Oracle B2C Service

Implementing Standalone Cobrowse

20B
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></td>
<td>i</td>
</tr>
<tr>
<td><strong>1 Cobrowse Overview</strong></td>
<td>1</td>
</tr>
<tr>
<td>Overview of Cobrowse</td>
<td>1</td>
</tr>
<tr>
<td>How Cobrowsing Differs from Screen Sharing</td>
<td>1</td>
</tr>
<tr>
<td>Cobrowse Terminology</td>
<td>2</td>
</tr>
<tr>
<td>Cobrowse Modes</td>
<td>2</td>
</tr>
<tr>
<td>How Instant Mode (ICB) Works</td>
<td>3</td>
</tr>
<tr>
<td>How Advanced Mode (ACB) Works</td>
<td>4</td>
</tr>
<tr>
<td>Considerations for Cobrowse Deployment</td>
<td>5</td>
</tr>
<tr>
<td><strong>2 Admin Console</strong></td>
<td>7</td>
</tr>
<tr>
<td>Cobrowse Admin Console</td>
<td>7</td>
</tr>
<tr>
<td>Log In to the Admin Console</td>
<td>7</td>
</tr>
<tr>
<td><strong>3 Working with Companies</strong></td>
<td>9</td>
</tr>
<tr>
<td>Select a Company</td>
<td>9</td>
</tr>
<tr>
<td>Create a New Company</td>
<td>9</td>
</tr>
<tr>
<td>Edit a Company</td>
<td>10</td>
</tr>
<tr>
<td><strong>4 Permissions</strong></td>
<td>11</td>
</tr>
<tr>
<td>Permissions</td>
<td>11</td>
</tr>
<tr>
<td><strong>5 Managing Users</strong></td>
<td>13</td>
</tr>
<tr>
<td>How You Manage Users</td>
<td>13</td>
</tr>
<tr>
<td>Edit My Profile</td>
<td>13</td>
</tr>
<tr>
<td>Edit a User</td>
<td>14</td>
</tr>
<tr>
<td>Add a User</td>
<td>16</td>
</tr>
<tr>
<td>Bulk Add Users</td>
<td>17</td>
</tr>
<tr>
<td><strong>6 Using Single Sign-On</strong></td>
<td>21</td>
</tr>
<tr>
<td>Single Sign-On (SSO)</td>
<td>21</td>
</tr>
</tbody>
</table>
7 Managing SiteIDs

SiteIDs
Add a New SiteID
Edit a SiteID

8 Assigning an Implementation Consultant

Overview of the Implementation Consultant Role
Assign an Implementation Consultant to Your Company
Unassign an Implementation Consultant from Your Company

9 Configuring the Cobrowse UI

Cobrowse UI Configuration
Select the UI Theme and Language
Design the Launch Button
Customize Text for Job Access with Speech (JAWS) Software
Make Additional UI Customizations
Save UI Customization Changes
Restore the Default UI

10 Managing Agent Controls

Agent Controls

11 Creating Configuration Files for Privacy and Security

Configuration Files for Privacy and Security
Configure Page Masking
Block a Field
Masking and Blocking Configuration Variable Summary
Configure IP Address Restrictions

12 Configuring Surveys

Display a Link to a Post-Cobrowse Survey

13 Configuring Your Company Deployment

Configure Your Company Deployment
Best Practices for Launch Point Design
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Using Integrated Cobrowse</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>How You Use Cobrowse with an Oracle Agent Desktop</td>
<td>61</td>
</tr>
<tr>
<td>15</td>
<td>Adding the In-App SDK</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Download the SDKs</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>In-App SDK for iOS</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>In-App SDK for Android</td>
<td>67</td>
</tr>
<tr>
<td>16</td>
<td>Using Cobrowse on Mobile Devices</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>Special Considerations for Using Cobrowse on Mobile Devices</td>
<td>69</td>
</tr>
<tr>
<td>17</td>
<td>Cobrowse Agent Training</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Best Practices for Cobrowse Agent Training</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Log In to the Agent Console</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Launch a Cobrowse Session</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>How You Cobrowse with a Customer</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Escalate to Advanced Mode</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>End a Cobrowse Session</td>
<td>74</td>
</tr>
<tr>
<td>18</td>
<td>Working with Reports</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Work with Reports</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Use an ExtKey Code</td>
<td>75</td>
</tr>
<tr>
<td>19</td>
<td>Viewing Statistical Data</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>View Statistical Data</td>
<td>77</td>
</tr>
<tr>
<td>20</td>
<td>Troubleshooting</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting Tips</td>
<td>79</td>
</tr>
<tr>
<td>21</td>
<td>Accessibility and Support</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Cobrowse Accessibility</td>
<td>81</td>
</tr>
</tbody>
</table>
Preface

This preface introduces information sources that can help you use the application and this guide.

Using Oracle Applications

To find guides for Oracle Applications, go to the Oracle Help Center Documentation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit Oracle's Accessibility Program at https://www.oracle.com/corporate/accessibility/.

Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Contacting Oracle

Access to Oracle Support

Customers can access electronic support through Oracle Support. For information, visit https://cx.rightnow.com/app/landing/get_started_support or visit https://www.oracle.com/corporate/accessibility/learning-support.html if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides. You can complete one of the following surveys:

- For guides: Oracle Service Cloud - Documentation Feedback.
- For tutorials: Oracle Service Cloud - Tutorial Feedback.
1 Cobrowse Overview

Overview of Cobrowse

Oracle Cobrowse Cloud Service (Cobrowse) is a collaboration tool that can be used during voice or chat interactions to enable an organization representative to see the screen of the customer that the representative is interacting with in realtime.

Cobrowse lets agents better understand a customer’s question or problem, and provide faster and more accurate help, leading to better resolutions and more satisfied customers. Today, more and more businesses are moving processes and critical business applications to the web. Many large organizations have multiple customer-facing websites and mobile applications to serve different audiences and business segments. All too often, customers and end-users get lost in complicated websites and grow frustrated or just give up. This can have a negative impact on customer satisfaction, adoption of the internet channel, and the ability to profitably serve customers.

Ensuring success of end-users on web platforms has become critical to business success, and so collaborative tools such as cobrowsing software have become must-haves. Cobrowsing is used to engage customers online and provide real-time assisted service or guidance when necessary, which increases customer satisfaction and online conversions. In many cases, a customer and an agent can resolve an issue more quickly, with a greater level of understanding and satisfaction, by viewing the same content at the same time. Cobrowsing is an indispensable sales conversion and customer support tool that drives business objectives as well as revenue. This document covers the end-to-end deployment process and the most effective best practices to consider when planning, deploying, and using Cobrowse, along with ways to measure its success.

Oracle provides Cobrowse as both a standalone solution as well as an integrated feature of other Oracle products.

How Cobrowsing Differs from Screen Sharing

While these terms can often be used interchangeably, in a business setting there is an important difference between screen sharing technology and cobrowsing technology, which comes down to the use case for which each is used.

- **Screen Sharing**—A web collaboration session where one person lets one or more other people view their computer screen. In business, the screen is typically shared by the sales or customer service agent who invites a customer to view an online demo, presentation, or web service. The “sharer” or “host” is the party that holds the license to use the screen sharing tool and is responsible for starting a sharing session.

- **Cobrowsing**—A screen sharing session that the customer initiates, where a sales or customer service agent can see the customer's screen and can provide guidance and insights with regard to what the customer is doing or seeing. In this case the “sharer” or “host” is the customer, but the license to use the cobrowsing tool is held by the company or agent. The customer doesn't have to sign up, download, or do anything other than click a button to start a session.
Cobrowse Terminology

Cobrowse uses this terminology.

- **Instant Cobrowse mode (ICB)**—The mode Cobrowse typically launches in, using HTML-based cobrowsing technology and running in the browser.
- **Advanced Cobrowse mode (ACB)**—The mode Cobrowse can switch to that allows cobrowsing outside of the browser or viewing more advanced, rich web technologies in the browser.
- **TrueView**—The Cobrowse option that lets agents switch views to perfectly match the browser size and configuration of the customer.
- **Agent Console**—The interface agents use to start and run a Cobrowse session.
- **Admin Console**—The interface Cobrowse administrators use to manage the Cobrowse product, including configuration panels and reporting.
- **In-App Cobrowse**—The Cobrowse option that can be built into a native mobile application.

### Cobrowse Modes

You can Cobrowse using one of two different technology approaches. The first approach uses HTML and the second uses screen sharing. Cobrowse combines both technology approaches with two modes.

**Instant Cobrowse (ICB): Fastest connection**—Cobrowse makes the initial connection between a customer and agent in Instant Cobrowse Mode. The launch time is typically less than 10 seconds to connect. ICB mode lets agents cobrowse with customers who are viewing web content on pages where the company has placed Cobrowse launcher script.

**Advanced Cobrowse (ACB): Greatest coverage**—Agents can escalate to Advanced Cobrowse Mode from within an active session that was started in ICB mode. Occasionally sessions will start directly in ACB mode if ICB mode is not supported. ACB mode lets agents cobrowse content outside of the company’s domain, including third party websites and desktop applications. ACB mode utilizes browser plug-ins and may require that a customer accept a certificate or download an executable. This process is described in detail later in this document.

You select Cobrowse modes when you configure your company deployment. See [Configure Your Company Deployment](#).

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Instant Cobrowse Mode (ICB)</th>
<th>Advanced Cobrowse Mode (ACB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect in less than 10 seconds</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Available to customers using a mobile browser</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cobrowse the company’s web pages</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Available when rich media present on web page (for example, Flash or Silverlight)</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cobrowse third-party sites (for example, partner or resource websites)</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
A Cobrowse session flow may follow this path.

In this example, at the point in the conversation where the agent needs to cobrowse content that is not browser-based, the session would cease supporting the interaction in a typical industry-standard scenario. However, with Cobrowse this agent has the option to switch to ACB mode for greater functionality, supporting the customer's need to cobrowse a document, settings window, or third-party website.

It's important to note that while switching to ACB mode lets you cobrowse documents, applications, and third-party sites, the company controls exactly what is visible to agents with their configuration of Cobrowse. So, it does not simply open up the customer's desktop for the agent to view because only approved websites, domains, and applications will be visible.

Note: ICB mode is not supported on some browsers. In these cases, Cobrowse will launch in ACB mode.

Related Topics
• Configure Your Company Deployment

How Instant Mode (ICB) Works

Cobrowse typically launches in ICB mode.

ICB mode requires a Cobrowse launcher script to be present on all web pages that will be cobrowsed, typically by placing the Cobrowse launcher script on the global header of the organization's website. For Integrated Cobrowse, this is
accomplished within the Oracle RightNow Customer Portal Cloud Service (Customer Portal) by using and editing various widgets.

Only website content tagged with the Cobrowse launcher script can be viewed by the agent when cobrowsing in ICB mode. For any content that includes sensitive customer data, the Cobrowse script can be configured to prevent the agent from viewing these pages. Additionally, field blocking can be applied to prevent viewing sensitive form fields during a cobrowse session, such as credit card numbers or social security numbers.

Here is how ICB mode connects and runs.

1. The Cobrowse engine uses JavaScript to collect a URL and page contents (including dynamic content like windows, options, and check boxes) and send data to the grid server through a secure websocket connection.
2. The agent's browser retrieves data through the same secure websocket connection and renders the content in HTML on a web page.
3. Ongoing data is captured and sent, including mouse moves, clicks, and keyboard events.

How Advanced Mode (ACB) Works

Agents can escalate to ACB mode if they need to access extended capabilities to continue serving the customer during a cobrowse interaction.

Here is how ACB mode connects and runs.

1. The agent clicks the Advanced Cobrowse mode button within the agent desktop.
2. The customer agrees to activate ACB mode.
3. The main server assigns the ACB mode to a grid server.
4. The grid server conducts the cobrowse session between the agent and customer.

ACB mode launches and runs using one of three technologies, depending on the customer's environment.

- **Option 1**—ACB mode using the Microsoft® .NET Framework.
  - This is the most commonly used technology and it is used with browsers that support the Click-Once installer (for example, Internet Explorer always supports ClickOnce).
  - The customer clicks Run.
  - No executable file is needed because the customer can simply use existing browser components to start ACB mode.

- **Option 2**—ACB mode using Java.
  - If the customer's browser supports Java, it can be used to launch ACB mode.
  - Certain browsers may require the customer to click Run this Time in a separate window to activate Java.
  - After Java is activated, a Java Security window may open where the customer must click Run to verify security of the Cobrowse application.
  - No executable file is needed.

