wrong credentials to a site using Basic Authentication and the wrong credentials are entered, the user is not prompted upon subsequent requests for the correct credentials.

Conditions: This condition is caused by a broken HTTP 1.1 server. Some servers do not properly re-request authentication when a request is made with invalid credentials. This behavior can be observed with or without the use of the DCA, provided the HTTP client uses HTTP version 1.1.

Workaround: Start a new DCA session to avoid use of incorrect cached credentials. If possible, upgrade the server.

Cisco Tracking Number: CSCma14029

Cannot log in an agent and caller on the same PC using a single browser

Symptom: In a test environment, users may want to mimic a DCA session on a single PC by logging in an agent and caller in separate browser windows. Because the DCA participant cookie identifies a participant as either an agent or caller, and because it is assigned on a one-per-browser basis, you cannot use the same browser to log in an agent and caller concurrently from a single PC.

Workaround: Open the agent and caller in different separate browsers (e.g., IE for the agent, Netscape for the caller).

Cisco Tracking Number: None

Users prompted for username/password when sharing MS Office files

Symptom: When an agent attempts to share an MS Word document (.doc file) or any other MicroSoft Office file (e.g., PPT, XLS), the caller and/or the agent will receive a network security dialog box prompting for a username/password to access the DCA server's cache.

Conditions: Occurs if the user (caller or agent) is using IE, in SSL, and has installed Office 2000/XP. MSOffice installs a browser 'plugin' which will intercept any urls with the extensions of doc, etc (any file type which office will recognize as its own), and will attempt to open the document. In SSL, DCA utilizes a static cache system which redirects the browsers through the cache and to the document. Unfortunately, MS Office attempts to connect to the url we provide (that being the cache) and since it does not have a cookie identifier, a network security prompt appears. Cancelling this prompt or 'oking' the prompt twice will cancel the attempt to connect to the cache server. This will then allow the url response to complete, redirecting the browser to the content.

Workaround: Click cancel on the security prompt. This cancels the attempt to connect to the cache server and allows the redirect to follow through.

Cisco Tracking Number: CSCma20339

DCA unable to take additional session requests if insufficient disk space is available to the Copy Server

Symptom: If the disk on which the Copy Server (and its directories) is installed runs out of available space, the DCA is unable to take additional session requests.

Conditions: Extremely rare. Unlikely to happen unless the Copy Server is installed on a partition smaller than the DCA's specified minimum of 4 Gb.

Workaround: Only install the Copy Server on a partition that meets Cisco's minimum requirement for available disk space.

Cisco Tracking Number: CSCma01069

Copy Server unable to create directories when under an extremely heavy load

Symptom: When the DCA writes pages to the Copy Server, the Copy Server creates directories in which to store the pages. On occasion, when the DCA is under heavy load, the Copy Server has problems creating directories.

Conditions: Occurs rarely, and only when the number of concurrent sessions is 250 or greater.

Workaround: None. However, the adverse effect is minimal — a minor performance penalty resulting from the need to retrieve the web page from the web content server.

Cisco Tracking Number: CSCma01067

DCA with SSL does not allow users to be redirected to custom 404 error pages

Symptom: Some sites create their own customized 404 error pages that are returned when a user enters an invalid URL. When using DCA with SSL, users are presented a standard 404 error page rather than any customized page that may exist.

Conditions: Occurs when using the DCA with SSL.

Workaround: None.

Cisco Tracking Number: CSCma22215

Resolved Caveats

This section describes DCA 2.0 and 1.0 issues resolved or otherwise obsoleted in DCA 2.01.

DCA 2.0 Resolved Caveats

This section describes DCA 2.0 issues resolved or otherwise obsoleted in DCA 2.01.

Remote Control does not update its caller list when a caller exits a session

Description: Callers dropped from a Collaboration Server session (after hanging up or disconnecting) continue to appear in the Collaboration Toolbar Remote Control user list. Callers will continue to appear in the Remote Control user list until their DCA participant cookie has timed out (a user's DCA participant cookie can persist even after a caller drops out of the associated CCS session).

Resolution: In DCA 2.01, a participant that exits a CCS session is automatically removed from the DCA session as well. Remaining participants are notified that the user has left the session and the user is removed from the Collaboration Toolbar Remote Control user list.

Cisco Tracking Number: CSCma16673

DCA users do not receive notification when their DCA session has expired

Description: Regular content sharing is necessary to keep a DCA session active. If users in a DCA session do not share content for a specified period of time (either because they are using other CCS features such as WhiteBoard, or because they have simply been idle) their DCA session may time out, even though their CCS session remains active. In this event, users do not receive notice that their DCA session has terminated. DCA session expiration is determined by a configurable timeout period. The default DCA session timeout is 30 minutes.

Resolution: In DCA 2.01, DCA sessions remain active and do not terminate until their corresponding CCS session has ended. In the unlikely event that the DCA connection to CCS is broken, DCA sessions terminate based on the DCA's session timeout setting, at which time users receive a message alerting them that their session has terminated.

