SYNTELLIS

Elevating. Performance. Together.

Security, Scheduler and Upgrades

(Based upon Version 2020.1)

Moderator: Anastasia Rundus, Client Relationship Executive

Deb Miller, Client Services Account Executive

Wil Coiner, Client Analyst

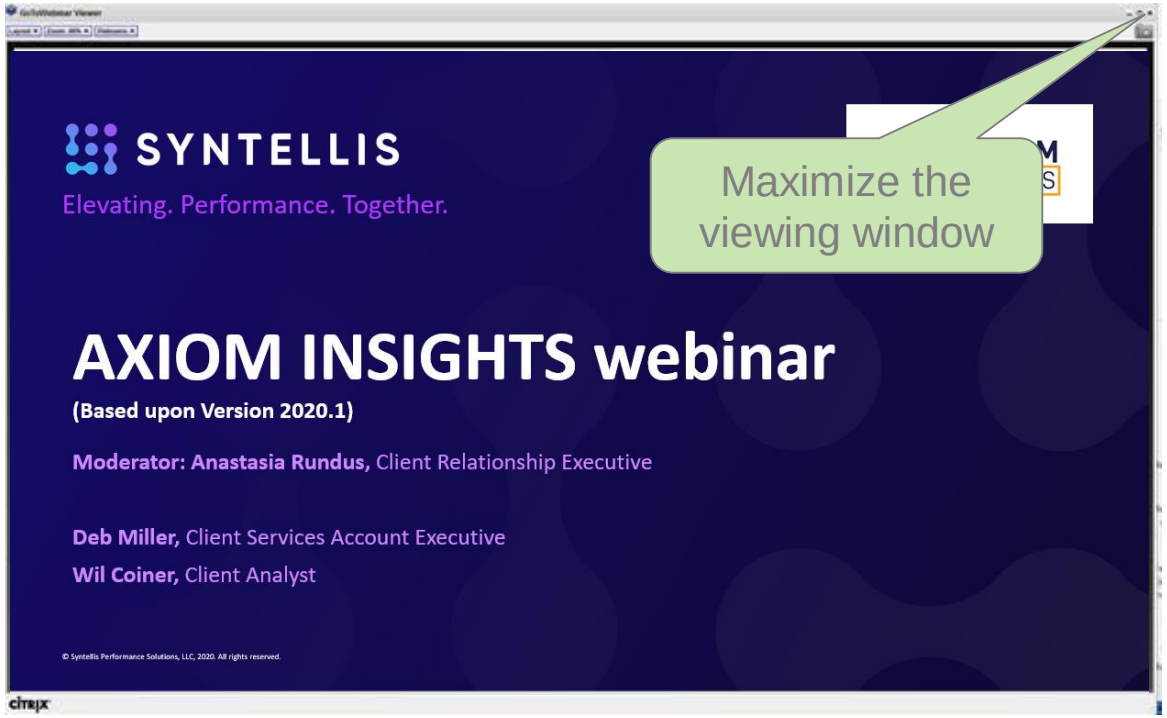
September 23, 2020

AGENDA

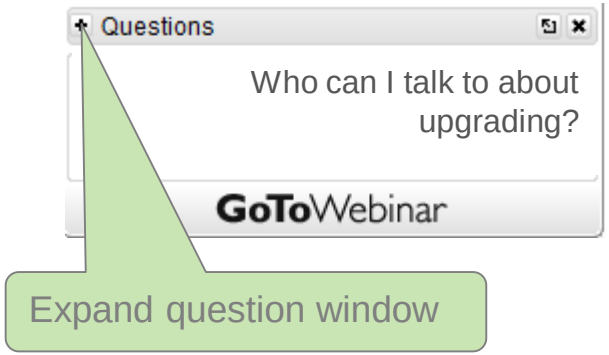
- Introductions & Webinar instructions
- Syntellis Overview
- Security and user permissions
- Scheduled Jobs
- Axiom Upgrades
- Questions and Answers