- **Option 3**—ACB mode using an alternative .NET Framework launcher.
  - This mode is used when the browser does not support the Click-Once installer or Java.
  - This is an executable file that is downloaded.
The executable file substitutes for the Click-Once installer to launch the .NET Framework.
The security benefits from using a .NET component within the browser are preserved because the
functionality that pertains to screen sharing does not reside within the executable file.

Considerations for Cobrowse Deployment

Before starting the configuration and deployment of Cobrowse, it's important to thoroughly consider and document
your use cases.

Many of your user interface (UI) and security configuration decisions will be made with these specific use cases in mind.
Get input and feedback from all of your stakeholders so there is agreement across the business on how Cobrowse is
intended to be used.

Questions to ask.

- Who will be cobrowsing with whom?
  - What customer segment(s)?
  - What agents in which contact centers?
- What will they need to look at together on the screen?
  - Websites?
  - Desktop applications?
  - Mobile applications?
- What should agents be able to do on the customer's screen?
  - View and point?
  - Click and type?
- Should all agents have the same permissions?
- Are there any web pages where agents should not be able to click or type, even if they have these permissions
  elsewhere?
2 Admin Console

Cobrowse Admin Console

The Cobrowse Admin Console is a standalone user interface used to manage Cobrowse, to customize the user interface and configure its deployment, to add and edit users, and to access Cobrowse reports.

You can set up your organization’s administrators and administrator-type roles to have different permissions within the Admin Console system.

The following Admin Console functionality is available for Configuration Administrators.

- User management.
  - Add, edit, and delete users, including bulk add users.
  - Search users in the assigned companies, and any sub-companies of those.
  - Edit their own profile.

- Company management.
  - Add, edit, and delete sub-companies.
  - Search in all assigned companies.

- Product management.
  - Cobrowse customization, configuration and masking.

- Reporting access to user, company and audit reports.
- Survey configuration.
- SiteID configuration.

Log In to the Admin Console

The Cobrowse Admin Console is a standalone user interface used to manage Cobrowse, letting administrators add and edit users, manage sub-companies, and access Cobrowse reports.

1. Go to Oracle Digital Engagement Channels Administrative Console Login.
2. Enter your login and password.
   - The Welcome screen of the Admin Console opens. You may occasionally see notifications of upcoming events or other important information from Oracle on this screen.
# 3 Working with Companies

## Select a Company

Select the company you want to work with.

When logged in, you are automatically placed into your top-level company. If your company has sub-companies set up, you can use the Select Company tab to work in a different company. For example, you may want to manage multiple deployments across geographic regions or product lines.

1. Click **Select Company**.
   - A search window opens with your top-level company name highlighted in the list of companies.
2. To select a sub-company, click the plus sign (+) next to a company to view all sub-companies and highlight your selection.
3. To search for a company, select the search criteria from the drop-down menu next to the Search field. Your search options are Company Name, Company ID, SiteID, Customer Account #, and Subscription ID.
   - To search by company name, enter at least 3 characters of the company name and press Enter. You can use an asterisk (*) wildcard to match any characters.
   - To search by ID number, enter the first six digits of the company ID and press Enter.
   - To search by SiteID, enter the first four digits and press Enter.

## Create a New Company

Follow this procedure to create a new company.

1. Click **Company Set Up**.
2. Click **Company Management**.
   - The **Company Management** window opens.
3. Click **Create New Company**.
4. Enter field information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Company/Department Name</td>
<td>Enter the company or department name.</td>
</tr>
<tr>
<td>*Company URL</td>
<td>Enter the company URL.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The expiration date is set automatically and cannot be edited.</td>
</tr>
<tr>
<td>Account Type</td>
<td>Click this drop-down menu to select an account type. Options are Free Trial, Paid Account, or Canceled Account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote Options</td>
<td>Click this drop-down menu to select remote options. Remote options define an agent’s control over a customer’s mouse and keyboard.</td>
</tr>
<tr>
<td>View and Point</td>
<td>With this option selected, agents can select from three options.</td>
</tr>
<tr>
<td></td>
<td>◦ View Only to view the active window (this option is selected by default in Advanced mode)</td>
</tr>
<tr>
<td></td>
<td>◦ View + Pointer to view the customer’s active window and use a labeled mouse as a pointing device on the customer’s screen (this option is selected by default in Instant mode)</td>
</tr>
<tr>
<td></td>
<td>◦ View + True Pointer to view the customer’s desktop and control the movement of the customer’s mouse or other pointing device (only available in Advanced mode)</td>
</tr>
<tr>
<td>Remote Control</td>
<td>With this option selected, agents can select from four options.</td>
</tr>
<tr>
<td></td>
<td>◦ View Only to view the active window (this option is selected by default in Advanced mode)</td>
</tr>
<tr>
<td></td>
<td>◦ View + Pointer to view the customer’s active window and use a labeled mouse as a pointing device on the customer’s screen (this option is selected by default in Instant mode)</td>
</tr>
<tr>
<td></td>
<td>◦ View + True Pointer to view the customer’s desktop and control the movement of the customer’s mouse or other pointing device (only available in Advanced mode)</td>
</tr>
<tr>
<td></td>
<td>◦ Full Control to view the customer’s active window, control all mouse or other pointing device functions (pointer and mouse clicks), navigate to other company web pages, use their keyboard to enter information on the customer’s active window and, in Advanced mode, access the customer’s desktop and cobrowse third party sites</td>
</tr>
<tr>
<td>Number of Seats</td>
<td>Enter the number of seats for the company.</td>
</tr>
<tr>
<td>Create In Root</td>
<td>Select this check box to create the company as a new top-level company.</td>
</tr>
</tbody>
</table>

**Edit a Company**

Follow this procedure to make changes to a company.

1. Click **Company Set Up**.
2. Click **Company Management**.
3. Click **Edit** for the company you want to edit.
   
   An edit window opens.
4. Make any changes and click **Save**.
4 Permissions

Permissions

Permissions control access to the Administrative Console. There are four predefined permission groups for every new company. These groups cannot be edited or deleted.

- **Users**—Have access to session reports and can change personal information.

- **Account Managers**—Have all permissions available to the Users group and has read-only access to administrative functionality available to administrator groups.

- **Account Administrators**—Have all permissions available to the Account Managers group and can manage companies and users. Account Administrators can add users to any permission group, including Account Administrators and Configuration Administrators.

- **Configuration Administrators**—Have the highest permission level with all permissions available to the Account Administrators group, plus can configure Cobrowse deployment. This permission can be assigned to an internal or external resource for configuration and implementation of the company's Cobrowse deployment. Configuration Administrators can add users to any permission group, including Configuration Administrators.
Managing Users

How You Manage Users

Manage users with the functions in the User Set Up tab. You can edit your own user information, add and edit users, and set permissions.

Note: This section is specific to Standalone Cobrowse. For Cobrowse added on to an Oracle platform (Oracle Service Cloud or B2B Service), see product documentation for the agent desktop to learn more about user management.

The My Profile page contains your information. This page shows the same user data regardless of the company or sub-company selected. You can change the following information on the My Profile page:

- First name
- Last name
- Contact information
- Password

The User Management page contains user information for the currently selected company. You can do the following on the User Management page:

- Search for users
- Add new users
- Edit users
- Delete users

The Permissions page lists the permission groups for your company. Every company has four predefined permission groups.

Edit My Profile

Follow this procedure to edit your profile on the My Profile page.

1. Click User Set Up.
2. Click My Profile.
   The My Profile window opens.
3. Edit field information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company/Department Name</td>
<td>Your top-level company appears and cannot be edited here.</td>
</tr>
</tbody>
</table>
Edit a User

Follow this procedure to edit a user.

Before editing a user, you must select the company of the user.

1. Click **User Set Up**.
2. Click **User Management**.
   The **User Management** window opens.
3. Search for the user by entering information in the search fields and clicking **Apply Filter**, or by clicking on the sort arrows next to the user fields.
4. Click **Edit** on the user’s row.
5. Edit field information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company/Department Name</strong></td>
<td>The company you are working with appears and cannot be edited here.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Login Type</strong></td>
<td>Login type is Reg by default for an administrator, though if your company is configured for Single Sign-On (SSO) then the SSO option is selected.</td>
</tr>
<tr>
<td><strong>Reg</strong></td>
<td>The Reg login is the default login type.</td>
</tr>
<tr>
<td><strong>SSO</strong></td>
<td>SSO agents are set up with the SSO login type as new users and log in with an SSO.</td>
</tr>
<tr>
<td><strong>First Name</strong></td>
<td>Enter the user's first name. This is a required field.</td>
</tr>
<tr>
<td><strong>Last Name</strong></td>
<td>Enter the user's last name. This is a required field.</td>
</tr>
<tr>
<td>**Contact phone</td>
<td>Ext**</td>
</tr>
<tr>
<td><strong>Login (Email)</strong></td>
<td>Enter the user's email.</td>
</tr>
<tr>
<td></td>
<td>This field only appears with the Reg login type. Login (Email) is unique within the database, so no two Reg users can have the same login (email) even if they are under different companies.</td>
</tr>
<tr>
<td><strong>Login</strong></td>
<td>Enter an alphanumeric login for the user.</td>
</tr>
<tr>
<td></td>
<td>This field only appears with the SSO login type. The login must be unique to the company.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>Enter an email for the user.</td>
</tr>
<tr>
<td></td>
<td>This field only appears with the SSO login type. SSO allows for multiple instances of the same email address.</td>
</tr>
<tr>
<td><strong>Enter New Password</strong></td>
<td>To create a new password, enter it in this field.</td>
</tr>
<tr>
<td></td>
<td>This field only appears with the Reg login type.</td>
</tr>
<tr>
<td><strong>Re-type New Password</strong></td>
<td>Re-enter the new password.</td>
</tr>
<tr>
<td></td>
<td>This field only appears with the Reg login type.</td>
</tr>
<tr>
<td><strong>Permissions Group</strong></td>
<td>Select a permissions group for the user.</td>
</tr>
</tbody>
</table>
Implementing Standalone Cobrowse

Chapter 5
Managing Users

### Add a User

Create new users and the information associated with them.

Before adding a user, you must select the user’s company.

1. Click **User Set Up**.
2. Click **User Management**.
   - The **User Management** window opens.
3. To add a new user profile, click **Add New User**.
4. Edit field information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company/Department Name</strong></td>
<td>The company you are working with appears and cannot be edited here.</td>
</tr>
<tr>
<td><strong>Login Type</strong></td>
<td>Login type is Reg by default, though if the company is configured for Single Sign-On (SSO), then the SSO option is enabled.</td>
</tr>
<tr>
<td><strong>Reg</strong></td>
<td>The Reg login is the default login type.</td>
</tr>
<tr>
<td><strong>SSO</strong></td>
<td>Select this login type if SSO is enabled, and you want the agent to log in with an SSO.</td>
</tr>
<tr>
<td><strong>First Name</strong></td>
<td>Enter the user’s first name. This is a required field.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Last Name** | Enter the user's last name. This is a required field.
**Contact phone|Ext** | Enter the user's contact phone information.
**Login (Email)** | Enter the user's email. This field only appears with the Reg login type. Login (Email) is unique within the database, so no two Reg users can have the same login (email) even if they are under different companies.
**Login** | Enter an alphanumeric login for the user. This field only appears with the SSO login type. The login must be unique to the company.
**Email** | Enter an email for the user. This field only appears with the SSO login type. SSO allows for multiple instances of the same email address.
**Permissions Group** | Select a permissions group for the user. This field only appears with the Reg login type. All SSO users are assigned the User permission group automatically.

5. **Click Add.**

An email confirmation is sent to a Login type Reg user with a temporary password and instructions on how to change it. Login type SSO users do not receive an email.

**Note:** If a user's password is lost, they can request a password reset by visiting LiveLOOK Forgot Password.

**Related Topics**
- Permissions
- Select a Company

---

### Bulk Add Users

Follow this procedure to add multiple users to a company.

1. **Click User Set Up.**
2. Click **User Management**.
The **User Management** window opens.

3. Click **Bulk add user**.

4. Enter field information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Type</td>
<td>Login type is Reg by default, though if the company is configured for Single Sign-On (SSO), then the SSO option is enabled.</td>
</tr>
<tr>
<td>Reg</td>
<td>The Reg login is the default login type.</td>
</tr>
<tr>
<td>SSO</td>
<td>Select this login type if SSO is enabled, and you want the agent to login with a SSO. All SSO users are Cobrowse Agents only.</td>
</tr>
<tr>
<td>Password</td>
<td>Leave this field blank so users can obtain passwords themselves through <strong>LiveLOOK Forgot Password</strong>, or enter a single password for the users. Users added through bulk adding do not receive an email to change their passwords. This field only appears with the Reg login type.</td>
</tr>
</tbody>
</table>

5. Click **Create Request**.
The bulk add request appears in the request table.

6. Click **Upload/View** of the request row.

7. Click **Choose File** to select the user data file to upload.
The file must be:
   - Tab delimited
   - UTF8 encoded to support special characters in names
   - Contains a header in the first line that reads FirstName LastName Login/Email PhoneNum PhoneExt. The PhoneNum and PhoneExt fields are optional.

