



Proficiency Plant Applications 2022

Security Management



Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2022, General Electric Company. All rights reserved.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Table of Contents

Security Management Node.....	4
Security Management Overview	4
Terms	4
Site User	4
Security Role.....	5
Security Groups	5
Access Rights	5
Entities.....	5
Security Groups	5
Administrator Security Group	6
User-Defined Security Groups.....	6
Display-Level Variable Security	6
Access Levels and Privileges	6
Creating User-Defined Security Groups.....	6
Importing Security Groups.....	7
Exporting Security Groups.....	7
Assigning Site Users to a Security Group	8
Site Users.....	8
Setting Up Users and Authentication	9
Managing Domain Names	10
Adding Site Users.....	10
Editing Site Users	12
Exporting site users	13
Assigning site users to a security group.....	14
Viewing Windows Domain Group Membership.....	15
System Users.....	15
AlarmMgr Parameters	16
Role-based Security.....	16
Step 1: Create role-based site user in Plant Applications	16
Step 2: Create Security Role	17
Step 3: Assign Windows Domain Group to Security Role	17
Step 4: Assign Security Role to Security Group	17


Creating a Role-based Site User.....	17
Creating Security Roles.....	18
Adding Members to a Security Role.....	18
Assigning site users to a security group.....	19
Exporting Security Roles.....	19
Importing Security Roles.....	20
Assigning Security Groups.....	20
Access Levels.....	21
Administrator Access.....	21
Administrator Access in the Administrator Security Group.....	21
Administrator Access in a User-defined Security Group.....	21
Manager Access.....	21
Manager Access in the Administrator Security Group.....	21
Manager Access in a User-defined Security Group.....	21
Read/Write Access.....	21
Read/Write Access in the Administrator Security Group.....	21
Read/Write Access in a User-defined Security Group.....	21
Read Access.....	22
Read Access in the Administrator Security Group.....	22
Read Access in a User-defined Security Group.....	22
Changing Access Levels.....	22
Access Levels and Privileges.....	22
Display Security Rules.....	46
Access Levels and Privileges for Client Displays.....	47
Alarm Display.....	47
Autolog Display.....	47
Downtime Display.....	48
Geneology View.....	48
Production Overview Display.....	48
Production Run Analyst (also known as "Operator Display").....	49
Relative View Display.....	49
Schedule View:.....	49
Sequence of Events Display.....	50

Security Management

Trend Displays	50
DT+ and WebUI Displays	50
Security Site Parameters	50
DefaultDomainName Site Parameter	51
Domain User Creation Site Parameter	52
WindowsAuthentication Site Parameter	52
UseDisplaySecurity Site Parameter	53

Security Management Node



 **Security Management** is where you add and maintain site users, roles, and security groups, and where you assign access rights to the members of a security group.

- From **Site Users**, you add and manage site users. Before anyone can have access to Plant Applications, they must first be added as a site user.
- From **System Users**, you edit the parameters of system users, which represent services or functions within Plant Applications.
- From **Security Groups**, you create and manage security groups and security group membership.
- From **Security Roles**, you create and manage security roles and security role membership.

Security Management Overview

Security Management enables you to control access to Plant Applications and to control and monitor changes to your Plant Applications display data. Additionally, Security Management is where you assign access rights to the members of a security group. Once your security groups are created, you can then assign one of the security groups to variables, specifications, production units, production lines, and displays.

NOTE: In order to configure security in Plant Applications, you must have Administrator access in the **Administrator security group**.

Before anyone can log in and use the Plant Applications Administrator, they must be added as a site user and be made a member of the Administrator security group.

IMPORTANT: If you do not assign a security group to an entity in Plant Applications, any Plant Applications user has the equivalent of [Manager access](#) to that [entity](#).

To set up and administer security in Plant Applications, you must follow these steps:

1. [Create a security group.](#)
2. [Determine the type of authentication, and set site parameters.](#)
3. [Create a site user.](#)
4. [Assign the site user to a security group.](#)
5. [Assign the security group to an entity.](#)

Terms

Site User

A site user is anyone who has been granted access to Plant Applications. You can add site users either manually or you can import your Windows users. Before anyone can do anything in Plant Applications, they must be added as a site user.

Security Role

A security role is the equivalent of a Windows (NT) domain group. You can either mirror your existing domain groups or you can create new security roles. Once a security role is created, you assign members to that security role. Members can be either domain groups or individual site users. For a site user to be assigned to a security role, they must first be identified as [role-based site users](#).

Security Groups

There are two types of security groups: the Administrator security group and user-defined security groups. The Administrator security group is created by default, and members of this group have unique privileges.

You can define any number of other security groups within Plant Applications. Once you have defined your security groups, site users or roles are made members of the various groups, with each site user or role being given specific rights in the group.

Access Rights

When a site user or role is made a member of a security group, you assign rights that determine what that site user or role can do. Members of the Administrator security group have special privileges, which are determined by the rights assigned to them.

Entities

With the proper access level in the Administrator group, you can apply security to the following entities:

- **Reasons:** Must have Administrator access in the Administrator group to apply security to Reasons.
- **Trees:** Must have Administrator access in the Administrator group to apply security to Trees.
- **Displays:** Must have Administrator or Manager access in the Administrator group to apply security to Displays.
- **Views:** Must have Administrator or Manager access in the Administrator group to apply security to Views.
- **Product Families:** Must have Administrator access in the Administrator group to apply security to Product Families.
- **Properties:** Must have Administrator access in the Administrator group to apply security to Properties.
- **Production Lines:** Must have Administrator access in the Administrator group to apply security to Production Lines.
- **Production Units:** Must have Administrator access in the Administrator group to apply security to Production Units.
- **Variable Groups:** Must have Administrator access in the Administrator group to apply security to Variable Groups.
- **Variables:** Must have Administrator or Manager access in the Administrator group to apply security to Variables.

Security Groups

In Plant Applications there are two types of security groups: [Administrator](#) and [user-defined](#). This section provides information about these two security groups, how to create them, and how to assign users to the groups.

Administrator Security Group

Access to the Plant Applications Administrator is controlled by the **Administrator** security group. Plant Applications users need at least **Read** access to the Administrator security group in order to access the Plant Applications Administrator. The Administrator security group is created by default when you first install the Plant Applications client applications. This special security group can not be deleted.

Even though you can assign the Administrator security group to Plant Applications [entities](#) (such as variables and displays), we recommend that you use the Administrator group only to control access to the Plant Applications Administrator program. This way, you can more easily control and monitor who has access to the Administrator program.

User-Defined Security Groups

You can create as many user-defined security groups as you need, and you can add as many members to each group as you need. After you've created your user security groups and defined the membership, you can assign a group to a Plant Applications [entity](#) (such as, variables and displays).

Display-Level Variable Security

A site parameter, [UseDisplaySecurity](#), enables you to defer variables with a designation of No Security Group to a display-level security group. When set to False, the default, variables (for example, in Autolog sheets) use variable-level security settings and when no security is assigned a default is used. When set to True, the security set for the display applies to all variables in the display that do not have variable-level security defined. Security for variables can now be set by changing the security for the display, thus avoiding having to set the security for each variable. Rights assigned at the variable level override rights at the display level.

Security for variables affects whether a user has rights to enter or change variable data. It also affects what variables can be accessed during a calculation or by the historian, which normally requires administrative privileges. Privileges can now be set at the display level to override default privileges for variables having no security group assigned.

Access Levels and Privileges

You can assign one of four access levels to a member of a user-defined security group. The access level determines what the user can do, depending on the entity to which the user group is assigned.

For a complete list of access levels and privileges, please see [Display Access Levels and Privileges](#).

Creating User-Defined Security Groups

User-defined security groups are used to control access to various [entities](#) and displays within the Plant Applications Client program. You can create as many security groups and assign as many members to those groups as you need.

There are two ways to add security groups to Plant Applications. You can either create new security groups, or you can import security groups from a different Plant Applications server. For more information about Proficy Workflow and Proficy Vision security, refer to the documentation for those products.

To create a new security group

Security Management

1. Expand  **Security Management**.
2. Right-click **Security Groups** and click **New Security Group**. An editable field is created inside the folder.
3. Type in the name of the new security group and press ENTER.

On each Plant Applications server, your security group names must be unique.

5. Assign members to the new security group. [How?](#)

To import a security group

1. Open the Excel workbook that contains the [exported security group](#)'s configuration information.
2. In the Excel workbook, under the **Selected** column, type an **X** in the cell that corresponds to the items that you want to import.
3. In the Plant Applications Administrator, expand  **Security Management**.
4. Right-click **Security Groups** and click **Import Configuration**.
5. Click **OK** to complete the import.
6. Refresh the server to see the new imported security group.

Importing Security Groups

You can import security groups from another Plant Applications server. Along with the security group name, the security group members and their access levels are also imported.

Before you import security groups, you will need to first [import the site users](#).