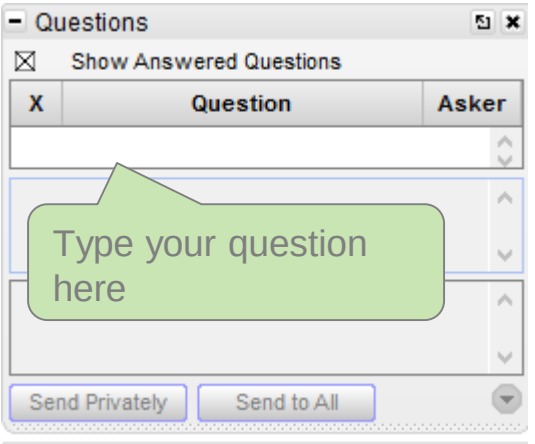
Webinar Information

Maximize your viewing window



Submit questions

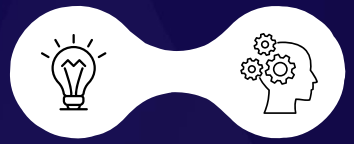




KAUFMAN HALL SOFTWARE IS NOW

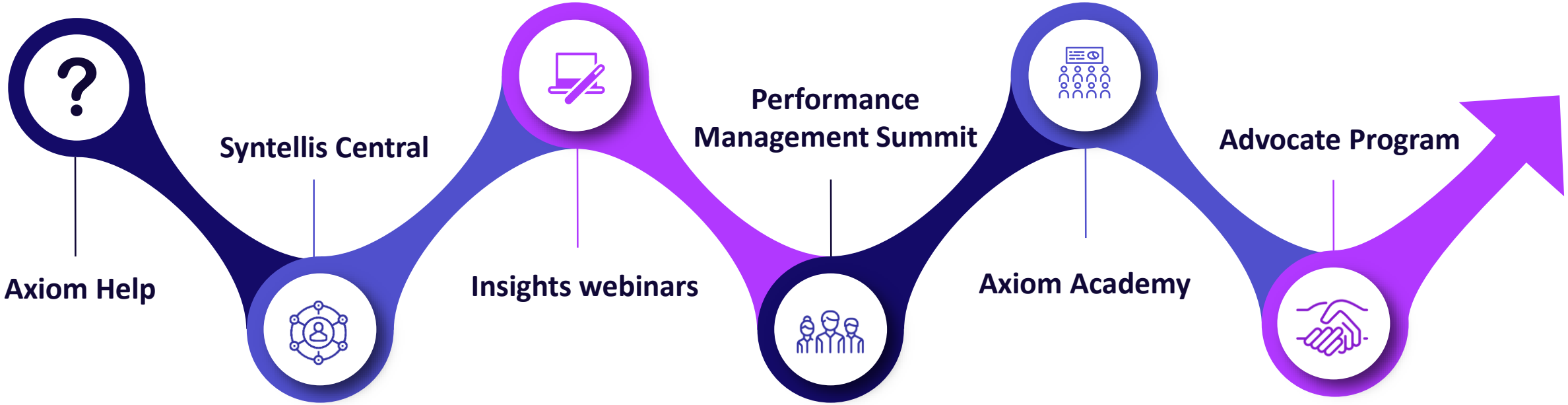
SYNTELLIS
PERFORMANCE SOLUTIONS

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

SYNTHESIS  INTELLIGENCE

Gain the Axiom Advantage

https://www.kaufmanhall.com/about/events-speaking/webinar-series-axiom-advantage



Evaluating Security Permissions

EVALUATING SECURITY PERMISSIONS

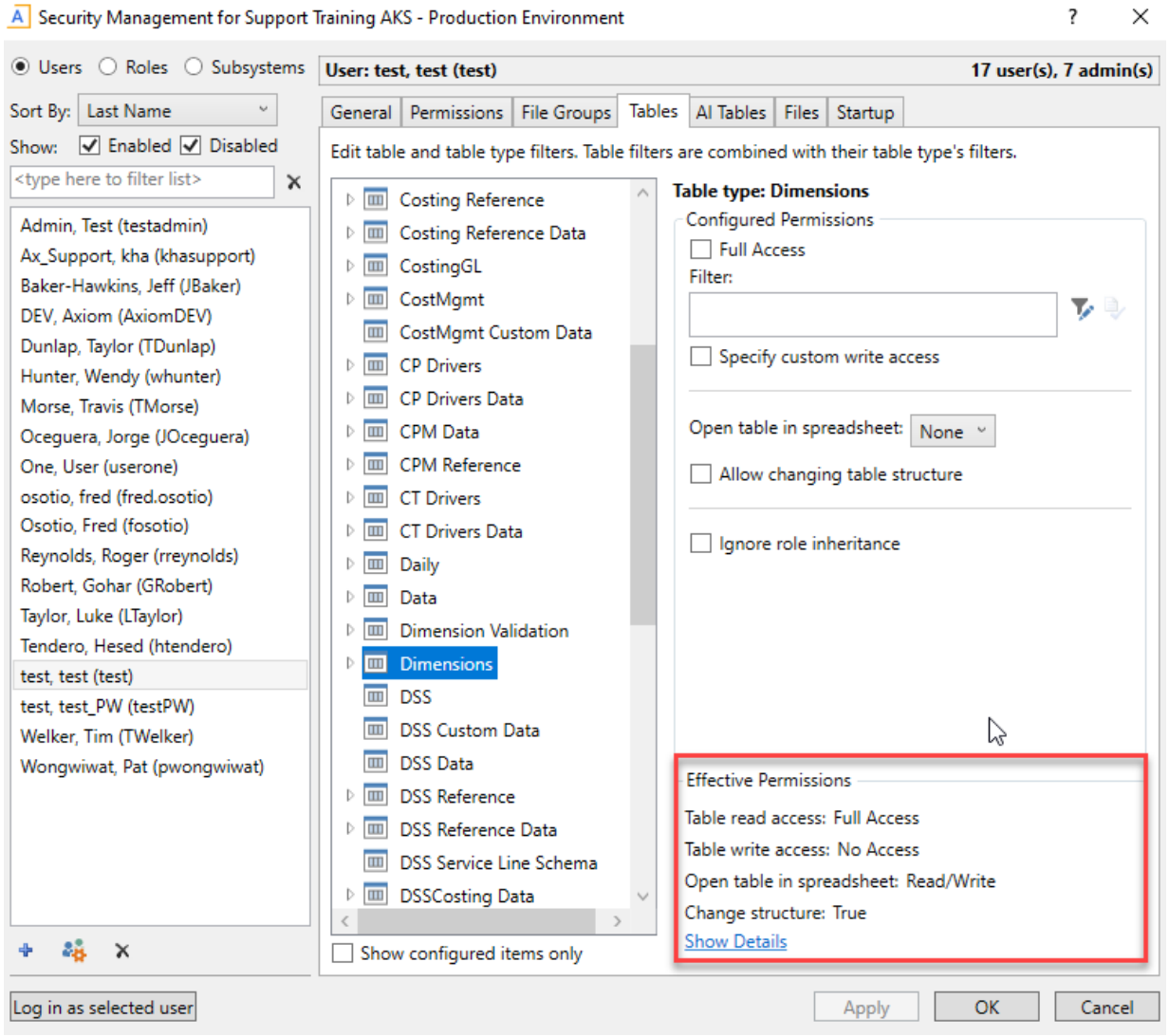
- Evaluating effective user permissions
- How user and role permissions interact
- Security best practices

