B2C Service

Securing B2C Service

B2C Service
Securing B2C Service

Part Number: F76294-03

Authors: The B2C Service Information Development Team

Oracle customers have access to electronic support through Oracle Support. For information, visit Get Started with Technical Support or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Contents

Preface i

1 Understanding Oracle B2C Service Security 1

Overview of Oracle B2C Service Security and Compliance 1
Network and Hosting Infrastructure 1
How You Develop a Security Plan 1
Administration Interface Configuration 3
How You Use Role Access to Define Permissions 3
Email Security 8
Abuse Detection 9

2 Configuring Security-Related Settings 11

Overview of Security-Related Configuration Settings 11
Security Level 11
Security Significance 15
Site Protection 18
Clickjacking Protection 20
Cross-Site Request Forgery 20
Redirect Security 20
Session-Data Security 21
File-Attachment Security 24
Chat Security 25
Server Protection 29
Chat API Protection 29
External-Queue Security 30
Channel Security 30
Self Service for Facebook Authentication 31
Twitter Security 31
Open Login Credentials for Social Accounts 31

3 Managing Customer and Staff-Member Passwords 33

Password Protection 33

How You Enforce Password Requirements 33
How You Secure Customer Passwords 34
How You Configure Staff-Member Passwords 35
How You Recover Forgotten Passwords 36

4 Deploying B2C Service in a Controlled Environment 37
Overview of Deploying B2C Service in a Controlled Environment 37
Important B2C Service Support Documentation 37
Supplemental Controls and Policies 38
How You Comply with Third-Party Standards 39
How You Use B2C Service Components in Controlled Environments 40

5 Deploying PCI and HIPAA 41
Data Protection 41
How You Secure Access to B2C Service 41
Audit and Read Logs 43
Mobile-Access Security 43
How You Evaluate PCI Vulnerability 44
How You Secure Integrations and Accelerators 44
Incident Thread Masking 45
How You Secure Email, Outreach, and Surveys 45
Analytics Security 46
Chat Security in PCI and HIPAA Deployments 47

Preface

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

Using Oracle Applications

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit Oracle's Accessibility Program at *Oracle Accessibility Program Website*.

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we're working to remove insensitive terms from our products and documentation. We're also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Contacting Oracle

Access to Oracle Support

Customers can access electronic support through Oracle Support. For information, visit *My Oracle Support* or visit *Accessible Oracle Support* if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides. See *Oracle B2C Service - Documentation Feedback*.

1 Understanding Oracle B2C Service Security

Overview of Oracle B2C Service Security and Compliance

An important part of product security is your diligence in configuring B2C Service 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 B2C Service experience secure by holding ourselves to industry-standard security and privacy requirements in our software development practices and operational methods. For added protection, B2C Service can be hosted within our community cloud environments that align with well-known regulatory control frameworks.

For guidance when deploying B2C Service in a regulated environment, refer to *Overview of Deploying B2C Service in a Controlled Environment* and the sections that follow it, in the *Securing B2C Service* guide.

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.

B2C Service 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.

How You Develop a Security Plan

When configuring your B2C Service 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 B2C Service 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 B2C Service 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 B2C Service. 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
- *Security Policy Templates*—for information about security training and security certification
- *OWASP Foundation*—A nonprofit organization focused on improving software security

Administration Interface Configuration

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 a B2C Service site, including your site controls and data.

B2C Service 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 B2C Service. 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 B2C Service. 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 which areas of B2C Service 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 of Navigation Sets
- Create a Navigation Set
- Assign a Navigation Set to a Profile
- Overview of Workspaces
- Custom Workspaces
- How You Customize Profiles

How You Use 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.

Although this table doesn't contain a complete list of all the permissions available, it does provide a list of those permissions having direct security ramifications.

Role-Access Scenario

Setting	Functionality	Roles
Administration		
Administration	Create and edit these items: • Custom Fields • Messages • Mailboxes • Currencies and Exchange Rates • Service Level Agreements • Response Requirements • Chat Hours • Quote Templates • Territories • Promotions • Strategies • Sales Periods • External Suppression List • Thread Type Correction	Administrator
Groups/Accounts/Distribution Lists	Access staff accounts and distribution lists.	Administrator Supervisor
System Error Log	Access log files under Site Configuration.	Administrator Supervisor
Workspace Designer	Access Workspaces and Workflows explorers and designers.	Administrator Supervisor
Scripting	Create and edit agent scripts.	Administrator Developer
Object Designer	Create custom objects.	Administrator Developer
Message Templates	Customize administrator notifications, administrator emails, and contact emails.	Administrator

