Cisco Collaboration Server Dynamic Content Adapter

Version 2.01

Installation and Integration Guide

Instructions for installing the Dynamic Content Adapter (DCA) 2.01 on Windows and Solaris Platforms and integrating with the Cisco Collaboration Server (CCS) 5.0.

Copyright

Table Of Contents

About DCA Documentation

Welcome to the Installation and Integration Guide for the Cisco Collaboration Server Dynamic Content Adapter (DCA) for Windows/Solaris, version 2.01. This guide contains instructions for getting the DCA installed, integrated, and functioning smoothly. It includes:

- System requirements
- Installation instructions (all supported platforms)
- Licensing information
- Instructions for integrating the DCA with Collaboration Server

Audience

This guide is intended for individuals who install and configure the DCA and Collaboration Server. It assumes that the reader is generally familiar with what the DCA is and how it works, and has knowledge of:

- The platforms and operating systems on which the DCA runs
- Cisco Collaboration Server
- Basic Web collaboration

Other DCA 2.01 Documentation

The following documentation is available for the DCA 2.01.

Document	Primary Audience	Description
DCA Product Overview Guide	All DCA users	High-level product information. Includes: • How the DCA works • DCA features list • Supported platforms • SPLIT content collaboration issues • Deployment map Available formats: HTML and PDF
DCA Installation and Integration Guide	DCA installers, Collaboration Server configuration specialists, system integrators	Instructions for getting the DCA installed and running. Includes:

		• System requirements • Installation instructions (all supported platforms) • Licensing information • Instructions for integrating the DCA with Collaboration Server Available formats: PDF available at the top level of the CD. Ignore the Installation Guide available at any other location of your CD.
DCA Administration and Configuration Guide	System integrators, DCA and Collaboration Server administrators, Web architects	Instructions for post-installation DCA configuration, customization, and administration. Includes: • DCA administration information • DCA configuration and customization information • Collaboration Toolbar configuration Available formats: HTML and PDF
DCA Parser API Javadoc	DCA configuration specialists	Specification for the DCA parser API. Available formats: HTML and PDF
Collaboration Toolbar Online Help	Collaboration agents	Instructions for Collaboration agents on using the DCA Collaboration Toolbar to share Web content. Available formats: HTML
DCA Reference Card	All DCA users	Hard-copy reference card included with the DCA CD. Includes quick start information on how to access DCA documentation, the DCA Admin Tool, and Cisco support services. Available formats: Hard copy only
Release Notes	All DCA users	The DCA Release Notes contain up-to-date information on known issues and workarounds and any special instructions not covered in this guide. Available formats: PDF

To Access DCA Documentation

Before installation: You will find this document, the 'install.pdf' at the top level of the DCA CD, in the ‘Documentation -> Installation’ folder. This document helps you to install DCA and configure DCA with the Collaboration Server.

You can access all other DCA documentation from the DCA Getting Started Page. To access the Getting Started Page, get local access to the DCA server, and open this file (getstart.htm) from the DCA root directory.

Note: To access the getstart.htm, you need to first install DCA.

DCA Document Conventions

DCA documentation uses the following conventions:

Note	Indicates information of particular interest or significance.
Caution	Indicates the possibility of an adverse condition, such as poor or improper performance, data loss, or a security risk.
<>	Indicates a variable. For example: <DCAservername> represents the name of your DCA server. When prefaced by "Press," a bracketed term represents a keystroke. For example, "Press <Enter>" means to press the Enter key.

How to Deploy the DCA

At its highest level, moving towards a live deployment of the DCA involves the basic steps described below. Consult the DCA Administration and Configuration Guide for more detailed instructions on configuring the DCA.

Step 1	**Install Cisco Collaboration Server**
	If you are not a current CCS user, you must install CCS prior to implementing the DCA. Cisco recommends that, whenever possible, you use a fresh CCS installation with the DCA.
Step 2	**Install the DCA**
	The DCA should be installed on its own server. Installation tasks include: 1. Installing prerequisite software. 2. Running the DCA Installer. 3. Installing the license file. 4. Testing the installation. Based on how you choose to deploy the DCA, you may also need to: • Enable firewall ports for the DCA. • Configure the DCA for a proxy server.
Step 3	**Integrate the DCA with CCS**
	After installing the DCA, you must integrate with the Collaboration Server. Depending on your CCS version, integration tasks include: 1. Assessing and possibly backing-up CCS customization that may be overwritten by the DCA-CCS Updater. 2. Running the DCA-CCS Updater on the CCS server.

	3. Creating the CCS connection to DCA. 4. Testing the DCA-CCS integration.
Step 4	**Perform post-installation configuration**
	In most cases, you can use the DCA as-is immediately after installing and integrating it with CCS; post-installation configuration is usually not necessary. You may need to: • Configure the DCA for SSL: To share secure content, you must configure the DCA for SSL. • Change the Admin Tool password: Cisco recommends that you do this shortly after installation.
Step 5	**Test your site with the DCA**
	Thoroughly test your site with the DCA. Based on the results of the test, you may choose to: • Further customize the DCA. • Make changes to your site to address any identified collaboration issues. After deploying the DCA, Cisco recommends that you re-test your site with the DCA whenever you add new pages or make changes to existing pages.
Step 6	**Train your agents to collaborate using the DCA**
	Because the methods for sharing Web content through the Collaboration Toolbar are different than those for standalone Collaboration, agents should be trained in the proper use of the tool.

See Also

For related information, see:

About Installing the DCA

About DCA-CCS Integration

The DCA Product Overview Guide

The DCA Administration and Configuration Guide

Section I: DCA Platform Specifications

About DCA Supported Platforms

The Dynamic Content Adapter 2.01 supports the following platforms:

Server Platform

Server Type	Operating System	Web Server	Servlet Engine
Windows	Windows 2000 with service pack 3	Microsoft Internet Information Server (IIS) 5.0	Servlet Exec 4.1 ISAPI (included in DCA installer)
Sun Sparc System	Solaris 8 with the patch 108528-19 or greater	Sun ONE 6 with SP6 or greater	Sun ONE Web Server

Note: The 'iPlanet Web Server' has been renamed to 'Sun ONE Web Server'.

CCS Server Platforms

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

The DCA to CCS is a one-to-one relationship

Due to connection and load limitations, you must use a separate DCA server for each CCS instance. Similarly, each CCS supports only one DCA connection.

CCS 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 on 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 **Note**: Netscape 4.x versions are not supported on Windows 98 or Windows 2000.

Note: CCS does not support Mac browsers for agents or callers.

See Also

For related information, see:

About DCA Hardware Requirements

About DCA Software Requirements

About DCA Server Hardware Requirements

The recommended hardware configuration for your DCA 2.01 is as follows:

Windows Platform

Minimum

- Processor: Dual 866 MHz Pentium 3
- Memory: 1 Gb RAM (minimum)
- Available Disk Storage Space: 2 Gb

Enterprise

- Processor: Dual 2.4 GHz Pentium 4
- Memory: 1 Gb RAM (minimum)
- Available Disk Storage Space: 4 Gb

Solaris Platform

Minimum

- Processor: 2 x Ultra Sparc III
- Memory: 1 Gb RAM
- Available Hard Disk Storage Space: 36 Gb

Recommended

- Processor: 2 x Ultra Sparc III
- Memory: 2 Gb RAM (recommended)
- Available Hard Disk Storage Space: 36 Gb

Number of Sessions for both Windows and Solaris Platform

As a rough guideline, the DCA 2.01 minimum configuration should deliver adequate performance for 40 concurrent sessions. The Enterprise configuration should deliver adequate performance for 100 or more concurrent sessions. Results of Cisco load tests performed against the minimum configuration are described in the *DCA 2.01 Administration and Configuration Guide*.

Caution: Cisco requires that the DCA have its own dedicated server. You CANNOT install the DCA and Cisco Collaboration Server (CCS) on the same server.

See Also

For related information, see:

About DCA Supported Platforms

About DCA Software Requirements

The DCA 2.01 Administration and Configuration Guide

DCA Server Software Requirements

Prior to installing the DCA 2.01, the following prerequisite software must be installed and properly configured.

Windows Platform

Prerequisite:	Version:	Notes:
Microsoft Windows 2000 (with the latest service pack)		Your Windows 2000 server must have: • A TCP/IP connection • A valid DNS entry • Must be able to access your Web content servers via TCP/IP
Microsoft Internet Information Server (IIS)	5.0	Regarding your IIS installation: • Cisco recommends that you use IIS's default installation options. • If your DCA uses SSL (that is, if you use the DCA to share secure content), an appropriate server certificate must be installed and SSL configured, as desired. • If you choose, you can install the IIS Lockdown Tool on your Windows 2000/IIS server, but ONLY AFTER installing the DCA. If the Lockdown Tool is already installed on your server, you must uninstall it before installing the DCA. Failure to do this will prevent the DCA from installing properly. Read About the IIS Lockdown Tool for more information.
Microsoft Internet Explorer or Netscape Navigator	IE: 5.01 or greater	Used to access the DCA Admin Tool and DCA documentation.
	NS: 4.76 or greater	**Note:** Netscape 4.x versions are not supported by Windows 98 or Windows 2000.

Solaris Platform

Prerequisite:	Version:	Notes:
Solaris	8 with the patch 108528-19 or greater	Your Solaris server must have: 1. A TCP/IP connection 2. You must to have a valid DNS entry for this server so that the IP address can be associated with a domain name and must be able to access your Web content servers via TCP/IP.

		3. The DCA install script loads all the files into the user mentioned directory, it is mandatory that the this directory has more space (Approximately 3-4 Gb) 4. Make sure that the home directory has enough space to store the iPlanet (Sun ONE) log
JDK	1.3.1	The JDK 1.3.1 is available in the DCA CD. You must install JDK 1.3.1 before installing Sun ONE Web Server. **Note:** Sun ONE Web Server installation prompts for JDK path. Provide the path where the JDK is installed.
Sun ONE Web Server	6 with Service Pack 6 or greater	Regarding your Sun ONE Web Server: 1. Install the Sun ONE Web Server as a 'root' before you begin to install the DCA. Refer to the section "Sun ONE Web Server Configurations for DCA". 2. Ensure that your Sun ONE Web server's instance meant for installing the DCA has not undergone any customization. 3. If your DCA uses SSL (that is, if you will be using the DCA to share secured content), install an appropriate server certificate, and configure SSL accordingly.
Microsoft Internet Explorer or Netscape Navigator	IE: 5.01 or greater	Used to access the DCA Admin Tool and DCA documentation.

Sun ONE Web Server Configurations for DCA

Install the Sun ONE Web Server as a "**root**" before you begin with installing the Cisco Dynamic Content Adapter (DCA) 2.01.

Note: The Sun ONE Web Server configurations will be a little different depending on whether you are installing the DCA as a "root" or as a "non-root".

a) Configuring Sun ONE Web Server if you are installing the DCA as a "root"

1. Among the Sun ONE Web Server installation options, select 'Typical Installation'.

2. At the appropriate prompt where you need to select the Sun ONE Web Server components, type:
   1,3,4,5
   and press <Enter>

   Note: Exclude the Java Runtime Environment (JRE) option while installing the various Sun One Web Server components.

