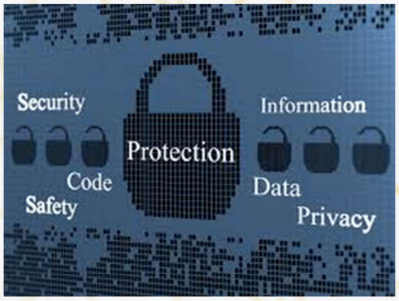
Security Features
Who gets access and why
Peter Keeler
April 18, 2017

Goals

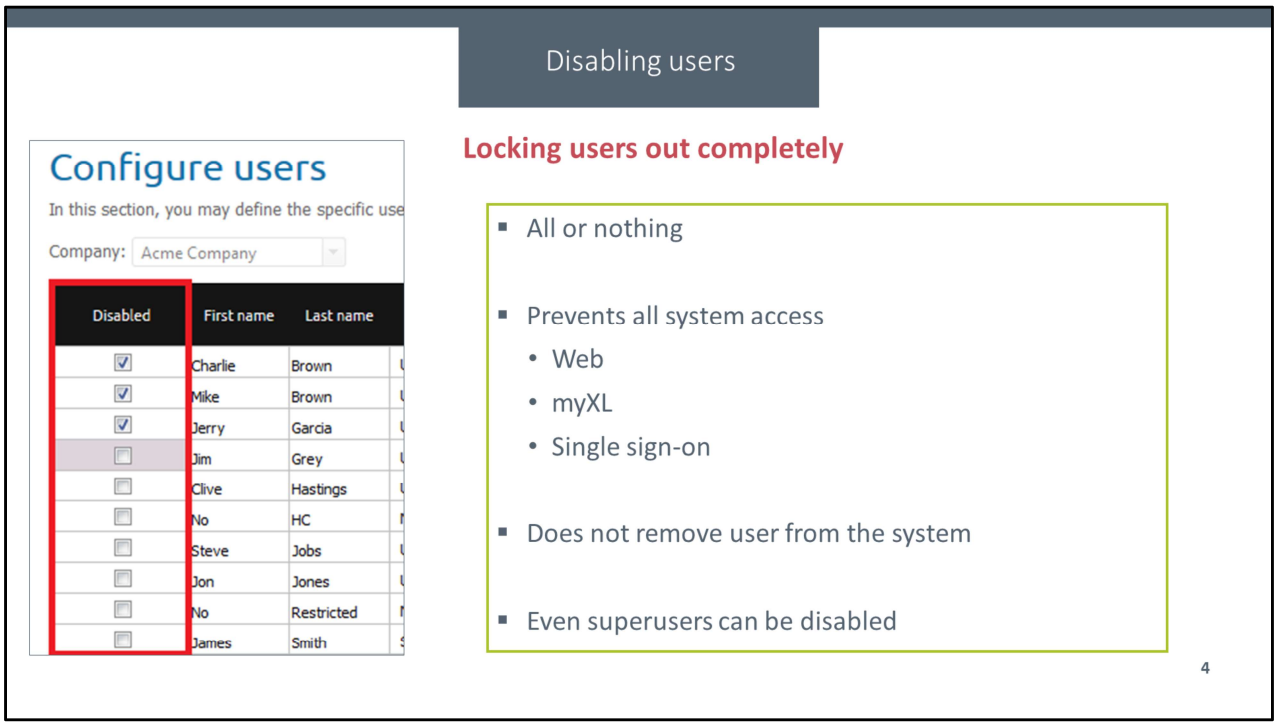
- Know what security features BudgetPak offers
- Understand how to configure the options



