



UNDERSTANDING USER SHARING

Summary

User Sharing controls access to user records. You can use the “View All Users” permission to grant a user Read access to all user records, regardless of the sharing settings. System administrators and users with the “Manage Users” permission automatically get the “View All Users” permission with User Sharing.

What is User Sharing?



Note: User Sharing is automatically available in new organizations in Winter '14. Existing organizations can contact Salesforce to enable this feature.

User Sharing enables you to show or hide an internal or external user from another user in your organization.

With User Sharing, you can:

- Assign the “View All Users” permission to users who need to see or interact with all users. This permission is automatically enabled for users who have the “Manage Users” permission.
- Set the organization-wide default for user records to Private or Public Read Only.
- Create user sharing rules based on group membership or other criteria, such as username and whether a user is active.
- Create manual shares to grant access to individual users or groups.
- Control the visibility of external users in customer or partner portals and communities.

Understanding User Sharing

Set organization-wide defaults for internal and external user records. Then, extend access using sharing rules based on membership to public groups, roles, or territories, or use manual sharing to share individual user records with other users or groups.

When you enable user sharing, users can see other users in search, list views, and so on only if they have Read access on those users.

Review these considerations before you implement user sharing.

“View All Users” permission

This permission can be assigned to users who need Read access to all users, regardless of the sharing settings. If you already have the “Manage Users” permission, you are automatically granted the “View All Users” permission.

Organization-wide defaults for user records

This setting defaults to Private for external users and Public Read Only for internal users. When the default access is set to Private, users can only read and edit their own user record. Users with subordinates in the role hierarchy maintain read access to the user records of those subordinates.

User sharing rules

General sharing rule considerations apply to user sharing rules. User sharing rules are based on membership to a public group, role, or territory. Each sharing rule shares members of a source group with those of the target group. You must create the appropriate public groups, roles, or territories before creating your sharing rules. Users inherit the same access as users below them in the role hierarchy.

Manual sharing for user records

Manual sharing can grant read or edit access on an individual user, but only if the access is greater than the default access for the target user. Users inherit the same access as users below them in the role hierarchy. Apex managed sharing is not supported.

User sharing for external users

Users with the “Manage External Users” permission have access to external user records for Partner Relationship Management, Customer Service, and Customer Self-Service portal users, regardless of sharing rules or organization-wide default settings for User records. The “Manage External Users” permission does not grant access to guest or Chatter External users.

User Sharing Compatibility

When the organization-wide default for the user object is set to Private, User Sharing does not fully support these features.

- Chatter Messenger is not available for external users. It is available for internal users only when the organization-wide default for the user object is set to Public Read Only.
- Customizable Forecasts—Users with the "View All Forecast" permission can see users to whom they don't have access.
- Salesforce CRM Content—A user who can create libraries can see users they don't have access to when adding library members.
- Standard Report Types—Some reports based on standard report types expose data of users to whom a user doesn't have access. For more information, see Control Standard Report Visibility.

Organization-Wide Defaults for User Records

Tip

Regardless the organization-wide defaults:

- Administrators and users with the “View All Users” permission retain Read access to all user records.
- Internal users have Read/Write access to their own records.
- Users have Read access to user records below them in the role hierarchy.

For user records, you can set the organization-wide sharing default to Private or Public Read Only. The default must be set to Private if there is at least one user who shouldn't see a record.

Let's say that your organization has internal users (employees and sales agents) and external users (customers/portal users) under different sales agents or portal accounts, with these requirements:

