May 2015

Security Practices

May 18, 2015

Part Number
E56160-05

Contents

1

Overview

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. An important constituent in product security is your diligence in configuring Oracle Service Cloud and your vigilance in its use. This document discusses important security issues and provides specific information about configuration settings that address product security.

Oracle Service Cloud security and compliance

The protection of our customers' assets is a high priority at Oracle. We strive to make your Oracle Service Cloud experience secure by holding ourselves to industry-standard security and privacy requirements in our software development practices and operational methods. For added protection, Oracle Service Cloud can be hosted within our community cloud environments that align with well-known regulatory control frameworks. Depending on the cloud environment you purchased, accreditations, attestations, and certifications may include:

- DIACAP—Department of Defense Information Assurance Certification and Accreditation Process
- DISA ATO—Defense Information Systems Agency–Authority to Operate
- FedRAMP pATO—Federal Risk and Authorization Management Program - Provisional Authority to Operate
- HIPAA—Health Insurance Portability and Accountability Act
- NIST 800-53—National Institute of Standards and Technology
- PCI-DSS—Payment Card Industry Security Standards Council
- SSAE 16 Type II
- SOC2 Type II

Network and hosting infrastructure

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

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

2

Developing a Security Plan

When configuring your Oracle Service Cloud site, your goal is to obtain the maximum effectiveness for your staff and your customers, while ensuring that your site is safe from threats. Although Oracle Service Cloud is designed and implemented with the highest levels of security, we recognize that our customers' needs vary. Therefore, we offer configuration options that let you accept various levels of risk. Your sensitivity to those risks should dictate the configuration and management options you use in your site.

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

Common security threats

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

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

Security considerations

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

The following list is a minimal set of considerations that relate to the use of Oracle Service Cloud.

- 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. The following is a list of suggested reading on security topics.

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

3

Configuring the Administration Interface

Properly configuring the **administration interface** is critical to your site security because staff members can be granted permission to view and modify virtually everything in an Oracle Service Cloud site, including your site controls and data. Oracle Service Cloud uses role-based access control through profile permissions, navigation sets, and workspaces that you define. All staff members are assigned a profile that is associated with a navigation set and one or more workspaces.

- **Navigation sets**—A navigation set is a combination of navigation buttons and their associated navigation lists. Each navigation list contains unique reports and items based on staff member responsibilities, and every profile must include a navigation set that all staff members with that profile use when working in Oracle Service Cloud. By carefully examining staff member responsibilities before you create navigation sets, you can grant access to functionality to only those individuals who require it.
- **Workspaces**—Workspaces define the appearance of the agent desktop when staff members add, view, and edit records in Oracle Service Cloud. Each profile has one or more workspaces that can be designed to provide only the functionality that is needed by the staff member. Along with navigation sets, workspaces provide macro-level control over access rights.
- **Profile permissions**—Profiles let you control what areas of Oracle Service Cloud your staff members can access and what specific actions they can perform in those areas.

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

Using role access to define permissions

Setting permissions carefully and thoughtfully greatly enhances the security of your site. This is particularly true regarding administrator permissions, which typically let staff members edit **configuration settings** and administrative controls.

One method for determining the permissions you grant is to use a role-access method. The following table is not a complete list of all the permissions available, but an abbreviated set representing those permissions with direct security ramifications. 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.

Note Communities in Oracle RightNow Social Experience have their own set of user types that are different from those listed in the scenario described here.

Table 1: Role-Access Scenario

Setting	Functionality	Roles
Administration		
Administration	Create and edit the following 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
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

Table 1: Role-Access Scenario (Continued)

Setting	Functionality	Roles
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 the following areas and functionality: • Password Configuration • Configuration Settings • Configuration Wizard • Message Bases • File Manager • Interfaces • Add-In Manager • Email Address Sharing	Administrator

Table 1: Role-Access Scenario (Continued)

Setting	Functionality	Roles
Business Process Settings	Define interface appearance and functionality, including: • Navigation Sets • Customizable Menus • Countries • Products/Categories/Dispositions • Standard Text • Variables • Holidays • Product Catalog • Price Schedules • Tracked Link Categories	Administrator Supervisor
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. **Note:** Oracle Service Cloud 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 Oracle Service Cloud 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
Mobile Agent App	Access Oracle Service Cloud on a mobile device through account authentication.	Administrator Supervisor Staff member