Topics

- Disabling users
- What users can *see*
- What users can *do*

3

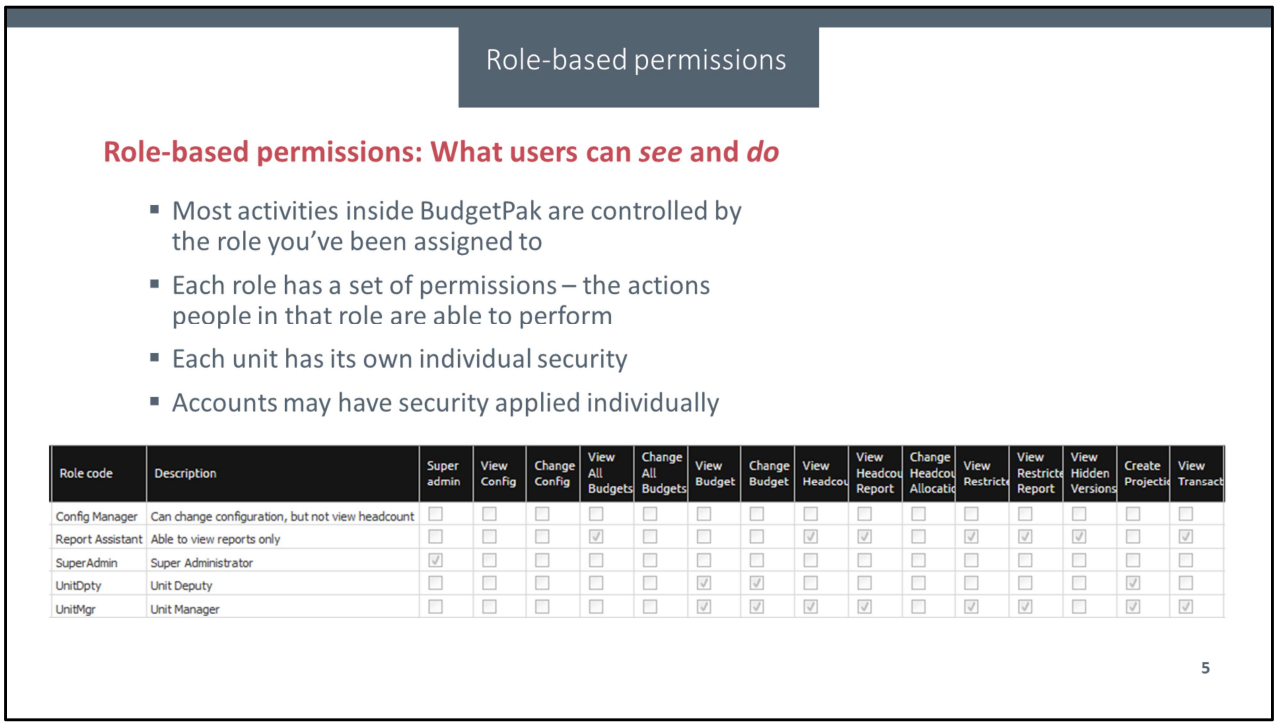


The simplest and most draconian form of security is to not let a user into the system at all. One way you can do that is to simply change their password, but that only takes effect the next time they log in, and doesn't work if they're using single sign-on. Instead, you can use the Configure Users page to mark users as disabled, preventing them from getting into BudgetPak at all. This takes place immediately; if they're in the system when you use it, the next time they try to save, discard, or generally click on just about anything in BudgetPak, they'll be kicked out to the login screen, and will be unable to get back in until they're not disabled anymore. However, they are not deleted, so their name will still show up as a budgetholder or budget assistant, and they do still count as licenses.

Disabling a user takes effect across the entire system – whether they're connecting from the regular login screen, myXL, or using single sign-on, they won't be able to access BudgetPak data. Even having superuser privileges doesn't override being disabled.

If anyone isn't familiar with it, BudgetPak has a single sign-on option available. Single sign-on basically means 'your users are authenticated in your own network, so don't make them sign on separately to BudgetPak.' If you have a system such as Microsoft's Active Directory, where users have a centrally-managed network login, then you can set up a special page on your network to use their existing credentials rather than a separate BudgetPak login.

If you delete a user instead of disabling them, they no longer count against your number of licensed users, but they can no longer be a budgetholder or budget assistant, and at some places in the system, such as on notes or files or in budget histories, they'll show up as 'Deleted user.'



• Much of what defines a user's ability to work in BudgetPak is defined by their role. The most common setup is to have a superuser role, which can do anything in the system, then a budget manager role, which includes the primary people responsible for individual budgets, and then a budget assistant role, which has people who help with or report on a budget, but who ultimately are not the ones responsible for the final budget.
• Roles can have different permissions assigned to them, which break down into two broad categories. The first category is 'access-based permissions' – what you're allowed to see within BudgetPak. We'll be going over those first.
•The other category is 'Function-based permissions' – what you're allowed to do within BudgetPak, within the things that you are allowed to see. We'll cover those later.
• These aren't broken down into separate sections inside the Configure User Roles page in BudgetPak – they're all just 'permissions' there, so you can mix and match them as your needs dictate.