Setting	Functionality	Roles
Access Control	Access the Access Control editor to configure staff and customer settings permissions for Community Self Service.	Administrator Supervisor
CP Promote	Promote customer portal pages from the staging area to the production area.	Administrator Developer
CP Stage	Copy customer portal development files to the staging area.	Administrator Developer
CP Edit	Access the Customer Portal Administration site and edit customer portal pages in the development area using WebDAV.	Administrator Developer
Rules View	View business rules.	Administrator Supervisor Staff member
Data Import	Import data, including answers, contacts, incidents, organizations, and custom objects.	Administrator Supervisor
Process Designer	Create custom processes.	Administrator Developer Supervisor Staff member
Virtual Assistant Edit	Access to configuration of the virtual assistant.	Administrator
Broadcast Notifications	Send messages to other staff members.	Administrator Supervisor
Configuration	Access to these areas and functionality: • Password Configuration • Configuration Settings • Configuration Wizard • Message Bases • File Manager • Interfaces • Add-In Manager • Email Address Sharing	Administrator
Business Process Settings	Define interface appearance and functionality, including: • Navigation Sets • Customizable Menus	Administrator Supervisor

Setting	Functionality	Roles
	• Countries • Products/Categories/Dispositions • Standard Text • Variables • Holidays • Product Catalog • Price Schedules • Tracked Link Categories	
Rules Edit	Edit business rules.	Administrator Supervisor
Profiles	Add and edit profiles.	Administrator
SSO Login (SAML 2.0)	Allows login only through an identity provider, that is, using a single sign-on process. B2C Service uses the SAML 2.0 protocol for single sign-on.	Administrator
Skill Edit	Access to configuration of advanced routing.	Administrator Supervisor
Agent Browser User Interface	Access to the B2C Service using the Agent Browser UI through account authentication.	Administrator Supervisor Staff member
Public SOAP API	Access the public SOAP API through account or session authentication.	Administrator Developer
Public Knowledge Foundation API	Access the public Knowledge Foundation API through account or session authentication.	Administrator Developer Supervisor Staff member
Organizations		
	Add, edit, delete, and view organizations.	Administrator
	Edit and view organizations.	Supervisor
	View organizations.	Staff member
Contacts		
	Add, edit, delete, view, and move contacts.	Administrator
	Add, email, edit, delete, and view contacts.	Supervisor
	Email, edit, and view contacts.	Staff member

Setting	Functionality	Roles
Service		
Incidents	Add, edit, view, and delete incidents; propose incidents as answers; respond to incidents.	Administrator Supervisor
	Add, edit, and respond to incidents.	Staff member
Answers	Add, edit, and delete answers; set answers to public status.	Administrator Supervisor
	Add and edit answers.	Staff member
Asset	Add, edit, delete, and view assets.	Administrator Supervisor
	View and edit assets.	Staff member
Opportunities		
	Create, edit, delete, view, respond to leads, and send quotes.	Administrator
	Create, edit, and view leads, and send quotes.	Supervisor
	View leads and send quotes.	Staff member
Outreach		
	Create, edit, delete, and view mailings, campaigns, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Administrator
	Edit and view mailings, campaigns, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Supervisor
	View mailings, campaigns, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Staff member
Feedback		
	Create, edit, delete, and view surveys, questions, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Administrator
	Edit and view surveys, questions, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Supervisor
	View surveys, questions, documents, templates, snippets, file attachments, tracked links, segments, and contact lists.	Staff member
Tasks		

Setting	Functionality	Roles
	Create, edit, delete, and view tasks.	Administrator
	Edit, view, and delete tasks.	Supervisor
	View tasks.	Staff member
Analytics		
	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.

B2C Service 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.

Authentication

Authentication assures the message recipient that the sender is who it appears to be and that no other parties are misrepresenting themselves as the sender.

> **Note:** If you use a general Service mailbox supplied by Microsoft, such as Outlook or Office 365, you need to configure your mailbox settings in B2C Service to use OAuth authentication. This is in keeping with Microsoft's end of service support for Exchange mailboxes. When you implement this email authentication correctly, you can continue to send emails to contact centers using Microsoft mailboxes without any mail delivery problems. For more information, see *Configure OAuth Authentication Settings*.

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 list of 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 *How to Control 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 SEC_EU_EMAIL_LINK_EXPIRE configuration setting. 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 *How You Secure 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.

Image Links in Incoming HTML Email

When HTML is rendered from a customer email, the EGW_VISUAL_EMAIL configuration setting defines how inline images are retrieved and rendered. These HTML image links could be used for unauthorized data transfer and tracking purposes. For example, when an incident is opened, a web page revealing an agent's location (IP address) or browser type might be automatically accessed.

You can disable image links in incoming HTML email by setting the EGW_VISUAL_EMAIL configuration setting to No. Keep in mind that this setting not only disables image links when creating the incident thread, but also renders the email as plain text, without any formatting. There are also cases where EGW_VISUAL_EMAIL does not affect HTML threads with images, for example, when some kind of integration has taken place. It is also important to note that even after the setting is disabled, existing incidents might still be vulnerable.