*You must have **Administrator access** to the Administrator security group to import security groups.*

To import security groups


1. Open the Excel workbook that contains the security group information.
2. In the **Selected** column, place an **X** in the cell that corresponds to the security group(s) you want to import.
3. Log in to the Plant Applications Administrator.
4. Open the **Security Management** folder.
5. Right-click on the **Security Groups** folder and select **Import Configuration**.
6. Click the **OK** button to complete the import.
7. Refresh the server.

Exporting Security Groups

You can export your security groups and then [import](#) them into another Plant Applications server. Along with the security group name, the security group members and their access levels are also exported into an Excel workbook.

*You must have **Administrator access** to the Administrator security group to export security groups.*

To export security groups

1. Log in to the Plant Applications Administrator.
2. Expand  **Security Management**.
3. Right-click on the **Security Groups** folder and select **Export Security Groups**. The **Export Configuration** dialog box appears



4. Click the **OK** button.

The export process will automatically open Excel and create the workbook.

5. Save your workbook.




Assigning Site Users to a Security Group

Members of a security group can be either individual site users or members of a [security role](#).

Anyone who needs access to the Administrator program, must be added to the Administrator security group.

*You must have **Administrator** access to the **Administrator** security group before you can edit the Administrator security group's membership.*

To assign members to a security group

1. In the Plant Applications Administrator program, expand  **Security Management**.
2. Expand **Security Groups**.
3. Right-click on the desired group and select **Edit <security group> Membership**. The **Edit Security Group Membership** dialog box appears.
4. Do one of the following:
 - To add members with the same access level:
 - a. In the **Non-Members** list, select one or more members to add to the Security Group.
 - b. Under **Access Level**, select the access level you want to assign to the selected members.
 - c. Click the **Move Selected**  button.
 - d. Close the **Edit Security Group Membership** dialog box.
 - To add members with different access levels:
 - a. In the **Non-Members** list, select one or more members to add to the security group.
 - b. Click the **Move Selected**  button.
 - c. Right-click on each member and select the access level.
 - d. Close the **Edit Security Group Membership** dialog box.

Site Users

Before anyone can have access to any of the applications in Plant Applications, they must first be added as a site user. If you are using security groups to control Plant Applications security, then you'll need to assign the site user to a security group.

NOTE: If you do not assign a security group to a Plant Applications *entity*, such as a Variable or Display, by default all site users have [Manager_access privileges](#) to that entity.


All Plant Applications site users are found inside the **Site Users** folder, which is located inside **Security Management**. When you click the **Site Users** folder, all of the site users are displayed in the right-hand pane. For each site user, the following information is displayed:

- **User Name:** This is the site user's name in Plant Applications.
- **User ID:** This is the identification number that Plant Applications automatically assigns to the site user. This number is unique to each site user.
- **User Description:** This is the description you enter when editing the site user's information in the **Edit User** dialog box. The description is optional.
- **Windows Login Info:** If the site user was imported from the network domain or aspected from Proficy Workflow, the Windows login information displays fully qualified domain name (FQDN) and domain user name in this format: **domainname\domainusername**. The domain user name does not have to be the same as the site user's name.

NOTE: For Windows authentication, new user accounts are automatically created when a new user logs in and assuming that the user is part of a valid group. If the *UseProficyClient* site parameter is set to "True," fully qualified domain names (FQDNs) are used for aspecting users. Refer to [Managing Domain Names](#).

- **Security Type:** The Security Type indicates whether the site user is a member of a role. **Security Group** indicates the site user must be added directly to a security group. **Role** indicates the site user must be added to a role (or has been automatically added to a role) before being added to a security group.
- **Login Mode:** **Login Mode** indicates how the site user is able to log in to Plant Applications. **Windows Login Only** indicates the site user must use their domain name and password to log in to Plant Applications. **Mixed Mode Login** indicates the site user can use either their domain name and password or their Plant Applications name and password to log in to Plant Applications.

TIP: If you do not see this information displayed in the right-hand pane, click the

[Description button](#)  on the **Server Manager** toolbar.

Setting Up Users and Authentication

Setting up authentication involves planning to determine what security credentials you want users to use to access the applications. Review the information in the following topics, which describe Plant Applications (Proficy) users, Windows (domain) users, mixed mode authentication, domain syntax, and aspecting users from Proficy Workflow or importing Windows users:

- [Managing Domain Names](#), including aspecting for Proficy Workflow and requirement for fully qualified domain names (FQDNs) for Windows authentication (domain users)
- Security Site Parameters: [DefaultDomainName](#), [DomainUserCreation](#), [WindowsAuthentication](#), [UseDisplaySecurity](#)
- [Site Users](#) and related topics for adding, importing from Excel or as Windows users, editing, and using FQDN

NOTE: Because you are mapping Windows (domain user) credentials to Plant Applications users (Proficy users), log in is not required for when logged in as a Windows user.

- [System Users](#) and ShowSystemUsersInAdmin site parameter
- [Security Groups](#), [Security Roles](#), and [Access Levels](#)

For more information about Proficy Workflow and Proficy Vision security, refer to the documentation for those products.

Managing Domain Names

Beginning with version 6.1.3, Plant Applications requires fully qualified domain names (FQDNs) for Windows authentication. This feature provides for users created through Proficy Workflow, which have fully qualified domain names (domain users), to be aspected (linked) to Plant Applications. In Plant Applications, the Windows (domain user) information is recorded in the [Windows Info field](#) for a user.

For FQDNs in Proficy Workflow to be linked with Plant Applications, the UseProficyClient site parameter must be set to "True." By default, new Plant Applications installations set the site parameter to "True." Setting the site parameter to "True" is typically encountered when upgrading from an earlier Plant Applications version that does not support the Proficy Workflow Client or when migrating to use the Unified Manufacturing Database. Once the UseProficyClient site parameter is set to "True," it cannot be changed to "False." Renaming of aspected items in the Plant Applications Administrator is permanently disabled.

NOTE: *With Windows authentication, new user accounts are automatically created when a new user logs in and assuming that the user is part of a valid group. If the UseProficyClient site parameter is set to "True," FQDNs are used.*

The Manage Domain Names utility is provided to change domain names associated with Plant Applications users. Use the utility to change the default domain for Windows users and to create FQDNs for domains defined by the short domain name. You can also use the utility to assign a new name to any domain name. The Domain Names utility is accessed by right-clicking on the Site Users folder or a user under Security Management and selecting Change Users Domain. The utility checks for correct format of DNS names and does not allow changes if the format is incorrect.

TIP: *If you changed the UseProficyClient site parameter to "True," a dialog presents a list of short domain names that must be changed to FQDNs. Use the Change Users Domain utility to change the short domain names to a FQDN by picking the short name from the drop-down **Domain Names** list.*


Adding Site Users

In order to grant access to Plant Applications, you must create a site user. Site users can be added in three ways:

- You can manually add them
- You can import current operating system users
- You can import existing Plant Applications users

NOTE: *If you have existing Plant Applications users, create users of the same name in the Proficy (Workflow) Client and ensure that passwords are the same. If you create users in the Proficy Client, they are automatically aspected to the Plant Applications data model for viewing in the Plant Applications Administrator. Manually set the password in Plant Applications after a user is aspected to be the same as assigned in the Proficy Client.*


To manually add site users:

1. Expand  **Security Management**.
2. Right-click **Site Users** and click **Add New User**. An editable field opens under the Site Users folder.

Security Management


3. Type the name of the site user, and press Enter. User names can be a maximum of 30 characters. You can use any combination of special characters, such as & or #, and numbers and letters.
 4. Right-click on the site user and click **Edit <user name> Properties**. The **Edit User** dialog box appears.
 5. Edit one or more of the following:
 - **Short description**: Use this field to type a brief description to help you identify the site user, particularly if your company uses ID numbers for the site user's name.
 - **Password**: Use this field to add or change the site user's password. If you leave the password field blank, then anyone who knows a site user's user name can access Plant Applications. Passwords can be a maximum of 30 characters. You can use any combination of special characters, such as & or #, and numbers and letters.
 - **Windows Info**: Use this to copy the site user's Windows user account information. If you do, the site user will have to use their network name and password to log in to Plant Applications, unless the Mixed Mode option is selected. If the UseProficyClient site parameter is set to "True," you must use a fully qualified domain name (FQDN). Refer to [Managing Domain Names](#).
-
- NOTE:** *The WindowsAuthentication site parameter must be set to **True** to use the Windows Info feature.*
-
- **Default View**: Use this field to define a default view for a site user. When the site user logs in to the Plant Applications Client program, the default view automatically opens.
 - **Active**: In order for the site user to be able to log in to any of the Plant Applications programs, this option must be selected. If this option is not selected, the site user can not log in to any of the Plant Applications programs.
 - **Role-Based**: If this option is selected, the site user must be added to a role before being made part of a security group.
 - **Mixed Mode**: If this option is selected, the site user can log in to Plant Applications using either their Plant Applications user name and password or their Windows network user name and password, if it's been copied using the Windows Info field.
6. Click the **Close** button.

