



Elevating. Performance. Together.



AXIOM INSIGHTS webinar

(Based upon Version 2020.1)

Moderator: Anastasia Rundus, Client Relationship Executive

Deb Miller, Client Services Account Executive

Luke Taylor, Technical Services Director

Teresa Holland, Lead Client Analyst

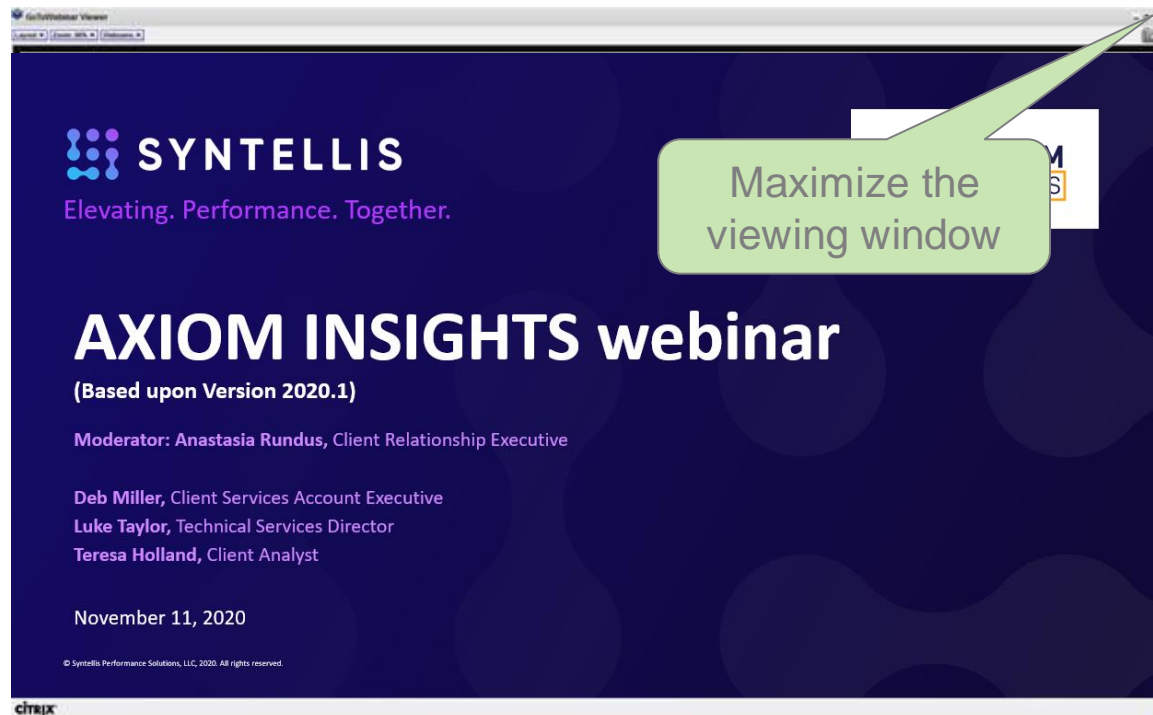
November 19, 2020

AGENDA

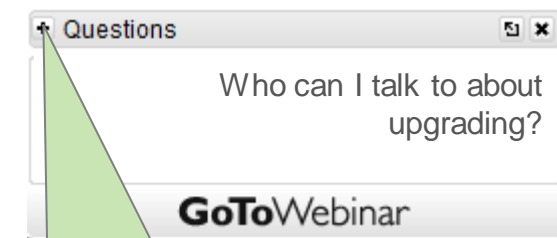
- Introductions & Webinar instructions
- Axiom Help and Syntellis Central Refresher
- Platform Upgrade Recommendations
- Managing Security
- Questions and Answers