3. You might want to retain the defaults for the Sun ONE System user and System group. To retain the defaults, at the appropriate prompts, press <Enter>.

Note: The respective defaults are **user:** nobody and **group:** nobody.

4. When you receive the prompt for the JDK path, provide the directory path for the JDK 1.3.1.

b) Configuring Sun ONE Web Server if you are installing the DCA as a "non-root"

Note: Contact your System Administrator to create the "non-root" DCA user, and to specify the group to which that user belongs, before you begin with the Sun ONE Web Server installation.

1. Among the Sun ONE Web Server installation options, select 'Typical Installation'.

2. At the appropriate prompt where you need to select the Sun ONE Web Server components, type:
   `1,3,4,5`
   and press <Enter>

   Note: Exclude the Java Runtime Environment (JRE) option while installing the various Sun One Web Server components.

3. When the Sun ONE Web Server installation prompts for the System user and System group, provide the same username and user group of the DCA non-root user created earlier.

   For example, if the DCA non-root entities for username and user-group that your System Administrator created are *dcauser* and *dcagroup* respectively, enter the same names: *dcauser* and *dcagroup* as the System user and System group during the Sun ONE Web Server installation as well.

4. When you receive the prompt for the JDK path, provide the directory path for the JDK 1.3.1.

Note: After installing the Sun ONE Web Server for DCA, ensure that Sun ONE Web server instance directory meant for the DCA has necessary write-permissions.

DCA Access to Collaboration Server

For test environments only, your Collaboration Server must be accessible by the same name both inside and outside of your network. For example, if your Collaboration Server is accessed from the Internet as `http://myCCS.mydomain.com`, then within your local network the DCA must be able to access it using that same name.

This ensures that the DCA can access the default CCS Call Me page file on your Collaboration Server. (The Call Me page is served to both agents and callers at the start of a CCS Call Me session.) In an actual production environment, this page is served from a Web content server, thereby removing this requirement.

See Also

For related information, see:

About DCA Supported Platforms

About DCA Software Requirements

About the IIS Lockdown Tool

Section II: Installing DCA on Windows and Solaris Platforms

About Installing the DCA

To install the DCA, follow the sequence of steps listed below. Cisco recommends that you review this list thoroughly before proceeding with the installation.

1. Review the DCA hardware requirements

Confirm that the server on which you are installing the DCA meets the DCA hardware requirements.

2. Install and configure prerequisite software

Confirm that all DCA prerequisite software is installed and properly configured.

Caution: On Windows 2000 platforms, you may choose to run the IIS Lockdown Tool on your DCA/IIS server. Note that the Lockdown Tool should be run only AFTER you install the DCA. If the Lockdown Tool is already installed on your server, you must uninstall it before installing the DCA. Failure to do this will prevent the DCA from installing properly.

Before proceeding, first read About the IIS Lockdown Tool for important information on Lockdown Tool settings.

3. Review the DCA Release Notes

Review the DCA Release Notes for any updates pertaining to DCA installation. The Release Notes are available at the top level of the DCA CD (release_notes.htm).

4. Review Upgrade Information

If you are upgrading from DCA 1.0, perform a short series of steps to prepare for the upgrade. **Note:** DCA for Solaris does not have Upgrades.

5. Install the DCA

In addition to itself, the DCA installation also installs ServletExec, and the Java Development Kit (JDK) for Windows Installation. For Solaris Installation there is no ServletExec. The Java Development Kit (JDK) needs to be manually installed and then configured with Sun ONE.

6. **Install your DCA license file**

   The DCA uses a license file that must be placed in the appropriate directory after you have installed the DCA. Your license file is delivered on its own CD with your DCA package.

7. **Enable ports on your firewall**

   If you are deploying the DCA behind a firewall, you must enable the ports used by the DCA.

8. **Configure the DCA for a proxy server**

   If your DCA server communicates with the Internet through a Web proxy, you must configure the DCA for a proxy server. Using a Web proxy with the DCA is not recommended for production environments, but is sometimes used in lab configurations.

9. **Test the installation**

   After installing the DCA, perform a few simple tests to verify that the installation was successful. Consult the section DCA Installation Troubleshooting to resolve installation issues.

10. **Integrate the DCA with your Collaboration Server**

    After installing the DCA, you must run the DCA-CCS Updater file on your Collaboration Server.

Post-Installation Configuration

In many cases, you can use the DCA as-is immediately after installing and integrating it with CCS; post-installation configuration is usually not necessary.

However, many users may choose to do the following shortly after installing the DCA:

- Configure the DCA for SSL: To share secure content, you must configure the DCA for SSL. Instructions for configuring the DCA for SSL are described in the *DCA Administration and Configuration Guide.*

- Change the Admin Tool password: Cisco recommends that you do this shortly after installation. Instructions for changing the Admin Tool password are described in the *DCA Administration and Configuration Guide.*

See Also

For related information, see:

How to Deploy the DCA

About DCA Hardware Requirements

About DCA Software Requirements

About Upgrading from DCA 1.0

How to Install the DCA on Windows 2000

How to Install Your DCA License

How to Deploy the DCA Behind a Firewall

How to Configure the DCA for a Proxy Server

How to Test the DCA Installation

About DCA-CCS Integration

About the IIS Lockdown

The DCA Administration and Configuration Guide

Installing the DCA for Windows

About Upgrading from DCA 1.0

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*.

If you are a DCA 1.0 user upgrading DCA 2.01, perform these steps prior to installing DCA 2.01:

1. **Inventory DCA 1.0 settings and customization**

   There is no automated way to port settings and customization from your DCA 1.0 server to DCA 2.01. Therefore, you should take an inventory of settings and customization you introduced to DCA 1.0, and decide which, if any, you will want to re-create on your DCA 2.01 server. Under no circumstances should DCA 2.01 properties files simply be overwritten with files from 1.0.

   Note that the following DCA 1.0 customization features have been deprecated in DCA 2.01. In 2.01, the behaviors available through these features can be achieved through parser customization.

   - Agent link deadening (used to disable specific link types, for example, SUBMIT buttons, for agents in a DCA session)
   - 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)
   - User patterns (used to define link parsing rules)

2. **Uninstall DCA 1.0**

   DCA 2.01 cannot be installed over DCA 1.0. If you plan to install DCA 2.01 on a machine on which DCA 1.0 was previously installed, you must first uninstall DCA 1.0. To ensure that DCA 1.0 uninstalls cleanly, be careful to follow the uninstall instructions included in your DCA 1.0 documentation.

   You should also delete the DCA 1.0 alias for the DCA Admin Tool defined in your Web Server software.

3. **Remove DCA 1.0 URL formatting from CCS scripts**

   For DCA 1.0, your company may have modified URLs in the Collaboration Server Agent Desktop Script area to point to the DCA. Because the DCA 2.01 uses a different, automatically imposed, URL format, DCA modifications made to URLs in the CCS Script area must be removed. (URLs modified for DCA 1.0 used this format: `http://<DCAservername>/DCA?url=http://<URL>&WLSession=<sessionID>`.)

4. **Remove DCA 1.0 code from the CCS Screen Pop configuration**

   For DCA 1.0, your company may have added code to the Collaboration Server Screen Pop file (`screenpop.jhtml`) that served to create DCA sessions at the start of a CCS session. This code is not needed for DCA 2.01 and should be removed if it exists.

See Also

For related information, see:

About Installing the DCA

About DCA Hardware Requirements

The DCA 2.01 Administration and Configuration Guide

The DCA 1.0 Installation and Configuration Guide

How to Install the DCA on Windows 2000

Once you have properly installed and configured the DCA prerequisite software, you can install the DCA. The DCA 2.01 CD for Windows 2000 includes an Install Wizard that installs the:

- DCA 2.01
- JDK 1.3.1
- ServletExec 4.1 ISAPI

Note: The JDK and ServletExec install transparently with the DCA. This means that:

- Their installation is not visible during the DCA installation.
- Windows program groups or desktop shortcuts are not created.
- They will not appear on the Windows Add/Remove Programs list

To Install the DCA

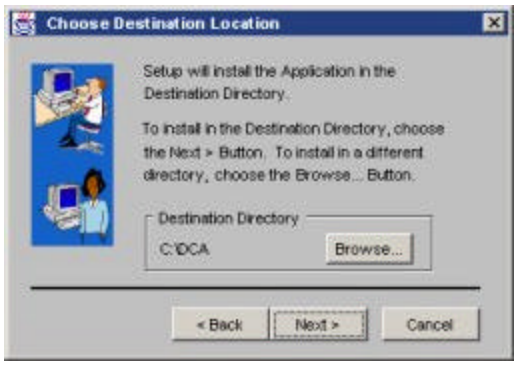
The installation instructions below only describe installer dialogs that require user input. To begin the DCA installation:

1. Stop your server's IIS Admin and WWW Publishing services. The DCA install CANNOT run while these services are running.
2. Insert the DCA 2.01 CD in your server's CD-ROM drive.
3. From the Windows Start Menu, select Run.
4. Browse to and double-click the DCA executable file located at the top level of the DCA CD. This file is named:
   - DCA-2.0-Win-128-K9.exe (US version)
   - DCA-2.0-Win-56-K8.exe (international version)

5. Click OK. The DCA Install Wizard opens.

6. In the **Choose Destination Location** window, select a location to install the DCA, or accept the default: `<defaultdrive>:\DCA`.

   You can install the DCA to any directory provided it is on a local drive.



7. If the installer detects a previously installed version of ServletExec, it will ask if you want to overwrite it. Select Yes.

8. When the installation is complete, click Finish.

9. Restart IIS.

See Also

For related information, see:

About Installing the DCA

How to Install Your DCA License

How to Deploy the DCA Behind a Firewall

How to Test the DCA Installation

Installing the DCA on Solaris

How to Install the DCA on Solaris

Once you have properly installed and configured the DCA prerequisite software, you can install the DCA. The DCA CD for Solaris includes the:

1. DCA folder that contains a tar file with an install script file.

2. Documentation folder contains a PDF file to help you install DCA and configure with the Collaboration Server

3. JDK 1.3.1 folder that needs to be installed before installing the Sun ONE web server.

Note: The JDK must be installed separately in the DCA Machine.

To Install the DCA

To begin the DCA installation, follow these steps:

1. Stop the Sun ONE (iPlanet) Server Instance

2. Install the DCA Server

Stop the Sun ONE (iPlanet) Server Instance

You must stop the Sun ONE (iPlanet) server instance on which you are going to install DCA. Follow the steps below to stop an Sun ONE (iPlanet) server instance.

a) Using a web browser, navigate to http://<DCA SERVER>:8888, assuming that the Sun ONE Admin server is installed on port 8888.

b) Login to the Sun ONE Administration web page using your administration username and password.

c) Select the Sun ONE (iPlanet) server instance on which you are going to install DCA and in the "Select a Server" pull-down menu, then click "Manage"

d) Click the "Server Off" button.

