1. Data Security
2. Control Access to Objects

Control Access to Objects

Learning Objectives

After completing this unit, you'll be able to:

- View existing profiles and create new ones.
- Modify access to objects using profiles.
- View all assigned users in a profile.
- Create new permission sets.
- Assign permission sets to single and multiple users.

Manage Object Permissions

The simplest way to control data access is to set permissions on a particular type of object. (An object is a collection of records, like leads or contacts.) You can control whether a group of users can create, view, edit, or delete any records of that object.

You can set object permissions with profiles or permission sets. A user can have one profile and many permission sets.

- A user’s profile determines the objects they can access and the things they can do with any object record (such as create, read, edit, or delete).
- Permission sets grant *additional* permissions and access settings to a user.

Use profiles to grant the minimum permissions and settings that all users of a particular type need. Then use permission sets to grant more permissions as needed. The combination of profiles and permission sets gives you a great deal of flexibility in specifying object-level access.

Object Permissions for the Recruiting App

As an example, let’s explore how you might configure object-level access in the Recruiting app. The app has four main types of users: hiring managers, recruiters, interviewers, and standard employees. What kinds of access to objects does each type of user need?

Hiring Managers

Ben, a hiring manager, should be able to access the recruiting records related to his open positions, but shouldn't have access to other recruiting records (unless they're owned by other hiring managers who report to him). Also, there are certain sensitive fields that he has no need to see, like the social security number field. Let’s consider the permissions Ben needs for each of the key custom objects in the app.

- **Position**—Ben should be able to post new positions, as well as update and view all fields for positions for which he's the hiring manager, but he should only be able to view other managers' positions.
- **Candidate**—Ben should only be able to view those candidates who have applied for a position on which he's the hiring manager. Also, since Ben has no reason to see a candidate's social security number, this field should be restricted from his view.
- **Job Application**— Ben needs to be able to update the status of job applications to specify which candidates should be selected or rejected. However, he should not be able to change the candidate listed on the job application, nor the position to which the candidate is applying, so we'll have to find a way of preventing Ben from updating the lookup fields on job applications.
- **Review**—To make a decision about the candidates who are applying, Ben needs to see the reviews posted by the interviewers, as well as make comments on them if he thinks the interviewer was being too biased in his or her review. Likewise, Ben needs to be able to create reviews so that he can remember his own impressions of the candidates he interviews.

Recruiters

Mario, a recruiter, needs to be able to create, view, and modify any position, candidate, job application, or review that's in the system. He also needs to view and modify the recruiting records that all of the other recruiters own, since all the recruiters work together to fill each position, regardless of who created it.

We need to make sure a recruiter will never accidentally delete a record with information about a candidate. That’s because state and federal laws require recruitment-related records be saved for a number of years, so that if a hiring decision is questioned, it can be defended in court.

Interviewers

Melissa is an engineer who interviews candidates for highly technical positions. She should be able to view only the candidates and job applications to which she's assigned as an interviewer. Also, she shouldn't be able to view the minimum and maximum salary values for any of the positions or the social security number of any candidate, as that’s sensitive information that has nothing to do with her job.

Standard Employees

Employees, such as Harry, are often the best resources for recruiting new hires, even if they are not active hiring managers or interviewers. For this reason, we need to make sure that employees can view open positions, but that they can't see the values for the positions' minimum and maximum salary fields—otherwise they might tip off friends to negotiate for a position's maximum salary value! Harry also shouldn't be able to view any other records in the Recruiting app.

Here are the required permissions for each of the four types of users.

Custom Object	Recruiter	Hiring Manager	Interviewer	Standard Employee

Custom Object	Recruiter	Hiring Manager	Interviewer	Standard Employee
Position	Read Create Edit	Read Create Edit*	Read (No min/max pay)	Read (No min/max pay)
Candidate	Read Create Edit	Read* (No SSN)	Read * (No SSN)	
Job Application	Read Create Edit	Read Edit (No lookup fields)	Read *	
Review	Read Create Edit	Read Create Edit	Read ** Create Edit **	

* Only for those records that are associated with a position to which the hiring manager or interviewer has been assigned.

