Learning About DataDental Security

Overview

Before you begin to use DataDental, you must secure your DataDental environment by specifying the appropriate user access privileges.

What are Access Privileges?

Access privileges are specifications that allow a user, or a group of users who do similar tasks, to perform certain operations from various DataDental modules. For example, you may want to define a set of access privileges to grant full access to the Member module, but allow the same users to only view information from the Group module. Or, you may want to specify another set of access privileges to make sure that only a few, experienced users can perform security or other administrative functions.

How Does DataDental Security Work?

To provide the greatest amount of flexibility, DataDental allows you to establish several levels of access privileges that are appropriate for your user community.

- **Login access**
  A user can only gain access to DataDental if the user ID and password required for the user to access the server on which DataDental is installed exists in a DataDental security profile.
- **DataDental module access**
  A user can gain access to a DataDental module only if they have been granted the appropriate access privilege for that module.
- **Module activity access**
  When you grant user access privileges to a particular module, that user can perform all activities available within that module. However, you can define the appropriate access privileges for just those module activities that you want the user to be able to perform.
- **Deny activity access**
  Once access privileges are granted to modules and activities, you can deny access to those activities that you do not want a particular user or group of users to perform.

In addition, DataDental allows you to use templates and profiles to help you define adequate security for your users without having to define individual specifications for each user.

What is a Security Template?

A *security template* is a profile you define that specifies the access privileges that apply to most or all of your users. For example, perhaps you want all of your users to view information about groups and members, but you do not want them to be able to add new or change existing information in the Group or Member modules. You can define a template that specifies view-only access privileges to the Group and Member modules. You can then copy the template to quickly create new group profiles.

What are Group Profiles?

DataDental allows you to define access privileges for groups of users with similar processing needs. A *group profile* contains the common access privileges needed by a particular group of users. Once defined, you can assign individual users to the group profile. Each user associated with the group profile automatically picks up the access privileges defined for the group.

What are User Profiles?

User profiles identify an individual user's logon ID and identify the group profile with which the individual is associated. User profiles may also contain additional access privileges if the user requires some type of access that is unique to the group. On rare occasions, you may need to define a complete set of unique access privileges for an individual user. You can create a user profile that is not associated with a group profile to define this standalone set of access privileges.

What is Supervisor Access?

Some users require access to all DataDental modules and activities, regardless of the user group to which they belong. You can quickly designate any user as a *Supervisor*, who has unlimited access to DataDental, including the ability to modify another user's security profile.

What is Group Supervisor Access?

If one or more users within a particular user group need to search for action items either assigned to or by someone in another user group, you can grant them *Group Supervisor access*.

Defining User Security

Overview

To ensure that users may access only those modules and activities you specify, you must define security for DataDental users. Several steps are involved in this process:

- Step 1: Identify your security requirements
- Step 2: Create a security template (or a group profile)
- Step 3: Grant module and activity access privileges
- Step 4: Copy a group profile from a security template
- Step 5: Create a user profile

Tip DataDental's Security module is quite flexible and allows you to define security in several ways. However, if you are a new DataDental Administrator learning how to define security for your user community, STC recommends completing these steps in the order listed above.

Step 1: Identify Your Security Requirements

The following suggestions are provided to help you research and identify the DataDental security requirements that are appropriate for your business.

- **Identify global access privileges**
  Identify the modules and activities that need to be accessed by all of your users. These are the global requirements to specify in one or more security templates.

- **Identify user groups and their unique access privileges**
  Identify groups of users with similar processing needs, and then identify the modules and activities each user group needs to access. These are the group profile requirements to specify in addition to the global settings copied from security templates.

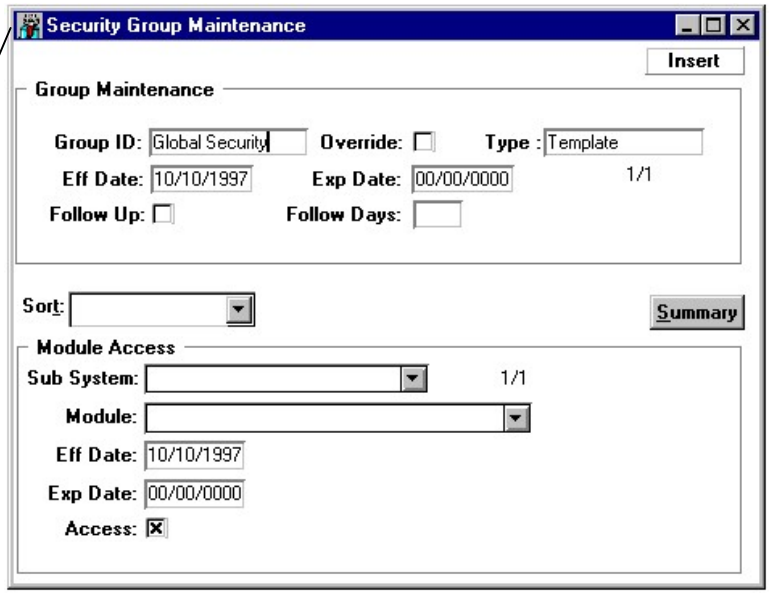
  Tip To get your DataDental system up and running quickly, you can start with three basic user groups: Administrators, Supervisors, and General Users. You can then add more user groups later, as necessary.

- **Identify individual users and their unique access privileges**
  Identify individual users and the groups with which they should be associated. In addition, identify whether or not certain users require additional access, and which users should be designated as DataDental Supervisors or Group Supervisors.

Step 2: Create a Security Template

You can define your global access privileges in a security template, and then copy the template to create other security profiles.

Use the Security Group Maintenance window to define a security template or a group profile



▶ To create a security template

Tip You can also use this procedure to create a user group profile. If you do, you do not need to subsequently copy the template to a group profile, as described in "Step 4: Copy a Group Profile."

Before you begin:

✓ Complete "Step 1: Identify Your Security Requirements"

1 On the **Modules** menu, point to **System Administration**, then point to **Security**, and then click **User Groups**. The Security Group Maintenance window appears.

Insert tool

2 On the Security Group Maintenance toolbar, click **Insert**

3 In the upper portion of the window, fill in security template information (for more information, see "About User Group Security Fields" after this procedure).

Save tool

4 On the Security Group Maintenance toolbar, click **Save**. The security template is saved, and the Security Group Maintenance window remains in Insert mode so you can specify another template or a user group profile.

5 Continue to Step 3, "Grant Module and Activity Access Privileges."