8. Click **Upload File**.
A table with the added user records appears. If a user already exists in the database, the line status will read **Login Exists in DB**, otherwise the line status will read **Inserted**.

9. Click **Add Users** to confirm the upload.
Only the person who created the request can perform the bulk add.
The Request table appears. The bulk add request has a Done status, and a message appears indicating how many users were successfully added.

Related Topics
- Permissions
6 Using Single Sign-On

Single Sign-On (SSO)

Oracle Standalone Cobrowse supports acceptance of a SAML 2.0 compliant ID federation. This permits use of an internal standard login and password to access the Cobrowse application.

It is assumed that access authorization will be managed and SAML ID federation permitted only after the user is authorized. This eliminates any need to maintain a list of authorized users in the Oracle Standalone Cobrowse environment.

The process for configuring Single Sign-On (SSO) is as follows:

1. Submit a Service Request for SSO and provide the primary Company Name and CompanyID as it appears in the Cobrowse application.
2. Having this information, Oracle will provide our SP metadata (SPID and Consumption URL) that should be communicated to your ADFS team.
   - Cobrowse uses Oracle OpenSSO Fedlet to process SAML2.0 assertion.
   - Our assumption is that both authentication and authorization to use Cobrowse is done on the company’s side. In other words, if the Cobrowse SSO application gets a valid assertion we assume that this user is authorized to use CoBrowse.
   - Accounts for any new agents will be auto-provisioned in the Oracle Cobrowse application. For auto-provisioning we can support follow parameters:
     - First Name
     - Last Name
     - Email
   - We collect these parameters from the ATTRIBUTES section of the SSO assertion. To have them configured, we need exact names for assertion ATTRIBUTES that have values for the Agent’s First Name, Last Name, and Email. All these values are optional and default values will be used if not passed.
   - There is one more ATTRIBUTE we can handle – Division Name. If this attribute is passed in assertion then we can auto-provision a new Agent under this particular Sub-Company/Division. If it is not passed then all Agents will be auto-provisioned under a default sub-company/division. For example “SSO Agent Accounts.”
3. To configure the SSO application we will need your “IDP metadata” file. Your Active Directory Federation Services (ADFS) team should be able to provide this file. In addition we need confirmation of the exact names for assertion ATTRIBUTES to be used.
4. After the SSO application is configured on our side, you can test, with help from your ADFS team if needed.
7 Managing SiteIDs

SiteIDs

A SiteID is an alpha numeric key that uniquely identifies the Cobrowse product’s appearance and behavior when deployed on a website, including the visual presentation of buttons, links, and text during a session; and security features such as page blocking and field masking.

All Cobrowse product configuration and customization is linked to a specific SiteID. For all configuration or customization pages in the Admin Console, the SiteID selection box is present in the upper right corner of the page. It is very important to ensure that the correct SiteID is selected when performing configuration and customization of the product. Only one SiteID can be defined for any single Oracle Service Cloud integrated deployment. The following functionality is available on the SiteID Management page:

- Add a New SiteID
- Edit a SiteID

Add a New SiteID

Site IDs are added at the company level, and are applied to all of the subcompanies in that company.

1. Click Configurations.
2. Click SiteID Management.
   The SiteID Management window opens.
3. Click Add New Site ID.
   The New Site ID form appears.
4. Select a country from the drop-down menu.
5. Enter a title for the Site ID.
6. Enter any notes.
7. Click Save.
   A new SiteID is created and the Deployment Instructions window opens.

Edit a SiteID

Follow this procedure to edit an existing SiteID.

1. Click Configurations.
2. Click SiteID Management.
   The SiteID Management window opens.
3. Click the Edit button on the row of the SiteID you want to edit.
   The Edit SiteID window opens.
4. Enter your edits.
5. Click **Save**.
Assigning an Implementation Consultant

Overview of the Implementation Consultant Role

Implementation Consultants are external, third-party consultants you can hire to configure your Cobrowse instance. Unlike other users, Implementation Consultants can be assigned to configure multiple companies at the same time.

An Implementation Consultant assigned to at least one company can perform the same functions as a Configuration Administrator. In addition, Implementation Consultants can select a company to manage from their list of assigned companies and search all companies to find companies they are assigned to.

Note: When an Implementation Consultant logs in to the Admin Console, the company he or she was most recently assigned to opens as the default. The Implementation Consultant can use the Select Company tab to select any assigned company to work with. If an Implementation Consultant has no assigned companies and logs in to the Admin Console, only the Implementation Consultant's own user profile and user reports are available.

Assign an Implementation Consultant to Your Company

An Implementation Consultant must be assigned to your company to have access to your company's configuration.

Implementation Consultants can only be assigned by Configuration Administrators. Implementation Consultants are assigned at the root company level, but can manage all sub-companies.

Note: You may not assign an existing company user to the role of Implementation Consultant. You can add a new user as an Implementation Consultant, or assign an Implementation Consultant that already exists in the Oracle system to your company.

1. Click User Set Up.
2. Click Manage External Access.
   A table displays the names of any Implementation Consultants already assigned to your company.
3. Enter the email address of the Implementation Consultant you want to assign in the text box.
4. Click Add.
   If the email address matches an Implementation Consultant already in the Oracle system, the page reloads with the name of the Implementation Consultant in the list of those assigned to your company. If the email address doesn't match an Implementation Consultant in the Oracle system, the page reloads to create a new Implementation Consultant user.
5. To create a new Implementation Consultant, enter the first and last names of the new Implementation Consultant in the appropriate text boxes, and click Add.
   An email is sent to the new Implementation Consultant with a temporary password. The page reloads with the name of the Implementation Consultant in the list of those assigned to your company.
Unassign an Implementation Consultant from Your Company

You can unassign an Implementation Consultant from your company.

You cannot delete an Implementation Consultant from the Oracle system, but you can unassign one from your company.

1. Click User Set Up.
2. Click Manage External Access.
   A table displays the names of all Implementation Consultants assigned to your company.
3. Locate the Implementation Consultant you wish to unassign from the displayed table, and click the Delete icon in that row.
   A confirmation message displays.
4. Click OK.
   A confirmation message displays and the name of the Implementation Consultant is removed from the table.
Chapter 9 Configuring the Cobrowse UI

Cobrowse UI Configuration

Many customers are still new to the idea of sharing a screen with an agent during a service interaction, and a well designed user interface (UI) will ensure a positive experience at each step of the process.

You may keep the default UI, but proper configuration of the full set of UI elements will enable:

- A brand-aligned customer experience
- Presentation of crucial information like phone numbers or other instructions
- Presentation of important terms and conditions

Before configuring a UI, select the company you want to work with. When a new SiteID has been created, it will be automatically selected.

The Deployment Instructions button is available on every configuration window.

Related Topics
- Select a Company

Select the UI Theme and Language

Follow this procedure to select a theme and language for the UI.

Always choose a theme and language before making customizations to the UI associated with the SiteID you are working with. Changing between themes resets the entire configuration. Changing the language associated with a UI design will result in the loss of any changes to font colors, loaded images, and custom button orientations, as the UI will revert to the default state for the newly chosen language.

1. Click Products.
2. Click Cobrowse.
3. Click UI Customization.
   - The UI Customization window opens.
4. Select a black or white Theme from the drop-down menu.
   - Themes define the color of buttons and windows within a Cobrowse session. The black theme is designed to work well on websites that use light color palettes, ensuring that the Cobrowse launch button shows clearly against the site background. Alternatively, the white theme is designed for use on websites using a dark color palette.
5. Select a language from the drop-down menu.
   - For companies that need multiple languages, a different SiteID can be used to configure each language required.
6. Click Save in the Preview window.
Design the Launch Button

Follow this procedure to customize the launch button.

1. Click **Products**.
2. Click **Cobrowse**.
3. Click **UI Customization**.
   - The **UI Customization** window with the Number Generated Screen displayed opens.
4. In the Sliding Block panel, select the position and orientation of the launch button.
   - **Note:** If you select **Right-Middle** or **Left-Middle** as the sliding position, the collapsed block (the Cobrowse launch button) will be positioned on the screen vertically. You will need to upload an image of a horizontal block as a vertical image will not be rotated.
5. Upload images.
   - a. To select a background image for the launch button, click **Upload** in the top section of the panel. Note that the image upload cannot be undone, and the image will stay active until another image is uploaded. The expanded button image should be 285 pixels (width) by 309 pixels (height).
   - b. Click **Upload** next to the Oracle icon and cancel icons to upload images for these icons, as well as any other launch button graphics.
     - An image for the phone icon should be 26 pixels by 26 pixels. An image for the Oracle icon should be 23 pixels wide by 24 pixels high.
6. Customize text for the launch button. Note that since custom text is not auto-translated, you should enter text in the language of the UI.
   - a. Enter any header text with your selections of font, size and color for the launch button. The default text is Cobrowse.
   - b. Enter text for a phone number if desired. A hyperlink to an external URL can also be placed in this area.
   - c. Enter any additional message text in the format you want.
     - It is recommended to leave the Provide Code Message block in its default format, but you can update it to accommodate your chosen terminology.
   - d. Enter any change to the background color of the session ID number box using the color picker.
     - It is recommended to pick a slightly different background color to draw attention to the session ID number.
   - e. Click **Upload**.
7. Select the style and size for the collapsed block and click **Upload**.
   - The collapsed button should be 157 pixels wide by 39 pixels high (reversed for horizontal).
8. Enter any text you wish for the hint block that appears when the customer hovers and click **Upload**.
   - You can upload an image containing text if you wish. The image should be 157 pixels wide by 78 pixels high.
9. Check the Preview window to see how the launch button will appear.
   - The button will appear the same on the Agent Connected Screen.
10. Click **Save**.
    - The Deploy button appears after you click Save.
11. Click **Deploy** to commit your changes to the cloud and apply them to Cobrowse sessions.
Customize Text for Job Access with Speech (JAWS) Software

Follow this procedure to customize text for Job Access with Speech (JAWS) software.

1. Click **Products**.
2. Click **Cobrowse**.
3. Click **UI Customization**.
   
   The **UI Customization** window opens.
4. Click the **ADA Compliance** link.
5. Customize text for JAWS software. This includes generating a number for a cobrowse session, opening and lowering the cobrowse button, and disconnecting a cobrowse session.
6. Click **Save**.

Make Additional UI Customizations

Follow this procedure to make additional UI customizations.

You can customize the UI with custom text and graphics. The following can be customized:

- Number Generation screen
- Agent Connected screen
- Unsupported Environment screen
- Taking Outside screen
- Session Escalation screen
- Terms & Conditions screen
- Close Confirmation screen
- Remote control screen
- Session Ended screen
- Other Intermediate Text

1. Click **Products**.
2. Click **Cobrowse**.
3. Click **UI Customization**.
   
   The **UI Customization** window opens.
4. Click the screen links for the customization you want to do.
5. Enter and upload content for your customized screen.
6. Check the Preview window to see how the screen will appear.
7. Click **Save**.
   
   Uploaded images do not need to be saved before being deployed.
8. Click **Deploy** to commit your changes to the cloud.
Number Generation Screen

The number generation screen is the first interaction a site visitor will have with the Cobrowse function.