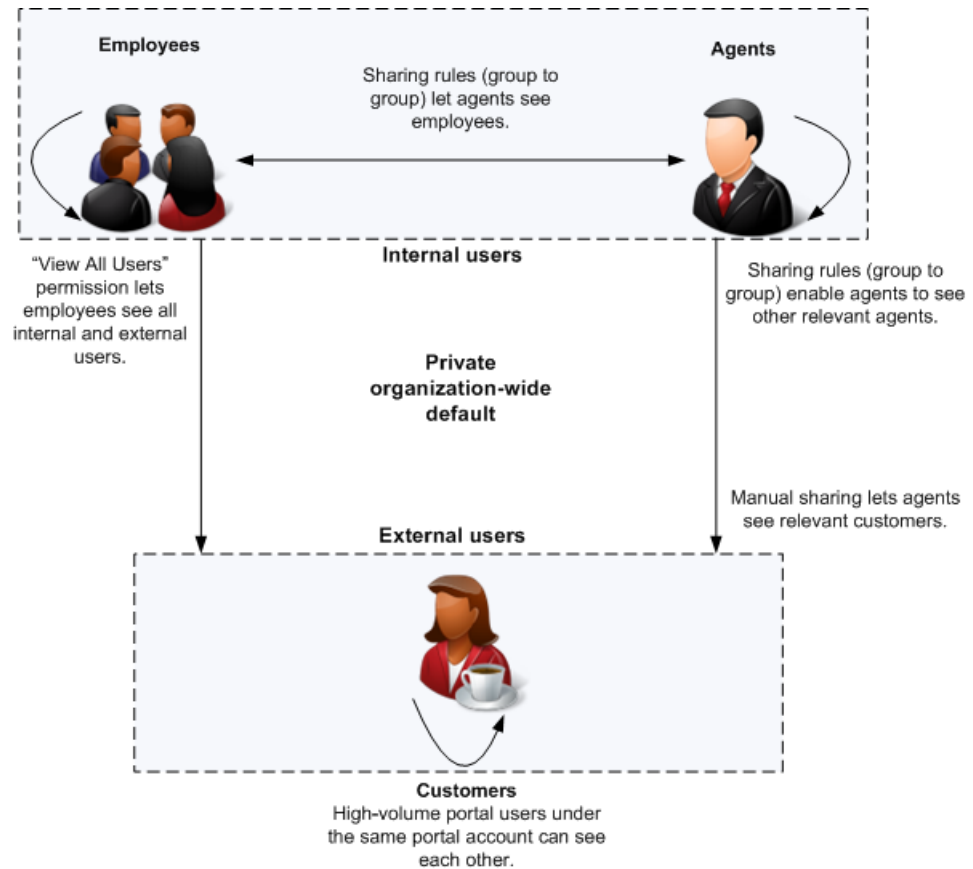
- Employees can see everyone.
- Sales agents can see employees, other agents, and their own customer user records only.
- Customers can see other customers only if they are under the same agent or portal account.

To meet these requirements, set the default external access to Private, and extend access using sharing rules, manual sharing, or user permissions.

This table explains what it means to have Read access on a user record.

Read access to the record?	What can you see?
No	User's name only.
Yes	User's name, profile, and detail page. You can also see the user in lookups, list views, ownership changes, user operations, and search. Internal users with Read/Write access can edit the record, excluding fields such as role, profile, or permissions. Portal users can't edit user records.

This graphic illustrates how the organization-wide defaults work with sharing rules, manual sharing, and the “View All Users” permission.



Setting the Organization-Wide Defaults for User Records

Permissions

You'll need the "Manage Sharing" permissions to set the organization-wide defaults.

When the feature is first turned on, the organization-wide default is Public Read Only for internal users and Private for external users.

To set the organization-wide defaults:

1. From Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select the default internal and external access you want to use for user records.
The default external access must be more restrictive or equal to the default internal access.
4. Click **Save**.

Users have Read access to those below them in the role hierarchy and full access on their own user record.

Controlling Who Community or Portal Users Can See

If your organization has enabled a community and has portal licenses provisioned for it, User Sharing is enabled automatically. When User Sharing is on, you can choose which other users community users can see by default. If your organization has Customer or Partner Portals, you can choose a default for them as well. Users who can see one another can interact on all the communities or portals in your organization. For example, if you would like to have a more private community, you can deselect the **Community User Visibility** checkbox and use other sharing features like sharing rules, manual shares, or portal access.

For Communities and Portals, you can choose different defaults.

Communities

The initial default is to allow community users to be seen by all other internal and external users in communities they are a member of. You can change the default to allow external users in communities to be seen only by themselves and their superiors in the role hierarchy. The setting provides Read access only and applies to all communities in your organization.

Visibility to users as a result of the **Community User Visibility** preference is not inherited through the role hierarchy. If a manager in the role hierarchy is not a member of a community, but their subordinate is, the manager does not gain access to other members of the community.

Portals

The initial default is to allow portal users to be seen by other portal users within the same account. You can change the default to allow external users in portals to be seen by only themselves and their superiors in the role hierarchy. The setting provides Read access only and applies to all of the portals in your organization.



Note: Partner portal users also have access to their channel manager.

