

Don't Let Your Employees Take Vacation

Keeping your business going when your employees take their login passwords on vacation with them

True story: Bonnie went on vacation for a few days. We thought we had everything covered when she was gone. But about half-way through the week we needed to do a wire from one of our “minor” bank accounts. But no one knew the password for the account – so we called Bonnie on her cell...no answer. And there was no answer for the entire day. We lost the whole day trying to track down Bonnie and in the meantime figure out who to call at the bank to let us into the account.

This was a text-book case of loss of business continuity. Our normal course of “getting things done” was interrupted by lack of information – not to mention the lost time doing other productive things while figuring out how the problem.

The Problem

More and more of our business processes and assets are moving outside of our buildings into “Cloud.” While the Cloud provides wonderful benefits, it also sparks brand new problems that we all have to deal with. In this case, it boils down to:

1. How do I gain access to our Cloud-based resources when the person primarily responsible is on vacation?
2. In general, how do I ensure that my business keeps running efficiently when I lose any one of my employees for any length of time?

This “business continuity” problem has been around since we’ve had computers. But the rise of the Cloud has complicated the problem due to the many different services that we use in the Cloud, each with their own login, user names, passwords, and administrative control mechanisms.

The Solution

IronStratus solves this problem in the following ways:

1. IronStratus serves as a place where the login information for all of your Cloud applications is stored. In other words, no sticky notes, no spreadsheets, no special secret schemes, and no browser password storage that locks a particular application to a particular computer.
2. IronStratus allows sharing and control of the login information for your Cloud applications. You can easily assign a secondary person to manage each individual application – but you don’t have to give them the passwords, so you can easily turn OFF secondary access when you want.

3. When a new employee is assigned, IronStratus can be used to easily transition all of the access responsibilities to the new person.

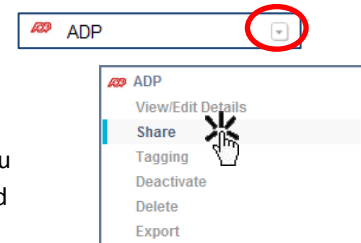
Examples

IronStratus is quite flexible in how it implements these solutions. The following examples show different ways you may use IronStratus based upon your company's needs.

In the following examples, let's suppose that an organization called "XYZ Corporation" has a manager named Eric and a financial controller named Bonnie.

Eric has already set-up IronStratus for XYZ Corp., and has entered all of his employees as users of IronStratus.

So each employee of XYZ has an "XYZ Corp Vault" where they can easily login to corporate applications. The organization uses many online applications include ADP online and portals into numerous corporate bank accounts and services.



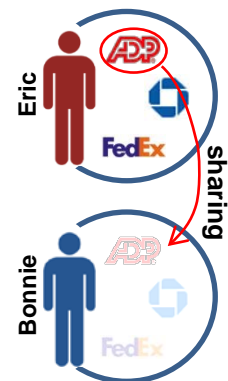
In these examples, we will be using "sharing" of login items in the users' vaults. You designate sharing by clicking on the selection arrow to the right of a Vault Item and choosing "Share."

Example 1 – Tight Control

In this scenario, Eric decides to tightly control all login information that pertains to the business and to delegate or share those logins with those who need to use them – like Bonnie.

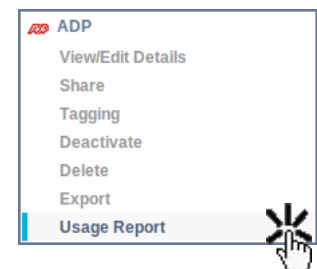
To effect tight control of these corporate resources, Eric does the following using IronStratus:

1. Create login items in IronStratus in his Vault within the organization (XYZ Corp) for each of the corporate applications that he wants to control. For this example, we'll assume they are ADP, FedEx, and a Chase bank account. He enters the corporate username (probably his e-mail) and password for each web site.
2. Then he shares those items with Bonnie, specifying that Bonnie can NOT see the passwords to the login items. Bonnie can log in just fine using the IronStratus Vault, but she can't see the passwords, and can therefore only log in through IronStratus.
3. Eric could share the login items with other people as a backup to Bonnie.



We consider this tight control because Bonnie has no knowledge of the passwords used to access the web sites; she can only login through IronStratus. The benefits of this approach are:

- **Continuity** – Eric always has access to the web-based resources that Bonnie uses, even when she is on vacation. Further, he can share logins with others, even temporarily, to keep the business moving when needed.
- **Visibility** – All of Bonnie's web-based resources are visible in IronStratus. So there is nothing hidden or forgotten.



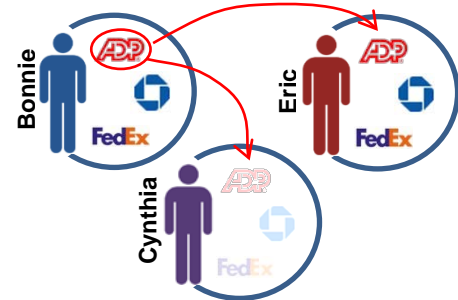
- **Control** – if Bonnie’s IronStratus access is disabled, she can no longer access the web sites, and since she hasn’t seen the passwords, she can’t login without IronStratus.
- **Monitoring** – Eric can generate reports from IronStratus detailing Bonnie’s login activity to the web sites.

