Oracle Service Cloud
Securing Service Cloud
This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display in any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

The business names used in this documentation are fictitious, and are not intended to identify any real companies currently or previously in existence.
# Oracle Service Cloud

## Securing Service Cloud

### Contents

- **Preface**

- **1 Understanding Oracle Service Cloud Security**
  - Overview: Oracle Service Cloud Security and Compliance
  - Network and Hosting Infrastructure
  - Developing a Security Plan
  - Configuring the Administration Interface
  - Using Role Access to Define Permissions
  - Email Security
  - Abuse-Detection Security

- **2 Configuring Security-Related Settings**
  - Overview: Security-Related Configuration Settings
  - Security Level
  - Security Significance
  - Site Protection
  - Clickjacking Protection
  - Cross-Site Request Forgery
  - Specifying Valid Redirect Domains
  - Session Data
  - File-Attachment Security
  - Chat Security
  - Server Protection
  - Chat API
  - External Queues
  - Social Experience Security
  - Channels
  - Social Monitor
  - Self Service for Facebook Authentication
  - Twitter Security
  - Open Login Credentials for Social Accounts

---

**ORACLE**
3 Managing Customer and Staff-Member Passwords

- Protecting Passwords 31
- Enforcing Password Requirements 31
- Securing Customer Passwords 32
- Configuring Staff-Member Passwords 33
- Recovering Forgotten Passwords 34

4 Deploying Oracle Service Cloud in a Restricted Environment

- Implementing Oracle Service Cloud in a Controlled Environment 35
- Before You Begin: Reviewing Important Support Documentation 35
- Understanding Supplemental Controls and Policies 36
- Complying with Third-Party Standards 37
- Using Oracle Service Cloud Components in Controlled Environments 38

5 Deploying PCI and HIPAA

- Protecting Data 41
- Securing Access Control 41
- Auditing and Logging 42
- Securing Mobile Access 43
- Evaluating PCI Vulnerability 44
- Securing Integrations and Accelerators 44
- Incident Thread Masking 45
- Securing Email, Outreach, and Surveys 45
- Securing Analytics 46
- Securing Chat 46
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 Accessibility

For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website. 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 Oracle Service Cloud Support or visit Accessible Oracle Support 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 Understanding Oracle Service Cloud Security

Overview: Oracle Service Cloud Security and Compliance

An important part of product security is your diligence in configuring Oracle Service Cloud and your vigilance in its use. Security is a changing landscape with new attack methods continuously developing, many of which are based on social engineering that takes advantage of user trust. The protection of our customers’ assets is a high priority at Oracle. We strive to make your Oracle Service Cloud experience secure by holding ourselves to industry-standard security and privacy requirements in our software development practices and operational methods. For added protection, Oracle Service Cloud can be hosted within our community cloud environments that align with well-known regulatory control frameworks.

See Implementing Oracle Service Cloud in a Controlled Environment, and the sections that follow it, for guidance when deploying Oracle Service Cloud in a regulated environment.

Network and Hosting Infrastructure

Oracle uses “defense in depth” with multiple levels of security crafted to protect everything in the hosted environment from the network infrastructure to the software.

Oracle Service Cloud sites are hosted in security-hardened pods where each is protected by redundant firewalls and a demilitarized zone architecture. All major services, which include web, database, and mail services, are separately hosted and load balanced. The pods are audited daily, both internally and externally, and every quarterly software release is subjected to a third-party audit. In addition, a dedicated security staff monitors all systems for events that could jeopardize system reliability or data integrity.

Developing a Security Plan

When configuring your Oracle Service Cloud site, your goal is to obtain the maximum effectiveness for your staff and your customers, while ensuring that your site is safe from threats.

Although Oracle Service Cloud is designed and implemented with the highest levels of security, we recognize that our customers’ needs vary. Therefore, we offer configuration options that let you accept various levels of risk. Your sensitivity to those risks should dictate the configuration and management options you use in your site.

Note: Never assume that your security system is foolproof. New attacks are designed every day, so you should expect that any weakness will eventually be exploited. Ongoing vigilance and process improvement are required to minimize risk.
Common Security Threats

Risks to using a web-facing software product like Oracle Service Cloud to collect and store data include but are not limited to:

- Data leaks to unauthorized persons.
- Attacks to subvert security measures.
- Vandalism of the host site.
- Attacks against site users.

Security Considerations

To start developing your security plan, we’ve compiled a list of questions and considerations that relate to the use of Oracle Service Cloud. Your answers should help determine the content of your security plan. Here are some things to consider.

- What type of data will you collect and store?
  - Is personal information such as name, address, telephone number, and email address collected?
  - Is medical or financial information collected and stored?
  - Are there required data security standards or certifications, such as HIPAA or PCI?

- What methods will be used to obtain the data?
  - Does information come over the Internet or a private intranet?
  - Does information come from a voice-based system?

- What is the access method for the data?
  - Are users required to provide credentials, such as a user name and password, or is data openly available?

- What are the risks associated with compromised data?
  - What is the monetary cost?
  - What is the non-monetary cost, such as loss of reputation?
  - Are there legal ramifications?

- Who are your user groups?
- What authentication methods are available and which should be used for each type of user?
- For each type of data, which types of users should have access and how should the authorization be accomplished?
- What communication methods will be used and what efforts should be made to protect communication from being compromised?

While there are many resources available that can help you develop security policies and procedures, keep in mind that you should rely only on those resources that you find reliable and trustworthy. If you want to read more about security, here are some suggestions.

- Writing Information Security Policies by Scott Barman
- Information Security Policies and Procedures by Thomas Peltier
- SANS Institute — for information about security training and security certification
- OWASP — A nonprofit organization focused on improving software security
Chapter 1
Understanding Oracle Service Cloud Security

Configuring the Administration Interface

Properly configuring the administration interface is critical to your site security because staff members can be granted permission to view and modify virtually everything in an Oracle Service Cloud site, including your site controls and data.

Oracle Service Cloud uses role-based access control through profile permissions, navigation sets, and workspaces that you define. All staff members are assigned a profile that is associated with a navigation set and one or more workspaces.

- **Navigation sets**—A navigation set is a combination of navigation buttons and their associated navigation lists. Each navigation list contains unique reports and items based on staff member responsibilities, and every profile must include a navigation set that all staff members with that profile use when working in Oracle Service Cloud. By carefully examining staff member responsibilities before you create navigation sets, you can grant access to functionality to only those individuals who require it.

- **Workspaces**—Workspaces define the appearance of the agent desktop when staff members add, view, and edit records in Oracle Service Cloud. Each profile has one or more workspaces that can be designed to provide only the functionality that is needed by the staff member. Along with navigation sets, workspaces provide macro-level control over access rights.

- **Profile permissions**—Profiles let you control what areas of Oracle Service Cloud your staff members can access and what specific actions they can perform in those areas.

> **Note:** You must create navigation sets before profiles in order for staff members to have access to reports and other components. In addition, if you use custom workspaces, we recommend creating them before creating profiles so you can assign the workspaces to specific profiles.

**Related Topics**
- Overview: Navigation Sets
- Create a Navigation Set
- Assign a Navigation Set to a Profile
- Overview: Workspaces
- Custom Workspaces
- Customizing Profiles

Using Role Access to Define Permissions

Setting permissions carefully and thoughtfully greatly enhances the security of your site. This is particularly true regarding administrator permissions, which typically let staff members edit configuration settings and administrative controls.
One method for determining the permissions you grant is to use a role-access method. While no contrived set of roles will represent any organization perfectly, the four job types used here demonstrate a general scenario of how permissions might be set up.

- Administrator—Staff member with access to all functionality.
- Supervisor—Staff member with supervisory responsibilities but no responsibility for configuring your site.
- Staff member—Staff member with access to data but no administrative controls.
- Developer—Staff member with access to development and integration interfaces.

This table doesn’t contain a complete list of all the permissions available, but provides an abbreviated set representing those permissions with direct security ramifications.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Functionality</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>See Select Administration Permissions</td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>Create and edit these items:</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>• Custom Fields</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mailboxes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Currencies and Exchange Rates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service Level Agreements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Response Requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chat Hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Quote Templates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Territories</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Promotions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strategies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sales Periods</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• External Suppression List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Thread Type Correction</td>
<td></td>
</tr>
<tr>
<td>Groups/Accounts/Distribution Lists</td>
<td>Access staff accounts and distribution lists.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Groups/Accounts/Distribution Lists</td>
<td>Access log files under Site Configuration.</td>
<td>Administrator</td>
</tr>
<tr>
<td>System Error Log</td>
<td>Access log files under Site Configuration.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Workspace Designer</td>
<td>Access Workspaces and Workflows explorers and designers.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Scripting</td>
<td>Create and edit agent scripts.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Object Designer</td>
<td>Create custom objects.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Setting</td>
<td>Functionality</td>
<td>Roles</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Message Templates</td>
<td>Customize administrator notifications, administrator emails, and contact emails.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Access Control</td>
<td>Access the Access Control editor to configure staff and customer settings permissions for Community Self Service.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>CP Promote</td>
<td>Promote customer portal pages from the staging area to the production area.</td>
<td>Administrator, Developer</td>
</tr>
<tr>
<td>CP Stage</td>
<td>Copy customer portal development files to the staging area.</td>
<td>Administrator, Developer</td>
</tr>
<tr>
<td>CP Edit</td>
<td>Access the Customer Portal Administration site and edit customer portal pages in the development area using WebDAV.</td>
<td>Administrator, Developer</td>
</tr>
<tr>
<td>Rules View</td>
<td>View business rules.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff member</td>
</tr>
<tr>
<td>Data Import</td>
<td>Import data, including answers, contacts, incidents, organizations, and custom objects.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>Process Designer</td>
<td>Create custom processes.</td>
<td>Administrator, Developer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supervisor, Staff member</td>
</tr>
<tr>
<td>Virtual Assistant Edit</td>
<td>Access to configuration of the virtual assistant.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Broadcast Notifications</td>
<td>Send messages to other staff members.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>Configuration</td>
<td>Access to these areas and functionality:</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>• Password Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuration Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuration Wizard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Message Bases</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• File Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add-In Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Email Address Sharing</td>
<td></td>
</tr>
<tr>
<td>Business Process Settings</td>
<td>Define interface appearance and functionality, including:</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td></td>
<td>• Navigation Sets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customizable Menus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Countries</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Functionality</td>
<td>Roles</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------</td>
</tr>
<tr>
<td>Rules Edit</td>
<td>Edit business rules.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>Profiles</td>
<td>Add and edit profiles.</td>
<td>Administrator</td>
</tr>
<tr>
<td>SSO Login (SAML 2.0)</td>
<td>Allows login only through an identity provider, that is, using a single sign-on process. Oracle Service Cloud uses the SAML 2.0 protocol for single sign-on.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Skill Edit</td>
<td>Access to configuration of advanced routing.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>Agent Browser User Interface</td>
<td>Access to the Oracle Service Cloud using the Agent Browser UI through account authentication.</td>
<td>Administrator, Supervisor, Staff member</td>
</tr>
<tr>
<td>Public SOAP API</td>
<td>Access the public SOAP API through account or session authentication.</td>
<td>Administrator, Developer</td>
</tr>
<tr>
<td>Public Knowledge Foundation API</td>
<td>Access the public Knowledge Foundation API through account or session authentication.</td>
<td>Administrator, Developer, Supervisor, Staff member</td>
</tr>
<tr>
<td>Organizations—See &gt;Select Organizations Permissions</td>
<td>Add, edit, delete, and view organizations.</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>Edit and view organizations.</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>View organizations.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Contacts—See Select Contacts Permissions</td>
<td>Add, edit, delete, view, and move contacts.</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>Add, email, edit, delete, and view contacts.</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>Email, edit, and view contacts.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Service—See Select Service Permissions</td>
<td>Add, edit, view, and delete incidents; propose incidents as answers; respond to incidents.</td>
<td>Administrator, Supervisor</td>
</tr>
<tr>
<td>Setting</td>
<td>Functionality</td>
<td>Roles</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Answers</td>
<td>Add, edit, and delete answers; set answers to public status.</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>Add and edit answers.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Asset</td>
<td>Add, edit, delete, and view assets.</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>View and edit assets.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Opportunities—See</td>
<td>Create, edit, delete, view, respond to leads, and send quotes.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Select Opportunities Permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create, edit, and view leads, and send quotes.</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>View leads and send quotes.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Outreach—See Select</td>
<td>Create, edit, delete, and view mailings, campaigns, documents, templates,</td>
<td>Administrator</td>
</tr>
<tr>
<td>Outreach Permissions</td>
<td>snippets, file attachments, tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit and view mailings, campaigns, documents, templates, snippets, file</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>attachments, tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View mailings, campaigns, documents, templates, snippets, file attachments,</td>
<td>Staff member</td>
</tr>
<tr>
<td></td>
<td>tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td>Feedback—See Select</td>
<td>Create, edit, delete, and view surveys, questions, documents, templates,</td>
<td>Administrator</td>
</tr>
<tr>
<td>Feedback Permissions</td>
<td>snippets, file attachments, tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit and view surveys, questions, documents, templates, snippets, file</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>attachments, tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View surveys, questions, documents, templates, snippets, file attachments,</td>
<td>Staff member</td>
</tr>
<tr>
<td></td>
<td>tracked links, segments, and contact lists.</td>
<td></td>
</tr>
<tr>
<td>Tasks—See Select</td>
<td>Create, edit, delete, and view tasks.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Tasks Permissions</td>
<td>Edit, view, and delete tasks.</td>
<td>Supervisor</td>
</tr>
<tr>
<td></td>
<td>View tasks.</td>
<td>Staff member</td>
</tr>
<tr>
<td>Analytics—See Select</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics Permissions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Setting | Functionality | Roles
--- | --- | ---
Create, edit, view, customize, print, export, and forward reports. | Administrator |
Edit, view, customize, print, export, and forward reports. | Supervisor |
View, edit, print, export, and forward reports. | Staff member |

Email Security

Although most email sent over networks is not encrypted, we recommend encrypting all data that you deem sensitive.

Oracle Service Cloud is designed to prevent the inadvertent release of information, but there are also a number of configuration settings related to email that you can use to increase your protection.

Certificates

Secure sockets layer (SSL) protocol provides encryption services for client-server communication security. To accomplish this, digital certificates are used to convey identification information and encryption keys. Since all agent desktop communication is over SSL, your site already uses a certificate issued by Oracle. This certificate can be used for other secure communication links, including staff member and customer access and email. See Configure SSL Security Settings, Configure SMIME Security Settings, and Certificate Validation Options.

For a discussion about the configuration settings you can use to protect your site and improve your security, see Site Protection.

Emailing Links to Answers

You can email links to answers from the customer portal or the administration interface. If a login is required for customers to access an answer, a user name and password will be required.

Answer visibility depends on who is trying to access the answer—a customer or a staff member—and where they are accessing it from—the customer portal or the administration interface. From the customer portal, visibility is controlled by a number of fields, including the Status field, which is defined on the administration interface. For example, if an answer status has been set to Private, then that answer is not visible to customers. See Controlling Answer Visibility.

For customers accessing answers from the customer portal, each answer link is protected by a security token with a limited lifetime that is defined in the configuration setting SEC_EU_EMAIL_LINK_EXPIRE. The default value is eight hours, meaning that a customer has eight hours to click the link and read the information published in the answer. We recommend using this security token to limit the time answers are available to customers. Because attackers need time to build phishing sites (for luring a user into clicking a link), the smaller the window of time you allow for access to your answers, the more secure your site will be.

For example, if an email with an answer link is copied by an attacker, access to the security token and the link has been compromised. If your site requires customers to log in to see an answer, the answer itself is safe, but the attacker can create a phishing scenario using a modified link that takes customers to an external site where their login credentials are stolen. It takes time to accomplish this, so the shorter the window of opportunity, the lower the likelihood of success. Setting the security token expiration in SEC_EU_EMAIL_LINK_EXPIRE helps discourage attackers. See Securing Customer Passwords.
From the administration interface, *profile* permissions control staff members’ access to answers. Permissions of the staff member who sends an email link to an answer do not transfer to the receiver, so data security is maintained.

**Abuse-Detection Security**

A potential threat to any website is a “denial of service” (DoS) attack where the attacker issues a large number of requests for service. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks and credit card payment gateways.

DoS attacks can slow the response time to legitimate visitors, overwhelm the database server, and generate excessive emails that interfere with normal operation. To prevent these attacks, Oracle Service Cloud provides web form and survey security through CAPTCHA, which automatically requires human validation when abuse is suspected. CAPTCHA validation is typically triggered only if there appears to be active abuse of a website. However, you can customize CAPTCHA requirements from the *customer portal*. See *Web Form and Survey Security* and *Web Form Security*.

**Related Topics**

- Require a CAPTCHA Validation on Every Submit
- Open the CAPTCHA Within a Form Instead of a Dialog
- Set the Abuse Detection Cookie
- Remove the ClickjackPrevention Widget from the Template
2 Configuring Security-Related Settings

Overview: Security-Related Configuration Settings

Certain configuration settings have a direct effect on security. Some affect the administration side of Oracle Service Cloud and others affect the customer portal or an external website.

By making a conscious decision to determine the appropriate level of security that fits your business, you can define configuration settings to reflect a suitable security level. Configuration settings that specifically impact security are detailed in the sections that follow. Paths to each setting in the Configuration Settings editor, descriptions, and default values are also listed. Configuration settings in this section are grouped into these categories.

- Site protection
- Session data
- Password protection
- File attachment security
- Chat security
- Social experience security

For a complete list of security-related configuration settings by security level and significance, see Security Level.

Note: Depending on your site’s configuration, some settings may be hidden. If you cannot find a certain configuration setting, contact your Oracle account manager.

Security Level

This table describes configuration settings that you should consider using or setting to achieve your designated level of security—high, medium, or low.

To make the settings easy to find, the list is ordered alphabetically with each setting’s respective path on the Configuration Settings editor.

<table>
<thead>
<tr>
<th>Path/Configuration Setting</th>
<th>For high-security environment</th>
<th>For medium-security environment</th>
<th>For low-security environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hidden</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAT_WS_API_IP_HOST</td>
<td>Set to allowed IP addresses and subnet masks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: To enable this hidden setting and define your allowed IP addresses and subnet masks, submit a service request on our support site.
<table>
<thead>
<tr>
<th>Path/Configuration Setting</th>
<th>For high-security environment</th>
<th>For medium-security environment</th>
<th>For low-security environment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chat/General/Server</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAT_CORS_WHITELIST</td>
<td>Set to allowed origins.</td>
<td>Set to allowed origins.</td>
<td>Blank (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow User Interface/General/Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIENT_SESSION_EXP</td>
<td>15 (default)</td>
<td>16 to 45</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td><strong>This setting is also used in the desktop usage administration feature.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow User Interface/Customer Portal/Login</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_CONTACT_LOGIN_REQUIRED</td>
<td>Yes</td>
<td>Yes</td>
<td>No (default)</td>
</tr>
<tr>
<td>CP_COOKIES_ENABLED</td>
<td>Yes (default) for all security environments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_FORCE_PASSWORDS_OVER_HTTPS</td>
<td>Yes (default)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CP_LOGIN_COOKIE_EXP</td>
<td>5 to 30</td>
<td>31 to 60 (default = 60)</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow User Interface/General/Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_LOGIN_MAX_TIME</td>
<td>As needed for all security environments (default = 0).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow User Interface/Customer Portal/Login</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_MAX_LOGINS</td>
<td>As needed for all security environments (default = 0).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_MAX_LOGINS_PER_CONTACT</td>
<td>0 (default)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common/General/Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP_REDIRECT_HOSTS</td>
<td>As needed for all security environments (default = blank).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow User Interface/General/End-User</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU_CUST_PASSWD_ENABLED</td>
<td>Yes (default)</td>
<td>Yes (default)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RightNow Common/Service Modules/Oracle Email</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EGW_PASSWD_CREATE</td>
<td>Yes (default)</td>
<td>Yes (default)</td>
<td>No</td>
</tr>
</tbody>
</table>
### Chapter 2

**Configuring Security-Related Settings**

<table>
<thead>
<tr>
<th>Path/Configuration Setting</th>
<th>For high-security environment</th>
<th>For medium-security environment</th>
<th>For low-security environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>EGW_SECURE_UPDATE_MODE</td>
<td>2 (default)</td>
<td>2 (default)</td>
<td>1</td>
</tr>
</tbody>
</table>

#### RightNow Common/3rd-Party Applications/Facebook

<table>
<thead>
<tr>
<th>FACEBOOK INCIDENTS_ENABLED</th>
<th>No (default = Yes)</th>
<th>As needed.</th>
<th>As needed.</th>
</tr>
</thead>
</table>

#### RightNow User Interface/Open Login/Oauth Apps

<table>
<thead>
<tr>
<th>FACEBOOK_OAUTH_APP_ID</th>
<th>Facebook application ID for all security environments (if Facebook is enabled).</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACEBOOK_OAUTH_APP_SECRET</td>
<td>Facebook secret key for all security environments (if Facebook is enabled).</td>
</tr>
</tbody>
</table>

#### RightNow User Interface/General/File Attach

<table>
<thead>
<tr>
<th>FATTACH_MAX_SIZE</th>
<th>As small as practical for your needs. Applies to all security environments (default and maximum allowable limit = 20 MB).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip: Consider the types of attachments that will be uploaded to your site, and then set this value to allow the minimum disk space that you need. As far as security goes, the more disk space you can fill, the better.</td>
<td>Note: File upload fails if the upload takes more than 5 minutes.</td>
</tr>
<tr>
<td>FATTACH_OPEN_ENABLED</td>
<td>No (default)</td>
</tr>
</tbody>
</table>

