

Salesforce Certified Admin and App Builder

Lesson 5—Security Controls



What You'll Learn

- Viewing Object Security and Record Access
- Sharing Settings and Field Accessibility
- Managing Session Settings and Network Access
- Viewing Setup Audit Trail
- Setting up Delegated Administration



Viewing Object Security

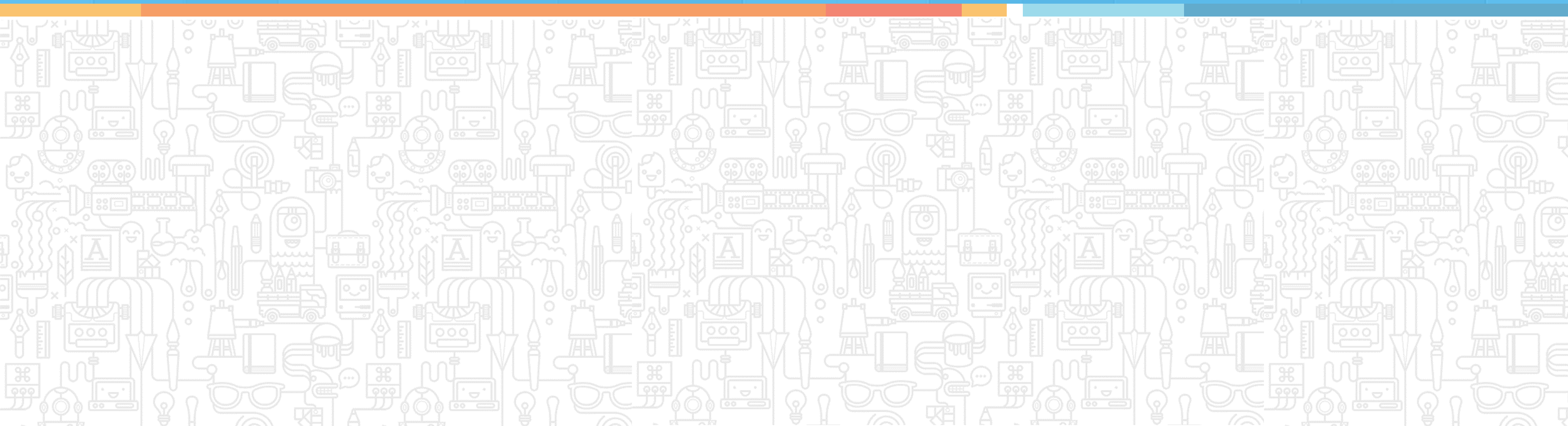


Keep the following points in mind when viewing object security:

- Salesforce has two types of Objects.
- Standard Objects are included with Salesforce.
- Custom Objects are created to store information unique to your company and business.
- To view object security, click on Security Controls.
- Click Sharing Settings.
- Click the arrow in the Manage Sharing settings drop down list.
- Choose the object you would like to view.

Organization-Wide Defaults Edit		
Object	Default Internal Access	Default External Access
Lead	Public Read/Write /Transfer	Public Read/Write /Transfer
Account, Contract and Asset	Private	Private
Contact	Controlled by Parent	Controlled by Parent
Order	Controlled by Parent	Controlled by Parent
Opportunity	Private	Private

Changing Default Record Access

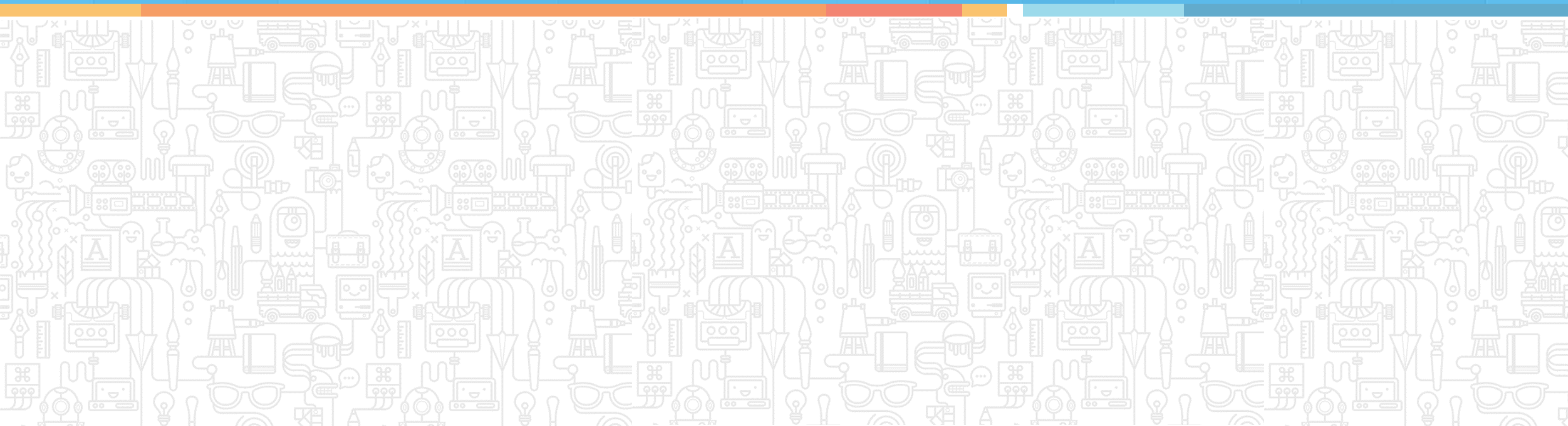


Here are some important facts about default record access:

- All objects are set to allow public read or write access by default.
- Settings for each object can be customized for your organization's security.
- Access options are private, public read only, public read or write, public read or write transfer, public full access, and controlled by parent.
- To change record access, click Security Controls.
- Click Sharing Settings, and then Edit.
- Click the Default Access drop down arrow next to the object to change.
- Select an option from the drop down list.
- Click Save.