Table 1: Role-Access Scenario (Continued)

Setting	Functionality	Roles
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
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

Table 1: Role-Access Scenario (Continued)

Setting	Functionality	Roles
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		
	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

Table 1: Role-Access Scenario (Continued)

Setting	Functionality	Roles
	Edit, view, customize, print, export, and forward reports.	Supervisor
	View, edit, print, export, and forward reports.	Staff member

4

Email Security

Most email sent over networks is not encrypted. However, we recommend encrypting all data that you deem sensitive. Oracle Service Cloud is designed to prevent the inadvertent release of information, but there are also a number of configuration settings related to email that you can use to increase your protection.

Certificates

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

For a discussion about the configuration settings you can use to protect your site and improve your security, see Customer Portal Settings for 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. For customers accessing answers from the customer portal, each answer link is protected by a security token with a limited lifetime that is defined in the configuration setting SEC_EU_EMAIL_LINK_EXPIRE. The default value is eight hours, meaning that a customer has eight hours to click the link and read the information published in the answer. We recommend using this security token to limit the time answers are available to customers.

Because attackers need time to build phishing sites (for luring a user into clicking a link), the smaller the window of time you allow for access to your answers, the more secure your site will be.

For example, if an email with an answer link is copied by an attacker, access to the security token and the link has been compromised. If your site requires customers to log in to see an answer, the answer itself is safe, but the attacker can create a phishing scenario using a modified link that takes customers to an external site where their login credentials are stolen. It takes time to accomplish this, so the shorter the window of opportunity, the lower the likelihood of success. Setting the security token expiration in SEC_EU_EMAIL_LINK_EXPIRE helps discourage attackers. See Customer Portal Settings for 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.

5

Abuse Detection Security

A potential threat to any website is a "denial of service" (DoS) attack where the attacker issues a large number of requests for service. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks and credit card payment gateways. These attacks can slow the response time to legitimate visitors, overwhelm the database server, and generate excessive emails that interfere with normal operation.

To prevent these attacks, Oracle Service Cloud provides web form and survey security through CAPTCHA, which automatically requires human validation when abuse is suspected. CAPTCHA validation is typically triggered only if there appears to be active abuse of a website. However, you can customize CAPTCHA requirements from the **customer portal**.

6

Security-Related Configuration Settings

Certain configuration settings have a direct effect on security. Some affect the administration side of Oracle Service Cloud and others affect the customer portal or an external website. By making a conscious decision to determine the appropriate level of security that fits your business, you can define configuration settings to reflect a suitable security level.

This section lists configuration settings that specifically impact security. Paths to each setting in the Configuration Settings editor, descriptions, and default values are also listed. Configuration settings in this section are grouped into the following categories.

- Site protection
- Session data
- Password protection
- File attachments
- Chat
- Social Experience

For a complete list of security-related configuration settings by security level and significance, see Recommendations for Security-Related Configuration Settings.

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.

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.

Table 2: 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. **Tip:** You can use this setting to issue a security statement, distribute terms of a use agreement, or any login message you want staff members to agree to before the Service Console opens.	Blank

Table 3: 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.) **Important:** 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	**Important:** 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

Table 3: Customer Portal Settings for Site Protection (Continued)

Configuration Setting	Description	Default Value
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.

Customer Portal

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

Note If your site must run in frames, you will need to remove the ClickjackPrevention widget from the template.

If you do not use frames, you can edit the *standard.php* file of your template file to minimize the risk of clickjacking.

Community

If Community is enabled on your site, X-Frame-Options can be used to implement restrictions for both public and private pages. These settings restrict the Community pages that can appear in frames.

The X-Frame-Options setting is set, by default, to DENY for both public and private pages. The DENY setting prevents any domain from framing your content. This setting can be accessed on the community's General Settings page.

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

Cross-site request forgery

Cross-site request forgery (CSRF) causes a user's browser to load pages (including forms) that typically require authentication in an attempt to perform actions on behalf of the user. If the user has a valid authenticated session for the site the attacker is causing to load into the browser, those requests will succeed. If proper protections are not in place, this may let the attacker perform unintended actions on behalf of the user.