#### Chat/General/Create Incident

<table>
<thead>
<tr>
<th>INC_PRIVATE_TRANSCRIPT_ONLY</th>
<th>Yes</th>
<th>Yes</th>
<th>No (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGIN_SECURITY_MSG</td>
<td>As needed for all security environments (default = blank).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### RightNow User Interface/Contact Services/Security

<table>
<thead>
<tr>
<th>MYSEC_AUTO_CUST_CREATE</th>
<th>No (default = Yes)</th>
<th>No</th>
<th>As needed.</th>
</tr>
</thead>
</table>

#### Common/General/Security

<table>
<thead>
<tr>
<th>SEC_BROWSER_USER_AGENT</th>
<th>Set to allowed user agent strings.</th>
<th>Blank (default)</th>
<th>Blank (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC_EU_EMAIL_LINK_EXPIRE</td>
<td>8 (default)</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>SEC_INVALID_ENDUSER_HOSTS</td>
<td>Set to allowed IP addresses.</td>
<td>Blank (default)</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>Path/Configuration Setting</td>
<td>For high-security environment</td>
<td>For medium-security environment</td>
<td>For low-security environment</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>SEC_INVALID_USER_AGENT</td>
<td>Set to user agent strings that are not allowed.</td>
<td>Blank (default)</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>SEC_SPIDER_USER_AGENT</td>
<td>Set to list of known web spider user agent strings.</td>
<td>Blank (default)</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>SEC_VALID_ADMIN_HOSTS</td>
<td>Set to allowed IP addresses.</td>
<td>Set to allowed IP addresses.</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>SEC_VALID_CHAT_API_HOSTS</td>
<td>Set to allowed hosts and subnet masks for all security environments (default = blank).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC_VALID_ENDUSER_HOSTS</td>
<td>Set to allowed IP addresses.</td>
<td>Set to allowed IP addresses.</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>SEC_VALID_INTEG_HOSTS</td>
<td>Set to allowed IP addresses.</td>
<td>Blank (default)</td>
<td>Blank (default)</td>
</tr>
<tr>
<td>SESSION_HARD_TIMEOUT</td>
<td>12 (default)</td>
<td>12-24</td>
<td>As needed.</td>
</tr>
</tbody>
</table>

**RightNow User Interface/General/Security**

| SUBMIT_TOKEN_EXP | 30 to 60 (default = 30) | 30 to 300 | 30 to 1000 |

**RightNow User Interface/Open Login/Oauth Apps**

<table>
<thead>
<tr>
<th>TWITTER_OAUTH_APP_ID</th>
<th>Twitter application ID for all security environments (if Twitter is enabled).</th>
</tr>
</thead>
<tbody>
<tr>
<td>TWITTER_OAUTH_APP_SECRET</td>
<td>Twitter secret key for all security environments (if Twitter is enabled).</td>
</tr>
</tbody>
</table>

**Outreach and Feedback/General/Campaigns**

<table>
<thead>
<tr>
<th>WEBFORM_ID_BY_COOKIE_DEFAULT</th>
<th>As needed for all security environments (default = No).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBFORM_ID_BY_LOGIN_DEFAULT</td>
<td>As needed for all security environments (default = No).</td>
</tr>
<tr>
<td>WEBFORM_ID_BY_LOGIN_REQUIRED_DEFAULT</td>
<td>As needed for all security environments (default = No).</td>
</tr>
<tr>
<td>WEBFORM_ID_BY_URL_PARAM_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td>WEBFORM_SET_COOKIE_DEFAULT</td>
<td>As needed.</td>
</tr>
</tbody>
</table>
Security Significance

This table describes recommended security-related settings by significance. They are grouped by high, medium, and low in security significance.

<table>
<thead>
<tr>
<th>Significance</th>
<th>Configuration Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>CHAT_WS_API_IP_HOST</td>
<td>Set to allowed IP addresses and subnet masks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To enable this hidden setting and define your allowed IP addresses and subnet masks, submit a service request on our support site.</td>
</tr>
<tr>
<td></td>
<td>CLIENT_SESSION_EXP</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This setting is also used in the desktop usage administration feature.</td>
</tr>
<tr>
<td></td>
<td>CP_FORCE_PASSWORDS_OVER_HTTPS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CP_LOGIN_COOKIE_EXP</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>CP_REDIRECT_HOSTS</td>
<td>Set to allowed hosts or leave default setting (blank) to prevent all redirects outside of the interface domain, including external sites.</td>
</tr>
<tr>
<td></td>
<td>EU_CUST_PASSWD_ENABLED</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SEC_VALID_ADMIN_HOSTS</td>
<td>Set to allowed IP addresses.</td>
</tr>
<tr>
<td></td>
<td>SEC_VALID_CHAT_API_HOSTS</td>
<td>Set to allowed hosts and subnet masks.</td>
</tr>
<tr>
<td></td>
<td>SESSION_HARD_TIMEOUT</td>
<td>12</td>
</tr>
<tr>
<td>Significance</td>
<td>Configuration Setting</td>
<td>Recommended Setting</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Medium</td>
<td>CHAT_CORS_WHITE_LIST</td>
<td>Set to allowed origins.</td>
</tr>
<tr>
<td></td>
<td>CP_CONTACT_LOGIN_REQUIRED</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>CP_LOGIN_MAX_TIME</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>EGW_PASSWD_CREATE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EGW_SECURE_UPDATE_MODE</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>FACEBOOK_INCIDENTS_ENABLED</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>FATTACH_OPEN_ENABLED</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>INC_PRIVATE_TRANSCRIPT_ONLY</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SEC_EU_EMAIL_LINK_EXPIRE</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>SUBMIT_TOKEN_EXP</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>WEBFORM_ID_BY_COOKIE_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>WEBFORM_ID_BY_LOGIN_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>WEBFORM_ID_BY_LOGIN_REQUIRED_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>WEBFORM_ID_BY_URL_PARAM_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>WEBFORM_SET_COOKIE_DEFAULT</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>WIDGET_INSTALLATION_HOSTS</td>
<td>Set to allowed domain names.</td>
</tr>
<tr>
<td>Low</td>
<td>CP_COOKIES_ENABLED</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>CP_MAX_LOGINS</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>CP_MAX_LOGINS_PER_CONTACT</td>
<td>As needed.</td>
</tr>
</tbody>
</table>

**Note:** If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.
## Chapter 2
### Configuring Security-Related Settings

<table>
<thead>
<tr>
<th>Significance</th>
<th>Configuration Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FACEBOOK_OAUTH_APP_SECRET</td>
<td>As needed.</td>
</tr>
<tr>
<td></td>
<td>FATTACH_MAX_SIZE</td>
<td>As small as practical for your needs.</td>
</tr>
</tbody>
</table>

**Note:** Regardless of the file attachment limits you define, file upload will fail if the upload takes more than 5 minutes.

|              | LOGIN_SECURITY_MSG                    | As needed.          |
|              | MYSEC_AUTO_CUST_CREATE                | As needed.          |
|              | SEC_BROWSER_USER_AGENT                 | As needed.          |
|              | SEC_INVALID_ENDUSER_HOSTS             | As needed.          |
|              | SEC_INVALID_USER_AGENT                 | As needed.          |
|              | SEC_SPIDER_USER_AGENT                  | As needed.          |
|              | SEC_VALID_ENDUSER_HOSTS                | As needed.          |
|              | SEC_VALID_INTEG_HOSTS                  | As needed.          |
|              | TWITTER_OAUTH_APP_ID                   | As needed.          |
|              | TWITTER_OAUTH_APP_SECRET               | As needed.          |

**Related Topics**
- Search for a Configuration Setting
- Edit a Configuration Setting

## Site Protection

One of the most important steps you can take to protect your site is to limit access to the greatest extent possible while still meeting the requirements of your staff members and customers.

By restricting access to your site or certain functionality within your site, you can reduce opportunities for unwanted visitors with malicious intent to gain access to your assets. Configuration setting descriptions that affect your site’s protection are listed in the following two tables.
### Common/General/Security

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC_VALID_ADMIN_HOSTS</td>
<td>Defines which hosts can access the administration interface.</td>
<td>Blank</td>
</tr>
<tr>
<td>SEC_VALID_INTEG_HOSTS</td>
<td>Defines which hosts can access the integration interface. Only staff members who log in from the listed IP addresses, including network groups, can access the API interface.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### RightNow User Interface/General/Security

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT_SESSION_EXP</td>
<td>Requires staff members to log in again after a specified period of inactivity on the Service Console. To reduce the risk of a misappropriated agent session, we recommend keeping the default value of 15.</td>
<td>15</td>
</tr>
</tbody>
</table>

*Note:* This setting is not used strictly for security. It is also used in the desktop usage administration feature.

### RightNow User Interface/Tool Bar/General

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGIN_SECURITY_MSG</td>
<td>Defines a message to display after staff members click the Login button on the Login window. You can use this setting to issue a security statement, distribute terms of a use agreement, or any login message you want staff members to agree to before the Service Console opens.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### Common/General/Security

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP_REDIRECT_HOSTS</td>
<td>Defines which hosts are allowed as redirect targets from the customer portal. The default setting (blank) prevents all redirects outside of your interface domain. If you have more than one interface that you need to redirect to, each interface domain name must be specified in CP_REDIRECT_HOSTS.</td>
<td></td>
</tr>
</tbody>
</table>

*Blank = Prevents all redirects outside of your interface domain.*
Clickjacking Protection

Clickjacking is an attack on browser security that can mislead your customers into clicking a concealed link.

On a clickjacked page, attackers load another page in a transparent layer over your original page. Users think they are clicking visible buttons, while they are actually performing actions on the hidden page. The hidden page may even be an authentic one, such as a page from a well-known, reputable business. This makes it possible for attackers to trick your customers into performing unintended actions.
A common defense against clickjacking is to attempt to block the site you are trying to protect from being loaded into a frame.

The ClickjackPrevention widget, included by default in the standard and mobile templates, ensures that your customer portal cannot be viewed inside a frame or iFrame.

If you do not use frames, you can edit the standard.php file of your template file to minimize the risk of clickjacking. For the complete procedure, see Remove the ClickjackPrevention Widget from the Template.

For more information on clickjacking, including definitions for X-Frame-Options response headers, search for the Clickjacking Defense Cheat Sheet on the OWASP website.

Related Topics
- Preventing iFrame Security Issues
- Configuring the Standard Template

Cross-Site Request Forgery

Cross-site request forgery (CSRF) causes a user’s browser to load pages (including forms) that typically require authentication in an attempt to perform actions on behalf of the user.

If the user has a valid authenticated session for the site the attacker is causing to load into the browser, those requests will succeed. If proper protections are not in place, this may let the attacker perform unintended actions on behalf of the user.

Submit tokens ensure that the contact who opened the page is the only contact who can submit the form. The SUBMIT_TOKEN_EXP configuration setting lets you define the amount of time the submit token is valid and is set, by default, to expire 30 minutes from the time the token was sent. After 30 minutes, the contact will receive a new token. The expiration process is invisible to the contact making for a seamless user experience.

For more information about CSRF vulnerabilities, search for the CSRF Prevention Cheat Sheet on the OWASP website.

Specifying Valid Redirect Domains

Linking from one page to another is a security risk you should consider. For example, you may have placed a link in your URL to redirect users to different locations within your site.

Typically, these are links to other files on your site but they can also be links to another interface, either on your site or on an external site. Attackers can take advantage of redirects by creating URL links in these locations.

- Questions on your page
- Uploaded files
- Emails

In each of these scenarios, an attacker bets that users will click the link they create and be redirected to an external site where data can be maliciously harvested.
To protect your site from this type of attack, you can set the value of CP_REDIRECT_HOSTS to a list of interface domains that are legitimate redirect targets. The default value is blank, which limits redirects to pages only within your interface domain. Keep in mind that redirects to domains specified in related configuration settings are implicitly allowed.

This table displays sample values for CP_REDIRECT_HOSTS.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
<td>Prevents all redirects outside of your interface. (Default)</td>
</tr>
<tr>
<td>*</td>
<td>Allows all redirects. (Not recommended.)</td>
</tr>
<tr>
<td>*.example.com</td>
<td>Allows redirects to all sites in the example.com domain.</td>
</tr>
<tr>
<td>one.example.com, two.example.com</td>
<td>Allows redirects to sites one and two in the example.com domain.</td>
</tr>
<tr>
<td>example.custhelp.com, *.test.com</td>
<td>Allows redirects to example.custhelp.com and any interface in the test.com domain.</td>
</tr>
</tbody>
</table>

For information about securely publishing answer links on your site, see Email Security.

Session Data

To maintain state information about staff members and customers, we use session data that is passed between the staff member’s or customer’s system and the web server.

When an individual is logged in, data from the session can provide the necessary authentication for accessing your data that would not otherwise be available. Session data security prevents attacks that stem from the trust the system has in authenticated users. Without session data security, attackers may be able to capture session data and reuse it. These are commonly referred to as “replay” attacks or “man-in-the-middle” attacks.

The SESSION_HARD_TIMEOUT configuration setting helps reduce session exploitation by forcing staff members to reauthenticate after a specified period of time. Set to twelve hours by default, this setting creates a new session while destroying the previous session each time the staff member reauthenticates. See Forcing Session Expiration.

The CP_FORCE_PASSWORDS_OVER_HTTPS configuration setting is enabled by default and helps protect staff members and customers from malicious activity such as password theft. This setting requires that all login operations, such as login name and password, be performed over HTTPS. Therefore, logged-in users interact entirely on HTTPS.

Note: Pages that use passwords within standard widgets are automatically redirected to HTTPS.

If your site is password protected, you should require customers to log in to the customer portal. Even if only your answer pages are password protected, the CP_CONTACT_LOGIN_REQUIRED configuration setting enforces secure logon to your pages and controls on the customer portal. The CP_CONTACT_LOGIN_REQUIRED variable also prevents unauthenticated chat sessions.
Oracle Service Cloud offers different session management schemes for the administration interface and the customer portal. However, for both interfaces, we perform these actions:

- Encrypt session data stored in cookies.
- Set the Secure flag and the HTTP Only flag on cookies.
- Make session data difficult to use from a different computer system.
- Require staff members to reauthenticate after twelve hours. See the SESSION_HARD_TIMEOUT setting description in the first table.
- Require staff members to reauthenticate after a specified period of inactivity. See the CLIENT_SESSION_EXP setting description in the first table.
- Require all login operations to be performed over HTTPS. See the CP_FORCE_PASSWORDS_OVER_HTTPS setting description in the second table.

Configuration setting descriptions that affect your site’s session data are listed in these tables.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RightNow User Interface/General/Security</td>
<td>CLIENT_SESSION_EXP</td>
<td>Requires staff members to reauthenticate after a specified period of inactivity on the Service Console.</td>
</tr>
<tr>
<td>Note: This setting is not used strictly for security. It is also used in the desktop usage administration feature. See Controlling Desktop Usage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SESSION_HARD_TIMEOUT</td>
<td>Requires staff members to reauthenticate after a specified period of time. This setting creates a new session each time the staff member reauthenticates. The previous session is destroyed.</td>
<td>12 hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RightNow User Interface/General/Security</td>
<td>CP_LOGIN_MAX_TIME</td>
<td>Defines the time (in minutes) a customer can be logged in without needing to log in again. If a session goes past the defined setting, the customer is required to log in again. The default is 0, which means that the time is set by CP_LOGIN_COOKIE_EXP.</td>
</tr>
<tr>
<td>Configuration Setting</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CP_CONTACT_LOGIN_REQUIRED</td>
<td>Defines whether the customer portal requires a customer to be logged in when accessing most pages or controls. Also prevents unauthenticated chat sessions.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This setting does not apply to the login, password recovery, and account creation pages, or pass-through authentication (PTA). PTA is described in the Pass-Through Authentication Guide. If you do not have this guide, contact your Oracle account manager.</td>
<td></td>
</tr>
<tr>
<td>CP_COOKIES_ENABLED</td>
<td>Defines whether the customer portal tries to set cookies on a visitor’s browser.</td>
<td>Yes</td>
</tr>
<tr>
<td>CP_FORCE_PASSWORDS_OVER_HTTPS</td>
<td>Requires all login operations to be performed over HTTPS. Pages that use passwords within standard widgets are automatically redirected to HTTPS.</td>
<td>Yes</td>
</tr>
<tr>
<td>CP_LOGIN_COOKIE_EXP</td>
<td>The time (in minutes) before the customer portal login cookie expires. Set the value to -1 if you want the cookie to expire when the browser is closed. Set the value to 0 if you never want the cookie to expire.</td>
<td>60</td>
</tr>
<tr>
<td>CP_MAX_LOGINS</td>
<td>Defines the total number of concurrent users that can be logged in to your support site at any given time. A value of 0 means there is no limit. If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.</td>
<td>0</td>
</tr>
<tr>
<td>CP_MAX_LOGINS_PER_CONTACT</td>
<td>Defines the total number of active, concurrent logins a single user can be logged in with. A value of 0 means there is no limit. If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.</td>
<td>0</td>
</tr>
</tbody>
</table>
File-Attachment Security

Attachments that Oracle Service Cloud allows for incidents, answers, community questions and comments, and features that are used in mailings and surveys are a security concern because they can contain malicious code (malware) or data that is part of an attack on your site.

All incoming attachments are scanned for malware, but you should always consider the possibility that attackers could evade detection. Uploaded files containing HTML are a particular problem because they can provide links to sites that can harvest private data from unsuspecting people. For example, an attacker could upload a file that appears to be a link to an incident, but is actually a link to the attacker’s site, which prompts the receiver to enter user name and password credentials. Staff members should never follow a link unless they are confident that it is safe, and no data should ever be entered to a linked site. If it is necessary to access a referenced site, instead of clicking a link, look at the web address and verify that it goes where you think it should. Then type the correct web address into your browser.

The other problem with HTML files is that they may contain executable code in the form of JavaScript or ActiveX controls that potentially can have a significant impact on your system. If browser security works properly, this should not happen. However, browsers are one of the least secure types of software. You can disable some of this functionality, but you may need it for many complex sites or applications, including Oracle Service Cloud. Therefore, be careful when working with data from untrusted sources and educate your users about the risks associated with improper handling of uploaded files.

As an additional precaution, you can prevent attachment viewing by requiring that users download file attachments in order to be viewed. This protects the Oracle Service Cloud application as well as the associated data, and it also allows additional levels of scanning to be applied. The configuration setting FATTACH_OPEN_ENABLED lets staff members view attachments on the agent desktop. As a preventative measure, this setting is disabled. Disabling FATTACH_OPEN_ENABLED does not change the display of attachments for customers, so attachments from external sources can be verified as safe before they are placed in answers.

Even so, it is possible for a malicious user to create incidents with very large attachments that could be used to attack site. To prevent this, the configuration setting FATTACH_MAX_SIZE controls the maximum allowable attachment. The default (and the maximum allowable limit) is approximately twenty megabytes per attachment.

Note: Regardless of the file-attachment limits you define, file upload will fail if the upload takes more than five minutes.

To learn how to restrict the number of file attachments on the Ask a Question page, see Configure File Attachments.

This table describes configuration settings for file attachments.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FATTACH_MAX_SIZE</td>
<td>Defines the maximum file size in bytes that can be uploaded to the server as an attachment. File upload will fail if the upload takes more than five minutes.</td>
<td>20971520 (20 MB)</td>
</tr>
</tbody>
</table>

The maximum allowable limit is 20 MB.
<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FATTACH_OPEN_ENABLED</td>
<td>Lets staff members open file attachments on the agent desktop.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Tip:** Too much available disk space can make your site vulnerable to DoS attacks. Consider the types of attachments that will be uploaded to your site, and then set this value to as small as practical for your needs. As far as security goes, the more disk space you can fill, the better.

**Chat Security**

Oracle RightNow Chat Cloud Service (Chat) lets customers experience interactive, real-time conversations with agents. There are a number of configuration options that protect these exchanges of information and the underlying services that make them possible.

For complete details and procedures about configuring Chat see these topics:

- Chat for Agents
- Chat for Supervisors
- Chat for Customers

This table describes Chat configuration settings.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAT_WS_API_IP_HOST</td>
<td>Defines the list of IP addresses and subnet masks to make requests to the Chat API. If this setting is enabled and left blank, all hosts are allowed. To enable this hidden setting and define your allowed IP addresses and subnet masks, submit a service request on our support site.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Common/General/Security**

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC_VALID_CHAT_API_HOSTS</td>
<td>Defines which hosts and subnet masks of hosts are allowed to access the Chat SOAP interface from any chat-related request coming from a customer to the server.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Note:** If this setting is left blank, the server accepts requests from all hosts.
<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP_CONTACT_LOGIN_REQUIRED</td>
<td>When enabled, enforces secure logon to prevent unauthorized chat sessions.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Chat/General/Server**

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHATCors_WHITELIST</td>
<td>Defines the list of origins allowed to make cross-origin requests through the Chat server.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

> **Note:** If this setting is left blank, the server accepts requests from all origins.

**Chat/General/Create Incident**

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC_PRIVATE_TRANSCRIPT_ONLY</td>
<td>Allows chat transcripts to be added to incidents as private notes.</td>
<td>No</td>
</tr>
</tbody>
</table>

> **Note:** If enabled, customers cannot see past chats.

---

### Server Protection

The Chat SOAP interface can be protected from potential threats by restricting access to valid chat servers.