To import operating system users

1. Expand  Security Management.
2. Right-click Site Users and click Import Operating System Users. The Import Windows Users dialog box appears.
3. Do the following:
 - a. **optional**: Under **Available Domains**, select the desired network domain.
 - b. Under **Available Windows Users**, select one or more of the network domain users to import as Plant Applications site users.
 - c. **optional**: Under **Copy Security from User**, select the Plant Applications user whose security group membership and access level you want to copy.
 - d. Click **OK**.
4. The selected domain users are now added as Plant Applications site users.

When you use this method to add a site user to Plant Applications, the site user is automatically given a randomly generated password, which can not be viewed without accessing the SQL table. It is important that you [edit the site users'](#) information and change the password to something that you know and can remember.


To import existing Plant Applications site users:

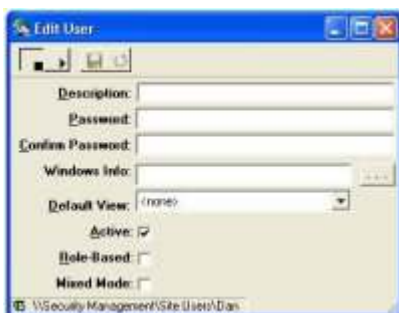
1. Open the Excel workbook that contains the [exported site user information](#).
2. In the workbook, under the **Selected** column, type an **X** in the cell that corresponds to the site users you want to import.
3. In the Plant Applications Administrator program, expand  **Security Management**.
4. Right-click **Site Users** and click **Import Configuration (From Excel)**.
5. Click **OK** to complete the import.
6. Refresh the server to see the imported site users.


Editing Site Users

Editing site users allows you to change the site user's profile in Plant Applications.

To edit a site user's profile


1. In the Plant Applications Administrator program, expand  **Security Management**.
2. Expand the **Site Users** folder.
3. Right-click on the desired site user and select **Edit <user name> Properties**. The **Edit User dialog box** appears.



4. Change any of the following fields:
 - **Description:** Type a brief description. You can use this field to help identify the site user or provide additional information about the site user. You are limited to 255 characters, including spaces and punctuation.
 - **Password:** Type a new password. If you are changing an existing password or typing a new password, you'll need to confirm the password in the **Confirm Password** field. Passwords are limited to 30 characters.
 - **Windows Info:** If you want to use the site user's Windows network user name and password to log in to Plant Applications, click the **Browse button**  to open the **Import Windows User dialog box**.

To use this dialog box, select the domain from the **Available Domains** drop-down list, and then select the user and click the **OK** button.



- **Default View:** To select a default view for the site user, click the drop-down arrow and select a view from the list. This view will be automatically loaded when the site user logs in to the Plant Applications Client program.
 - **Active:** This option is selected by default. If you do not want this site user to have access to any of the Plant Applications programs, remove the checkmark from the check box.
 - **Role-Based:** Select this option if you want this site user to participate in the [role-based security](#).
 - **Mixed Mode:** Select this option to allow the site user to use either their Plant Applications user name and password or their Windows network user name and password to log in to Plant Applications programs. If you have copied a Windows network user's information, and this option is not selected, then the site user must use their Windows network user name and password to log in to Plant Applications programs.
5. Click the **Close button**  to close the **Edit User** dialog box and to accept your changes.

Exporting site users

You can export site users into an Excel workbook, and then use this workbook as a source file for importing site users into Plant Applications, either on the same server or on a different server. If you import the site users back into Plant Applications on the same server, you will need to edit at least one of the selected site user's fields in the workbook.

The following columns are automatically created during the export:

- **Return Messages:** This column will display status messages after the import.
- **Selected:** This column is used to select the site user(s) you want to import. To select a site user, simply type an X in the appropriate cell.
- **User Name:** This column displays the Plant Applications site user's name.
- **User Description:** This column displays the site user's description, if there is one. A blank cell indicates that the site user has no user description.
- **Password:** On export, the cells in the column are blank, even if the site user has a password, in order to maintain the integrity of the Plant Applications security. If you want to include a password for a site user, simply type the password in the cell for the selected site user.
- **Active:** TRUE indicates that the site user is active. FALSE indicates that the site user is not active.

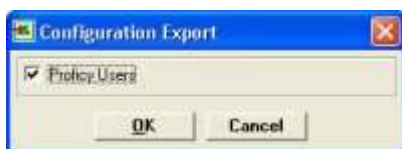
- **Default View:** The cells in this column will display the site user's default view. A blank cell in this column means that the site user has not been assigned a default view.
- **Windows User Info:** If the site user is based on a domain user, the domain name and domain user name will be displayed in the cells in this column.
- **Role-Based:** TRUE indicates that the site user is part of the role-based security. FALSE indicates that the site user is not part of the role-based security.
- **Mixed Mode:** TRUE indicates that the user can log in with either their domain name and password or their Plant Applications name and password. FALSE indicates that the user must log in with their domain name and password.

To export site users

1. Log in to the Plant Applications Administrator application.

*You must have **Administrator** access in the **Administrator** security group to export site users.*

2. Open Security Management.
3. Right-click on the **Site Users** folder and select **Export Site Users**. The **Configuration Export dialog box** appears.



4. Click the **OK** button.
5. Plant Applications will automatically create the Excel workbook.

Once the workbook has been created, you can change any of the data in the worksheet and the use the worksheet to import the information into Plant Applications on the same server or on a different server.


Assigning site users to a security group

Members of a security group can be either individual site users or members of a [security role](#).



Anyone who needs access to the Administrator program, must be added to the Administrator security group.

*You must have **Administrator** access to the **Administrator** security group before you can edit the Administrator security group's membership.*

To assign members to a security group

1. In the Plant Applications Administrator program, expand  **Security Management**.
2. Expand **Security Groups**.
3. Right-click on the desired group and select **Edit <security group> Membership**. The **Edit Security Group Membership** dialog box appears.
4. Do one of the following:
 - To add members with the same access level:
 - a. In the **Non-Members** list, select one or more members to add to the Security Group.

Security Management

- b. Under **Access Level**, select the access level you want to assign to the selected members.
 - c. Click the **Move Selected**  button.
 - d. Close the **Edit Security Group Membership** dialog box.
- To add members with different access levels:
 - e. In the **Non-Members** list, select one or more members to add to the security group.
 - f. Click the **Move Selected**  button.
 - g. Right-click on each member and select the access level.
 - h. Close the **Edit Security Group Membership** dialog box.

Viewing Windows Domain Group Membership

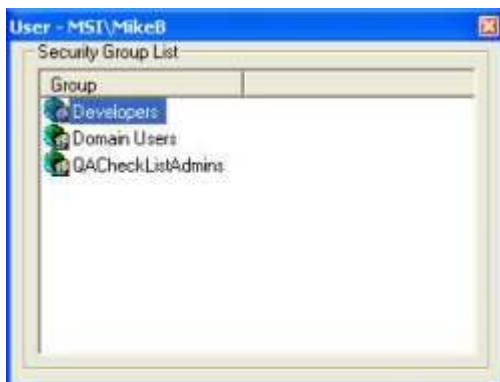
You can view the Windows domain groups a site user belongs to if the site user is:

- Participating in role-based security
- An imported Windows domain user

*You must have **Administrator** access to the Administrator security group to view a site users Windows domain group membership.*

To view Windows domain group membership

1. Log in to the Plant Applications Administrator.
2. Open the **Security Management** folder and then open the **Site Users** folder.
3. Right-click on the desired site user and select **View Windows user Group membership**. The **User <Windows username> dialog box** opens listing the Windows domain group(s) to which the site user belongs.



4. Click the **Close**  button to close the dialog box.

System Users

Plant Applications system users include users such as Event Manager, Database Manager, and Alarm Manager. These users have a User ID like the other users, but do not have any login credentials. When the ShowSystemUsersInAdmin site parameter is enabled, the system users are shown under **Security Management** in the **System Users** folder. Each user has a set of parameters that are applicable to the service or function they represent. Also useful are additional parameters that can be added and then set, such as **DebugMode** and **FullLogging**. These parameters provide the

same debug functionality that is now available through Plant Applications **Control Services (Server Management > Control Services)**.

To set the System User Parameter

1. Enable the **ShowSystemUsersInAdmin** site parameter. How?
2. Refresh the server.
3. Expand **Server Management**.
4. Expand **System Users**.
5. Right-click on the desired system user and select **Edit <system user name> Parameters**. The **User Parameters - <system user name>** dialog box appears.
6. Do one of the following:
 - **To edit an existing parameter:**
 - a. Double-click a parameter. The **Edit Parameter** dialog box appears.
 - b. Type a new value in the **Value** box.
 - **To add a new parameter:**
 - c. Click **Add**. The **Add Parameter** dialog box appears.
 - d. Type a value in the **Value** box.
7. Click **OK**.
8. Click the Close button to close the **User Parameters - <system user name>** dialog box.