Object	Default Internal Access
Lead	Public Read/Write/Transfer
Account, Contract and Asset	Private Public Read Only Public Read/Write Public Read/Write/Transfer

Sharing Settings



Important points to keep in mind are:

- Access to data can be controlled at many different levels.
- Sharing settings control access to data at the record level.
- Organization-wide default sharing settings give you a basic level of access for each object.
- You can extend that level of access using hierarchies or sharing rules.
- There are additional sharing settings you can control.
- Other settings can control Standard Report Visibility, Manual Sharing for user records, and Manager Groups.

Account Sharing Rules

[New](#)[Recalculate](#)

Action	Criteria	Shared With
Edit Del	Account: Account Record Type EQUALS Client	<u>Group: Staff</u>
Edit Del	Owner in All Internal Users	<u>Role: Project Specialist</u>

Field Accessibility



Important points to consider are:

- Field-level security restricts a user's access to fields by setting them to visible, editable, or read only.
- Page layouts and profile can also add restrictions.
- To check a field's accessibility, click on Customize.
- Click an object and then click fields.
- Click a field label.
- Click the View Field Accessibility button.


Field Name	Field Type	Visible
Account Name	Name	<input checked="" type="checkbox"/>
Account Number	Text	<input type="checkbox"/>
Account Owner	Lookup	<input checked="" type="checkbox"/>
Account Record Type	Record Type	<input checked="" type="checkbox"/>
Account Site	Text	<input type="checkbox"/>
Account Source	Picklist	<input checked="" type="checkbox"/>

Password Policies



Remember the following points when setting up password policies:

- For security purposes, set up password policies for your organization.
- You can determine the complexity of passwords, length, expiration, invalid attempts, and so on.
- Go to setup and click Security Controls.
- Click Password Policies.
- Set restrictions and login/logout policies.
- Add a message for lockout assistance.

User passwords expire in	<input type="text" value="Never expires"/>
Enforce password history	<input type="text" value="No passwords remembered"/>
Minimum password length	<input type="text" value="5"/> 

Session Settings



Keep the following points in mind:

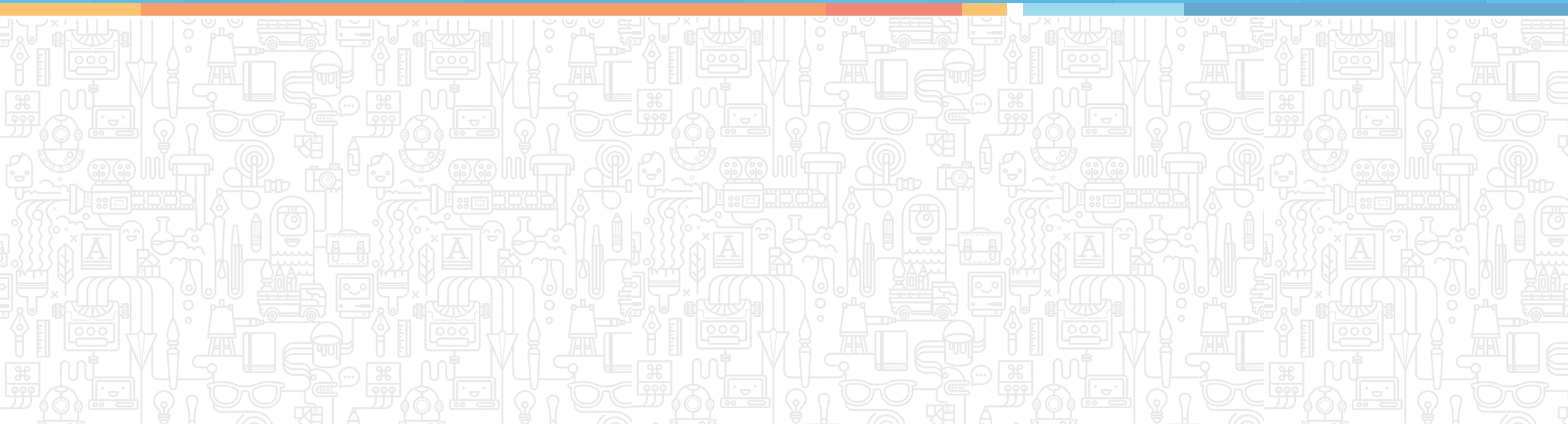
- After login, a user establishes a session with the platform.
- If a user leaves the computer on while still logged in, there is a security risk to the network.
- You can control the time for a session timeout for inactivity.
- To configure session settings, go to setup, and click Security Controls.
- Click Session Settings.
- Click the drop down arrow to add your Timeout Value.
- You have the option to check/uncheck other settings in session settings.
- Click Save.

