WebDialer

WebDialer Overview

Cisco WebDialer is installed on a Unified Communications Manager node and used along with Unified Communications Manager. It allows Cisco Unified IP Phone users to make calls from web and desktop applications.

Cisco WebDialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call. Cisco WebDialer supports both IPv4 and IPv6 addressing.

In the Cisco Unified Communications Self-Care Portal, from the Directory window, launch Cisco WebDialer using a URL similar to the following:

```
https://<IP address of Cisco Unified Communications Manager server>:8443/webdialer/
Webdialer
```

In the **Cisco WebDialer** screen click **Login** to access the WebdDialer system. A new pop-up window allows you to enter Unified Communications Manager **User ID** and **Password** to perform the necessary Make Call activities.

WebDialer Prerequisites

Cisco WebDialer requires the following software components:

- CTI-supported Cisco Unified IP Phones

WebDialer Configuration Task Flow

Before you begin

- Review WebDialer Prerequisites, on page 1.

Procedure

	Command or Action	Purpose
Step 1	Activate WebDialer, on page 3	Activate the WebDialer service.
Step 2	(Optional) Enable WebDialer Tracing, on page 3	To view WebDialer traces, enable tracing.
Step 3	(Optional) Configure WebDialer Servlet, on page 4	Configure the WebDialer servlet.
Step 4	(Optional) Configure Redirector Servlet, on page 4	If you have multi cluster applications that you develop using HTML over HTTPS interfaces, configure the Redirector servlet.
Step 5	(Optional) Configure WebDialer Application Server, on page 5	To configure Redirector for Cisco WebDialer.
Step 6	(Optional) To Configure Secure TLS Connection to CTI, on page 5, complete the following sub tasks: • Configure WDSecureSysUser Application User, on page 6 • Configure CAPF Profile • Configure Cisco WebDialer Web Service	WebDialer uses WDSecureSysUser application user credentials to establish a secure TLS connection to CTI to make calls. Follow these procedures if your system is running in mixed mode.
Step 7	Configure Language Locale for WebDialer , on page 8	Determine which language WebDialer displays by setting the locale field in the Cisco Unified Communications Self Care Portal menu.
Step 8	Configure WebDialer Alarms, on page 9	If there are any issues with the Web Dialer feature it alerts the administrator.
Step 9	(Optional) Configure Application Dial Rules, on page 9	If your application requires multiple clusters, configure application dial rules.
Step 10	Add Users to Standard CCM End User Group, on page 10	Add each WebDialer user to the Standard End User Group for Cisco Unified Communications Manager.
Step 11	(Optional) To Configure Proxy User, on page 10, complete the following sub tasks: • Add a WebDialer End User, on page 11 • Assign Authentication Proxy Rights, on page 11	If you use makeCallProxy HTML over HTTP interface to develop an application for using Cisco WebDialer, create a proxy user.

Activate WebDialer

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, check the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

Step 5 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to confirm that the CTI Manager service is active and is in start mode.

For WebDialer to function properly, the CTI Manager service must be active and in start mode.

What to do next

Configure Language Locale for WebDialer , on page 8 or complete any or all of the following optional tasks:

- Enable WebDialer Tracing, on page 3
- Configure WebDialer Servlet, on page 4
- Configure Redirector Servlet, on page 4
- Configure WebDialer Application Server, on page 5
- Configure Secure TLS Connection to CTI, on page 5

Enable WebDialer Tracing

To enable Cisco WebDialer tracing, use the Cisco Unified Serviceability Administration application. Trace settings apply to both the WebDialer and Redirector servlets. To collect traces, use the Real Time Monitoring Tool (RTMT).

To access the WebDialer trace files, use the following CLI commands:

- **file get activelog tomcat/logs/webdialer/log4j**
- **file get activelog tomcat/logs/redirector/log4j**

For more information about traces, see the *Cisco Unified Serviceability Administration Guide*.

Before you begin

Activate WebDialer, on page 3

Procedure

Step 1 From the navigation drop-down list of the Cisco Unified Communications Manager application, choose **Cisco Unified Serviceability** and then click **Go**.

