Security for Admins Cheatsheet

Overview

Force.com provides built-in security features and protections, which can be utilized by administrators to control login and authentication, establish password policies and manage session settings. Also see the Security Cheat Sheet for Developers.

Login and Authentication Settings

Login and Authentication features and restrictions. These settings should be enabled as appropriate for your company.

Setting Name	Description	Location
Prevent Access by IP Address	Set an allowed Login IP Range on a specific profile. Access is completely denied from outside the range.	From Setup, enter `Profiles` in the **Quick Find** box, then select **Profiles**.
Require Identity Verification	Set a Trusted IP Range. Access from outside the range prompts the user for identity confirmation (via text message, email, etc.).	From Setup, enter `Network Access` in in the **Quick Find** box, then select **Network Access**.
Time of Day Restrictions	User logins can be restricted to specified times of the day.	From Setup, enter `Profiles` in the **Quick Find** box, then select **Profiles**.
Single Sign-On using Security Assertion Markup Language (SAML)	Instead of requiring a password, salesforce.com verifies an HTTP request from an identity provider to authenticate a user.	From Setup, enter `Single` in the **Quick Find** box, then select **Single Sign-On Settings**.
Delegated Authentication	Instead of requiring a password, salesforce.com makes a Web services call to your organization to authenticate a user.	Contact Support to enable this feature.
Two-Factor Authentication for User Interface Logins	Requires users to authenticate using two different methods, such as a password and a device- generated code.	Two-factor Authentication for User Interface Logins permissions setting on the profile (cloned profiles only) or permission set.
Two-Factor Authentication for API Logins	Requires users to authenticate for API access using two different methods. Enable Two-Factor Authentication for User Inteface Logins, first.	Two-factor Authentication for API Logins permissions setting on the profile (cloned profiles only) or permission set.
Authentication Providers	Enable users to log into your Salesforce organization using their login credentials from an external service provider such as Facebook© and Janrain©, or OpenID Connect providers (Google, Amazon, and Paypal).	From Setup, enter `Auth` in the **Quick Find box**, then select **Auth. Providers**

Password Policies

Controls available for enabling password restrictions and account lockout settings. From Setup, enter Password in the **Quick Find** box, then select **Password Policies**.

You can also apply these to individual profiles.

Setting Name	Description	Recommended
User passwords expire in	Frequency to automatically expire passwords.	90 days or less
Enforce password history	Number of previous passwords to save to prevent password re-use.	3 or more passwords remembered
Minimum password length	Minimum length of a password.	8 characters
Password complexity requirement	Controls whether the password contains a mix of letters and numbers.	Must mix alpha, numeric, and special characters, or more complex
Password question requirement	Require the user's password hint to not contain the password.	Cannot contain password
Maximum invalid login attempts	Number of invalid logins allowed before locking out the account.	3
Lockout effective period	Length of time an account remains locked out.	15 minutes
Obscure secret answer for password resets	Hides answers to security questions as you type.	Yes
Require a minimum 1 day password lifetime	Prevents more than one password change in a 24 hour period. Increases security, but might require an administrator to reset a user's password.	Yes
Expire All Passwords	From Setup, enter `Expire` in the **Quick Find box,** then select **Expire All Passwords**	Only as necessary. You can expire passwords for all users (except those with the "Password Never Expires" permission) any time you want to enforce extra security for your organization.

Security for Admins Cheatsheet

Session Settings

Controls available for general session handling settings, including session timeout. From Setup, enter Session in the **Quick Find** box, then select **Session Settings**.

You can apply some of these to individual profiles or permission sets.

Setting Name	Description	Recommended
Timeout value	Allowed idle session time before automatically logging user out of Salesforce.	2 hours or less
Disable session timeout warning popup	Disable the warning browser pop-up when a user is about to be logged out from the idle session timeout.	Yes
Lock sessions to the IP address from which they originated	Force the user session to remain locked to the IP address from which the user authenticated. May impact AppExchange installations.	Yes (if possible)
Require secure connections (https)	Require HTTPS on all page requests.	Yes
Enable caching and autocomplete on login page	Allow the user's browser to store and auto- complete usernames or passwords after first login.	No
Require HttpOnly attribute	Restricts session ID cookie access. A cookie with the HttpOnly attribute is not accessible via JavaScript.	Yes
Allow Lightning Login	Allow users to log in password-free with their username and Salesforce Authenticator.	Yes
Allow location-based automated verifications with Salesforce Authenticator	Allow users to automate verifications from anywhere, from trusted IP addresses only, or not at all.	Yes
Let users authenticate with a security key (U2F)	Allow a registered U2F security key device as a second factor.	Yes
Clickjack protection	Protects against clickjack attacks on Visualforce and non-setup Salesforce pages	Yes
Set High Assurance Session Security Levels	Require two-factor authentication for logins. In the user profile, set the *Session security level required at login* to High Assurance. Then set session security levels to apply the policy for login methods such as username and password, SAML single sign-on, or social sign-on.	Yes

Auditing and Logging

Salesforce provides several types of audit logs for monitoring logins and changes to your organization.