** Only for those records that the interviewer owns.

In the rest of this module, you'll learn how you can use the platform to implement these rules in the Recruiting app. As you’ll see, this will require configuring security controls at all three levels: objects, fields, and records.

Use Profiles to Restrict Access

Each user has a single profile that controls which data and features that user has access to. A profile is a collection of settings and permissions. Profile settings determine which data the user can see, and permissions determine what the user can do with that data.

- The settings in a user’s profile determine whether she can see a particular app, tab, field, or record type.
- The permissions in a user’s profile determine whether she can create or edit records of a given type, run reports, and customize the app.

Profiles usually match up with a user's job function (for example, system administrator, recruiter, or hiring manager), but you can have profiles for anything that makes sense for your Salesforce org. A profile can be assigned to many users, but a user can have only one profile at a time.

Standard Profiles

The platform includes a set of standard profiles. Some examples are:

- Read Only
- Standard User
- Marketing User
- Contract Manager
- System Administrator

Each standard profile includes a default set of permissions for all standard objects available on the platform. For example, a Standard User can create and edit records while a Read Only user can view records, but not create or edit them. The System Administrator profile has the widest access to data and the greatest ability to configure and customize Salesforce. The System Administrator profile also includes two special permissions:

- View All Data
- Modify All Data

These permissions override all other sharing settings, so use caution when assigning them to any profile other than System Administrator. You can view a list of all standard and custom profiles in Setup.

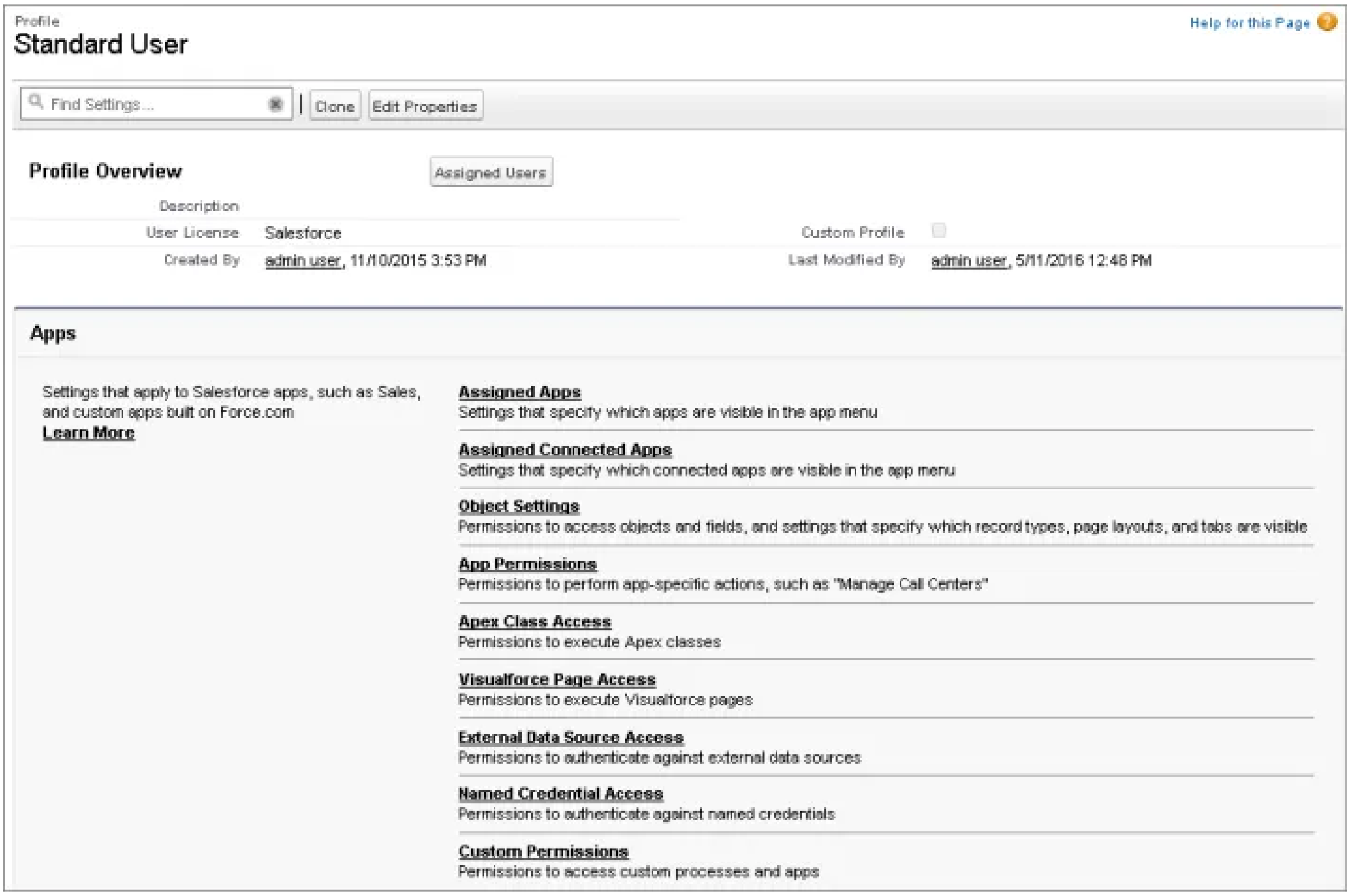
You can't edit the object permissions on a standard profile. However, you can clone any existing profile, and use that as the basis for a new profile, adjusting the apps and system settings as needed. For example, in the Recruiting app, you might create three new profiles, one each for recruiters, interviewers, and hiring managers. Each profile can then be configured to provide the specific type of data access required for a particular role. You can then use permission sets to grant additional permissions, as required.