Step 2 Choose **Trace** > **Configuration**.

Step 3 From the **Server** drop-down list, choose the server on which to enable tracing.

Step 4 From the **Service Group** drop-down list, choose CTI Services.

Step 5 From the **Service** drop-down list, choose the **Cisco WebDialer Web Service**.

Step 6 In the **Trace Configuration** window, change the trace settings according to your troubleshooting requirements.

Note For more information about WebDialer trace configuration settings, see the *Cisco Unified Serviceability Administration Guide*.

Step 7 Click **Save**.

Configure WebDialer Servlet

The WebDialer servlet is a Java servlet that allows Cisco Unified Communications Manager users in a specific cluster to make and complete calls.

Before you begin

Activate WebDialer, on page 3

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the Cisco Unified Communications Manager server on which to configure Cisco WebDialer web service parameters.

Step 3 From the **Service** drop-down list, choose **Cisco WebDialer Web Service.**

Step 4 Configure the relevant WebDialer Web Service parameters. For detailed information about the parameters, see online help.

Step 5 Restart the Cisco WebDialer Web Service for new parameter values to take effect.

Configure Redirector Servlet

The Redirector servlet is a Java-based Tomcat servlet. When a Cisco WebDialer user makes a request, the Redirector servlet looks for that request in the Cisco Unified Communications Manager cluster and redirects the request to the specific Cisco WebDialer server that is located in the Cisco Unified Communications Manager cluster. The Redirector servlet is available only for multi-cluster applications that are developed by using HTML over HTTPS interfaces.

Before you begin

Activate WebDialer, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the Cisco Unified Communications Manager server on which to configure the Redirector Servlet.

Step 3 From the **Service** drop-down list, choose the Cisco WebDialer Web Service.

Step 4 Configure the relevant WebDialer Web Service parameters. For detailed information about the parameters, see online help.

Step 5 Restart the Cisco WebDialer Web Service for new parameter values to take effect.

For more information on WebDialer Web Service, see the *Cisco Unified Serviceability Administration Guide*.

Configure WebDialer Application Server

Application server is required to configure the Redirector Servlet. Redirector is required only when you have multiple Unified Communications Manager servers configured in a cluster.

Before you begin

Activate WebDialer, on page 3

Procedure

Step 1 From Cisco Unified Communications Manager Administration Application server window, choose **System** > **Application Server**.

Step 2 From the **Application Server Type** drop-down list, choose a **Cisco WebDialer application server**.
The server appears in the **List of WebDialers** field in the **Service Parameter Configuration** window for the Cisco WebDialer Web Service.

Configure Secure TLS Connection to CTI

WebDialer uses WDSecureSysUser application user credentials to establish a secure TLS connection to CTI to make calls. To configure the WDSecureSysUser application user to establish a secure TLS connection, complete the following tasks.

Before you begin

- Install and configure the Cisco CTL Client. For more information about CTL Client, see Security Guide for Cisco Unified Communications Manager .

- Verify that the Cluster Security Mode in the Enterprise Parameters Configuration window is 1 (mixed mode). Operating the system in mixed mode impacts other security functions in your system. If your system is not currently running in mixed mode, do not switch to mixed mode until you understand these interactions. For more information, see Security Guide for Cisco Unified Communications Manager.
- Verify that the Cluster SIPOAuth Mode field is set to Enabled.
- Activate the Cisco Certificate Authority Proxy Function service on the first node.
- Activate WebDialer, on page 3

Procedure

	Command or Action	Purpose
Step 1	Configure WDSecureSysUser Application User, on page 6	Configure a WDSecureSysUser application user.
Step 2	Configure CAPF Profile	Configure a CAPF profile for the WDSecureSysUser application user.
Step 3	Configure Cisco WebDialer Web Service	Configure service parameters for the Cisco WebDialer Web service.

Configure WDSecureSysUser Application User

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Find**.

Step 3 From the **Find and List Application Users Application** window, choose **WDSecureSysUser**.