Webinar Information

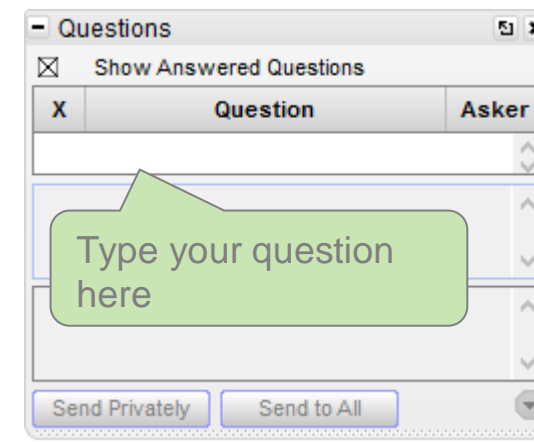
Maximize your viewing window



Submit questions



Expand question window



KAUFMAN HALL SOFTWARE IS NOW



SYNTELLIS

PERFORMANCE SOLUTIONS

We offer solutions that turn data into intelligence,
transforming raw information into a clear path forward ...
resulting in elevated client performance.

SYNTHESIS



INTELLIGENCE

*Note: In order to continue receiving important product announcements, thought leadership and best practices from Syntellis, please request that your IT department **add the following new IP address to your Corporate Allow List:**
192.28.158.208*

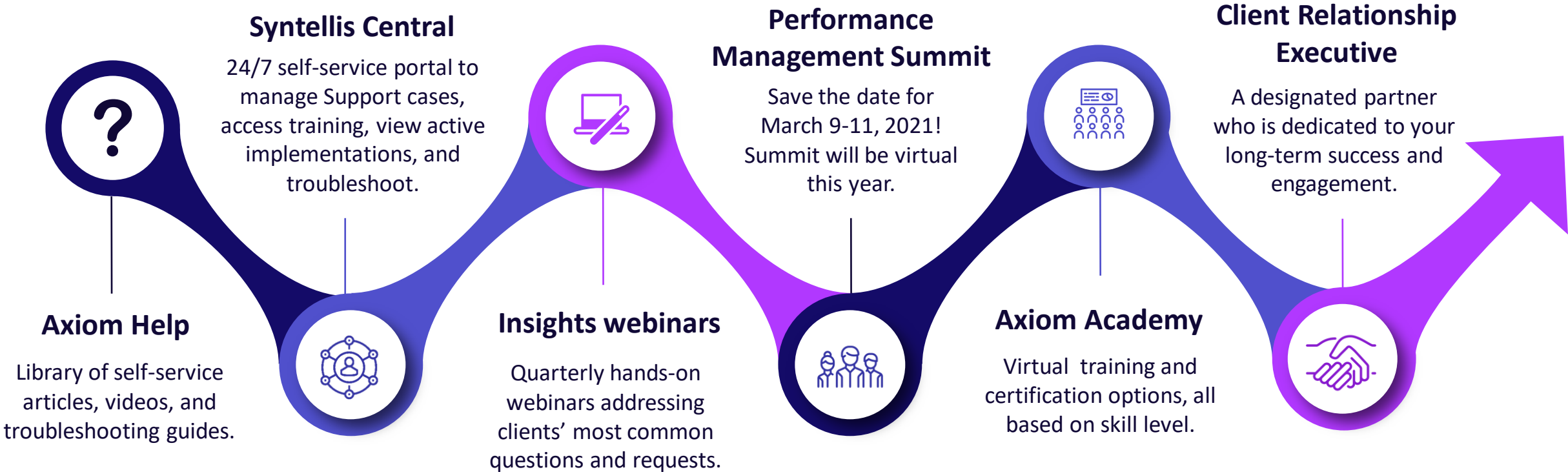
We value your feedback!

Please take our [10-minute survey](#) to help us understand the challenges and opportunities facing your industry and how Axiom software equips you to solve them.

The first 400 respondents who complete the survey will receive a \$15 Amazon e-gift card.