Evaluating effective user permissions

Admin | Security | Security Manager

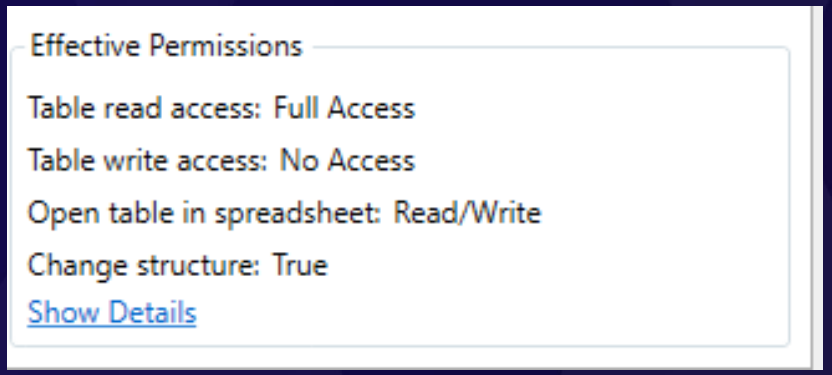
- The best option for determining why a user does or does not have the level of access expected is the **Effective Permissions** section of Security Manager

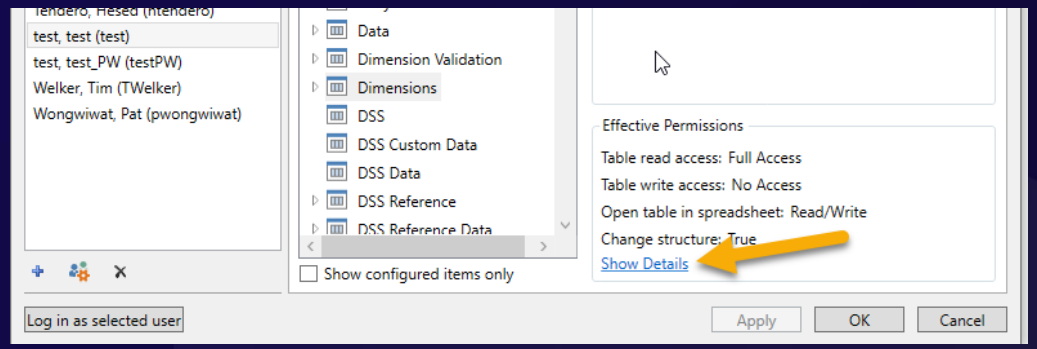
- Both the preview box and ‘Show Details’ box provide the final effective permissions and how they are determined



Effective Permissions

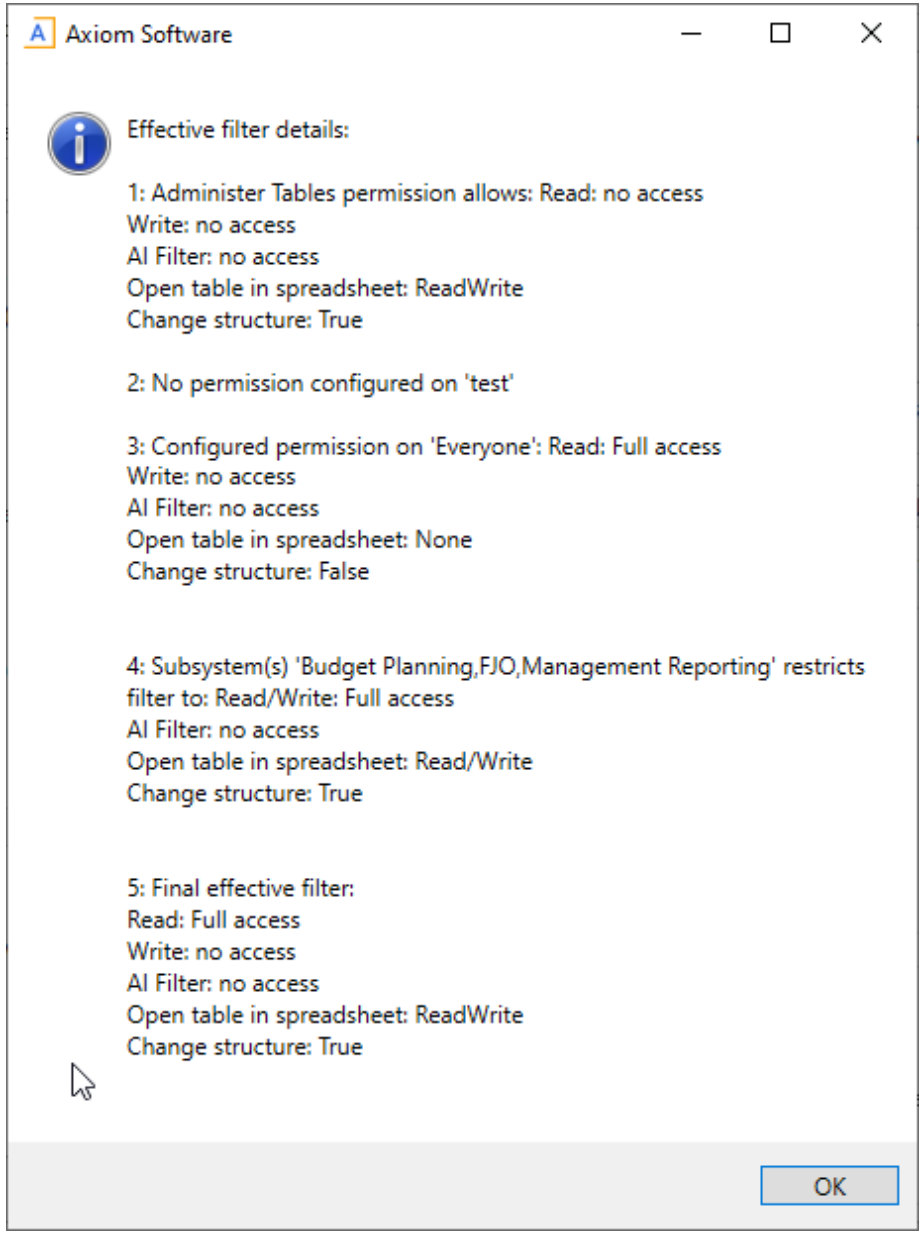
- The Effective Permissions box provides the final permission set for the selected user, including ALL role permissions that are used to evaluate the final permissions
- This is great snapshot of the user's access level to the selected table or file. A great starting point for determining what their access is
- The next step is to use 'Show Details' to see how the effective permissions are being evaluated