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

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

Specifying valid redirect domains

Linking from one page to another is also a security risk you should consider. For example, to redirect users to different locations within your site, you may have placed a link in your URL. 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 containing a redirect to a page that exploits users in some way. Those links could be placed in the following locations:

- Questions on your page
- Uploaded files
- Emails

In each of these scenarios, an attacker bets that users will click the link they create and be redirected to an external site where data can be maliciously harvested.

To protect your site from this type of attack, you can set the value of CP_REDIRECT_HOSTS to a list of interface domains that are legitimate redirect targets. The default value is blank, which limits redirects to pages only within your interface domain. Keep in mind that redirects to domains specified in related configuration settings are implicitly allowed.

Table 4: 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 Emailing links to answers.

Session data

To maintain state information about staff members and customers, we use session data that is passed between the staff member's or customer's system and the web server. When an individual is logged in, data from the session can provide the necessary authentication for accessing your data that would not otherwise be available.

Session data security prevents attacks that stem from the trust the system has in authenticated users. Without session data security, attackers may be able to capture session data and reuse it. These are commonly referred to as "replay" attacks or "man-in-the-middle" attacks.

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

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, we recommend requiring that customers log in. The CP_CONTACT_LOGIN_REQUIRED configuration setting enables customer access to your pages and controls on the customer portal. Oracle Service Cloud offers different session management schemes for the administration interface and the customer portal. However, for both interfaces, we perform the following 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 following table.
- Require staff members to reauthenticate after a specified period of inactivity. See the CLIENT_SESSION_EXP setting description in the following table.
- Require all login operations to be performed over HTTPS. See the CP_FORCE_PASSWORDS_OVER_HTTPS setting description in Customer Portal Settings for Session Data.

Table 5: 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.	15 minutes

Table 5: Administration Interface Settings for Session Data (Continued)

Configuration Setting	Description	Default Value
SESSION_HARD_TIMEOUT	Requires staff members to reauthenticate after a specified period of time. **Note:** This setting creates a new session each time the staff member reauthenticates. The previous session is destroyed.	12 hours

Table 6: 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 setting, the customer is required to log in again. **Note:** The default is 0, which means that the time is set by CP_LOGIN_COOKIE_EXP.	0
RightNow User Interface > Customer Portal > Login		
CP_CONTACT_LOGIN_REQUIRED	Defines whether the customer portal requires a customer to be logged in when accessing most pages or controls. **Note:** This setting does not apply to the login, password recovery, and account creation pages, or pass-through authentication (PTA). PTA is described in the *Pass-Through Authentication Guide*. If you do not have this guide, contact your Oracle account manager.	No
CP_COOKIES_ENABLED	Defines whether the customer portal tries to set cookies on a visitor's browser.	Yes

Table 6: Customer Portal Settings for Session Data (Continued)

Configuration Setting	Description	Default Value
CP_FORCE_PASSWORDS_OVER_HTTPS	Requires all login operations to be performed over HTTPS. **Note:** 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. **Important:** 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. **Important:** If you set a value for this setting, you must also set a non-zero value for CP_LOGIN_MAX_TIME.	0

Password protection

If the data protected by a password is not critical or subject to privacy legislation, the default values in Oracle Service Cloud may be acceptable. The most compromising dangers to passwords include:

- Password cracking by brute-force attack or an exhaustive key search.
- Nefarious activities, such as phishing and other social engineering attacks.

- Inadvertent release by users (staff members or customers) who write down their passwords, send them in emails, or expose them to the public in other ways.

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

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

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

No matter your security situation, you have considerable flexibility in setting up passwords for your staff and your customers. The following sections describe your configuration options and identify some tips for configuring secure passwords throughout your system.

Staff member passwords

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

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.

The options available to you in setting up password requirements can enhance security on your site as well as help protect your customers' information.

Table 7: 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). **Note:** In Oracle Service Cloud, the default is 5 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.) **Important:** 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.

Table 7: Password Security Benefits (Continued)

Password Configuration	Security Benefit
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?.(Defaults = 1.)
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. We recommend allowing 6 to 10 previous passwords. (Default = 10.)

Customer passwords

You have two ways to configure customer passwords in Oracle Service Cloud.

Configuration settings

The configuration setting EU_CUST_PASSWD_ENABLED controls the visibility of the Password field on the customer portal Log In page. 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 Log In page by disabling this setting.