Installing the DCA

You can install the DCA either as a “root” and or as a “non-root” user. Depending on whether you are installing the DCA as a root or as a non-root, you will have to install the Sun ONE Web Server accordingly. For details about the differences in the Sun ONE Web Server installations, refer to the section “Sun ONE Web Server Configurations for DCA”.

The DCA installation script reconfigures an existing Sun ONE (iPlanet) Web Server instance to successfully run the DCA.

Note:

a) Before installing the DCA ensure that you have write-permissions to the Sun ONE Web Server instance directory for which the DCA is configured.

b) Do not install any other product on the server instance that contains your DCA server.

Steps for Installing DCA:

1.	Insert the DCA 2.01 CD into the DCA Machine's CD drive.
2.	The install script is located in the directory: DCA
3.	Run the DCA install script from this directory using ./install
4.	The install script prompts for confirmation about whether or not you want to continue with the installation. Type ‘Yes’ to continue.
5.	The DCA installation prompts for the Sun ONE server instance directory to which DCA needs to be configured. Type the appropriate path and press <Enter> **Note:** If you are installing the DCA as a non-root, ensure that the non-root user has write permissions to access the Sun ONE Web Server instance for the DCA.

6.	The install script prompts for the path where you want to install the DCA. To install in the default location press <Enter> and the files get installed under the directory '/<users_home>/Cisco_DCA'. If you want to install the DCA in another location, create the directory prior to installing the DCA or provide any existing directory in the system for which the user has write permissions.
7.	The install script continues to extract and install the DCA in the selected directory.
8.	After installation, ensure that the user and group ownership of the DCA directories 'DCA' and the 'DCA-webroot' are same as that of the Sun ONE server instance directory that is configured for this DCA. **Note:** The 'root' user has the privilege to change user ownership and the group ownership. If Sun ONE Web Server and the DCA are installed as the 'root' user then the Sun ONE Web Server's System user and System group must be defaults (nobody:nobody). Also change the ownership of the 'DCA' and the 'DCA-webroot' directories to nobody:nobody. That is: *chown –R nobody:nobody DCA DCA-webroot* If the DCA is installed by the 'non-root' for the Sun ONE web server instance that has the System user and System Group as user as dcauser:dcagroup, ensure that the ownership of the 'DCA' and the 'DCA-webroot' directories are dcauser:dcagroup. That is: *chown –R dcauser:dcagroup DCA DCA-webroot*
9.	Start the server. That is, in the command prompt, go to the Sun ONE Web Server instance and type: ./start When the DCA server instance starts, you must be able to see the message in the command prompt, 'http://<DCAservername>, Port Number ready to accept requests'. If you are not able to see this message restart the server. **Note:** The DCA *non-root* user must start the web server by logging in as a *root*.

How to Install Your DCA License

Your DCA 2.01 license is a separate file that you place in the appropriate directory after installing the DCA. You will find it on the *DCA License File* CD delivered with your DCA package.

Each DCA license is valid for a single DCA server and allows an unlimited number of seats. If you have additional questions regarding you DCA license, contact your Cisco Professional Services representative.

To Install Your DCA License

To install your DCA license for Windows, copy the file (`license.lic`) from your *DCA License File* CD to this location on your DCA server: `DCA\webapp\WEB-INF\Cisco\license` directory.

For Solaris, copy the file (`license.lic`) from your *DCA License File* CD to this location on your DCA server: `DCA/webapp/WEB-INF/Cisco/license` directory.

It is necessary to restart the server after installing the license.

Caution: Never attempt to modify the contents of your DCA license file. Altering the file will render it unreadable by the DCA.

See Also

For related information, see:

About Installing the DCA

How to Install the DCA on Windows 2000

How to Test the DCA Installation

DCA Installation Troubleshooting

About DCA Directory Structures

How to Test the DCA Installation

After installing the DCA, you should test your installation by:

- Making sure that you can access the DCA Admin Tool.
- Requesting several non-secure and secure (if your server is configured for SSL) pages through the DCA Collaboration Toolbar.

These brief tests are only to offer quick confirmation that the DCA installation was successful. You should perform more extensive testing after you have integrated the DCA with Collaboration Server, including testing pages from your own Web site.

To Access the Admin Tool

To access the DCA Admin Tool:

1. Open a Web browser and in the Address line, enter: `http://<DCAservername>/uiroot` (case-sensitive). Or, if your DCA server is set up to use SSL, you can enter https as the protocol.
2. Press <Enter>. The Admin Tool Login screen opens. **Note:** In Solaris Installation, if the page is not loaded properly refer to 'DCA Installation Troubleshooting'
3. Enter your DCA Admin username and password. The default values for these are Admin and Admin (case-sensitive) respectively.
4. Depending on your localization configuration, you may also have the option of choosing a different on-screen language to use for the current session.
5. Click Login.

To Request Pages Through the DCA Collaboration Toolbar (Quick Method)

Loading and requesting pages through the DCA Collaboration Toolbar can be performed from the DCA server or from any networked PC. It does not require the use of CCS.

Note: This method loads the Collaboration Toolbar in standalone mode (independent

of CCS). It is intended for internal testing purposes only. It is not supported for, and should not be used to conduct, actual collaboration sessions.

To load and request pages through the DCA Collaboration Toolbar:

1. Open a Web browser.
2. In the address bar enter:
   - `http://<dcaservername>/uiroot` (to test non-secure pages), or...
   - `https://<dcaservername>/uiroot` (to test secure pages. Requires the DCA to be first configured for SSL -- see the *DCA Administration and Configuration Guide*).
3. Press <Enter>. The Available Entry Points page opens.
4. Click the DCA Caller link. A login screen opens.
5. Enter any value for Name, Session, and Starting URL (the first page to be displayed when the Toolbar opens). Or you can leave any or all of these fields blank.
6. Click Log In. The DCA Collaboration Toolbar opens.
7. In the Toolbar, access pages by entering URLs in the Toolbar's address bar, or by clicking page links.

See Also

For related information, see:

About Installing the DCA

DCA Installation Troubleshooting

The DCA Administration and Configuration Guide

How to Deploy the DCA Behind a Firewall

If you are deploying the DCA behind a firewall to ensure security, you must enable access to the ports used by the DCA. By default, the DCA uses the following ports:

- HTTP Port: 80/TCP (default)
- HTTPS Port: 443/TCP (default)

In a typical deployment, your DCA and Collaboration servers are located within the same DMZ. However, if a firewall stands between the DCA and CCS, you must also enable the following ports on that firewall for the DCA-CCS connection:

- RMI Registry Port: 1099/TCP

  The port the DCA uses to register a connection instance with CCS.

- RMI Connection Port: TCP (no default, defined when you create the DCA-CCS connection)

  The port CCS uses to connect to and communicate with the DCA.

No other configuration is necessary to use the DCA behind a firewall.

See Also

For related information, see:

About Installing the DCA

How to Create the DCA-Collaboration Server Connection

DCA Installation Troubleshooting

How to Configure the DCA for a Proxy Server

If your DCA uses a Web proxy server for outbound connections, you must configure the DCA as described below. This configuration is only necessary for true Web proxies (e.g., WinProxy) located between the DCA and the Internet; firewalls (e.g., PIX) and network address translators (NATs) do not require this configuration.

Note: Cisco recommends that you DO NOT use a Web proxy server with the DCA in production environments. Using the Web proxy server with the DCA in production environments is not necessary and it might degrade the performance. In test environments, however, the use of proxy servers is fairly common.

To Configure the DCA for a Proxy Server

To configure the DCA to use a proxy server:

1. After installing the DCA, in a text editor, open the `Proxy.properties` file located at: `DCA\webapp\WEB-INF\Cisco\properties` for windows and `DCA/webapp/WEB-INF/Cisco/properties` for Solaris.

2. Uncomment and specify values for the following properties:

   HttpProxyServer: The proxy server's fully qualified DNS (e.g., `myproxy.mydomain.com`) or IP address.

   HttpProxyPort: The HTTP port the proxy server uses to receive internal requests.

   HttpsProxyServer: If the DCA uses a proxy server for SSL connections, it is the fully qualified DNS or IP address that you specify.

   HttpsProxyServerPort: The HTTPS port the proxy server uses to receive internal requests.

3. Save the file and restart the DCA.

Note: By default, the properties listed above are commented out in the `Proxy.properties` file. Because of this, they are not visible when the file is displayed in the DCA Admin Tool, thus creating the need to edit the file in a text editor.

See Also

For related information, see:

About Installing the DCA

DCA Installation Troubleshooting

DCA Installation Troubleshooting

The following table lists suggestions for troubleshooting problems encountered immediately after DCA installation. These suggestions assume that:

- The Sun ONE Web Server should be configured and the prerequisites should be met as mentioned in the section 'Sun ONE Web Server Configurations for DCA'.
- Your DCA server meets the requirements for DCA hardware and prerequisite software.
- Web content you are attempting to access is valid and available from a properly configured and functioning Web server.

Symptom	Possible Cause	Possible Solution
Unable to access both the DCA Collaboration Toolbar and the DCA Admin Tool -AND- Browser displays a 404 ("Page Not Found") error.	DCA Web server is stopped.	Restart Web server on DCA.
Unable to access any or certain Web pages through the DCA Collaboration Toolbar -AND- Browser displays DCA default error message.	Connection to Internet or to a particular Web content server is down -OR- Incorrect URL entered.	Re-establish connection -OR- Re-enter URL.

Symptom	Possible Cause	Possible Solution
Unable to access any Web pages through the DCA Collaboration Toolbar -- browser displays a 404 ("Page Not Found") error -OR- DCA Admin Tool pages display as raw text -OR- ServletExec Admin and DCA Admin pages load but input is lost on server restart.	DCA installed over IIS Lockdown Tool installation that used improper settings -OR- Improper IIS permission settings -OR- URLScan running on server (URLScan is a Microsoft filter that screens "suspiciously formatted" URLs.	To remedy Lockdown Tool installation issues: Uninstall and reinstall IIS Lockdown Tool as described in About the IIS Lockdown Tool. -OR- To remedy improper permission settings: Ensure that IIS uses the following permission settings: • File Permissions for Anonymous Users: Allow Write permissions to content directories. • Virtual Directories: Allow Execute permissions to the Scripts directory and its subdirectories. After changing settings, a server reboot followed by a reinstall of the DCA may be required. -OR- To remedy URL Scan issues: 1. Determine if URL Scan is running by checking for the presence of the UrlScan.log file at: <Windowsrootdirectory>\system32\intetsrv\urlscan. 2. Use Add/Remove Programs to remove URLScan (listed as IIS UrlScan). **Note**: If URLScan was installed during as part of Lockdown Tool installation, uninstalling the LockDown Tool will also remove URLScan .
Unable to access any Web pages through the DCA Collaboration Toolbar -- Toolbar "hangs" when attempting to a load page -AND- DCA server communicates with the Internet through a Web proxy server.	DCA not configured to use a proxy.	Configure the DCA to use a proxy as described in 'How to Configure the DCA for a Proxy Server'.
Unable to access secure (HTTPS) Web pages through the DCA Collaboration Toolbar -AND- Browser displays the DCA default error message.	DCA Collaboration Toolbar not configured for SSL -OR- DCA server not configured for SSL (i.e., valid server certificate not installed).	Configure the Collaboration Toolbar for SSL as described in the *DCA 2.01 Administration and Configuration Guide* -OR- Configure the DCA server for SSL.

