About Realms

Maybe you share your QuickBase applications with your clients, but wish you could send them to a URL that included your company name and displayed your own branding on every page. Or perhaps security concerns are more important to you and you'd like to implement stricter sign-in and access controls across all your QuickBase applications.

QuickBase has introduced a new offering to address these needs. You can now group accounts together within a **Realm**.

What is a Realm?

If you've been using QuickBase, you're used to signing into www.quickbase.com to access your account and the applications that live within it. A realm is kind of like your own version of www.quickbase.com. You create your own domain—literally—when you send users to your custom URL (details follow below). Multiple QuickBase billing accounts (if you have more than one) and any applications related to these accounts, live within your realm. This setup provides you with centralized control over all these applications and their users. Special features and rewards that come with implementation of a realm follow below.

Frequently Asked Question
After I create my realm and start working in it, can I access an application on www.quickbase.com?
Yes, you can access applications in multiple realms, using the same user account and/or screen name. The only catch is that you may need to sign in with a different password in each realm, as the password requirements could easily differ in each. (Read more about passwords on page 2.)

Custom User Experience

Realms offer some great features that can extend your QuickBase experience:

Custom URL

You love QuickBase, but maybe you wish your application could live on your own Web site, under your own domain name instead of on quickbase.com. Through a realm, you can create your own custom URL to host all your applications. This URL can start with your company name, or whatever text you wish. For example, you could send users to: myfabulouscompany.quickbase.com or companyproject.quickbase.com.

Custom Branding

If you use QuickBase to interact with customers, you were probably glad to read that you could direct clients to a URL containing your company name. What could be better? How about making the pages under that URL look more like your own Web site with your own branding? With realms, you can enhance your QuickBase application by displaying your own logo and corporate colors in the header and footer of each page.

Enhanced Security

Say you'd like tighter control over who's accessing applications within your accounts. For example, maybe you'd like to ensure that no one outside your firm ever has access to one of your applications.

Realms give you added control over who can access your QuickBase applications. As you'll read, you can tie QuickBase account logins to your corporate login and enforce passcode policies that match your corporate policies. You can also limit access to applications based on a new feature specific to Realms, which is Realm User Status.

Implement Custom Passcode Policies

A lot of network administrators have high standards when it comes to password security. If you have a special password format that you require members of your organization to use, you'd probably like to carry those requirements over to your firm's QuickBase applications. No problem. Realms enable you to set your own specific password policies across all your QuickBase accounts and applications. You can:

- Set password length
- Require that users use both upper and lower case letters.
- Require a combination of alphabetic and numeric characters
- Force users to change passwords regularly by setting a password expiration period. You can require a change every 60, 90, 120, or 360 days.

Controlling User Sessions

Do you ever worry about the user who never closes the browser accessing one of your QuickBase applications and then leaves his workstation unattended for hours at a time? Clamp down on this practice by implementing a **Session Timeout**. When you do so, QuickBase automatically closes out after the time limit you specify passes. This session timeout is not tied to inactivity. Instead, it's meant to prohibit users from remaining signed in for exceptionally long periods—like more than a day, for instance.

In addition, you can tell QuickBase whether or not you want the program to let users access your realm without having to sign in each time. If you "Allow a user to stay signed in across sessions" then any user can turn on a checkbox labeled **Keep me signed in on this computer unless I sign out** (located on the sign-in page). When a user turns this option on, they don't need to enter their user name and password to gain entry to your realm (unless they actively sign out). This can compromise your security in a number of ways. For instance, an unauthorized person might gain access to their computer.

Realms provide the ability to remove this option altogether, thereby forcing everyone to sign in with a valid user name and password each time they access your realm.

Limit Application Access

Realms provide you with additional gate-keeping features to help track and control access to your applications. A major tool in this arsenal is **Realm Approval Status**. You assign each user an approval status to help you track and control who can see what.

Realm Approval Status

Within your realm, you'll give one of three approval status levels to a user:

- **Approved.** "Approved" users are individuals to whom you have manually granted "approved" status within your realm. Or, if you prefer to automate this process, they are users who match an entry in your central network user directory. (Read more about the latter option within the **LDAP** section on page 5.)
  NOTE: Just because a user has approved status, doesn't mean that they can access any application. It only means that they can sign into the Realm. Application Managers still have the power to share applications with only chosen users. However, within a realm, you can specify that a specific application be accessible only to "approved" users. This is an easy way to do something like ensure that only your employees can access certain information.
- **Denied**. Use this status setting to prohibit a user from logging into your realm. For instance, if an individual leaves your company, change his or her status to Denied to terminate access to any of your accounts. (Read more about denying access in the next section.)
- **Guest.** QuickBase automatically designates any user who is not "approved" the status of "guest." This status lets QuickBase know not to let that user access any application that is for "approved" users only. The program does let "guests" access any other applications, as long as the managers of those applications have furnished the "guest" an invitation to do so.