Table 8: 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.	8

Table 8: Customer Portal Settings for Passwords (Continued)

Configuration Setting	Description	Default Value
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 Staff member passwords). The only differences between the two editors are the default values.

Forgotten passwords

There's no way around it—user names and passwords can be forgotten. For administrators, there is no way to recover forgotten credentials other than to contact their Oracle account manager. Other staff members can recover both their user name and password by using the Oracle Service Cloud account self-service feature. You can also use this functionality as a tool to maintain the integrity of your organization's login policies for all staff members.

The account self-service feature, accessed by clicking Login Help on the Login window, 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 the configuration settings descriptions in the following table for your options.

Table 9: 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 Login window. See • 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 Log In page on the customer portal. In both cases, if the password is forgotten, the correct user name must be entered, and then a link to the Password Reset page is emailed to the address associated with that user name. The password is reset when the link is sent and login is not allowed until the process is completed. Customers must do this within the time frame contained in SEC_EU_E-MAIL_LINK_EXPIRE. See Customer Portal Settings for Passwords and Emailing links to answers.

Secure password recommendations

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

- Lock staff accounts after three to five invalid login attempts. (The default is 5 in Oracle Service Cloud.)
- Set password length to a minimum of 10 characters.
- Require special characters and numbers.
- Require both uppercase and lowercase characters.
- Avoid using words or phrases that can be identified with a person, such as their name, address, telephone number, job title, type of car, and so on.
- Encourage users to choose passwords that are easy to remember and to type. For example, common words, song lyrics, poems and so on, with slightly misspelled words, go a long way toward security.
  - 2BeOrNot2Bee?
  - MaryhadaL1ttlelam
  - JollyBARN+be4Cow
- Stress the importance of keeping passwords secure by memorizing them and keeping them secret.

File attachment security

Oracle Service Cloud allows for attachments to incidents and answers as well as documents, templates, and snippets that are used in mailings and surveys. Attachments are a security concern because they can contain malicious code (malware) or data that is part of an attack on your site. All incoming attachments are scanned for malware, but you should always consider the possibility that attackers could evade detection.

Uploaded files containing HTML are a particular problem because they can provide links to sites that can harvest private data from unsuspecting people. For example, an attacker could upload a file that appears to be a link to an incident, but is actually a link to the attacker's site, which prompts the receiver to enter user name and password credentials. Staff members should never follow a link unless they are confident that it is safe, and no data should ever be

entered to a linked site. If it is necessary to access a referenced site, instead of clicking a link, look at the web address and verify that it goes where you think it should. Then type the correct web address into your browser.

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

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

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

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

Table 10: 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 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.	20971520 (20 MB) **Note:** The maximum allowable limit is 20 MB.
FATTACH_OPEN_ENABLED	Lets staff members open file attachments on the agent desktop.	No

Chat security

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

Table 11: 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. **Important:** To enable this hidden setting and define your allowed IP addresses and subnet masks, submit an incident to 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. **Important:** If this setting is left blank, the server accepts requests from all hosts.	Blank
Chat > General > Server		
CHAT_CORS_WHITELIST	Defines the list of origins allowed to make cross-origin requests through the Chat server. **Important:** If this setting is left blank, the server accepts requests from all origins.	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

Server protection

The Chat SOAP interface can be protected from potential threats by restricting access to valid chat servers. The configuration setting SEC_VALID_CHAT_API_HOSTS defines the list of IP addresses and subnet masks specifying the legal chat servers that are allowed to access the Chat SOAP interface. If this setting is left blank, all hosts are allowed.

Additionally, users can be protected from cross-origin resource sharing (CORS) attacks by defining the origins allowed to make CORS requests in CHAT_CORS_WHITELIST.

Chat API

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

Important Access to the Chat API is defined by the hidden configuration setting CHAT_WS_API_IP_HOST. To enable this setting and specify the IP addresses and subnet masks you want to allow, submit an incident to our support site.

User protection

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

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

Cross-origin resource sharing protection

Cross-origin resource sharing (CORS) lets client-side code make requests from one origin to another origin. This functionality can be abused by an attacker to retrieve information from your site or to perform actions as a valid user. You can protect your site from potential threats

by restricting access to valid requests. The CHAT_CORS_WHITELIST configuration setting defines the list of hosts or IP addresses allowed to make cross-origin domain requests. If this setting is left blank, all origins are allowed.