The first state is the collapsed button, and the second state is the expanded button; both states are customized within the Number Generation Screen configuration area. While it is recommended that the default black or white theme be utilized, in this window the entire look and feel of the button UI can be changed by uploading new images and adjusting the various element controls.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Size Requirements (width x height in pixels); Text Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sliding block (the expanded button background)</td>
<td><img src="image1.png" alt="Sample Image" /></td>
<td>285 x 309</td>
</tr>
<tr>
<td>Collapsed button background</td>
<td><img src="image2.png" alt="Sample Image" /></td>
<td>157 x 39</td>
</tr>
<tr>
<td>Collapsed button background horizontal (for left-middle or right-middle placement)</td>
<td><img src="image3.png" alt="Sample Image" /></td>
<td>39 x 157</td>
</tr>
<tr>
<td>Hint block</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replacing this image with an image containing text is optional, as text can be superimposed within the hint block using the Hint Block Text First Line and Hint Block Text Second Line text fields.</td>
<td><img src="image4.png" alt="Sample Image" /></td>
<td>157 x 78</td>
</tr>
</tbody>
</table>
### Screen Element

<table>
<thead>
<tr>
<th>Sample Image</th>
<th>Size Requirements (width x height in pixels); Text Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone icon</strong></td>
<td><img src="image" alt="Phone Icon" /></td>
</tr>
<tr>
<td><strong>Cobrowse icon</strong></td>
<td><img src="image" alt="Cobrowse Icon" /></td>
</tr>
<tr>
<td><strong>Header text (text on the collapsed button)</strong></td>
<td><img src="image" alt="Header Text" /></td>
</tr>
<tr>
<td><strong>Phone Number Block</strong></td>
<td><img src="image" alt="Phone Number Block" /></td>
</tr>
<tr>
<td><strong>Provide Code Block</strong></td>
<td><img src="image" alt="Provide Code Block" /></td>
</tr>
<tr>
<td><strong>Number Box</strong></td>
<td><img src="image" alt="Number Box" /></td>
</tr>
<tr>
<td><strong>Terms &amp; Conditions</strong></td>
<td><img src="image" alt="Terms &amp; Conditions" /></td>
</tr>
<tr>
<td>Screen Element</td>
<td>Sample Image</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Powered By</td>
<td><img src="image" alt="Sample Image" /></td>
</tr>
<tr>
<td>This should read “powered by Oracle Cobrowse” unless your contract stipulates removal of Oracle branding.</td>
<td></td>
</tr>
<tr>
<td>Separator line</td>
<td></td>
</tr>
<tr>
<td>Hint Block Text First Line</td>
<td>When hovering over the Cobrowse button, a Help window will appear. This is the first line of that Help text.</td>
</tr>
<tr>
<td>Hint Block Text Second Line</td>
<td>When hovering over the Cobrowse button, a Help window will appear. This is the second line of that Help text.</td>
</tr>
<tr>
<td>Close Button</td>
<td></td>
</tr>
<tr>
<td>Minimize Button</td>
<td></td>
</tr>
</tbody>
</table>

Agent Connected Screen

After an online visitor gives a session ID code to an agent, and the agent enters that code into his Agent Console, a cobrowse session becomes active and the Agent Connected screen appears.
<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Size Requirements (width x height in pixels); Text Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded button background</td>
<td><img src="image" alt="Expanded button background" /></td>
<td>285 x 309</td>
</tr>
<tr>
<td>Collapsed button background</td>
<td><img src="image" alt="Collapsed button background" /></td>
<td>157 x 39</td>
</tr>
<tr>
<td>Disconnect background</td>
<td><img src="image" alt="Disconnect background" /></td>
<td>142 x 28</td>
</tr>
<tr>
<td>Disconnect background on hover</td>
<td><img src="image" alt="Disconnect background on hover" /></td>
<td>142 x 28</td>
</tr>
<tr>
<td>Minimize icon</td>
<td><img src="image" alt="Minimize icon" /></td>
<td>17 x 12</td>
</tr>
<tr>
<td>Cobrowse icon</td>
<td><img src="image" alt="Cobrowse icon" /></td>
<td>23 x 24</td>
</tr>
<tr>
<td>Header text</td>
<td><img src="image" alt="Header text" /></td>
<td>Cobrowse is the default header text. Text, font, text size, text color, bold, italic</td>
</tr>
<tr>
<td>Header number</td>
<td><img src="image" alt="Header number" /></td>
<td>Font, text size, text color</td>
</tr>
<tr>
<td>Content text</td>
<td><img src="image" alt="Content text" /></td>
<td>Text, font, text size, text color, bold, italic</td>
</tr>
<tr>
<td>Disconnect button text</td>
<td><img src="image" alt="Disconnect button text" /></td>
<td>Text, font, text size, text color (regular and hover)</td>
</tr>
</tbody>
</table>
## Not Supported Environment Screen

The Not Supported Environment Screen appears in the rare case that a website visitor’s device or browser does not support cobrowsing.

This screen can include a link to more information and can be customized to communicate any chosen message to the customer.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Size Requirements (width x height in pixels); Text Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded button background</td>
<td><img src="image" alt="Expanded button background" /></td>
<td>285 x 309</td>
</tr>
<tr>
<td>Collapsed button background</td>
<td><img src="image" alt="Collapsed button background" /></td>
<td>157 x 39</td>
</tr>
<tr>
<td>Screen Element</td>
<td>Sample Image</td>
<td>Size Requirements (width x height in pixels); Text Options</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Hint block</td>
<td><img src="image" alt="Sample Image" /></td>
<td>157 x 78</td>
</tr>
<tr>
<td>Minimize icon</td>
<td><img src="image" alt="Sample Image" /></td>
<td>17 x 12</td>
</tr>
<tr>
<td>Cobrowse icon</td>
<td>The Oracle icon is the default image.</td>
<td>23 x 24</td>
</tr>
<tr>
<td><strong>Header text</strong></td>
<td>Cobrowse is the default header text.</td>
<td>Text, font, text size, text color</td>
</tr>
<tr>
<td>When the Unsupported Environment Screen is displayed, this is the text that appears at the top. In most cases, companies keep this consistent with the header text on the Number Generation Screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Content text</strong></td>
<td><img src="image" alt="Sample Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
<tr>
<td>This is the message that appears to alert a site visitor that his browser does not support cobrowsing. It is a good idea to include messaging for how the customer can obtain assistance without cobrowsing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Footer text</strong></td>
<td><img src="image" alt="Sample Image" /></td>
<td>Text, font, text size, text color, URL</td>
</tr>
<tr>
<td>This is typically configured as a link to more information or other resources.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Taking Outside Screen

During a cobrowsing session, the customer may navigate to content on another web page that is not set up as approved content for cobrowsing.

A message displays alerting the customer that he or she is navigating outside of the cobrowse session and provides the option to open the web page in a new browser instead of interrupting the active cobrowse session.

- This window appears in the middle of the customer's screen. The background color of this screen is customizable using the color picker.
- The text that appears on the screen is customizable, as is the “click here” text that opens the content in a new browser window for the customer.
- The Close Button is a customizable 11 x 10 pixel image.
Session Escalation Screen

In cases where the agent and customer need to cobrowse content that is not a tagged web page, such as a PDF document on the customer’s desktop, or a third party website, the agent can escalate the session into Advanced Cobrowse mode (ACB).

When the agent clicks the button in his Agent Console to escalate into Advanced Cobrowse mode, a new window opens on the customer’s screen alerting them to this and asking for permission to start the Advanced Cobrowse mode.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog text</td>
<td><img src="image1.png" alt="Dialog Text Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
<tr>
<td>Dialog button</td>
<td><img src="image2.png" alt="Dialog Button Image" /></td>
<td>Text, font, text size, text color (regular and hover)</td>
</tr>
</tbody>
</table>

The text of the dialog button can be updated to display any message. For example, “OK,” “Accept,” or “Continue.”
## Terms & Conditions Screen

The Terms & Conditions Screen is different from the Terms & Conditions link that can appear on several of the UI windows.

The Terms & Conditions Screen is an optional UI that is presented at the first click of the Cobrowse button, before the Session ID window is displayed. This interim screen is most often used to display terms and conditions information, though it can be utilized for any purpose. A button at the bottom of the screen must be clicked in order to proceed and generate the session ID number.

The background color of this screen can be customized using the color picker, but a custom image cannot be uploaded to replace this background. The following table lists the elements of this screen that are customizable. The remaining elements from this window are customized in the Number Generation Screen.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headline text</td>
<td><img src="image" alt="Headline text Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
<tr>
<td>Main text</td>
<td><img src="image" alt="Main text Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
</tbody>
</table>

### Dialog button background

The background for the dialog button in both its standard state and hover state can be uploaded.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog button background</td>
<td><img src="image" alt="Dialog button background Image" /></td>
<td>Options</td>
</tr>
</tbody>
</table>
## Screen Element

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Size Requirements (width x height in pixels); Text Options; Color Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Session Button text</td>
<td><img src="image" alt="Sample Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
<tr>
<td>Start Session Button text shadow</td>
<td></td>
<td>1 x 21</td>
</tr>
<tr>
<td>Start Session Button</td>
<td></td>
<td>1 x 28</td>
</tr>
<tr>
<td>Start Session Button Hover</td>
<td></td>
<td>1 x 28</td>
</tr>
<tr>
<td>Scroll</td>
<td></td>
<td>Color picker for two colors</td>
</tr>
</tbody>
</table>

When there are multiple lines of text in the Headline or Main text areas, a scroll bar appears on the screen and is visible in the Preview window. You can customize the scroll bar with two colors.

**Note:** The customized colors are only visible on the customer’s page if the page includes this script:

```html
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>
```

If you don’t include the script, the default scroll bar appears without your customized colors.

### Related Topics
- Number Generation Screen

## Close Confirmation Screen

The Close Confirmation Screen is a window that displays for the customer near the Cobrowse button that asks for confirmation that the customer is intending to end an initiated session.

No and Yes buttons appear on the Close Confirmation Screen when a customer has clicked on a collapsed button and has been presented with a generated session number screen, and when an agent has not yet connected. When an agent connects to a session, a Disconnect button appears for the customer to end an active session.

The No and Yes buttons are customizable by uploading replacement images for standard and hover behavior. Additionally, the main text and button text are all customizable, including font, text size, text color (and hover color...
for the buttons), bold and italic. The background and border colors for this screen are customizable by using the color picker.

Remote Control Screen

When cobrowsing in Advanced Cobrowse mode (ACB), an agent with sufficient permissions may request remote control access in order to click and type on the customer’s screen.

Remote control access can help speed up certain types of interactions and ensure more accurate assistance. To enable this level of control, permission must be granted by the customer. This window displays when the agent selects Remote Control from the Modes drop-down list in the Agent Console.

Note: When an agent uses Remote Control in Instant Cobrowse mode (ICB), no permission screen is presented to the customer. This is because the agent can only interact with tagged Web pages during an ICB session, and cannot click or type on any other Web page or desktop application.

The background of this window is not customizable. The main text and button text are customizable, along with text size.
Session Ended Screen

When a cobrowse session is ended by either the customer or the agent, a Session Ended confirmation screen is presented to the customer.

The background color of this dialog box is configurable using the color picker. The image that appears on the right side of the window, the Close button, and the X icon at the top-right are customizable by uploading replacement images.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Sample Image</th>
<th>Text Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog text</td>
<td><img src="image.png" alt="Sample Image" /></td>
<td>Text, font, text size, text color</td>
</tr>
</tbody>
</table>
### Screen Element | Sample Image | Text Options
--- | --- | ---
Dialog description | ![Sample Image](image1.png) | Text, font, text size, text color
Feedback text  
This is the text that links to the Survey you have configured in the Surveys section to be presented to customers at the close of a session. | ![Sample Image](image2.png) | Text, font, text size, text color
Close button | ![Sample Image](image3.png) | Text, font, text size, text color, button width

### Other Intermediate Text

There are certain scenarios where you may want additional text to display that are not part of the main UI screens outlined in this document.

The text that appears on these other windows can be updated using the Other Intermediate Text section of the UI Customization area. If during testing you identify additional UI components that you’d like to customize, check the Other Intermediate Text section to locate the fields to make the appropriate changes.

### Save UI Customization Changes

You must be sure all changes you make are propagated to a web server for use in cobrowse sessions.

You must save any configuration or customizations you make. Uploaded images are saved automatically. Your saved changes are committed automatically. If you make changes without saving, a warning message appears that your changes have not been saved.  
Click **Deploy** to deploy your changes to the cloud. This may take several minutes.
Restore the Default UI

You can undo all customizations for the selected SiteID and return to the default UI.

When you restore the default UI, you undo all customizations made on any IU customization screen and return to the default UI for the SiteID displayed in the selection box in the upper right corner of the page.

1. Click Products.
2. Click Cobrowse.
3. Click UI Customization.
   The UI Customization window opens.
4. Click the SiteID drop-down menu in the upper right corner of the page and select the SiteID you want to restore to default settings.
5. Click Restore default UI.
   A confirmation window opens.
6. Click Restore.
   The window reloads with default values and displays a message indicating the restoration was successful. A Deploy icon appears in the Preview window.
7. Click Deploy to deploy your changes to the cloud.
10 Managing Agent Controls

Agent Controls

Different agent permission controls can be set based upon an agent's role or business unit.

It is possible for one group of agents to have View and Point level permissions while a different group of agents may have Remote Control level permissions. These permissions are assigned on a company level. Thus, you may have a “root level” (parent) group which are assigned View and Point permissions while a “sub-company” (child) can be assigned Remote Control permissions. This is performed in the Company Configuration section by selecting the appropriate Remote Option for the appropriate group. All users assigned to each of those groups through User Management will inherit that group's permission level.

You have the ability to suspend remote control on certain pages which can be configured in the page masking file.
11 Creating Configuration Files for Privacy and Security

Configuration Files for Privacy and Security

For cobrowsing to be effective, customers must be assured that their privacy and security are maintained during an interaction where an agent can see the customer’s screen.