Show Details

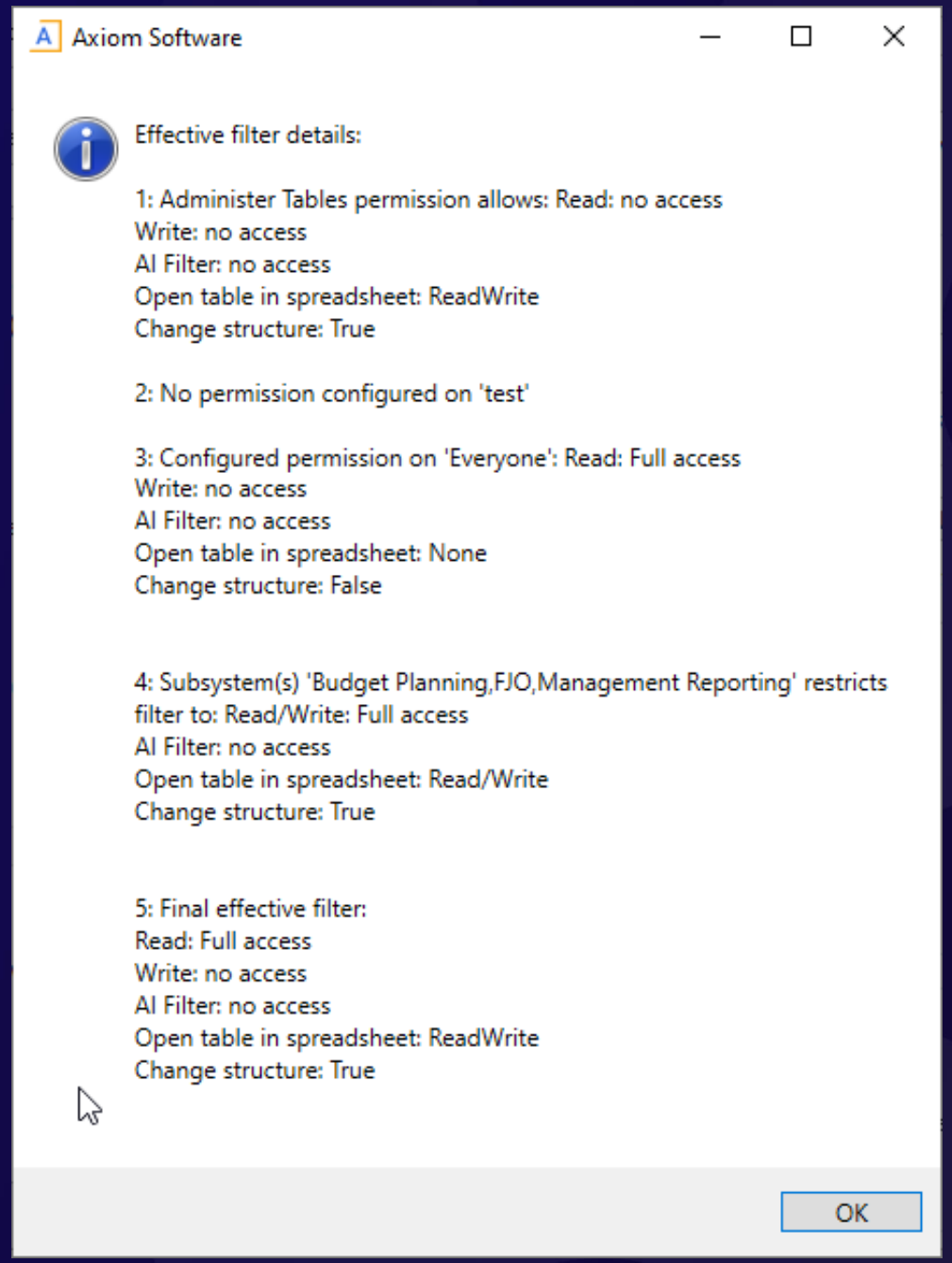
- The Show Details box will provide each role and user permission that is used to evaluate the final effective permissions of the user
- Each number corresponds to a role or user permission set defined in security and what those permissions are
- **Final Effective Filter** - provides the final permissions based upon the combination of permissions numbered above



Show Details Example

- This is an example of a user's permissions to the Dimension table type, which includes tables like DEPT, ACCT, etc.