The configuration setting SEC_VALID_CHAT_API_HOSTS defines the list of IP addresses and subnet masks specifying the legal chat servers that are allowed to access the Chat SOAP interface. If this setting is left blank, all hosts are allowed.

Additionally, users can be protected from cross-origin resource sharing (CORS) attacks by defining the origins allowed to make CORS requests in CHATCors_WHITELIST. See “Cross-origin resource sharing protection” in Chat API.

### Chat API

Oracle Service Cloud supports a Chat API that must be enabled by Oracle. When enabled, the API is protected by a configuration setting that specifies the IP addresses and subnet masks to make requests to the Chat API. If this setting is enabled and left blank, all hosts are allowed.

> **Note:** Access to the Chat API is defined by the hidden configuration setting CHAT_WS_API_IP_HOST. To enable this setting and specify the IP addresses and subnet masks you want to allow, submit a service request on our support site.
User Protection

By enabling INC_PRIVATE_TRANSCRIPT_ONLY, you can change the privacy of the information in a Chat exchange. Instead of being added to an incident as public information, it is added as a private note, which restricts access to the data. If there is a chance that staff members will enter sensitive information during a chat session, this setting should be enabled.

It is also possible to configure Chat to allow off-the-record chats in which the exchanged data is not recorded and can be seen only in real time by the agent. See Configure Chat off the Record.

Cross-Origin Resource Sharing Protection

Cross-origin resource sharing (CORS) lets client-side code make requests from one origin to another origin. This functionality can be abused by an attacker to retrieve information from your site or to perform actions as a valid user. You can protect your site from potential threats by restricting access to valid requests. The CHAT_CORS_WHITELIST configuration setting defines the list of hosts or IP addresses allowed to make cross-origin domain requests. If this setting is left blank, all origins are allowed.

Tip: Keep in mind that restricting cross-origin resource sharing does not prevent cross-site request forgery (CSRF). For information about CSRF protection, see Cross-Site Request Forgery and Social Experience Security.

For more information about testing for CORS vulnerabilities, search “Test cross origin resource sharing” on the OWASP website.

External Queues

External chat queues allow sites outside of Oracle Service Cloud that use the Chat API to access Oracle Service Cloud chat data.

Since external queues may be subject to more risk, we recommend allowing only those external queues that are operationally necessary. To prevent potential misuse, you must add the chat queues that you deem acceptable from the Chat Session Queue editor on the Customizable Menus page. Then, you must designate those queues for use with third-party-initiated chat requests as external. Chat requests pre-routed to the external queues you define will be routed to agent desktops by an external routing system. The chat server and the external routing system exchange data through the third-party queue API. See Add or Edit a Chat Session Queue.

Social Experience Security

Oracle RightNow Social Experience (Social Experience) is your organization’s gateway to the social cloud and includes three features.

- Channels
- Social Monitor
- Self Service for Facebook
Related Topics

- Overview: Social Experience

Channels

When providing service through social media, it is essential to maintain the security and confidentiality of your organization’s social account logins.

For this reason, Oracle Service Cloud lets you define channel accounts, which are shared credentials that allow designated agents to perform service functions through your social media accounts by securely storing the account logins and passing authentication parameters on behalf of your agents. If you are currently providing service through social media channels directly through the web, we strongly recommend considering the security benefits of managing those efforts within Oracle Service Cloud instead. See Understanding Social Channels.

When monitoring certain channel types, Oracle Service Cloud can store your customers’ social media user names in their contact records. By tracking this identifying information, Oracle Service Cloud can associate incoming social monitor incidents with contacts based on their social media accounts. However, unlike channel accounts, channel types do not store passwords—they are used only to track the social identities of your customers across different services. See Storing Social Media User Names.

You may also want to consider SSL encryption options for social media services. Then traffic between Oracle Service Cloud and the social media site is encrypted. See Email Security.

⚠️ Note: Social Experience includes several APIs so you can access major social features from custom code. APIs offer tremendous flexibility, but it is important to recognize that accessing any part of Oracle Service Cloud through an API moves a significant part of the security responsibility to the external code.

Social Monitor

There are opportunities to access external data and code from within Social Experience, such as Oracle RightNow Social Monitor Cloud Service (Social Monitor).

Consequently, these features may not have the same level of security as Oracle Service Cloud and the exchange of data may not be secure. Configuring your site in a high-security environment requires special care when implementing social features.

Related Topics

- Overview: Social Monitor
Self Service for Facebook Authentication

Oracle RightNow Self Service for Facebook Cloud Service (Self Service for Facebook) lets you embed a set of Oracle Service Cloud service and community features directly on your organization’s Facebook page.

After you create a Facebook page, you must enable Facebook on the Configuration Settings editor (FACEBOOK_ENABLED). When the Self Service for Facebook application is installed on your Facebook page, it provides two values—your application ID and your secret key. You must assign these values to their respective configuration settings (FACEBOOK_APPLICATION_ID and FACEBOOK_APPLICATION_SECRET) in order to authenticate the link between Facebook and Oracle Service Cloud. To ensure the integrity and security of your connection, you should keep these values confidential.

In addition, incidents can be created from your Facebook page. This functionality is enabled by default (FACEBOOK_INCIDENTS_ENABLED) so your customers can submit questions without leaving Facebook. If you do not want incidents to be created from your Facebook page, then you must disable this setting. See Open Login Credentials for Social Accounts.

To learn more about Self Service for Facebook, see Overview: Self Service for Facebook.

Twitter Security

When you add Twitter channel accounts, designated agents can respond to Twitter messages publicly or privately from the agent desktop.

Due to Twitter’s unique functional design, we recommend that you encourage your customers to communicate privately when resolving support issues through the Twitter channel. Because your organization’s tweets can be read, reposted, and replied to by any other Twitter user, using public tweets to resolve sensitive service issues can be risky. For this reason, it is vital that your agents follow the best practices for using Twitter’s private messaging feature. See Responding to Twitter Posts.

If you prefer that all Twitter searches be done securely over an SSL channel, contact your Oracle account manager.

Open Login Credentials for Social Accounts

Oracle Service Cloud supports two open login standards, OAuth and OpenID. Both allow easy integration of sites that support either one of those open login standards from the customer portal.

For details on the customer portal open login as it relates to Facebook and Twitter, as well as other customer portal login methods, see Logging in to the Customer Portal. When your Facebook page or your Twitter account is created, they provide two values—your application ID and your secret key. To allow single sign-on, these values must be assigned to their respective configuration settings in Oracle Service Cloud.

- FACEBOOK_OAUTH_APP_ID and FACEBOOK_OAUTH_APP_SECRET
- TWITTER_OAUTH_APP_ID and TWITTER_OAUTH_APP_SECRET

This table describes Social Experience configuration settings.
## RightNow Common/3rd-Party Applications/Facebook

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACEBOOK_APPLICATION_ID</td>
<td>Specifies the Facebook application ID used to host Facebook for Oracle Service Cloud.</td>
<td>Blank</td>
</tr>
<tr>
<td>FACEBOOK_APPLICATION_SECRET</td>
<td>Specifies the Facebook application secret key used to host Facebook for Oracle Service Cloud. This setting is also used to authenticate staff members and customers who use Self Service for Facebook.</td>
<td>Blank</td>
</tr>
<tr>
<td>FACEBOOK_INCIDENTS_ENABLED</td>
<td>Lets customers and staff members create private incidents from your Facebook page.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## RightNow User Interface/Open Login/OAuth Apps

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACEBOOK_OAUTH_APP_ID</td>
<td>Specifies the Facebook application ID used to request the customer’s or staff member’s credentials for open login with Self Service for Facebook.</td>
<td>Blank</td>
</tr>
<tr>
<td>FACEBOOK_OAUTH_APP_SECRET</td>
<td>Specifies the Facebook secret key used to request the user’s credentials for open login with Self Service for Facebook.</td>
<td>Blank</td>
</tr>
<tr>
<td>TWITTER_OAUTH_APP_ID</td>
<td>Specifies the Twitter application ID used to request the customer’s or staff member’s credentials for open login with the Oracle Service Cloud channel, Twitter.</td>
<td>Blank</td>
</tr>
<tr>
<td>TWITTER_OAUTH_APP_SECRET</td>
<td>Specifies the Twitter secret key used to request the customer’s or staff member’s credentials for open login with the Oracle Service Cloud channel, Twitter.</td>
<td>Blank</td>
</tr>
</tbody>
</table>
3 Managing Customer and Staff-Member Passwords

Protecting Passwords

No matter your security situation, you have considerable flexibility in setting up passwords for your staff and your customers. If the data protected by a password is not critical or subject to privacy legislation, the default values in Oracle Service Cloud may be acceptable. The most compromising dangers to passwords include:

- Password cracking by brute-force attack or an exhaustive key search.
- Nefarious activities, such as phishing and other social engineering attacks.
- Inadvertent release by users (staff members or customers) who write down their passwords, send them in emails, or expose them to the public in other ways.

The choice of password controls depends on your security situation. For example, if users do not log in often, setting password expiration parameters can result in unnecessary locked accounts and frustrated users. While locking accounts can prevent some brute-force and denial-of-service attacks, it can also increase administrative overhead.

If you require your users to change their passwords regularly, you need to save history data to prevent reuse (at least five previous passwords). It is common for users to make a minor change to their password and eventually cycle back to the original, so it is difficult to assess the value of this strategy.

If you are concerned that passwords could be compromised by poor user-handling (writing passwords down) or by some form of attack, consider requiring regular changes. However, mandating frequent password changes in an environment where they are strong and are not shared does not enhance security and may actually hamper it by creating an environment that causes people to store passwords in electronic or written media.

No matter your security situation, you have considerable flexibility in setting up passwords for your staff and your customers. The topics in this section provide helpful information about your configuration options and identify tips for configuring secure passwords throughout your system.

Enforcing Password Requirements

After assessing your specific security situation, you may want to consider enforcing password requirements.

- Lock staff accounts after three to five invalid login attempts. (The default is 5 in Oracle Service Cloud.)
- Set password length to a minimum of 10 characters.
- Require special characters and numbers.
- Require both uppercase and lowercase characters.
- Avoid using words or phrases that can be identified with a person, such as their name, address, telephone number, job title, type of car, and so on.
- Encourage users to choose passwords that are easy to remember and to type. For example, common words, song lyrics, poems and so on, with slightly misspelled words, go a long way toward security.
Securing Customer Passwords

Configuration settings and password requirements enable you to secure customer passwords in Oracle Service Cloud.

Configuration Settings

The configuration setting EU_CUST_PASSWD_ENABLED controls the visibility of the Password field on the customer portal login window. This setting is enabled by default because it offers significant protection for your organization and your customers. However, if your organization does not require customer passwords, you can remove the Password field from the login window by disabling this setting.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC_EU_EMAIL_LINK_EXPIRE</td>
<td>Defines the duration in hours that a temporary link to reset a customer’s password is valid. This setting also defines the length of time a customer has access to answers on your site. See Emailing links to answers in Email Security.</td>
<td>8</td>
</tr>
</tbody>
</table>

Password Requirements

As with staff member passwords, you can define requirements to strengthen passwords on your customer portal. The editor for configuring customer passwords contains the same fields as those for staff passwords (see Configuring Staff-Member Passwords). The only differences between the two editors are the default values.

See Define Customer Password Requirements for the procedure to define requirements for customers accessing your customer portal.
Configuring Staff-Member Passwords

You can strengthen passwords by defining requirements such as minimum password length, maximum number of character repetitions and occurrences, and the minimum number of upper and lowercase characters, numbers, and special characters allowed.

You configure passwords for your staff from the configuration list on the navigation pane (Configuration > Staff Management > Password Configuration). See Configure Password Requirements.

The options available to you in setting up password requirements can enhance security on your site as well as help protect your customers’ information. This table describes the security benefits of defining specific requirements for passwords.

<table>
<thead>
<tr>
<th>Password Configuration</th>
<th>Security Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Invalid Logins</td>
<td>Locking accounts after a designated number of consecutive login failures makes it more difficult, but not impossible, for attackers to use brute-force password cracking. If an attacker is able to obtain an encrypted password, they can guess the algorithm used to encrypt it and simply run different strings looking for a match. While time-consuming, current computing technology makes it possible to guess up to - million passwords per second (and this number increases by 10 percent per year). In Oracle Service Cloud, the default is 5 invalid login attempts before the account is locked.</td>
</tr>
<tr>
<td>Expiration Interval</td>
<td>The password expiration interval helps mitigate risk for accounts that have been compromised or accounts that have not been used for long periods of time. By setting a conservative value for the number of days a password stays in effect, you can help lower the risk of attack. (Default = 90.)</td>
</tr>
<tr>
<td>Password Length</td>
<td>While it is helpful to use case changes and special characters to enlarge the character set, enforcing longer passwords is an easy way to improve password strength. (Default = 8.) For example, if 76 characters are used randomly, it takes no more than 12 hours to crack a 6-character password. Cracking time increases to 6 years for an 8-character password, and it would take 230 million years to crack a 12-character password. Of course, password cracking typically takes advantage of the tendency to use common words in passwords so dictionary attacks can break passwords more quickly. For maximum security, even longer passwords (no less than 10 characters) are necessary. For example, a 12-character password composed of 3 words from a 100,000 word dictionary could take more than 7 years to crack. Add a small amount of randomness to the password, and the cracking time rapidly increases to 230 million years.</td>
</tr>
<tr>
<td>Numbers and Special Characters</td>
<td>Requiring numbers and characters can add to the random factor of a password. They also make it easier for a user to come up with a password that is easy to remember, but still unique. For example, MaryhaddaL1tlelam. (Default = 0.)</td>
</tr>
<tr>
<td>Uppercase and Lowercase Characters</td>
<td>Requiring a mix of upper and lowercase characters can add to the random factor of a password. They also make it easier for a user to come up with a password that is easy to remember, but still unique. For example, 2BeOrNot2Bee?. (Default = 1.)</td>
</tr>
<tr>
<td>Number of Previous Passwords</td>
<td>Password history prevents the repetition of passwords when a staff member changes a password that is set to expire. Enforcing password expiration without setting the number of previous</td>
</tr>
</tbody>
</table>

**Note:** PCI-compliance requires expiration interval to be 90 days or less.
Managing Customer and Staff-Member Passwords

Recovering Forgotten Passwords

Administrators must contact their Oracle account manager to recover forgotten password credentials. Other staff members can recover both their user name and password by using the Oracle Service Cloud account self-service feature.

You also can use this functionality as a tool to maintain the integrity of your organization’s login policies for all staff members. Accessed by clicking Login Help on the Login window, the account self-service feature can be set up to open the login procedure in online help or send staff an email if they have forgotten their user name or password. This functionality is also available if your site has single sign-on (SSO) enabled. See Redirecting Users to the Oracle Service Cloud Login Page.

This table describes the configuration settings for your forgotten-password options.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCT_RECOVER_STATUS</td>
<td>Specifies the functionality of the Login Help link on the Oracle Service Cloud Login window. See Configuring Login Help.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>• 0 = Opens the login procedure in online help.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = Sends an email containing user name or a link to the Password Reset page for entering a new password (default).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 = Changes the email message staff members receive when they click Login Help. The alternate message is defined in ACCT_RECOVER_ALT.</td>
<td></td>
</tr>
<tr>
<td>ACCT_RECOVER_ALT</td>
<td>Specifies the alternate email message to send when the configuration setting ACCT_RECOVER_STATUS is set to 2.</td>
<td>Blank</td>
</tr>
</tbody>
</table>

Customers can also recover user names and passwords from the login window on the customer portal. See Change the Open Login Options and Remove the Open Login Options. In both cases, if the password is forgotten, the correct user name must be entered, and then a link to the Password Reset page is emailed to the address associated with that user name. The password is reset when the link is sent and login is not allowed until the process is completed. Customers must do this within the time frame contained in SEC_EU_EMAIL_LINK_EXPIRE. See Securing Customer Passwords and Email Security.
4 Deploying Oracle Service Cloud in a Restricted Environment

Implementing Oracle Service Cloud in a Controlled Environment

For added protection, Oracle Service Cloud can be hosted within cloud environments that align with payment card, health insurance, and U.S. government regulatory control frameworks.

Within the Oracle cloud environment, Oracle monitors and protects the operational information as well as the physical infrastructure. Oracle applies industry standard practices and current technology to aid in the protection and safety of your data. The information in these sections provides guidance on deploying Oracle Service Cloud in a manner that suits several regulations. It is meant for anyone involved in building a solution that implements any of these regulatory environments:

- Oracle Service Cloud in a Payment Card Industry (PCI)
- Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act
- Federal Risk and Authorization Management Program (FedRAMP)

**Note:** Authorize To Operate (ATO) support from a U.S. Cloud Operations public sector compliance analyst is included when purchasing Oracle RightNow Government Cloud Platform Cloud Service. We include reference to FedRAMP in this document because it is also a PCI attested environment, so the controls described here apply and may offer assistance.

Before You Begin: Reviewing Important Support Documentation

You should be thoroughly familiar with how Oracle Service Cloud is deployed, hosted, and implemented before planning a deployment in a regulation-controlled environment.

- Review all available deployment, operational, and administrative documentation. Start with the Oracle Service Cloud reference page on Oracle Help Center.
- While a majority of Oracle Service Cloud components are managed by Oracle, you are responsible for some local environmental considerations. The Deploying Oracle Service Cloud is helpful if you are deploying the .NET Agent Console. In addition, Answer ID 31 - Oracle Service Cloud Infrastructure Requirements offers helpful version-specific environment guidance.
- With the introduction of the Agent Browser User Interface in the November 2016 release, your agents and administrators can now view and manage their Oracle Service Cloud data using any browser interface. Browsing software is controlled and maintained in your local environment. You have the responsibility to protect your end users against known vulnerabilities and have the proper configurations for this type of software. These resources can provide more helpful information.
• Review the Oracle Cloud Hosting and Delivery Policy. This document describes the policies that govern how Oracle manages its Cloud Service environments to insure that they are safe and secure. It covers Oracle security, continuity, service levels, change management, and other policies. Each of these has been evaluated by third-party assessors for the relevant standard or regulation.

Understanding Supplemental Controls and Policies

For customers seeking to implement Oracle Service Cloud in a regulation-controlled environment, we implement and manage a series of supplemental controls and policies.

There are supplemental Oracle-managed controls that are specific to the Oracle SaaS offering. These controls are automatically established when deploying an instance of Oracle Service Cloud within the specific cloud environment.

Oracle Staff Restrictions | Segregation | Cryptography | Secure Protocols | Masked Data

Oracle Staff Restrictions

For Oracle environments that are designed to meet additional controls such as PCI or HIPAA, Oracle incorporates access control mechanisms that restrict Oracle personnel based on need-to-know, relevant compliance training, and functional responsibilities. Oracle staff must use a multifactor authentication process. Oracle also provides annual awareness training for selected personnel who support certain environments.

Segregation

Customer instances are logically segregated within Service Cloud. Each customer’s instance is deployed on its own database schema. Oracle also protects each instance by not allowing any direct database access. Customer connections to data within Oracle Service Cloud are through standard application program interfaces (APIs).

For more information, see the Oracle Service Cloud Integrate page.

Cryptography

Oracle implements industry tested and recognized cryptography technologies to protect the continued integrity and confidentiality of sensitive information. We have developed encryption requirements that are based on National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) 140 and 180 guidelines. We also employ SHA-256 to protect passwords.

All file systems are encrypted to protect customer data at rest. This includes all files attached to objects in the Oracle Service Cloud, all reports published to files, and all Service Cloud instance databases, including database backups.

Secure Protocols

By default, all connectivity to Oracle Service Cloud employs encrypted methods. While standard commercial customers can disable this encryption, Oracle does not advise this. For customers within regulated environments, Oracle strongly recommends HTTPS using TLS 1.2.
Masked Data

PCI regulated environments require that specific types of data be obfuscated from unauthorized people. Oracle employs technology that obfuscates payment account numbers (PAN) and U.S. social security numbers. Data of these types are rendered unreadable on the user's display by automatically substituting all digits with asterisks.

The Luhn algorithm is used to obfuscate credit card (PAN) data. A pre-defined pattern check is used for social security numbers (nine digits separated by dashes, periods or spaces in the sequence of [3, 2, 4]). PANs and social security numbers are also masked when using APIs to retrieve information, and in file attachments that are downloaded from PCI environments as long as the file is text-based and not an image, zip, or binary file type.

Complying with Third-Party Standards

While we comply with a number of third-party standards, you are ultimately responsible for ensuring that your Oracle Service Cloud implementation is in compliance.

The following topics offer guidance about configuring a compliant environment:

- Securing Access Control
- Auditing and Logging
- Securing Mobile Access
- Evaluating PCI Vulnerability
- Securing Integrations and Accelerators
- Incident Thread Masking
- Securing Email, Outreach, and Surveys
- Securing Analytics
- Securing Chat

Oracle’s control status regarding a regulation does not mean that your Service Cloud implementation is automatically considered to be compliant. Your environment(s) must be assessed by an approved third-party organization to ensure controls are properly in place.

On a periodic basis, Oracle Service Cloud is audited by third-parties to validate that controls are in place which are designed to address various regulations. As a Cloud Service Provider (CSP), Oracle Service Cloud has many safeguards in place to ensure the security of Oracle’s infrastructure and our customers’ data assets.

However, as the data controller, you retain many obligations. For payment account numbers (PANs) or protected health information (PHI), we recognize that you can extend the data model to retain sensitive information, or choose to use the service to process and transmit sensitive data. For Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, there are controls that you can configure during a deployment that contribute to protecting your data.