Abuse Detection

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, B2C Service 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 CAPTCHA Validation on Submit
- Open CAPTCHA Within a Form
- Set the Abuse Detection Cookie

2 Configuring Security-Related Settings

Overview of Security-Related Configuration Settings

Certain configuration settings have a direct effect on security. Some affect the administration side of B2C Service 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

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.

Recommended Security-Related Settings

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
Hidden			
CHAT_WS_API_IP_HOST	Set to allowed IP addresses and subnet masks. **Note:** To enable this hidden setting and define your allowed IP addresses and subnet masks, *Submit a Service Request*.		

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
Chat/General/Server			
CHAT_CORS_ALLOWLIST	Set to allowed origins.	Set to allowed origins.	Blank (default)
RightNow User Interface/General/Security			
CLIENT_SESSION_EXP This setting is also used in the desktop usage administration feature.	15 (default)	16 to 45	0
RightNow User Interface/Customer Portal/Login			
CP_CONTACT_LOGIN_REQUIRED	Yes	Yes	No (default)
CP_COOKIES_ENABLED	Yes (default) for all security environments.		
CP_FORCE_PASSWORDS_OVER_ HTTPS	Yes (default)	Yes	Yes
CP_LOGIN_COOKIE_EXP	5 to 30	31 to 60 (default = 60)	-1
RightNow User Interface/General/Security			
CP_LOGIN_MAX_TIME	As needed for all security environments (default = 0).		
RightNow User Interface/Customer Portal/Login			
CP_MAX_LOGINS If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.	As needed for all security environments (default = 0).		
CP_MAX_LOGINS_PER_CONTACT If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.	0 (default)	0	0
Common/General/Security			
CP_REDIRECT_HOSTS	As needed for all security environments (default = blank).		
RightNow User Interface/General/End-User			
EU_CUST_PASSWD_ENABLED	Yes (default)	Yes (default)	No
RightNow Common/Service Modules/Oracle Email			

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
EGW_PASSWD_CREATE	Yes (default)	Yes (default)	No
EGW_SECURE_UPDATE_MODE	2 (default)	2 (default)	1
EGW_VISUAL_EMAIL	No (default = Yes)	No (default = Yes)	Yes
RightNow Common/3rd-Party Applications/Facebook			
FACEBOOK_INCIDENTS_ENABLED	No (default = Yes)	As needed.	As needed.
RightNow User Interface/Open Login/Oauth Apps			
FACEBOOK_OAUTH_APP_ID	Facebook application ID for all security environments (if Facebook is enabled).		
FACEBOOK_OAUTH _APP_SECRET	Facebook secret key for all security environments (if Facebook is enabled).		
RightNow User Interface/General/File Attach			
FATTACH_MAX_SIZE **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.	As small as practical for your needs. Applies to all security environments (default and maximum allowable limit = 20 MB). **Note:** File upload fails if the upload takes more than 5 minutes.		
FATTACH_OPEN_ENABLED	No (default)	No	As needed.
Chat/General/Create Incident			
INC_PRIVATE_TRANSCRIPT_ONLY	Yes	Yes	No (default)
LOGIN_SECURITY_MSG	As needed for all security environments (default = blank).		
RightNow User Interface/Contact Services/Security			
MYSEC_AUTO_CUST_CREATE	No (default = Yes)	No	As needed.
Common/General/Security			
SEC_BROWSER_USER_AGENT	Set to allowed user agent strings.	Blank (default)	Blank (default)
SEC_EU_EMAIL_LINK_EXPIRE	8 (default)	12	24

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
SEC_INVALID_ENDUSER_HOSTS	Set to allowed IP addresses.	Blank (default)	Blank (default)
SEC_INVALID_USER_AGENT	Set to user agent strings that are not allowed.	Blank (default)	Blank (default)
SEC_SPIDER_USER_AGENT	Set to list of known web spider user agent strings.	Blank (default)	Blank (default)
SEC_VALID_ADMIN_HOSTS	Set to allowed IP addresses.	Set to allowed IP addresses.	Blank (default)
SEC_VALID_CHAT_API_HOSTS	Set to allowed hosts and subnet masks for all security environments (default = blank).		
SEC_VALID_ENDUSER_HOSTS	Set to allowed IP addresses.	Set to allowed IP addresses.	Blank (default)
SEC_VALID_INTEG_HOSTS	Set to allowed IP addresses.	Blank (default)	Blank (default)
SESSION_HARD_TIMEOUT	12 (default)	12-24	As needed.
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/			
TWITTER_OAUTH_APP_ID	Twitter application ID for all security environments (if Twitter is enabled).		
TWITTER_OAUTH_APP_SECRET	Twitter secret key for all security environments (if Twitter is enabled).		
Outreach and Feedback/General/Campaigns			
WEBFORM_ID_BY_COOKIE_ DEFAULT	As needed for all security environments (default = No).		
WEBFORM_ID_BY_LOGIN_ DEFAULT	As needed for all security environments (default = No).		
WEBFORM_ID_BY_LOGIN_ REQUIRED_DEFAULT	As needed for all security environments (default = No).		