Symptom	Possible Cause	Possible Solution
Unable to access any Web pages through the DCA Collaboration Toolbar -AND- Browser displays a "Missing or Corrupt License File" or "Server License has Expired" message.	DCA license file not installed.	Install license file as described in 'How to Install Your DCA License'.
DCA Collaboration Toolbar displays message "ServletExec Max Concurrent Requests Exceeded."	DCA was installed directly over a previous DCA installation.	Properly uninstall and reinstall the DCA as described in 'How to Reinstall the DCA'.
DCA Admin Tool *Select and View Logs* screen displays a null pointer exception.	DCA was installed directly over a previous DCA installation.	Properly uninstall and reinstall the DCA as described in 'How to Reinstall the DCA'.
Admin Tool window does not display the graphics in this page.	Sun ONE Document Root path is not set	Login to the Sun ONE Admin console, http://<DCAservername>:8888/ In the 'Manage Servers', select the DCA server instance and click on 'Manage'. Click on 'Virtual Server Class' and in this page under 'Tree View of the Server' click the DCA instance page. Click on 'settings' and in this page set the 'Document Root' to /DCA-webroot and click on 'Reset'.
Unable to access any SSL (https) Web pages through the DCA Collaboration Toolbar -- browser displays a 404 ("Page Not Found") error	DCA not configured with Sun ONE or Required DCA library files may be missing in location: /DCA/lib	The library files ccisCommonNative.jar, libcrypto.so, libuuid.so, libciscoguid.so, libciscoguid.so.1.0.0, libssl.so, and libSSLWrappers128.so or libSSLWrappers40 may be missing and need to be copied to the location: /DCA/lib The DCA library path must be appended to the 'LD_LIBRARY_PATH' in the 'start' script of the Sun ONE (iPlanet) that is located at /usr/iplanet/servers/https-<dcahost>
Unable to execute the DCA installation script while installing the DCA on Solaris Platform.	The install script file may not have the execute permissions for this user.	Change the permissions of the install script to give execute permissions for the file.

Symptom	Possible Cause	Possible Solution
While installing the DCA for Solaris Platform, after providing the DCA installation path, unable to install DCA.	The directory where you have specified that you want to install the DCA might not have *modify* permissions. or The directory where the DCA installation files are copied may not have *write* permissions.	Provide the directory where you can modify the permissions. or Provide the write permissions for the directory where the DCA installation files are copied.

Other Troubleshooting Information

Troubleshooting information related to DCA-CCS integration problems can be found at About DCA-CCS Integration Troubleshooting. Troubleshooting information related to page parsing problems can be found in the *DCA 2.01 Administration and Configuration Guide*.

See Also

For related information, see:

How to Test the DCA Installation

About DCA Hardware Requirements

About DCA Software Requirements

How to Install Your DCA License

How to Deploy the DCA Behind a Firewall

About the IIS Lockdown Tool

How to Configure the DCA for a Proxy Server

How to Reinstall the DCA

DCA-CCS Integration Troubleshooting

The DCA Administration and Configuration Guide

Section III: Integrating the DCA with CCS

About DCA-Collaboration Server Integration

After installing the DCA, you must integrate it with your Collaboration Server. Integration modifies CCS to include DCA features and turns off some unneeded CCS controls.

Required Integration Tasks

Integrating the DCA with Collaboration Server consists of these steps:

1. **Assess Pre-Existing CCS Customization**

   Prior to integrating the DCA with CCS, determine what, if any, pre-existing CCS customization will be affected when you run the DCA-CCS Updater. Note that whenever possible Cisco recommends you use a fresh CCS installation with the DCA.

2. **Install the DCA Updater on your Collaboration Server**

   The DCA-CCS Updater is a patch to CCS that allows it to function with the DCA.

3. **Test the Updater Installation**

   Verify that the Updater installed properly by checking for the presence of several settings in the `wlserver.properties` file.

4. **Create the DCA-Collaboration Server Connection**

   The DCA-CCS connection establishes an Agent Reporting and Management (ARM) service that makes DCA session information available to Collaboration Server reports. The service also allows the automatic cleanup of DCA sessions when their associated Collaboration sessions are terminated.

5. Add DCA Code to Localized CCS Files

During integration, the DCA modifies or overwrites a number of files on CCS, adding code that the DCA needs to function. However, the DCA-CCS updater only modifies the English versions of these files; IF you localize CCS to use non-English versions of these files (either before or after integration), you must manually add some code to these localized file versions. Failure to do this will prevent the DCA from functioning.

Optional Integration Tasks

After completing the required integration tasks listed above, you may want to perform the following optional tasks as well.

1. Hide Native Controls in the Caller Browser Window

In a DCA session, callers must navigate your Web site using the navigation controls on the DCA Collaboration Toolbar (the Collaboration Toolbar loads automatically in the caller's browser window at the start of a DCA session).

To prevent confusion, it's a good idea to remove all native navigation controls (i.e., menus and toolbars) from the browser window callers will use to share content. A common way to do this is to open the window through a JavaScript link on your Web site that excludes menus and toolbars.

2. Reintroduce Customization

During integration, the DCA modifies or overwrites a number of files on CCS. If you have customized your CCS (for example, by adding your own code to any of these files) you may need to reintroduce this customization after integration.

3. Re-enable App Sharing and/or White Board

DCA-CCS integration automatically disables Collaboration Server's Single-Session Agent App Share and White Board features. It does this by setting the CCS Caller Complexity Mode to Simple, and by hiding the controls in the Agent and Caller desktops used by these features. If you plan to use these features, you must re-enable them after integrating the DCA with CCS.

See Also

For related information, see:

How to Deploy the DCA

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

About DCA 2.01 Changes to Agent Role Settings

How to Install the DCA-CCS Updater

How to Test the Updater Installation

How to Create the DCA-Collaboration Server Connection

How to Add DCA Code to Localized CCS Files

How to Re-Enable White Board and App Share

DCA-CCS Integration Troubleshooting

How to Uninstall the DCA-CCS Updater

DCA-CCS Integration on Windows

About the DCA-CCS Updater

The first step in integrating the DCA with Collaboration Server is to install the DCA-CCS Updater file on your Collaboration Server. The DCA-CCS Updater is a patch to CCS that allows it to function with the DCA. The Updater:

- Configures CCS to automatically load the Collaboration Toolbar for agents and callers.
- Hides or disables controls in the CCS Agent and Caller Desktops that conflict with the DCA.
- Sets caller complexity mode to Simple (to eliminate security warnings).
- Modifies the CCS ScriptBuilder so that it automatically routes content requests to the DCA.

The DCA-CCS Updater must be run on each Collaboration Server you plan to use with the DCA.

Preserving Pre-existing CCS Customization

The DCA-CCS Updater works by modifying and replacing a number of configuration files on your Collaboration Server (it also adds several new files). If you are not using a fresh install of CCS with the DCA, it is possible that these files these files contain customization that will be lost when you run the Updater. Therefore, before running the Updater, Cisco recommends that you:

A. Review DCA 2.01 Changes to CCS Files. It lists the CCS files affected by the Updater and describes the nature of the changes.

B. Determine whether you have customized CCS by modifying these files. Assess the extent and nature of this customization, and whether you want this customization to continue after CCS is integrated with the DCA.

C. As necessary, make copies of the affected files prior to running the Updater.

D. After running the Updater, reintroduce any desired customization that was lost. DO NOT do this by overwriting the Updater-modified files with the originals. Rather, re-enter or copy and paste code, settings, etc. in the files as necessary. When you do this, be careful not to change any settings or code required by the

DCA (DCA-required settings/code are commented as such in files the DCA overwrites but not in those it modifies).

Updated File Backups

The DCA-CCS Updater automatically creates backups of CCS files it modifies or replaces. These backups represent the files, as they existed BEFORE the Updater was run. For files that the Updater:

- Modifies, it creates a copy of the original with the extension .bak. (for example, `myfile.properties.bak`). These are stored in the same directory as the original file.
- Replaces, it creates a copy of the original and stores it in a zip file named `DCA_2.01_CCS4x_Updater-JHTML.zip`). The zip file is placed in `<CCSrootdirectory>\Uninst`.

Caution: These automatic backup files are what the DCA uses to restore your original CCS configuration if you ever choose to uninstall the Updater. Therefore, do not modify, rename, or change the location of these files.

Uninstalling the DCA-CCS Updater

If necessary, you can uninstall the DCA-CCS Updater from your Collaboration Server. Uninstalling the Updater reverses any changes it made to your original Collaboration Server configuration, PROVIDED that the affected files were not modified subsequent to installing the Updater.

Note: Affected files that HAVE been modified subsequent to installing the Updater can be restored manually from their backups.

How to Install the DCA-CCS Updater

The DCA-CCS Updater is a patch to CCS that allows it to function with the DCA. It must be installed on every Collaboration Server you plan to use with the DCA.

Caution: Before installing the Updater, be sure to review the checklist of items in About DCA-CCS Integration.

To Install the DCA-CCS Updater

To install the DCA-CCS Updater on your Collaboration Server:

1. Stop your Collaboration Server's Web server software.

2. Insert the DCA 2.01 CD in your Collaboration Server's CD drive (or you can copy the Updater file from its location on your DCA server (<DCArootdirectory>\Updaters).

3. Start the Updater file, DCA-2.0-CCS5.exe. It is located at: <dcaCDroot>\updater.

4. The Patch Destination Directory should point to the Collaboration Server root directory. Change this path only if you are certain that the CCS root directory is located elsewhere.

5. For the DCA server's hostname, specify your DCA Server's fully-qualified DNS (for example, mydcaserver.mydomain.com).

6. Click Install.

7. When the Updater has finished running, restart the Web server software on your Collaboration Server.

How to Test the Updater Installation

After running the DCA-CCS Updater, you can verify that it installed properly by checking for the presence of several settings in the CCS wlServer.properties. file.

To Test the DCA-CCS Updater Installation

To test the Updater installation:

1. Open wlServer.properties in a text editor. wlServer.properties is located at: <CCSrootdirectory>\servlet\properties.

2. Verify that these entries exist in the file and that their values are correct:

   ```
   wlServer.dca.DCAHOSTNAME = <DCAservername>

   wlServer.dca.DCAPROTOCOL = http
   ```

Note: The DCA server name should be your DCA server's fully-qualified DNS as specified when you ran the Updater (for example, mydcaserver.mydomain.com).