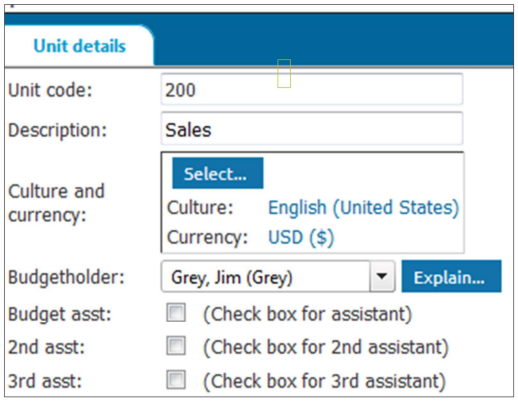
What users can see

Unit security: Budgetholders and assistants

- The budgets any person has responsibility for are defined by the Configure Units page
  - Budgetholders

    Can see this unit and all units below it
  - Budget assistants (up to 3)

    Can see this unit only
- Further controlled by role permissions
  - More on this later



6

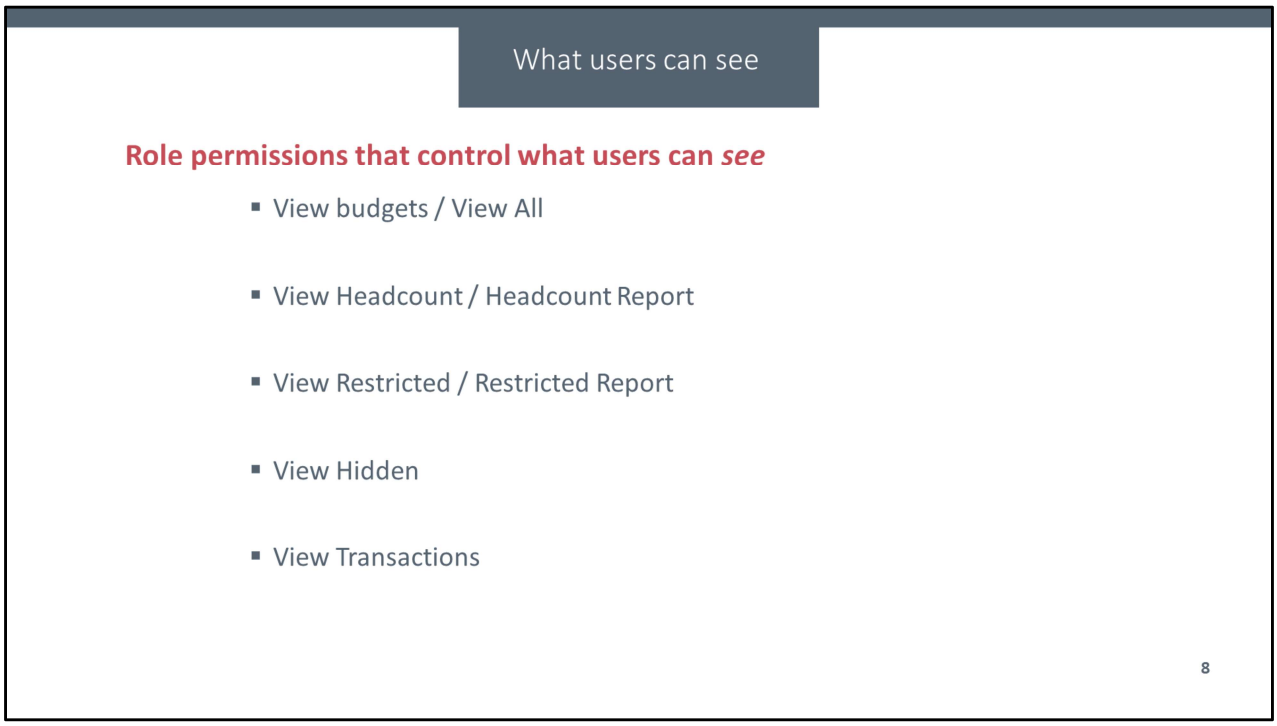
• The most common way to define security in BudgetPak is through assigning budgetholder and budget assistants for units. This is defined on a person-by-person basis; each individual user in your system can be assigned to exactly and only the units where they have some degree of budget responsibility. The budgetholder of a budget is ultimately the person who is responsible for the numbers their budget produces. In a rollup unit, the budgetholder is also allowed to see the units that roll up into that unit, since those numbers also make up the rollup unit's budget. Budget assistants only get access to that specific unit, not the units underneath it.
• Users who are not assigned to a unit, or to a rollup unit above that unit, will not be able to see that unit's budget
• Obviously, if you can't see a unit, then you can't do anything with their numbers. This is useful from both the administrator's perspective and the user's perspective. For the administrator, it means that you have data privacy; users can only see the information that's relevant to them, and can't see anyone else's data. From the user side, this is useful because they don't have to hunt for the items that are their responsibilities; everything they can actually see in the system is relevant to them.