Step 4 Configure the fields in the **Application User Configuration** window and click **Save**.

What to do next

Configure CAPF Profile

Configure CAPF Profile

Certificate Authority Proxy Function (CAPF) is a component that performs tasks to issue and authenticate security certificates. When you create an application user CAPF profile, the profile uses the configuration details to open secure connections for the application.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User CAPF Profile**.

Step 2 Perform one of the following tasks:

- To add a new CAPF profile, click **Add New** in the **Find** window.
- To copy an existing profile, locate the appropriate profile and click the **Copy** icon for that record in the **Copy** column.

To update an existing entry, locate and display the appropriate profile.

Step 3 Configure or update the relevant CAPF profile fields. See the Related Topics section information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 Repeat the procedure for each application and end user that you want to use security.

CAPF Profile Settings

Setting	Description
Application User	From the drop-down list, choose the application user for the CAPF operation. This set This setting does not appear in the **End User CAPF Profile** window.
End User ID	From the drop-down list, choose the end user for the CAPF operation. This setting dis This setting does not appear in the **Application User CAPF Profile** window.
Instance ID	Enter 1 to 128 alphanumeric characters (a-z, A-Z, 0-9). The Instance ID identifies the You can configure multiple connections (instances) of an application. To secure the co instance that runs on the application PC (for end users) or server (for application users This field relates to the CAPF Profile Instance ID for Secure Connection to CTIMana
Certificate Operation	From the drop-down list, choose one of the following options: • **No Pending Operation**—This message is displayed when no certificate operatio • **Install/Upgrade**—This option installs a new certificate or upgrades an existing l
Authentication Mode	The authentication mode for the Install/Upgrade certificate operation specifies By Auth a locally significant certificate only when the user or administrator enters the CAPF a
Authentication String	To create your own authentication string, enter a unique string. Each string must contain 4 to 10 digits. To install or upgrade a locally significant certificate, the administrator must enter the auth This string supports one-time use only; after you use the string for the instance, you ca
Generate String	To automatically generate an authentication string, click this button. The 4- to10-digit
Key Size (bits)	From the drop-down list, choose the key size for the certificate. The default setting is Key generation, which is set at low priority, allows the application to function while t

Setting	Description
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which The values that are displayed apply for the first node. Use this setting with the **CAPF Operation Expires in (days)** enterprise parameter, which s must be completed. You can update this parameter at any time.
Certificate Operation Status	This field displays the progress of the certificate operation, such as pending, failed, or suc You cannot change the information that is displayed in this field.

Configure Cisco IP Manager Assistant

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server on which the Cisco WebDialer Web service is active.

Step 3 From the **Service** drop-down list, choose the **Cisco WebDialer Web** service.
A list of parameters appears.

Step 4 Navigate to and update the CTIManager Connection Security Flag and CAPF Profile Instance ID for Secure Connection to CTIManager parameters.

To view parameter descriptions, click the parameter name link.

Note CTIManager supports IPv4 and IPv6 addresses.

Step 5 Click **Save**.

Step 6 Repeat the procedure on each server on which the service is active.

What to do next

Refer to the Manager Assistant Task Flow for Shared Lines to determine the next task to complete.

Configure Language Locale for WebDialer

Use the Cisco Unified Communications Self Care Portal to configure a language locale for Cisco WebDialer. The default language is English.

Before you begin

Activate WebDialer, on page 3

Procedure

Step 1 From the Cisco Unified Communications Self Care Portal, click the **General Settings** tab.

Step 2 Click **Language**.

Step 3 From the **Display Language** drop-down list, select a language local, and then click **Save**.

Configure WebDialer Alarms

Cisco WebDialer service uses Cisco Tomcat to generate alarms.

Before you begin

Configure Language Locale for WebDialer , on page 8

Procedure

Step 1 From Cisco Unified Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the server on which to configure the alarm and then click **Go**.

Step 3 From the **Services Group** drop-down list, choose **Platform Services** and then click **Go**.

Step 4 From the **Services** drop-down list, choose **Cisco Tomcat** and then click **Go**.