AlarmMgr Parameters

There are parameters that can be edited that affect the AlarmMgr service.

- **AlarmVarSpecCacheSize:** This parameter specifies the number of product changes to store in the AlarmMgr var spec cache.
- **EmailspLocal:** When you configure alarms to send email notifications to a specific email group, you can write a custom stored procedure (spLocal) to pre-fill the Subject (varchar(7000)) and Content (varchar(7000)) of the email. The name of the stored procedure must be provided using site parameter EmailspLocal. When the AlarmMgr service sends an email for an alarm, the stored procedure identified by this site parameter will be run. The stored procedure is passed the AlarmId and EmailGroupId as inputs. For more information, see Configuring Alarms.

Role-based Security

As another method for managing security within the Plant Applications Administrator, role-based security allows you to integrate your network security configuration with the security in Plant Applications. When you assign a network security group to a Plant Applications Security Role, any new or existing site users can be automatically assigned to the same Security Role, if the site user is added as a role-based user.

In order to configure role-based security, you must be using a computer that is part of the domain and you must be logged on as a user of that domain.

Step 1: Create role-based site user in Plant Applications

First off, you need to decide if you want to use role-based security. Don't worry, it's not an "all or none" decision. You can have some site users participate in role-based security, while others don't

have to. And, you can always change your mind. Role-based security is very flexible. When you create a new Plant Applications site user, you simply select the **Role-Based** option. [Tell me how...](#)

Step 2: Create Security Role

Once you've decided to use role-based security, you will need to create Security Roles. [Tell me how...](#)

Step 3: Assign Windows Domain Group to Security Role

After creating Security Roles, you will need to edit the security role membership. This is where you assign Windows domain groups to your newly created Security Roles. [Tell me how...](#)

Step 4: Assign Security Role to Security Group

Now that you've created your Security Role and assigned Windows domain groups to the Security Role, you can assign the role to a security group. [Tell me how...](#)

Example:

For example, let us assume you have a domain group called **Bakery_ShiftC**, which consists of all employees who work Shift C on the Bakery line. You also have a domain group called **Bakery_Supv**, which consists of supervisors on the Bakery line. Supervisor Bob works during Shift C and is also a supervisor. Therefore, he is a member of both domain groups. Let us further assume that you have created a Security Role named, **Role_Bakery_ShiftC**, and you assign the domain **Bakery_ShiftC** to it. You create another Security Role named, **Role_Bakery_Supv**, and you assign the domain group **Bakery_Supv** to it. When you add Supervisor Bob to Plant Applications as a role-based site user, Supervisor Bob would automatically be assigned to any Security Group that has **Role_Bakery_Supv** or **Role_Bakery_ShiftC** assigned as a member.

Keep in mind that every role-based site user who belongs to one of the Windows domain groups will be part of the security group to which the Security Role belongs. What this means is that if you create a role-based site user who is a member of two Windows domain groups, and then add the two domain groups to Security Roles, that site user is automatically a member of any security group to which the Security Roles have been assigned.

Creating a Role-based Site User

Before a Plant Applications site user can be made a member of a Security Role, they must be identified as a **role-based** site user.



NOTE: For more information about Proficy Workflow and Proficy Vision security, refer to the documentation for those products.

You must have **Administrator access** in the Administrator security group to create a role-based site user.

If a site user is a member of any Security Groups, changing that site user to a role-based user will remove the site user from those Security Groups.

To create a role-based site user

1. Log in to the Plant Applications Administrator program.
2. Open **Security Management**.
3. Open the **Site Users** folder.
4. Right-click on a site user and select **Edit <user name> Properties**. The **Edit User** dialog box appears.

5. Select the **Role-Based** option.
6. Click the **Save**  button.
7. Click the **Close**  button to close the dialog box and to accept your changes.

To change multiple site users to role-based

1. Log in to the Plant Applications Administrator application.
2. Open **Security Management**.
3. Right-click on the **Site Users** folder and select **Export Site Users**. The **Configuration Export** dialog box appears.
4. Click the **OK** button.
5. Plant Applications will automatically create the Excel workbook.
6. In the Excel workbook, for each site user you want to change to role-based, change the value in the **Role-Based** column from **FALSE** to **TRUE**.
7. In the **Selected** column, type an **X** in the cell that corresponds to each site user you want to change.
8. Go back to the Plant Applications Administrator program.
9. Right-click on the **Site Users** folder and select **Import Configuration**.
10. Click **OK** to complete the import.
11. Refresh the server.

Creating Security Roles

It might be helpful to think of Security Roles as being somewhat similar to site users, in that you create Security Roles and then assign Security Roles to a Security Group. After you create a Security Role, you need to attach a Windows domain user group to the role. Keep in mind that after you attach the Windows domain user group to the Security Role, every role-based site user who is a member of the Windows domain user group will be a member of the Security Role and will be a member of any Security Group to which the Security Role belongs.

You must have Administrator access in the Administrator security group to create roles.

A role cannot have the same name as a site users.

To create a role


1. After logging in to the Plant Applications Administrator program, open **Security Management**.
2. Right-click on the **Security Roles** folder and select **Add New Security Role**.
3. Type the name of the new Security Role and press ENTER.

Adding Members to a Security Role



You can add individual site users to a security role, or you can attach a domain user group to security role. If you attach a domain user group to a security role, every role-based site user who is a member of the domain user group will automatically be a member of the security role.

You must have Administrator access in the Administrator security group to add members to a security role.

To add members to a Security Role

1. Log in to the Plant Applications Administrator program and expand  **Security Management**.
2. Expand **Security Roles**.
3. Right-click on a security role and click **Edit <security role> Membership**. The **Edit Security Role Membership** dialog box appears.
4. Select one or more members from the **Non-Members** list.

This list will contain both domain user groups and individual role-based site users.

5. Click the **Move Selected**  button to move the selected non-members to the **Members** list.
6. Click the **Close**  button to close the dialog box and accept your changes.




Assigning site users to a security group

Members of a security group can be either individual site users or members of a [security role](#).

Anyone who needs access to the Administrator program, must be added to the Administrator security group.


*You must have **Administrator** access to the **Administrator** security group before you can edit the Administrator security group's membership.*

To assign members to a security group

1. In the Plant Applications Administrator program, expand  **Security Management**.
2. Expand **Security Groups**.
3. Right-click on the desired group and select **Edit <security group> Membership**. The **Edit Security Group Membership** dialog box appears.
4. Do one of the following:
 - To add members with the same access level:
 - a. In the **Non-Members** list, select one or more members to add to the Security Group.
 - b. Under **Access Level**, select the access level you want to assign to the selected members.
 - c. Click the **Move Selected**  button.
 - d. Close the **Edit Security Group Membership** dialog box.
 - To add members with different access levels:
 - e. In the **Non-Members** list, select one or more members to add to the security group.
 - f. Click the **Move Selected**  button.
 - g. Right-click on each member and select the access level.
 - h. Close the **Edit Security Group Membership** dialog box.

Exporting Security Roles

To export security role configuration

1. In the Plant Applications Administrator, expand  **Security Management**.
2. Do one of the following:


- a. To export all security roles and members, right-click **Security Roles** and select **Export Configurations**. The **Configuration Export** dialog box appears.
 - b. To export a specific security role and its members, expand **Security Roles**, right-click a security role and select **Export Configurations**. The **Configuration Export** dialog box appears.
3. Ensure **Plant Applications Security Roles** is selected and click **OK**. Excel automatically creates a worksheet containing the security role configuration.

Importing Security Roles

After you export your security role configurations, you can edit the information and import the changes into any Plant Applications server. If you edit the security role, a new role with the associated security role member is created. If you edit the security role member or security group description of an existing security role, a new security role member and security group are created. You can create a new role, members and group by adding a new row to the worksheet.

Action	Result
Add or edit a security role	A new security role is created
Add or edit a security role member	A new security role member is created and is a member of the associated security role.
Add or edit a security group	A new security group is created with the associated security role as a member.
Edit access level	If only access level is change and the change is imported back into the source Plant Applications server, no change is made. If the change is imported into a different Plant Applications server, the security role has the new access level.

To import security role configurations

1. Ensure the worksheet with the security role configurations is open and the configurations to import are selected.
2. In the Plant Applications Administrator, expand  **Security Management**.
3. Right-click **Security Roles** and select **Import Configuration**. Your selected configurations will be imported.
4. Click **OK** and refresh the server.

Assigning Security Groups

Assigning security groups to the various entities in Plant Applications is optional. However, assigning a security group will help protect your valuable data from unauthorized changes. If you do not assign a security group, then by default, any site user has [Manager access](#) to the entity.

To assign a security group

1. In the Plant Applications Administrator, select the [entity](#) to which you want to assign a security group.

Security Management

2. Right-click on the entity, and click **Change <entity> Security**. The **Object Security** dialog box appears.
3. Select the security group from the drop-down list.
4. Click the **Close** button.