Session Timeout

Timeout Value

- ☒ Disable session timeout warning popup
- ☒ Force logout on session timeout

Login Flows

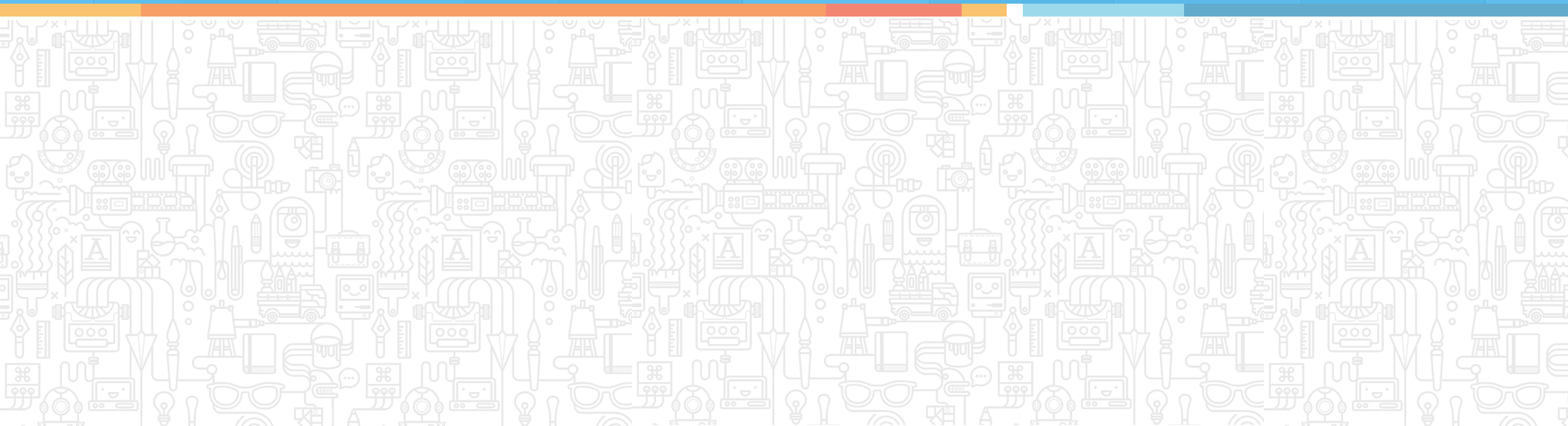


Keep the following in mind when creating login flows:

- Login Flows can be applied to Salesforce organizations, communities, and portals.
- Login Flows can be used to collect registration information, terms of service acceptance form, and so on.
- Flows can be applied to multiple profiles.
- To create a Login Flow, go to setup, and click Security Controls.
- Click Login Flows and create a name.
- Choose the flow you would like to apply.
- Select a user license and profile.

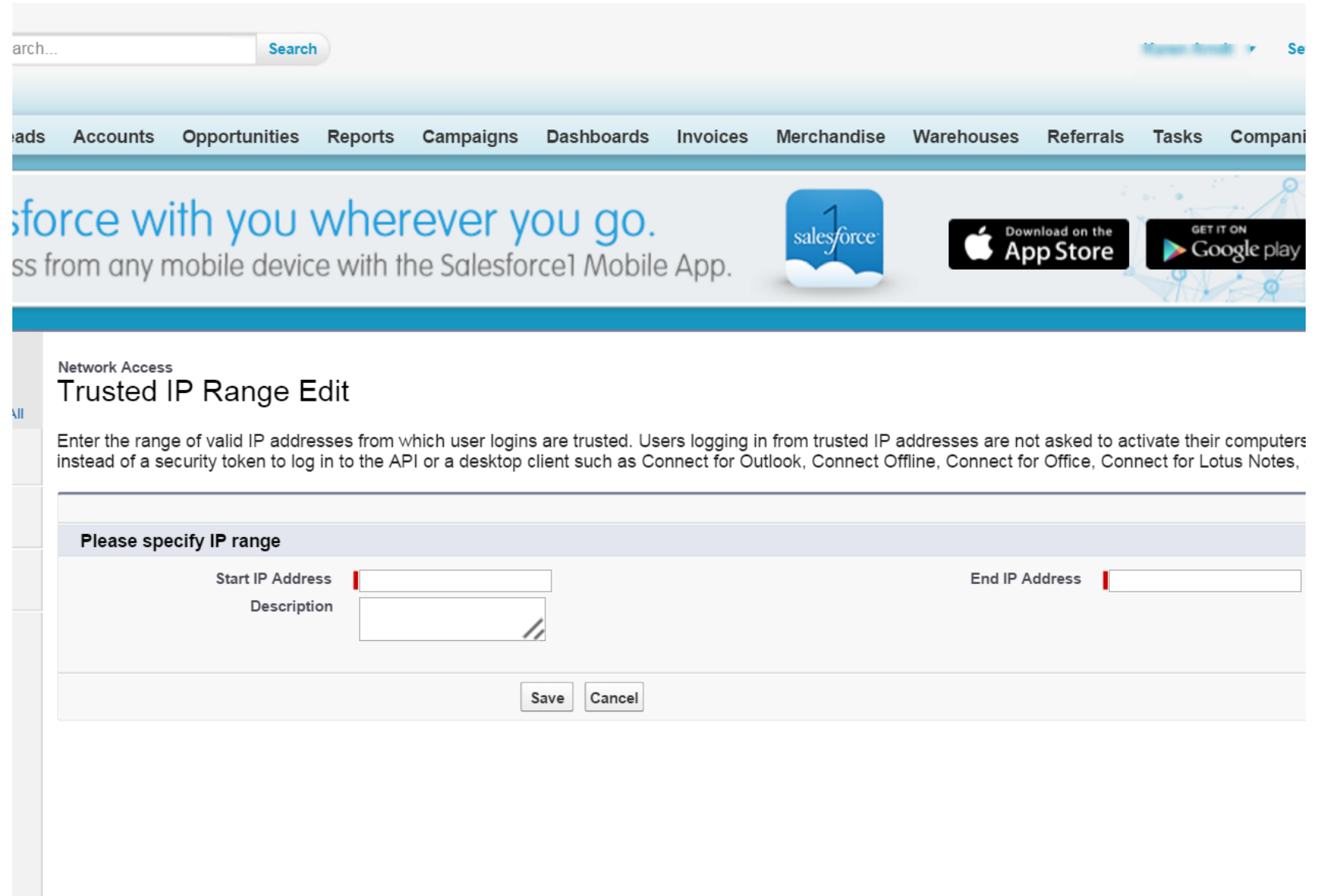
Name	<input type="text" value="Main Office"/>
Flow	<input type="text" value="--None--"/>
User License	<input type="text" value="Force.com - App Subscription"/>
Profile	<input type="text" value="Business Analyst"/> 