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
WEBFORM_ID_BY_URL_PARAM_ DEFAULT	As needed.	As needed.	No (default)
WEBFORM_SET_COOKIE_DEFAULT	As needed.	As needed.	No (default)
RightNow User Interface/Customer Portal/Syndicated Widgets			
WIDGET_INSTALLATION_HOSTS	As needed.	As needed.	Blank (default)

Related Topics

- Email Security
- Search for a Configuration Setting
- Edit a Configuration Setting

Security Significance

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

Recommended Security-Related Settings By Significance

Significance	Configuration Setting	Recommended Setting
High	CHAT_WS_API_IP_HOST	Set to allowed IP addresses and subnet masks. **Note:** To enable this hidden setting and define your allowed IP addresses and subnet masks, *Submit a Service Request*.
	CLIENT_SESSION_EXP	15 This setting is also used in the desktop usage administration feature.
	CP_FORCE_PASSWORDS_OVER_ HTTPS	Yes
	CP_LOGIN_COOKIE_EXP	As needed.
	CP_REDIRECT_HOSTS	Set to allowed hosts or leave default setting (blank) to prevent all redirects outside of the interface domain, including external sites.

Significance	Configuration Setting	Recommended Setting
	EU_CUST_PASSWD_ENABLED	Yes
	SEC_VALID_ADMIN_HOSTS	Set to allowed IP addresses.
	SEC_VALID_CHAT_API_HOSTS	Set to allowed hosts and subnet masks.
	SESSION_HARD_TIMEOUT	12
Medium	CHAT_CORS_ALLOWLIST	Set to allowed origins.
	CP_CONTACT_LOGIN_REQUIRED	As needed.
	CP_LOGIN_MAX_TIME	As needed.
	EGW_PASSWD_CREATE	Yes
	EGW_SECURE_UPDATE_MODE	2
	EGW_VISUAL_EMAIL	No (default = Yes)
	FACEBOOK_INCIDENTS_ENABLED	Yes
	FATTACH_OPEN_ENABLED	Yes
	INC_PRIVATE_TRANSCRIPT_ONLY	Yes
	SEC_EU_EMAIL_LINK_EXPIRE	8
	SUBMIT_TOKEN_EXP	30
	WEBFORM_ID_BY_COOKIE_ DEFAULT	As needed.
	WEBFORM_ID_BY_LOGIN_ DEFAULT	As needed.
	WEBFORM_ID_BY_LOGIN_ REQUIRED_ DEFAULT	As needed.
	WEBFORM_ID_BY_URL_PARAM_ DEFAULT	As needed.
	WEBFORM_SET_COOKIE_DEFAULT	As needed.
	WIDGET_INSTALLATION_HOSTS	Set to allowed domain names.

Significance	Configuration Setting	Recommended Setting
Low	CP_COOKIES_ENABLED	As needed.
	CP_MAX_LOGINS	As needed.
	CP_MAX_LOGINS_PER_CONTACT	As needed. **Note:** If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.
	FACEBOOK_OAUTH_APP_ID	As needed.
	FACEBOOK_OAUTH _APP_SECRET	As needed.
	FATTACH_MAX_SIZE	As small as practical for your needs. **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.

Administration Interface Settings for Site Protection

Configuration Setting	Description	Default Value
Common/General/Security		
SEC_VALID_ADMIN_HOSTS	Defines which hosts can access the administration interface.	Blank
SEC_VALID_INTEG_HOSTS	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.	Blank
RightNow User Interface/General/Security		
CLIENT_SESSION_EXP	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. **Note:** This setting is not used strictly for security. It is also used in the desktop usage administration feature.	15
RightNow User Interface/Tool Bar/General		
LOGIN_SECURITY_MSG	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 or the Agent Browser UI opens.	Blank

Customer Portal Settings for Site Protection

Configuration Setting	Description	Default Value
Common/General/Security		
CP_REDIRECT_HOSTS	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. • Blank = Prevents all redirects outside of your interface domain. • * = Allows all redirects, including redirects to external sites. (Not recommended.) **Note:** Redirects within your interface domain, as well as hosts specified in related configuration settings are implicitly allowed. Therefore, those domains do not need to be listed in the CP_REDIRECT_HOSTS setting.	Blank
SEC_VALID_ENDUSER_ HOSTS	**Note:** This setting applies only to PHP pages. It does not block access to static assets such as URLs, images, JavaScript, folders, or files. For more information, contact your Oracle account manager. Defines which hosts can access the customer portal. Only customers coming from a host in the valid list are allowed access to the customer portal. **Tip:** The valid list is practical only if the set of allowed hosts is confined to 10 or fewer domains.	Blank
SEC_INVALID_ENDUSER_ HOSTS	Defines which hosts are not allowed access to the customer portal. The invalid list is used to prevent spiders from known locations.	Blank
RightNow User Interface/General/Security		
SUBMIT_TOKEN_EXP	Defines the amount of time, in minutes, that the submit token used for token verification is valid.	30

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 ClickjackPrevention 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 Foundation* website.