Access Levels

Administrator Access

Administrator Access in the Administrator Security Group

Administrator access in the Administrator security group provides unlimited access to all Plant Applications programs. Therefore, it is very important that the number of people given this level of access be limited.

For a complete list of privileges, please see [Access levels and privileges in the Administrator](#).

Administrator Access in a User-defined Security Group

Administrator access in a user-defined security group provides you with full access to all the functions in each of the Plant Applications displays, which are accessed through the Plant Applications Client program. For a complete list of display privileges, please see [Display Access Levels and Privileges](#).

Additionally, Administrator access in a user-defined security group provides limited access to functions in the Plant Applications Administrator. For a complete list of privileges, please see [Access levels and privileges in the Administrator](#).

NOTE: A user must be a member of the Administrator security group to have access to the Plant Applications Administrator.

Manager Access

Manager Access in the Administrator Security Group

For a complete list of privileges, please see [Access levels and privileges in the Administrator](#).

Manager Access in a User-defined Security Group

If a user has manager access in a user-defined security group, that user's privileges in the Plant Applications Administrator are governed by the user's access level in the Administrator security group. For a complete list of display privileges, please see [Display Access Levels and Privileges](#).

NOTE: A user must be a member of the Administrator security group to have access to the Plant Applications Administrator.

Read/Write Access

Read/Write Access in the Administrator Security Group

For a complete list of privileges, please see [Access levels and privileges in the Administrator](#).

Read/Write Access in a User-defined Security Group

If a user has read/write access in a user-defined security group, that user's privileges in the Plant Applications Administrator are governed by the user's access level in the Administrator security group. For a complete list of display privileges, please see [Display Access Levels and Privileges](#).

NOTE: A user must be a member of the Administrator security group to have access to the Plant Applications Administrator.

Read Access

Read Access in the Administrator Security Group

For a complete list of privileges, please see [Access levels and privileges in the Administrator](#).

Read Access in a User-defined Security Group

If a user has read access in a user-defined security group, that user's privileges in the Plant Applications Administrator are governed by the user's access level in the Administrator security group. For a complete list of display privileges, please see [Display Access Levels and Privileges](#).

NOTE: A user must be a member of the Administrator security group to have access to the Plant Applications Administrator.


Changing Access Levels

After you've added members to a security group, you can change a member's access level in a couple of different ways. You can either edit the user or you can edit the group. If you edit the user, you can change the access level for each group the user belongs to. If you edit the group, you can change the access level for each member of the group.

To edit the user's access level

1. In the Plant Applications Administrator program, open the **Security Management** folder.
2. Open the **Site Users** folder.
3. Right-click on a site user, and select **Edit User Membership**. The **Edit User Membership** dialog box appears.
4. In the **Members** list, right-click on the group that you want to change the access to, and select the appropriate access level from the pop-up menu.
5. To change access levels in other groups, repeat step 4.
6. Close the **Edit User Membership** dialog box.

To edit a group member's access level

1. In the Plant Applications Administrator program, open the **Security Management** folder.
2. Open the **Security Groups** folder.
3. Right-click on the group and select **Edit Security Group Membership** from the pop-up menu. The **Edit Security Group Membership** dialog box appears.
4. Right-click on the member whose access level you want to change and select the appropriate access level from the pop-up menu.
5. To change the access levels for other members of the group, repeat step 4.
6. Click the **Close button**  to close the **Edit Security Group Membership** dialog box.

Access Levels and Privileges

You must be a member of the **Administrator** security group in order to have access to the Plant Applications Administrator program. There are five levels of security that control access to the

Security Management

functionality in the Plant Applications Administrator. The five levels, listed in order of greatest access to least access, are as follows:

1	Administrator access to the Administrator security group.
2	Manager access to the Administrator security group.
3	Administrator access to a user-defined security group and Read/Write or Read access to the Administrator security group.
4	Read/write access to the Administrator security group.
5	Read access to the Administrator security group.

IMPORTANT: Administrator access to the Administrator security group allows unlimited access to all the functions and features in Plant Applications. Therefore, it is important to limit the number of users who have this level of access.

If a user is a member of the Administrator security group and a user-defined security group that is assigned to an entity in the Administrator, the user's access rights are determined by the access level in the Administrator security group, except when the user has Administrator access to the user-defined security group. If the user has any access level other than Administrator access to a user-defined security group, the user's access rights are determined by the access level of the Administrator security group. This only applies to the entities that have been assigned a user-defined security group.

The following table lists all of the available commands and the access level required to perform the command.

	1	2	3	4	5
Global Configuration					
Schedule Statuses					
New Schedule Status	X	X			
Export Schedule Statuses	X				
Import Configuration	X				
<Status>	View	View	View	View	View
Add New Schedule Status	X	X			
Rename <schedule status>	X	X			
Set <schedule status> Color	X	X			

Set <schedule status> Movable	X	X			
Data Types					
Add New Data Type	X	X			
Export Data Types	X				
Import Configuration	X				
<Data Type>	View	View	View	View	View
Add New <data type>	X	X			
Delete <data type>	X	X			
Rename <data type>	X	X			
New Phrase	X	X			
<Phrase>	View	View	View	View	View
New Phrase	X	X			
Delete <phrase>	X	X			
Rename <phrase>	X	X			
Deactivate <phrase>	X	X			
Comment Required for <phrase>	X	X			
Data Source Types					
<Data Source>	View	View	View	View	View
Add New Data Source	X				
Activate/Deactivate <data source>	X				

Security Management

Modify System Cross References	X				
Export Cross Reference	X				
Import Configuration	X				
Color Schemes					
New Color Scheme	X	X			
< Color Scheme >	View	View	View	View	View
New <color scheme>	X	X			
Delete <color scheme>	X	X			
Duplicate <color scheme>	X	X			
Edit <color scheme>	X	X			
Rename <color scheme>	X	X			
Reason Trees					
Reasons					
Add New Reason	X	X	X		
Export Reasons	X				
Import Configuration	X				
< Reason >	View	View	View	View	View
Add New Reason	X	X	X		
Add Comment to <reason>	X	X			
Edit External Link	X	X			
Rename <reason>	X	X			

Change <reason> Security	X				
Categories					
Add New Reason Category	X	X			
<Category>	View	View	View	View	View
New Reason Category	X	X	X		
Rename <reason category> (user-defined only)	X	X			
Delete <reason category> (user-defined only)	X	X			
Trees					
Add New Reason Tree	X	X			
Export Trees	X				
Import Configuration	X				
<Tree>	View	View	View	View	View
Add New Reason Tree	X	X			
Rename <reason tree>	X	X			
Delete <reason tree>	X	X			
Change <reason tree> Security	X				
Reason Level Titles					
Add New Reason Level Title	X	X			
<Reason Level Title>	View	View	View	View	View
New Reason Level Title	X	X			

Security Management

Rename < <i>reason level title</i> >	X	X			
Delete < <i>reason level title</i> >	X	X			
Reason Tree					
Edit Reason Tree Membership	X	X			
Add New Reason	X	X			
Paste	X	X			
Export Reason Tree	X				
Import Configuration	X				
< <i>R_n Reason</i> >	View	View	View	View	View
Edit Membership	X	X			
Add New Reason	X	X			
Edit Next Level Reason Membership	X	X			
Add New Reason To Next Level	X	X			
Copy < <i>reason</i> >	X	X			
Paste	X	X			
Attach Categories	X	X			
Subscription Information					
New Subscription Group	X				
Export Subscription Groups	X				
Import Subscription Groups	X				

<Subscription Group>					
New Subscription Group	X				
Subscription Group Properties	X				
Delete Subscription Group	X				
Rename Subscription Group	X				
New Subscription	X				
Export Subscriptions	X				
Import Configuration	X				
<Subscription>					
New Subscription	X				
Subscription Properties	X				
Delete Subscription	X				
Rename Subscription	X				
Engineering Units					
Units					
Add New Engineering Unit	X				
Export Engineering Units	X				
Import Configuration	X				
<Engineering Unit>					
Add New Engineering Unit	X				
Edit Engineering Unit	X				

Security Management

Delete Engineering Unit	X				
Engineering Conversions					
Export Conversions	X				
Import Conversions	X				
Administer Site Parameters					
Edit Site Parameters	X				
Administer Production Statuses					
Edit Production Status	X				
Export Production Statuses	X				
Import Configuration	X				
Administer Calculations					
Administer Calculations	X	X			
Administer Alarms					
Administer Alarms	X	X			
Export Alarms	X				
Import Configuration	X				
Administer Events					

Administer Events / Event Subtypes	X	X	X		
Export Events / Event Subtypes	X				
Import Configuration	X				
Administer Models					
Administer Models	X	X			
Administer Language Prompts					
Administer Language Prompts	X	X			
Administer Multi-Lingual Translations					
Administer Multi-Lingual Translations	X	X			
Server Management					
Control Services					
Control Services	X	X			
Troubleshoot Services					
Troubleshoot Services	X	X			
Administer Licensing					
Administer Licensing	X	X			