What users can see

Account security: Restricted accounts

- The Configure Accounts page can mark accounts as 'restricted'
- Any section with a restricted account will not appear in the budget navigation map to users who do not have permission to see restricted accounts
- Restricted accounts will not appear in reports without the right permission as well

Account number	Description	Account source	Account class	Enterprise account	Restricted?	Must have user comment?	Instructions
10001	Student Fees	user	Income	3000: Revenue	☐	☐	Student Fees are calculated us
10003	Merchandise Revenue	user	Income	3000: Revenue	☐	☐	Please use your Excel sales rev
10002	Undergraduate Tuition Revenu	calculation	Income	3000: Revenue	☐	☐	Please edit the 'Annual Underg
10004	Graduate Tuition Revenue	calculation	Income	3000: Revenue	☐	☐	Please edit the monthly 'Gradu
1000	Salaries - Faculty	headcount-bas	Expense	1111: Salaries	☑	☐	
1001	Salaries - PT	headcount-bas	Expense	1111: Salaries	☑	☐	
1002	Salaries - FT	headcount-bas	Expense	1111: Salaries	☑	☐	
1003	Stipends	headcount-bas	Expense	1111: Salaries	☑	☐	
1100	Bonus	headcount-bas	Expense	1112: Bonus	☑	☐	
1004	Standard Wages - Hourly	headcount-bas	Expense	1111: Salaries	☐	☐	
1005	Overtime & Holiday Wages - H	headcount-bas	Expense	1111: Salaries	☐	☐	

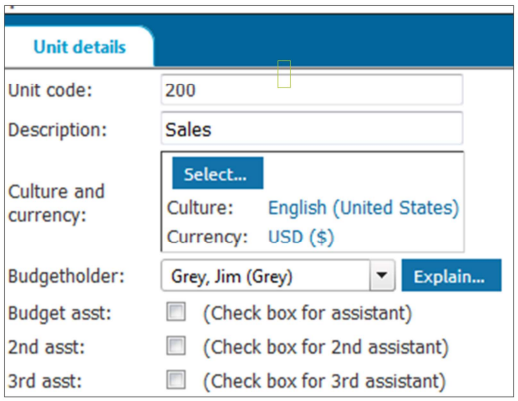


• Much of what defines a user's ability to work in BudgetPak is defined by their role. The most common setup is to have a superuser role, which can do anything in the system, then a budget manager role, which includes the primary people responsible for individual budgets, and then a budget assistant role, which has people who help with or report on a budget, but who ultimately are not the ones responsible for the final budget.
• Roles can have different permissions assigned to them, which break down into two broad categories. The first category is 'access-based permissions' – what you're allowed to see within BudgetPak. We'll be going over those first.
•The other category is 'Function-based permissions' – what you're allowed to do within BudgetPak, within the things that you are allowed to see. We'll cover those later.
• These aren't broken down into separate sections inside the Configure User Roles page in BudgetPak – they're all just 'permissions' there, so you can mix and match them as your needs dictate.

What users can see

View budgets / View all

- Roles affect what users can see and do after being assigned to units
  - *Superadmin* can do everything
  - *View* permission allows viewing budgets for assigned units
  - *View all* permission allows viewing budgets for all units, assigned or not