To ensure that we are in compliance with the standard, Oracle obtains a Payment Card Industry Data Security Standard (PCI DSS) Attestation of Compliance (AoC) from Oracle’s third party Qualified Security Assessor (QSA) every year. Oracle Service Cloud is attested for compliance with PCI DSS Service Provider Level 1. Although this can aid you when you are assessed, it is not transferable to the you, and does not mean that you are purchasing a PCI certification.

Similar to the PCI DSS AoC, HIPAA has an AT-101 report from the appropriate external parties. Also, in context of the HIPAA / HITECH rules, Oracle is a Service Provider in a Business Associate role where customers have executed a Business...
Associate Agreement. If applicable to the order, the Business Associate Agreement (BAA) between the customer and Oracle describes the obligations for each party.

In addition there may be other accreditations, attestations, and certifications available for Oracle Service Cloud in the environment you purchased. These may include:

- Cyber Essentials Plus
- HMG Cloud Security Principles
- IRAP (Information Security Registered Assessor Program)
- NIST (National Institute of Standards and Technology) Special Publication 800-53, including U.S. government programs:
  - CJIS (Criminal Justice Information Services) Security Policy
  - DFARS (Defense Federal Acquisition Regulation Supplement)
  - DISA SRG (Defense Information Systems Agency Security Requirements Guide)
  - FedRAMP (Federal Risk and Authorization Management Program)
  - FERPA (Family Educational Rights and Privacy Act)
  - FISMA (Federal Information Security Management Act) Baseline
  - IRS (Internal Revenue Service) 1075
  - MARS-E (Minimum Acceptable Risk Standards for Exchanges)
  - NIST 800-171
- SOC-1 and SOC-2

Attestation or accreditation reports for standards and regulations are available upon request through an Oracle account representative.

Using Oracle Service Cloud Components in Controlled Environments

While Oracle Service Cloud can be purchased with a variety of add-ons, only specific components are available for use in controlled environments.

The services listed below apply to all documentation included here, unless specifically noted. If there is a product or service not identified within this document, additional validation should be performed to determine the product’s control status. In addition, some products have version-specific capabilities and research should be performed to validate control expectations before enabling it in any specific environment.

- Agent Desktop Cloud Service (includes Web Customer Service and Cross Channel Contact Center)
- Chat
- Experience Routing
- Social Monitor
- Foundation Agent Knowledgebase
- Advanced Agent Knowledgebase
• Policy Automation (OPA)
5 Deploying PCI and HIPAA

Protecting Data

If you diverge from the default data model, ensure that proper controls are maintained.

Oracle Service Cloud does not have any specific fields defined in the default data schema intended to store payment account numbers (PAN), social security numbers, or protected health information (PHI); however, there are supported methods to customize the data model. You can extend and customize the Service Cloud data model to best fit your needs. Whenever you diverge from the default data model, be sure to validate that proper controls are maintained.

It is important for you to know what data will be captured, how it will be used, and who should have access. In regulated environments, even though your data is stored within the Cloud Service Provider (CSP) database, it is still your responsibility to define your data classification and how you will govern your data.

Securing Access Control

There are multiple methods available to access the Oracle Service Cloud, like the Customer Portal, integration frameworks, and the Agent Console. Each of these methods should include defining who will have access, as well as determining how the connection and the in-transit data are protected.

Restricting Host Access

Restricting access to the customer’s site can help reduce opportunities for unauthorized access. You can define which hosts can access or are not allowed access with the Customer Portal configuration settings SEC_VALID_ENDUSER_HOSTS, SEC_VALID_ADMIN_HOSTS, and SEC_VALID_INTEG_HOSTS. See the Service Cloud documentation Secure page for more information.

Establishing Credentials

In PCI and HIPAA environments, users must have unique identifiers and complex passwords. While Service Cloud customers control their own password complexity, requirements specified by the PCI DSS are expected in a PCI environment and are a good rule of thumb for all other environments.

These are the current minimum requirements for passwords in a compliant environment:

- They must have a minimum length of at least seven (7) characters.
- They must contain both numeric and alphabetic characters.
- They must be forced to change periodically.
- They cannot be the same as the previous four (4) passwords.
- They must provide a temporary lock-out after six (6) invalid attempts.
By default, Service Cloud enforces most of these minimum requirements, and in some cases enforces stricter minimums. We provide the ability for you to configure the settings in a PCI-compliant matter. You are responsible for documenting your settings and supplying guidance to your users on circumstances under which passwords should be changed (for example, when there is suspicion that a password has been compromised).

You can find instructions for setting these configurations in Configure Password Requirements.

Additionally, access to any public-facing interface is encrypted by default, but you should also consider using the SESSION_HARD_TIMEOUT and CLIENT_SESSION_EXP configuration settings. These control agent and staff member re-authentication time limits.

Setting Data-Management Policies

You should align your data-management policies to your business policies. For example, you can determine how long closed incidents remain in the database and how long archived incidents remain in the archive. The control settings for these are ARCHIVE_INCIDENTS and PURGE_ARCHIVED_INCIDENTS. You can find more information about these at Answer ID 7105 - Default settings for incident archiving and archived incident purging.

Enforcing a Secure Protocol

Customers who deploy Customer Portal can also determine which pages and widgets require authentication by end-users. As a best practice, enforce a secure protocol when transmitting login credentials. The CP_FORCE_PASSWORDS_OVER_HTTPS configuration setting enables passwords to be sent over an encrypted connection. This customer-facing configuration helps protect users from malicious activity like password theft, profile hijacking, or eavesdropping of non-public data. It enables an encrypted connection during both the login process and all subsequent operations by logged in users.

When using the CP_FORCE_PASSWORDS_OVER_HTTPS with custom login pages and/or input widgets on the Customer Portal, communication will need to be directed over HTTPS. To do this, incorporate the page meta tag force_https. See the Service Cloud documentation Configure and Extend page for more information.

If you choose not to require passwords for end-users, it is still possible to enforce HTTPS with SEC_END_USER_HTTPS. This same setting forces HTTPS for Chat sessions and affects the absolute URLs generated in outgoing email messages. You should work with your account manager or technical support to change this setting. Be careful, because you could break your instance if it is not set up properly at the Web server to accept SSL. For customers with a vanity URL, exercise caution when changing this setting. Reference the SEC_END_USER_HTTPS configuration setting when contacting Oracle Service Cloud Technical Support.

Securing Connectivity

You can access the Service Cloud from nearly anywhere. Since the Service Cloud is accessible from the internet, consider the typical precautions when connecting to the Service Cloud. You should have the proper encryption, antivirus, and network rules implemented per your own security policies. PCI DSS and HIPAA frameworks require that all connectivity must be made using an encrypted connection. Both PCI DSS V3.2 and NIST strongly recommend no less than TLS 1.2 be used to provide secure transmission of sensitive data.

Auditing and Logging

Audit and read logs allow customers to see actions taken on their data.
In addition to tracking selected object create, update, and delete transactions, Service Cloud offers optional auditing of Incident Thread and Contact reads. Incident Thread read logging is enabled by default for HIPAA instances. For HIPAA customers, this feature is configured at provisioning. When properly enabled, this feature builds upon the standard audit functionality by adding an audit log entry whenever an Incident Thread is viewed and who viewed it.

**Note:** You can only account for all disclosures of PHI via the Incident Thread object. PHI data captured in other areas of the product do not have read transactions logged. Oracle recommends that PHI only be stored in the Incident Thread.

For non-HIPAA customers, read logging is disabled by default. To enable the read logging capability, an authorized customer representative must submit a service request to Oracle Technical Support to enable READ_LOGGING_ENABLED for Incident Threads and/or CONTACT_READ_LOGGING_ENABLED for Contacts. Once enabled, any reads of incidents and/or contacts are logged by the Service Cloud.

**Note:** Only incidents and/or contacts are logged. Reads of other objects are not.

When using the Read Logging feature, you are responsible for making read transactions visible in the Agent Console audit log. To do this:

1. Open the Workspace Designer.
2. Open the desired incident or contact workspace.
3. Set Show Read Transactions to On.

**Note:** This setting is visible in the Workspace Designer only when READ_LOGGING_ENABLED and/or CONTACT_READ_LOGGING_ENABLED are enabled.

Use care when debugging Custom Process Management processes. When testing custom developed scripts, sensitive data may inadvertently be captured in the logs. For customers concerned with developers viewing sensitive data, Oracle recommends using test data and properly vetting the data that appears in logs.

For more information, see the Service Cloud documentation Administer page.

### Securing Mobile Access

Use caution when allowing Oracle Service Cloud to be used with a mobile device.

With the August 2016 release of Oracle Service Cloud, an accelerator was provided with new ways to use the Oracle Service Cloud services through a mobile device. This solution uses the Oracle Mobile Application Framework (MAF) which allows you to develop both iOS and Android applications from a single code base. For more information see Answer ID 5436.

The MAF accelerator contains supplemental objects as well as software that use REST APIs. You should become familiar with the MAF architecture and capabilities of the Oracle Mobile Application Framework before deploying and developing code.

As with all accelerators, the provided code is a sampling of what features can be developed. The sample code has not gone through a third party assessment for any regulation framework. While the included code may function directly upon deployment, it only uses basic authentication which may not be appropriate for deployment within a regulated environment.

The MAF architecture provides for encryption of data on end-user devices. When MAF is utilized within a PCI compliant implementation of Oracle Service Cloud, PAN data, and social security numbers displaying on the device will be unreadable.
One exception to this rule is in the case of push notifications. Since notifications sent from Oracle Service Cloud are configured as events and pushed out of Oracle Service Cloud, sensitive data sent in push notifications does not get masked. You should validate that no fields that could contain PII, PAN, or PHI data are included in push notifications that would appear on a mobile device.

Similar to other integrations, take care when implementing this mobile solution on iOS. Based on usage requirements of the Apple Push Notification Service (APNs), the sample code uses Oracle Mobile Cloud Service as an intermediary service. You should understand how Oracle Mobile Cloud Service protects and persists data before you implement it.

Evaluating PCI Vulnerability

The PCI vulnerability evaluation analyzes all customer generated code in search of vulnerabilities and insecure processes to protect Oracle and its customers in the PCI environments.

If you purchase the Oracle RightNow PCI Certified Cloud Platform Cloud Service, you must engage a Technical Account Manager (TAM) to conduct a PCI vulnerability assessment before you implement the service and annually thereafter.

For more information, talk to an Oracle account representative about Oracle Technical Account Management for PCI Certification Services.

Securing Integrations and Accelerators

You should closely examine integrations between Oracle Service Cloud and external applications to prevent mishandling of sensitive data.

The value of Oracle Service Cloud increases when data is exposed to other applications and shared across functional groups. Subsequently, a wide variety of methods to integrate with applications external to Oracle Service Cloud are available. These include public APIs, productized integrations, and accelerators. You must carefully plan your integrations so that sensitive data is protected throughout the entire lifecycle, and ensure that sensitive data is either not moved or is only moved to environments having adequate controls.

Although Oracle Service Cloud can integrate with customer on-premise applications or other Oracle Cloud products, the ability to share sensitive data with another application does not mean the other product maintains all the same regulatory controls that Oracle Service Cloud has. You are responsible for validating which controls are in place across system architecture where your sensitive data will transmit and persist. For example, if PHI data within Oracle Service Cloud will be shared with Oracle Sales Cloud, you should contact Oracle and validate that Oracle Sales Cloud has the necessary HIPAA controls. You cannot presume that the appropriate regulatory controls exist because the products in question are from the same vendor.

When determining how to move data out of Oracle Service Cloud, consider whether the data is being pulled out or pushed out. This concept is relevant to sensitive data masking. In general, sensitive data in Oracle Service Cloud being pulled out will be masked and sensitive data pushed out will not be masked. For example, when using the Representational State Transfer (REST) API, you could use an on-premise application to get (pull) data from Oracle Service Cloud. Oracle Integration Cloud Service (ICS) is an example where connections enable data to be pushed out of Oracle Service Cloud.

Oracle Service Cloud’s API, integration and accelerator documentation contains example integrations to other packaged applications, which includes examples of how to perform various integrations using approved technologies (such as,
JavaScript, SOAP, REST, etc.) and what data is available. Please be aware that these examples are not analyzed for impact by Oracle to any regulation requirements.

**Related Topics**

- API documentation
- Integration documentation
- Accelerator documentation

### Incident Thread Masking

Incident thread masking protects data by automatically masking content in the incident thread when written to the database.

All databases and file systems associated to your instance are maintained on encrypted file systems. The Oracle Service Cloud PCI environment automatically redacts payment account numbers (PAN) and social security numbers from displaying when this data is detected during read operations.

However, by default, Oracle Service Cloud does not prevent you from storing sensitive data in the database. If you want PAN, social security numbers, or sensitive personally identifiable information (PII) to be permanently redacted when stored in the incident thread object within the database, then you need to configure incident thread masking.

Incident thread masking protects data by automatically masking content in the incident thread when it is written to the database. Data matching the masking patterns will be permanently redacted and stored in the database with an X replacing each redacted character. The original data being redacted is unrecoverable.

By default, Oracle Service Cloud provides three mask algorithms for credit cards, social security numbers, and phone numbers. You can define up to five additional custom masks.

Incident thread masking is included in the Enterprise and Enterprise Contact Center user seat license tier. To learn how to configure this feature, see [Masking Information in Incident Threads](#). To enable this feature in a site instance, enable `THREADS_AUTO_MASKING_ENABLED`, or contact either Technical Support or your account manager for assistance.

### Securing Email, Outreach, and Surveys

Although Oracle Service Cloud follows industry standard practices to protect the integrity of hosted mail domains, you must exercise care regarding the information placed within messages and as attachments.

You should never send card holder or other sensitive data using email technologies. Oracle claims no responsibility for cardholder data transmitted across this communication channel, because email is not necessarily secured across the internet and is not considered a compliant method for sending or receiving cardholder data.

The Oracle Service Cloud Outreach Service enables customers to send emails and campaigns to targeted audiences. The Survey Service provides a method to request information from specific customers via email (as well as other options). In these scenarios, the send works under the controls customers have implemented based on the above information. In order for end-user responses to be received via SSL, customers must use the end-user SSL configuration `SEC_END_USER_HTTPS`. 

---

*ORACLE*********************************************************
This configuration setting can only be changed through a request to Technical Support, and the use of this setting must be carefully planned.

Related Topics

- Best Practice: Sending Email
- Email Security

Securing Analytics

Use care regarding permissions and accessibility of reports, including data in a report being exported to another system outside of the Oracle Service Cloud.

The Oracle Service Cloud has a rich set of analytics features for reporting on data within the customer’s instance. It is your responsibility to manage what reports remain published and which staff members have access to selected reports.

Exercise caution when distributing reports via email. When reports are scheduled to automatically be emailed to a person or group, in a PCI environment, PAN and social security numbers saved in the database could appear on these reports without being obfuscated. Additionally, if an agent chooses to forward a report using the email functionality, the report contents will not be subject to masking.

When using the Report Caching feature, where an often executed report is created automatically at a set interval, you should put an appropriate process in place to disable a cached report when it is not needed as frequently.

For HIPAA customers, there may be a concern that analytics could expose PHI from the incident thread. There is a setting that prevents analytics from having access to the threads.note field which is where PHI should be persisted. To enable this feature for a customer’s instance, the THREADS_NOTE_ANALYTICS_VISIBLE configuration setting is automatically enabled for a HIPAA customer’s site. This setting provides assurance that threads.note is not permitted to be included on a custom report.

Note: This setting prevents customers from running ANY reports containing this field. Some standard Service Cloud reports will produce an error for HIPAA instances or any time THREADS_NOTE_ANALYTICS_VISIBLE is enabled. These reports are:

- Incident Details By Survey (/Public Reports/Feedback/Service Surveys)
- Email Response (/Public Reports/Service/Email Reports)
- Incident Message Transactions (/Public Reports/Service/Views - Service/Editor Reports – Service)

The error produced is: Invalid reference to threads note. Your site is not configured to allow reporting on thread note. You will need to edit the report to resolve these errors.

Securing Chat

For customers planning to interact with end-users via Chat, there are several security factors to consider.
When Chat is purchased with Oracle Service Cloud, it can be covered by the Oracle Service Cloud PCI Cloud Service and/or the HIPAA Cloud Service. If purchased standalone, the ability of the service to meet requirements will depend on how it is deployed and which other products it is deployed with. The standalone implementation is not covered in this document.

When deploying Chat in conjunction with Oracle Service Cloud in our PCI environment, data masking occurs automatically within the chat conversation. In other words, when an agent and end-user are interacting, PAN or SSN data typed by the end user will be redacted when displayed for the customer’s agent. The reverse direction is also true.

To prevent capturing PAN or any PII in an incident, customers can instruct their agents to inform end-users to use the Off the Record button while in a Chat conversation. This enables an end-user to send unrecorded messages that will not be saved in any location. The only indication there was off-the-record communication is an entry within the chat transcript or the incident thread saying username: Message Removed.

Chat customers have a Sneak Preview feature. This allows a customer’s agents to preview what the end user is typing before the end user presses Enter and could display data for the agent that should have been redacted. This feature is disabled by default. We recommend that you use this feature in accordance with your own privacy and internal security requirements and policies.

If you have purchased the Engagement Engine, Video Chat or Cobrowse offerings that integrate with Chat, be aware these products have not been audited for use with Oracle Service Cloud in a restricted environment. While these products do not process or store data, there are situations where your agents could view your customer’s protected data. Therefore, you will need to put additional controls in place to protect this from occurring. The Cobrowse and Engagement Engine user guides describe methods for helping you protect your customer’s data that is not covered in this document.

**Related Topics**

- Using Standalone Cobrowse
- Oracle Engagement Engine Cloud Service Documentation
Glossary

absolute time

An exact date and time defined in an escalation action for business rules or a comparison period for custom reports. In standard reports, absolute time is the amount of time passed based on a 24-hour clock. See also relative time.

access level conditional section

A method of controlling the visibility of a portion of an answer. Only those customers with permission to view the access level assigned to the answer section can view it.

accessibility

The characteristics of a website that allow all users, regardless of disability, to have complete access to the information and features of the site.

account self-service

A feature for staff members to get help when logging in to the administration interface. If staff members forget their login information, they can request their user name or password by clicking Login Help on the Login window. Account self-service can also be set up to open the login procedure in online help or to convey an alternate message.

action

The part of a business rule that defines what happens when an object (answer, contact, incident, chat session, opportunity, organization, target, or task) meets the rule’s conditions. Actions are also a part of script and workspace rules, and a component of campaigns that can perform one of several functions.

action arrow

An arrow on a workspace field or control that displays available editing options.
activate

A process that is manually run after making changes to a state, function, or rule in a rule base to check for errors, archive the current rule base, and convert the edited rule base to the active rule base. See business rules.

Active

One of the default opportunity statuses and status types. An opportunity with the Active status is currently advancing in the system toward a sale.

add-in

A custom .NET component that is loaded and activated by Oracle Service Cloud to add new features and integration capabilities.

Add-In Manager

A utility for adding, updating, and deleting add-ins in Oracle Service Cloud. The Add-In Manager is also used to set add-in permissions for each interface.

administration interface

The graphical user interface that staff members use to configure and manage Oracle Service Cloud. See also agent desktop and Service Console.

administrator

A staff member who configures, customizes, and maintains an Oracle Service Cloud application.

administrator login

The default login used by the administrator to download Oracle Service Cloud and log in the first time. This special login is not a defined staff account and has no navigation set or profile associated with it. Using this login, the administrator must create a navigation set, profile, and staff account in order to access all functionality. See navigation set, profile, and staff account.
administration site

See *Customer Portal Administration site*.

advanced mode

A survey editing mode for creating detailed questionnaires using an extended feature set that includes survey branching and automation elements.

Agedatabase

A scheduled utility that operates on the knowledge base data to maintain dynamic answers and make searching more efficient for staff members and customers.

agent

A staff member who may be assigned incidents and chats with customers, and who may also maintain contact and organization records.

agent desktop

The graphical user interface that staff members use when working with records, mailings, surveys, campaigns, and standard and custom reports. Agent desktop also refers to a set of complementary features in Oracle Service Cloud, including workspaces, workspace rules, guides, agent scripts, script rules, workflows, and add-ins, each representing a different, powerful way of interacting with records in the knowledge base. While each component serves a distinct purpose, they can be used together to create a highly adaptive work environment. See also *administration interface* and *Service Console*.

agent scripting

A feature that helps guide staff members as they enter information into records on *workspaces*. See also *script*.

aging

An automatic process that reduces an answer’s solved count as the frequency with which the answer is viewed by customers declines. As the solved count is lowered, the answer will move down the list of answers and be less visible to customers.
**alias**

A word that represents another word or phrase. Aliases and the words or phrases they represent can be added to the synonym list to enhance customer searching. See *wordlist file*.

**anchor**

A node on an action or decision in a campaign used to create a path. Actions and decisions have anchors for incoming and outgoing paths. Anchor also refers to a destination for hyperlinks placed at locations within documents for use in mailings and questionnaires for surveys and in answers when linking to other answers.

**answer**

Any knowledge base information that provides solutions to common customer support questions.

**answer access level**

A method of controlling what information is visible to customers. The default answer access levels are Help and Everyone, and custom access levels can be added.

**answer custom field**

A field for gathering and displaying additional information about answers. Answer custom fields appear when adding or editing an answer and on the Answers and answer details pages.

**answer relationship**

The relationship between two or more related answers. Answer relationship types include sibling, manually related, and learned link. Sibling and manually related answer relationships are defined by staff members. Learned link answers are automatically defined through customer activity. See *learned link*, *manually related answer*, and *sibling answer*.