Related Topics

- iFrame Security Issues

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 Foundation* website.

Redirect Security

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 the CP_REDIRECT_HOSTS configuration setting 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.

Sample Values for CP_REDIRECT_HOSTS

Value	Meaning
Blank	Prevents all redirects outside of your interface. (Default)
*	Allows all redirects. (Not recommended.)
*.example.com	Allows redirects to all sites in the example.com domain.
one.example.com, two.example.com	Allows redirects to sites one and two in the example.com domain.
example.custhelp.com, *.test.com	Allows redirects to example.custhelp.com and any interface in the test.com domain.

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

Session-Data Security

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 *How You Force 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 setting also prevents unauthenticated chat sessions.

B2C Service 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.

Administration Interface Settings for Session Data

Configuration Setting	Description	Default Value
RightNow User Interface/General/Security		
CLIENT_SESSION_EXP	Requires staff members to reauthenticate after a specified period of inactivity on the Service Console. **Note:** This setting is not used strictly for security. It is also used in the desktop usage administration feature. See *Desktop Usage Control*.	15 minutes
SESSION_HARD_TIMEOUT	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.	12 hours

Customer Portal Settings for Session Data

Configuration Setting	Description	Default Value
RightNow User Interface/General/Security		
CP_LOGIN_MAX_TIME	Defines the time (in minutes) a customer can be logged in without needing to log in again. If a session goes past the defined	0

Configuration Setting	Description	Default Value
	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.	
RightNow User Interface/Customer Portal/Login		
CP_CONTACT_LOGIN_ REQUIRED	Defines if the customer portal requires a customer to be logged in when accessing most pages or controls. Also prevents unauthenticated chat sessions. **Note:** This setting does not apply to the login, password recovery, and account creation pages, or pass-through authentication (PTA). PTA is described in *Configuring Pass-Through Authentication*.	No
CP_COOKIES_ENABLED	Defines if the customer portal tries to set cookies on a visitor's browser.	Yes
CP_FORCE_PASSWORDS_ OVER_ HTTPS	Requires all login operations to be performed over HTTPS. Pages that use passwords within standard widgets are automatically redirected to HTTPS.	Yes
CP_LOGIN_COOKIE_EXP	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.	60
CP_MAX_LOGINS	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.	0
CP_MAX_LOGINS_PER_ CONTACT	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.	0

File-Attachment Security

Attachments that B2C Service 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.

Here are some guidelines to consider when working with attachments.

- 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.
- HTML files might 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.
- 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 B2C Service. 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 B2C Service application as well as the associated data, and it also allows additional levels of scanning to be applied. The FATTACH_OPEN_ENABLED configuration setting 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 FATTACH_MAX_SIZE configuration setting 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.

Settings for File Attachments

Configuration Setting	Description	Default Value
RightNow User Interface/General/File Attach		
FATTACH_MAX_SIZE	Defines the maximum file size in bytes that can be uploaded to the server as	20971520 (20 MB)

Configuration Setting	Description	Default Value
	an attachment. File upload will fail if the upload takes more than five minutes. **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.	The maximum allowable limit is 120 MB.
FATTACH_OPEN_ENABLED	Lets staff members open file attachments on the agent desktop.	No

Chat Security

B2C Chat (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.

Settings for Chat

Configuration Setting	Description	Default Value
CHAT_WS_API_IP_HOST	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 request on our *support site*.	Blank
Common/General/Security		
SEC_VALID_CHAT_API_HOSTS	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. **Note:** If this setting is left blank, the server accepts requests from all hosts.	Blank

Configuration Setting	Description	Default Value
CP_CONTACT_LOGIN_REQUIRED	When enabled, enforces secure logon to prevent unauthorized chat sessions.	No
Chat/General/Server		
CHAT_CORS_ALLOWLIST	Defines the list of origins and domains allowed to make cross-origin requests through the Chat server. If chat sessions in the Service Console include content such as images or URLs, that are not included on this allow list, a warning message prompts the agent to continue or cancel the action. **Note:** If this setting is left blank, the server accepts requests from all origins. Changes made to this allow list only apply to new, and not existing, chat sessions on the Service Console.	Blank
Chat/General/Create Incident		
INC_PRIVATE_TRANSCRIPT_ ONLY	Allows chat transcripts to be added to incidents as private notes. **Note:** If enabled, customers cannot see past chats.	No

The CHAT_INPUT_ALLOWLIST_JSON configuration setting describes a valid set of tags, attributes, and protocols to allow in message posts and in common fields used in chat sessions.