Advantage Program

New and enhanced programs support user expertise, time to value and improved satisfaction





Refresher: Axiom Help and Syntellis Central

Axiom Help & Syntellis Central

- Axiom Help – What has changed?
- Syntellis Central – Creating a login
 - New features
 - Access to videos and training

Axiom Help

Axiom Help can be accessed from within the software application

- Product specific Help
- Platform Help (Advanced Help)

Training videos

- Moved to Syntellis Central to allow broader access

AXIOM HELP – overview

NOTE - With the release of Version 2019.4, all HELP options have been moved to the MAIN | AXIOM MAIN or ADMIN | AXIOM ADMIN menus

The image displays three screenshots of the AXIOM software interface, illustrating the location of the Help menu across different views: MAIN, ADMIN, and AXIOMMAIN.

MAIN View: The Help menu is located in the Applications group, represented by a question mark icon. It is circled in red.

ADMIN View: The Help menu is located in the Help group, represented by a question mark icon. It is circled in red.

AXIOMMAIN View: The Help menu is located in the Help group, represented by a question mark icon. It is circled in red.

Syntellis Central

Client Portal (Syntellis.com/Central)

- Access Help documentation
- Locate technical training materials
- Submit a Support ticket
- Add additional information to an existing Support case
- Find the status of a Support case
- Access a training video
- Register for training
- Allows access to users who do not have Axiom installed on their workstation

Register and create a login ID

- Use your work email – connected to your email domain name for your organization
- Webinar – July 22 - https://ideas.syntellis.com/I/axiom-advantage-series?utm_source=outlook&utm_medium=email&utm_campaign=gi-sw-wbnr-axiom-advantage-series



Platform Upgrade Recommendations

Platform Upgrade Considerations

- The 2020.x Axiom Software platform update(s) require:
 - .Net Framework 4.8 or higher on end user workstations hosting:
 - Axiom Windows client
 - Axiom Excel client
 - Cloud Integration Service (CIS) server.
 - Supported operating system versions for end user workstations are:
 - Windows 8.1 or Windows 10.
 - Supported operating system version for the cloud integration service server are:
 - Windows Server 2016 or 2019.
 - If you are currently running version 2019.1 or earlier
It is required to upgrade the Axiom Cloud Integration Service when your Axiom Cloud system is upgraded to version 2020.3.
 - If you are currently running version 2019.2 or higher
You can upgrade the cloud integration service, but, it is not required.
 - Note that *.khaepmcloud.com and *.axiomepmcloud.com are being deprecated and replaced with *.axiom.cloud.