1) The Administer Tables permission provides Read/Write access to the table when opened in a spreadsheet
2) There are no user configured permissions
3) The Everyone role provides full read access to the table (access level to data when querying table in a report)
4) The Subsystem defines maximum permissions but does not set permissions. If a role/user permissions exceeds the permission of the subsystem, that permission will evaluate to the maximum allowed
5) **Final effective filter** is the combination of permissions provided by each role and user permission set



Effective Permissions

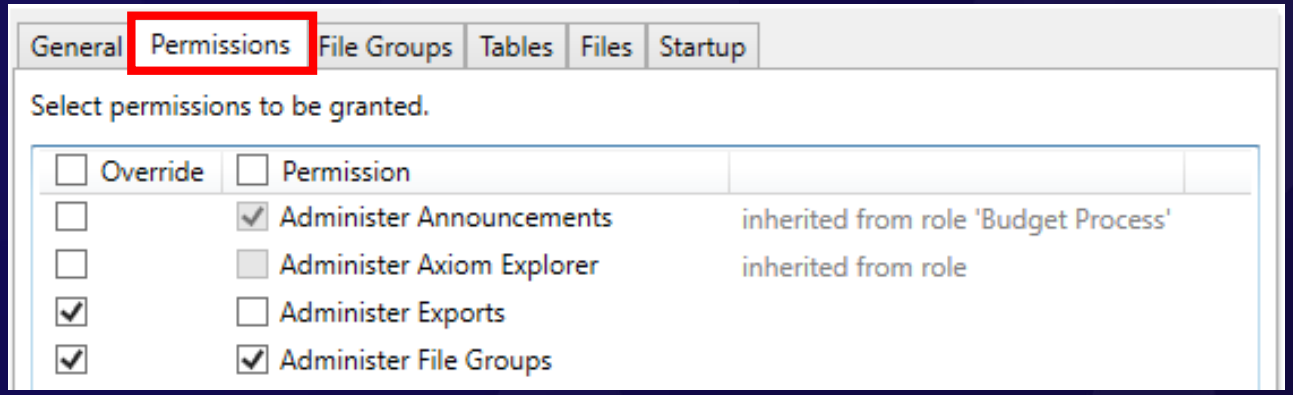
- The information gathered via Effective Permissions and Show Details can then be used to adjust user and/or role permissions to the desired level of security for the user(s)

- We will discuss security adjustment best practices later in the presentation

How user and role permissions interact

- In general, role rights are additive.
  - Roles are intended to grant, not deny permissions
- Be sure to review Effective Permissions for a user within a role each time you adjust role security
- We will look into how user and role permissions interact under each tab of Security Manager
  - Permissions
  - Startup documents
  - File groups
  - Tables and Files