Setting Name	Description	Location
User Login History	All successful and failed login attempts are recorded and saved for 180 days.	**Setup | Manage Users | Login History**
Setup Audit Trail	Every configuration (Setup) change is logged and archived for 180 days.	From Setup, enter `Audit` in the **Quick Find** box, then select **View Setup Audit Trail**
Object History Tracking	Selected standard and custom fields can be enabled to track the change history.	Set History Tracking field in the object settings**.**
Identity Usage Report	A new custom report includes usage information for both SAML and OAuth connected apps.	From Setup, enter `Report` in the **Quick Find** box, then select **Report Types**. Click New Custom Report Type, Set the Primary Object to Identity Event Logs

Access Control

Salesforce provides three ways to assign access permissions to users.

Setting Name	Description	Location
Delegated Administration	Use delegated administration to assign limited administrative privileges to selected non-administrator users in your organization.	From Setup, enter `Delegated` in the **Quick Find** box, then select **Delegated Administration** (contact Salesforce to enable this feature)
Permission Sets	Create permission sets with specific access policies, and then assign the permission set to individual Users in your salesforce.com organization.	From Setup, enter `Permission` in the **Quick Find** box, then select **Permission Sets**
Profiles	Create (or edit existing) profiles with specific access policies, and then assign a user to that profile.	From Setup, enter `Profiles` in the **Quick Find** box, then select **Profiles**.

OAuth Settings

Salesforce supports a variety of authentication flows using the OAuth 1.0 and 2.0 protocols to grant external apps (connected apps) access without exposing individual user credentials. You can manage the OAuth settings for individual connected apps.

Setting Name	Description	Location
Permitted Users	Determines who can run the connected app; all users or only admin approved users.	From Setup, enter `Apps` in the **Quick Find** box, then click **"Edit"** next to the name of the connected app to modify
IP Restrictions	Use the IP restrictions set in the org or profile, or relax the IP restrictions for the connected app. Optionally, require a second factor authentication to relax the IP restrictions.	From Setup, enter `Apps` in the **Quick Find** box, then click **"Edit"** next to the name of the connected app to modify
Control refresh of access tokens (via login)	Set the required user login intervals to once, every time a user tries to use the connected app, or after a specified period of time.	From Setup, enter `Apps` in the **Quick Find** box, then click **"Edit"** next to the name of the connected app to modify
High Assurance session required	Only users meeting the High Assurance requirements, such as two-factor authentication, for their org can use the connected app.	From Setup, enter `Apps` in the **Quick Find** box, then click **"Edit"** next to the name of the connected app to modify
Mobile session timeout	If the connected app uses the Salesforce Mobile SDK, the developer can enable an option to provide a configurable session timeout for mobile apps.	From Setup, enter `Apps` in the **Quick Find** box, then click **"Edit"**next to the name of the app to modify. Select PIN Protect
Mobile PIN length	If the connected app uses the Salesforce Mobile SDK, the developer can enable an option to control the use and length of user PINs (Personal Identification Numbers) for authentication.	From Setup, enter Apps in the **Quick Find** box, then click **"Manage"** next to the name of the app to modify. Set your preferences in Moblie Integration
Block/ Unblock OAuth connected apps	Monitor the usage of connected apps and block/unblock individual connected apps, manually.	From Setup, enter `Connected` in the **Quick Find** box, then select **Connected Apps OAuth Usage**

Sensitive Permissions

When using profiles, we recommend reviewing profiles for these sensitive permissions. From Setup, enter `Profiles` in the **Quick Find** box, then select **Profiles**.

Permission	Description
Author Apex	Can modify and deploy Apex. By default, Apex code runs with full administrative privileges.
Customize Application	Make configuration changes to the organizational settings.
Download AppExchange packages	Install or uninstall packages from the AppExchange.
Manage Users	The ability to create or modify user accounts, including logins, sharing rules, and login restrictions.
Modify All Data	This permission gives the user the ability to create, edit, or delete all data in Salesforce.
Password Never Expires	Prevent the password from expiring.
View All Data	View all data owned by other users.

For other cheatsheets:
http://developer.salesforce.com/cheatsheets

salesforce

developer.salesforce.com