Managing Security in Axiom

Use of Subsystems and Roles

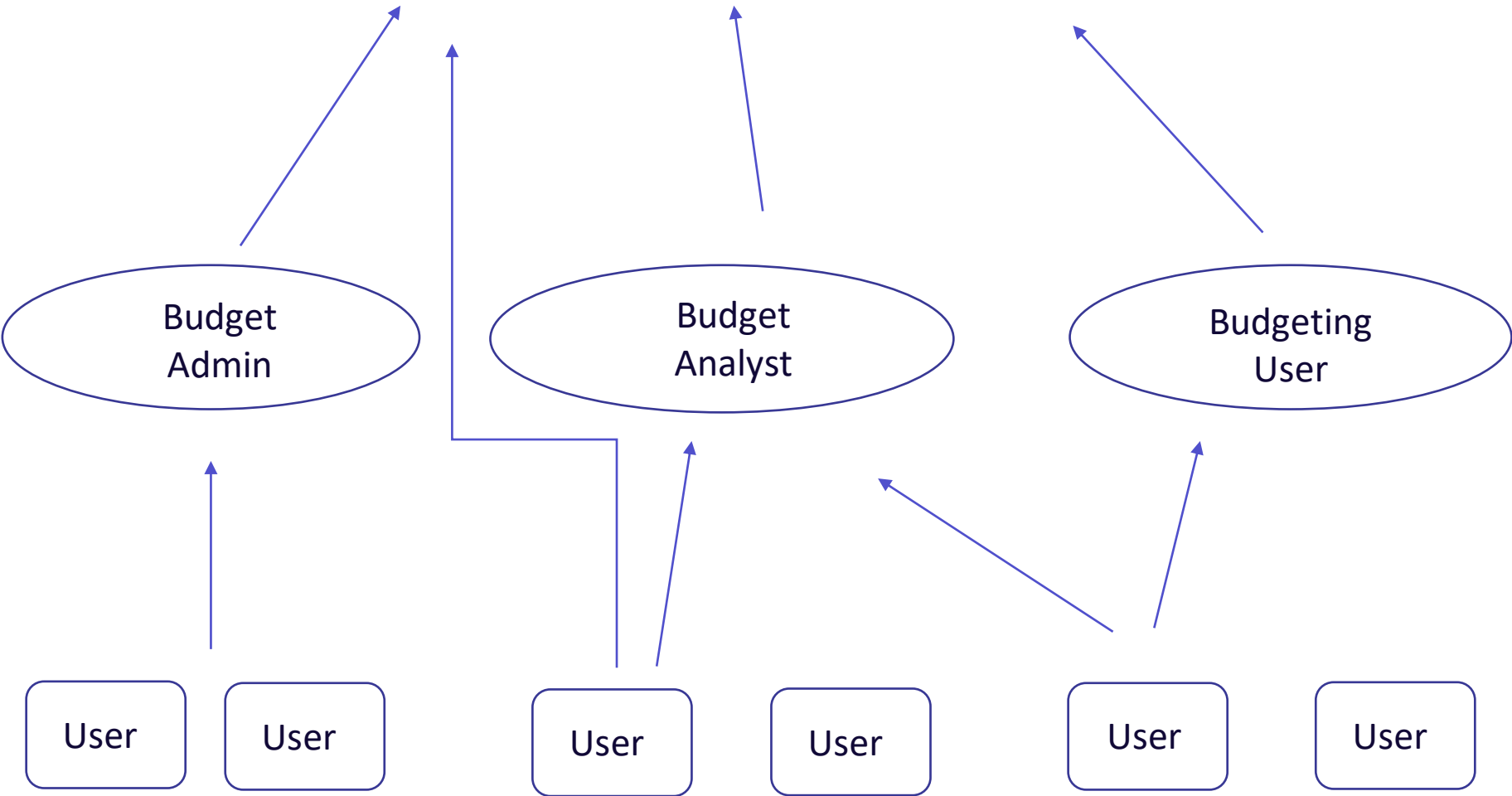
Subsystems, Roles and User Security

- Subsystems
- Roles
- Users
- Best Practices
- Help Files

Subsystem

Budget Planning

Role



User

Security Design

Axiom Security is comprised of three major components - Subsystems, Roles, & User level security.

- **Subsystems** define the maximum level of security.
- **Roles** define what assets a user can access.
- **User** level security grants access to the data tables & plan files by assigning filters to each user.

What is a Subsystem?

- Security subsystems allow you to define groups of users to be managed as a distinct "subset" of users within the system
- Typical subsystems
 - Budget Planning
 - Capital Planning
 - Cost Accounting
 - Financial Planning
 - Management Reporting
 - Productivity
 - Rolling Forecast
 - Comparative Analytics

The screenshot displays the 'Security Management for Demo Dev Prime (Copy) | COVID-19' window. The 'Subsystems' tab is selected, and 'Budget Planning' is chosen from the left-hand list. The main area shows the configuration for 'Subsystem: Budget Planning'. The 'General' tab is active, showing fields for 'Name' (Budget Planning) and 'Description'. Below these are 'Subsystem-Specific Roles' and 'Assigned Users' lists. The 'Assigned Users' list includes: Admin, Bud (badmin); Admin, Client (cladmin); Administrator, System (admin); Baker, Sam (Sbaker); Banta, Logan (lbanta); Bartlett, Stephanie (sbartlett); Bird, Jason (JBird); Brockermeyer, Roger (RBrockermeyer); Casmer, Kelly (KCasmer); Clark, Stewart (sclark); Colbert, JoAnn (JColbert); Correll, Suzie (SCorrell); Crane, Dave (DCrane); Crosson, Nathan (ncrosson); and Dean, Yolanda (YDean). The 'Subsystem Admins' section is empty. At the bottom, there are 'Apply', 'OK', and 'Cancel' buttons.