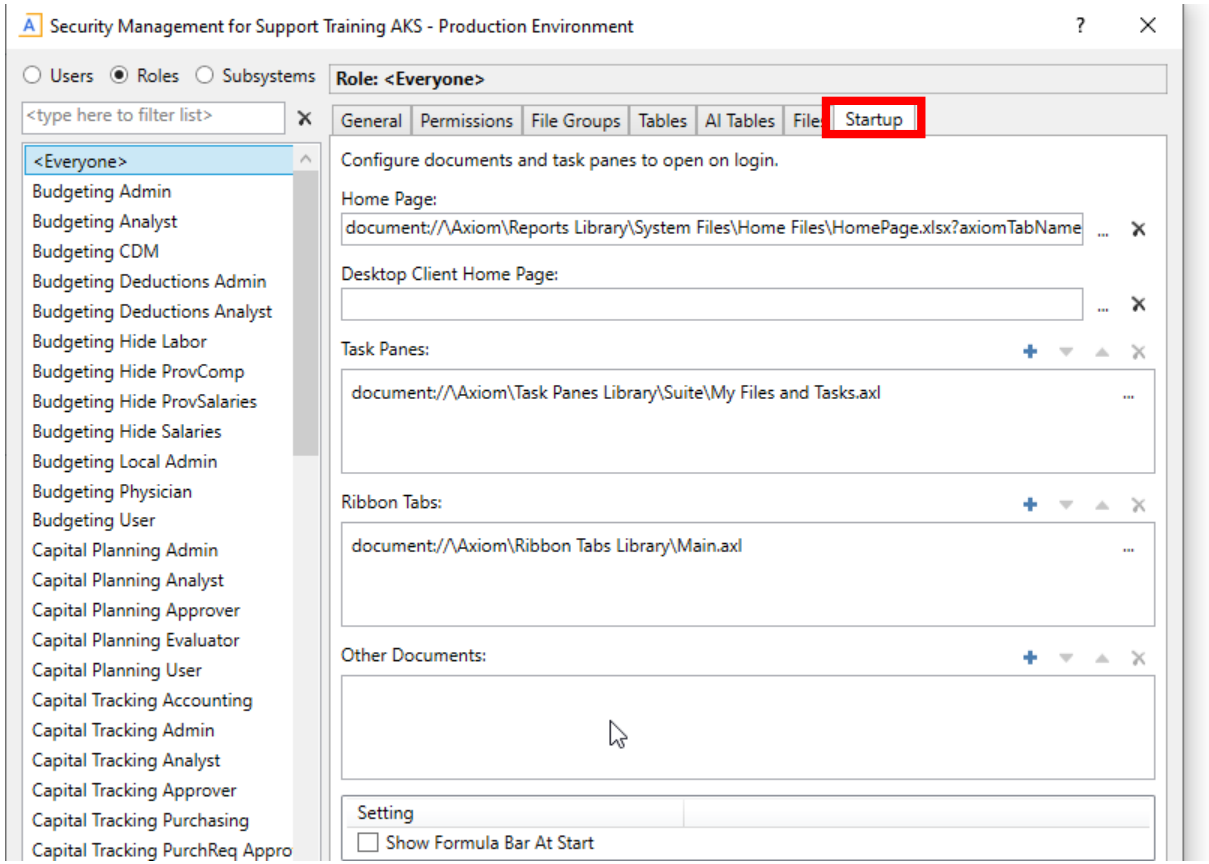
Permissions tab



- Defines access rights for specific Axiom features
- Users inherit any security right to Permissions via any roles they are assigned to
- You can override this inheritance for a user on a per permission basis
- In the example, we are overriding the role permissions for Administer File Groups
  - No role they are in grants rights to this Permission. We clicked Override then selected the Administer File Groups permissions to grant the right at the user level

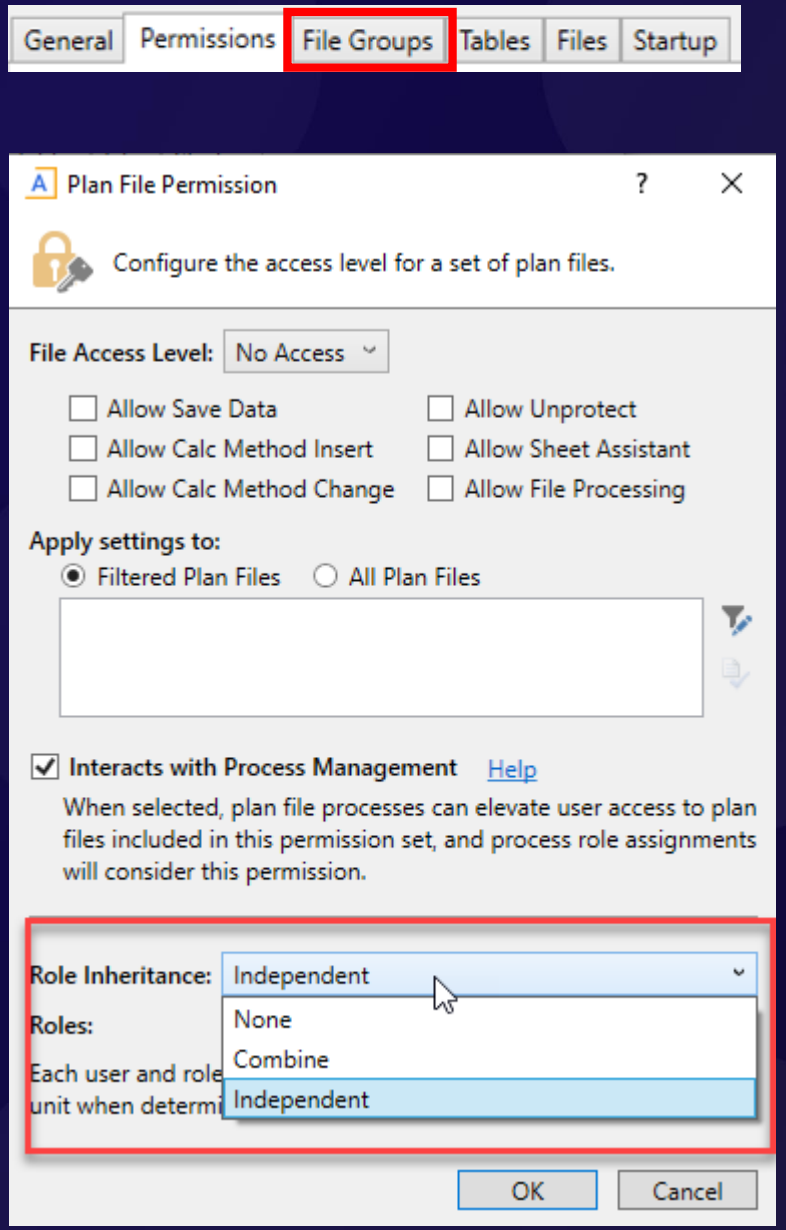
Startup documents

- Specifies files that open when a user starts Axiom software, such as the home page, task panes, and ribbon tabs
- Users inherit startup files from roles in addition to their own assigned start up files
- Each user can only have one home page.
  - If a user has an individual home page, that file will be used and any role home page will be ignored
  - If no home page is assigned, the default homepage is used for both role and user permissions