Note: Don't confuse *Realm Approval Status* with *user roles* in an application. Users with **Approved** and **Guest** status are free to use any application according to limits of their role within that application. (Users with **Denied** status, can't access any application in any of your realm's accounts, of course.)

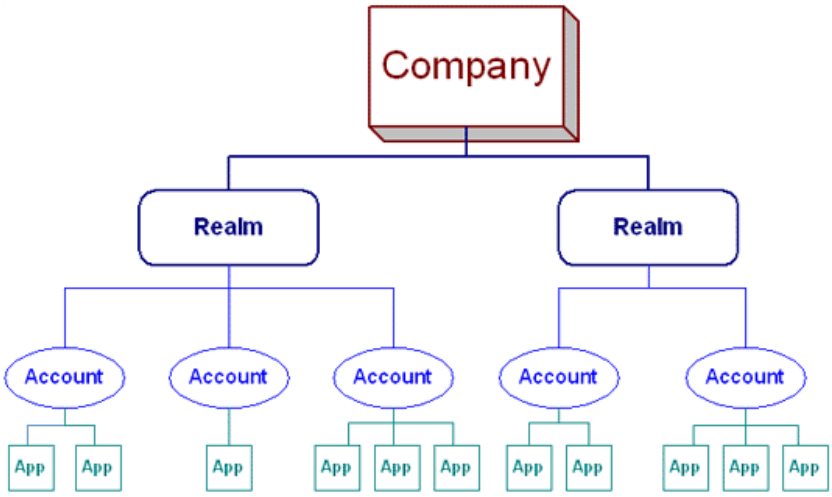
Centralized User Management

Manage all your QuickBase accounts, applications and users from one central location.

Realm Directory Structure

The new account structure that Realms provide let you group multiple accounts under one corporate umbrella for the first time. Though, you're not limited to only one realm, of course.

Here's how it works: One company can have multiple realms. Each realm can contain multiple accounts. Each account can contain multiple applications (as pictured below).



What this means is that a Realm Administrator can control users across many different applications and accounts. This is especially useful for reasons you're about to read about.

See Who's Using What

QuickBase for Corporations edition offers instant visibility into account usage. You can:

- **Track account usage by Division/Team.** Do you need to split out the cost of QuickBase? This feature lets you see exactly what percentage of your monthly cost to charge back to individual departments.
- **Monitor user activity.** See who is accessing what applications. Get stats on who shared their application with a particular user and when the user's accessed any application.
- **Keep application user lists up-to-date.** Do you have a user who hasn't accessed any applications in months? If so, it's probably time to remove her from the account. But you don't need to track this information manually. You can set up alerts to tell you if a user's visits fall below the norm for a particular application. Since no two applications are alike, you can customize this setting for each one. After all, some applications may require a visit every day, while others are accessed only every month or two.
- **See which applications are open to *Everyone on the Internet*.** If you've granted application managers the right to share applications with the public, you can use this feature to keep an eye on them.
- **See which applications are accessed by users outside your company.** Get a list of users outside your company (sorted by e-mail domain, if you want) and see what applications they can access.
- **See which application managers generate the most users or applications.** Maybe you have one application manager who's using up more than his share of the user budget. It's easy to see who's invited the most users into the account and who's created the most applications.

- **List applications by size.** Are some applications getting too big? View a list of extra-large applications, so you can contact their managers about size limits.

Denying User Access

Having one command center for all your QuickBase applications can cut down on confusion and increase security. For example, imagine that an employee, Penelope, resigns from your sales department. Penelope's boss removes her from the Sales QuickBase account and application. However, no one in sales knows that Penelope was also a user of the QuickBase account created by your Research and Development department, where no one's heard of Penelope's departure. The result? She still has access to confidential company information. Now, through Realms, you can circumvent communication problems like this by controlling Penelope's access at the very highest level. Deny a user access to an entire realm and all your accounts are secured at once.

Frequently Asked Question

An employee has left my company. I understand that if I add him to the Deny list, he won't be able to access my realm but can he use the same login on www.quickbase.com?

If your ex-employee has already set up a user account on the General QuickBase site (www.quickbase.com) using his office e-mail address, he'll still be able to access applications there. If you own his e-mail address (in other words, it belongs to your company's domain), you can deactivate his user account. When you do so, he can't use that e-mail address to log into any QuickBase realm, including the general QuickBase site, www.quickbase.com.

Use LDAP

When you're working on a large network and signing into a variety of software tools, you often must enter a different login and password each time. Typing in all those combinations taxes your memory and your fingertips. Wouldn't it be nice to have to remember only one user name and password? Many organizations have implemented just such a solution, called LDAP (Lightweight Directory Access Protocol), to let users access multiple secure directories using only their network login. Realms are compatible with LDAP, saving your users the need to remember separate user names and passwords.

An added advantage to using LDAP authentication is that you can give any user who squares with your LDAP directory "approved" status in your realm (refer back to page 3). This is a handy way to automate application access restrictions.