The configuration setting, which you can find in **Chat/General/Chat Session**, has an extensive list of default values.

Default Values for the CHAT_INPUT_ALLOWLIST_JSON Configuration Setting

Allowed Tags	Allowed Attributes (Allowed Protocols, if applicable)
a	• href (http, https) • referrerpolicy • title
audio	• controls • loop • muted • src (http, https)
b	
blockquote	cite (http, https)
br	

Allowed Tags	Allowed Attributes (Allowed Protocols, if applicable)
caption	
cite	cite (http, https)
code	
col	• span • width
colgroup	• span • width
dd	
div	
dl	
dt	
em	
figcaption	
figure	
h1	
h2	
h3	
h4	
h5	
i	
img	• align • alt • height • referrerpolicy • src (http, https) • title • width
li	
ol	• start • type
p	
pre	

Allowed Tags	Allowed Attributes (Allowed Protocols, if applicable)
q	cite (http, https)
small	
source	• src (http, https) • type
span	
strike	
strong	
sub	
sup	
table	• summary • width
tbody	
td	• abbr • axis • colspan • rowspan • width
tfoot	
th	• abbr • axis • colspan • rowspan • scope • width
thead	
tr	
u	type
ul	
video	• controls • height • loop • muted • poster (http, https)

Allowed Tags	Allowed Attributes (Allowed Protocols, if applicable)
	• preload • src (http, https) • width
:all (indicates allowed attributes on all tags)	• dir • id • lang • muted • style • title • translate

For example:

- {"h1": {}} indicates that the <h1> tag is allowed, but that no attributes are allowed.
- {"a": {"href": ["ftp","http","https","mailto"]}} indicates that the <a> tag is allowed.

Server Protection

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

The SEC_VALID_CHAT_API_HOSTS configuration setting 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 the CHAT_CORS_ALLOWLIST configuration setting. See “Cross-Origin Resource Sharing Protection” in *Chat API Protection*.

Chat API Protection

B2C Service 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 CHAT_WS_API_IP_HOST configuration setting. To enable this setting and specify the IP addresses and subnet masks you want to allow, *Submit a Service Request*.

User Protection

By enabling the INC_PRIVATE_TRANSCRIPT_ONLY configuration setting, 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.

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_ALLOWLIST 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*.

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

External-Queue Security

External chat queues allow sites outside of B2C Service that use the Chat API to access B2C Service 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*.

Channel Security

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

For this reason, B2C Service 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 B2C Service instead.

B2C Service can store your customers’ social media user names in their contact records. By tracking this identifying information, B2C Service can associate incoming 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 socialidentities of your customers across different services.

You may also want to consider SSL (secure sockets layer) encryption options for social media services. Then traffic between B2C Service and the social media site is encrypted. See *Email Security*.

Related Topics

- Overview of Channels

Self Service for Facebook Authentication

B2C Service Self Service (Self Service) lets you embed a set of 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 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 B2C Service. 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. The FACEBOOK_INCIDENTS_ENABLED configuration setting is enabled by default 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*.

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.

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

B2C Service 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 *How Customers Log 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 B2C Service.

- FACEBOOK_OAUTH_APP_ID and FACEBOOK_OAUTH_APP_SECRET
- TWITTER_OAUTH_APP_ID and TWITTER_OAUTH_APP_SECRET

Configuration Settings for Social Experience

Configuration Setting	Description	Default Value
RightNow Common/3rd-Party Applications/Facebook		
FACEBOOK_APPLICATION_ ID	Specifies the Facebook application ID used to host Facebook for B2C Service.	Blank
FACEBOOK_APPLICATION_ SECRET	Specifies the Facebook application secret key used to host Facebook for B2C Service. This setting is also used to authenticate staff members and customers who use B2C Service Self Service for Facebook.	Blank
FACEBOOK_INCIDENTS_ ENABLED	Lets customers and staff members create private incidents from your Facebook page.	Yes
RightNow User Interface/Open Login/OAuth Apps		
FACEBOOK_OAUTH_APP_ID	Specifies the Facebook application ID used to request the customer's or staff member's credentials for open login with Self Service for Facebook.	Blank
FACEBOOK_OAUTH_APP_ SECRET	Specifies the Facebook secret key used to request the user's credentials for open login with Self Service for Facebook.	Blank
TWITTER_OAUTH_APP_ID	Specifies the Twitter application ID used to request the customer's or staff member's credentials for open login with the B2C Service channel, Twitter.	Blank
TWITTER_OAUTH_APP_ SECRET	Specifies the Twitter secret key used to request the customer's or staff member's credentials for open login with the B2C Service channel, Twitter.	Blank

3 Managing Customer and Staff-Member Passwords

Password Protection

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 B2C Service 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.

How You Enforce 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 B2C Service default is five.)
- 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.
  - 2BeOrNot2Bee?
  - MaryhadaL1ttlelam
  - JollyBARN+be4Cow
- Stress the importance of keeping passwords secure by memorizing them and keeping them secret.