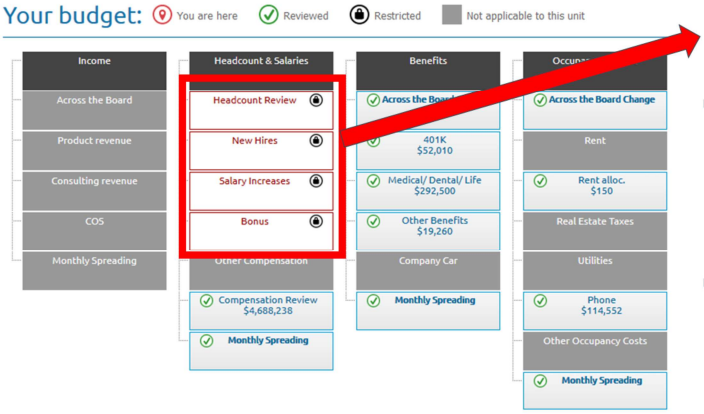


9

• The most common way to define security in BudgetPak is through assigning budgetholder and budget assistants for units. This is defined on a person-by-person basis; each individual user in your system can be assigned to exactly and only the units where they have some degree of budget responsibility. The budgetholder of a budget is ultimately the person who is responsible for the numbers their budget produces. In a rollup unit, the budgetholder is also allowed to see the units that roll up into that unit, since those numbers also make up the rollup unit's budget. Budget assistants only get access to that specific unit, not the units underneath it.
• Users who are not assigned to a unit, or to a rollup unit above that unit, will not be able to see that unit's budget
• Obviously, if you can't see a unit, then you can't do anything with their numbers. This is useful from both the administrator's perspective and the user's perspective. For the administrator, it means that you have data privacy; users can only see the information that's relevant to them, and can't see anyone else's data. From the user side, this is useful because they don't have to hunt for the items that are their responsibilities; everything they can actually see in the system is relevant to them.
• There are some roles that can see all units. I suspect that most of the people at this conference have the 'superadmin' role, which lets them see all units, for example.
• For people who aren't superadmins, you can define what set of units they're allowed to see with the 'View budget' and 'View all budgets' permissions. These are part of the user's role. If you have 'view' permissions, then you're allowed to see the budget for a unit; if you have 'view all' permissions, then you can see the budget for all units. If you don't have one of these permissions, then even if you're assigned as budgetholder, you won't be able to see the budget, which is not normally a desirable situation.

What users can see

Headcount and account restrictions



- Headcount restrictions
  - If a user does not have the 'View headcount' role permission, the headcount-related sections will not be visible or accessible
- Restricted accounts
  - If a user does not have the 'view restricted' role permission, sections containing restricted accounts will not be visible or accessible
- Report-only access
  - Users can be given access to headcount and restricted accounts in reports even if they don't have access within the budgeting process

10

•Individual accounts may be flagged as 'restricted.' Only users whose role has the 'View restricted' permission will be able to see these. Other users will see an indication that they are not able to view all sections, so they know they have an incomplete view of the budget. If you choose the 'Show ALL sections' option on the Budget Navigation map, you'll be able to see sections that contain restricted accounts. Be aware that if you put a restricted account into a section, that entire section becomes restricted and not visible to users who can't view restricted accounts.

• Access to headcount information can be restricted separately from restricted accounts. Users whose role does not include the 'View headcount' permission will not even be able to see the headcount review, raise, bonus, or similar sections. As shown in this example, users who can't see headcount information also can't see headcount sections unless they turn on the 'Show ALL sections' option, and even then they just see that the section exists but is not accessible, just like a restricted account.

• Frequently, headcount-based accounts (particularly salaries and bonuses) will be marked as restricted accounts. If a user is not allowed to see headcount details, but can see the aggregate totals, then they might be allowed to see the account but not the headcount.

• A user's role can also be set so that they're not allowed to view or edit budget information within a unit, but are allowed to see that information in reports. For this reason, the 'View restricted' and 'View headcount' role-based permissions also include separate options for 'View restricted reports' and 'View headcount reports'. A use case for this would be if you have a user who explicitly does not have authority to make headcount decisions, but does need to be able to see those decisions.