Important Keep in mind that restricting cross-origin resource sharing does not prevent cross-site request forgery (CSRF). For information about CSRF protection, see Cross-site request forgery and Social Experience security.

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

External queues

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

Social Experience security

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

- **Communities**
- **Channels**
- **Social Monitor**
- **Self Service for Facebook**

When providing service through social media, it is essential to maintain the security and confidentiality of your organization's social account logins. For this reason, Oracle Service Cloud lets you define channel accounts, which are shared credentials that allow designated agents to perform service functions through your social media accounts by securely storing the account logins and passing authentication parameters on behalf of your agents. If you are currently

providing service through social media channels directly through the web, we strongly recommend considering the security benefits of managing those efforts within Oracle Service Cloud instead.

When monitoring certain **channel types**, Oracle Service Cloud can store your customers' social media user names in their contact records. By tracking this identifying information, Oracle Service Cloud can associate incoming social monitor incidents with contacts based on their social media accounts. However, unlike channel accounts, channel types do not store passwords—they are used only to track the social identities of your customers across different services.You may also want to consider **SSL** encryption options for social media services. Then traffic between Oracle Service Cloud and the social media site is encrypted. See Certificates.

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

Communities and Social Monitor

There are also opportunities to access external data and code from within Social Experience, such as Oracle RightNow Social Experience communities (communities) and Oracle RightNow Social Monitor Cloud Service (Social Monitor). Consequently, these features may not have the same level of security as Oracle Service Cloud and the exchange of data may not be secure. Configuring your site in a high-security environment requires special care when implementing social features. Private and public keys are used to encrypt data between Oracle Service Cloud and the communities. For COMMUNITY_PRIVATE_KEY and COMMUNITY_PUBLIC_KEY setting descriptions, see Settings for Social Experience.

Community administration settings are used to configure all aspects of the community, including its members, hives, and content. Several of these settings can be used to reduce the vulnerability of your site.

Token verification

Token verification is enabled on your community pages to protect your site from cross-site request forgery (CSRF). Cross-site request forgery causes a user's browser to load pages 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, such as changing an email address, home address, password, or making a purchase. For more information about CSRF vulnerabilities, search for the CSRF Prevention Cheat Sheet on the OWASP website.

Cross-site scripting

Another community administration setting worth noting can be used to mitigate the risk of malicious code introduced by a community administrator, such as a cross-site scripting attack. While administrators are trusted users and administrator-initiated attacks are rare, we recommend selecting the Prevent Client-Side Scripts as Inputs for Admin Settings check box. To help prevent reflected cross-site scripting, select the Prevent Client-Side Scripts as Query String Parameter Value check box. Both of these check boxes are accessed on the community's General Settings page.

Cross-site flashing

In a cross-site flashing attack, a malicious user causes code to be executed within other users' browsers by linking to an off-site Flash application. (It is considered "off-site" because the URL that calls the Flash application can live on an unrelated server in the cloud.) This allows malicious users to control the content other users see and, potentially, to steal user data such as session cookies, user names, and passwords.

Community administrators can create post and comment types, user profile fields, and page panels that allow users to link to off-site Flash files through the community Flash File field in the post or comment type. If a user submits a post or comment that links to a Flash file through such a field or panel, the Flash file executes in the browser of any user that views the post. If the Flash file is malicious, a cross-site flashing attack can result.

Cross-site flashing can be prevented by not including a Flash File field in a comment or post type, a user profile field, or a panel. Because of potential misuse by malicious users, we recommend Flash field types be used with caution or not at all.

Self Service for Facebook authentication

Oracle RightNow Self Service for Facebook Cloud Service (Self Service for Facebook) lets you embed a set of Oracle Service Cloud service and community features directly on your organization's Facebook page. After you create a Facebook page, you must enable Facebook on the Configuration Settings editor (FACEBOOK_ENABLED).

When the Self Service for Facebook application is installed on your Facebook page, it provides two values—your application ID and your secret key. You must assign these values to their respective configuration settings (FACEBOOK_APPLICATION_ID and FACE-

BOOK_APPLICATION_SECRET) in order to authenticate the link between Facebook and Oracle Service Cloud. To ensure the integrity and security of your connection, you should keep these values confidential.