How You Secure Customer Passwords

Configuration settings and password requirements enable you to secure customer passwords in B2C Service.

Configuration Settings

The EU_CUST_PASSWD_ENABLED configuration setting 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.

Customer Portal Settings for Passwords

Configuration Setting	Description	Default Value
Common/General/Security		
SEC_EU_EMAIL_LINK_ EXPIRE	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*.	8
RightNow User Interface/General/End-User		
EU_CUST_PASSWD_ ENABLED	Displays the password field on the customer portal page.	Yes

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 *How You Configure 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.

How You Configure 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**).

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.

Password Security Benefits

Password Configuration	Security Benefit
Number of Invalid Logins	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 B2C Service, the default is five invalid login attempts before the account is locked.
Expiration Interval	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.) **Note:** PCI-compliance requires expiration interval to be 90 days or less.
Password Length	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.
Numbers and Special Characters	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.)
Uppercase and Lowercase Characters	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.)

Password Configuration	Security Benefit
Number of Previous Passwords	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 passwords allowed makes password expiration less effective. (Default = 10.)

How You Recover 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 B2C Service 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 *Redirection to the B2C Service Login Page*.

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

Account Self-Service Settings for Passwords

Configuration Setting	Description	Default Value
RightNow User Interface/Tool Bar/General		
ACCT_RECOVER_STATUS	Specifies the functionality of the Login Help link on the B2C Service Login window. See *Login Help Options*. • 0 = Opens the login procedure in online help. • 1 = Sends an email containing user name or a link to the Password Reset page for entering a new password (default). • 2 = Changes the email message staff members receive when they click Login Help. The alternate message is defined in ACCT_RECOVER_ALT.	1
ACCT_RECOVER_ALT	Specifies the alternate email message to send when the configuration setting ACCT_RECOVER_STATUS is set to 2.	Blank

Customers can also recover user names and passwords from the login window on the customer portal. 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 the SEC_EU_EMAIL_LINK_EXPIRE configuration setting. See *How You Secure Customer Passwords* and *Email Security*.

4 Deploying B2C Service in a Controlled Environment

Overview of Deploying B2C Service in a Controlled Environment

For added protection, B2C Service 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 B2C Service in a manner that suits several regulations. It is meant for anyone involved in building a solution that implements any of these regulatory environments:

- B2C Service 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 Government Cloud Platform. We include reference to FedRAMP inthis document because it is also a PCI attested environment, so the controls described here apply and may offer assistance.

Important B2C Service Support Documentation

You should be thoroughly familiar with how B2C Service is deployed, hosted, and implemented before planning a deployment in a regulation-controlled environment.

- Review all available deployment, operational, and administrative documentation. Start with *Oracle B2C Service Get Started* on Oracle Help Center.
- While a majority of B2C Service components are managed by Oracle, you are responsible for some local environmental considerations. The *Deploying B2C Service* guide is helpful if you are deploying the .NET Agent Console. In addition, *Answer ID 31* 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 B2C Service 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.
    - *Using the Agent Browser User Interface*
    - *Answer ID 8598*

- *Answer ID 8173*

- Review the *Oracle Cloud Hosting and Delivery Policies*. 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.

Supplemental Controls and Policies

For customers seeking to implement B2C Service 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 B2C Service within the specific cloud environment.

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 B2C Service. 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 B2C Service are through standard application program interfaces (APIs).

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 B2C Service, all reports published to files, and all B2C Service instance databases, including database backups.

Secure Protocols

By default, all connectivity to B2C Service 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.

How You Comply with Third-Party Standards

While we comply with a number of third-party standards, you are ultimately responsible for ensuring that your B2C Service implementation is in compliance.

The following topics offer guidance about configuring a compliant environment:

- *How You Secure Access to Oracle B2C Service*
- *Audit and Read Logs*
- *Mobile-Access Security*
- *How You Evaluate PCI Vulnerability*
- *How You Secure Integrations and Accelerators*
- *Incident Thread Masking*
- *How You Secure Email, Outreach, and Surveys*
- *Analytics Security*
- *Chat Security in PCI and HIPAA Deployments*

Oracle's control status regarding a regulation does not mean that your B2C Service 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, B2C Service 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), B2C Service 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. B2C Service 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 B2C Service 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.

How You Use B2C Service Components in Controlled Environments

While B2C Service 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)
- B2C Chat
- Experience Routing
- Foundation Agent Knowledgebase
- Advanced Agent Knowledgebase
- Intelligent Advisor

5 Deploying PCI and HIPAA

Data Protection

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

B2C Service 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 B2C Service data model to best fit your needs. Whenever you diverge from the default data model, be sure to validate that proper controls are maintained.