Administer Web Server					
Administer Web Server	X	X			
Administer Web Parts					
Administer Web Parts	X	X			
Administer FTP					
FTP Configuration	X	X			
E-Mail Engine Configuration					
Import Configuration	X				
Export Configuration	X				
E-Mail Groups					
New Email Group	X	X			
<Email Group>	View	View	View	View	View
New Email Group	X	X			
Rename <email group>	X	X			
Edit Membership	X	X			
Delete <email group>	X	X			
E-Mail Recipients					
New Recipient	X	X			
<Recipient>	View	View	View	View	View

New Recipient	X	X			
Recipient Properties	X	X			
Delete Recipient	X	X			
Rename Recipient	X	X			
E-Mail Messages					
Edit Email Messages	X	X			
Historian Connections					
New Historian	X	X			
<Historian>	View	View	View	View	View
New Historian	X	X			
Delete <historian>	X	X			
Edit <historian> Properties	X	X			
Rename <historian>	X	X			
Set <historian> As Default Historian	X	X			
Security Management					
Site Users					
Add New User	X				
Import Operating System Users	X				
Export Site Users	X				
Import Configuration (From Excel)	X				
<Site User>	View	View own	View own	View own	View own
New User	X				

Security Management

Edit <site user> Properties	X				
Rename <site user>	X				
Edit <site user> Parameters	X				
Duplicate <site user>	X				
Edit User Membership	X				
View Windows User Group Membership	X				
<Role>	View	View own	View own	View own	View own
Go to Security Role	X				
Remove <role>	X				
<Group>	View	View own	View own	View own	View own
Access Level	X				
Go To Security Group	X				
Remove <group>	X				
System Users					
<System User>	View				
Add New User	X				
Edit <system user> Parameters	X				
Security Groups					
New Security Group	X				

Export Security Groups	X				
Import Configuration	X				
<Security Group>	View	View	View	View	View
New Security Group	X				
Add Comment to <security group>	X				
Edit External Link	X				
Delete <security group>	X				
Edit <security group> Membership	X				
Rename <security group>	X				
<Security Group Member>	View	View own	View own	View own	View own
Access Level	X				
Go To User	X	X		X	X
Remove Security Group Member	X				
Security Roles					
Add New Security Role	X				
<Security Role>	View	View	View	View	View
Add New Security Role	X				
Rename <security role>	X				
Deactivate/Activate <security role>	X				
Edit <security role> Membership	X				
View Security Group Membership	X				

Security Management

<Security Role Member>	View				
Remove Security Role Member	X				
View Security Group Membership	X	X			
Client Management					
Displays					
New Display Group	X	X			
Export Displays	X				
Import Configuration	X				
<Display Group>	View	View	View	View	View
New Display Group	X	X			
Delete <display group>	X	X			
Rename <display group>	X	X			
Edit <display group> Membership	X	X			
Change <display group>Security	X	X			
Add New Display	X	X	X		
Export <display group>	X				
Import Configuration	X				
<Display>	View	View	View	View	View
Add New Display	X	X	X ¹		
Edit <display>	X	X	X ¹		
Create Comment	X	X	X ¹		
Edit External Link	X	X	X ¹		

Delete <display>	X	X	X ¹		
Duplicate <display>	X	X	X ¹		
Rename <display>	X	X	X ¹		
Deactivate/Activate <display>	X	X	X ¹		
Change <display> Security	X	X			
Export <display>	X				
User Views					
Add New View Group	X	X			
<View Group>	View	View	View	View	View
Add New View Group	X	X			
Delete View Group (user-defined only)	X	X			
Rename <view group>	X	X			
Edit <view group> Membership (user-defined only)	X	X			
Change <view group> Security	X				
<View>	View	View	View	View	View
Rename <view>	X	X			
Delete <view>	X	X			
Change <view> Security	X				
Product Management					
Product Families					

Security Management

Add New Product Family	X	X	X	X	
Export Configuration	X				
Import Configuration	X				
<Product Family>	View	View	View	View	View
Add New Product Family	X	X	X	X	
Add Comment to <product family>	X	X	X	X	
Edit External Link	X	X	X	X	
Delete <product family>	X	X	X	X	
Rename <product family>	X	X	X	X	
Edit <product family> Membership	X	X	X	X	
Change <product family> Security	X				
Add New Product	X	X	X	X	
Export Configuration	X				
Import Configuration	X				
<Product>	View	View	View	View	View
Add New Product	X	X	X	X	
Delete <product>	X	X	X	X	
Edit <product> Properties	X	X	X	X	
Specification History	X	X	X	X	X
Duplicate <product>	X	X	X	X	
Product Properties					

New Property	X	X			
Export Product Properties	X				
Import Configuration	X				
<Property>	View	View	View	View	View
Add New Property	X	X			
Edit <i><property></i> Properties	X	X			
Delete <i><property></i>	X	X			
Change <i><property></i> Security	X				
Enter Specifications for <i><property></i>	X	X	X	X	
Add New Characteristic	X	X	X	X	
Add New Specification	X	X	X	X	
Export <i><property></i>	X				
Import Configuration	X				
Characteristic Groups					
Add New Characteristic Group	X	X	X	X	
<Characteristic Group>	View	View	View	View	View
New Characteristic Group	X	X	X	X	
Create Comment	X	X	X	X	
Edit External Link	X	X	X	X	
Delete Characteristic Group	X	X	X	X	
Edit Characteristic Group Membership	X	X	X	X	
Rename Characteristic Group	X	X	X	X	

Characteristics					
Add New Characteristic	X	X	X	X	
<Characteristic>	View	View	View	View	View
Add New Characteristic	X	X	X	X	
Add Comment to <characteristic>	X	X	X	X	
Edit External Link / Information	X	X	X	X	
Delete <characteristic>	X	X	X	X	
Rename <characteristic>	X	X	X	X	
Specification History	X	X	X	X	X
Specification Variables					
Add New Specification	X	X	X	X	
<Specification>	View	View	View	View	View
Add New Specification	X	X	X	X	
Delete <specification>	X	X	X	X	
Edit <specification> Properties	X	X	X	X	
Specification History	X	X	X	X	X
Product Groups					
Add New Product Group	X	X	X	X	
Export Product Groups	X				

Import Configuration	X				
<Product Group>	View	View	View	View	View
Add New Product Group	X	X	X	X	
Add Comment to <i><product group></i>	X	X	X	X	
Edit External Link	X	X	X	X	
Delete <i><product group></i>	X	X	X	X	
Edit <i><product group></i> Membership	X	X	X	X	
Rename <i><product group></i>	X	X	X	X	
Export <i><product group></i>	X				
Import Configuration	X				
Specification Transactions					
Pending					
<Pending Transaction>	View	View	View	View	View
Approve <i><transaction></i>	X	X	X	X	X
Add Comment to <i><transaction></i>	X	X	X	X	X
Delete <i><transaction></i>	X	X	X	X	X
View <i><transaction></i>	X	X	X	X	X
Rename <i><transaction></i>	X	X	X	X	X
Approved					
Add New Approved Group	X	X	X	X	

Security Management

<Approved Group>	View	View	View	View	View
Add New Approved Group	X	X	X	X	
Delete <i><approved group></i>	X	X	X	X	
Rename <i><approved group></i>	X	X	X	X	
Edit <i><approved group></i> Membership	X	X	X	X	
<Approved Transaction>	View	View	View	View	View
Add Comment to <i><approved transaction></i>	X	X	X	X	
View <i><approved transaction></i>	X	X	X	X	
Rename <i><approved transaction></i>	X	X	X	X	
Administer Bill of Materials					
Administer Bill of Materials	X	X	X	X	
Administer Cross Reference					
Product Cross Reference	X	X	X	X	
Administer Corporate Specifications	X				
Production Management					
Administer Customer					
Administer Customers	X	X			
Export Customers	X				
Import Configuration	X				

Administer Customer Orders					
Administer Customer Orders	X	X			
Export Customer Orders	X				
Import Configuration	X				
Administer Customer Shipments					
Export Customer Shipments	X				
Import Configuration	X				
Administer Production Schedule					
Export Production Schedule	X				
Import Configuration	X				
Administer Crew Schedule					
Administer Crew Schedule	X	X			
Export Crew Schedule	X				
Import Configuration	X				
Administer Non-Productive Time					
Administer Non-Productive Time	X				
Export Non-Productive Time	X				