Network Access



Trusted IP Ranges is a list of IP addresses that users can log in without being challenged for identity verification.

- To configure network access, go to setup, and click on Security Controls.
- Click Network Access.
- Click New.
- Type the beginning and ending range of the IP address.
- Click Save.



The screenshot shows the Salesforce 'Trusted IP Range Edit' page. At the top, there is a search bar and a navigation menu with links like 'Leads', 'Accounts', 'Opportunities', 'Reports', 'Campaigns', 'Dashboards', 'Invoices', 'Merchandise', 'Warehouses', 'Referrals', 'Tasks', and 'Company'. Below the navigation menu is a banner for the Salesforce mobile app with the text 'Salesforce with you wherever you go.' and 'Access from any mobile device with the Salesforce1 Mobile App.' There are also buttons for 'Download on the App Store' and 'GET IT ON Google play'. The main content area is titled 'Network Access' and 'Trusted IP Range Edit'. It contains a text box for 'Start IP Address', a text box for 'End IP Address', and a text area for 'Description'. There are 'Save' and 'Cancel' buttons at the bottom right.

Activations



Remember the following points when reviewing activations:

- On the activations page, you can see different IP addresses and client browsers that have been activated for an organization.
- Admins can revoke the activation status for all user devices.
- To go to the activation page, click on Security Controls.
- Click Activations.

Remove			
Username ↑	Login IP	Created Date	Is Authenticated
acamacho@cloudcreations.com	181.66.220.231	12/9/2015 9:13 AM	✓
acamacho@cloudcreations.com	201.240.116.245	12/9/2015 6:10 PM	✓
acamacho@cloudcreations.com	201.240.109.102	12/15/2015 8:55 AM	✓

Session Management



Keep the following points in mind when configuring session management:

- On the User Session Information page you can review active sessions and details.
- An administrator can remove a user from an active session if they suspect suspicious activity.
- To view the user session information, go to setup, and click on Security Controls.
- Click Session Management.
- To remove a user, click the checkbox next to their username.

Username ↑	Session ID	Parent Session ID	Session Type
acamacho@cloudcreations.com	0Akj0000096THQO		Oauth2
acamacho@cloudcreations.com	0Akj0000096THVo	0Akj0000096THQO	Aura

Login Access Policies

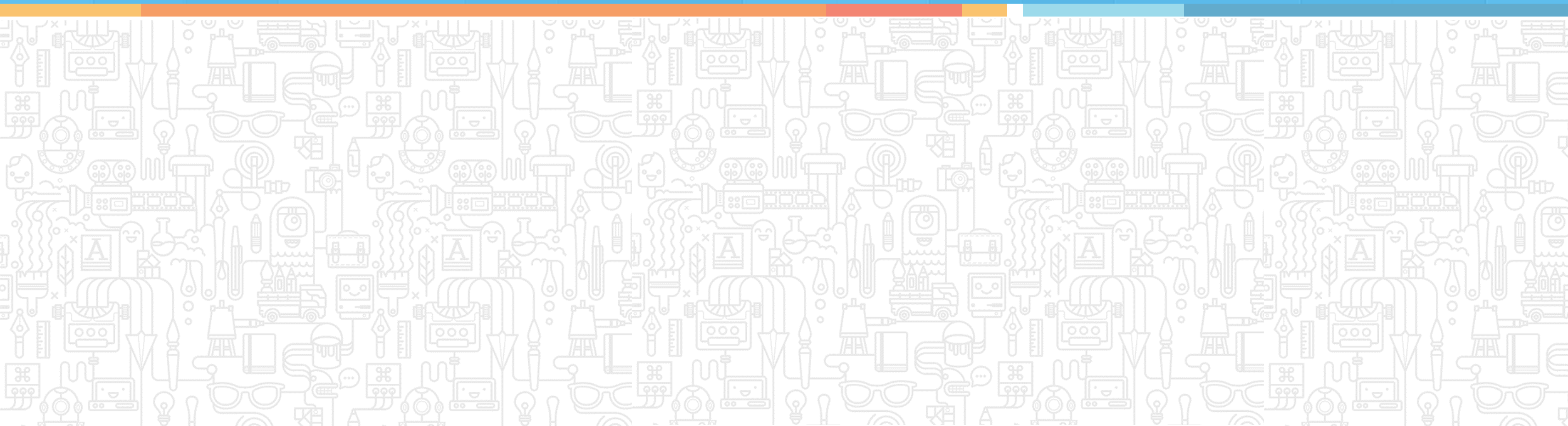


Remember the following points regarding login access policies:

- If the “Administrators Can Log in as Any User” checkbox has been enabled, administrators with “Modify All Data Permission” or “View Setup and Configuration” permission can log in as any user.
- The user will not have to grant the administrator access.
- You can allow or exclude login access for certain admins, technical staff, or apps from the AppExchange.

Support Organization	Packages	Available to Users
Salesforce.com Support		
salesforce.com Support	<u>SFDC Channel Order</u>	Not Available
salesforce.com Support	<u>Salesforce for Google AdWords</u>	Not Available

Certificate and Key Management

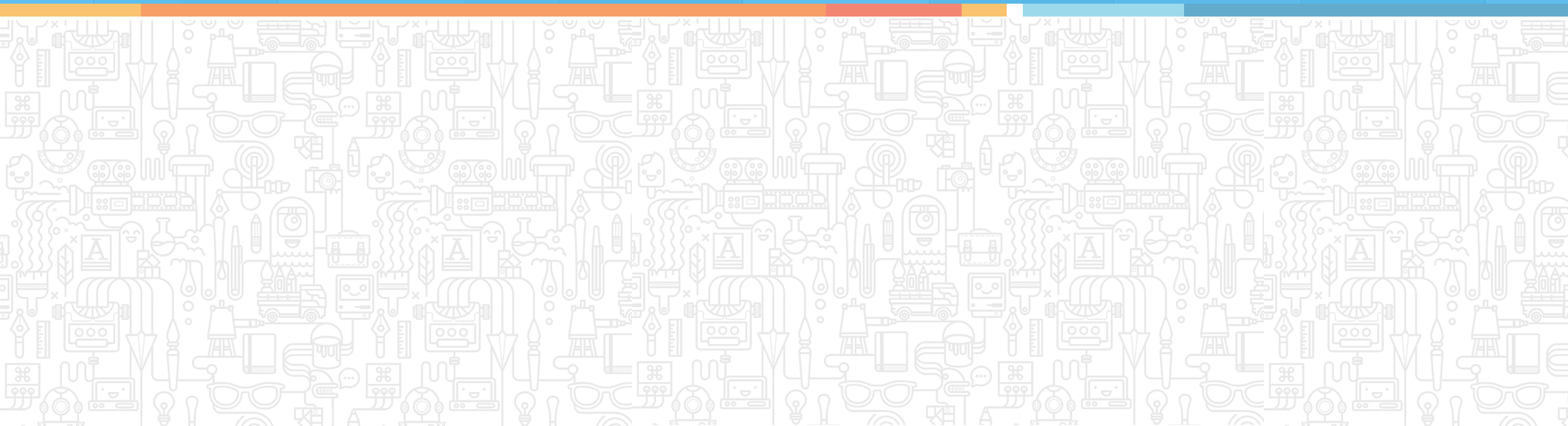


Keep the following points in mind:

- Certificates are used for authenticated SSL communications with an external website or when using your organization as an Identity Provider.
- To access the Certificate and Key Management Page go to Security Controls.
- Click Certificate and Key Management.
- You can also upload or download a secure certificate from this page.

Certificates		Create Self-Signed Certificate		Create CA-Signed Certificate		
		Export to Keystore		Import from Keystore		
Action	Label ↑	Type	Active	Key Size	Expiration Date	Created Date
Edit	<u>SelfSignedCert_27May2015_152034</u>	Self-Signed	<input checked="" type="checkbox"/>	2048	5/27/2017	5/27/2015 8:20 AM

Viewing Setup Audit Trail



Remember the following points when viewing the audit trail:

- The setup audit trail tracks changes to Administration, Customizations, Sharing and Security, Data Management, Development, and Use of the application.
- The audit trail tracks the date, user, and their action.
- You can download the information to a .csv file.
- Go to setup and click Security Controls.
- Click View Setup Audit Trail.