Step 5 If your configuration supports clusters, check the **Apply to All Nodes** check box to apply the alarm configuration to all nodes in the cluster.

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

Note For more information about the Alarm configuration settings, see the *Cisco Unified Serviceability Guide*.

Step 7 Click **Save**.

What to do next

Add Users to Standard CCM End User Group, on page 10 or (optionally) if your application requires multiple clusters, see Configure Application Dial Rules, on page 9.

Configure Application Dial Rules

Before you begin

Configure WebDialer Alarms, on page 9

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Dial Rules** > **Application Dial Rules**.

Step 2 In the **Name** field, enter a name for the dial rule.

Step 3 In the **Description** field, enter a description for the dial rule.

Step 4 In the **Number Begins With** field, enter the initial digits of the directory numbers to which you want to apply this application dial rule.

Step 5 In the **Number of Digits** field, enter the length of the dialed numbers to which you want to apply this application dial rule.

Step 6 In the **Total Digits to be Removed** field, enter the number of digits that you want Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule.

Step 7 In the **Prefix With Pattern** field, enter the pattern to prepend to dialed numbers that apply to this application dial rule.

Step 8 For **Application Dial Rule Priority**, choose the dial rule priority as top, bottom, or middle.

Step 9 Click **Save**.

Add Users to Standard CCM End User Group

To use the Cisco WebDialer links in the User Directory windows in Unified Communications Manager, you must add each user to the Standard Unified Communications Manager End Users Group.

Procedure

Step 1 Choose **User Management** > **User Group**.

Step 2 In the **Find and List User Group** window, click **Find**.

Step 3 Click **Standard CCM End Users**.

Step 4 In the **User Group Configuration** window, click **Add End Users to Group**.

Step 5 In the **Find and List Users** window, click **Find**. You can enter criteria for a specific user.

Step 6 To add one or more users to the user group, complete one of the following steps:

- To add one or more users, check the check box beside each user to add and then click **Add Selected**.
- To add all users, click **Select All** and then click **Add Selected**.

The users appear in the Users in Group table of the **User Group Configuration** window.

Configure Proxy User

If you use makeCallProxy HTML over HTTP interface to develop an application for using Cisco WebDialer, create a proxy user. For information about the makeCallProxy interface, see the makeCallProxy section in the *Cisco WebDialer API Reference Guide*.

Note MakeCallProxy HTTP Methods is a service parameter under WebDialer Service. This parameter controls the HTTP methods that the MakeCallProxy API accepts. HTTP GET is considered insecure because the credentials required by the API are included as parameters in HTTP GET requests. Hence these HTTP GET parameters can be captured in the application logs and in the web browser's history.

When the service parameter MakeCallProxy HTTP Methods is set to Secure, request made by the HTTP GET will be rejected. By default the parameter MakeCallProxy HTTP Methods is set to Insecure, so that the API accepts both GET and POST methods and the backward compatibility is maintained.

Before you begin

Add Users to Standard CCM End User Group, on page 10

Procedure

	Command or Action	Purpose
Step 1	(Optional) Add a WebDialer End User, on page 11	Add a new user. If the user exists, you can proceed to the next task.
Step 2	Assign Authentication Proxy Rights, on page 11	Assign authentication proxy rights to an end user.

Add a WebDialer End User

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter a **Last Name**.

Step 4 Enter and confirm a **Password**.

Step 5 Enter and confirm a **PIN**.

Step 6 Complete any remaining fields in the **End User Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Assign Authentication Proxy Rights

Perform the following procedure to enable authentication proxy rights for an existing user.

Procedure

Step 1 Choose **User Management** > **User Group**.
The **Find and List User Group** window appears.

Step 2 Click **Find**.

Step 3 Click the **Standard EM Authentication Proxy Rights** link.
The **User Group Configuration** window appears.

Step 4 Click **Add End Users to Group**.
The **Find and List Users** window appears.

Step 5 Click **Find**. You can also add a criteria for a specific user.

Step 6 To assign proxy rights to one or more users, complete one of the following steps:

Step 7 To add a single user, select the user and then click **Add Selected**.