Note

The profiles functionality in an org depends on the user license type.

Managing Profiles

The profile overview page provides an entry point for all of the settings and permissions for a single profile. In Setup, use the Quick Find box to find **Profiles** and click the profile you want to view.



Profile

Standard User

Profile Overview

Description

User License: Salesforce

Custom Profile: □

Created By: admin user, 11/10/2015 3:53 PM

Last Modified By: admin user, 5/11/2016 12:48 PM

Apps

Settings that apply to Salesforce apps, such as Sales, and custom apps built on Force.com
Learn More

Assigned Apps
Settings that specify which apps are visible in the app menu

Assigned Connected Apps
Settings that specify which connected apps are visible in the app menu

Object Settings
Permissions to access objects and fields, and settings that specify which record types, page layouts, and tabs are visible

App Permissions
Permissions to perform app-specific actions, such as "Manage Call Centers"

Apex Class Access
Permissions to execute Apex classes

Visualforce Page Access
Permissions to execute Visualforce pages

External Data Source Access
Permissions to authenticate against external data sources

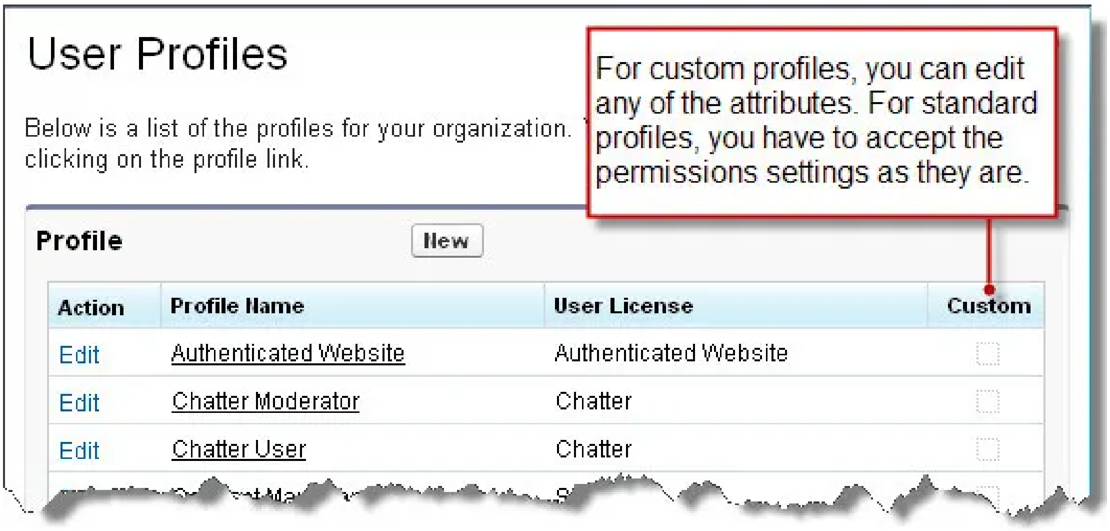
Named Credential Access
Permissions to authenticate against named credentials

Custom Permissions
Permissions to access custom processes and apps

Create a Profile

The easiest way to create a profile is to clone an existing profile that’s similar to the one you want to create, and then modify it.

Salesforce has an enhanced profile user interface that makes it easy to find and modify profile settings. That’s what we’ll use for this exercise. To do that, find `User Management Settings` in the **Quick Find** box in Setup, then enable **Enhanced Profile User Interface** and click **Save**.



User Profiles

Below is a list of the profiles for your organization.
clicking on the profile link.

For custom profiles, you can edit any of the attributes. For standard profiles, you have to accept the permissions settings as they are.

Action	Profile Name	User License	Custom
Edit	Authenticated Website	Authenticated Website	☐
Edit	Chatter Moderator	Chatter	☐
Edit	Chatter User	Chatter	☐

1. In Setup, use the Quick Find box to find **Profiles**.
2. Click **Clone** next to a profile similar to the one you want to create.
3. Give your new profile a name, and save.

Assign a Profile

Once you've created a profile, you'll want to customize it to match the needs of a set of users, and then assign the profile to those users.

1. Find `Profiles` in Setup.
2. Select a profile and then click **Object Settings**. Click **Edit** to see its settings.
3. Set the most restrictive settings and permissions you can for this user type, and save. (Don’t worry about blocking the user from doing things they need to do. We'll open up more possibilities for them later, when we give them permission sets.)
4. Find `Users` in Setup and click **Edit** next to one of them.
5. From the **Profile** dropdown select the profile you just set up, and save.

Use Permission Sets to Grant Access

A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.

Permission sets make it easy to grant access to the various apps and custom objects in your org, and to take away access when it's no longer needed.

Users can have only one profile, but they can have multiple permission sets.

You'll be using permission sets for two general purposes: to grant access to custom objects or apps, and to grant permissions—temporarily or long term—to specific fields.