Subsystem

- What a Subsystem IS:
 - Typically equals a licensed Syntellis Product
 - Grants full access to Reports, Data, Plan files, etc. WITHIN the Product.
 - Subsystem rights DO NOT cross products
- What a Subsystem IS NOT:
 - Subsystems are *not* an alternative to roles.
 - Roles and User level adjust the subsystem security levels down

What is a Role?

- Users inherit the security settings defined for their assigned roles.
- Role rights are additive.
- Roles are intended to grant permissions, not deny permissions
- Roles do not provide access to data, only to files.
 - **User** security provides access to data.

The screenshot shows a software interface for configuring roles. At the top, there are three tabs: 'Users', 'Roles', and 'Subsystems'. The 'Roles' tab is selected and circled in red. Below the tabs is a search bar with the text '<type here to filter list>'. A list of roles is displayed on the left, with 'Budgeting Admin' highlighted. The right pane is titled 'Role: Budgeting Admin' and contains several tabs: 'General', 'Permissions', 'File Groups', 'Tables', 'Files', and 'Startup'. The 'General' tab is active, showing 'Edit general information.' fields for 'Name' (Budgeting Admin), 'Subsystem' (Budget Planning), and 'Description' (Budget Administrator). To the right of these fields is a list titled 'Assigned Users' containing names and IDs such as 'Admin, Bud (badmin)', 'Admin, Client (cladmin)', 'Administrator, System (admin)', 'Baker, Sam (Sbaker)', 'Banta, Logan (lbanta)', 'Bartlett, Stephanie (sbartlett)', 'Bird, Jason (JBird)', 'Brockermeyer, Roger (RBrockermeyer)', 'Casper, Kelly (KCasper)', 'Clark, Stewart (sclark)', 'Colbert, JoAnn (JColbert)', 'Correll, Suzie (SCorrell)', 'Crane, Dave (DCrane)', 'Crosson, Nathan (ncrosson)', and 'Deweese, Dawn (DDeweese)'. At the bottom right are 'Apply', 'OK', and 'Cancel' buttons.

Product Roles

Systems with installed products will have roles that are designed for use with the product.

- **Product Admin:** Person(s) responsible for the configuration of the product and oversees the administration of the process
- **Product Analyst:** Person(s) assisting product users in the planning process. Have ability to read/write reports and facilitate Q&A on the plan files
- **Product User:** Typical End-User of the product.

The screenshot displays the Syntellis Roles configuration interface. At the top, there are three tabs: 'Users', 'Roles' (which is selected and circled in red), and 'Subsystems'. Below the tabs is a search bar with the placeholder text '<type here to filter list>'. A list of roles is displayed below the search bar, with 'Capital Planning Admin' highlighted in blue. Red arrows point from the list items to the bulleted descriptions on the left. The right panel shows the details for the 'Capital Planning Admin' role, including its name, subsystem, and description.

Role: Capital Planning Admin

General Permissions File Groups Tables Files

Edit general information.

Role Details

Name Capital Planning Admin

Subsystem Capital Planning

Description:

Capital Planning Administrators

Axiom Role Examples

General Roles

- Everyone
- Suite Administrator
- Security Admin
- Global Driver Management

Product Specific Roles

- Budgeting Admin
- Budgeting Analyst
- Financial Planning Admin
- Financial Planning Analyst

What is a User?

- **User** security grants access to the data tables & plan files by assigning filters to each user.
- User level security provides access to DATA within the following:
 - Tables (ACT20xx, ACT_PAY27_202xx)
 - Files: Reports and Utilities
 - File Groups: Plan files, Drivers, Process Definitions
- User JSmith:
 - Subsystem: Management Reporting
 - Role: Management Reporting User
 - Result: He can open up the Month End Dashboard, but unless he has User filters defined he won't get any data in the report.