Step 8 To add all users that appear in the list, click **Select All** and then click **Add Selected**.
The user or users appear in the **Users in Group** table in the **User Group Configuration** window.

WebDialer Interactions

Feature	Interaction
Client Matter Codes (CMC)	When you use CMCs, you must enter the proper code at the tone; otherwise, the IP phone disconnects and the user receives a reorder tone.
Forced Authorization Codes (FAC)	When you use FACs, you must enter the proper code at the tone; otherwise, the IP phone disconnects and the user receives a reorder tone.
ApplicationDialRule table	Cisco WebDialer uses change notifications on the ApplicationDialRule database table to track and use updated dial rules.
Client Matter Codes and Forced Authorization Codes	Web Dialer supports CMCs and FACs in the following ways: • A user can enter the destination number in the dial text box of the WD HTML page or SOAP request, and then manually enter the CMC or FAC on the phone. • A user can enter the destination number followed by the FAC or CMC in the dial text box of the WD HTML page or SOAP request. For example, if the destination number is 5555, the FAC is 111, and the CMC is 222, a user can make a call by dialing 5555111# (FAC), 5555222# (CMC), or 5555111222# (CMC and FAC). **Note** • WebDialer does not handle any validation for the destination number. The phone handles the required validation. • If a user does not provide a code or provides the wrong code, the call will fail. • If a user makes a call from the WebApp with a DN that contains special characters, the call goes successfully after stripping the special characters. The same rules do not work in SOAP UI.

WebDialer Restrictions

Feature	Restrictions
Phones	Cisco WebDialer supports phones that run Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) that Cisco Computer Telephony Integration (CTI) supports. **Note** Few older phone models do not support Cisco Web Dialer that run SIP.

WebDialer Troubleshooting

Authentication Error

Problem

Cisco WebDialer displays the following message:

Authentication failed, please try again.

Possible Cause

User entered wrong user ID or password.

Solution

Ensure that you use your Unified Communications ManagerCisco Unified Communications Manager user ID and password to log in.

Service Temporarily Unavailable

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later.

Possible Cause

The Cisco CallManager service became overloaded because it has reached its throttling limit of three concurrent CTI sessions.

Solution

After a short time, retry your connection.

Directory Service Down

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later: Directory service down.

Possible Cause

The Cisco Communications Manager directory service may be down.

Solution

After a short time, retry your connection.

Cisco CTIManager Down

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later: Cisco CTIManager down.

Possible Cause

Cisco CTIManager service that is configured for Cisco Web Dialer went down.

Solution

After a short time, retry your connection.

Session Expired, Please Login Again

Problem

Cisco WebDialer displays the following message:

Session expired, please login again.

Possible Cause

A Cisco Web Dialer session expires:

- After the WebDialer servlet gets configured
- If the Cisco Tomcat Service is restarted.

Solution

Log in by using your Unified Communications Manager User ID and Password.

User Not Logged In on Any Device

Problem

Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

The user chooses to use Cisco Extension Mobility from the Cisco WebDialer preference window but does not get log in to any IP phone.

Solution

- Log in to a phone before using Cisco WebDialer.
- Choose a device from the Cisco WebDialer preference list in the dialog box instead of choosing the option **Use Extension Mobility**.

Failed to Open Device/Line

Problem

After a user attempts to make a call, Cisco WebDialer displays the following message:

User not logged in on any device.

Possible Cause

- The user chose a Cisco Unified IP Phone that is not registered with Unified Communications Manager. For example, the user chooses a Cisco IP SoftPhone as the preferred device before starting the application.
- The user who has a new phone chooses an old phone that is no longer in service.

Solution

Choose a phone that is in service and is registered with Unified Communications Manager.

Destination Not Reachable

Problem

Cisco WebDialer displays the following message on the End Call window:

Destination not reachable.

Possible Cause

- User dialed the wrong number.
- The correct dial rules did not get applied. For example, the user dials 5550100 instead of 95550100.

Solution

Check the dial rules.