The DCAProtocol setting determines the DCA Collaboration Toolbar's ability to share secure (SSL) Web content. The default value is http. To share secure content, set the value to https and then restart your Collaboration server's Web server software.

See Also

For related information, see:

How to Deploy the DCA

About DCA-CCS Integration

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

About DCA 2.01 Changes to Agent Role Settings

How to Install the DCA-CCS Updater

How to Test the Updater Installation

How to Uninstall the DCA-CCS Updater

DCA-CCS Integration Troubleshooting

The DCA Administration and Configuration Guide

DCA-CCS Integration on Solaris

How to run the DCA-CCS Updater

The DCA-CCS Updater script is patch to CCS that allows it to function with the DCA. This script is run on the Collaboration Server that you plan to use with the DCA.

Caution: Before running the Updater Script, be sure to review the checklist of items in About DCA-CCS Integration.

Note: Cisco recommends that the DCA-CCS Updater is used for a new CCS installation on Soalris. Otherwise it is recommended that all the files in this directory: Cisco_CS/servlet/properties get backed up and then run the Updater.

To run the DCA-CCS Updater

To run the DCA-CCS Updater script on your Collaboration Server:

1. Stop your Collaboration Server's Web server software.
2. Insert the DCA 2.01 CD in your Collaboration Server's CD drive and in the updater folder (CCS_DCA_Updater) find the ccs_dcs_install script.
3. Run the Updater script. That is, at the location where the script is available, run: ./ccs_dca_install
4. The Patch Destination Directory should point to the Collaboration Server root directory. For example, /Cisco_CS.
5. For the DCA server's hostname, specify your DCA Server's fully-qualified DNS (for example, `mydcaserver.mydomain.com`).
6. Once the script executes, restart the Web server software on your Collaboration Server.

See Also

For related information, see:

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

How to Test the Updater Installation

How to Uninstall the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

The DCA-CCS Updater adds, modifies, or overwrites the Collaboration Server configuration files listed below. If you have modified one or more of these files previously, you should assess the extent and nature of this modification to determine whether any desired settings or customization will be lost when you run the Updater. Of course, this is not an issue when deploying the DCA with a new CCS installation.

The DCA-CCS Updater automatically creates backups of CCS files it modifies or replaces. After running the Updater, you can reintroduce any desired customization that was lost. DO NOT reintroduce customization by overwriting the Updater-modified files with the originals. Rather, re-enter or copy and paste code, settings, etc. in the files as necessary. When you do this, be careful not to change any settings or code required by the DCA (DCA-required settings/code are commented as such in files the DCA overwrites but not in those it modifies).

Note: In the 'Location' column the directory path '\' refer to the windows path. For Solaris, the path is "/".

Files Added to CCS

The DCA-CCS Updater adds these new files on your CCS Server:

File	Location	Description
DCARolesOverride.properties	<CCSrootdirectory>\servlet\properties	Sets multi-session and single-session agent role properties required by the DCA. Primarily, this consists of Disables items in the agent desktop that conflict with the DCA.
startdca.jhtml	<CCSrootdirectory>\pub\html\caller	For multi-session configurations, loads the Collaboration Toolbar for callers and agents.
AgentWrapper.jhtml	<CCSrootdirectory>\pub\html\agent	Provides a wrapper for the agent desktop that allows it to forward JavaScript function calls (for example, from ScriptBuilder) to the DCA.

Overwritten CCS Files

The DCA-CCS Updater completely overwrites these files on your CCS Server (sorted by directory):

File	Location	Description of Change
AgentFrame.jhtml	<CCSrootdirectory>\pub\html\agent	Adds a hidden frame to the agent desktop frameset which stores AgentWrapper.jhtml.
screenpopbody.jhtml	<CCSrootdirectory>\pub\html\agent\default	Creates the Reload Toolbar button on the Agent Desktop.
RequestinProcess.jhtml	<CCSrootdirectory>\pub\html\caller\default	Resolves a timing issue related to the loading the Collaboration Toolbar for callers.
CallForm.html CallMe.html MscCallForm.html msccallme.jhtml	<CCSrootdirectory>\pub\html\forms	InitSessionPage in caller forms is commented out, thus allowing the DCA CCS Collaboration Toolbar to load in its place.
AgentPanel.jhtml	<CCSrootdirectory>\pub\html\multichatui	Adds a JavaScript function required by the DCA for page sharing.
callerinfo.jhtml	<CCSrootdirectory>\pub\html\multichatui	For multi-session configurations, allows the DCA to keep track of sessions as agents switch back and forth between them.
Multichatui.jhtml and nowDefunctWindow.jhtml	<CCSrootdirectory>\pub\html\multichatui	Removes the Forward, Back, and Refresh buttons from the multi-session chat Agent Desktop.
PageDisplay.jhtml	<CCSrootdirectory>\pub\html\multichatui	For multi-session configurations, removes the browser controls from the agents' external Shared View window (for single-session configurations, this is done in the agent.properties file).
sessionMirror.jhtml	<CCSrootdirectory>\pub\html\multichatui	For multi-session configurations, causes pages to be pushed through the DCA rather than CCS's page display applet.
Toolbar.jhtml	<CCSrootdirectory>\pub\html\multichatui	Removes the Page Synch button from the multi-session chat Agent Desktop.
UIComponents.jhtml	<CCSrootdirectory>\pub\html\multichatui	For multi-session configurations, prevents the External View toggle button in the Agent Desktop from displaying an internal view.

Modified CCS Files

The DCA-CCS Updater makes changes to these files on your CCS Server without overwriting them. Modified settings are denoted by comments within the files.

File	Description / Location	Description of Change
caller.properties	caller.properties stores settings for controls and behaviors in the single-session caller desktop. <CCSrootdirectory>\servlet\properties	Disables items in the caller desktop that conflict with the DCA. Sets the Caller Complexity Mode to Simple.
msccaller.properties	Stores settings for controls and behaviors in the multi-session Caller Desktop. <CCSrootdirectory>\servlet\properties	Disables items in the caller desktop that conflict with the DCA. Sets the Caller Complexity Mode to Simple.
wlserver.properties	wlserver.properties stores basic settings for Collaboration Server, including server connection, database, and session settings. <CCSrootdirectory>\servlet\properties	Adds the DCA host name so that CCS knows how and from where to load the Collaboration Toolbar. Also establishes the protocol (HTTP or HTTPS) used by the DCA.
Agent.properties	<CCSrootdirectory>\servlet\properties	Agent.properties stores settings for controls and behaviors of the Agent UI.
WlConfigMgr.default	<CCSrootdirectory>\servlet\properties	WLConfigManager.default is used to load property files.

See Also

For related information, see:

About DCA-CCS Integration

About the DCA-CCS Updater

About DCA 2.01 Changes to Agent Role Settings

How to Add DCA Code to Localized CCS Files

How to Install the DCA-CCS Updater

About DCA 2.01 Changes to Agent Role Settings

During integration, the DCA automatically set values it requires for the following CCS agent role settings. These settings are then disabled and cannot be modified in the CCS Administration Desktop.

Settings for Multi-Session Agent Roles

DCA-integrated CCS uses the following settings for Multi-Session agents.

Settings Group	Setting / DCA Value	Description
Session URL Settings	Start session page URL - startdca.jhtml	DCA uses a special page, startdca.jhtml, that loads the Collaboration Toolbar for callers and agents at the start of a session.
External View Settings	Auto external shared view - selected.	DCA requires the use of an external shared view.
Feature Settings	Page share - not selected.	Supplanted by a similar command in the DCA Collaboration Toolbar.

Settings for Single-Session Agent Roles

DCA-integrated CCS uses the following settings for Multi-Session agents.

Settings Group	Setting - DCA Value	Explanation
Session URL Settings	Start session page URL - startdca.jhtml	DCA uses a special page, startdca.jhtml, that loads the Collaboration Toolbar for callers and agents at the start of a session.
External View Settings	Auto external shared view - selected.	DCA requires the use of an external shared view.
Session Initiation Settings	Start Session as Leader - not selected.	Session Leadership is deprecated. In DCA, the agent is always the de facto session leader.
Session Initiation Settings	Auto Follow Me - not selected.	Supplanted by a similar command in the DCA Collaboration Toolbar.
Feature Settings	Page Share - not selected.	Supplanted by a similar command in the DCA Collaboration Toolbar.
Feature Settings	Form Share - not selected.	Supplanted by a similar command in the DCA Collaboration Toolbar.
Feature Settings	Follow Me - not selected.	Supplanted by a similar command in the DCA Collaboration Toolbar.

Feature Settings	Change Leader - not selected.	Session Leadership is deprecated . In DCA, the agent is always the de facto session leader.
Feature Settings	White Board - not selected.	Disabled by default by DCA-CCS integration. Can be re-enabled (see next section).
Feature Settings	Application Share - not selected.	Disabled by default by DCA-CCS integration. Can be re-enabled (see next section).

Additional Notes for DCA Agent Role Settings

These additional notes pertain to DCA agent roles:

- Do not use the Logon Form Setting Override (under General Agent Settings) in such a way that it modifies agent settings required by the DCA.
- For Single-Session Agent Roles, the History feature is not disabled by the DCA but serves no practical purpose. It's recommended that you turn this feature off for users.
- The following Agent Desktop user preferences have no affect in DCA-integrated CCS. While they still appear in the agents list of user preferences, their settings are overridden by DCA functionality:

  In the Single-Session Desktop:

  - Automatically take leadership of new session
  - Turn follow-me on in a new session
  - Open shared space in an external view

  In the Multi-Session Desktop:

  - Automatically shared space in an external view

See Also

For related information, see:

About DCA-CCS Integration

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

How to Install the DCA-CCS Updater

How to Re-Enable White Board and App Share

How to Create the DCA-Collaboration Server Connection

The DCA-CCS connection allows communication between the DCA and CCS for agent reporting and tracking. The connection establishes an Agent Reporting and Management (ARM) service that:

- Makes information on Web content shared during DCA sessions available for CCS reports.
- Allows the automatic cleanup of DCA sessions when their associated CCS sessions are terminated.

Note that in the event of a failed connection, the DCA will continue to function otherwise correctly. However, any session integration made possible by the ARM will be unavailable.

Creating the DCA-CCS connection consists of the following steps:

Step 1. Define the DCA connection on CCS

Step 2. Transfer the authentication/configuration files

Step 3. Configure the connection for SSL (optional)

Step 4. Enable the connection on the DCA

Step 5. Test the connection

Step 1: Defining the DCA Connection on CCS

The first step in creating the DCA-CCS connection is to define the connection on Collaboration Server. To define the connection on Collaboration Server:

1. Open the CCS Administration desktop.
2. From the Administration desktop menu, select Server Setup > Connections > Create. The Connect Wizard screen opens.

3. Select Dynamic Content Adapter. Click Next.

   In the DCA Connection Name field, specify a name for the connection. The name must:

   - Include alphanumeric characters and underscores only.
   - Be 30 characters or less.
   - Be unique (from DCA Connection Names you have created for other CCS servers, if any).