- **Page masking** is applied to block certain web content from showing on an agent's screen.
- **Application masking** is applied to specific applications.
- **Field blocking** masks specific areas on a page that must be blocked from an agent’s view, such as a credit card number field on a web form.
- **Agent controls** define what the agent can see and what functions they can perform.

Security and privacy options are handled differently within the two modes of Oracle Cobrowse:

- In Instant Cobrowse mode, only website content tagged with Cobrowse Javascript can be viewed by the agent. For any content that includes sensitive customer data, the Cobrowse script can be configured to prevent the agent from viewing these pages. Additionally, field blocking can be applied to prevent viewing sensitive form fields during a Cobrowse session (credit card numbers or social security numbers).
- In Advanced Cobrowse mode, any combination of website and desktop content can be visible to the agent. This is not limited to website pages tagged with Cobrowse Javascript, but is controlled within the configuration.

**Planning your configuration:** As part of initial scoping or planning for a Cobrowse configuration project, it is important to identify requirements for each of the areas listed above. Think through what information should be masked from an agent's view. Content subject to Payment Card Industry Data Security Standard (PCI) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance (for example, credit card numbers and social security numbers) is often masked. Additionally, password reset pages as well as responses to validation questions (for example, “in what city were you born”) are often masked. Submit buttons to purchase products or execute trades are often where agents are prevented from using full control.

**Working with masking files:** Masking should be performed at the root company level as it is Site ID dependent. Before you can configure your masks on your site, you must first create a configuration file in an .xml format to be uploaded to your site. Page blocking may be configured by page title, page URL, or by both page title and URL. When masking by both page title and URL, the application will use titles only if the browser does not support URL-based masking.

**Note:** For certain Cobrowse ICB deployments (for example, Cloud) the presence of a page masking configuration affects the deployment instructions available on the Cobrowse V4 /Configuration page.
Configure Page Masking

Follow this procedure to configure page masking by page title and URL.

Details on preparing your page blocking files are in the following procedures:

- **How You Mask Pages by Page URL**
- **Use Wildcards in URL Page Masking**
- **Example of Page Masking by Page URL**
- **Application Masking**

1. Click **Products**, and then select **Cobrowse V4 > Masking Configuration (V3/V4)**.
2. Select the SiteID you are configuring page masking for.
   - In the Status column, a red button indicates that a configuration file has not been uploaded and a green button indicates that a configuration file has been uploaded.
3. Click **Configure** in the Page blocking row to upload a page masking configuration file.
   - The page will reload.
4. Click **Choose Configuration File** and browse to your configuration file in xml format.
5. Click **Save**.
   - The configuration file is committed. If you try to leave this page without saving your changes, a warning message appears that your changes will be lost.
6. Once the configuration file is committed, click **View configuration** to view the file.
7. If you want to delete a configuration file that has been committed, click **Delete configuration**.

**How You Mask Pages by Page URL**

There are three properties to configure for page masking by page URL.

Configure a list of URL patterns to show (ltb_urls), a list of URL patterns which should be masked inside of the previous list (ltb_urls_exc), and a list of URLs to show but were included in the previous list under general rules (ltb_urls_force_inc). URL patterns are used to configure URL-based page blocking. The URL can be represented with the following structure:

```
<PROTOCOL>://<DOMAIN>/<PATH>?<PARAMS>#<HASH>
```

For example, with this URL:

http://retail.com/coffeemakers/FastBrew.html?q=fdserew&t=retail#email

- `<PROTOCOL>` is http, `<DOMAIN>` is retail.com, `<PATH>` is coffeemakers/FastBrew.html, `<PARAMS>` is q=fdserew&t=retail, and `<HASH>` is email.

**Use Wildcards in URL Page Masking**

You can use wildcards (* and +) as a first or last character in each part of the URL pattern for page blocking configurations.
The wildcard ‘*’ means that there can be zero or more characters in place of the ‘*’ symbol. The only special case here is when the ‘*.’ appears at the beginning of the <DOMAIN>. For example, http://*.google.com/**## matches both http://www.google.com and http://www.google.com URLs.

**Note:** The MS Edge browser removes “www” from URLs, so do not include “www” in your wildcard masking pattern. For example, use http://*.google.com/**## to match https://www.google.com instead of http://www.google.com/**##.

The wildcard ‘+’ means that there should be at least one character in place of the ‘+’ symbol.

While it is usually sufficient to have ‘*’ in place of <PARAMS>, you can further specify it if you need more fine-grained configuration with a “<KEY_1>=<VALUE_1> and <KEY_2>=<VALUE_2>…” format and using a wildcard as a first or last character in the <VALUE> part.

**Examples**

http://*.retail.com/**##

This pattern matches all URLs from the retail.com domain:

- http://www.retail.com
- http://retail.com

http://ecommerce.retail.com/kitchen/basket.aspx

This URL only matches http://ecommerce.retail.com/kitchen/basket.aspx. The following URLs do not match this:

- http://ecommerce.retail.com/kitchen/basket.aspx#payppcc~

**Example of Page Masking by Page URL**

The following XML code is an example of a URL-based page masking configuration.

```xml
<configuration>
  <siteCode id="<SITE_ID>" currentState="Active">
    <module id="LTB" scope="SITE">
      <param id="ltb_urls">
        <value text="http://*.livelook.com/**##" title="" seqId="0"/>
      </param>
      <param id="ltb_urls_exc">
        <value text="https://*/*##" title="" seqId="0"/>
      </param>
      <param id="ltb_urls_view_only_mode">
        <value text="https://www.livelook.com/checkout.aspx" title="" seqId="0"/>
      </param>
    </module>
  </siteCode>
</configuration>
```
With this configuration, all HTTP URLs from the livelook.com domain and only one HTTPS page (https://www.livelook.com/checkout.apsx) will be visible, as illustrated in the image below. The black boxes represent masked URLs, and the white boxes represent visible URLs.

The variable `<param id="ltb_urls_view_only_mode">` further specifies that remote control access is suspended on https://www.livelook.com/checkout.apsx and the agent may only view the page. The agent will see a red border on that page and will receive a notification that control is suspended.

### Application Masking

Application masking controls the visibility of specific desktop applications in Advanced Cobrowse mode.

Application masking is defined in the same file as page masking. To accurately implement application masking, process names are used to identify the applications that should be visible.

The following XML code is an example of an application masking configuration allowing Turbotax and Quickbooks applications to be visible during a session.

```xml
<configuration>
  <siteCode id="<SITE_ID>" currentState="Active">
    <module id="LTB" scope="SITE">
      <param id="ltb_apps">
        <value text="QBW32" title="" seqId="0" />
        <value text="quickset" title="" seqId="0" />
        <value text="qw" title="" seqId="0" />
        <value text="Turbotax" title="" seqId="0" />
      </param>
    </module>
  </siteCode>
</configuration>
```

To specify that the customer's browser settings are visible to an agent during a cobrowsing session, use this XML variable:

```xml
<param id="ltb_show_browser_settings">
  <value text="yes" title="" seqId="0" />
</param>
```

To specify that the content of the customer's browser tabs are not visible to an agent during a cobrowsing session, use this XML variable:

```xml
<param id="ltb_show_content_only">
  <value text="yes" title="" seqId="0" />
</param>
```
Block a Field

Administrators can set up a Cobrowse configuration to block a field from the agent’s view.

Field blocking protects sensitive form data from being viewed by an agent or even transmitted at all during a cobrowsing session. Field blocking is often used to protect customer privacy when fields like credit card numbers and social security numbers are visible on a page that may be cobrowsed during a customer service interaction.

The Cobrowse system must be able to identify each field that should be blocked. The simplest and preferred method is to set up a field class attribute for blocked fields. For example, a class named “LLBlocked” can be established, where any field on a page that includes both the Cobrowse JavaScript code and references this class attribute will be blocked. The XML code for this example would be:

```xml
<tr>
  <td class="divLabel LLBlocked">Card Number:</td>
  <td class="Field"><input name="tbAccountNumber" type="text" maxlength="16" size="20" id="tbAccountNumber" /></td>
</tr>
```

**Note:** To mask a drop down field, in addition to the field class attribute, the URL of the page with the drop down field must be configured in Cobrowse.

A secondary method is to use the field ID. The disadvantage is that any time it is required to add a new blocked field, the ID of this field must be provided to the Configuration Administrator in order to configure it for privacy. From the example, this time the field class is not set and you would need the `ID=tbAccountNumber` to configure blocking:

```xml
<tr>
  <td class="divLabel">Card Number:</td>
  <td class="Field"><input name="tbAccountNumber" type="text" maxlength="16" size="20" id="tbAccountNumber" /></td>
</tr>
```

1. After writing the xml for field blocking using either a field class or field ID attribute, mark the field to be blocked with a subtle color shift for the field border and text.
   This enables the image capture algorithm to recognize that this is a blocked field. Colors are selected using a color picker, such as the Eltima Software Absolute Color picker.

   **Note:** The color chosen must not be used anywhere else on the page or masking artifacts can appear. An example artifact is a masking dot where there should not be a masking symbol. It may take several tries to find a color combination that has no masking artifacts.

2. On the Admin Console, click **Products**, and then select **Cobrowse V4 > Masking Configuration (V3/V4)**.
3. Select the SiteID you are configuring page masking for.
   In the Status column, a red button indicates that a configuration file has not been uploaded and a green button indicates that a configuration file has been uploaded.
4. Click **Configure** in the Field blocking row to upload a field masking configuration file.
   The page will reload.
5. Click **Choose Configuration File** and browse to your configuration file in xml format.
6. Click **Save**.
The configuration file is committed. If you try to leave this page without saving your changes, a warning message appears that your changes will be lost. Once the configuration file is committed, you can view the file by clicking View configuration. If you want to delete a configuration file that has been committed, click Delete configuration.

7. Click Deployment Instructions on the Configuration tab to see and email instructions.

The field blocking script appears in this window as an fmset.js script and can be sent to the email you provide.

8. Copy and paste the full text of the fmset.js <script> tag from the deployment instructions as the last element in the <head> tag on every page to be blocked or which contains fields to be blocked.

The following is an example of a field blocking script. You will need to use your unique URL from the deployment instructions.

```html
<script type="text/javascript" src="https://b6ac25f4e1c9-9b11bfce.ssl.cf2.com/llscripts/fmset.js"></script>
```

## Mask Data Displaying in a Div Overlay

Administrators can set up a Cobrowse configuration to block sections from the agent’s view.

Use the LLBlocked class to block fields such as credit card numbers (see Block a Field). Use the LLPageBlocked class to block sections such as call detail. In Advanced mode, the whole page will be masked if a page section tagged with the LLPageBlocked class becomes visible. In Instant mode, only the appropriate section of the page will be masked.

1. If the fields or sections which should be masked are added to the page after the page is loaded (for example by AJAX request) use the following JavaScript code after appropriate fields or sections are added to the page (become part of the Document Object Model (DOM):

   ```javascript
   if (typeof LiveLookFM != "undefined") {
     LiveLookFM.fieldMask("");
   }
   ```

2. If sections are not added dynamically but exist in the DOM and their visibility is changed through JavaScript, do one of the following:
   - To mask a section tagged with LLPageBlocked class, the element itself should include either the style property display:none or visibility:visible such as:
     ```html
     <div class="LLPageBlocked" style="display:none;"></div>
     ```
   - To unmask a section tagged with LLPageBlocked class, the element itself should include either the style property display:block or visibility:hidden such as:
     ```html
     <div class="LLPageBlocked" style="display:block;"></div>
     ```

## Examples of Field Blocking

The following are example XML files for identifying fields that should be masked.

### Using field IDs

```xml
<configuration>
  <siteCode id="Example:SC43636199:AU:1" currentState="Pending">
    <module id="FM" scope="SITE">
      <param id="fm_border_color">value="C8DEC6" title="" seqID="0" /></param>
      <param id="fm_text_color">value="0D0C24" title="" seqID="0" /></param>
      <param id="fm_html_field_ids">
        <value text="cardNumber" title="" seqID="0" /></value>
        <value text="cardDateMonth" title="" seqID="0" /></value>
        <value text="cardDateYear" title="" seqID="0" /></value>
    </param>
  </module>
</configuration>
```
Using field class attributes

Masking and Blocking Configuration Variable Summary

These variables may be used to configure page blocking and field blocking.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ltb_apps</td>
<td>recordset</td>
<td>Applications to show</td>
</tr>
<tr>
<td>ltb_show_browser_settings</td>
<td>value</td>
<td>Show browser settings</td>
</tr>
<tr>
<td>ltb_show_content_only</td>
<td>value</td>
<td>Show browser window content only</td>
</tr>
<tr>
<td>ltb_urls</td>
<td>recordset</td>
<td>Browser URLs to show</td>
</tr>
<tr>
<td>ltb_urls_exc</td>
<td>recordset</td>
<td>Browser URLs to mask</td>
</tr>
<tr>
<td>ltb_urls_force_inc</td>
<td>recordset</td>
<td>Browser URLs to show even if in the mask list</td>
</tr>
<tr>
<td>ltb_urls_view_only_mode</td>
<td>recordset</td>
<td>Browser URLs to suspend remote control</td>
</tr>
<tr>
<td>ltb_view_pointer_mode</td>
<td>recordset</td>
<td>Browser URL and title pairs to allow only view and pointer mode on the page. The pair must be separated by a pipe: “URL</td>
</tr>
<tr>
<td>fm_border_color</td>
<td>value</td>
<td>Border color</td>
</tr>
</tbody>
</table>
Configure IP Address Restrictions

IP restrictions restrict the range of IP addresses from which an agent can connect to a cobrowse session.