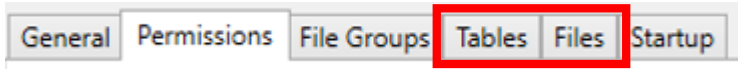


File Groups

- Defines access rights for plan files in file groups
  - NOTE: Does NOT provide access to what data they can see in each plan file
- Role inheritance depends on the permission set up at the user level
- Can set role inheritance to be:
  - Combine - Combined with user settings
  - Independent - role settings are inherited independently for user settings
  - None - role settings are ignored



Tables and files



- For all other areas of Security, including tables and files, the user inherits the **most permissive set of rights** amongst their user settings and any roles
- Suppose the following access level 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.
- Since role permissions are additive, it CANNOT reduce user permissions

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) and add the users to that role
   - Any changes made to a standard product role will be reverted when the system takes an upgrade
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

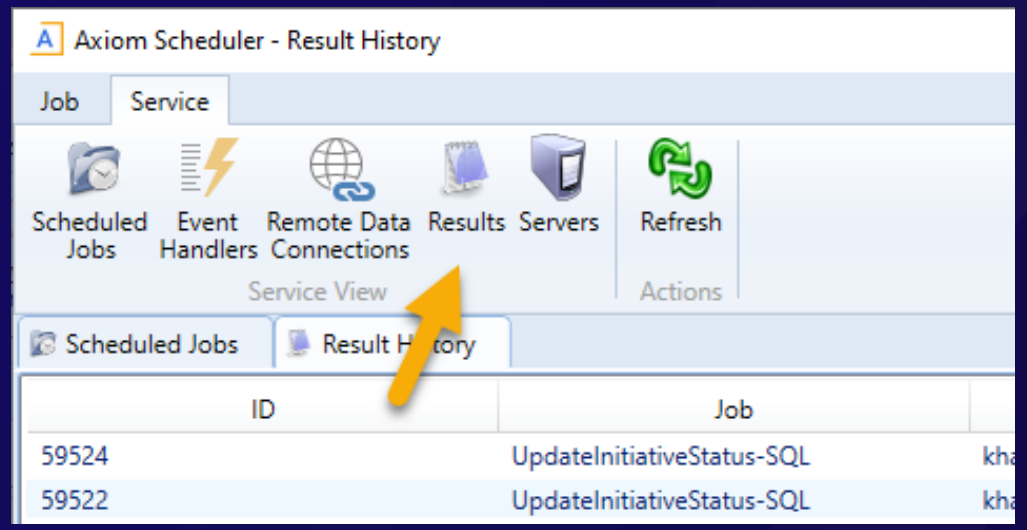
Reviewing and Troubleshooting Scheduled Jobs

REVIEWING AND TROUBLESHOOTING SCHEDULER JOBS

- Accessing job results
- Reviewing job results detail
- Interpreting scheduler messages
- Recommended troubleshooting steps
- Scheduler best practices

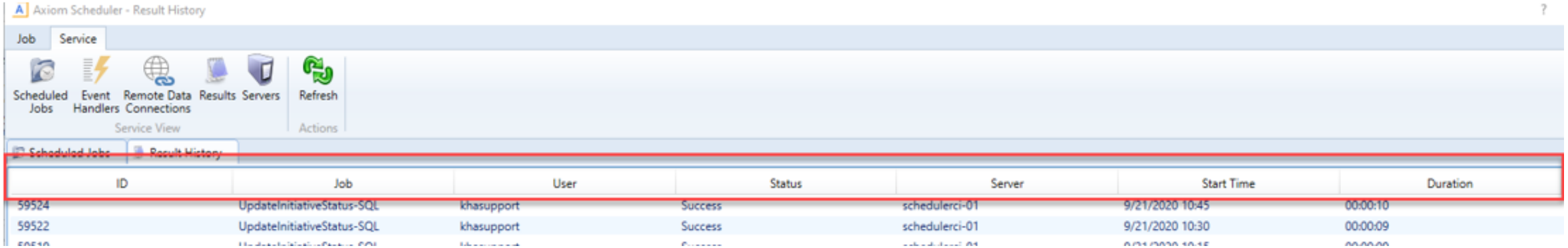
Accessing Job Results

- Job results are accessed via the ADMIN ribbon | Scheduler
- Click on the Results icon at the top