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

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

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

When your Facebook page or your Twitter account is created, they provide two values—your application ID and your secret key. To allow single sign-on, these values must be assigned to their respective configuration settings in Oracle Service Cloud:

- FACEBOOK_OAUTH_APP_ID and FACEBOOK_OAUTH_APP_SECRET

- TWITTER_OAUTH_APP_ID and TWITTER_OAUTH_APP_SECRET

Table 12: Settings for Social Experience

Configuration Setting	Description	Default Value
RightNow Common > RightNow Social		
COMMUNITY_PRIVATE_KEY	Defines the private key to be used to encrypt data between Oracle Service Cloud and communities in Social Experience.	Blank
COMMUNITY_PUBLIC_KEY	Defines the public key to be used to encrypt data between Oracle Service Cloud and the communities in Social Experience.	Blank
RightNow Common > 3rd-Party Applications > Facebook		
FACEBOOK_APPLICATION_ID	Specifies the Facebook application ID used to host Facebook for Oracle Service Cloud.	Blank
FACEBOOK_APPLICATION_SECRET	Specifies the Facebook application secret key used to host Facebook for Oracle Service Cloud. This setting is also used to authenticate staff members and customers who use Self Service for Facebook.	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

Table 12: Settings for Social Experience (Continued)

Configuration Setting	Description	Default Value
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 Oracle Service Cloud 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 Oracle Service Cloud channel, Twitter.	Blank

7

Recommendations for Security-Related Configuration Settings

The tables in this section can help you look at configuration settings in a logical way as they pertain to security. The settings are categorized by security levels—high, medium, and low. Once you've evaluated your security requirements, you can use these recommendations to achieve the level of security that fits your organization's needs.

Important To make an accurate determination of your organization's security needs, you must have a comprehensive knowledge of your site and its use.

Security level

The following list represents configuration settings that you should consider using or setting to achieve your designated level of security—high, medium, or low. To make the settings easy to find, the list is ordered alphabetically with each setting's respective path on the Configuration Settings editor.

Table 13: Recommended Security-Related Settings

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
CHAT_WS_API_IP_HOST	Set to allowed IP addresses and subnet masks. **Important:** To enable this hidden setting and define your allowed IP addresses and subnet masks, submit an incident to our support site.		

Table 13: Recommended Security-Related Settings (Continued)

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
Chat > General > Server			
CHAT_CORS_WHITELIST	Set to allowed origins.	Set to allowed origins.	Blank (default)
RightNow User Interface > General > Security			
CLIENT_SESSION_EXP **Note:** 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 **Important:** 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 **Important:** 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

Table 13: Recommended Security-Related Settings (Continued)

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
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			
EGW_PASSWD_CREATE	Yes (default)	Yes (default)	No
EGW_SECURE_UPDATE_ENABLED	Yes (default)	Yes (default)	No
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.

Table 13: Recommended Security-Related Settings (Continued)

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
Chat > General > Create Incident			
INC_PRIVATE_TRANSCRIPT_ONLY	Yes	Yes	No (default)
RightNow User Interface > Tool Bar > General			
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
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)

Table 13: Recommended Security-Related Settings (Continued)

Path/Configuration Setting	For high-security environment	For medium-security environment	For low-security environment
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).		
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)

Security significance

In the following list, the configuration settings are grouped by high, medium, and low in security significance.

Table 14: 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. **Important:** To enable this hidden setting and define your allowed IP addresses and subnet masks, submit an incident to our support site.
	CLIENT_SESSION_EXP	15 **Note:** 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.
	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

Table 14: Recommended Security-Related Settings By Significance (Continued)

Significance	Configuration Setting	Recommended Setting
Medium	CHAT_CORS_WHITELIST	Set to allowed origins.
	CP_CONTACT_LOGIN_REQUIRED	As needed.
	CP_LOGIN_MAX_TIME	As needed.
	EGW_PASSWD_CREATE	Yes
	EGW_SECURE_UPDATE_ENABLED	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.

Table 14: Recommended Security-Related Settings By Significance (Continued)

Significance	Configuration Setting	Recommended Setting
Low	CP_COOKIES_ENABLED	As needed.
	CP_MAX_LOGINS	As needed.
	CP_MAX_LOGINS_PER_CONTACT	As needed. **Important:** 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.

Index

A

C

E

F

N

P

S

T