IP address restrictions limit agents outside of pre-defined IP addresses from connecting with your customers.

Note: IP restrictions are performed at the parent company level and apply to all sub-companies and divisions.

1. From the Admin Console, click Company Set-up.
2. Click Company Configuration.
3. On the IP Address Restriction page, add IP restriction blocks in “slash notation” to represent the range of IP addresses to be configured: [IP address of a network] / [subnet mask number].

Note: The IP address of a network must be aligned to the beginning of a block (e.g., 10.0.0.0/27). Use slash 32 to configure a single IPv4 address (e.g., 192.168.0.100/32). If you get an invalid IP response when saving your IP configuration, check with your network source to ensure you have a valid IP address block.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fm_html_class_name</td>
<td>value</td>
<td>HTML field class name</td>
</tr>
<tr>
<td>fm_html_field_ids</td>
<td>recordset</td>
<td>HTML field IDs</td>
</tr>
<tr>
<td>fm_text_color</td>
<td>value</td>
<td>Text color</td>
</tr>
</tbody>
</table>
12 Configuring Surveys

Display a Link to a Post-Cobrowse Survey

Oracle Cobrowse includes the ability to display a post-cobrowse survey for both customers and agents.

This capability incorporates a URL that is presented in the Session Ended window enabling the participants to complete the survey. It's important to note that this feature only adds the link to a web-based survey tool of your choice, where you have previously configured your desired survey questions. Survey results are accessible through your chosen survey tool and are not visible in the Cobrowse Admin Console. Integrated Cobrowse customers can choose to utilize Oracle Service Cloud Feedback as their survey mechanism.

You can enable surveys for customers, agents, or both.

1. From the Admin Console, click **Surveys**.
   
   A submenu opens with Client Survey and Agent Survey tabs.

2. Click **Client Survey** or **Agent Survey**.

3. For a client survey, select the SiteID from the dropdown menu that displays in the header.
   
   The SiteID selection is only needed for a client survey.

4. Click **Enable**.
   
   A textbox displays.

5. Enter the URL to your web-based survey in the textbox.

   You can configure agent surveys to be different for a root company and for a subcompany so that agents will see different surveys at the end of a Cobrowse session depending on whether they are under a root company or a subcompany.

6. Click **Save Changes**.

7. To disable a survey, click **Client Survey** or **Agent Survey**.
   
   a. Select **Disable**.
   
   b. Click **Save Changes**.

Sample agent questions:

- Were you able to connect to the customer and see his or her screen? (Y/N)
- How satisfied were you with your ability to help the customer with Cobrowse? (5 point scale Not Satisfied to Extremely Satisfied)
- How likely are you to recommend Cobrowse to your colleagues and co-workers? (5 point scale Not Satisfied to Extremely Satisfied)
- Would you proactively ask your customers to use the Cobrowse service? (Y/N)

Sample customer questions:

- How satisfied were you with your ability to get help using Cobrowse? (5 point scale Not Satisfied to Extremely Satisfied)
- How satisfied were you with the Cobrowse ease of use? (5 point scale Not Satisfied to Extremely Satisfied)
- How likely are you to recommend Cobrowse to your friends as a way to work with this company? (5 point scale Not Satisfied to Extremely Satisfied)
13 Configuring Your Company Deployment

Configure Your Company Deployment

You configure deployment of Cobrowse at the root company level. A newly created siteID is selected by default.

1. Click **Products**.
2. Click **Co-Browse V4**.
3. Click **Configuration**.
   - The Configuration (Co-Browse V4) window opens.
4. Select either **Standard Deployment** (both Instant and Advanced modes) or **ICB-only deployment** (Instant mode only).
   - **Note:** Standard Deployment is selected by default and is highly recommended to ensure support for current and future use cases.
5. Select the Launch Point for the button that launches a Cobrowse session.
   - **Launch Point 1** is the default selection (recommended) to have the button appear on the page as defined by the Number Generated Screen selections.
     - The Cobrowse button will be visible on the website, but can be concealed with Stealth mode, described in steps 9 and 10 of this procedure.
   - **Launch Point 2** to have the launch icon appear when a site visitor clicks on a specified link or image.
     - During a cobrowse session, when the specified link or image is clicked, the button appears on the page as defined by the Number Generated Screen selections. When Launch Point 2 is selected, you will need to provide an ID for the launch button.
     - See **Best Practices for Launch Point Design** for more information on launch point options and best practices.
6. Click the **Optional Configuration** link.
7. Enter websites that customers can navigate to during a Cobrowse Instant mode session in the **ICB URL**s field without triggering a warning message to customers that they are navigating to a screen not visible to the agent.
   - Wildcard characters can be used for any pages beyond the URL listed.
     - If you enter **//www.Company_Domain.com/***, the customer will receive a warning for any navigation away from any page on the entire site.
     - If you enter **//www.Company_Domain.com/Folder_1/* or //www.Company_Domain.com/Folder_2/subFolder_3/***, for example, the customer will receive a warning when they navigate away from those specific pages of the domain during the ICB session.
8. Enter websites where a Cobrowse session automatically starts in Advanced mode in the **URLs to Force ACB Mode** field.
   - Wildcard characters can be used for any pages beyond the URL listed.
     - Enter **//www.Company_Domain.com/***, for example, to force Advanced mode for the entire company website.
     - Enter **//www.Company_Domain.com/Folder_1/***, for example, for a specific page.
     - When the customer navigates to one of these pages while in ICB mode, the session remains in Instant mode.
     - This field only appears when **Standard Deployment** is selected.
9. Select the **Stealth Mode** checkbox to make the launch point invisible on every page of the deployment.
This checkbox only appears when Launch Point 1 is selected. This mode is useful for pilot deployments or when you don't want your customers to click on it without being prompted by the agent.

If the customer is using a PC or laptop, the launch point displays by pressing Ctrl+Enter. On mobile devices, the launch point displays after holding two or three fingers on the screen for 2 to 3 seconds, and then releasing. The number of fingers you should hold down depends on the make and model of your device, and individual settings.

10. Enter websites where Stealth Mode is automatically triggered in the **URLs to Force Stealth Mode** field. Wildcard characters can be used for any pages beyond the URL listed.
   - Enter `http://www.Company_Domain.com/AboutUs.aspx`, for example, to trigger stealth mode on that page.
   - Enter `http*://www.Company_Domain.com/*.html`, for example, for all html pages on http or https.

This field only appears when Launch Point 1 is selected.

11. Click the **End-user consensus for ICB full control** checkbox to ask for end-user consensus when the agent activates full control in ICB mode.

12. To delay the Launch Point button display for a specified number of seconds after loading, enter the number of seconds in the delay the **Delay Timer (seconds)** field.

This field only appears when Launch Point 1 is selected.

13. If you selected Launch Point 2, enter the **Launch Button ID**.

    The javascript code for the button must be present on all customer pages, and should reference the same button ID on all of them.

14. Enter **Custom Data**.

15. Enter **Custom Functions**.

16. Click **Save**.

    Your changes are committed to the cloud and applied to Cobrowse sessions.

**Related Topics**
- Design the Launch Button

**Best Practices for Launch Point Design**

Starting a Cobrowse session requires that customers click a launch button, referred to as the Cobrowse Launcher.

The Cobrowse Launcher can be displayed and designed in a multitude of ways, similar to the many ways Live Chat can be presented on a website: as a link, a button, or an icon. The Launcher can be highly visible on a web page, or it can be placed conspicuously in a footer menu. It can be visible on every page of a website, or just on a few specific pages.

To underscore the importance of a well thought out launch experience, let's examine some of the most common reasons Cobrowse is used during a service interaction:

- A frustrated customer is experiencing a problem on the website.
- A customer can’t find what they need on the site on their own.
- A less tech-savvy customer is having trouble navigating the site or using self-service tool.
- An agent wants to engage a customer at risk of abandoning the site before completing a purchase.

In all cases, it is critical to create a low effort cobrowse launch experience that is easy to find, easy to use, and quick to connect. This ensures that cobrowsing works as designed, to enhance and expedite the interaction. A poorly designed launch experience can have the opposite effect, causing additional frustration for the customer and agent.
Like Chat, Cobrowse launch points can be displayed in many ways and the decision for how to display the launch button is typically impacted by several factors:

- Branding and design
- Customer experience strategy
- Site usability
- Channel strategy

Oracle Cobrowse can be launched from two distinct categories, Launch Point 1 and Launch Point 2.

**Launch Point 1 (recommended):** Using Launch Point 1, the Cobrowse button is always visible on the website, unless otherwise defined with Stealth mode, in the position specified in the configuration (for example, top left, bottom right, or offset by 100 pts.). Launch Point 1 is the default option. You don't need to do anything to enable it.

**Launch Point 2:** Using Launch Point 2, the launch button is not automatically visible to customers on the website. The website has a link or an image from which a Cobrowse session would launch. The link or image has a unique ID associated with the Cobrowse Launch within the Cobrowse Administrative Console. When a site visitor clicks on the link or image configured to be the launch point, the Cobrowse Panel to initiate a session appears in the location specified in the configuration (for example, top-left, bottom-right, or offset 100 pts.).

**Best Practices for Launch Point Location and Visibility**

These are some best practices for launch point location and visibility.

**Launch point location:** The most successful Cobrowse deployments utilize a site-wide floating button placement, as is the default configuration of Oracle Cobrowse Launch Point 1. This ensures that customers do not have to navigate off the page they are on when they need help. It also eliminates the frustration that can occur when an agent is attempting to direct a customer to a launch point over the phone that requires the customer to navigate to a new page, scroll down to a footer, or look for a link within other site content. Requiring a customer to navigate to a non-obvious location in order to start a cobrowse session will increase call handling times, result in abandonment, and add to customer frustration as they are tasked with locating a resource elsewhere on the page or site.

**Launch point visibility:** The hovering button style of Oracle Cobrowse Launch Point 1 stays visible on every page throughout the customer's visit, unless otherwise defined, remaining in view while the customer scrolls through the page content. The hovering button can be placed in any location on the page, but most commonly will be set to appear at the bottom right or on the middle of the right or left side of the page. Offset controls enable companies to specify exactly where on the page the Cobrowse button should appear.

Though the best practice is to set the Cobrowse button to be visible on every page, there are often business reasons why companies do not want a Cobrowse button to appear on certain pages, such as for customer privacy, or may want them located only on certain pages, such as the Contact Us page or Help page. As with considering the customer experience associated with the launch point location, it is just as important to consider how visibility of the launch button will impact the interaction. The launch point can be concealed with Stealth mode, which is useful for testing and pilot deployments, or for specifying specific URLs where it should not appear.

**What happens when a customer clicks the Cobrowse button by mistake:** This is a common concern when companies consider adding a site-wide Cobrowse button. By setting up the Cobrowse UI to carefully communicate its purpose to
customers, curiosity clicks are kept to a minimum. Cobrowse sessions are never active until an agent who is talking to a customer on the phone already receives and inputs that customer’s session ID code into the Cobrowse Agent Console. Clicking the button itself does nothing but expand the Cobrowse UI to display messaging. It does not initiate a session, connect to an agent, add an incident to a queue or consume web sessions.

Related Topics
- Configure Your Company Deployment

Domain Whitelisting

If your network has firewall rules, email anti-relay or anti-spam measures, proxy firewalls, antivirus or other filtering mechanisms, you might need to revise the rules to whitelist the Fully Qualified Domain Names (FQDNs) associated with the Oracle Cobrowse platform.