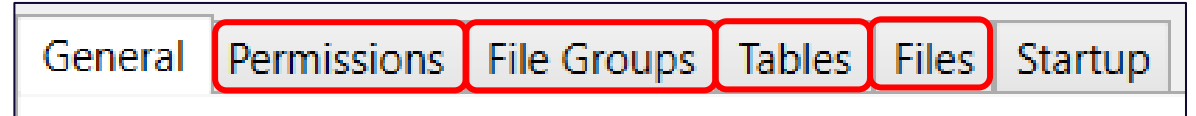
Security Setup for users

Initial security setup involves the following:

1. Assign the User to Subsystems
2. Assign the User to Roles
3. For each user, assign Files & Table data Access
4. For each user, establish Plan File Filters & Access.

Syntellis provides tools to apply standard data filters in bulk.

Security Setup



Security is configured by 4 sections

Permissions: Granted at Subsystem level. General administrative functions.

File Groups: Determines access to what file groups, what Plan Files, and what abilities within those File Groups.

Tables: Determines access to Data tables.

Files: Determines access to select Axiom files. Eg: reports.

Security Setup

The screenshot displays the 'Security Setup' interface for user **Holland, Teresa (tholland)**. The interface includes tabs for **General**, **Permissions**, **File Groups** (highlighted with a red box), **Tables**, **Files**, and **Startup**. The **File Groups** tab is active, showing a list of file groups including **Budget-2020_v3**, **Cost Management-2018 (CostManagement-2018)**, **Financial Planning-2017**, and **Financial Planning-2018**. A red box highlights the **File Groups** tab and the **Budget-2021** section.

An **Axiom Software** dialog box titled 'Effective permission details:' is open, displaying four points:

- 1: User configured permission of 'Plan files: DEPT.VP = 'Sally Klein', Access level: Read Only, Calc Methods: None, Interacts with Process Management: True'
- 2: Subsystem-specific role 'Budgeting User' permission reduced by subsystem 'Budget Planning' to Plan files: No plan files, Access level: Read Only, Calc Methods: Insert, Interacts with Process Management: True
- 3: Role 'Budgeting User' allows 'Plan files: No plan files, Access level: Read Only, Calc Methods: Insert, Interacts with Process Management: True'
- 4: Subsystem Budget Planning restricts permissions to:
Plan files: DEPT.VP = 'Sally Klein', Access level: Read Only, Calc Methods: None

The **Budget-2021** section shows **Configured Permissions** for **Plan Files**. A red box highlights the **Plan file access:** row, which shows **DEPT.VP = 'Sally Klein'** and **Access Level: Read Only**. Another red box highlights the **Interacts with Process Management: True** row. The **Effective Permissions** section shows the same permissions for **Plan file access:** and **Interacts with Process Management: True**. A red box highlights the **Show Details** link at the bottom of the **Effective Permissions** section.

The interface also includes a **Log in as selected user** button and **Apply**, **OK**, and **Cancel** buttons at the bottom.

File Groups: Role Inheritance

- Defines access rights for plan files in file groups
- Role inheritance depends on the permission set up at the user level
- Can set role inheritance to be:
 - **None** - role settings are ignored
 - **Combine** - Combined with user settings (Recommended)
 - **Independent** - role settings are inherited independently for user settings

General Permissions **File Groups** Tables Files Startup

Plan File Permission ? X

Configure the access level for a set of plan files.

File Access Level: No Access

☐ Allow Save Data ☐ Allow Unprotect
☐ Allow Calc Method Insert ☐ Allow Sheet Assistant
☐ Allow Calc Method Change ☐ Allow File Processing

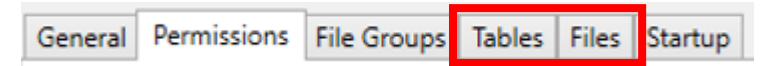
Apply settings to:
☒ Filtered Plan Files ☐ All Plan Files

☒ Interacts with Process Management [Help](#)
When selected, plan file processes can elevate user access to plan files included in this permission set, and process role assignments will consider this permission.