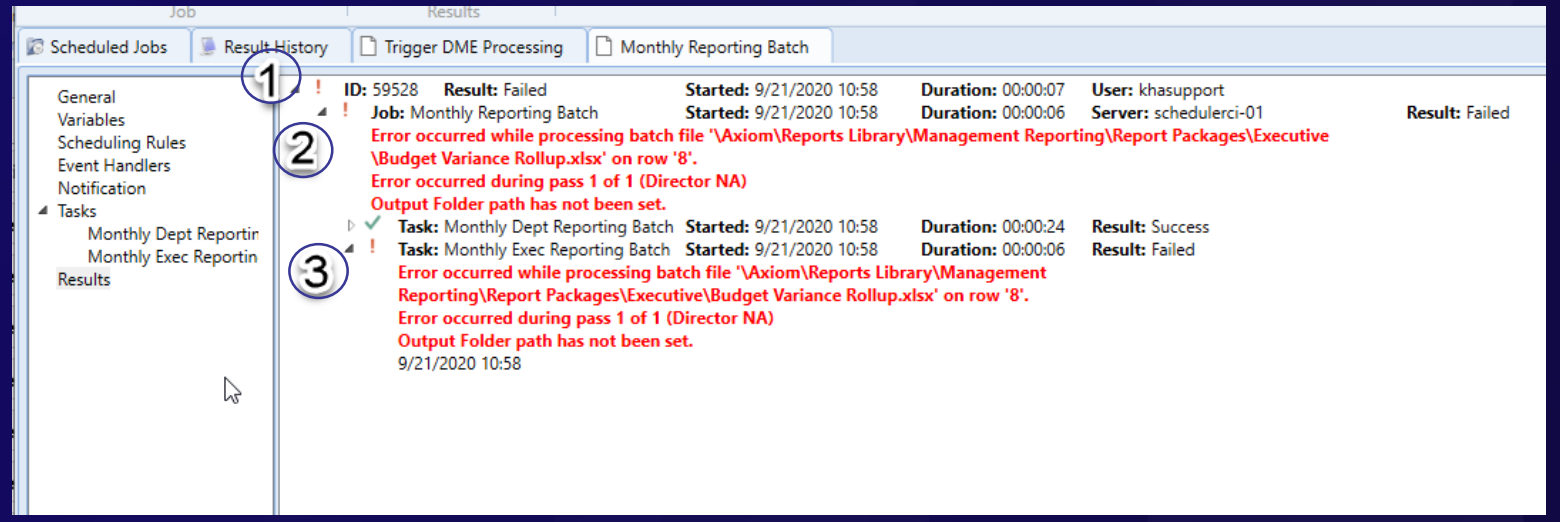
- From here you can review all currently running and recently ran results

Accessing Job Results



- On the Result History tab you can review:
  - Job – name of the job
  - User - the user ID of who scheduled or manually kicked off the job
  - Status - the status of the job
  - Server – the scheduler server that the job ran on
  - Start Time – when did the job start
  - Duration – how long did it take
- From the Results tab you can double-click any job to view the details of the job as well as the job results for each instance of that job

Reviewing Job Results Detail



1. Once the job is opened you can click ‘Results’ to view the results from each time the job was ran, along with the details
2. Click the triangle to expand the task results
3. Click the triangle again to view the details of each task, including more details of any error messages or output detail

Interpreting Scheduler Messages

- NOTE - Scheduler messages are often warnings or notifications. They are not always error messages
  - The message either provides an explicit cause or at least good clues as to where the issue lies
  - Messages will often mirror the messages received when running the file manually
    - This includes report processing and import processing errors

Recommended Troubleshooting Steps

- Troubleshoot in the **Windows Client**,
  - All scheduled jobs run using the Windows Client as a process engine
- Run the file(s) from the job manually by opening the source file and running it as scheduler does (Multipass, Save2DB, etc.)
  - Scheduled jobs that run report or import processing will often return the same message when running the file outside scheduler
  - Running the source file provides you the tools to resolve the issue
- If the file(s) run successfully outside of scheduler, we then need to look at other causes
- If the job ran successfully before, check to see if any recent changes have been made to either the job or the source files accessed by the job

Scheduler Best Practices

- Break up large jobs
  - It can be difficult to both diagnose and support large jobs
  - Breaking up large jobs will put less stress on the system
  - Smaller jobs may complete successfully so you have results to review
- When and how to schedule large jobs
  - Recommend running large scheduled jobs after hours when users are not in the system
  - Look at other scheduled jobs and timing to minimize overlapping times which may cause unexpected delays in results
    - Include the schedule for nightly system\network backups or scheduled downtimes

SYNTELLIS

Axiom Upgrades & Updates

When and how to apply

Axiom Upgrades & Updates

- **Platform** – Always applied during any product upgrade
  - Upgrade – Move to a new version such as 2020.1 or 2020.2
  - Update – Interim patches between upgrades
  - Confirm backwards compatibility with your technical services team member
- **Product upgrades** – Specific to industries such as Healthcare, Financial Institutions and Higher Education receive product updates
  - Upgrades are product specific
  - Product upgrades can be selective

How To Upgrade

- Contact Support
  - Log a case with Syntellis Central
  - Send an email to Support@Syntellis.com
    - Include “TAM Upgrade Request” or “TAM Update Request” in the subject line

- Syntellis technical services will confirm:
  - Timing of upgrade
  - Length of expected down time
  - Platform version to be applied
  - Product(s) to be updated

Upgrade Process

- **Production vs Sandbox (Test) System**
  - Copy Production to Sandbox
  - Upgrade Sandbox
  - Client to review upgraded Sandbox
  - Contact Support to upgrade Production
  - Upgrade Production
  - Client to review upgraded Production
  - Confirm upgrade complete
- **Client Responsibilities**
  - Provide appropriate business and technical resources
  - Read and Review platform and product release notes
  - Review upgraded systems
  - Confirm upgrade is completed

When To Upgrade

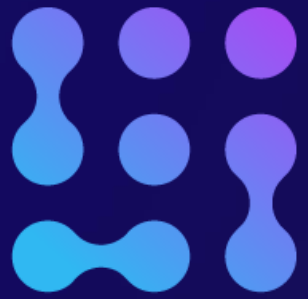
- **Timing**
  - Prior to the start of a planning process such as Financial Planning, Capital Planning or Budgeting
  - Beginning of a new fiscal year
  - Recommend upgrading as often as possible but at least 1-2X per year to stay current

Questions and Answers

Please send suggestions for future webinars to

ClientRelations@syntellis.com

(Note new email address)



SYNTELLIS

ELEVATING PERFORMANCE