Site Administration Best Practices

Get Familiar with the Site Hierarchy

NocTel Insight navigation once logged in encompasses a simple content hierarchy: **Projects > Workbooks > Reports/Worksheets**

Projects are the highest order of the content hierarchy. By default, Insight provides several (where applicable) projects with your Site:

- NocTel Operations: Where NocTel hosted voice standard reports and Workbooks are located
- Flow Operations: Where NocTel Flow hosted contact center standard reports and Workbooks are located

Workbooks are collections of reports/Worksheets that generally encapsulate a focus, such as a Workbook containing generalized summary reporting for the Site or a Workbook that specifically reports on activity regarding Phone Numbers on the Site. Each Project can have many Workbooks associated with it, but Workbooks can only be associated with a *single Project*. Reports within the same Workbook can be conveniently navigated via tabs displayed in the open report. *Cross Workbook tabs do not exist* and requires the user navigates to the appropriate Workbook or report.

Reports/Worksheets are published as part of a Workbook and what end users ultimately view. If the open report is one of several published to the same parent Workbook, the user can navigate conveniently between reports via tabs. Reports are published specifically to a single Workbook. This means it's possible for there to be reports with the same name, but associated with different Workbooks. These are *distinctly different reports* and have no relation to one another directly.

Users and Groups

Aside from the content hierarchy described above, users in the Site can also be assigned to created Groups. Groups are a convenient way to give standard permissions to users to various content. An example of this application might be having a Phone System group and a Call Center group. Managers of the Call Center group really only have an interest in the Flow reports and the NocTel hosted voice data is out of their scope of interest. The Call Center group's default permissions would include access to the Flow Operations project and any Workbooks and reports published within it, but no access to the NocTel Operations project. The non-call center users, the inverse might be true: they only need access to the NocTel Operations project and no access to the Flow Operations project and content.

However, exceptions do exist. When there is a specific user that shouldn't be given blanket or standard permissions in Groups, individual user permissions can be applied to the content hierarchies.

How Permissions are Applied

While we have defined two separate hierarchies - one for users and the other for content - the two are applied in different ways.

For users, the individual user permissions, if any, are given precedence over any Group assignment. This applies both to exceptions for inclusion as well as *exclusion*.

For content, unless permission is set at the Project level and blanketed down, users and Groups must have sufficient permission working down the hierarchy. For example, User A might have access to Project X that has Workbooks 1 and 2 in it. However, User A only has permission set for Workbook 1. This means User A would be able to navigate into Project X but would only see Workbook 1 and not both 1 and 2. This same example works similarly at the Workbook and report/Worksheet level. A User who has access to a Workbook may not access to all the reports/Worksheets within.

Permission Example Exercises

This section provides some practical examples for permissions to help illustrate how a Site Administrator may choose to administer access permissions for users.

For this section, we presume the following:

- There are two projects: **Ops** and **Analysis**
    - The Ops Project has one Reporting Workbook called **History** with three reports contained in it
    - The Analysis Project has two Reporting Workbooks with two reports in each. Call these Reporting Workbooks **Public** and **Private**.
- There are three users: **John, Troy, and Anna**
- There are two user Groups to start with the following user assignments: **Ops Users** (John) and **Analysis Users** (Troy, Anna)
    - **Ops Users** has permission to access all the Reporting Workbooks and reports published inside of the **Ops** Project
    - **Analysis Users** has permission to access *only* the **Public** Reporting Workbook under the **Analysis** Project

These users and reporting resources are fictitious!

Scenario 1: Anna Needs Exclusive Access to the Private Reporting Workbook in the Analysis Project

In this situation we must give access to a Workbook that none of our users has access to originally.

There are two simple methods of solving this problem:

1. We make a third user Group called **Analysis Private** that has access specifically to the **Private** Reporting Workbook under the Analysis project. We then assign Anna to this Group while keeping her a member of the Analysis Users Group. This is a good option if we expect the number of analysts to grow in the future and do not want to administer multiple individual users - particularly if scope of role changes over time.
2. We modify the **Private** Reporting Workbook specifically and create a user permission set for Anna giving her access. This means we've made an exception for Anna and not Troy.

Scenario 2: Anna Needs Access to a Specific Report in the History Reporting Workbook of the Ops Project

Like the previous scenario, there are a few solutions:

1. Add Anna to the Ops Users Group. However, because Anna does not need access to the other two reports published under the History Reporting Workbook, this overreaches what permissions are really needed. If we reasonably expect Anna will need access to the other reports in this Reporting Workbook, it's not a particular concern. Otherwise this solution violates the notion of least privilege, which is often the basis used in infosec audits.
2. Create a user exception for Anna on the specific report she needs access to within the History Reporting Workbook. We do not need to set exceptions for Anna at the Ops Project or History Reporting Workbook levels.

You may have realized we could have gotten the same result if we had modified the report in question to be available to the Analysis Users Group. This is certainly valid, but brings along the same concerns and considerations as the first solution does: it creates overreach of permission, which may be undesirable depending on your organization and the definition of roles.

Scenario 3: Troy Transfers Departments to Operations and Replaces John Who is Leaving the Company

Since John is transferring elsewhere and won't be working as a Business Analyst, we need to make sure that permissions are assigned appropriately.

The solution here is simple:

- Compare what John has permissions to access now and create the same settings for Troy. Most obvious of these changes would be adding John to the Ops Users Group.
- Deactivate and Delete John's user account from Insight to prevent erroneous license utilization.

While this is a simple scenario, it illustrates a best practice: make sure that you don't create gaps in terms of who can access what. Without practicing due diligence to make sure one user transitions (or a new user is brought in) well, you can create gaps and potentially orphaned reporting that none of your users knows exists. Worse, if employees are exiting it is standard best practice to ensure accounts and access to privileged and proprietary data are closed out to prevent exited employees potential insider threats. If John's account was not deleted or otherwise modified to prevent his access upon leaving the company, he could still potentially access the organization's reporting content.