Security Management

Import Configuration	X				
Plant Model					
New Department	X	X			
Export Plant Model	X				
Import Configuration	X				
<Department>	View	View	View	View	View
Add New Department	X	X			
Delete <i><department></i>	X	X			
Rename <i><department></i>	X	X			
Variable Sheet	X	X			
Export <i><department></i>	X				
Import Configuration	X				
Add New Production Line	X	X			
<Production Line>	View	View	View ²	View	View
Add New Production Line	X	X			
Edit External Link / Information	X	X	X		
Rename <i><production line></i>	X	X	X		
Delete <i><production line></i>	X	X			
Add Comment to <i><production line></i>	X	X	X		
Change <i><production line></i> Security	X				
Configure Execution Paths for <i><production line></i>	X	X	X		
Edit Unit Hierarchy for <i><production line></i>	X	X	X		

Variable Sheet	X	X	X		
Add New Unit to <production line>	X	X	X		
Export <production line>	X				
Import Configuration	X				
<Production Unit>	View	View	View	View	View
Add New Production Unit	X	X	X ³		
Edit <production unit> Properties	X	X	X		
Rename <production unit>	X	X	X		
Delete <production unit>	X	X	X ³		
Add Comment to <production unit>	X	X	X		
Change <production unit> Security	X				
Configure Events on <production unit>	X	X	X		
Enter Specifications for <production unit>	X	X	X	X	
Search For Captured Data Sets	X	X	X	X	
Search For Run Summary Statistics	X	X	X	X	
View Run Summary Statistics	X	X	X		
View <production unit> Timeline	X	X	X		
Variable Sheet	X	X	X		
Add New Group to <production unit>	X	X	X		
Export <production unit>	X				
Import Configuration	X				
<Variable Group>	View	View	View	View	View

Security Management

Add New Variable Group	X	X	X ⁴		
Edit External Link	X	X	X		
Rename <variable group>	X	X	X		
Delete <variable group>	X	X	X ⁴		
Add Comment to <variable group>	X	X	X		
Change <variable group> Security	X				
Enter Specifications For <variable group>	X	X	X	X	
Import Variables From Historian	X	X	X		
Variable Sheet	X	X	X		
Add New Variable	X	X	X		
Add New Standard Calculation	X	X	X		
Add New SPC Calculation	X	X	X		
Export <variable group>	X				
Import Configuration	X				
<Variable>	View	View	View	View	View
Add New Variable	X	X	X ⁵		
Add New Child Variable	X	X	X ⁵		
Add New Standard Calculation	X	X	X ⁵		
Add New SPC Calculation	X	X	X ⁵		
Edit <variable>	X	X	X ⁵		
Calculation	X	X	X ⁵		
Create Standard Calculation	X	X	X ⁵		

Create SPC Calculation	X	X	X ⁵		
Rename <variable>	X	X	X ⁵		
Delete <variable>	X	X	X ⁵		
Add Comment to <variable>	X	X	X ⁵		
Change <variable> Security	X	X	X ⁵		
Edit External Link for <variable>	X	X	X ⁵		
Replicate Variable	X	X	X ⁵		
Replicate <variable> By Count	X	X	X ⁵		
Replicate <variable> By Sample Type	X	X	X ⁵		
Specification History	X	X	X	X	X
View Variable Data for <variable>	X	X	X	X	X
View Adhoc Trend for <variable>	X	X	X	X	X
Deactivate <variable>	X	X	X ⁵		

¹ A user-defined security group must be assigned to the display group. Assigning a security group to an individual display controls who can open it in the Plant Applications Client program.

² Access rights propagate to all production units under the production line.

³ This feature is not available if the user-defined security group is assigned at the unit level and not at the line level.

⁴ This functionality is not available if the user-defined security group is assigned at the group level and not at the line or unit level.

⁵ This functionality is available only if the user-defined security group is assigned at the group level, unit level, or line level.

Display Security Rules

Display security is used as the first level of data access security for the Plant Applications Client program. If security has been assigned to variables, the variable-level security will override the display security.

If no security group has been assigned to a display group, the following rules apply when opening displays in the Plant Applications Client program.

Security Management

- If a user is a member of a security group, that user will have access only to displays that have no security group assigned to them and to displays that have the user's security group assigned to them.
- If a user is not a member of a security group, that user will have access only to displays that have no security group assigned to them.

If a security group has been assigned to a display group, the following rules apply when opening displays in the Plant Applications Client program.

- If a user is not a member of a security group, that user will not have access to any displays.
- If a user is a member of the security group assigned to the display group, that user will have access to the displays assigned to the user's security group and displays that have no security group assigned to them.
- If a user is a member of a security group other than the one assigned to the display group, that user will have access only to the displays that are assigned to the user's security group.

NOTE: When no security group is assigned to a display, every site user has [Manager access](#) by default.

For a complete list of access levels and privileges in the various displays, please see [Display Access Levels and Privileges](#).

Access Levels and Privileges for Client Displays

Alarm Display

	Admin	Mgr	R/W	Read
Alarm Display				
Trend to Ad hoc	X	X	X	X
Go to Time	X	X	X	X
Create Ad hoc Trend	X	X	X	X
Display Hyperlinks	X	X	X	X
Enter Comment	X	X	X	X
Filter	X	X	X	X
Acknowledge Alarms	X	X	X	
Edit Alarm	X	X	X	
Search for Alarms	X	X	X	X

Autolog Display

	Admin	Mgr	R/W	Read
AutoLog Display				
Add trends to Ad-hoc display	X	X	X	X
Array Data				
Test history	X	X	X	X
View calculation	X	X	X	X
Dynamic rows	X	X	X	X
Maximize comment	X	X	X	X
Specification window	X	X	X	X
Reject limits	X	X	X	X
Target	X	X	X	X
User Limits	X	X	X	X
Warning Limits	X	X	X	X

Test Frequency	X	X	X	X
Reports	X	X	X	X
Cell Information	X	X	X	X
Test History	X	X	X	X
Add Trend	X	X	X	X
Print Event Label	X	X	X	X
Goto Specific Time	X	X	X	X
Goto Last Product Run	X	X	X	X
Goto Event	X	X	X	X
Change Product	X	X		
Edit Event	X	X	X	X
Defect Entry	X	X	X	X
Align Column	X	X	X	X
Insert Column	X	X		
Delete Column	X	X		
Last Product Runs to Operator *	?			
Product Specs to Operator *	?			
Thumbchart Trend for this Display **	?			
Auto Label	X	X	X	X

* An Operator display must be open in addition to the AutoLog display.

** UseWebApps must be set to TRUE.

Downtime Display

	Admin	Mgr	R/W	Read
Downtime				
Print spread sheet	X	X	X	X
Delete row	X	X		
Insert row	X	X		
Column visibility	X	X	X	X
Goto specific time	X	X	X	X
Time formats	X	X	X	X
Add comment	X	X	X	X
Append clipboard	X	X	X	X
Open new Downtime item	X	X		
Close Downtime item	X	X		
Copy reason	X	X		
Paste reason	X	X		

Geneology View

	Admin	Mgr	R/W	Read
Geneology View				
Open Geneology View	X	X	X	X
Perform all update functionality	X	X	X	

Production Overview Display

Security Management

	Admin	Mgr	R/W	Read
Production Overview				
Full access	X	X	X	X

Production Run Analyst (also known as "Operator Display")

	Admin	Mgr	R/W	Read
Operator Display				
Create captured data set	X	X	X	X
Insert Product Specifications	X	X	X	X
Insert captured data set	X	X	X	X
Insert summary data set	X	X	X	X
Insert last summary data set	X	X	X	X
Insert last 3 grade runs	X	X	X	X
Delete selected column	X	X	X	X
Select new current product	X	X	X	X
Set the trend time	X	X	X	X
Update Product	X	X	X	X
View variable comments	X	X	X	X
View product comments	X	X	X	X
Add Trend	X	X	X	X
Summary Comments	X	X	X	X

Relative View Display

	Admin	Mgr	R/W	Read
Relative View				
Read only	X	X	X	X

Schedule View:

	Admin	Mgr	R/W	Read
Schedule View				
Print	X	X	X	X
Production Schedule View	X	X	X	X
Dock to Process Order Summary View	X	X	X	X
Edit Process Order	X			
View Process Order History	X	X	X	X
View Process Order Comment	X	X	X	X
Edit Production Schedule Run Times	X			
Create Child Process Order	X			
Process Order Transitions	X	X		
UnBind Process Order	X			
Add Sequence	X			
Edit Sequence	X			
Show Sequence History	X	X	X	X
View Sequence Comment	X	X	X	X
Select Sequence Columns	X	X	X	X

Sequence Transitions	X	X		
Add Pattern	X			
Edit Pattern	X			
Show Pattern History	X	X	X	X
View Pattern Comment	X	X	X	X
Select Pattern Columns	X	X	X	X
Move Pattern Back	X	X		
Move Pattern Forward	X	X		
Pattern Transitions	X	X		
Edit Property	X			
Print	X	X	X	X
Process Order Detail View	X	X	X	X
Production Schedule Query	X	X	X	X
Sort Production Schedule By Path	X	X	X	X
Add Process Order	X			
Edit Process Order	X			
View Process Order History	X	X	X	X
View Process Order Comment	X	X	X	X
Edit Production Schedule Run Times	X	X	X	X
Create Child Process Order	X			
Re Work Process Order	X			
Select Process Order Columns	X	X	X	X
Process Order Transitions	X	X		
UnBind Process Order	X			

Sequence of Events Display

	Admin	Mgr	R/W	Read
Sequence of Events				
Everything	X	X	X	
Everything, but adding user-defined events	X	X	X	X

Trend Displays

	Admin	Mgr	R/W	Read
Trend Display				
Read-only	X	X	X	X

DT+ and WebUI Displays

Security controls for the Downtime+ and WebUI Displays are set in the Display Options tab of the Edit Display screen (sheet). For a particular control, select the lowest level Security Group that you want to have rights.