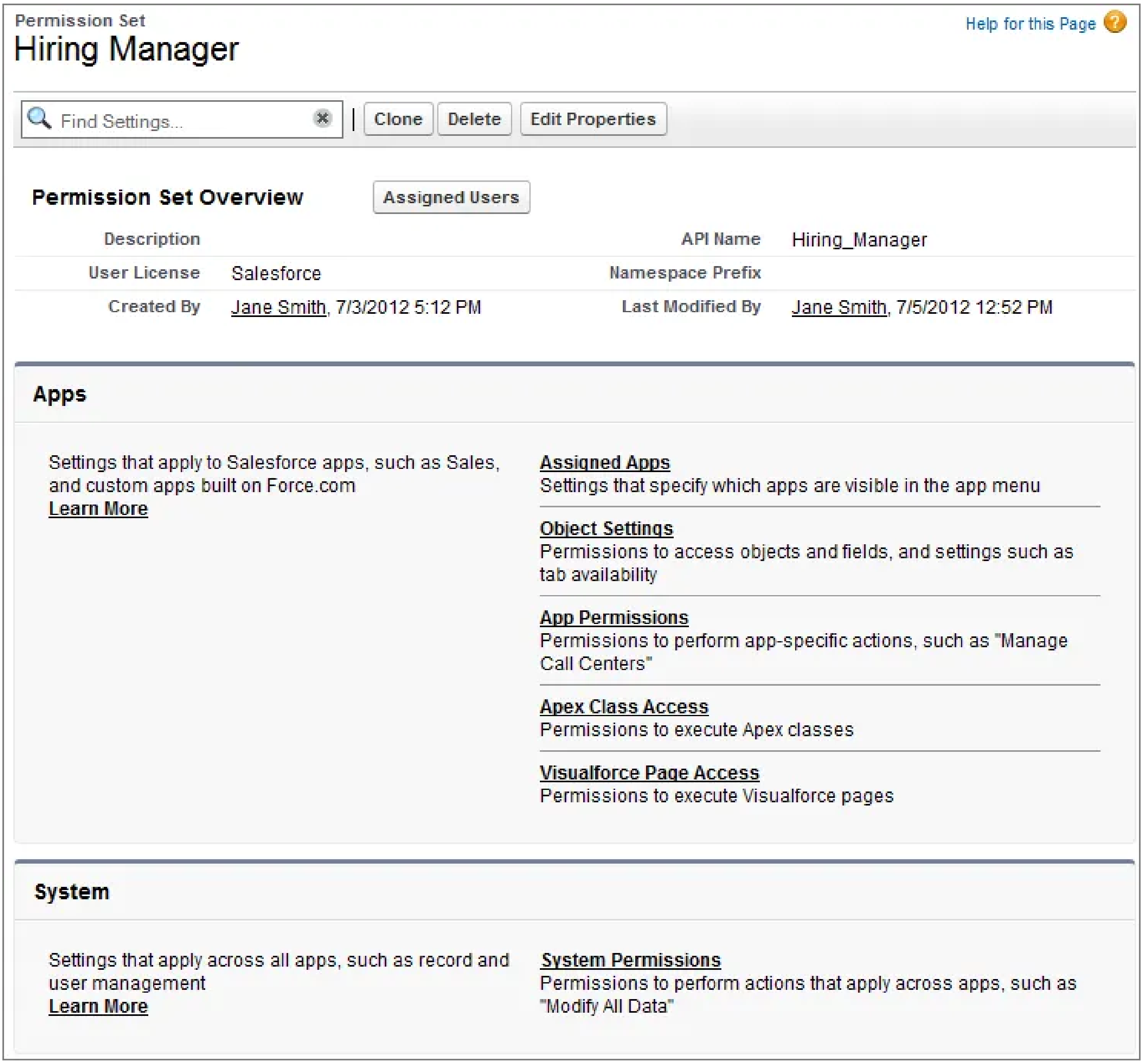
Grant access to custom objects or apps.
Let's say you have many users in your org with the same fundamental job functions. You can assign them all one profile that grants them all the access they need to do their job. But a few of those users are working on a special project and they need access to an app no one else uses. And a few other users need access to that app, as well as another app that the first group doesn't need. If we only had profiles, you'd have to create more profiles customized to those few users' needs, or take your chances and add more access to the original profile, making the apps available to users that don't need them. Neither of these options is ideal, especially if your org is growing and your users' needs change regularly.

Grant permissions to specific fields.
Let's say you have a user, Tom, who needs temporary edit access to a field while his co-worker is on vacation. You can create a permission set that grants access to the field and assign the permission set to Tom. When Tom's co-worker returns from vacation and Tom no longer needs access to the field, you just remove the permission set assignment from Tom's user record.

> **Note**
>
> If a user has a permission in their base profile, you can't remove it by assigning a permission set to that user. A permission can only *add* permissions. To take away a permission, you have to remove it from the user's base profile and from any permission sets the user may have.