A whitelist consists of a list or registered entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition. “Whitelist” can mean “to authorize.” It is the opposite of a “blacklist” which consists of a list or compilation that identifies entities that are denied access to a system. Oracle strongly recommends that you whitelist all the FQDNs prior to the start of the Cobrowse deployment process. These Oracle FQDNs are for the specific use of Oracle products. We advise you contact your organization’s IT department for assistance with whitelisting. The following FQDNs must be whitelisted:

- *.livelook.com
- *.livelook.net
- *.showscreen.com
- *.rightnowtech.com
- *.rightnow.com
- *.custhelp.com

Deploy Your Settings

Commit your changes to the cloud and tag web pages to be cobrowsed with a reference to the Cobrowse Launcher Script.

All web pages to be cobrowsed must be tagged with a reference to the launcher script. Additionally, if field masking is configured for the selected SiteID, then additional java script code must be added to each page that includes fields that should be masked.

1. Click Products.
2. Click Co-Browse V4.
3. Click Configuration.
   The Configuration (Co-Browse V4) window opens.
4. After all UI customization, configuration and masking configuration changes are complete, click Save at the bottom of the Configuration (Co-Browse V4) screen.
5. Click **Deployment Instructions** to see and email instructions. The launcher script appears in the email request window and is sent to the email you provide.

6. Include the launcher script JavaScript code on every page that needs to be cobrowsed in each domain. The code also provides for the launch point. Best practice is to put this code in a common header or footer. This is an example of a launcher script:

```
<script type="text/javascript" src="https://17be418f2dd110f26041-631cc621b1140045e77e413cd09d5315.ssl.cf2.rackcdn.com/llscripts//launcher.js"></script>
```

The field masking script appears in this window as an fmset.js script and can be sent to the email you provide. Copy and paste the full text of the **fmset.js** tag from the deployment instructions as the last element in the `<head>` tag on every page to be blocked or which contains fields to be blocked. You will need to use your unique URL from the deployment instructions. This is an example of a field masking script:

```
<script type="text/javascript" src="https://b6ac25f4e1c9-9b11bfce.ssl.cf2.com/llscripts/fmset.js"></script>
```

**Note:** Support for cobrowsing of iFrame content requires deployment of the Cobrowse launcher script on both the main website as well as the content that is delivered within the iFrames. If any content displayed in iFrames is served by a third party, that third party content provider will need to add your Cobrowse launcher .js script to the iFrame content.
Chapter 14
Using Integrated Cobrowse

14 Using Integrated Cobrowse

How You Use Cobrowse with an Oracle Agent Desktop

For integrated Cobrowse, agent accounts are set up in the Oracle Service Cloud Agent Desktop.

See documentation for the release version of your Agent Desktop (Answer ID 5168 for Oracle Service Cloud, or Cloud Documentation).
15 Adding the In-App SDK

Download the SDKs

Download the SDKs from the Oracle Software Delivery Cloud.

1. Visit Oracle Software Delivery Search Software.
2. Search for Oracle Cobrowse SDK (with no space or dash).
3. Click Select Platform and select Apple iOS, Google Android, or both.
4. Click Select.
5. Click Continue.
6. Click Continue.
7. Select the check box to accept the Oracle Standard Terms and Restrictions, and click Continue.
8. Click Download.

In-App SDK for iOS

Oracle Standalone Cobrowse capability can be added to a native iOS application environment to enable cobrowsing of in-app content.

The following procedures outline the steps required to add Oracle Standalone Cobrowse capability to a native iOS application.

- Import the Library
- Import the Framework
- Import the Header File

Import the Library

Import the In-App Cobrowse library into the iOS application where cobrowse capability is required.

1. Right click on the project in the Navigator sidebar and select Add file to project name.
   The File dialog window will open with OracleCobrowseSDK.framework selected.
2. Click Add.

Import the Framework

Import the framework into the iOS application where cobrowse capability is required.

Import SystemConfiguration.framework.

Your Framework folder should look like this image:
Import the Header File

Follow this procedure to import the header file.

1. In your AppDelegate.m, import the header file of the OCBManager.h class.
   - Objective_C: #import <OracleCobrowseSDK/OCBManager.h>
   - Swift: import OracleCobrowseSDK

2. Locate -application:didFinishLaunchingWithOptions: and add the following lines.
   - Objective-C: OCBManager *manager = [[OCBManager sharedInstance] startWithURL: <your_launcher_url>];

   ```
   #import "AppDelegate.h"
   #import <OracleCobrowseSDK/OCBManager.h>

   @implementation AppDelegate

   -(BOOL)application:(UIApplication *)application didFinishLaunchingWithOptions:(NSDictionary *)launchOptions {
      //Override point for customization after application launch.
      //Oracle Cobrowse SDK
      [[OCBManager sharedInstance] startWithURL:@"<YOUR_LAUNCHER_URL>" ];
      return YES;
   }

   - (BOOL)application: application didFinishLaunchingWithOptions: launchOptions {

   - Swift: let manager = OCBManager.sharedInstance() manager.start(withURL: "<your_launcher_url>"

```
The value for the launcherURL parameter will be provided by your Oracle Cobrowse implementation team. This launcherURL controls the design and position of the Cobrowse launch point.

You’ll then see the Cobrowse button appear, as designed, within a second after launching your application.

## Application States

At each moment of time, the Cobrowsing application is in an application state. The application state determines application functionality.

<table>
<thead>
<tr>
<th>Application State</th>
<th>Description</th>
<th>Available Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCBSessionStateNone</td>
<td>Application is not initialized yet.</td>
<td>Subscribe to cobrowsing events.</td>
</tr>
<tr>
<td>OCBSessionStateInit</td>
<td>Application is initializing.</td>
<td>Subscribe to cobrowsing events.</td>
</tr>
</tbody>
</table>
| OCBSessionStateReady      | Application has finished initializing, no active cobrowsing session is detected. | • Subscribe to cobrowsing events.  
                            |                                    | • Start cobrowsing session.         |
| OCBSessionStateStarting   | Application is in the process of starting a cobrowsing session. An access code has not yet been received. | • Subscribe to cobrowsing events.  
                            |                                    | • Stop cobrowsing session.          |
| OCBSessionStateActiveWait | A cobrowsing session ID was generated but an agent has not yet connected. | • Subscribe to cobrowsing events.  
                            |                                    | • Stop cobrowsing session.          |
| OCBSessionStateActive     | Session is in progress. At least one agent is connected. | • Subscribe to cobrowsing events.  
                            |                                    | • Stop cobrowsing session.          |
## OCBManager Methods and Properties

The methods and properties listed here can be accessed through the OCBManager singleton class.

Before any methods described below are called, the caller must make sure that the Cobrowsing application is in the required application state in order to proceed. See *Application States*.

<table>
<thead>
<tr>
<th>Method</th>
<th>Required Application State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ (OCBManager *) sharedInstance</td>
<td>All</td>
<td>Returns OCBManager instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The first call configures OCBManager to use a custom or default UI. There is no way to reconfigure OCBManager after the first call.</td>
</tr>
<tr>
<td>-(void) startWithURL: (NSString *) url</td>
<td>All</td>
<td>This method has several functions. The very first call initializes the OCBManager engine, reading all necessary data from the server, and saves the current activity context. Subsequent calls update activity context which is used by the OCBManager engine. You should call this method after each activity transition. The value for the launcherURL parameter will be provided by your Oracle Cobrowse implementation team.</td>
</tr>
<tr>
<td>-(void) startSessionWithURL: (NSString *) url</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>-(void) generateAccessCodeWithCompletionHandler</td>
<td>Ready</td>
<td>Sends a request to the Oracle servers to start a cobrowsing session. Success or failure of the request can be further tracked through activity state.</td>
</tr>
<tr>
<td>(void) (^) (NSString *accessCode) completionHandler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-(void) sessionDisconnect</td>
<td>Starting, Active Waiting, Active</td>
<td>Initiates a request to stop the cobrowsing session. Success or failure of the request can be further tracked through activity state.</td>
</tr>
<tr>
<td>NSString *launcherURL</td>
<td>All</td>
<td>Gets the Cobrowse iOS In-App SDK launcherURL.</td>
</tr>
<tr>
<td>Method</td>
<td>Required Application State</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>OCBSessionState state</td>
<td>All</td>
<td>Returns the OCBSessionState.</td>
</tr>
<tr>
<td>NSString *SDKVersion</td>
<td>All</td>
<td>Gets the Cobrowse iOS In-App SDK version.</td>
</tr>
<tr>
<td>NSString *supportedOSVersion</td>
<td>All</td>
<td>Gets the supported OS version.</td>
</tr>
</tbody>
</table>

**In-App SDK for Android**

Oracle Standalone Cobrowse capability can be added to a native Android application environment to enable cobrowsing of in-app content.

The following procedures outline the steps required to add Oracle Standalone Cobrowse capability to a native Android application.

- Install the SDK
- Integrate the SDK

**Install the SDK**

Follow this procedure for setting up the SDK.

Upgrading: If you were previously using another release of the Oracle Cobrowse Android SDK, delete all cobrowse source files from your project before proceeding.

Make sure to include Android v4 Support Library (revision 19.1.0 or greater) in your project. See Support Library for more information on support libraries.

1. Download the latest version of the Oracle Cobrowse Android SDK.
2. Open the Modules settings in Project Structure.
3. Click the + sign.
4. Select Import JAR/AAR Package and click Next.
5. Provide the path to the LLAndroidLibrary.aar file and click Finish.
6. Click Apply to synchronize your project.
   After synchronization is complete, you see the LLAndroidLibrary in the modules list.
7. Open the Dependencies settings in Project Structure.
8. Select the app module.
9. Select Module Dependency in the Declared Dependencies section and click the + sign.
10. Select LLAndroidLibrary and click OK.
11. Click Apply to synchronize your project.

The Cobrowse In-App SDK for Android library set up is complete. You can close the Project Structure settings.
Integrate the SDK

Follow this procedure for integration.

1. In your application’s manifest `AndroidManifest.xml`, add your launcher URL as Meta Data.

2. In `AndroidManifest.xml`, add the following inside the application tag:

   ```xml
   <meta-data android:name="com.oracle.cobrowse.android.sdk.LauncherURL"
               android:value="launcherURL"/>
   ```

   The value for the launcherURL parameter will be provided by Oracle.

3. In `AndroidManifest.xml`, request the following permissions:

   ```xml
   <uses-permission android:name="android.permission.INTERNET" />
   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
   ```

4. Import the Cobrowse package by adding the following to the import list of your activity:

   ```java
   import com.oracle.cobrowse.android.sdk.
   ```

5. Subclass `FragmentActivity` or `Activity` for your activity class.

6. In `onResume`, call the `start(activity)` method:

   ```java
   CobrowseManager.getInstance().start(this)
   ```

7. Repeat steps 4 through 6 for every other activity in your application.

   Calling `CobrowseManager.getInstance().start(this)` in every activity will reconnect it to the already opened session instead of creating a new one.

8. By default, the SDK does not capture dialogs. If you have dialogs in your app and you want to share them with the agent during a cobrowse session, pass the dialog instance to the SDK as soon as it becomes visible using the `screenDialog(dialog)` method.

   ```java
   CobrowseManager.getInstance().screenDialog(dialog)
   ```

After you have integrated the Oracle Cobrowse SDK and have completed this procedure, everything should be up and running. You’ll see the Live Expert button within a second after launching your application.
16 Using Cobrowse on Mobile Devices

Special Considerations for Using Cobrowse on Mobile Devices

Take note of these differences for some features of Cobrowse when you use mobile devices.

- ACB mode is not supported on mobile devices.
- Full Control is not supported in the mobile SDK.
- In Stealth mode, the launch point displays after holding two or three fingers on the screen for 2 to 3 seconds, and then releasing. The number of fingers you should hold down depends on the make and model of your device, and individual settings.

**Note:** The Cobrowse Admin Console is best accessed on a computer rather than a mobile device.
17 Cobrowse Agent Training

Best Practices for Cobrowse Agent Training

An effective agent training and roll-out program for Cobrowse will include these elements.

- Scripting ideas for how to introduce the option to cobrowse with a customer (for example, “Let’s cobrowse so we can do this together” or “We can use our Cobrowse feature so I can show you”).
- Examples of use cases where Cobrowse is envisioned as an effective tool, along with guidance that it’s not a tool for every call.
- An overview of any security and privacy settings applied to the deployment (for example, “You won’t be able to cobrowse on these pages…” or “You can cobrowse PDF documents, but nothing else on the customer’s desktop”).
- Role-playing as part of the training – this is mission-critical to ensure that agents are comfortable and confident in usage of the Cobrowse tool.
- A printed tips sheet is an effective roll-out mechanism to cover the basics, like how to start a session, or what can and can’t be cobrowsed.
- A collaborative roll-out campaign is a great way to bring attention to the tool – encourage agents to share use case stories, circulate these and reward agents willing to be early adopters.
- Agent focus groups early on will help you identify any questions or concerns about the Cobrowse tool that can be addressed with updated training.
- Agent surveys are a great way to capture ongoing feedback to enhance training programs.
- Monitor usage reports to identify agents with high usage rates – these are important resources to get feedback from that can be circulated to the full team to encourage usage.