Example 2 – Relaxed Control

Suppose, instead, that XYZ Corp. has a more relaxed control requirement. In this case, Eric doesn’t really need to be involved unless Bonnie is unable to do what she needs to do. Essentially, management and control is pushed down to Bonnie.

In this example, Bonnie establishes the logins for the corporate web applications in IronStratus. Then she shares those applications with her “back-up” when she is on vacation. The passwords are NOT shown to her back-up (in this case Cynthia) so that when Bonnie returns, she can turn off the sharing and Cynthia can no longer access those web resources.

In addition, Bonnie could share her web-based resources to Eric so he could be a back-up to Bonnie and Cynthia. You can imagine that Bonnie elects to allow Eric to see the login passwords for the corporate web sites.



All of the benefits of the Tight Control model apply to the more Relaxed model, with these differences:

- Bonnie can see her passwords, so it is possible that she can login to the web-based resources without using IronStratus. This limits the reporting capability and ability to turn-off Bonnie’s access when she leaves the Company.
- Bonnie is in control of the process making it easy for her to plan for vacation without bothering Eric, sharing access to her web-based resources in a secure way. The person to whom she shared access doesn’t learn the passwords.
- While Bonnie manages the process, including ensuring that she has a back-up, Eric can be the fail-safe backup.
- Eric can still monitor the use of the web sites, even if Cynthia is using them.

Most installations of IronStratus implement a security model that is a combination of both the tight and relaxed models, but some use mechanisms in between the two as well.

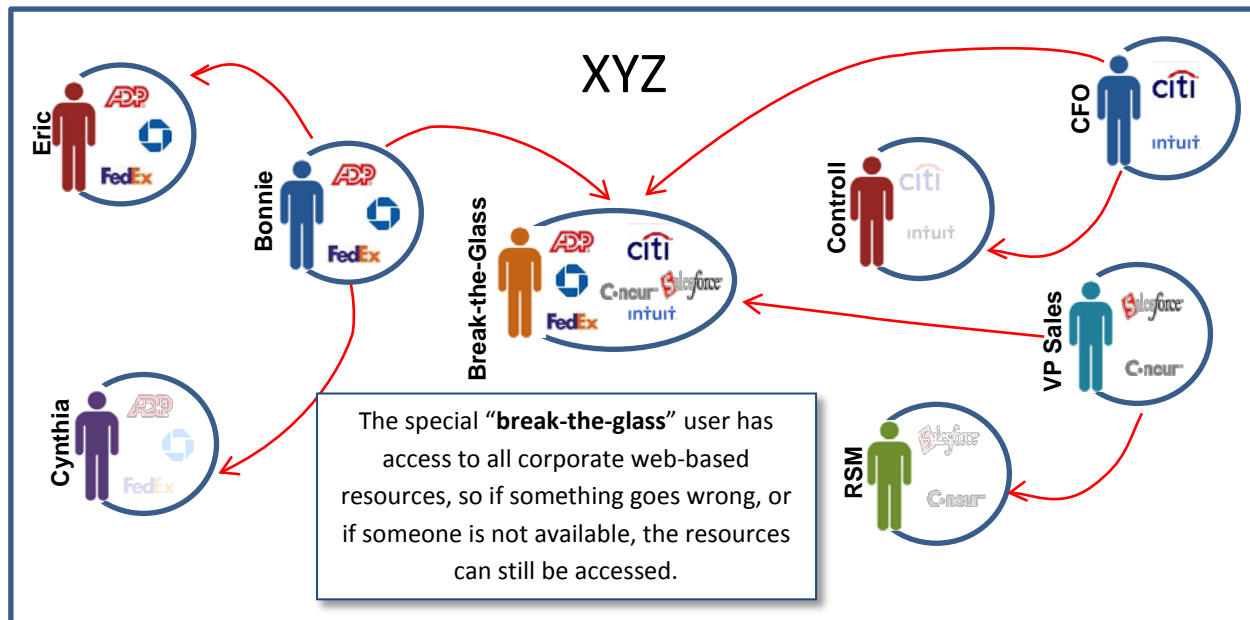
For example, suppose you were to create a special “break the glass” IronStratus user. The idea here is that this special fictional user has a login password that is known only by a select few people. All employees would share corporate application logins for which they have the login information to this user. Then, when a person responsible for a particular web-based resource is unavailable, someone with the Break-the-Glass password can gain access to those resources.

In this example, numerous people are responsible for different web-based resources. They all share the logins with the special account, as well as to others who manage those resources on a day-to-day basis.

Example 3 – Somewhere in Between

There are some very important benefits and details related to this approach:

- The organization is allowed to grow organically without a central (person) point of failure. The only major requirement is that the “break-the-glass” user must be kept up-to-date with corporate resources.
- This example illustrates that resource sharing can be wide and varied – and although it may not be obvious, this sharing is probably happening today in your organization. IronStratus gives you a mechanism for controlling it, and reporting on it.
- As with the other examples, this provides a high level of Control, Visibility, Reporting, and Continuity – but does so in a way that fits your organization, growing and changing with it.



The Wrap up

IronStratus is a very powerful tool for maintaining business Continuity, Visibility, Control, and Monitoring for all of your web-based resources. And this document only covers part of the story.

For more IronStratus use cases, please check-out the IronStratus web site at www.ironstratus.com/what-we-do