**answer status**

A method of controlling the visibility of an answer. The default answer statuses are Public, Private, Proposed, and Review, and custom answer statuses can be added.
answer status type

The status of an answer that determines whether it can be viewed by customers. The default answer status types are Public and Private.

answer type

The format in which answers are displayed to customers. Answer types include HTML, URL, and file attachment. See File attachment answer, HTML answer, and URL answer.

answer update notification

A way for customers to sign up to be notified whenever a particular answer is updated. Customers can also sign up for notification whenever any answer associated with a specific product or category is updated.

Answers page

A page on the customer portal where customers can view answers and search the knowledge base. Customers can view individual answers or search the knowledge base using selection criteria to narrow their search. If additional elements are enabled, customers can also search documents, websites, and communities. See also Web Indexer and Oracle RightNow Social Experience communities.

API (application program interface)

An interface that enables programmers to communicate with the Oracle database. The API includes functionality to create, update, delete, and retrieve answers, contacts, hierarchical menus, incidents, opportunities, organizations, quotes, SLA instances, staff accounts, and tasks.

application menu

An interface element containing a list of options for working in Oracle Service Cloud, including access to other areas of the product and shortcuts for adding records and items to the knowledge base. The application menu also contains options for changing personal settings and password and customizing the content pane and navigation pane display. Staff members can also exit their application from this menu. See file menu.
Ask a Question

A page on the customer portal where customers can submit a question when they cannot find an answer in the knowledge base.

asset

Any product or service associated with an organization’s customers. Assets can require serial numbers or not and can be registered by customers on the customer portal or by agents on the agent desktop.

asset product

Any product or service sold or provided by an organization that can be tracked in Oracle Service Cloud. Asset products are configured using the product catalog.

asset record

Information about a specific product or service provided to a specific customer that is tracked and maintained in Oracle Service Cloud.

audience

All of the contacts belonging to the lists and segments associated with a mailing or survey. See also contact list and segment.

audience sampling mode

A market testing option for transactional mailings and surveys that sends a sample of test messages to portions of your audience. If more than one message is created, market testing rotates through the test messages. See market testing.

audit log

A list of all the actions performed on a report, record, or item in the knowledge base, including who performed the action, what the action was, and the date and time of the action.
auto filter

A control added to report columns for filtering report data by values in the columns.

automatic logout

A way of managing desktop user sessions by automatically logging out inactive sessions after a specified time of inactivity. Automatic logout is part of desktop usage administration, which assists organizations in lowering seat usage for licensing compliance. See also force logout.

backup directory

The directory that contains all the backup files created by the File Manager.

backup file

A file that is automatically saved each time a file is edited through the File Manager. Before the file is overwritten, the backup file is saved. The restore function can be used to revert to the backup file.

basic page set

The template and set of customer portal pages that have been optimized for display on browsers with limited or no JavaScript capabilities.

billable task

A way of classifying and recording the amount of time agents spend working on incidents. The default billable task is Miscellaneous, and custom billable tasks can be added.

block

A section of widget code that can be customized to extend the view of a standard widget. Widget code that is not within a block cannot be modified.
block quotes

A symbol or HTML tag that designates a section of text that is not part of the most current email reply, such as previous entries in the email conversation. See also checksum and techmail.

boolean searching

A knowledge base search that allows customers to connect multiple keywords using & (AND) and |(OR) operators.

bounced email

Email that is undeliverable. Emails can be bounced when email accounts are not functioning properly or are full at the time the mailing is sent. Outreach and Feedback tracks bounced emails. See also email management.

broadcast mailing

A mailing sent to one or more contact lists or segments. Broadcast mailings can be sent at a scheduled time and can also be used in campaigns.

broadcast survey

A survey sent as a broadcast mailing in which the message, audience, and mailing options are defined in the survey.

builder

A community member whose primary role is to create hives and groups for a community. Access to builder functions is provided by the Builder–Custom and Builder–Template user types. See user type.

Bulkdel

A utility for deleting several incidents at once.
**business objects**

The page of the Customer Portal Administration site that defines the set of answer, contact, and incident fields that can be used to define input and output fields on the customer portal.

**business rules**

A component for defining processes to automate workflow, notification, and escalation. Business rules can automatically route incidents, opportunities, and chat sessions; send email and Outreach messages; escalate answers, incidents, opportunities, and tasks; update records; assigns SLAs; and create Offer Advisor targets. See also script rules, target rules, and workspace rules.

**cached data**

Report data that has been temporarily stored in the database for quicker report generation. This data is cached nightly by the Agedatabase utility and can be purged regularly. Cached data also refers to local cache files stored on a staff member’s workstation. This includes all option lists data (any data accessed from a drop-down menu or menu list such as customizable menu items) plus additional data such as report and workspace definitions, questions, documents, and standard text.

**Campaign**

A multiple-step marketing process based on business logic. Campaigns can contain any number of actions and decisions and move contacts through a series of steps when specified criteria have been met.

**Canceled**

A mailing and survey status that indicates a mailing or survey has been manually canceled before being completed.

**case section**

A logical group of conditional sections where one, and only one, conditional section displays to the customer. As soon as the first conditional section is matched, the content for that conditional section is added, and no other conditional sections within the case section are evaluated. Case sections make content more relevant and targeted to a specific audience than independent conditional statements. See also condition.
Case statement

A type of conditional element used for multiple-choice decisions that allows more diverse branching capabilities to be added to campaigns and surveys based on conditions defined in the workflow. Case statements are unique because they have an outgoing path for every condition. As soon as the first choice (condition) is matched, the path for that choice is followed, and no other conditions within the case statement are evaluated.

category

An option for grouping answers and incidents that allows more precise organization in the knowledge base. Staff members can classify answers and incidents by category and up to five additional levels of sub-categories, allowing more refined searching by customers and staff members. See also product.

category page

A custom page that serves as a landing page for grouping and accessing custom content pages in a community.

certificate

A digital piece of information for email and Internet security that includes the name of the certification authority, the holder of the certificate, the certificate holder’s public key, the dates the certificate is valid, the serial number, and the digital signature of the certification authority. Certificates are also called public and public key certificates.

certificate revocation list

A list of certificates that have been suspended or revoked before they have expired. The certification authority maintains, updates, and publishes the certificate revocation list at regular intervals.

certification authority

A third party authorized to issue certificates and authenticate the identity of the holder of the certificate.
channel

The source of an incoming incident or outgoing response. Channels are grouped as standard email channels (Service Email, Outreach Email, Phone, Fax, Post, Service Web, Outreach Web, Chat, and Email) and social channels (Community, Twitter, YouTube, RSS feeds, and Facebook). Channels are also used to indicate contact, opportunity, and organization notes.

channel account

A shared credential that permits one or more designated staff accounts to pass through a social media site when login and password authentication is required. Channel accounts can be created for communities, Facebook, and Twitter.

channel type

The social channels tracked in contact records when storing social account user names and associating social monitor incidents to contacts. Channel types include Facebook, Twitter, and YouTube.

chart style

A collection of display settings that can quickly be applied to charts used in reports. Chart styles control most of the graphical configuration of charts.

chat agent status

A method of tracking an agent’s availability to chat. The default chat agent statuses are Unrestricted, Unqualified, Unspecified, In Meeting, and On Break, and custom statuses can be added.

chat agent status type

The status of an agent’s availability to chat. Default chat agent status types are Available, Unavailable, and Logged Out.

chat session

A real-time, two-way dialog between a customer and one or more chat agents. See Oracle RightNow Chat Cloud Service.
chat session queue
A sequence of unassigned requests for chat sessions. The default chat session queue is Default Chat Queue, and custom queues can be added. Requests are added to chat session queues automatically by business rules.

chat session routing
A process of routing customer requests for a chat to a specific chat session queue based on rules in the Chat rule base.

checksum
A calculated value that represents the content of a block of quoted text. This value is sent within the block quote tags of the email message and is used to determine if text has been added to the original message. See also techmail.

choice question
A question type that allows customers to choose their answer from a menu, option, check box, or list.

Click-Once installer
A utility used to install the Oracle Service Cloud Smart Client on staff members’ workstations.

client
The interface that displays on a customer’s computer when submitting a request to chat with an agent.

clone
To create an exact copy of an existing site or interface.

Closed
One of the default opportunity statuses and status types. An opportunity with the Closed status has resulted in a sale.
cloud search

A search of social networking sites in order to track customer reaction to an organization’s products, services, and overall reputation. In addition to searching the social cloud, staff members can schedule cloud searches, ignore or respond to posts, and create incidents from posts.

clustering

An automatic process that groups the knowledge base into clusters of related answers and labels each cluster group with keywords that define those answers. See also data mining and topic browsing.

cobrowse

A feature in Chat that enables agents to guide customers through web pages using their mouse or other pointing device to demonstrate actions. Cobrowsing may also be available on incident workspaces to let customers share their desktop with agents when they are on the phone.

Code Assistant

A Customer Portal tool to aid migration of custom code from earlier framework versions to a newer version. The tool offers code suggestions for migrating widgets, converting to a new UI version, and removing features that are no longer supported.

color scheme

A collection of colors that can be applied to chart styles. Multiple colors can be defined and combined into one color scheme. Charts that use the same scheme use the same set of colors.

comment

A form of content created by members when responding to posts in a community.

community

A social web solution consisting of customizable hives, members, groups, and custom pages.
community privacy level

The level of privacy that determines whether a login is required to access community content.

comparison period

A reporting parameter used to compare a report’s time period to an identical length of time in the past. Comparison periods are defined when creating or editing a custom report and can be included in standard reports.

compatibility set

A set of Customer Portal widgets designed to be used together. Best practice recommends using widgets from the same compatibility set on any given customer portal page rather than combining them from different compatibility sets.

competitor

An option for identifying other parties pursuing the same opportunity.

compile

A process that runs the compiler engine to check states, functions, and rules within a rule base to ensure there are no errors. See activate.

Completed

A mailing and survey status that indicates a broadcast mailing or broadcast survey has been sent. The system automatically sets the status to Completed from the Sending status.

complex expression

A search technique that enables customers and staff to search for a broader set of content. This technique allows wildcard searching using an asterisk (*) at the end of a word or partial word and a tilde (~) before a word to perform a similar phrases search on that word only. Word stemming and logical operators are also supported. This technique is available on the administration interface and the customer portal.
computed field

A column whose value is derived from calculations performed on database fields. Computed fields can be added to output levels in custom reports.

condition

The part of a business rule that determines whether an answer, contact, incident, chat session, opportunity, organization, target, or task matches a business rule. Rules can contain multiple conditions. Conditions are also a part of script and workspace rules.

conditional formatting

A method of highlighting specific information in report columns that does not require creating data exceptions.

conditional section

A section of text in a document that appears only to those contacts meeting certain criteria. Conditional sections can also be placed in answers and tagged with specific answer access levels. In message templates, conditional sections can be used to filter content by contact, profile, runtime variable, or record type. See also access level conditional section.

conference

A feature in Chat that enables an agent to conference another agent into a chat session with a customer.

configuration button

The button in a staff member’s navigation set containing a list of all the configuration items necessary to configure and customize an organization’s application. Items can be added to or removed from this button from the Navigation Sets editor or, with the Customize Navigation Sets profile permission, the Customize List window. See also configuration list.

Configuration Settings editor

The interface element used to customize the functionality and features of the administration interface and the customer portal.
configuration list

All of the configuration items associated with the configuration button in a staff member’s navigation set. The configuration list is organized in a tree on the navigation pane.

configuration settings

All of the settings accessed from the Configuration Settings editor to configure and customize the administration interface and the customer portal in Oracle Service Cloud.

Configuration Wizard

An interactive utility for configuring web indexing on the customer portal. Web indexing allows customers to search the knowledge base along with web pages and other web-accessible documents within a specified domain. See Web Indexer.

Connect Object Explorer

A ROQL query interface that helps Customer Portal developers become familiar with the Connect for PHP API and explore Connect objects and metadata.

contact

Any individual with a contact record in the knowledge base. Contact records can be added by staff members on the Service Console and by customers on the customer portal. Contact records are also added automatically when a customer without a record submits a question on the Ask a Question page of the customer portal. See also primary contact.

contact custom field

A field for gathering and displaying additional information about contacts. Contact custom fields appear when adding or editing a contact record and on the Your Account page of the customer portal.

contact list

A static or fixed group of contacts that is used to choose the contacts who receive a broadcast mailing or survey. Contacts can be added to lists.
contact role
An option for classifying contacts by their roles in opportunities.

contact type
An option for classifying contacts by types, such as job positions or decision-making roles.

Content Library
A component for creating content that can be used in mailings, web pages, and surveys. Content includes documents, tracked links, files, templates, and snippets.

content page
A type of custom page to which community content and functions can be added using panels. See also category page.

content pane
The area on the console where staff members work with items selected from the navigation pane or the application menu.

content pane tabs
An interface element for switching between the items currently open on the Service Console. Content pane tabs display at the top of the content pane by default. Staff members can click a tab to return to a report or item or right-click a tab and select from a number of options.

context-sensitive answers
A subset of SmartAssistant that allows organizations to construct special Related Answer links from any web page to provide additional information to their customers. See also help access level.
control

A tool for placing titles, spacers, reports, and other advanced features on a workspace.

cross tab

A method of displaying report data in a table format.

CSV (comma-separated value)

A file format with commas separating one column value from the next. Each row is delineated by a hard return. Also called *comma-delimited*.

cultures

A predefined set of attributes, such as decimal symbols and display formats, used to populate fields on the Currencies editor. Cultures are comparable to regions in Microsoft Windows. See also *Currency*.

Currency

A monetary denotation based on country of origin. Currencies can be defined for each country or province in which an organization does business. See also *Exchange rate*.

custom field

A field for gathering and displaying additional information about answers, contacts, incidents, opportunities, organizations, quotes, sales products, staff accounts, and tasks. Custom fields appear when adding and editing records. Depending on the type and visibility, they may also appear on the customer portal.

custom object

Any custom table created or managed from the object designer. Custom objects can be added to Oracle Service Cloud to integrate organization-specific data with the database. Although custom objects are not native to Oracle Service Cloud, they can be tied to standard objects and added to workspaces, workflows, custom reports, and navigation sets. See also *object* and *Oracle Service Cloud standard object*. 
custom page

A category or content page that can be fully customized to extend areas of a community in need of additional resources or exposition. See category page and content page.

custom report

A report that is created by copying and editing one of the standard reports in Oracle Service Cloud and saving it as a new report, or by combining data from selected tables in the database to create a new report. Custom reports can include customized output, data computation, and scheduling. See also standard reports.

customer

A contact or organization that has a service or purchase history in the knowledge base.

customer account

Information consisting of a user ID and password that allows customers to access certain functions on the customer portal, such as the Account Overview page. Customers can create an account by clicking the Sign Up link or the Your Account tab on the customer portal. Customer accounts are also automatically created when a customer without an account submits a question, which adds a contact record to the knowledge base.

Customer Portal Administration site

The site where administrative tasks, such as selecting the page set, viewing widget definitions and logs, and defining page set mapping, are performed.

dashboard

Any combination of individual reports shown together in one report. Using dashboards, staff members can search for and view a wide range of data from different reports without opening each report individually. The customer portal also includes a dashboard on the Customer Portal Administration site.
**data dictionary**

A list of all the tables in the Oracle database that can be accessed from the Service Console. Data dictionary also refers to the list of available tables and fields that can be used in custom reports and is accessed from the report designer. Functions, output variables, and computed fields can also be selected from the data dictionary when working with a custom report.

**data import template**

A saved format used by the Data Import Wizard to map columns in a CSV file to columns in the database. See [Data Import Wizard](#).

**Data Import Wizard**

An interactive utility used for importing records into the database.

**data lifecycle management**

Provides built-in policies to archive and purge unused or unrequired data automatically and periodically.

**data mining**

The exploration and analysis of large quantities of data to discover meaningful patterns and rules. Data mining enables organizations to turn raw data into information they can use to gain a marketplace advantage.

**data set**

The database tables and table joins that determine what data can be returned in a report. Data set also consists of the database columns a segment (dynamic list in Outreach and Feedback) will have access to and what filters will be used to determine the final data set.

**data type**

A set of data having predefined characteristics such as strings, integers, or dates. Each column in a database table is assigned a data type. Data type also refers to the type of custom field specified when adding answer, contact, incident, opportunity, organization, quote, sales product, staff account, and task custom fields. Data types for custom fields consist of menu, radio, integer, date, date/time, text field, and text area fields.
database

The tables that store information that is retrieved, edited, and added in an Oracle Service Cloud application. See also *data dictionary*.

Dbaudit

A utility that builds and populates the schema and performs the database portion of the Oracle Service Cloud update. Dbaudit can also be used to view the database schema.

Dbstatus

A scheduled utility that escalates incidents, answers, tasks, and opportunities based on business rules. Dbstatus also sends emails to those customers who have requested to be notified when a particular answer has been updated, and processes private Twitter messages for the social monitor. See Answer update notification, Business rules, and Social monitor.

Dead

One of the default opportunity statuses and status types. An opportunity with the Dead status is no longer being pursued by a sales representative.

decision

A component of a campaign. Decisions filter contacts by specified criteria and can have Yes and No paths.

decryption

The process of converting encrypted text into readable text using private keys assigned to authorized persons.

default directory

The directory containing original default copies of all the files customizable through the File Manager. During an update, any files that have changed will also be updated in the default directory. Using the restore function, a file can be restored to the original configuration. See *File Manager*. 
**deliverability**

The degree to which an email message aligns with industry-accepted practices to ensure delivery to an intended recipient. Emails with low deliverability are often blocked by ISPs and spam filters.

**dependency**

A relationship or association between items in the database in which the use of one item impacts the functionality of the other item. When a dependent item is deleted, such as deleting a contact list used in a mailing, all items that use the dependent item become invalid and must be manually updated.

**deploy**

To stage customer portal pages from the development folder and then promote the staged files into production. See also *stage* and *promote*.

**deployment log**

The record of actions taken on customer portal files, including staging, promoting, rolling back, and updating through upgrades and service packs.

**deprecated**

A condition that indicates a feature or widget has been replaced with different functionality or a newer widget.

**design space**

The section of the workspace designer where fields and controls are added, edited, moved, and removed to create a workspace.

**desktop usage administration**

Functionality for managing desktop user sessions to help organizations lower seat usage for licensing compliance and reduce costs. The administrator can manage both active and inactive sessions using force logout and automatic logout options. See *automatic logout* and *force logout*. 
desktop workflow

A sequence of workspaces, scripts, decisions, and actions presented to staff members as a dynamic interface to support complex business processes.

development area

The set of customer portal files that can be edited and viewed without being available to customers. Designers and developers can work on these files and test their changes until they are satisfied that the files can be made publicly available to their customers, at which point the development files are staged and promoted to the production area. See also production area.

display position

The position where a new answer appears on the Answers page. Options include Historical Usefulness; Place at Top, Middle, or Bottom; Fix at Top, Middle, or Bottom. The display position is selected from the answer’s Display Position drop-down menu.

disposition

An option for classifying and recording how incidents are ultimately resolved. Up to six levels of dispositions are available.

distribution list

A mailing list of non-staff member email addresses used for scheduling reports or any mailing event.

docked filter

A runtime selectable filter or output variable that is added to the top of a report. Docked filters let report users select different runtime filter values and output variables in the report, bypassing the Search window.

document

The material used in a survey or mailing, or served as a web page that can contain text, snippets, conditional sections based on contact filters, merge fields, links, and web forms.
DomainKeys (DK)
A form of email authentication that uses a cryptographic signature to verify that an email message originated from a specific organization. DomainKeys differs from DKIM authentication primarily by the email headers used to generate the signature.

DomainKeys Identified Mail (DKIM)
A form of email authentication that uses a cryptographic signature to verify that an email message originated from a specific organization. DKIM differs from DomainKeys authentication primarily by the email headers used to generate the signature.

dormant incident
An incident that is not returned when performing word- or phrase-based searches. After remaining in the Solved status for a specified time, incidents become dormant to ensure that the knowledge base is populated with the most useful and timely information.

Draft
The preliminary status of a mailing or survey. When a mailing or survey is created, it is set to the Draft status. The status will also return to Draft if the mailing or survey’s schedule is canceled.

drill down
To start at a top or general level and become more specific at each lower level. The drill-down feature enables access to additional output levels in reports.

drill-down filter
The fields in an output level used to filter the data returned when drilling down to another output level. This impacts what data is returned in the drill-down level.

drill-down link
The field in an output level that is used as a link to drill down to the next output level.
**dynamic form**

A form that hides or displays fields based on a customer’s response to other fields on the form.

**editor**

A layout format on the content pane when working with records and configuration items. Editors contain the fields for adding and editing records and items.

**Else clause**

The clause that follows the Then clause of a business rule. If the conditions of a rule are met, the actions in the Then clause are invoked. If the rule’s conditions are not met, the actions in the Else clause are invoked.

**email address sharing**

Functionality that allows a single email address to be shared by multiple contacts, such as members of a family or team. When enabled, a contact-matching process is used to associate records and transactions initiated by a shared email address.

**email answer**

A feature that enables customers to email answers they are viewing to a specific email address.

**email management**

Functionality that sends and receives email messages, processes bounced messages, intelligently routes incoming inquiries based on business rules, and automatically suggests answers to inquiries.