What users can see

Hiding versions from budgetholders

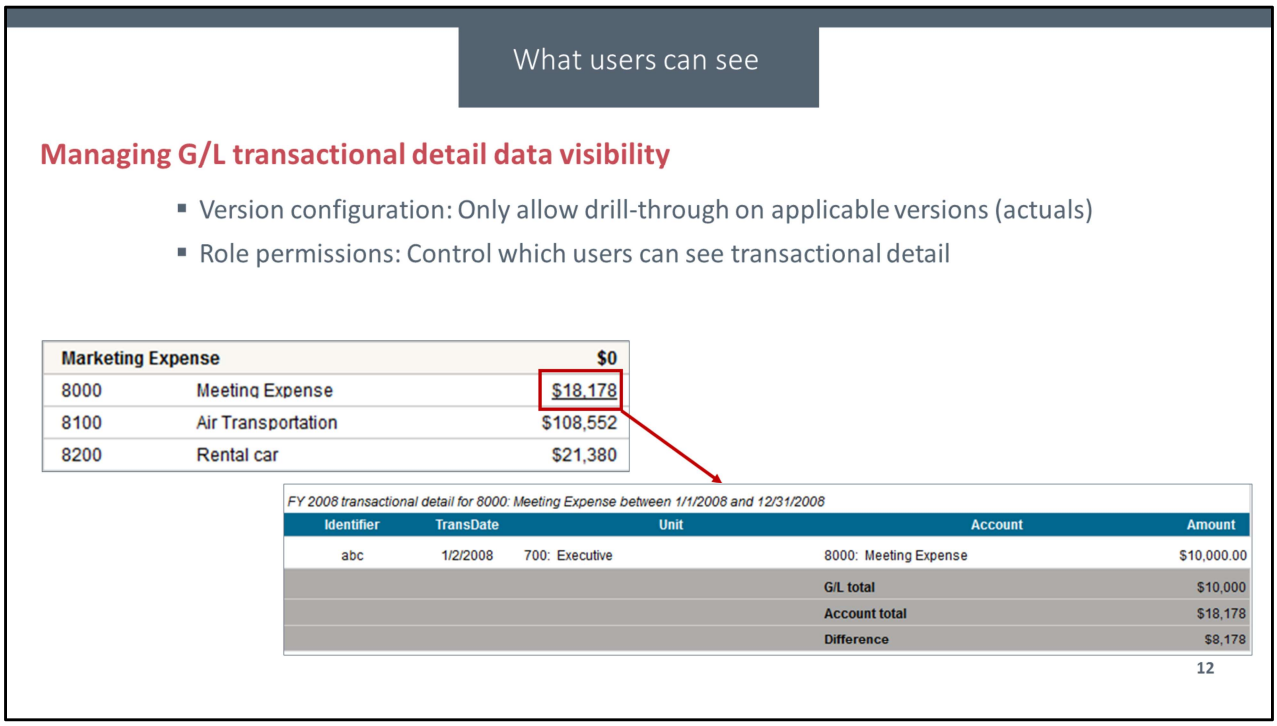
- Only show users the versions they can budget
- Hide versions with sensitive data
- Any role with the 'Hidden versions' permission can see them
- Prepare a version before it's ready for use (e.g. prepop data)
  - Un-hide only when it's ready for use

Fiscal year	F/X set	Version code	Description	Version type	First period in version	Last period in version	Read-only	Active	Hidden
2011	R2010 - Copy	FY2011-D-21	2011 Baseline Budget	Budget	Jan	Dec	☑	☑	☐
2011	R2010 - Copy	FY2011-PREPOP	2011 Prepop source	Reference	Jan	Dec	☑	☑	☑
2011	R2010 - Copy	FY2011-D-24	2011 Draft	Budget	Jan	Dec	☐	☑	☐
2011	R2010 - Copy	FY2011-D-23	2011 Final Budget	Budget	Jan	Dec	☐	☑	☐

FY2011-D-21	2011 Baseline Budget
FY2011-D-23	2011 Final Budget
FY2011-D-24	2011 Draft

11

• On the Configure Versions page, you can mark unit as being 'hidden'. Hidden versions will not show up on the 'Open different' page, or in the quick-switch dropdowns, or anywhere else in the system.
• A common use case for this is to hide your prepopulated data sources from users, since they can't edit that data, and the data flows directly into their budgets. Prepopulated data sources usually are not complete budgets, either, so showing them is just confusing.
• Another common use case would be to create budgets for scenarios you don't want your users to see – for example, you might not want some users to see the actual expenses as they come in over the course of the year, or you might have a 'pessimistic' scenario being developed.
• You can define which users are allowed to see hidden versions or not. The 'View hidden' role-based permission defines this. As always, superusers can always see everything.



• On the Configure Versions page, if you've requested to have transactional detail enabled, you can also mark a version as 'Show GL detail.' When you have a version marked as showing GL detail, that means that your users can drill through into the actual transactions that make up your budget. Usually, this will be active only for the reference version that contains your actuals, and sometimes for a mid-year forecast. That way, the transactions should line up exactly with the actual income or expenses. Allowing transactional detail for a budget version can be useful if you want to get a very detailed look at differences between budget and actuals, but the recommended practice is to restrict the transactions to your reference version or forecasts only.

• You also have to assign the 'View transactions' permission to the user's role. Users without that permission aren't allowed to see transactional detail, even in versions that otherwise allow it. That way, you have control over whether users can see the finest-grained detail about your data.

What users can do

Role permissions that determine what a user can *do*

- Superadmin
- View / Change Configuration
- Change budgets / Change all
- Change Headcount Allocations
- Create Projections

Role code	Description	Super admin	View Config	Change Config	View All Budgets	Change All Budget	View Budget	Change Budget	View Headcou	View Headcou Report	Change Headcou Allocatic	View Restricte	View Restricte Report	View Hidden Versions	Create Projectic	View Transact
Config Manager	Can change configuration, but not view headcount	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Report Assistant	Able to view reports only	☐	☐	☐	☑	☐	☐	☐	☑	☑	☐	☑	☑	☑	☐	☑
SuperAdmin	Super Administrator	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
UnitDpty	Unit Deputy	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐
UnitMgr	Unit Manager	☐	☐	☐	☐	☐	☑	☑	☑	☑	☐	☑	☑	☐	☑	☑

13

The next major category of permissions are the function-based permissions. These define what you're allowed to actually do within BudgetPak, within the scope of what you're allowed to see. We'll be going over each of these individually.