Cisco Tracking Number: CSCma18301

Page sharing commands do not work if the sending user's URL has not changed since the last share

Description: The DCA predicates page shares on a determination of whether a user's URL has changed since the last shared event. As a result, page sharing commands (Page Share, Follow Me, FormShare) may not trigger a share if a user attempts to share the same page consecutive times. In certain scenarios, this can prevent an agent from using page share to "synch up" with a caller when one or the other has navigated to a different page.

Resolution: DCA 2.01 resends pages whenever a page sharing command is used, regardless of whether or not the sender's URL has changed since the last page share.

Cisco Tracking Number: CSCma19707

DCA 1.0 Resolved Caveats

This section describes DCA 1.0 issues resolved or otherwise obsoleted in DCA 2.01.

Conflicts can occur if ProxyBasePath is set to /Admin, /, or a long string

Description: URL conflicts can occur if the ProxyBasePath parameter in the WLProxy.properties file is set to /Admin, /, or an extremely long string. The DCA default for this property is /DCA. Occurs when the ProxyBasePath parameter is set to one of the values described in the previous paragraph.

Resolution: Proxy base path is set automatically in DCA 2.01. It is not user-editable. Note also, in DCA 2.01 WLProxy.properties is renamed to Proxy.properties.

Cisco Tracking Number: CSCma00478

May need to adjust your Virtual Machine memory after installing the DCA

Description: At installation, the DCA sets your Virtual Machine memory to 256 Mb. If your DCA hardware configuration includes 256 Mb or less of physical memory, Cisco recommends that after installation you adjust your VM memory to a lower number than your physical memory.

Resolution: New minimum memory requirements render this issue obsolete.

Cisco Tracking Number: none

Online documentation on the DCA server cannot be accessed remotely

Description: The DCA online documentation installed on the DCA server cannot be accessed remotely (over the Internet). Local network access to the DCA server is required to access the installed documentation. Resolution: The DCA treats every remote request as a request for content from another server. The DCA has no facility for serving requests from the local machine.

Resolution: Resolved in DCA 2.01.

Cisco Tracking Number: CSCma00284

SSL does not work between the DCA for IIS and Web content servers using JWS 1.1.x

Description: Due to a problem with the JWS 1.1.x implementation of SSL, you cannot use SSL between a DCA server running IIS and a Web content server running JWS 1.1.x. Occurs between the DCA using NT 4.0 IIS 4.0 and a Web content server using JWS 1.1.x.

Resolution: These platforms are no longer supported in DCA 2.01.

Cisco Tracking Number: CSCan03161

When using the Snaplet, the DCA Admin Tool may not display the correct number of session participants

Description: When using the Snaplet, the session participant number displayed in the DCA Admin Tool may be higher than the actual number of session participants. Occurs if a session participant has multiple participant cookies accumulated from previous DCA sessions.

Resolution: Snaplet is no longer supported in DCA 2.01.

Cisco Tracking Number: CSCma00957

Upgrade Guidance

DCA 2.01 is not simply an update to DCA 1.0 -- it is a separate application based on a different architecture. DCA 2.01 uses different mechanisms for session creation, page sharing, and other core functionality.

Due to DCA 2.01's more advanced feature set, its hardware requirements and performance specifications are different than those for DCA 1.0. You cannot install DCA 2.01 over DCA 1.0. Consult the *DCA 2.01 Installation and Integration Guide* for more information on upgrading from DCA 1.0 to DCA 2.01.

Obtaining Technical Assistance

The following resources are available to DCA users:

Online Resources

Additional DCA information is available online at:

- Latest DCA user documentation: www.cisco.com
- Technical tips: www.cisco.com/warp/customer/640/
- Known issues and workarounds: www.cisco.com/cgi-bin/Support/Bugtool/home.pl (listed as: Cisco Collaboration Server Dynamic Content Adapter)

Note Note: Some resources on the Cisco Web site require you to have an account. Register for an account at: www.cisco.com/register/

Cisco Technical Assistance Center

You can get technical assistance with the DCA by contacting Cisco's Technical Assistance Center (TAC).

Contacting TAC

To open a request for technical assistance with the DCA, contact TAC at:

Online:	www.cisco.com/tac/
Email:	tac@cisco.com (please include "Dynamic Content Adapter" in the Subject line)
Telephone:	In North America: 1.800.553.2447 Outside North America: 1.408.526.7209

Providing Information to TAC

To assist you in troubleshooting a problem, the Cisco TAC may ask you to provide the following. You can expedite matters by having it available when you contact them:

1. Copies of your DCA Trace and Error log files. To ensure that your log files contain information on an error:
   a. Set the DCA log's logging level to Local Dump (its most verbose level).
   b. Restart the DCA.
   c. Repeat the actions that caused the error.
2. URLs of the page(s) on which the error occurred if they are external to your Web site.
3. Copies of your DCA parser XML files if you have customized the DCA parser.