**email message**

An email that is automatically sent to customers or staff members. The process of sending email messages is triggered by events in Oracle Service Cloud. For instance, when a customer submits a question, the Question Receipt message will be sent to the customer’s email address. Using the Message Templates editor, staff members can customize each message and standardize their design to give them all the same look and feel. See message templates and Global template.
encryption

The process of translating a text message into unreadable text to ensure security. Encrypted messages may be read only by authorized persons with access to a private key that allows them to convert the message back into readable text.

escalation

A means of tracking answers, incidents, opportunities, and tasks using business rules. When a rule’s conditions are met, the rules engine schedules escalation to the new level. When the scheduled time (based on absolute or relative time) arrives, the rules engine sets the escalation level and takes the action specified by the rule, such as sending an email, notifying a manager, or following up with a customer. See business rules.

even split mode

A market testing option for broadcast mailings and surveys that sends test messages to equal portions of an audience. See market testing.

event (Named/Exit/Finish)

An action defined in a script rule or workspace rule that can be used to trigger other rules or workflow connectors. Events are defined by adding event fire actions, such as the Fire a Named Event action.

Everyone access level

An access level designed to allow answers to be visible to all customers depending on the answer status.

exception

A method of highlighting report data that meets certain criteria. Data exceptions also allow email alerts to be sent when data in a scheduled report meets the exception criteria.

exchange rate

A scale of monetary conversion from one currency to another. See Currency.
explorer

A layout format on the content pane that displays a tree on the left, containing folders and other items, and a detailed list of the selected folder’s contents (subfolders and files) on the right. Explorers are available for certain configuration items and components in Oracle Service Cloud.

expression

A component of fixed and runtime selectable filters that defines a function, database column, value, or any combination of the three.

extend

Using the widget builder to create a new widget by modifying the behavior and attributes of an existing widget.

external event

A program or script that runs as the result of an event occurring in Oracle Service Cloud, an action specified in a business rule, or an action in a marketing campaign.

external suppression list

An email delivery filter used to exclude an explicit set of email addresses from all mailings and surveys. When a mailing or survey is launched, contacts with email addresses in the list are filtered from the audience by default.

FCRR (first contact resolution rate)

A statistic that reports how often staff members or groups solve incidents with only one response. This number is displayed as the percentage of incidents solved with only one staff response.

file

A file that is uploaded to Outreach for attaching as a link in a document or snippet. From the Content Library, files can be uploaded and their characteristics can be defined.
file attachment

A file that is attached to an answer, contact, incident, opportunity, organization, or task, or sent with an incident response or quote. Files that are permanently attached to an incident or answer can be viewed by customers who view the record. Files that are sent with an incident response can be opened with the customer’s email client and are not permanently attached to the record.

file attachment answer

A type of answer that appears as a file attachment.

file link

A clickable link to a file attachment that is inserted in a snippet or a document.

File Manager

The interface used to modify files for Oracle Service Cloud products. Administrators can modify files used to customize a site’s Chat images, custom scripts, wordlist files, dictionary files, and certificate directories.

File menu

The interface element used to access the application menu. The File menu is located to the left of the Home tab on the ribbon. See also application menu.

final message

A mailing format used to send the mailing as final. In broadcast mailings and surveys, final messages are sent to all audience members who have not yet received a test message.

first due

A queuing pull policy that uses the incident due date or longest wait to determine which incidents or chats to retrieve from the queue.
fixed filter

A component of Analytics and Outreach and Feedback segments used to define the data set available in the report or segment. Fixed filters are statements constructed from expressions, functions, and operators, and cannot be altered when using a segment or when running a report. See also custom report and segment.

flag

A method for defining the priority of a record. A flag displays at the top of records and staff members can add text to the flag and change the flag importance (red=high, blue=medium, green=low, white=no importance).

flow diagram

A graphical representation of a campaign, survey, or desktop workflow. Flow diagrams allow staff members to diagram the events and decisions of a campaign, survey, or business process. When a campaign or survey is launched, contacts are automatically moved through the flow based on the specified criteria. When a desktop workflow is associated with a record editor in a profile, staff members with that profile will move through the flow when opening a record of the corresponding type. See also desktop workflow.

force logout

A way of managing desktop user sessions by manually logging out staff accounts who are currently logged in. Force logout is part of desktop usage administration, which assists organizations in lowering seat usage for licensing compliance. See also automatic logout and desktop usage administration.

forecast

A projection of revenue for an opportunity that may close in a given sales period.

foreign key

A column or columns that contain values found in a primary key of another table. Foreign keys are used to ensure relational integrity and are rarely primary keys. See also primary key.
Forward to Friend link

A link that enables contacts to forward the message to another email address. This type of link can be added to documents, templates, and snippets for use in mailings, surveys, or web pages.

framework

The underlying code structure of the Customer Portal, which offers a standard reference implementation as well as the ability to customize code for particular applications.

function

A mathematical operator that can be applied to data from database fields to modify the data that is returned in an output column. Function also refers to a container for business rules. Functions are used anywhere in a business process that dictates doing the same thing in more than one place. Functions reduce the number of rules needed by allowing the same rules to be evaluated from multiple states. See also business rules and rule state.

Give Feedback

A link on the sidebar on the Customer Portal template that customers can click to submit feedback about an organization’s website, customer service, or product satisfaction.

Global header

The global header, located at the top of the Agent Browser ui, contains options for working in oracle service cloud.

Global template

An element of message templates functionality containing the content that frames the message-specific content in each system-generated notification and email message. The global template is used to standardize the design of outgoing messages to give them the same look and feel. See message templates.

group

A way to organize staff accounts in Oracle Service Cloud. In communities, group refers to a collection of members based on a common interest, cause, or organization.
group type

A classification used to organize groups in a community and expand searching of related members and content.

grouping

A method for grouping data in a segment. Filters can be used when grouping and are applied to the data after the grouping is completed.

guest

Any community visitor who is not logged in with a community account.

guide

A collection of branching questions, responses, answers, and text explanations used in guided assistance. Guide also refers to information about a promotion generated by a marketing staff member. This information appears on the Offer Advisor window to help agents present the promotion to customers. See guided assistance and Offer Advisor.

guided assistance

A component that helps agents quickly locate answers and text explanations using branching questions to guide them to the answers they need. The answers and explanations agents find can be sent to customers in incident responses or relayed to customers over the phone. Guides can also be made available to customers on the customer portal to help them find their own answers to questions.

hash

A ten-digit alphanumeric string used to identify a specific hive, page, group, or member for certain community functions.

help access level

An answer access level for context-sensitive answers. Help answers are not visible to customers except through special hyperlinks. See context-sensitive answers.
Hosting Management System (HMS)

An application used to manage a Service Cloud update. It manages scheduling and notifications, and includes checklists of tasks that must be performed prior to and following an update to a new release.

hive

A resource entity, such as a blog or message board, used by community members to communicate about a central topic, theme, or goal. Hives are sometimes referred to as resources.

hive permissions

The set of permissions that allow members to perform specific actions in the hive, such as adding members, posting content, or commenting on posts.

hive privacy level

The hive access status determined by the community privacy level and hive permissions. See community privacy level and hive permissions.

hive template

A hive that is set to the Template status, making it accessible as a design template but not editable or searchable by the community. See also hive.

hive type

A classification used to organize hives and expand searching of related content.

HTML answer

A type of answer that appears to customers as standard HTML on the customer portal.
HTML editor

A WYSIWYG (what you see is what you get) editor for formatting and editing answers, mailings, campaigns, documents, questionnaires, invitation messages, and message templates in HTML without previous HTML experience.

identity provider

A third party that authenticates user information and sends verification to a service provider, such as Oracle Service Cloud, allowing single sign-on for the user. See also SAML 2.0 open login.

IMP (import) file

A data file with an extension of .imp that is used by the Kimport utility to map values in the CSV file to columns in the database.

In Meeting

One of the default chat agent statuses. This status indicates that the agent is in a meeting and is unavailable to chat. The In Meeting chat agent status has an Unavailable status type.

Inactive

One of the default opportunity statuses and status types. An opportunity with the Inactive status is no longer being pursued but could be activated at a later date.

inbox

An agent’s personal queue consisting of all the incidents that have been assigned to the agent.

inbox limit

The maximum number of incidents in an agent’s inbox that cannot be exceeded when pulling from a queue. The inbox limit is set in the profile to which the agent is assigned.
incident

Any question or request for help submitted by a customer through the Ask a Question page, email, a chat session, site or answer feedback, or from an external source using the API. Incidents can also be added by agents when they work with customers by phone, fax, or mail, and when responding to a private Twitter message.

incident archiving

A process that permanently removes incidents from the database. Archived incidents are then stored in searchable data files. Staff members can access archived incidents once the Archived Incidents component has been added to their navigation set.

incident custom field

A field for gathering and displaying additional information about incidents. Incident custom fields appear when adding or editing an incident and on the Ask a Question and Support History pages on the customer portal.

incident thread masking

A method of protecting sensitive customer information, such as social security and credit card numbers, from displaying in incident threads. Three default system masks are available and custom masks can be created.

incident queue

A sequence of unassigned, unresolved incidents. When an incident queue is added, it can be defined as the default queue. Incidents are added to queues automatically by business rules or manually by re-queuing and are handled in a first-in, first-out manner.

incident severity

An option for classifying and recording an incident’s importance and urgency.

incident status

A method of tracking an incident’s state. The default incident statuses are Solved, Unresolved, Updated, and Waiting, and custom statuses can be added.
incident status type

The status of an incident as it moves through the system. Default incident status types are Solved, Unresolved, and Waiting.

incident thread

The list of all activity on an incident, including the original question, agent responses and updates, customer updates, records of conversations, and internal notes about the incident (which are not visible to customers). The incident thread lists activity in chronological order and can be filtered by thread type.

index

A database item that can be added to a database field to speed up searches for information in the field. Adding an index to a field increases the amount of time it takes to write information to the field, and indexing a large number of fields decreases the overall responsiveness of the database. Generally, only fields containing a large amount of information that are regularly searched on should be indexed. In Oracle Service Cloud, indices can be added to most custom fields and custom objects. See also custom field and custom object.

indexing

A process in which the text of an answer or incident is stemmed and indexed into keywords and phrases. These keywords and phrases are used to build the answer and incident phrases tables that are used during text searching. When an answer is added or updated, the Keywords, Summary, Question, and Answer fields are stemmed and indexed to create one-, two-, and three-word phrases. When an incident is added or edited, the Subject field and incident thread are stemmed and indexed to create one-word phrases.

industry type

An option for classifying organizations by type of industry.

information gaps

A report that clusters incidents and compares the topics to answer clusters, allowing organizations to pinpoint those areas (or gaps) in the knowledge base needing additional answers.
initial state

A required state in every rule base. The rules engine evaluates a new or updated object using all rules in the initial state. Unless one or more rules in the initial state transition the object to a function or different state, the rules engine stops after all the rules in the initial state have been processed. See also rule state.

inline

A method of displaying output definitions and filter definitions as lines of text in the report. See also output definition.

inlay

A portion of code controlling a number of functions that you can deploy on an external web page or on traditional customer portal pages.

inline editing

A feature for editing values directly on a report without having to open each record to make changes. Staff members can edit individual values in one record or select several rows to change values in multiple records. Staff members must have permission in their profile to edit the specific record type, and inline editing must be enabled in the report.

inner join

A relational database operation that selects rows from two tables on the condition that the value in the specified column of the primary table is equal to the value in the specified column of the secondary table. See also outer join.

interface

The console, windows, and pages used by staff members and customers to access an Oracle Service Cloud application and interact with a single knowledge base. The interface name determines the URL for the website, the name of the executable, and the .cfg directory name. See also administration interface and agent desktop.

Interface Manager

A utility for managing multiple interfaces using one knowledge base.
invitation method

A way of distributing a broadcast survey, transactional survey, or website link survey.

Kexport

A utility for exporting either single tables or an entire database from an Oracle Service Cloud application.

Keywordindexer

A utility that creates an index of the keywords found in incidents, answers, file attachments, and documents indexed by the Web Indexer. The keyword indexes are used when searching incidents, answers, file attachments, and other indexed documents. See also Web Indexer.

Kimport

A utility for importing data, either single tables or an entire external database, into the database.

knowledge base

All information (such as answers, assets, incidents, contacts, organizations, opportunities, products, staff accounts, tasks, mailings, and campaigns) maintained and presented by Oracle Service Cloud in a meaningful way. Knowledge base also refers to the interrelationships among the pieces of information.

knowledge engineer

The staff member responsible for populating and maintaining the answers in the knowledge base. Responsibilities may include identifying when answers should be added, editing proposed answers, and reviewing existing answers to keep them current.

Langcvt

A utility for changing the language pack in Oracle Service Cloud from English to an alternative language pack. This utility converts the message bases and pre-populated knowledge base to the new language.
language

The language for a specific interface that determines, in part, what answers are visible for viewing by customers.

Launched

A mailing and survey status that indicates a transactional mailing or transactional survey has been launched and can be included in a rule or campaign.

layout

A predefined format that can be used in custom reports to apply fonts, colors, and other display options. Layouts can also be used in dashboards to apply a predefined structure for inserting reports.

lead

A potential opportunity. A lead is a contact discovered through a marketing campaign and forwarded to a sales representative through Opportunity Tracking. See opportunity and Opportunity Tracking.

lead rejection type

An option for classifying and recording the reasons for rejecting a lead.

leaf level

A level of product, category, or disposition that does not contain any sublevels. See product linking.

learned link

Related answers that have a learned relationship as a result of customer activity.

Live Chat

A link on the sidebar on the Customer Portal template that customers can click to submit a request to chat with a chat agent.
Live Media bar

The toolbar that displays when Chat is enabled. The Live Media bar allows agents to log in, log out, set their status, and manage chats. See Oracle RightNow Chat Cloud Service.

local settings

Customizations made by staff members to dialog and tool window sizes and locations, as well as content pane and navigation pane settings, console color and tint, toast notifications, and report appearance, including display and data settings and column formatting. Changes made by staff members to customize these settings affect only their workstation. In addition, staff members can return to the system defaults at anytime.

logical expression

An expression that defines the relationship between report filters or business rule conditions. The components of a logical expression are joined using Boolean logic and can be grouped and joined with AND, OR, and NOT operators.

logical operators

The symbols, (+) and (–), that can be used in most search techniques in Service to explicitly find answers that have a word (+) or that do not have a word (–).

Login window

A dialog box for entering user name, password (if required), and site information to access the administration interface of an Oracle Service Cloud application.

Lookup field

A field in a custom object designated to store values that are used as the names of the object’s records. These names display on editor tabs and the navigation pane’s Recent Items list. For instance, the Recent Items list displays incident reference numbers since the Reference # field is designated as the lookup field for incidents. Values in lookup fields are also displayed in reports instead of the ID values from fields in other tables that link to the lookup field’s table. For instance, while the incidents table’s Assigned Account field stores account ID numbers, the values displayed for this field in reports are from the accounts table’s Full Name field.
Lost

One of the default opportunity statuses and status types. An opportunity with the Lost status has been lost, for example, to a competitor.

mailbox

An email box specified in Oracle Service Cloud and dedicated to collecting email inquiries sent by customers, responses to mailings, and bounced messages. Incoming emails are processed by the Techmail utility. See also Oracle-managed Service mailbox and Techmail.

mailer daemon (rnmd)

A utility that monitors Outreach and Feedback, listening for requests from other components to start the email process. The mailer daemon is installed during the initial installation and can be configured to send messages in the most efficient manner for an organization.

mailing

A collection of one or more messages sent to one or more contacts. A mailing can contain multiple messages for testing purposes.

mailing status

A method of tracking the state of a mailing. The default mailing statuses include Draft, Launched, Scheduled, Preparing to Send, Sending, Suspended, Suspended by Error, Canceled, and Completed.

manual policy

A pull policy that enables agents to manually pull incidents into their inbox from any queue designated in their profile.

manually related answer

A relationship between two or more answers manually defined by a staff member.
market testing

A method for testing different message formats in mailings and surveys on a percentage of the audience before launching a final email. For broadcast mailings and surveys, market testing is available in even split and random sampling modes. For transactional mailings and surveys, market testing is available in audience sampling mode. See audience sampling mode, even split mode, and random sampling mode.

mask

A defined pattern that determines the format of information that can be typed in a field.

Master template

The settings that define a community’s navigation elements, footer content, and fine print text.

matrix question

A question type for displaying a series of survey questions in a table. Matrix questions are useful when a group of questions can be responded to with the same set of answer choices.

member

A community user who has a login and can be associated with one or more groups in the community.

member type

A classification for community group members that defines their role and provides access to certain group functions.

merge field

A variable field that looks up account, contact, incident, opportunity, organization, or tracked link information and inserts it in the text of a document, snippet, document template, message template, quote template, or the message content and mail attributes of mailings and surveys.
merge report

A report that can be included in marketing and survey content that dynamically limits the data returned so that customers see only their own information. For instance, if the report lists contacts and their open incidents, customers see only their own open incidents.

message

An email consisting of a collection of HTML, text, and images in a particular format.

message base

An editable text string that allows international language support and customization of headings, labels, buttons, and other text on the administration interface and customer portal and in email messages and notifications.

Message Bases editor

The interface element used to customize the message bases, including all the headings, labels, buttons, and other text, on the administration interface and customer portal.

message templates

A component for customizing and standardizing the content of administrator notifications, administrator emails, and contact emails. Message templates consist of a global template, which is used to standardize the design of outgoing messages, and a set of system-generated messages. See also global template.

migration

The process of moving from one version of the Customer Portal framework to a newer one. Migration can occur independently of upgrading to a newer version of Oracle Service Cloud. See also upgrading.

mobile customer portal

The template and set of customer portal pages that have been optimized for display on mobile devices such as iPhones, Androids, and Palms. See also template and reference implementation.
**model question**

The associated question and answer that reside in the Virtual Assistant database. Model questions are linked to answers in the knowledge base and are displayed as similar questions on the Answers page of the customer portal. See Oracle RightNow Virtual Assistant Cloud Service.

**Monitor**

A feature in Chat that allows a supervising agent to monitor the chat sessions of other agents and to intervene when necessary.

**Msgtool**

A utility for creating a configuration report for an Oracle Service Cloud site, or for changing configuration settings when an error has been made in one of the settings that subsequently locks staff members out of the Configuration Settings editor.

**multi-select**

A feature for updating more than one record at a time.

**multiline**

A method of displaying report data grouped under headings based on common values in report columns.

**natural language**

Any approach that accepts and correctly handles human language. For example, English, French, and Japanese are natural languages, while computer languages, such as FORTRAN and C, are not. The knowledge base can be searched using natural language technology.

**navigation buttons**

The buttons on the navigation pane associated with record types and components. Clicking a button displays the record type or the component’s navigation list.
navigation list

All the reports, folders, and items associated with a specific record type or component in Oracle Service Cloud. Navigation lists are organized in a tree on the navigation pane.

navigation pane

The area on the left and right side of the console where staff members work with navigation lists, select items to open on the content pane, and search the knowledge base. In the default configuration, the left navigation pane contains Recent Items and Navigation tool windows; the right navigation pane contains the Quick Search tool window. What appears on the navigation pane depends on the navigation set assigned in each staff member’s profile and the permissions assigned in the profile. Each navigation pane can also be customized by staff members. See also Configuration button, navigation buttons, and Tool window.

navigation set

Any combination of navigation buttons and their associated navigation lists. The Configuration button can also be added to navigation sets. Staff members are assigned a default navigation set in their profile.

next-update checklist

The UMS checklist that keeps track of all recurring tasks for each product enabled in your application. When the next update is scheduled, the tasks in this list checklist are automatically added to the pre-update checklist.

normalized URL

A URL that has been reformatted to ensure that documents that are referred to by multiple URLs will be indexed only once. Normalization may include reformatting domain names (for example, removing capital letters) or removing query parameters.

note

Information that can be added to campaigns, contacts, documents, mailings, opportunities, organizations, and surveys for internal reference. Notes can also be added to incidents in the incident thread.
notification

A message that notifies appropriate staff members about incidents, answers, mailings, campaigns, opportunities, and system errors. See also Answer update notification.

object

Any standard or custom table in the Oracle database. Object also refers to the specific answer, contact, incident, chat session, opportunity, organization, target, or task that is evaluated by the rules in the object’s rule base. See also custom object, Oracle Service Cloud standard object, and rule base.

object event handler

A PHP script with an integrated test harness (automated test script) that executes as the result of an event occurring on a standard or custom object in Oracle Service Cloud. See also custom object, Oracle Service Cloud standard object, and process model.

offer

A promotion developed by marketing personnel or a product suggestion generated automatically by Offer Advisor that is presented to a customer by an agent.

Offer Advisor

Functionality for creating and presenting promotions to customers and for making automatic recommendations based on customer attributes and purchase history.

On Break

One of the default chat agent statuses. This status indicates that the agent is on break and is not available to chat. The On Break chat agent status has an Unavailable status type.

open login

The ability to log in to the customer portal using an already established external account, such as Facebook, Twitter, or Google. When the external site validates the customer and the customer approves the transfer of information to Oracle.
Service Cloud, a contact record is created using the email address and the customer is automatically logged in to the customer portal.

**operating system**

The program that, after being initially loaded onto the computer by a bootstrap program, manages all other programs in a computer. UNIX, Windows, VMS, OS/2, and AIX are all examples of operating systems.

**operational database**

The database that contains the live data that is viewed, retrieved, and edited in an Oracle Service Cloud application. While reports that are run on the operational database can access real-time data, the reports cannot process as much information as reports that are run on the report database. See also report database.

**operator**

A symbol or word that represents a mathematical or logical action that can be applied to a condition or value.

**opportunity**

Information about a specific sale or a pending deal that is tracked and maintained in the knowledge base.

**opportunity custom field**

A field for gathering and displaying additional information about opportunities. Opportunity custom fields appear when adding or editing an opportunity.