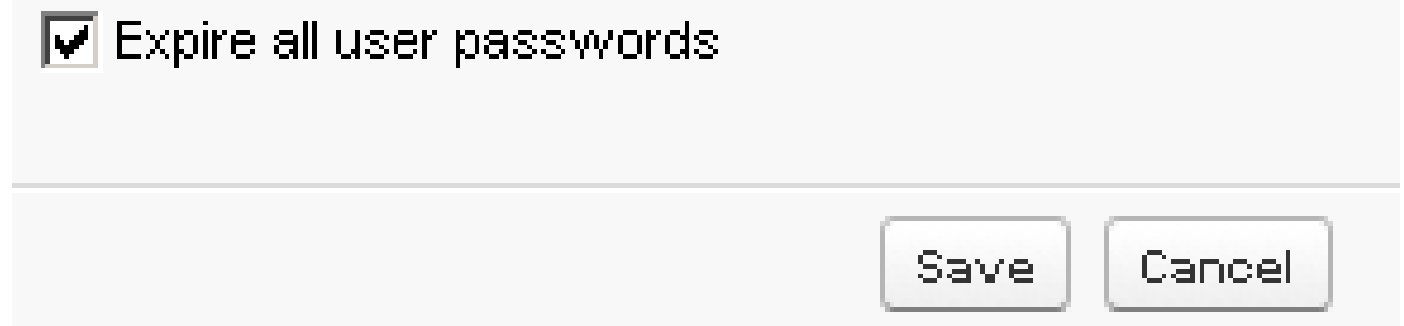
Date	User	Action	Section
1/24/2016 9:11:00 PM PST	jdavis@cloudcreations.com	Changed profile Chief Accounting Officer: field-level security for Extension Request: Extension Date Approved was changed from Read/Write to Read Only	Manage Users

Executing Expire All Passwords



Remember the following when expiring passwords:

- Administrators can expire all passwords for all users at any time.
- The next time users login, they will be prompted to set a new password.
- To configure “Expire All Passwords” go to Security Controls.
- Click Expire All Passwords.
- Click the box next to Expire All Passwords.
- Click Save.



A screenshot of a user interface showing a checkbox labeled "Expire all user passwords" which is checked. Below the checkbox are two buttons: "Save" and "Cancel".

Delegated Administration



Keep the following points in mind:

- If you want to assign limited administrative privileges to users who aren't administrators, use delegated administration.
- Users can be edited in specified and subordinate roles.
- You can reset passwords, set quotas, create default opportunity teams, and personal groups.
- They would be able to also login as users who have granted login access to their administrators.

Delegated Group Edit Save Cancel

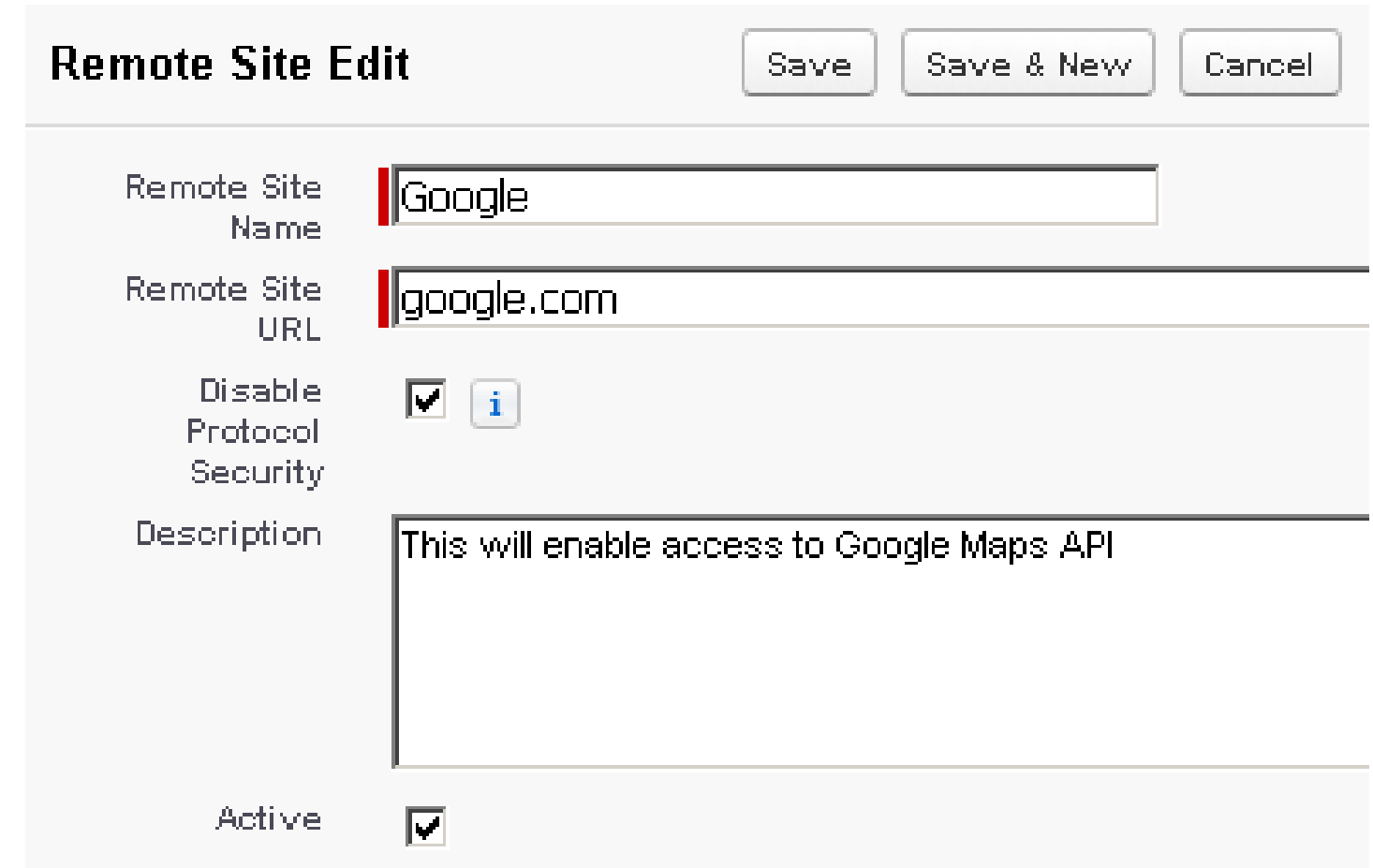
Delegated Group Name	<input type="text" value="Sales Team Admin"/>	Enable Group for Login Access	<input checked="" type="checkbox"/>
Developer Name	<input type="text" value="Sales_Team_Admin"/> i		