1. From Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Deselect the **Portal User Visibility** checkbox to allow users to be seen by only themselves and their superiors. Or select the checkbox to let portal users be seen by all other portal users within the same account.
4. For **Community User Visibility**, deselect the checkbox to allow users to be seen only by themselves and their superiors. Select the checkbox to allow community users to be seen by all other users in their communities.



Note: This option only appears if Salesforce Communities is enabled.

5. Click **Save**.

Selecting either of these options is a quick way of overriding an organization-wide default setting of Private for external access to the User object for Community or Portal users.

Once you have set these defaults, you can selectively expand access to users.

When do I need to use user sharing rules or manual shares?

Tip

Users inherit the same level of access as users below them in the role hierarchy.

You can't grant a more restrictive access than your organization-wide defaults. If a user gains access to a record by more than one way (for example, organization-wide defaults and sharing rules), the higher level of access is maintained.

User sharing rules grant additional access beyond the organization-wide defaults, based on group membership (role, groups, or territories) or other criteria. User sharing rules based on membership enable user records belonging to members of one group to be shared to members of another group.

Manual sharing grants additional access to user records, but on an individual basis. For example, you can use manual sharing in these examples:

- You want to share your user record on a one-time basis.
- You want to extend access to your user record to an individual user below you in the role hierarchy.
- You're extending access to external users such as high-volume portal or guest users so that internal users may see them.



Note: You can extend access to High-volume portal users and guest users using manual shares, but not sharing rules, since they don't have roles. High-volume portal users can be shared with internal users via manual sharing, but not the other way around. Guest users can be shared with internal users via manual sharing, and vice versa.

Creating User Sharing Rules

Permissions

You'll need the "Manage Sharing" permission to create sharing rules.

User sharing rules can be based on membership to public groups, roles, or territories, or on other criteria such as Department and Title. By default, you can define up to 300 user sharing rules, including up to 50 criteria-based sharing rules.

To create user sharing rules:

1. From Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings**.
2. In the User Sharing Rules related list, click **New**.
3. Enter the **Label Name** and click the **Rule Name** field to auto-populate it.
4. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
5. Select a rule type.
6. Depending on the rule type you selected, do the following:
 - a. **Based on group membership**—Users who are members of a group can be shared with members of another group. In the *Users who are members of* line, select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 groups, roles, or territories).
 - b. **Based on criteria**—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
7. In the *Share with* line, specify the group that should have access to the user records. Select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.

8. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records. They can see target users in list views, lookups, search, and interact with them on Chatter.
Read/Write	Users can view and update records.

9. Click **Save**.

Creating Manual Shares for User Records

Permissions

You can share your own record to another user for whom you have Read access, or you can share any record if you have the "Manage Users" permission.

To grant access to a user record:

1. From Setup, enter *Users* in the **Quick Find** box, then select **Users**. Click the name of the user you want to share.
2. On the User Detail page, click **Sharing**.
3. Click **Add**.
4. From the drop-down list, select the group, user, role, or territory to share with.
5. Choose which users have access by adding them to the Share With list.
6. Select the access level for the record you are sharing.
Possible values are Read/Write or Read Only, depending on your organization-wide defaults for users. You can only grant a higher access level than your organization-wide default.
7. Click **Save**.
8. To change record access, on the user's Sharing Detail page, click **Edit** or **Del**.

Restoring User Visibility Defaults

User Sharing enables you to control who sees who in the organization. You can restore your defaults if you have previously used User Sharing.

To restore user visibility defaults:

1. From Setup, enter *Sharing Settings* in the **Quick Find** box, then select **Sharing Settings**.
2. Set the organization-wide defaults to Public Read Only for internal access and Private for external access.
3. Enable portal account user access.
On the Sharings Settings page, select the **Portal User Visibility** checkbox. This option enables customer portal users to see other users under the same portal account. Additionally, partner portal users can see the portal account owner.
4. Enable network member access.

On the Sharing Settings page, select the **Community User Visibility** checkbox. This option enables community members to be seen by all other users in their communities.

5. Remove user sharing rules.

On the Sharing Settings page, click **Del** next to all available user sharing rules.

6. Remove HVPU access to user records.

On the Customer Portal Setup page, click **Del** next to all available sharing sets for HVPU.

After user visibility is restored to the defaults, all internal users are visible to each other, portal users under the same portal account are visible to each other, and community members in the same community are visible to each other.