4. In Description, if desired, enter a description for the connection to be used in the Collaboration Administration desktop.

5. In DCA Host Name, enter the DCA server's unique host name (for example, myDCA.mydomain.com) or its static IP address.

6. Registry Port on DCA specifies the port the DCA uses to register a connection instance with CCS. You MUST use the default, 1099.

   - If the DCA will communicate with CCS through a firewall, you must enable a one-way connection from the DCA to CCS on your firewall for this port.

7. In CCS Password, create a password the DCA will use to authenticate itself to Collaboration.

8. In Verify CCS Password, re-enter the password.

9. In Registry Port on CCS, specify the port CCS should use to register a connection instance with the DCA. Cisco recommends that you use the default, 1099.

   - If you previously defined the CCS registry port for a different server connection (for example, Cisco Media Blender), CCS will automatically use that same port for your DCA connection.

10. In Connection Port on CCS, specify the port CCS should use to connect to and communicate with the DCA. If left blank, CCS will search for and use the first available port.

    - If the DCA will communicate with CCS through a firewall, you must specify a specific port, and then enable that port on your firewall.

11. In CCS Password, create a password the DCA will use to authenticate itself to Collaboration . If left blank, no password will be used.

12. In Verify CCS Password, re-enter the password.

13. Check the `Disable Automatic Connect` check box. This ensures that Collaboration Server operates in RMI "server" mode, while the other applications (i.e., the DCA) operate in RMI "client" mode.

14. Click Finish.

15. Restart the Web server on CCS.

Step 2: Transferring the Authentication/Configuration Files

When you define the CCS-DCA connection in the CCS Admin Tool, two files used to authenticate the connection are automatically created on your CCS server. These files must be copied to your DCA server.

To copy the authentication files:

1. On your Collaboration server, navigate to: `<CCSrootdirectory>\Servlet\Properties\dca\<connectionname>\.`

2. In the `<connectionname>` directory, locate these two files: `<connectionname>.properties` and `messageadapter.properties.`

3. Transfer the files to your DCA server, and place them here: `DCA\WebApp\WEB-INF\Cisco\properties.`

   Note: The target directory on your DCA server will already contain a file named `messageadapter.properties`. Overwrite the existing file with the new one.

Step 3: Configuring the Connection for SSL

Optionally, you may want to configure the CCS-DCA connection for SSL. This ensures that data sent from the DCA to CCS are encrypted. Configuring the connection for SSL requires first generating keystore and truststore files for your connection using the JDK Keytool utility that ships with the DCA.

To Configure the DCA-CCS Connection for SSL:

1. Using the JDK Keytool utility, generate a keystore and truststore for your DCA-CCS connection. When you generate the keystore, you will also create a certificate that you will export to the truststore.

   - Additional information on generating DCA keystores and truststores is included in the CCS Administration Desktop online Help. Additional information on using the Keytool is available at: http://java.sun.com/j2se/1.4/docs/tooldocs/windows/keytool.html. Steps for

creating a sample keystore and truststore are available at:
http://java.sun.com/j2se/1.4/docs/guide/security/jsse/JSSERefGuide.html#RMISample

- Although you can create a keystore and truststore on any server, because the DCA 2.01 uses an earlier version of the JDK (1.3.1) than CCS, it's recommended that you generate your keystore and truststore on the DCA.

2. After generating the files, transfer the keystore file to any location on your Collaboration Server. Move the truststore file to a desired location on your DCA server.

3. On your **Collaboration Server**, in the `<connectionname>.properties` file, uncomment the lines pertaining to SSL and keystore. Provide the values as requested. Do not uncomment the lines pertaining to truststore.

   After editing, the SSL section of your `<connectionname>.properties` file on Collaboration Server should look something like this:

```
# Uncomment this property to enable SSL
  DCA_Conn_1.rmi.SocketType = SSL
# Location of key store (absolute path)
  DCA_Conn_1.rmi.KeyStore = c:\cisco_cs\mykeystore.keystore
# Type of key store
  DCA_Conn_1.rmi.KeyStoreType = JKS
# Key store password
  DCA_Conn_1.rmi.KeyStorePassword = mykeystore_password
# Key password
# DCA_Conn_1.rmi.KeyPassword=
# Location of trust store (absolute path)
# DCA_Conn_1.rmi.TrustStore=
# Type of trust store
# DCA_Conn_1.rmi.TrustStoreType=JKS
# Trust store password
# DCA_Conn_1.rmi.TrustStorePassword=>
```

4. Restart the Web server on CCS.

5. On your **DCA server**, in the `<connectionname>.properties` file, uncomment the lines pertaining to SSL, key password, and truststore. Provide the values as requested. Do not uncomment the lines pertaining to keystore.

   After editing, the SSL section of the `<connectionname>.properties` file on the DCA should look something like this:

```
# Uncomment this property to enable SSL
  DCA_Conn_1.rmi.SocketType = SSL
# Location of key store (absolute path)
# DCA_Conn_1.rmi.KeyStore=
# Type of key store
# DCA_Conn_1.rmi.KeyStoreType=JKS
# Key store password
```

```
# DCA_Conn_1.rmi.KeyStorePassword=
# Key password
  DCA_Conn_1.rmi.KeyPassword = mykey_password
# Location of trust store (absolute path)
  DCA_Conn_1.rmi.TrustStore = c:\dca\mytruststore.truststore
# Type of trust store
  DCA_Conn_1.rmi.TrustStoreType = JKS
# Trust store password
  DCA_Conn_1.rmi.TrustStorePassword = mytruststore_password
```

Step 4: Enabling the DCA-CCS Connection on the DCA Server

After creating the DCA-CCS connection and copying the authentication files to the DCA, you must enable the connection on the DCA server.

To enable the DCA-CCS connection:

1. In the DCA Admin Tool, select Configuration > ProxyProperties.
2. Set the enableDCACCSConnection property to True.
3. Click Submit.
4. Restart the DCA.

Step 5: Testing the DCA-Collaboration Connection

After creating the DCA-CCS connection, you may want to test to verify that it is active.

To test the DCA-Collaboration connection:

1. Open the Collaboration Administration desktop.
2. From the Administration desktop menu, select Server Setup > Connections > Monitor. The Connection Monitor screen opens, displaying the status of all Collaboration connections.

See Also

For related information, see:

How to Deploy the DCA

About DCA-Collaboration Server Integration

How to Deploy the DCA Behind a Firewall

DCA-CCS Integration Troubleshooting

How to Add DCA Code to Localized CCS Files

During integration, the DCA modifies or overwrites a number of files on CCS, adding code that the DCA needs to function. However, the DCA-CCS updater only modifies the English versions of these files; If you localize CCS (either before or after integration) to use non-English versions of these files, you will need to manually add some code to the localized file versions.

Caution: Failure to do this will prevent the DCA from functioning.

To add DCA code to localized CCS files:

In a text editor, modify localized CCS files as shown in the table below. In the table below, the third column (To:) shows what the code should look like after DCA code is added, with newly added code shown in **bold** face.

In (localized file):	**Modify the Line(s):**	**To:**
ACDblended.html ACDblendedICM.html callForm.html callFormICM.html softblendedICM.html These files are located at: <CCSrootdirectory>/pub/html/forms	document.callback.initSessionPage.va =buttonAddress; -AND- <INPUT TYPE="hidden" NAME="initSessionPage">	**//**document.callback.initSessionPage.value= buttonAddress; -AND- <**!**INPUT TYPE="hidden" NAME="initSessionPage">
callme.html This file is located at: <CCSrootdirectory>/pub/html/forms	newWindow = window.open("callFrame.html", "Caller");	newWindow = window.open("callFrame.html", "Caller"**,"resizable=yes,toolbar= no,location=no, status=yes,scrollbars=yes,menubar= no"**);
msccallme.html This file is located at: <CCSrootdirectory>/pub/html/forms	newWindow = window.open("mscCallFrame.html", "Caller");	newWindow = window.open("mscCallFrame.html", "Caller"**,"resizable=yes,toolbar= no,location=no, status=yes,scrollbars=yes,menubar= no"**);
index.html <CCSrootdirectory>/pub/html/forms	newWindow = window.open(url, "Caller"); -AND- <a href="/meetme">	newWindow = window.open(url, "Caller"**,"resizable=yes,toolbar= no,location=no,status=yes, scrollbars=yes, menubar=no"**); -AND- <a href=**'javascript:callMeWindow ("/meetme")'**>

See Also

For related information, see:

About DCA-CCS Integration

How to Re-Enable White Board and App Share

DCA-CCS integration automatically disables the CCS White Board and App Share features available to Single-Session agents. If you want, after integration you can re-enable these features. Note that re-enabling White Board and/or App Share will reintroduce the security warning users receive when the applet used by these features downloads during a session.

Note: Re-enabling White Board or App Share enables the feature for all CCS users. It is not possible to re-enable either feature for select agents roles.

To Re-Enable White Board or App Share:

1. Set Caller Complexity mode to Complex:
   - In a text editor, open `caller.properties`, located at: `<CCSrootdirectory>\servlet\properties`.
   - Set `complexityMode` to Complex. (Before proceeding, it's recommended that you review the *CCS Administration Guide* for information and caveats regarding complexity mode
2. In a text editor, open `DCARolesOverride.properties`, located at: `<CCSrootdirectory>\servlet\properties`.
3. To re-enable White Board, set `dcaRolesOverride.ssEnableWhiteboard` to `True`.
4. To re-enable App Share, set `dcaRolesOverride.ssEnableShareApp` to `True`.
5. Save the file.
6. Restart the CCS Web server.

Caution: Do not attempt to affect behavior by commenting out any of the properties in `DCARolesOverride.properties`. Doing so will cause the role properties pages in the CCS Admin Desktop to fail.

See Also

For related information, see:

About DCA-Collaboration Server Integration

About DCA 2.01 Changes to Agent Role Settings

DCA-CCS Integration Troubleshooting

DCA-CCS Integration Troubleshooting

The table below lists suggestions for troubleshooting problems encountered immediately after integrating the DCA with CCS. These suggestions assume that:

- Your DCA server is otherwise configured and running properly.
- Your Collaboration server is configured and running properly.
- Web content you are attempting to access is valid and available from a properly configured and functioning Web server.

Symptom	Possible Cause	Possible Solution
CCS is configured for SSL but pages accessed via the DCA Collaboration Toolbar are not secure.	DCA Collaboration Toolbar not configured for SSL.	Configure the Collaboration Toolbar for SSL as described in the *DCA 2.01 Administration and Configuration Guide.*
The Collaboration Toolbar does not display the default CCS Call Me page file at the start of a session.	Collaboration Server is accessed by a different name in and out of the network.	For test environments only, your Collaboration Server must be accessible by the same name both inside and outside of your network. For example, if your Collaboration Server is accessed from the Internet as http://myCCS.mydomain.com, then within your local network the DCA must be able to access it using that same name.
DCA connection to CCS is down	Physical connection between the servers is down -OR- messageadapter.properties and <connectionname>.properties files not copied to correct location on DCA -OR- Connection not enabled on DCA -OR- Connection configuration uses invalid ports or ports not enabled on firewall.	Verify that physical connection between servers is active -OR- Verify connection settings as specified in How to Create the DCA-Collaboration Server Connection.
CCS localization is lost after DCA integration.	During integration, the DCA modifies or overwrites a number of files on CCS in English.	Merge and re-localize affected files as described in How to Re-localize CCS After Integration.