Remote Site Settings




Keep the following points in mind:

- An external site must be registered in the Remote Site Settings page. Otherwise, a call to the site from any Visualforce page, Apex callout, or JavaScript code using XMLHttpRequest in an s-control or custom button will fail.
- Remote Site Setting extends the metadata type and inherits its name field.
- Remote Site Setting components are stored in the Remote Site Settings directory of the corresponding package directory.
- The file name matches the unique name of the remote site setting, and the extension is .remoteSite.



The image shows a 'Remote Site Edit' form with the following fields and values:

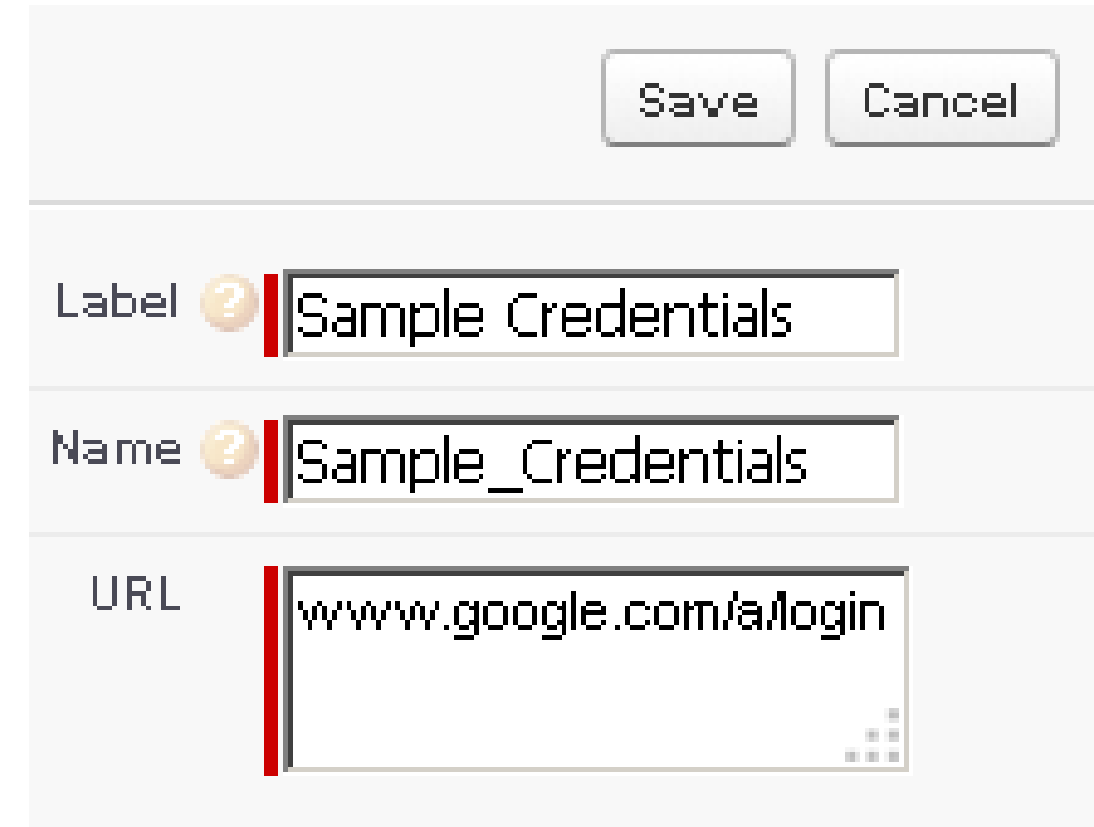
Remote Site Edit		Save	Save & New	Cancel
Remote Site Name	Google			
Remote Site URL	google.com			
Disable Protocol Security	<input checked="" type="checkbox"/> 			
Description	This will enable access to Google Maps API			
Active	<input checked="" type="checkbox"/>			