What users can do

Permission: Superadmin

- Everything!

14

Being the superadmin means you can do anything that BudgetPak has to offer. You automatically have every permission in the system. In this case, with great responsibility, comes great power.

What users can do

Permission: View/change configuration

- Not quite everything!
- Still subject to other permissions
  - Unit scope: can only budget for units they are assigned to
  - View headcount: cannot see salary and related information even in configuration pages
  - View restricted: cannot see restricted account values even in configuration pages
  - View transactions: cannot see transaction data configuration pages

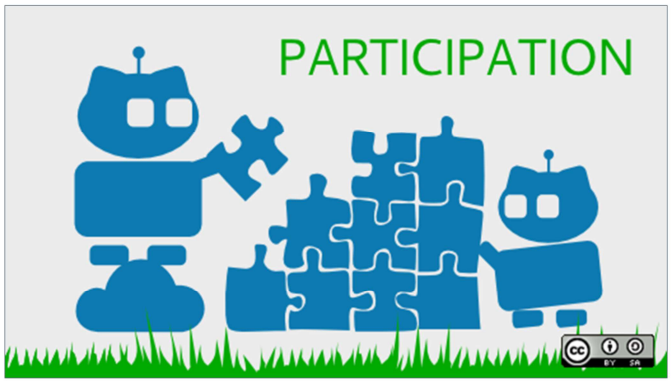
15

•There's another level of permissions one step down from the superuser. That's view and edit configuration. When you have these, you have access to the configuration pages, but all of the user-side restrictions are still in place – you can only sign off budgets that are in your scope, you can't see headcount or restricted sections unless you have that permission, and so on.
•There are also some limitations within the configuration pages themselves.
• Users who can edit configuration but aren't superusers do not automatically get access to other companies in the system, if you have multiple companies set up.
• Users who don't have view headcount permissions DO still have access to the 'Edit employee data' and related pages, because they have to have that access to make some adjustments depending on other configuration changes. However, those users do not get to see some of the information for the headcount, particularly including the salary data and last raise or last bonus data.
• Users who can't see transactional data also can't configure transactional data.
• Users who can't see hidden versions DO still have access to all the versions on the Configure Versions page; they will not, however, be able to see any hidden versions from any budget-side pages, such as the quick-switch dropdowns.

What users can do

Permission: Change budgets / change all

- Controls ability to edit budgets
- Separation of 'view' and 'edit'
  - Some users need to be able to see budgets, but not edit them
- *Overrides* unit roles
  - Users with 'change all' permission can change budgets they are budgetholder for
- Bulk operations on the status page
  - Bulk sign off, bulk approve, bulk revokes
  - Without *change all*, those options are not available



16

• Obviously, one of the most important functions of BudgetPak is to enter budgets. In order to do that, users need to have the 'Change budgets' permission. This allows them to actually modify the budgets that are in their scope. Without this permission, they have view-only access. For some users who only do reporting, that can be what you want – but most of your budget managers will need to have the ability to enter their budgets.
• Since users can only modify budgets they can see, the 'Change all budgets' permission might seem to be redundant. It does, however, have some important capabilities.
• First, users with the 'change all budgets' permission can edit budgets for ANY unit in BudgetPak, even if they haven't been assigned as budgetholder or budget assistant. Make sure to grant this permission sparingly!
• Second, only users with the 'change all budgets' permission can sign off or revoke signoff in bulk from the Status page. This is a convenience feature that allows administrators or budgetholders to manage a whole branch of their unit hierarchy at a time. For example, if budgets all got signed off at the base level, and then a higher-level manager saw that the total budget was coming in too high, the manager might revoke signoff for the entire branch and give everyone instructions to reduce spending by X percent.
• Third, users with the 'change all budgets' permission but not the 'view all budgets' permission do have the ability to write data to all budgets, even ones they're not allowed to actually view. If someone has a specialized model for some particular account that's in multiple budgets, you could grant that person the 'change all budgets' permission and then provide them with a myXL sheet they could use to update budgets they can't actually see.

What users can do

Permission: Change headcount allocations

- Headcount allocations, not calculations
- Able to affect other budgets by allocating new hires (and their costs) to other units
  - … even after they sign off
  - Grant with caution!