**opportunity status**

A method of tracking an opportunity’s state. The default opportunity statuses are Lead, Reject, Active, Closed, Lost, Inactive, and Dead. Custom statuses can also be added.

**opt-in**

The explicit granting of permission by a contact to receive email communications from an organization. Opt-ins can be specific to certain mailing lists or applied globally across all mailing lists.
**opt-out**

An explicit request by a contact to be removed from a specific mailing list or from all lists, most often communicated by email or web form. Also called *Unsubscribe*.

**Oracle-managed Service mailbox**

The recommended type of Service mailbox created by Oracle. Oracle configures the initial mailbox setup, including enabling incoming email and defining the Pop Server, POP Account, and Password fields. Administrators can also create general Service and Outreach mailboxes for their application.

**post-update checklist**

A *UMS* checklist that contains tasks that are specific to and created by your organization. The tasks on this list are enabled when your update is complete. See also *pre-update checklist* and *next-update checklist*.

**Oracle RightNow Analytics Cloud Service (Analytics)**

A business reporting solution that enables organizations to capture, organize, present, and disseminate real-time actionable knowledge with speed and ease. Using Analytics, organizations can increase insights by identifying customers based on previous interactions across all channels.

**Oracle RightNow Chat Cloud Service (Chat)**

A component that provides customers with access to chat agents for questions and issues that require human interaction.

**Oracle RightNow Connect Desktop Integration (JavaScript API)**

A public API that enables customers and partners to integrate data contained on a workspace with a web page that is contained on the workspace. If external information is presented about the current record in a web page, this API can be used to update or read workspace data from the web page. See also *workspace*. 
Oracle RightNow Connect PHP API Cloud Service (Connect PHP API)

A backward-compatible, public API that enables customers and partners to integrate with the Oracle Service Cloud platform using PHP scripts. Connect PHP API is primarily used to integrate with the customer portal, but it can also be accessed through the File Manager, process designer, and analytics. Connect PHP API leverages the Connect Common Object Model, which is also leveraged by Connect Web Services for SOAP.

Oracle RightNow Connect Web Services for SOAP (Connect Web Services)

A backward compatible, public API that enables customers and partners to integrate with the Oracle Service Cloud platform using industry leading standards such as WSDL 1.1 and SOAP 1.1. It provides broad support for a wide variety of languages, platforms, and tools. Connect Web Services leverages the Connect Common Object Model, which is also leveraged by Connect PHP API. See also Oracle RightNow Connect PHP API Cloud Service.

Oracle RightNow Customer Portal Cloud Service (Customer Portal)

The website interface that customers access for customer support. The customer portal is integrated with Service so customers can query the knowledge base for answers, ask questions, provide feedback, manage their customer account, and request chat sessions. It consists of a standard set of files that can be customized, uploaded, staged, and promoted to make the site available to customers. See also Mobile customer portal.

Oracle RightNow Cloud Service (Service)

A customer service and support solution that intelligently assists both customers and agents with inquiry resolution across standard and social channels. Service assists customer service and support organizations that need to easily capture, respond to, manage, and track all service interactions in one consolidated application.

Oracle RightNow Desktop Add-Ins Cloud Service (desktop add-ins)

An add-in framework for the Oracle Service Cloud platform that enables customers and partners to build custom .NET components, controls, and applications for the agent desktop. See also Agent desktop.
Oracle RightNow Feedback Cloud Service (Feedback)

A customer survey tool for gathering information about customers’ experiences with an organization. With a wide range of customization and formatting options, questions types, and full analytics for efficient reporting, surveys provide organizations with a flexible method of tracking customer satisfaction.

Oracle RightNow Opportunity Tracking Cloud Service (Opportunity Tracking)

A sales automation solution that enables staff members to easily manage all opportunity, organization, and contact information and track all quote interactions in one consolidated application.

Oracle RightNow Outreach Cloud Service (Outreach)

An email and campaign solution for delivering personalized, richly formatted email communications to targeted segments of customers and prospects and for launching full-scale marketing campaigns.

Oracle RightNow Self Service for Facebook Cloud Service (Self Service for Facebook)

A Facebook application that provides access to customer-facing features of Oracle Service Cloud, such as Find Answers and Ask a Question, directly from Facebook’s web and mobile interfaces.

Oracle RightNow Social Experience (Social Experience)

A set of complementary components, including Communities, Channels, Social Monitor, and Self Service for Facebook, each representing a different, powerful way of interacting with customers using social media. While each component serves a distinct purpose, they can be used together to create a wide-ranging social web presence.

Oracle RightNow Social Experience communities

A comprehensive social web solution consisting of Oracle RightNow Support Community Cloud Service and Oracle RightNow Innovation Community Cloud Service that lets customers connect, discuss, and contribute through forum discussions, question-and-answer sessions, resource libraries, and suggestions for service improvements.
Oracle RightNow Social Monitor Cloud Service (Social Monitor)

A monitoring tool for gathering and acting on information about an organization and its products that appears on social networking services such as Twitter and YouTube.

Oracle RightNow Virtual Assistant Cloud Service (Virtual Assistant)

A solution for identifying the intention behind a customer’s question using semantic search technology and linguistic dictionaries to return highly relevant search results and provide virtual assistant chats.

Oracle RightNow Wireless

The interface for accessing Service from a wireless phone or any device with a WAP (wireless application protocol) browser, such as a PDA (personal digital assistant).

Oracle Service Cloud

A customer experience suite combining web, social, and contact center experiences for a unified, cross-channel service solution in the cloud.

Oracle Service Cloud Smart Client

The web-based software that allows local applications to interact with the server-based applications. The smart client can be installed on staff workstations using the Click-Once installer. See also Click-Once installer.

Oracle Service Cloud standard object

Any standard table that is native to Oracle Service Cloud. Standard objects store data, including record types such as answer, contact, incident, opportunity, organization, and task. Other standard objects include accounts (staff accounts), assets, quotes, and sales products. See also custom object and object.
organization

Any company, business unit of a large company, or government agency that has an organization record in the knowledge base.

organization address type

A way of storing multiple addresses for a single organization. The default organization address types are Billing and Shipping; custom address types can be added.

organization association

A feature for associating a contact with a specific organization. Organization association links the incident and opportunity history of the contact and organization.

organization custom field

A field for gathering and displaying additional information about organizations. Organization custom fields appear when adding or editing an organization.

organization hierarchy

A feature for creating or changing the hierarchy of organizations. A hierarchy can be created by making one or more organizations subordinate to another organization. Twelve hierarchy levels can be used.

outer join

A relational database operation that selects rows from two tables regardless of whether the specified columns contain corresponding values. An outer join will return all rows from the primary table and any rows from the secondary table where the value in the specified column of the primary table is equal to the value in the specified column of the secondary table. See also inner join.

output definition

A description of a report that can be viewed when generating a report or when hovering over the report title and columns. Output definitions are predefined for all standard reports and can be defined when creating a custom report.
output level

A distinct section of a report that outputs report data. Reports can have multiple output levels, each of which can have their own filters, groupings, data exceptions, headers, footers, and descriptions. Output levels in a report are related through drill-down links and drill-down filters.

owner

The member who holds complete authority over a community group or hive. A member who creates a group or hive is designated as its owner unless ownership is transferred.

page

A web page or a customer portal page in an Oracle Service Cloud application.

page set mapping

The customer portal functionality that allows a specific page set to be mapped to a specific user agent. Customers are then directed to the most appropriate page set as determined by the browser or user agent accessing the customer portal.

panel

A customizable object used to display dynamic content on community pages. Panels can be added to custom pages and some standard pages. See also custom page.

path

The connector between items in a campaign flow diagram. A path can be one of four types (Standard, Submit, Yes, or No) and can connect two actions or an action and a decision in campaigns. See also action and decision.

Personal settings

An application option that lets staff members override settings in their staff account and customize settings that apply to the interface defaults in Oracle Service Cloud. Settings defined in staff accounts that can be changed include default currency,
default country, time zone, and email notifications. The staff account settings changed from the Personal Settings option will also be made to the corresponding settings in the staff account.

**pipeline**

Calculated revenue that has not yet been acquired but is forecasted to close in a specified time period.

**polling survey**

A survey that displays as a single question on a customer portal page or any page external to the customer portal. After customers submit their response, they see a poll results chart or a thank you message. See also Oracle RightNow Customer Portal Cloud Service.

**post**

Content added by users of a social media site, such as a Facebook status update or a text entry in Social Experience communities. See Oracle RightNow Social Experience communities.

**post type**

The structure of a post as defined by the sequence of fields and controls used to create its content.

**pre-update checklist**

The UMS checklist that becomes active when you request an update. It includes a list of Oracle-created tasks and any custom tasks that should be completed before your update.

**preliminary screen pop**

The toast notification that displays when an incoming chat request is received. The preliminary screen pop displays as a two-column table, and agents can view information about the chat request before accepting or declining the request.

**Preparing to Send**

A mailing and survey status that indicates a broadcast mailing or broadcast survey is about to be sent.
**price schedule**

An option for creating various pricing levels that can be assigned to sales products. Price schedules allow the same product to have different prices, such as wholesale and retail prices.

**primary contact**

The main individual associated with an incident or opportunity. All primary contacts have an associated contact record in the knowledge base. In Service, a primary contact must be associated with an incident for agent responses. In Opportunity Tracking, either a primary contact or an organization must be associated with an opportunity to serve as a point of contact for sales representatives during the sales process. See also contact.

**primary key**

A database table column that is indexed to enforce a unique constraint, meaning that a given value cannot appear more than once in the column. This column is used to uniquely identify each record in the table. Primary keys are often the target of a foreign key in a different table. See also foreign key.

**priority**

A ranking that defines the order in which incidents are pulled from multiple queues. The priority ranking also identifies which queues agents can retrieve incidents from.

**private**

One of two default answer status types. Answers that are marked Private are never visible to customers. See Answer status type.

**private key**

A password-protected key used by the holder to create digital email signatures and decrypt messages that were encrypted using the holder’s associated public key.
privileged access answers

Answers that are assigned a custom access level for viewing by certain contacts and organizations assigned to the appropriate service level agreement (SLA). See SLA.

process model

The virtual container that encompasses all event handlers (standard and custom) in Oracle Service Cloud. Using the process designer, a process model can be exported, imported, deployed, and rolled back. See also custom object, object event handler, and Oracle Service Cloud standard object.

product

An option for grouping answers and incidents that allows more precise organization in the knowledge base. Staff members can classify answers and incidents by product and up to five additional levels of sub-products, allowing more refined searching by customers and staff members. See also category.

product catalog

The list for organizing sales and asset products. See Asset product and Sales product.

product linking

An option for linking products to categories and products to dispositions so that category and disposition choices are narrowed to only those associated with the selected product for staff members working with incidents and customers searching on the customer portal.

Production area

The set of publicly available customer portal files and pages. The production area is updated when files in the development folder are staged and promoted. See also Development area.

profile

A mechanism for controlling access to administration functions and for assigning staff members specific permissions, default workspaces, a default navigation set, and report access.
promote

To copy all customer portal pages from the staging area into the production folder, where they become publicly available on an organization’s website.

promotion

A specific message (for example, a discount, renewal notice, or announcement) delivered to a specific group of customers using Offer Advisor. Promotions are generally created by marketing staff members and presented to customers by agents. See Offer Advisor.

proof

A way to review the content of a mailing or survey to ensure the message is approved by the necessary contacts and staff members and as a final check for any mistakes. Proofs can be sent to a proof list or group of staff members who, in turn, can accept or reject the proof. Proof messages can also be sent to staff members when changes have been made to message templates. See also message templates.

proof list

A contact list that is available to receive proof messages, enabling its contacts to review mailings and surveys before they are finalized.

propose answer

A function for proposing that an incident’s solution be added to the answers available to customers. The proposed answer is reviewed by the knowledge engineer, who determines if it should be made public and, if so, its access level, status, language, and visibility.

Proposed

One of the default answer statuses. This answer status indicates that the answer has been proposed by a staff member from an incident. Answers with a Proposed status are not visible to customers. See Answer status.
Public

One of the default answer statuses and status types. Answers marked Public may be visible to customers depending on their access level and language. See Answer status and Answer status type.

public certificate

See Certificate.

public key

Public information that may be attached to email messages to allow those who reply to the message to encrypt their response. The public key also verifies that the digital signature was created with the associated private key, thereby ensuring the integrity and authenticity of the message. Public keys are often referred to as public certificates, although certificates hold additional information besides the public key.

public key certificate

See Certificate.

publish report

A method of preserving a report’s graphical and tabular output as a snapshot. Once a report is published, it cannot be modified and the report data will remain unchanged even as the knowledge base is updated.

pull policy

The method for determining which queues agents can retrieve incidents or receive chat requests from and in what order. Pull policies include Strict Priority, Manual, and First Due.

pull quantity

The specified number of incidents to be retrieved from the queue at one time when an agent pulls incidents.
question

The main element in a survey. Text, choice, and matrix question types can be created. Questions can be used in multiple surveys, mixing and matching as necessary. See Choice question, Matrix question, and Text question.

questionnaire

The complete set of questions and all the pages in a survey. Using the HTML editor, staff members can create dynamic surveys using a graphical interface to add questions and create survey branches based on how customers answer. A questionnaire must be created for each survey.

queue

See Chat session queue and Incident queue.

queued report

A report that has been manually or automatically scheduled to run in the background after entering the report’s search criteria. When a queued report has been generated, a toast notification displays with a link to open the report.

Quick Access toolbar (QAT)

One or more buttons used as shortcuts to commands on the ribbon. The initial set of buttons on the Quick Access toolbar is specified by what is displayed on the content pane, but staff members can customize the toolbar to add frequently used buttons. By default, the Quick Access toolbar appears above the ribbon.

Quick Search

A component used to search for records and files when only limited information is known. Quick Search can be used to search the knowledge base no matter what navigation list is displayed or what is open on the content pane. Oracle Service Cloud contains a number of default Quick Search reports, and other reports can be added to the Quick Search button in navigation sets.

quota

The revenue goal assigned to a sales representative during a specified time period, such as month or quarter.
quote

A formal price assigned to a sales product for a particular customer during a sales period. Quotes also include any discounts applied as well as the valid dates for the quote.

quote custom field

A field for gathering and displaying additional information about quotes. Quotes custom fields appear when sending a quote with an opportunity.

quote template

A template defined for a specific type of quote. Quote templates are used when generating a quote for an opportunity. See also quote.

random sampling mode

A market testing option for broadcast mailings and surveys that sends test messages to a specified percentage of the audience. See market testing.

record

Any individual answer, asset, contact, incident, opportunity, organization, or task in the knowledge base. Records can also be created for custom objects, which can be added to Oracle Service Cloud to integrate organization-specific data with the Oracle database. See also Custom object, Oracle Service Cloud standard object, and Record type.

record type

A database table that stores all records of the same type, such as answers and incidents. See Record.

record pool

The memory space used to temporarily store all records loaded in a single desktop workflow session. See Desktop workflow.
record tabs

The layout of information contained in a record. Each tab contains specific fields and options related to the record that can be viewed and updated as necessary.

recurrence

A scheduling method used to send or initiate the same report, mailing, survey invitation, campaign, or cloud search on a regular daily, weekly, monthly, or annual basis.

reference implementation

The standard set of files used to create the default customer portal as it exists without customization.

regular expression

A combination of operators and character strings used to define a search field or a condition statement in a business rule.

Reject

One of the default opportunity statuses and status types. A lead with the Reject status has been rejected by a staff member.

related answers

A feature that assists customers in finding answers to questions related to the current web visit. Related answers appear on the answer details page and are sorted by relatedness those answers that appear at the top of the list are most related to the answer being viewed.

relationship item

A control used to create workspaces. Relationship items can include lists of records as well as other information such as audit logs and file attachments.
relative time

The amount of time between events based on the business work hours defined in service level agreements or default response requirements. Some functions, such as `rel_date_diff()`, support relative time values, as do some database fields such as `inc_performance.rel_time`. Note that the Relative option available for use in some filters has a different meaning where a dynamic time period can be defined instead of a time period using a static date and time. See also absolute time.

relative value

A field value set by a workflow, script rule, or workspace rule that adds or subtracts, appends, or prepends, a value to the field’s previous value (for instance, increasing the value of an integer field by 1).

report

Any standard report, custom report, or list of records accessed from a navigation list on the navigation pane. Standard and custom reports can also be accessed from the Reports explorer. Reports are also used to display lists of answers or a customer's incidents on the customer portal.

report database

A copy of the operational database that is used for reporting purposes. Reports that are run on the report database can process more information than reports run on the operational database. The data in the report database is copied from the operational database at scheduled intervals and therefore may not be as current as the data in the operational database. Also called replication database. See also operational database.

report control

A control that inserts a report into a workspace. See also workspace.

report linking

A feature for creating links between reports. Linked reports and dashboards can be seamlessly opened from other reports, just as report levels can be opened from other levels in the same report. Both conditional and unconditional links can be created.
report schedule

An option for subscribing to a standard or custom report. Staff members can schedule the report to be sent to an individual staff member, a group of staff members, a distribution list, an external email address, or any combination of these options.

report section

A section of an output level that contains a component of the report’s output, such as a title, chart, or tabular data.

report variable

An item added to a report that is used to return different data or data in different formats in the same column. For example, a single report can be created that displays the number of incidents by staff member, group, queue, or status. When running a report, the variable value is selected from the Search window or from docked filters.

Reportgen

A scheduled utility that sends out scheduled reports. See Report schedule and Scheduled report.

re-queuing

The action of moving an incident from an agent’s inbox into a queue.

resolution time

The maximum allowable time (in minutes) set by a service organization for resolving incidents. See also response requirements.

response interval

The days of the week and times when a service organization makes itself available to respond to and solve incidents on a daily basis. Days and hours can be specified. See also response requirements.
response requirements

The maximum time allowed (in minutes) for incident response and resolution within the operating hours defined by the organization. The response requirements are used to measure agent performance in responding to and solving incidents and can also be used for SLAs that do not have customized response requirements. See also SLA and response interval.

response time

The maximum allowable time (in minutes) set by a service organization for initially responding to new incidents. See also response requirements.

result grouping

A feature in a report definition for selecting fields to group data by. Result grouping provides a more organized view of a report. Multiple levels can be defined for result grouping. The more levels used, the finer the detail will be.

Review

One of the default answer statuses. This status can be used to notify the knowledge engineer when a public answer needs to be reviewed. See also answer status.

ribbon

All the tabs and buttons for performing actions and functions on an entire report, individual records in a report, or items in an explorer tree or list. The buttons on each tab are grouped by related functions, and each group is labeled. The tabs and buttons on the ribbon change based on what is displayed on the content pane.

rollover

A method of displaying additional report details by hovering over data described in the report’s output definition.

rollup

A method of displaying report data that groups records together by specific fields. The grouped records are displayed under headings that can be expanded or collapsed to display or hide the records under the heading.
root certificate

A self-signed certificate generated by a party that signs other public certificates. Certification authorities may authorize other entities to issue certificates. The root certificate belongs to the top-level certification authority.

round-robin queue

A type of incident queue in which unresolved incidents are automatically assigned to agents in a rotating fashion.

RPA (responses per assignment)

A statistic that calculates the average number of times a staff member or group responded to each incident.

RSS (Really Simple Syndication)

The primary standard used for the syndication of web content. RSS is an XML-based format used primarily for distributing news headlines on the Internet. Oracle Service Cloud contains an RSS channel so staff members can monitor RSS feeds for content. See Oracle RightNow Social Monitor Cloud Service.

rule

See Business rule.

rule base

All rules, states, functions, and variables associated with a particular object type (answers, contacts, incidents, chat sessions, opportunities, organizations, targets, and tasks) in business rules.

rule log

A feature for viewing the rule or rules that have fired against a specific answer, contact, incident, opportunity, organization, or task. See also business rules.
rule state

A container for business rules. Every rule base must contain an initial state, and states can be added to handle all stages of object processing. Rules in the initial state can transition objects to other states in the rule base. See also initial state.

rules engine

The software that evaluates objects to determine if they meet the conditions of any rules in the rule base and then executes the actions defined in the rules.

runtime selectable filter

A component that defines the initial data set available in a report and allows staff members and customers to customize the data returned. Runtime selectable filters are statements constructed from expressions, functions, and operators, and can be customized when running a report.

S/MIME (Secure Multipurpose Internet Mail Extensions)

A standard for sending secure email messages that can verify the sender’s identity. S/MIME emails can be encrypted for security and signed to verify authenticity.

safe mode

A login method that allows staff members to log in to Oracle Service Cloud without activating add-ins. Safe mode is available after malfunctioning add-ins have prevented administrators and staff members from logging in. See Add-in.

sales period

The period of time used to track the revenue goals assigned to each sales representative. The default sales periods are annual, semi-annual, quarterly, monthly, and weekly.

sales product

An option for identifying items or services sold by an organization. Sales products can be added to quotes and promotions.
sales products custom field

A field for gathering and displaying additional information about sales products. Sales products custom fields appear on the Custom Fields page of the Product Details editor.

sales representative

A staff member who may be assigned opportunities and who may also maintain contact and organization records.

SAML (Security Assertion Markup Language)

An XML-based protocol in which an identity provider authenticates a user’s identity and passes that information to a service provider, which can then decide to allow the user access to the service without requiring an additional login procedure. See also identity provider, SAML 2.0 open login, and single sign-on.

SAML 2.0 open login

A type of single sign-on that uses Security Assertion Markup Language (SAML) and is the protocol that Oracle Service Cloud uses for its single sign-on feature. See also SAML and single sign-on.