Named Credentials



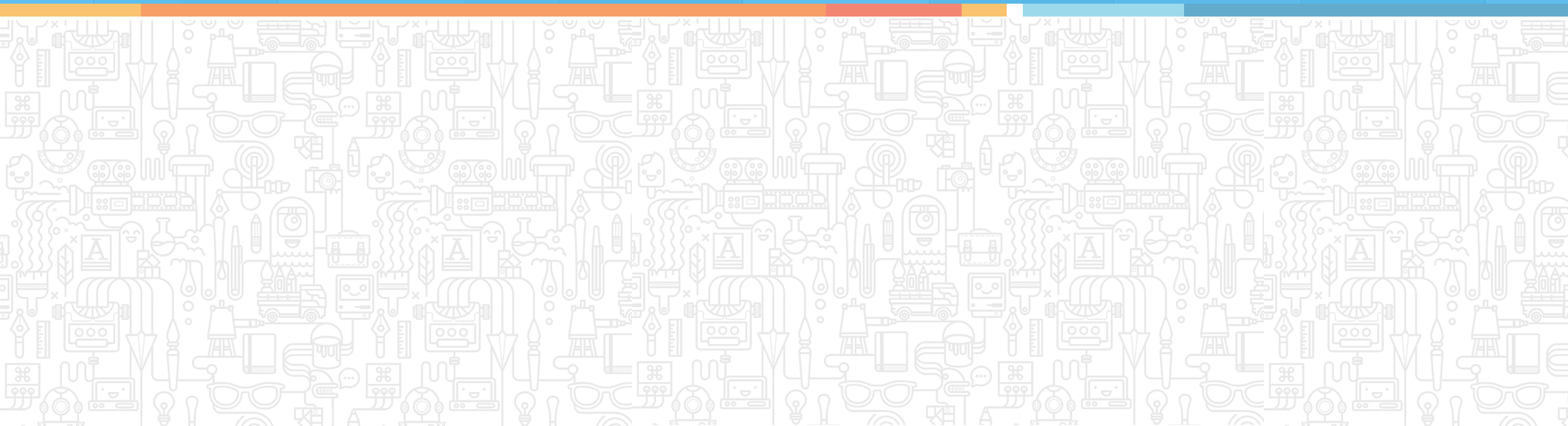
Keep in mind the following when creating named credentials:

- A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition.
- You can simplify the setup of authenticated callouts by specifying a named credential as the callout endpoint.
- Alternatively, you can specify a URL as the callout endpoint and register that URL in your organization's remote site settings.
- However, in that case, you handle the authentication yourself, for example, in your code for an Apex callout.



The screenshot shows a configuration window for a named credential. At the top right are 'Save' and 'Cancel' buttons. Below them are three input fields, each with a label and a help icon (a question mark in a circle). The first field is labeled 'Label' and contains the text 'Sample Credentials'. The second field is labeled 'Name' and contains the text 'Sample_Credentials'. The third field is labeled 'URL' and contains the text 'www.google.com/a/login'. The URL field has a small icon in the bottom right corner, possibly representing a link or a warning.

File Upload and Download Security



Keep in mind the following points:

Your organization may want to specify how the files are handled during upload and download due to security reasons. Don't enable the "Don't Allow HTML" uploads setting if you are using the partner portal, as it prevents you from customizing the appearance of the partner portal.

There are three choices for download behavior.

1. Download – (recommended) The file, regardless of type, is downloaded.
2. Execute in Browser – The file is executed and displayed automatically when accessed in a browser or through an HTTP request.
3. Hybrid – It uses the default browser execution behavior, but downloads Chatter and Salesforce CRM Content Files.

☐ Don't allow HTML uploads as attachments or document records [i](#)

File Type	Download Behavior i
.avi	Hybrid
.doc, .dot	Download
	Execute in Browser
	Hybrid



QUIZ 1

Where in Setup can you adjust org-wide defaults?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



QUIZ 1

Where in Setup can you adjust org-wide defaults?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



The correct answer is **a**.

Org-wide defaults are controlled in the Sharing Settings area.

QUIZ 2

Where can you adjust visibility of field access?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



QUIZ 2

Where can you adjust visibility of field access?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



The correct answer is **b**.

The ability to make a field viewable, and/or editable is found in Field Accessibility.

QUIZ 3

Where can you control User login locations?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



QUIZ 3

Where can you control User login locations?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



The correct answer is **c**.

User login locations can be controlled from the Network Access area.

QUIZ 4

Where can you adjust session timeout?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



QUIZ 4

Where can you adjust session timeout?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. Session Management



The correct answer is **d**.

The timeout period can be adjusted in the Session Management area.

QUIZ 5

Where can you find changes made to Salesforce?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. View Setup Audit Trail



QUIZ 5

Where can you find changes made to Salesforce?

- a. Sharing Settings
- b. Field Accessibility
- c. Network Access
- d. View Setup Audit Trail



The correct answer is **d**.

Changes made to Salesforce can be found in the View Setup Audit Trail.



Case Study

Scenario

Analysis

Solution

United Containers has employees working from home, on the road, as well as from different office locations. Currently, employees are logging in through unsecured connections at coffee shops and book stores, when the company strictly prohibits this action. United Containers needs to find a way to restrict access to Salesforce while still allowing some employees to login from home.

Scenario

Analysis

Solution

United Containers decided to implement Security Controls in Salesforce for the following reasons:

1. Network Access allows Administrators to restrict access to certain IP addresses.
2. Session Settings allow Administrators to set shorter timeouts for increased security.
3. Password Policies can be configured to require longer and more complex passwords.

Scenario

Analysis

Solution

The United Containers system administrator took the following steps to resolve their security issues:

1. Org-wide sharing defaults were made private.
2. Password policies were set to require a 12-character password.
3. Session Settings were changed to two hours.
4. The Setup Audit Trail was monitored for any unauthorized access or changes.

Key Takeaways

- Setting up object security is an important aspect of administration.
- Sharing settings can be customized to include only certain fields.
- Session and network access can be controlled.
- The audit trail shows all changes made to the system.



This concludes 'Security Controls.'

The next lesson is 'Profiles.'