Security Site Parameters

DefaultDomainName Site Parameter

Use the **DefaultDomainName** site parameter to specify the domain or server name that will be used to manage security roles by domain groups. If a domain is not specified, then the default domain will be the domain the Plant Applications Server is logged on to.

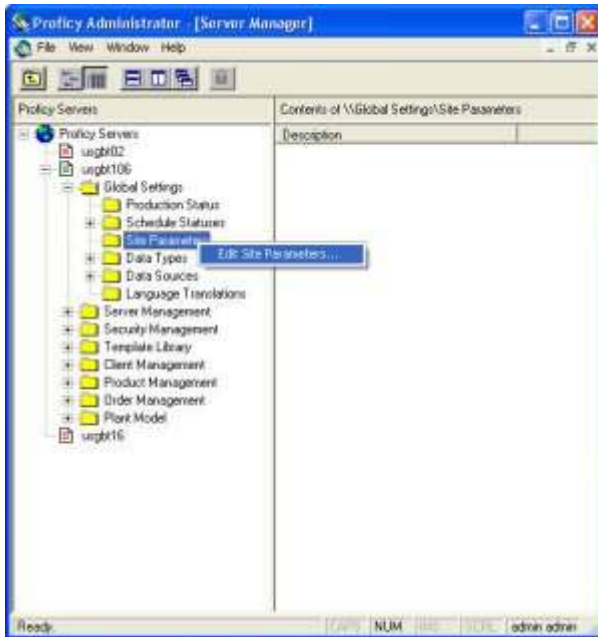
If you specify a domain name, any user who logs on that does not belong to the specified domain must log on with their domain name and user name in this format: **<domain name>\user name**.

Beginning with version 6.1.3, Plant Applications requires fully qualified domain names (FQDNs) for Windows authentication when aspecting is turned on. Users will enter an FQDN when logging into a domain other than the default domain. Refer to [Security Overview](#) and [Managing Domain Names](#).

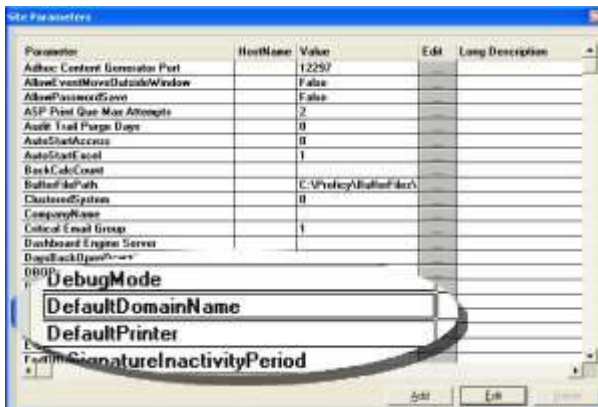
NOTE: You must have **Administrator access** to the Administrator security group to edit site parameters.

To specify a domain:

1. Log on to the Plant Applications Administrator program.
2. Open the **Global Configuration** folder.
3. Right-click on the **Site Parameters** folder and select **Edit Site Parameters**. [Example:](#)




4. In the **Site Parameters** dialog box, double-click on **DefaultDomainName**.



- In the **Edit Parameter** dialog box, enter the domain name in the **Value** field.



- Click the **OK** button to save your changes and to close the **Edit Parameter** dialog box.
- Click the **Close**  button to close the **Site Parameters** dialog box.

Domain User Creation Site Parameter

The **Domain User Creation** site parameter automates the creation of Plant Applications site users based on your site's Windows domain security groups.

When this site parameter is set to **True**, a Plant Applications site user is automatically created when a new user first logs into Plant Applications, if the following conditions are met.

- There is no existing Plant Applications site user that is mapped to the user's Windows domain account.
- The Domain User Creation and [WindowsAuthentication](#) site parameters are both set to **True**.
- The user's Windows domain account is a member of at least one Windows domain security group that is assigned to an existing Plant Applications [security role](#).

WindowsAuthentication Site Parameter

This site parameter works in conjunction with both Windows Info and Mixed Mode.

- If this site parameter is set to **True** and you imported the user's Windows information and you selected the Mixed Mode option, then the user can log in with either their Plant Applications name and password or their Windows name and password. When the user starts either the Administrator or Client program, Plant Applications will use their Windows name and password to automatically log them in.
- If this site parameter is set to **True** and you imported the user's Windows information and you did not select the Mixed Mode option, then the user must log in using their Windows name and password. When the user starts either the Administrator or Client program, Plant Applications will use their Windows name and password to automatically log them in.
- If this site parameter is set to **False**, then the user must log in with their Plant Applications name and password.

*You must have **Administrator access** in the Administrator security group to edit site parameters.*

To set the WindowsAuthentication site parameter

- Log on to the Plant Applications Administrator program.
- Open the **Global Configuration** folder.
- Right-click on the **Site Parameters** folder and select **Edit Site Parameters**. The **Site Parameters** dialog box appears.

Security Management



4. Double-click **WindowsAuthentication**. The **Edit Parameters** dialog box appears.



5. Make a selection from the **Value** drop-down list.
6. Click the **OK** button to close the **Edit Parameters** dialog box.
7. Click the **Close** button to close the **Site Parameters** dialog box.

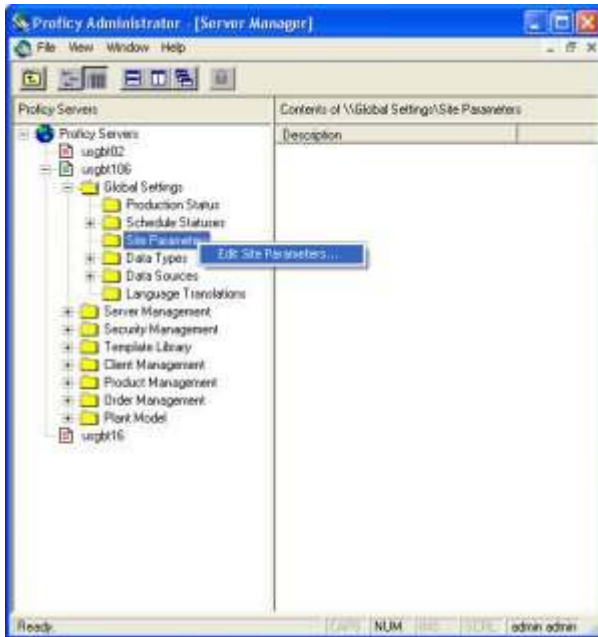
UseDisplaySecurity Site Parameter

Use the **UseDisplaySecurity** site parameter to defer variables with a designation of No Security Group to a display-level security group. When set to False, the default, variables (for example, in autolog sheets) use variable-level security settings and when no security is assigned a default is used. When set to True, the security set for the display applies to all variables in the display that do not have variable-level security defined.

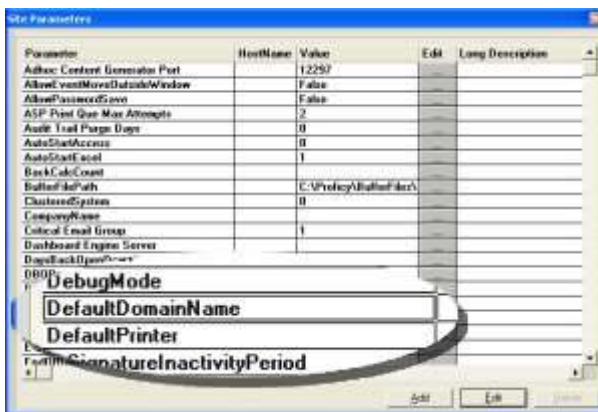
NOTE: You must have **Administrator access** to the Administrator security group to edit site parameters.

To specify a value for the site parameter:

1. Log on to the Plant Applications Administrator program.
2. Open the **Global Configuration** folder.
3. Right-click on **Administer Site Parameters**, and select **Edit Site Parameters**. [Example:](#)



4. In the **Site Parameters** dialog box, double-click on **UseDisplaySecurity**.



5. In the **Edit Parameter** dialog box, enter True or False (default) in the **Value** field.



6. Click the **OK** button to save your changes.
7. Click the **Close** button to close the **Site Parameters** dialog box.