Scheduled

A mailing and survey status that indicates a broadcast mailing or broadcast survey is ready to be sent and will be emailed at the scheduled send date and time.

scheduled report

A report that is sent as an HTML email or HTML email attachment to staff members, distribution lists, or external email addresses at specified times. Scheduled reports can also be sent when alerts defined in data exceptions are triggered. See also exception.

schema

The structure of a database system described in a formal language supported by the database management system. In a relational database, the schema defines the tables, the fields in each table, and the relationships between fields and tables.
score

A calculated value that ranks the order of displayed answers. An answer’s score is determined by its solved count and any display position that was set when the answer was added or updated. Score also refers to the relative weight assigned to each choice in a choice question for surveys. Score values can be used for survey calculations to trigger rules or campaign actions based on a contact’s answers and also for reporting purposes.

screen pop

See Third-party screen pop.

script

A control that can be added to a custom workspace to help staff members enter record information in a logical order. Scripts can contain multiple pages with fields and other controls as well as branching logic to guide staff members to different pages based on actions they take on a script page.

script rules

A type of rule used to trigger actions, such as setting the value of a field, on script pages when specified conditions are met.

search and selection criteria

The runtime selectable filters and sorting options that can be defined when searching for a particular record. See also runtime selectable filter.

search index

A matrix that includes a list of important words within a document and their document of origin, allowing efficient searching. In some cases, the matrix is a database table. In other instances, the matrix is a file stored on a hard drive. For a word or phrase to be searchable within an incident, answer, file attachment, or external document, it must first be indexed.

search priority word

A word that is associated with an answer or a document. The associated answer or document will always be displayed to customers when the search priority word is included in their search text.
secure email

Incoming and outgoing email that has authenticity (the sender is who it appears to be), integrity (content has not changed during transmission), and privacy (only the intended recipient can read it).

seeding

The initial set of answers in the knowledge base.

segment

The criteria for creating dynamic lists of contacts based on user-defined filters. Multiple filters can be created and logical expressions can be used to create the exact data set needed to target contacts. Once a segment is created, it can be used in broadcast mailings and surveys and the group of contacts will be constantly adjusted and updated as they meet or fall outside of the segment’s requirements.

self-learning knowledge base

The automatic generation of self-service content based on customer interactions so that the most pertinent information is presented. See also knowledge base.

sender ID

A form of email authentication that identifies IP addresses authorized to send mail on behalf of a specific organization. Sender ID differs from SPF authentication primarily by the components of the email used to authenticate the message.

Sender Policy Framework (SPF)

A form of email authentication that identifies IP addresses authorized to send mail on behalf of a specific organization. SPF differs from Sender ID authentication primarily by the components of the email used to authenticate the message.

Sending

A mailing and survey status that indicates the broadcast mailing or broadcast survey is currently being sent to contacts. The system automatically sets the status to Sending after the mailing or survey is done being prepared to send or at the scheduled date and time.
Service Console

The user interface where staff members work in Oracle Service Cloud. Staff can add and edit records and items, generate standard reports and create custom reports, access their notifications, and chat with customers from this console. Administrators can also configure and customize their application from the console. Also called administration interface or agent desktop.

service level agreement

See SLA.

sharing

The process of sharing contacts, tasks, or both between Microsoft Outlook and Oracle Service Cloud. All sharing functions are initiated from Outlook.

Sibling answer

Related answers that share the same product or category. Sibling answers may also contain the same file attachments.

single sign-on

A method for a user (in Oracle Service Cloud, a staff member or customer) to log in to one application, known as an identity provider, and then be authenticated and logged in to another application, such as Oracle Service Cloud, without being required to log in separately to the second application. See also identity provider and SAML 2.0 open login.

SLA (service level agreement)

A contract that is applied to contacts and organizations specifying the level and type of customer service they are eligible to receive. Generic SLAs are created by administrators, and SLA instances are applied to specific customers, either automatically through business rules or manually by staff members. SLA instances are called service contracts on the customer portal and can be accessed from the Account Overview page. See also response requirements.
SLA instance

A customer’s individual copy of an SLA. An SLA is a generic contract that has not been applied to a specific customer. An SLA instance is a copy of the generic SLA applied to a specific customer.

slicing

A method of grouping tabular report data by a common element. When slicing, a common value in a field can be chosen and only those rows that have that value will be returned in the report. Other slice groups can be selected from links or a tree element.

Smart Interaction Hub (SIH)

Functionality for directing customer interactions to the most qualified source for resolution by leveraging agent skills.

Smart merge

A feature that allows staff members to merge similar answers in the knowledge base to provide more meaningful answers to customers and to reduce answer duplication.

SmartAssistant

Oracle technology that uses business rules to automatically suggest possible answers to customers’ email questions and Ask a Question queries. Staff members can use SmartAssistant to search for answers in the knowledge base that are related to an open incident or a current chat session. See also suggested answers.

SmartSense

Oracle technology that estimates a customer’s emotional state or attitude based on the words and language the customer uses when submitting a question in Service. SmartSense also rates the incident responses sent by agents. The SmartSense ratings for both customer and agent appear wherever they have been placed on the workspace. In Feedback, SmartSense evaluates text questions submitted by customers in surveys. In social monitoring, SmartSense evaluates posts returned from cloud searches.
snippet

Any text or part of a document that can be used in more than one document. Snippets can be added to documents from the Content Library component.

Social Monitor

A component for searching social networking sites to monitor and act on conversations about an organization and its products. See also Oracle RightNow Social Monitor Cloud Service.

Solved

One of the default incident status types and incident statuses. An incident marked Solved has been resolved.

solved count

The method for determining where an answer will display in the list of answers. The most useful answers (those with the highest solved count) are pushed to the top of the list, while those with the lowest ratings are moved down on the list. When a customer clicks one of the options in “Is this answer helpful?” on the answer details page, it directly affects the solved count. The solved count is increased for answers that are viewed, and the last answer viewed has a higher solved count than answers viewed earlier in the same web visit. The solved count is also increased when an agent uses a SmartAssistant suggested answer when responding to a customer’s question. By default, customer influence on an answer’s ranking accounts for 75 percent of an answer’s score, and agents affect 25 percent. Over time, an answer’s solved count gradually declines as it is viewed less frequently.

sort order

The sort order of a report’s output columns. The default sort order is defined when generating a report and can be modified when running the report.

Spacer

A control that is manually added to a workspace to maintain the row and column arrangement when fields and controls are moved and removed or to create white space in a workspace.
spider
See Web spider.

SSL (secure sockets layer)
An industry standard for secure Internet-based transfer of information.

staff account
The settings for a staff member authorized to access an Oracle Service Cloud application, including user name, password, profile, group assignment, and email information.

staff account custom field
A field for gathering and displaying additional information about staff members. Staff account custom fields appear on the Custom Fields page of the Staff Accounts editor.

staff member
Any employee with a staff account and profile authorized to access an Oracle Service Cloud application.

stage
To compile and optimize all the customer portal pages from the development folder, where they are created and tested, into the staging folder, where they appear exactly as they will when the staged files are promoted into production. Stage also refers to the level of completion of a particular opportunity within a specific strategy. Tasks can be defined within a stage and can be required to be completed before the opportunity can move to the next stage. See also promote, strategy, and task.

standard reports
The complete set of predefined reports available in Oracle Service Cloud. Standard reports can be copied and used to create custom reports.
standard text

Any text prepared in advance that can be sent to customers when responding to incidents, appended to responses by a business rule, or sent by an agent during a chat session. Also called standard response.

State

A field that classifies how contacts and organizations were added and what actions have occurred since their creation. The State field is automatically populated when a contact or organization record is added or updated, and staff members can also manually update the State field. State field options include Service, Outreach, Opportunities, and any combination of the three. State also refers to the current stage of an object in rules processing. See Rule state.

status

The current state of an answer, incident, mailing, opportunity, survey, or task. See Answer status, Incident status, Mailing status, Opportunity status, Survey status, and Task status.

status type

The current state of an answer, incident, or opportunity. Default answer status types are Public and Private. Default incident status types are Unresolved, Solved, and Waiting. Default opportunity status types are Active, Closed, Dead, Inactive, Lead, Lost, and Reject.

stopword

A word that is not included in the keyword indexes in Service and is not searchable as a result. Pronouns, articles, and adverbs are common stopwords.

strategy

A sales plan defined by an organization that includes stages and associated tasks that must be completed in order for opportunities to move through each stage. Strategies allow organizations to define multiple sales plans based on their business processes and help ensure that policies and procedures are enforced.
strict priority

A pull policy that defines the order in which the system pulls incidents or chats from multiple queues. The strict priority ranking also identifies from which queues agents can retrieve incidents.

style

All of the specifications that can be defined for presenting graphical and tabular data in a report, including fonts, colors, and borders.

subscription

A type of cloud search that pulls all available thread content from a custom Facebook or RSS channel account at regular intervals. See also cloud search.

suggested answers

The list of answers from the knowledge base that is returned when SmartAssistant is invoked, either by staff members working on incidents or engaged in chat sessions or through business rules that append answers to email questions and Ask a Question queries from customers. See also SmartAssistant.

suggestion

A product recommendation automatically generated by Offer Advisor using a predictive model based on customer purchase history.

Support Home

The entry page on the customer portal. This page provides customers with quick access to the tools they need to answer their questions and receive immediate customer service.

survey

A method of gathering customer responses and feedback. Surveys can be sent as mailings, served as a web page, or sent as events triggered by a campaign or business rule. See Oracle RightNow Feedback Cloud Service.
**survey status**

A method of tracking the state of a survey. The default survey delivery statuses include Draft, Scheduled,Launched, Recurrence Scheduled, Preparing to Send, Sending, Suspended, Expired, Suspended by Error, Canceled, and Completed.

**Suspended**

A mailing and survey status that indicates a mailing or survey has been temporarily suspended from the Sending or Launched status.

**Suspended by Error**

A mailing and survey status that indicates a transactional mailing or transactional survey encountered an error and has been temporarily suspended.

**synchronization**

The process of collecting and combining contact and task records in Oracle Service Cloud and Microsoft Outlook to ensure data is consistent between applications. Also called *sync*.

**syndicated widget**

A Customer Portal widget that can access the Oracle Service Cloud database from any external web page. The code used to place the syndicated widget on a web page is available under tag documentation on the Customer Portal Administration site.

**system attribute**

A customized field that can be added to account (staff account), answer, asset, contact, incident, opportunity, organization, quote, sales product, and task standard objects. System attributes can be displayed in reports and workspaces, and can be used when defining relationships between standard and custom objects. See Custom object and Oracle Service Cloud standard object.

**table instance**

A component of a data set that specifies the database tables that data can be selected from and how database tables are joined in a report or segment.
target
A specific group of customers sharing common characteristics to whom a promotion is presented. A customer may belong to more than one target.

target rule
A type of business rule that has the sole purpose of creating a target consisting of contacts who meet the conditions established by the rule.

task
An action or activity scheduled to be completed within a specified time. Tasks can be standalone, or they can be associated with answers, campaigns, contacts, documents, incidents, mailings, opportunities, organizations, surveys, and stages in a sales strategy.

task custom field
A field for gathering and displaying additional information about tasks. Task custom fields appear when adding or editing a task.

task inheritance
A feature for linking a task’s assigned staff member, contact, or organization to the equivalent value in a record associated with the task.

task status
A method of tracking a task’s state. The default task statuses are Not Started, In Progress, Completed, Waiting, and Deferred.

Techmail
A scheduled utility that retrieves mail from specified POP3 mailboxes. Service processes some of the mail into new incidents and routes the incidents using business rules (depending on settings). Outreach and Feedback process bounced messages to assist in tracking incorrect email addresses.
template
A structured format used in a document in which specified sections are locked and cannot be edited and a section is open for customized content. The customer portal also uses templates to apply a uniform style to individual pages of the support site. Templates are also available as a starting point for creating a workflow’s flow diagram, and templates can be added for community groups and hives.

territory
A specific geographical sales region configured in Opportunity Tracking. Sales representatives can be assigned specific territories for opportunity assignment. Up to twelve levels of territories can be defined.

test message
A mailing message that can be sent to small cross-sections of an audience to test a response before launching a final message.

text explanation
A text field that can be associated with a response in a guided assistance guide. The text explanation is displayed after an agent selects the associated response from a question in the guide. See Guided assistance.

text field
A customizable field containing text that is commonly added to reports. Once a text field is created, it can be added to any custom report and then adjusted as necessary.

text matching
A feature in Offer Advisor that enables agents to search for specific terms that best express the customer’s interests. After a search, the list of promotions and suggestions on the Offer Advisor window will be reordered, and the ranking of each will reflect its relevance to the terms entered by the agent. See Offer Advisor.

text question
A question type that allows customers to type their answer to a question.
**theme**

A group of related text responses to a survey question. Themes are created by topic monitoring and identified by common keywords. Themes are also used in social monitoring to group related cloud search results and in the customer portal to apply CSS styling to multiple elements of a support site by applying a single theme. See Oracle RightNow Customer Portal Cloud Service, Oracle RightNow Social Monitor Cloud Service, and Topic monitoring.

**third-party screen pop**

A feature that lets staff members open a Service Console or report from a third-party application. See Service Console.

**Time Billed**

A way to track the time spent responding to incidents. Data from the Time Billed field can be used for customer billing and for determining average incident resolution time.

**Tool window**

A default interface control on the Service Console for accessing reports, records, and items, and for searching the knowledge base. Recent Items and Navigation tool windows appear on the left navigation pane, and the Quick Search tool window appears on the right navigation pane. Tool windows can be put in any order, displayed in separate, floating windows, or removed from the console.

**toolbar**

One or more icons used as commands on a workspace. The initial set of icons on the workspace’s toolbar is specified in the record type’s workspace configuration, but administrators can customize the toolbar to add frequently used icons.

**topic browsing**

A feature that provides clustering and guided browse functionality on the customer portal so customers can browse specific topics to find related answers.
topic monitoring

A process that groups survey text responses into clusters of related responses called themes and labels each theme with keywords that define the responses. Topic monitoring is also used in social monitoring to group related cloud search results. See also data mining and themes.

tracked link

A link that can be tracked by Outreach and reported on for statistical purposes.

tracked link category

An option for classifying tracked links for reporting purposes. A tracked link category can have one subcategory level.

transactional mailing

A mailing that is sent only when an event occurs. Transactional mailings are sent to a contact when the contact meets specified criteria in a campaign and can be scheduled to be sent immediately, on a specific date, or at an interval in the future.

transactional survey

A survey that is sent only when an event occurs. Transactional surveys are sent to a contact when the contact meets specified criteria in a campaign or business rule and can be scheduled to be sent immediately, on a specific date, or at an interval in the future.

transfer

A feature in Chat that enables an agent to transfer a customer to another agent during a chat session.

trending

A method of predicting a trend for a specified date range in the future based on a report’s current data. Trending periods are defined when creating or editing a custom report and can be included in standard reports.
trigger

The part of a script or workspace rule that defines the event that causes the rule conditions to be evaluated and (if matched) the rule action to occur.

Unqualified

One of the default chat agent statuses. This status indicates that the agent is not available to chat. The Unqualified chat agent status has an Unavailable status type.

Unresolved

One of the default incident status types and statuses. Incidents with an Unresolved status have recently entered the system, either by a customer or by an agent.

Unrestricted

One of the default chat agent statuses. This status indicates that there are no restrictions to the agent’s availability to chat. The Unrestricted chat agent status has an Available status type.

Unspecified

One of the default chat agent statuses. This status indicates that the agent is logged out of Chat. The Unspecified chat agent status has a Logged Out status type and is displayed to agents by default.

Unsubscribe link

A link in a mailing that contacts can click to opt out of future mailings or surveys.

Updated

One of the default incident statuses. An incident marked Updated has been updated by a customer from Your Account. Updated incidents have an Unresolved status type.
Upgrade site

A site created during the update process. It has the latest version of the software, and data from your current production site. You can use it to test, configure, and prepare your site for the update.

upgrading

The process of moving from one release of Oracle Service Cloud to a newer release. See also migration.

Update Management System (UMS)

A dynamic checklist tool that guides you through a series of tasks that test the core functionality of your updated site.

URL answer

A type of answer that consists of a link to an external URL. The URL address and the content of the web page are displayed.

user agent settings

The shortcut on the customer portal administration dashboard that allows page set mapping. See also page set mapping.

User link

A navigation element on community pages containing links to the logged-in user’s profile, inbox, favorites, and subscriptions, and a sign-out option.

user type

The community role of a member account as defined by the nature of actions that the member is permitted to take.

utility

Any of a number of programs in Oracle Service Cloud to help manage and configure an installation. Utilities include Agedatabase, Bulkdel, Dbaudit, Dbstatus, Kexport, Kimport, Langcvt, Msgtool, Reportgen, Techmail, and Wltool.
validation

The process of error-checking items such as desktop workflows, scripts, rules, advanced surveys, and campaigns. Items are validated to ensure that all required properties have been completed and that the configuration is functional. Oracle Service Cloud also validates email addresses for industry-accepted formatting.

variable

A temporary data item in a rule base. The variable is assigned an initial value that can be modified through rule actions, used as a rule condition to trigger other actions, and restored to its initial value for the next round of rules processing. Variables also refer to shortcuts defined for a larger string that can be inserted in the body of an answer or inserted inline during a chat session. When the variable is inserted in the body of the answer or in a chat response, it is replaced with the value specified in the variable.

versioning

The system of numbering the Customer Portal framework and widgets to denote varying levels of changes. Major and minor changes are not backward compatible, while nano changes are applied automatically to all Customer Portal installations.

view partial

A reusable segment of code for common functionality that can be called from widget views to avoid duplicating the same code in multiple widget view files.

virtual assistant

A process of routing incoming chats to a simulated agent that uses knowledge base data to respond to customer questions. Virtual assistant chats can ease the volume of chats requiring an agent. See Oracle RightNow Virtual Assistant Cloud Service.

visibility

A setting that determines where a custom field or customizable menu item will appear. Visibility settings specify the interfaces in a multiple-interface installation where these fields appear. The settings can also define whether the fields appear on the administration interface and customer portal and whether certain custom fields with customer visibility can be edited.
visit

See Web visit.

Waiting

One of the default incident status types and incident statuses. An incident marked Waiting has been responded to by a staff member and is waiting for a response from the incident creator.

web form

A document in Outreach that allows contacts to input information that can be submitted to the database. Web forms are served as web pages by Oracle Service Cloud.

Web Indexer

A search method that lets customers simultaneously search the knowledge base along with web pages and other web-accessible documents within a specified domain.

Web spider

A software application that reads web pages and other documents and indexes the content for a search engine, often following hyperlinks from one web page to another.

web visit

The period of time a customer spends looking for a satisfactory answer to a question. The end of a web visit generally occurs when a customer closes the browser or leaves the interface or when a specified time period elapses.

web visit tracking

A feature that tracks information about a customer’s current web visit. That is, it tracks the pages on the customer portal that the customer clicked before submitting a question.
website link survey

A type of survey that is published as a web page and can be linked to from any source.

weight

A displayed value given to resulting answers of a text search. The value is equal to the sum of the weights (for indexed words) of all the matched words from the text search. Weight also refers to an internal value given to each indexed keyword for an answer or incident. The value is relative to a constant and is based on number of occurrences, capitalization, and location of the word (ranked high to low: Keywords, Summary, Question, and Answer field for answers; Subject field and incident thread for incidents).

widget

A collection of files that generates a specific function when it is placed on a page of the customer portal. Widgets can be buttons, fields, reports, or other elements that can access the Oracle Service Cloud database and communicate with other widgets through events or to the server through AJAX requests.

widget builder

A tool that generates custom widget code, including placeholders to allow additional editing of the code. The widget builder, accessed on the Customer Portal Administration site, can extend an existing widget or create a new one.

Win/loss reason

An option for classifying and recording reasons for winning or losing an opportunity.

Wltool

A utility that is manually run after making changes to one of the wordlist files. See Wordlist file.

word stemming

A feature used in keyword indexing and text searching that finds the root of each word and stores the stemmed root instead of the whole word, thereby saving large amounts of space while making a search broader and more appropriate.
wordlist file

Any of the files that can be modified to customize indexing, text searching, and SmartSense emotive ratings. See File Manager.

workflow

See Desktop workflow.

workgroup

All of a record’s open, associated records (for instance, an incident’s contact, organization, and tasks) that are docked to the Service Console. All records in a workgroup are saved and closed in a single operation. When another non-associated record is opened, the records in the workgroup are collapsed on a single content pane tab.

working record

The record being evaluated or acted upon by a workflow element or connector. For instance, a workspace element can display the first or last record opened in the workflow or a record named elsewhere in the workflow. See Desktop workflow.

workspace

The configuration of the content pane when working with answers, contacts, incidents, opportunities, organizations, and tasks; when working in Chat; and when working with quotes, quote products, and service opportunities. Standard workspaces exist for each type of workspace, and custom workspaces can be created. The workspaces staff members use depend on the workspaces selected in their profile.

workspace rules

A type of rule used to dynamically adjust the display, behavior, and values of fields and controls on a workspace based on staff member actions. Each rule is triggered by one or more events and conditions.

Workspace designer

The tool used to create and edit custom workspaces.
**WYSIWYG (what you see is what you get)**

See HTML editor.

**Your Account**

A tab on the customer portal that opens the Account Overview page where customers can view and update all the questions they have previously submitted and view any answer or product/category notifications to which they are subscribed. They can also view their service contracts, edit their account information, and change their password. This component is restricted and requires a customer account.