Log In to the Agent Console

Follow this procedure to log in to the Agent Console.

1. Do one of the following:
   - Click the Agent Widget icon on your system tray if it has been installed. The widget may be installed through Install Agent Widget.
   - Access the Agent Console URL at Oracle Digital Engagement Channels Administrative Console Login.
2. Enter your login. This is your email, or, if your company uses single sign-on (SSO), this is your alphanumeric SSO login.
3. Enter your password.
   - Note: If you forgot your password, you can click the Forgot Password link, or you can request a password reset by visiting LiveLOOK Forgot Password. An email will be sent to you.
4. Click Continue.
   - The Agent Console opens.
Launch a Cobrowse Session

When a customer calls for assistance, you may determine that the customer’s issue would be solved more quickly or efficiently if you could see the customer’s screen.

With your Agent Console open, you can invite the customer to start a cobrowse session using company-approved scripting (for example, “Let’s start a cobrowse session so I can walk you through this more quickly.”).

1. **Enter your name on the Agent Console.**
   
   Your name displays automatically after the first time you enter it on the Agent Console.

2. **Ask the customer to click the Cobrowse button on your company website.**
   
   **Note:** How this button displays can be customized and branded by your company. It can be displayed as a hovering button (best practice), a link, or an icon. It can be displayed on every page of the site (best practice) or displayed on a contact page. The button may be labeled Cobrowse, Live Help, or whatever the company has chosen.

3. **Ask the customer to read the 6-digit Session ID code displayed in the cobrowse window.**
   
   The cobrowse window minimizes automatically after a few seconds, but the 6-digit code remains visible to the customer.

4. **Enter the 6-digit Session ID code onto the Agent Console.**

5. **Click Connect to start the cobrowse session.**

   The customer can see that the session is connected by the green dot that appears on the Cobrowse button.

How You Cobrowse with a Customer

While cobrowsing with a customer, you use the controls and information on the Agent Console.

Your viewing and cobrowsing options are limited depending on how your company has set up the Cobrowse deployment. Privacy settings can differ when you cobrowse in Instant Cobrowse mode or Advanced Cobrowse mode. Your company’s Cobrowse administrator configures the privacy settings.

In Instant Cobrowse Mode, only company web pages may be viewable. Options available are View Only and View + Pointer. Depending on how your company is set up, the Full Control option may also be available in Instant Cobrowse mode.

In Advanced Cobrowse mode, privacy settings may be configured to limit cobrowsing to specific web pages, the browser only, or specific applications. All other applications and the customer’s desktop can be masked. Additionally, specific fields on the page you are cobrowsing can be masked for the customer’s privacy, such as social security or credit card numbers. Options available are View Only, View + Pointer, and View + True Pointer. Depending on how your company is set up, the Full Control option may also be available.

<table>
<thead>
<tr>
<th>Button/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID Code</td>
<td>The Session ID code displays so that additional agents or subject matter experts can be asked to join the active session if needed.</td>
</tr>
</tbody>
</table>
## Button/Field Description

<table>
<thead>
<tr>
<th>Button/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the session connection displays, alerting the agent to any connectivity issues that may cause the session to proceed slowly or cause disruption.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL of the customer's current web page displays. Click the drop-down menu to select a URL in the customer’s history for the active window. The drop-down menu is available only in Full Control state.</td>
</tr>
<tr>
<td>Mode</td>
<td>Click to select a cobrowse state, which specifies how much control you have over the customer’s active window. Not all states may be available. Your company administrator defines the states available to you when cobrowsing in Instant or Advanced Cobrowse modes.</td>
</tr>
<tr>
<td>View Only</td>
<td>Select to view the active window. This option is selected by default in Advanced Cobrowse mode.</td>
</tr>
<tr>
<td>View + Pointer</td>
<td>Select to view the customer’s active window and use a labeled mouse as a pointing device on the customer’s screen. With this option selected, mouse-click functionality does not work on the customer’s active window. This option is selected by default in Instant Cobrowse mode.</td>
</tr>
<tr>
<td>View + True Pointer</td>
<td>Select to view the customer’s active window and control the movement of the customer’s mouse or other pointing device. With this option selected, mouse-click functionality does not work on the customer’s desktop.</td>
</tr>
<tr>
<td>Full Control</td>
<td>Select to view the customer’s active window, control all mouse or other pointing device functions (pointer and mouse clicks), navigate to other company web pages, and use your keyboard to enter information on the customer’s active window (for instance, to help the customer fill out a form). In Advanced Cobrowse mode, you can access the customer’s desktop and cobrowse third party sites. The customer receives a consent message to allow or deny full control.</td>
</tr>
<tr>
<td>Advanced Mode</td>
<td>Click to escalate to the Advanced Cobrowse mode.</td>
</tr>
<tr>
<td>Client Info</td>
<td>Displays the customer’s environment information for operating system, browser version, client version, and escalation mode. This information may be helpful if there is a technical problem.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Click to end the cobrowse session.</td>
</tr>
<tr>
<td>True View</td>
<td>True View is enabled by default and lets you view the customer’s desktop exactly as it is seen by the customer when in Instant Cobrowse mode. Click to turn True View off in situations where the customer’s settings prevent you from navigating efficiently.</td>
</tr>
<tr>
<td>Zoom In</td>
<td>Click to zoom in on the customer’s desktop. This button is available only in Advanced Cobrowse mode.</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>Click to zoom out on the customer’s desktop.</td>
</tr>
</tbody>
</table>
# Escalate to Advanced Mode

In certain cases, you will need to escalate to Advanced Cobrowse mode in order to assist a customer.

Reasons to escalate to Advanced Cobrowse mode include the following.

- You need to see content that resides outside of the corporate website pages visible in Instant Cobrowse mode (for example, a desktop application, a document, or a third-party resource website).
- On-page elements are not displaying properly in Instant Cobrowse mode (for example, with Flash, dynamic content, or Silverlight).

1. Click **Advanced Mode**.
   An invitation is sent to the customer to activate Advanced Cobrowse mode.

2. Follow the instructions that appear on the **Agent Console** to help you guide the customer through any next steps that might be necessary to activate Advanced Cobrowse mode.
   Advanced Cobrowse mode uses one of three technologies to run, depending on the customer’s environment, including Java which may require the customer to activate it within the browser.

---

### End a Cobrowse Session

Both the agent and customer can end a Cobrowse session at any time.

Click **Disconnect** at the top of the Agent Console. Customers can click **Disconnect** on the cobrowse button displayed on their screen.

Oracle Standalone Cobrowse includes an option to display a survey to both customers and agents after the cobrowse session. If your company has included this option, a survey URL appears in the **Session Ended** window enabling the participants to complete the survey.
18 Working with Reports

Work with Reports

The Reporting tab contains reports for agents and administrators of the selected company as well as agents of all sub-companies.

The reports include session number, session type (Instant or Advanced), start time, end time, and agent name. User reports include only information for the user, while Company reports list data for the company as a whole, and the Audit report is a record of management and configuration changes made by an administrator.

1. Click Reporting.
2. To view just your own reporting data, click User Reports > Co-Browse.
   The report includes summary information on the number of sessions run and the number of total minutes, as well as details for individual sessions.
   a. Click the arrows on any field headings to sort the reports by that field.
   b. Click Export to export the data in a csv format.
3. To view reporting data for the company you are working with, click Company Reports > Co-Browse.
   See Select a Company to change the company you are working with.
   a. Enter filtering criteria and click Run Report.
      
        Note: If a session escalates from an ICB to an ACB session, two records will be written into the report table as separate sessions.
      
   b. Click Export Data to export the data in a .csv file format.
4. To view a record of configuration or management changes, click Audit Reports.

Use an ExtKey Code

Oracle Cobrowse can support the inclusion of custom parameters within Cobrowse session reporting.

The Oracle Cobrowse launcher package must be included on a web page for custom parameter reporting to work properly.

The values of such parameters are generated by the hosting party, and should be passed to the Oracle Cobrowse application when a cobrowsing session is initiated. The information captured in this type of custom parameter has specific meaning for the hosting party. For example, custom parameters can be used to map a specific user session on a hosting party website with a specific cobrowsing session.

While custom parameter values are typically utilized to enable the company to uniquely identify a particular user session, it should be configured to not expose any private user information. When a custom parameter value is passed to the Oracle Cobrowse application prior to the start of a Cobrowse session, this value will be displayed in a dedicated column within Cobrowse reports.

1. Use JavaScript code for the custom parameter value to be passed to the Oracle Cobrowse reporting system.
The code should be executed before the cobrowsing session is initiated. To run this code after the web page (and the Oracle Cobrowse launcher package) is loaded, we recommend using the `Cobrowse.ready` function as in the example below.

```javascript
Cobrowse.ready().then(function(){
  Cobrowse.API.setReportingId({ "extKey": "THE_VALUE_FOR_REPORTING" });
});
```

2. Open a report with the ExtKey parameter.
   The value which was passed as an ExtKey parameter will be displayed in the report in a dedicated ExtKey column.
19 Viewing Statistical Data

View Statistical Data

The Statistics area provides access to statistical information on ICB Cobrowse sessions for the company you are working with.

The data include agent connection time statistics and the number of Cobrowse button clicks on a customer website/number of Cobrowse sessions. See Select a Company to change the company you are working with.

1. Click Statistics > Statistics.
   The Statistics window opens.
2. Select Connection Time or Curiosity Clicks from the data you are interested in drop-down menu.
3. Specify the data time interval, statistics display type, and the maximum number of entries you want displayed.
   The data display.
4. Click Previous or Next to view additional data pages.
20 Troubleshooting

Troubleshooting Tips

Review these troubleshooting tips for issues that can occasionally come up during implementation, configuration and maintenance of a Cobrowse deployment.

- A Cobrowse session was lost on the customer side when transitioning from one page to another. The UI with the session code is no longer displayed on the customer’s side; the agent sees a dialog with a message: 'Customer navigated away, or is experiencing network issues.' See Possible Reasons and Resolutions for Lost Cobrowse Session for troubleshooting tips.

- Agent sees a white screen instead of the customer’s page, or the agent is stuck on the screen with the message 'Establishing secure connection... Please wait.' UI on the customer's side indicates that the agent is connected (the green icon near the presentation code is present), but the agent console cannot actually connect. See Possible Reasons and Resolutions for Agent Connection Issue for troubleshooting tips.

Possible Reasons and Resolutions for Lost Cobrowse Session

These are possible reasons and resolutions for a lost Cobrowse session.

- The page belongs to a third-party website, where the Cobrowse launcher script is not deployed by design.

  Resolution—Make configuration changes in V4 configuration on the Admin Console (restrict ICB URLs to show which domains and/or pages should be supported; redirects to other pages will open a new browser tab and will not disrupt active sessions).

- The page belongs to a domain which should be supported, but the script is not present on the page due to deployment misconfiguration. The session cannot be initiated on this page; the UI is not visible, and does not come up after the customer presses Ctrl+Enter, or by clicking the link which initiates the cobrowsing session.

  Resolution—The Cobrowse launcher package should be deployed on all pages where sessions should be supported.

- The browser is Internet Explorer, and the session was lost because the two pages belong to different security zones (Tools > Internet Options > Security). The session is lost in transition from a less-restrictive security zone like 'Trusted sites' or 'Intranet' to a more restricted zone like 'Internet' or 'Restricted'; non-IE browsers like Google Chrome do not lose the session in the same transition.

  Resolution—All the domains in the session should belong to the same security zone in Internet Explorer.

- The customer’s browser is specifically restricted to disallow localStorage, cookies, and any other means of storing session information.

  Resolution—Allow localStorage access in the browser configuration.
Possible Reasons and Resolutions for Agent Connection Issue

These are possible reasons and resolutions for agents seeing a white screen or stuck on the connection screen.

- Connection to Oracle Cobrowse grid servers (*.livelook.net) is prohibited either on the customer's network, or in the network on the agent side.

  Resolution—Change firewall/security configuration to allow https connections to *.livelook.net.

- Customer is on https:// link, but the page has security certificate errors clearly visible in the browser (an expired or invalid https certificate is usually indicated by a strucked-through https icon or red-colored URL bar).

  Resolution—Resolve the security certificate problems, or test ICB in another environment.
21 Accessibility and Support

Cobrowse Accessibility

Cobrowse is natively accessible, and does not require any specialized configuration or setup to enable accessibility.

Support

Support is available.

If you need support, visit our support site.