Managing Permission Sets

A permission set's overview page is the entry point for all of the permissions in a permission set. To open a permission set overview page, find `Permission Sets` in Setup, then select the permission set you want to view. In each permission set, permissions and settings are organized into app settings, system settings, object permissions, and field permissions.



Permission Set

Hiring Manager

Permission Set Overview

Description

API Name Hiring_Manager

User License Salesforce

Namespace Prefix

Created By Jane Smith, 7/3/2012 5:12 PM

Last Modified By Jane Smith, 7/5/2012 12:52 PM

Apps

Settings that apply to Salesforce apps, such as Sales, and custom apps built on Force.com
Learn More

Assigned Apps
Settings that specify which apps are visible in the app menu

Object Settings
Permissions to access objects and fields, and settings such as tab availability

App Permissions
Permissions to perform app-specific actions, such as "Manage Call Centers"

Apex Class Access
Permissions to execute Apex classes

Visualforce Page Access
Permissions to execute Visualforce pages

System

Settings that apply across all apps, such as record and user management
Learn More

System Permissions
Permissions to perform actions that apply across apps, such as "Modify All Data"

Create a Permission Set

Create a permission set to grant additional permissions to specific users, on top of their existing profile permissions, without having to modify existing profiles, create new profiles, or grant an administrator profile.

1. Use the Quick Find box to find **Permission Sets** in Setup.
2. Click **Clone** next to the set you want to copy.

Note

A cloned permission set has the same user license as the original. To create a set with a different license, click **New** instead.

3. Enter a label and a description.
   The API name is a unique name used by the API and managed packages. It automatically replicates the label, but you can modify it.
4. If this is a new permission set, select a user license option.

   - If you plan to assign this permission set to multiple users with different licenses, select `--None--`.
   - If only users with one type of license will use this permission set, select that user license.

5. Click **Save** to go back to the permission set overview page.
6. In the permission set toolbar, click **Manage Assignments**, then click **Add Assignments**.
7. Select the users to assign to this permission set and click **Assign**.
   Review the messages on the Assignment Summary page. If any users weren't assigned, the Message column tells you why.
8. Click **Done** to return to a list of the users assigned to the permission set.

Profiles and Permission Sets for the Recruiting App

Now that you've seen how to create and modify profiles and permission sets, let's set up the appropriate object-level access for our Recruiting app. The app has four main types of users: recruiters, hiring managers, interviewers, and standard employees.

Here are the key considerations for deciding whether to create a profile or permission set for each type of user.

Recruiters
These represent a clearly defined job function, and they need access to different types of data than other users. Hence, it makes sense to create a profile for recruiters.

Hiring Managers
For most orgs, a hiring manager in Sales will need access to a different type of data than a hiring manager in Engineering. However, all hiring managers still need the same types of access to recruiting data—reviews, candidates, positions, and job applications. Hence, it's convenient to create a hiring manager permission set that can be assigned to various types of users.

Interviewers
An employee from any department and in any job function might be called upon to perform an interview and requires access to recruiting information only for a limited amount of time. It makes sense to define a permission set for interviewers, since permissions can be easily assigned and revoked as needed.

Standard Employees
This is a generic group that doesn't reflect a particular job function. For most employees, you can create a base profile that provides access to a small set of data, and then depending on what their specialties are, create and assign permission sets to give them more access as needed.

So from what we've seen, the optimal way to configure object permissions for the Recruiting app is like this:

1. Create two profiles: Recruiters and Standard Employees.
2. Create two permission sets: Hiring Managers and Interviewers.
3. Assign the Standard Employee profile to hiring managers and interviewers, and then grant the appropriate permission set for their function.

Resources

- Viewing Profile Lists
- Considerations for Permission Sets
- Security Implementation Guide

Assessment Complete!

+500 points

Data Security
100%
Progress: 100%
Retake this Challenge
View more modules