Cannot log in an agent and caller on the same PC using a single browser.	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.	Open the agent and caller in different separate browsers (e.g., IE for the agent, Netscape for the caller).

Other Troubleshooting Information

Troubleshooting information related to DCA installation problems can be found at DCA Installation Troubleshooting. Troubleshooting information related to page parsing problems can be found in the *DCA 2.01 Administration and Configuration Guide*. For additional information on other DCA runtime issues, see the *DCA 2.01 Release Notes*.

See Also

For related information, see:

About DCA-Collaboration Server Integration

How to Test the Updater Installation

How to Create the DCA-Collaboration Server Connection

How to Re-localize CCS After Integration

DCA Installation Troubleshooting

Section IV: Uninstalling-Reinstalling the DCA

Uninstalling-Reinstalling the DCA on Windows

How to Uninstall the DCA on Windows

Uninstalling the DCA also automatically uninstalls the JDK and ServletExec.

Caution: If you are uninstalling the DCA as part of a reinstallation, and you have customized settings in the DCA properties files or parser, you may want to backup these files before proceeding.

To Uninstall the DCA

1. Stop the DCA server.

   Caution: Failure to do this will prevent the DCA from uninstalling properly.

2. From the Windows Start Bar, select Settings > Control Panel > Add/Remove Programs > Dynamic Content Adapter 2.01.

3. Delete the DCA directory, along with all of its subdirectories.

   The DCA Uninstaller will not fully remove the DCA. After running the uninstall, use Windows Explorer to delete it.

4. Reboot your server.

   Caution: Certain files used by the DCA uninstall are not removed from the system until the server is rebooted. Failure to reboot the server after an uninstall can adversely affect a subsequent reinstallation of the DCA.

How to Reinstall the DCA on Windows

If you need to reinstall the DCA, follow the steps described below.

To Reinstall the DCA

1. Backup the DCA properties files.

   If you customized DCA settings in your current installation, it's a good idea to backup the DCA properties files prior to uninstalling the DCA. After the new install, you can restore your settings by overwriting the new properties files with

the backups. The properties files are located at: `<DCArootdirectory>\webapp\WEB-INF\Cisco\properties`.

2. Uninstall the DCA.

   Caution: To reinstall the DCA, you must first uninstall the DCA. DO NOT attempt to reinstall the DCA over a current installation. Uninstalling the DCA also removes the JDK and ServletExec.

3. Install the DCA.

4. Restore the properties files.

   If desired, overwrite the newly installed properties files with your backed up copies.

   Caution: Only restore backup properties files IF you are reinstalling the DCA to the same location on the same server.

5. Restart the DCA server's Web server software.

How to Uninstall the DCA-CCS Updater

If necessary, you can uninstall the DCA-CCS Updater from your Collaboration Server. After uninstalling the Updater, your Collaboration Server will not function with the DCA.

Uninstalling the Updater reverses any changes it made to your original Collaboration Server configuration, PROVIDED that the affected files were not modified subsequent to installing the Updater. Affected files that HAVE been modified subsequent to installing the Updater can be restored manually from their backups.)

To Uninstall the DCA-CCS Updater

To uninstall the DCA-CCS Updater from Collaboration Server running IIS under Windows:

1. Stop the IIS Admin and WWW Publishing services.

   Caution: Failure to stop these services will prevent the DCA-CCS Updater from uninstalling properly.

2. From the Windows Start Menu, select Settings > Control Panel > Add/Remove Programs > Dynamic Content Adapter 2.01 CCS Updater.

3. When the uninstall procedure is complete, delete the contents of the `pageCompile` directory, located at `<CCSrootdirectory>/install/`.

4. Restart the IIS Admin and WWW Publishing services.

See Also

For related information, see:

How to Uninstall the DCA

How to Reinstall the DCA

DCA Installation Troubleshooting

About DCA Directory Structures

How to Stop and Start the DCA Server

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

The DCA Administration and Configuration Guide

Uninstalling-Reinstalling the DCA on Solaris

How to Uninstall the DCA on Solaris

Caution: If you are uninstalling the DCA as part of a reinstallation, and you have customized settings in the DCA properties files or parser, you may want to backup these files before proceeding.

To Uninstall the DCA

1. Stop the DCA server.

   Caution: Failure to stop the DCA from uninstalling properly.

2. Run the DCA uninstall script from the location: /DCA/bin with the command: ./uninstall

3. The uninstall script prompts to delete the DCA. Type 'Yes'. This deletes the DCA and DCA-webroot directory and all their sub directories.

4. This script also replaces the backed up files in the Sun ONE (iPlanet) server instance. For example, /usr/iplanet/servers/<https-dcahost>/config.

   Caution: Certain files used by the DCA uninstall are not removed from the system until the server is rebooted. Failure to reboot the server after an uninstall procedure can adversely affect a subsequent reinstallation of the DCA.

   Note : Cisco recommends to completely uninstall the Sun ONE web server instance by manually deleting the server instance that was configured for this DCA.

How to Reinstall the DCA on Solaris

If you need to reinstall the DCA, follow the steps described below.

To Reinstall the DCA

1. Backup the DCA properties files.

   Note: If you customized DCA settings in your current installation, it's a good idea to backup the DCA properties files prior to uninstalling the DCA.

After the new installation, you can restore your settings by manually changing the new properties files with the backups files without altering the properties configured by the installation. The properties files are located at: `DCA/webapp/WEB-INF/Cisco/properties`.

2. Uninstall the DCA.

Caution: To reinstall the DCA, you must first uninstall the DCA. DO NOT attempt to reinstall the DCA over a current installation.

3. Install the DCA.

4. Restore the properties files.

If desired, modify the newly installed properties files with your backed up copies.

5. Restart the DCA server's Web server software.

How to Uninstall the DCA-CCS Updater

If necessary, you can uninstall the DCA-CCS Updater from your Collaboration Server. After uninstalling the Updater, your Collaboration Server will not function with the DCA.

Uninstalling the Updater reverses any changes it made to your original Collaboration Server configuration, PROVIDED that the affected files were not modified subsequent to installing the Updater. Affected files that have been modified subsequent to installing the Updater can be restored manually from their backups.

To Uninstall the DCA-CCS Updater

To uninstall the DCA-CCS Updater from Collaboration Server running Sun ONE under Solaris:

1. Stop the iPlanet server instance.

2. Insert the DCA 2.01 CD in your DCA Machine's CD drive and the CD mounts automatically.

3. In the CD, the 'ccs_dca_uninstall' script is located in the directory path: CCS_DCA_Updater/ccs_dca_uninstall

4. Run the 'ccs_dca_uninstall' script with the command: ./ccs_dca_uninstall.

5. This script updates the Collaboration Server to its earlier configurations and the DCA connection is removed.

See Also

For related information, see:

How to Uninstall the DCA for Solaris

How to Reinstall the DCA

DCA Installation Troubleshooting

About DCA Directory Structures

How to Stop and Start the DCA Server

About the DCA-CCS Updater

About DCA 2.01 Changes to CCS Files

Section V: Reference

About DCA Directory Structures

The following table shows the DCA 2.01 directory tree that installs on your server, and gives a brief description of the files stored in each directory. Note especially that:

- All configurable DCA files are located within DCA\webapp\WEB-INF\Cisco. Do not modify DCA files outside of this directory unless specifically instructed to do so.
- Files used to update Cisco Collaboration Server to integrate it with the DCA are located in the DCA\Updaters directory.

The DCA installs the JDK and ServletExec within the DCA root directory for Windows. For Solaris we need to install the JDK manually and configure while installing the Sun ONE Web Server. The directory DCA/jdk and DCA/servletexec does not exist for Solaris installation.

Directories and subdirectories	**Directory Description:**
DCA	DCA root directory.
DCA/docs and subdirectories	DCA user documentation.
DCA/jdk and subdirectories	Java Development Kit program files.
DCA/servletexec and subdirectories	ServletExec program files.
DCA/uiserver and subdirectories	Cisco UIServer program files. Provides communication between the DCA Server and the Collaboration Toolbar.
DCA/Uninst	DCA uninstall information used by the DCA Uninstaller.
DCA/Updaters and subdirectories	DCA-CCS Updater files. Includes individual copies of DCA-modified CCS configuration files.
DCA/webapp/client	JSP pages used by Collaboration Toolbar.
DCA/webapp/WEB-INF	Container for DCA program and configuration files.
DCA/webapp/WEB-INF/Cache	Files stored by DCA Static Cache.

DCA/webapp/WEB-INF/Cisco	Stores DCA configuration directories.
DCA/webapp/WEB-INF/Cisco/license	Stores DCA license file.
DCA/webapp/WEB-INF/Cisco/logs	Stores DCA log files.
DCA/webapp/WEB-INF/Cisco/properties and subdirectories	Stores DCA configurable properties files.
DCA/webapp/WEB-INF/Cisco/Responses	Stores user-defined custom error pages.
DCA/webapp/WEB-INF/classes and subdirectories	DCA program files.
DCA/webapp/WEB-INF/Copies	Default directory used to store Copy Server pages.
DCA/webapp/WEB-INF/lib	DCA program files.

See Also

For related information, see:

About DCA 2.01 Changes to CCS Files

The DCA Administration and Configuration Guide

How to Stop and Start the DCA

The following sections describe how you can stop and start the DCA on Windows and Solaris.

Stop and Start the DCA for Windows Platform

To Stop the DCA

Stop the DCA on a Windows server by stopping the IIS Admin and WWW Publishing Services:

1. From the Windows Start menu, select Settings > Control Panel > Admin Tools > Services.
2. Right-click IIS Admin Service.
3. From the popup menu, select Stop.
4. A dialog opens listing dependant services that will also be shut down. This list should include the WWW Publishing Service. Click OK.

To Start the DCA

Start the DCA on a Windows server by starting the IIS WWW Publishing Services:

1. From the Windows Start menu, select Settings > Control Panel > Admin Tools > Services.
2. Right-click WWW Publishing service.
3. From the popup menu, select Start.

Note: Services whose Startup Type is set to Automatic will also restart automatically when you reboot the server.

Stop and Start the DCA for Solaris Platform

You can stop and start the DCA either from the Web Server Administration Console or from the Solaris Command Line.

Stopping the DCA

From the Web Server Administration Console, stop the DCA on a Solaris server by stopping the iPlanet (Sun ONE) instance:

1. Using your web browser, go to the administration page at http://<DCA Server>:8888, where <DCA Server> is the name of the server on which you installed DCA.