One method for customizing the data model is to define encrypted custom attributes in custom objects, incidents, and contacts. Custom attribute encryption masks sensitive information, such as credit card details, to enable you to adhere to the Payment Card Industry (PCI) Data Security Standards. To do this, you create the new custom attribute and encrypt it on the Service Console, see *Add a Field to a Custom Object*. Encrypted fields are available only in the Agent Browser User Interface (Agent Browser UI), and can be decrypted only by agents with the Allow Custom Attribute Decryption permission. See *Overview of Custom Attribute Encryption*.

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.

How You Secure Access to B2C Service

There are multiple methods available to access B2C Service, like the Customer Portal, integration frameworks, and the Service 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 a customer site can help reduce opportunities for unauthorized access. You can define the hosts that can and cannot access a site with the Customer Portal SEC_VALID_ENDUSER_HOSTS, SEC_VALID_ADMIN_HOSTS, and SEC_VALID_INTEG_HOSTS configuration settings. See the B2C Service documentation *Oracle B2C Service Secure* page for more information.

Establishing Credentials

In PCI and HIPAA environments, users must have unique identifiers and complex passwords. While B2C Service 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, B2C Service 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 Staff-Member Passwords*.

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*.

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 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`.

If you choose not to require passwords for end-users, it is still possible to enforce HTTPS with the SEC_END_USER_HTTPS configuration setting. 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 B2C Service Technical Support.

Securing Connectivity

You can access B2C Service from nearly anywhere. Since B2C Service is accessible from the internet, consider the typical precautions when connecting to it. 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.

Audit and Read Logs

Audit and read logs allow customers to see actions taken on their data.

In addition to tracking selected object create, update, and delete transactions, B2C Service 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 through 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 (the READ_LOGGING_ENABLED configuration setting for Incident Threads and/or the CONTACT_READ_LOGGING_ENABLED configuration setting for Contacts), an authorized customer representative must submit a service request on our *support site*. After these settings are enabled, any reads of incidents and/or contacts are logged by B2C Service.

> **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 make them visible:

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.

Mobile-Access Security

Use caution when using B2C Service on a mobile device.

In a previous release of B2C Service, an accelerator was provided with new ways to use B2C Service services through a mobile device. This solution uses the Oracle Mobile Application Framework (MAF), which lets 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 B2C Service, PAN data, and social security numbers displaying on the device will be unreadable.

One exception to this rule is push notifications. Since notifications sent from B2C Service are configured as events and pushed out of B2C Service, sensitive data sent in push notifications do not get masked. You should validate that fields containing PII, PAN, or PHI data are not included in push notifications that might 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 B2C Service Mobile as an intermediary service. You should understand how B2C Service Mobile protects and persists data before you implement it.

How You Evaluate 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 B2C Service PCI Certified Cloud, 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.

How You Secure Integrations and Accelerators

You should closely examine integrations between B2C Service and external applications to prevent mishandling of sensitive data.

The value of B2C Service 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 B2C Service 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 B2C Service 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 B2C Service 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 B2C Service will be shared with Oracle B2B Service, you should contact Oracle and validate that B2B Service 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 B2C Service, consider whether the data is being pulled out or pushed out. This concept is relevant to sensitive data masking. In general, sensitive data in B2C Service 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 B2C Service. Oracle Integration Cloud Service (ICS) is an example where connections enable data to be pushed out of B2C Service.

The B2C Service 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

- Answer ID 5169
- Integration documentation
- Answer ID 5436

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 B2C Service 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, B2C Service 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, B2C Service provides three mask algorithms for credit cards, social security numbers, and phone numbers. You can 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 *Incident Thread Masking*. To enable this feature in a site instance, enable THREADS_AUTO_MASKING_ENABLED, or contact either Technical Support or your account manager for assistance.

How You Secure Email, Outreach, and Surveys

Although B2C Service 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.

B2C Service Outreach enables customers to send emails and campaigns to targeted audiences. The Survey Service provides a method to request information from specific customers through 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 through SSL, customers must use the end-user SSL SEC_END_USER_HTTPS configuration setting. 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 Practices for Sending Email
- Email Security

Analytics Security

Use care regarding permissions and accessibility of reports, including data in a report being exported to another system outside of the B2C Service.

B2C Service has a rich set of analytics features for reporting on data within a customer 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 using 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 instance, the THREADS_NOTE_ANALYTICS_VISIBLE configuration setting is automatically enabled for a HIPAA customer 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 that contain this field. Some standard B2C Service 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 you'll see 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.

Chat Security in PCI and HIPAA Deployments

For customers planning to interact with end-users through B2C Chat, there are several security factors to consider.

When B2C Chat is purchased with B2C Service, it can be covered by the Oracle PCI Certified Cloud 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 B2C Service 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 customer 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 B2C Co-browse offerings that integrate with Chat, or have Oracle Messaging enabled to integrate with Chat, be aware these products have not been audited for use with B2C Service 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. *Using Standalone Cobrowse* describes methods for helping you protect customer data that is not covered in this document.