Role Inheritance: Independent
Roles: None
Each user and role unit when determined: **Combine**
Independent

OK Cancel

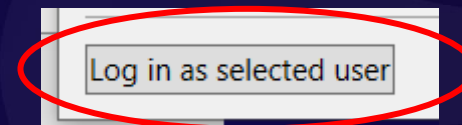
Tables and files



- For Tables and Files, the user inherits the **most permissive set of rights** among their user settings and any roles
- Suppose the user has the following settings for a report folder:
 - User: Read-Only
 - Role1: None
 - Role2: Read/Write
- Examples:
 - Role1 + Role2 = Read/Write access to that report folder
 - Role1 only = Read-Only access since their user permissions grant Read-Only.

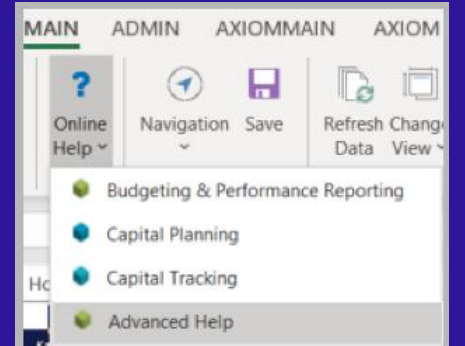
Security Best Practices

1. Always test a subset of users after making a role or user permission change and ***check the users' effective permissions*** to confirm the change took effect
2. Do not modify any product included roles
 - If you would like to add a custom permission to a set of users:
 - Create a new custom role
 - Provide the permission(s)
 - Add the users to that role
3. Limit number of user level changes made to permissions
 - Always think role first when granting permissions
 - Requires less security maintenance by managing a small set of roles instead of a large set of users
4. Remember to log in as the test user to confirm permissions



Axiom Help

Main Menu | Online Help | Advanced Help



AXIOM

Was this information helpful?

Search

Security

About Axiom Software security

The Security Management dialog

Managing users and roles

Security settings

Security subsystems

About subsystems

Enabling subsystems

Managing subsystems

Managing subsystem roles

Managing subsystem users

Bulk edit of security

Security tools

Security integration

Other Administration

Home > Security > Security subsystems

Security subsystems

Security subsystems allow you to define groups of users to be managed as a distinct "subset" of users within the system. Using subsystems, you can:

- Define a group of users to belong to the subsystem and be limited to a certain maximum level of permissions. When you create a subsystem, you are essentially drawing a permissions boundary that users who belong to the subsystem cannot cross.
- Assign one or more subsystem administrators who can manage security for the users that belong to the subsystem. This allows you to give certain users the right to manage other users' permissions, without needing to grant them full administrator rights or even full security administration rights.

Subsystems are *not* an alternative to roles. Roles grant permissions as a group; roles cannot be used to deny permissions or to grant user management rights. Subsystems are intended for situations where you need to create independently-managed user groups that work within the same system but only need access to specific defined areas of that system. Roles can then be used to grant permissions within the limits of the subsystem.

NOTE: Subsystems are optional in systems without installed products. Subsystem features are only available if you have enabled them using the system configuration settings.

AX2591

Remove Highlights

Topics in this section

About subsystems

Enabling subsystems

Managing subsystems

Managing subsystem roles

Managing subsystem users

Related PDF

Subsystems Guide.pdf

Get more information and training resources: www.kaufmanhall.com

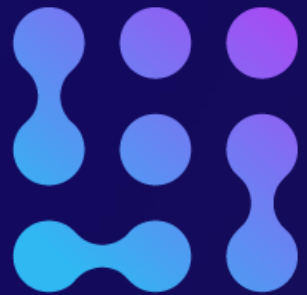
subsystems.htm

Questions and Answers

Please send suggestions for future webinars to

ClientRelations@syntellis.com

(Note new email address)



SYNTELLIS

ELEVATING PERFORMANCE