2. Select the DCA server instance you want to stop. Click ‘Manage’.

Note: The default server instance that is selected is the first server instance that was created when Sun ONE was installed.

3. The Server On/Off Page shows whether the server is ON or OFF. If the server isn’t already OFF, click ‘Server Off’. This shuts the server down and stops all the running processes.

Starting the DCA

From the Web Server Administration Console, start the DCA on a Solaris server by stopping the iPlanet (Sun ONE) instance:

1. Using your web browser, go to the administration page at http://<DCA Server>:8888, where <DCA Server> is the name of the server on which you installed DCA.

2. Select the DCA server instance you want to stop. Click ‘Manage’.

Note: The default server instance that is selected is the first server instance that was created when Sun ONE was installed.

3. The Server On/Off Page shows whether the server is ON or OFF. If the server isn’t already OFF, click ‘Server Off’. This shuts the server down and stops all the running processes. After you start the server, it may take a few seconds for the server to start all the process and for the status to change to ‘ON’.

Starting And Stopping DCA from the Command Line

DCA can be started and stopped from the command line by using the commands below. To stop the DCA we need to stop the Sun ONE server.

Command	Description
/usr/iplanet/servers/https-<DCAhost>/start	Starts the Sun ONE Web Server
/usr/iplanet/servers/https-<servername>/stop	Stops the Sun ONE Web Server

Note: This may depend on the specific location for where Sun ONE is installed.

See Also

For related information, see:

About DCA 2.01 Changes to CCS Files

The DCA Administration and Configuration Guide

As necessary, you can use the DCA Admin Tool to confirm the version and build number of your DCA Server software.

To Confirm the DCA Build Number

To confirm the version and build number of your DCA Server:

In the Admin Tool, select Server Administration. Your DCA version and build number are displayed.

See Also

For related information, see:

The DCA Administration and Configuration Guide

How to Use the ServletExec Admin Tool (For Windows only)

While usually not necessary, you may on occasion want to adjust settings in ServletExec (for example, to adjust your server's Virtual Machine memory or to modify Copy Server properties.

To Access the ServletExec Admin Tool

ServletExec includes a Web-based administration tool that can be used to adjust ServletExec settings. Access to the ServletExec Admin Tool is limited to the local machine, by default.

To access the admin tool:

In a Web browser, navigate to `http://localhost/servlet/admin`. For example: `http://myserver/servlet/admin`

See Also

For related information, see:

How to Modify Java Virtual Machine Memory

The DCA Administration and Configuration Guide

How to Modify Java Virtual Machine Memory

For performance reasons you may want to increase the amount of memory available to the Java Virtual Machine on your DCA server. Note that Cisco recommends JVM memory never be lower than 512 Mb, the default set by the DCA is installation.

To Change Virtual Machine memory for Windows Platform

To change the amount of memory available to Java Virtual Machine on your DCA server:

1. Open the ServletExec Admin Tool.
2. In the Admin Tool navigation frame, click Virtual Machine > Settings.
3. In Max Heap Size, adjust the amount of available memory.
4. Click Submit.
5. Restart IIS.

To Change Virtual Machine memory for Solaris Platform

In the Sun ONE configuration, in the file /usr/iplanet/servers/https<servername>/config/jvm12.conf, uncomment the earlier property and place a new line for the jvm.minHeapsize to change the minHeapsize property.

Example:

```
#jvm.minHeapSize=1048576
jvm.maxHeapSize=536870912
```

Likewise, you might want to change the maxHeapSize too, depending on your requirements.

After changing the Virtual Machine memory file, you need to restart the Sun ONE server.

See Also

For related information, see:

How to Use the ServletExec Admin Tool

The DCA Administration and Configuration Guide

About the IIS Lockdown Tool

On Windows 2000 platforms, you may choose to run the IIS Lockdown Tool on your DCA/IIS server. The IIS Lockdown Tool is a wizard which reduces IIS's vulnerability to virus attack by turning off unnecessary IIS features. It is available at:

http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp

Running the IIS Lockdown Tool on Your DCA Server

The IIS Lockdown Tool should be run only AFTER the DCA has been installed on your server. If the Lockdown Tool has already been run, you must uninstall it prior to installing the DCA. Failure to first remove the Lockdown Tool will prevent the DCA from installing properly.

After the DCA is installed, you can reinstall the Lockdown Tool using the settings described below.

Note: The information in this guide is based on the Lockdown Tool, version 2.1. For information on subsequent versions, consult your Cisco representative.

Detecting a Previous Lockdown Tool Installation

To detect whether the Lockdown Tool was previously run on your server, check the `DCA\System32\inetsrv` directory for the presence of files named `oblt-rep.log` and/or `oblt-log.log`. The presence of either of these files indicates that the Lockdown Tool has been run.

Uninstalling the Lockdown Tool

If necessary, uninstall the Lockdown Tool by running it a second time. Running the Lockdown Tool wizard over a current installation causes it to uninstall. When run over a current installation, the wizard displays a message asking you to confirm the uninstall. If instead of this message the wizard displays a license agreement, the previous installation has already been removed.

Installing the Lockdown Tool - DCA Settings

When you install the Lockdown Tool, you are prompted to select a template that most closely matches the role of your server. Select the PROXY SERVER template. This template automatically uses the settings required by the DCA. Specifically, these include:

- Services: Web Service (HTTP) enabled.
- File Permissions for Anonymous Users: Writing to content directories enabled.
- Virtual Directories: Scripts directory enabled.
- URL Scan Filter: Not installed.

See Also

For related information, see:

About DCA Software Requirements

DCA Installation Troubleshooting

The DCA Administration and Configuration Guide

DCA Glossary

The following important terms appear in the DCA documentation.

A

Admin Tool

The DCA Web interface for administering, monitoring and configuring the DCA.

agent

An individual using the Agent Desktop to access Collaboration Server (for example, an agent in a call center).

App Share

A Collaboration feature that allows you to share an open application on your desktop with other session participants.

C

caller

An individual using the Caller Control Panel to access Collaboration Server (for example, a call-center customer).

caller complexity mode

A Collaboration Server setting which determines if and when the CCS caller applet is downloaded to caller machines. The presence or absence of the caller applet in turn affects the type of content agents and callers can share.

The DCA automatically sets caller complexity mode to "simple." Simple mode, prevents the caller applet from downloading, thus eliminating security warnings otherwise displayed to callers. However, it also prevents participants from using two of CCS's advanced content sharing features -- App Sharing and White Boarding.

Caller Remote Control

A Collaboration feature that allows agents to trigger a content sharing event (for example, page share) from a caller's browser.

CCS

See Collaboration Server.

Cisco Collaboration Server

The Cisco Collaboration Server, an application that provides online Web site assistance through features like online chat, callback, desktop sharing, and Web content collaboration.

client-side processing

Includes Java applets, JavaScript and Visual Basic scripts, plugins, and a number of other mechanisms used to alter content after it has been received by the client browser.

collaboration

The act of sharing a view to Web content among multiple users.

Collaboration Toolbar

The DCA's Collaboration Toolbar is a set of Web tools that you use to view and share Web content in a Collaboration session. The Collaboration Toolbar is used by both agents and callers. It loads automatically in the Collaboration Server's Shared View area at the start of a Collaboration session.

complexity

See *caller complexity mode*.

cookie

Data that can be used to identify a user to a Web server. Each time the user returns to that server, the user's browser presents the same cookie. The cookie can be updated as the user inputs information or performs actions on the site, from session to session.

Copy Server

A DCA service used to store unexpired pages after they have been forced from the DCA cache.

custom error

DCA feature in which a user-defined html file is returned when a DCA user encounters a Web browser or server error condition.

D

DCA

The Dynamic Content Adaptor, an application that extends the Cisco Collaboration Server's (CCS) functionality to allow successful sharing of pages that contain SPLIT content.

DCA cache

Pages returned to the DCA from a Web content server are initially stored in the DCA cache where they are available to satisfy subsequent user requests. Pages can expire in the cache, after which they are unavailable. Unexpired pages that are forced from the cache due to space constraints are stored in the Copy Server.

DCA server

The server on which the DCA is installed. The DCA cannot be installed on the same server as Cisco Collaboration Server.

dynamic content

Web content that is generated dynamically based on factors like the time it was requested or information provided by the user. Includes live, interactive, personalized, and transactional content.

F

Follow Me Browsing

A Collaboration feature that allows participants to browse a Web site together. Each page the session leader navigates to is automatically sent to other participants.

Form Share

A Collaboration feature that allows you to share data you have entered in an online form with to other participants in your session.

frameproofed pages

Web pages with JavaScript code that prevents the pages from opening in a frame of another Web page.

G

GET

Method of submitting an online form in which form data are passed in a query string appended to a URL. This makes GETs subject to a URL's maximum size limitation (typically, 2Kb). See also, POST.

I

interactive content

Content that is contingent upon a user's interaction with a Web page.

L

live content

Content that changes based on factors such as the time it was requested or actions the user has performed previously.

O

output cache

After a page is stored in the DCA's Response cache, the DCA reconstructs it and passes it to the Output cache, where it is available to users. Subsequent requests for the page are satisfied directly from the Output cache.

P

Page Share

A Collaboration feature that allows you to send the page you are currently viewing to other participants in your session.

participant

Any individual engaged in a DCA or CCS session (i.e., an agent or client).

personalized content

Content that is specific to the user requesting it. A Web content server typically determines what Personalized content to display based on a user cookie or other state information.

POST

Method of submitting an online form in which form data are attached to the end of the POST request in its own object. See also, GET.

properties files

A set of files you use to configure and customize the DCA. Properties files can be edited through the Admin Tool.

R

remote control

See *Caller Remote Control*.

response cache

When a page is initially returned to the DCA from a Web content server, the DCA parses the page, redirects all links on the page to the DCA, and then stores the page as a Java object in its Response cache.

S

secure socket layer

A standard technology that encrypts content sent between Web browsers and servers. When Cisco Collaboration Server is SSL-enabled, the padlock in the upper right corner of the agent desktop is engaged.

session

A successful connection between an agent and a caller. Collaboration agents using the multi-session chat desktop can participate in multiple online chat sessions.

secure content

Content that is access-controlled to a specific user or group of users. Access can be controlled in a number of ways, for instance by a login password or by a user's IP address.

Shared View

The Collaboration Shared View is either a frame or full browser window that displays the content that agents and callers are sharing. Collaboration Toolbar users must use an external shared view.

SPLIT content

An acronym for secure, personalized, live, interactive, and transactional Web content that cannot be shared by simple URL sharing.

T

transactional content

Content that is returned based on data a user submits to a back-end system, for example, by submitting an order form.

W

White Board

A Collaboration feature that allows you to share a drawing program with other session participants.

Cisco Support for the DCA

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:
- (listed as: Cisco Collaboration Server Dynamic Content Adapter)

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

To Open a Technical Assistance Call

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

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.

To Contact the Cisco 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

Index