17

• Another one of the security features of BudgetPak is the ability to decide who gets to do one particularly tricky bit of budgeting – headcount allocations. This feature needs extra authorization around it because it can do things that users otherwise don't generally have the power to do - change someone else's budget, and change numbers after signoff has already happened.
• If you have this permission, you're allowed to allocate your new hires within a budget. If you're allocating them, then that means some of their headcount expenses are going into other units, changing their numbers. This also means that if you've previously allocated a new hire into some other unit, and then that unit got signed off, you could still come back to this new hire and modify them – alter their start date or salary, for example – and have an effect on that signed-off budget. As a result, a BudgetPak administrator has to explicitly give users this ability; by default, only administrators can set up employees with cross-unit impacts.

What users can do

Create projections

- Anyone can view projections they're assigned to
- Only allowed users can create projections
- Account restrictions still apply
- Hidden versions still apply

18

• The last permission-based topic we'll be going over today is the 'create projections' permission. Anyone is allowed to view and edit a projection if the creator of the projection assigned them that ability, which can be done on a projection-by-projection basis. However, only users who've been explicitly granted permission can create new projections of their own. There's a separate session for projections, so I won't go into them too much right now. From a security standpoint, it's useful to know that even when setting up a projection, the other restrictions still apply – if a user can't see restricted accounts or hidden versions, they can't include restricted accounts or hidden versions in their projections.

Common role configurations

Collections of permissions: Common role configurations

- Superuser
  - Able to do anything in the system
- Configuration manager (no headcount)
  - Able to edit configuration, but not see salary data
- Unit manager
  - Able to see everything within their assigned units
- Unit deputy
  - Able to see their assigned units, but not sensitive data (headcount and restricted accounts)
- Executive (read-only)
  - Able to view reports for all units, but not edit any budgets

Role code	Description	Super admin	View Config	Change Config	View All Budgets	Change All Budgets	View Budget	Change Budget	View Headcou	View Headcou Report	Change Headcou Allocatic	View Restricte	View Restricte Report	View Hidden Versions	Create Projecti	View Transact
Config Manager	Can change configuration, but not view headcount	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Report Assistant	Able to view reports only	☐	☐	☐	☑	☐	☐	☐	☑	☑	☐	☑	☑	☑	☐	☑
SuperAdmin	Super Administrator	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
UnitDpty	Unit Deputy	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐
UnitMgr	Unit Manager	☐	☐	☐	☐	☐	☑	☑	☑	☑	☐	☑	☑	☐	☑	☑

19

Password Strength

A tip on passwords

- Longer is better than more complex

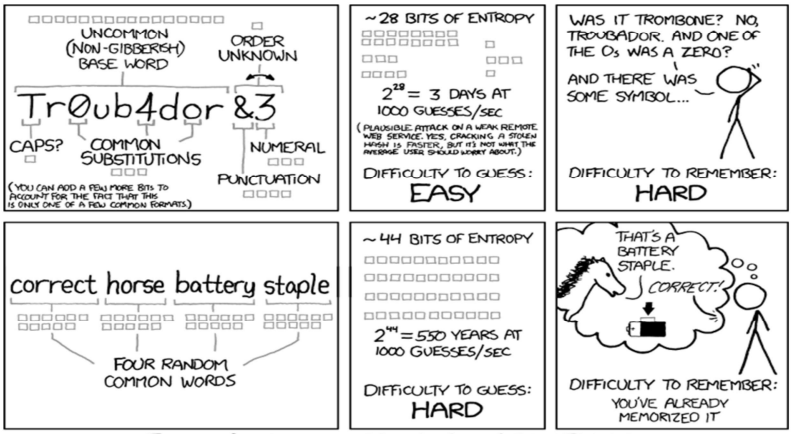


Image courtesy of XKCD: https://imgs.xkcd.com/comics/password_strength.png

20

And finally, we come to my favorite slide of the day. Many of you are not actually responsible for the password policies your organization uses, but this applies to more than just BudgetPak. It's true for any system that involves passwords. There are all sorts of caveats and complexities involved in passwords, and the most common kind of 'security breach' is called social engineering – that is, a human being gets tricked into giving up their password. But mathematically, longer passwords are harder to crack than complicated ones. Adding lots of numbers and special characters certainly looks more secure, but making a password that users can remember means computers have a harder time guessing it and they won't have to do insecure things like leave their password on a post-it note.

Just don't actually use 'correcthorsebatterystaple' as listed in this comic. They released a list of common passwords last year, and thanks to this comic strip, that one was in the top hundred.

Q&A
Thank you!
XLERANT