Security Administrator System Technical Bulletin

Building Technologies & Solutions

www.johnsoncontrols.com

2021-11-23

LIT-1201528

Release 11.0

Contents

Document Introduction

The Security Administrator system authenticates and authorizes users of Metasys® servers, including the Application and Data Server (ADS), Extended Application and Data Server (ADX), Open Data Server (ODS), and Open Application Server (OAS), and Metasys network engines, including Network Automation Engines (NAE35, NAE45, NAE55, and LSC8500), Network Control Engines (NCE25), SNC and SNE devices.

The Security Administrator feature of the extended architecture browser-based interface manages user accounts. This document describes how to create local user accounts and add Microsoft® Active Directory® service users to the Metasys system. It describes how to define user roles and assign access permissions. This document also focuses on new security features and enhancements.

Note: The Metasys system for the ADS/ADX/ODS/OAS has two types of users: local users and Active Directory service users. The Metasys system for the network engines has one type of user: local users. A local user is defined in the Security Administrator system and is authenticated against the Metasys Security database. An Active Directory service user is created and stored in an Active Directory service domain and is added as a Metasys system user with the Metasys Security Administrator tool. This user is authenticated against an Active Directory service domain.

In this document, general use of the term user refers to any of the three types of users, unless differentiated.

Note: Any users with Basic Access are converted to Standard Access when you upgrade to SCT 14.0.

Summary of changes

The following information is new or revised for the Security Administrator Technical Bulletin at Release 11.0:

- Removed any RADIUS content as RADIUS users are no longer supported at release 11.0.
- Updated the access to include the new API Access which is supported from release 11.0. See API Access .
- Removed information about BasicSysAgent (Basic Access) account as it is no longer supported from release 11.0 and after. All users with Basic Access are converted to Standard Access users when you upgrade the archive with System Configuration Tool (SCT) release 14.0.
- Added a note to state that Active Directory users and Local users cannot have the same user name. See Username Semantics.
- Active Directory Federation Services (ADFS) is added to release 11.0 for Metasys UI only. See Authentication Overview.

Related Documentation

Table 1: Security Administrator System Related Documentation

For Information On	See Document
Use of Metasys System (online) or Creating User Views	*Metasys Site Management Portal Help (LIT-1201793)*
Use of Metasys System Configuration Tool (SCT) (offline) or Working with the Security Database	*Metasys SCT Help (LIT-12011964)*
Use of the Metasys UI, User Management, User Authorization (for Spaces), and Cyber Health Dashboard	*Metasys UI Help (LIT-12011953)*
Metasys System Basics	*Metasys System Configuration Guide (LIT-12011832)*
Understanding Active Directory Service Concepts Related to the Metasys System	*Network and IT Guidance Technical Bulletin (LIT-12011279)*
Use of the ODS System	*Open Data Server Help (LIT-12011942)*
Use of the OAS System	*Open Application Server (OAS) Commissioning Guide (LIT-12013243)*

Security Administrator Overview

Use the Security Administrator tool to create Metasys local user accounts and grant Metasys system access to Active Directory service users. The Audit Log of the Site Director allows you to log specific tasks (audits) using the audit trail. The Security System logs the successful and failed login attempts and all administrative tasks.

To access the Security Administrator system, click **Tools > Administrator** in the SMP UI or SCT.

The Metasys UI User Management feature facilitates the creation and management of users and their roles, category-based permissions, and privileges directly in Metasys UI Online, without the need to install software on client machines. Administrators can create and manage user details for Active Directory and Metasys local users. This feature is also available in the Metasys Site Management Portal (SMP).

Authentication Overview

Security is based on user accounts and roles. Roles are groups of users with a specific function within the Metasys system. To access the system, an administrator provides a username and the password. When creating users within the Metasys system, use ASCII characters only. Do not use the characters @ or \ to create Metasys local user names. The @ and \ characters are reserved for Active Directory service usernames that are added to the system.

ⓘ **Note:** If the Microsoft Active Directory service feature and Microsoft Windows® Workstation SSO are both enabled for use in the Metasys system, you generally do not need to specify your username and password. The Active Directory service credentials that you specified when you log on are automatically passed to the Security Administrator system for authentication. For details, see Overview of Active Directory Service Implementation on the Metasys System.

Click **Login** on the Login screen to send your user credentials. If Active Directory service is enabled, you also need to select your user domain or enter a local username and select **Metasys Local** from the domain selection drop-down menu.

For local users, the extended architecture Security Administrator system authenticates the user's information against the Security database. For Active Directory service enabled users, the selected Active Directory service domain authenticates the user and no Security database authentication occurs.

Microsoft® Active Directory Federation Services (ADFS) and Microsoft AD Lightweight Directory Access Protocol (LDAP) is supported in MUI only. ADFS integration with two-factor authentication is an add-on, licensed feature to add support for Metasys using ADFS, a single sign-on solution developed by Microsoft®. ADFS can then, in turn, be used to provide two-factor authentication for access to Metasys. ADFS helps prevent unauthorized access to Metasys, which, if not prevented, could result in data, financial, and reputational loss, system disruption, and other negative consequences. LDAP authenticates your identity against AD for Metasys access as a user of the system.

ⓘ **Note:** For Active Directory users, Metasys saves the domain name separate from the user id. Therefore if you add a Metasys local user with your JCI global id, you cannot also add an Active Directory login with the same name.

A unique session opens when your user credentials match the logon requirements. The session provides access to the system for a configurable period. When the credentials do not match, a dialog box appears indicating that the credentials are incorrect or user access is denied. For more details on possible logon error messages, see Table 6. The security system generates an audit trail and tracks all logon attempts.

ⓘ **Note:** The default password for the MetasysSysAgent user and Operator user accounts on new or re-imaged devices has a default password that is expired and must be changed at the first login.

When you click **Login**, the IPv4 address of the computer you are using is recorded in the Metasys Audit file. You can view the login transaction by opening the Audit Viewer. If the user logs in to the Metasys Advanced Reporting System and the SMP UI, the SMP UI login time is recognized as the last login time. If the user logs in for the first time, the status box indicates **Never** as the last login time.

Authorization Overview

Authorization provides users with the appropriate permissions and privileges for the Building Automation System (BAS). Use the Security Administrator to create Metasys local user accounts, add Active Directory service users, and grant privileges to system functionality through roles or direct user assignment.

Warning Banners

If you enable a Warning Banner on the Site object, a special warning statement appears every time an unauthorized user logs on to the SMP UI from an ADX, ADS, OAS, or NAE8500 server and all their child devices.

To configure this setting, complete the following steps:

1. In the SMP UI of the Site Director, display the site object, click the **Site View** tab, click the **Advanced** button in the top right and then click **Edit**.
2. Scroll to the bottom of the window to locate the **Warning Banner** attribute.
3. From the **Warning Banner** list, select one of the following options:
   - None

- U.S. Department of Defense (DOD) Warning Banner
- U.S. General Services Administration (GSA) Warning Banner
- U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) Warning Banner

ⓘ **Note: None** is selected by default.

4. Click **Save**. The setting takes from three to five minutes to become effective.

When you enable a warning banner, it appears for all local and Active Directory users when they log on to the SMP UI. The user must click **OK** or **I agree** to proceed.

ⓘ **Note:** The login page has a timeout of 30 seconds to put in your user name and password. After 30 seconds the page displays the selected Warning Banner.

The Metasys audit log presents any changes to the warning banners and the user who makes the change.

ⓘ **Note:** Warning banners do not appear when you log on to SCT.

Figure 1: U.S. Department of Defense (DOD) Warning Banner

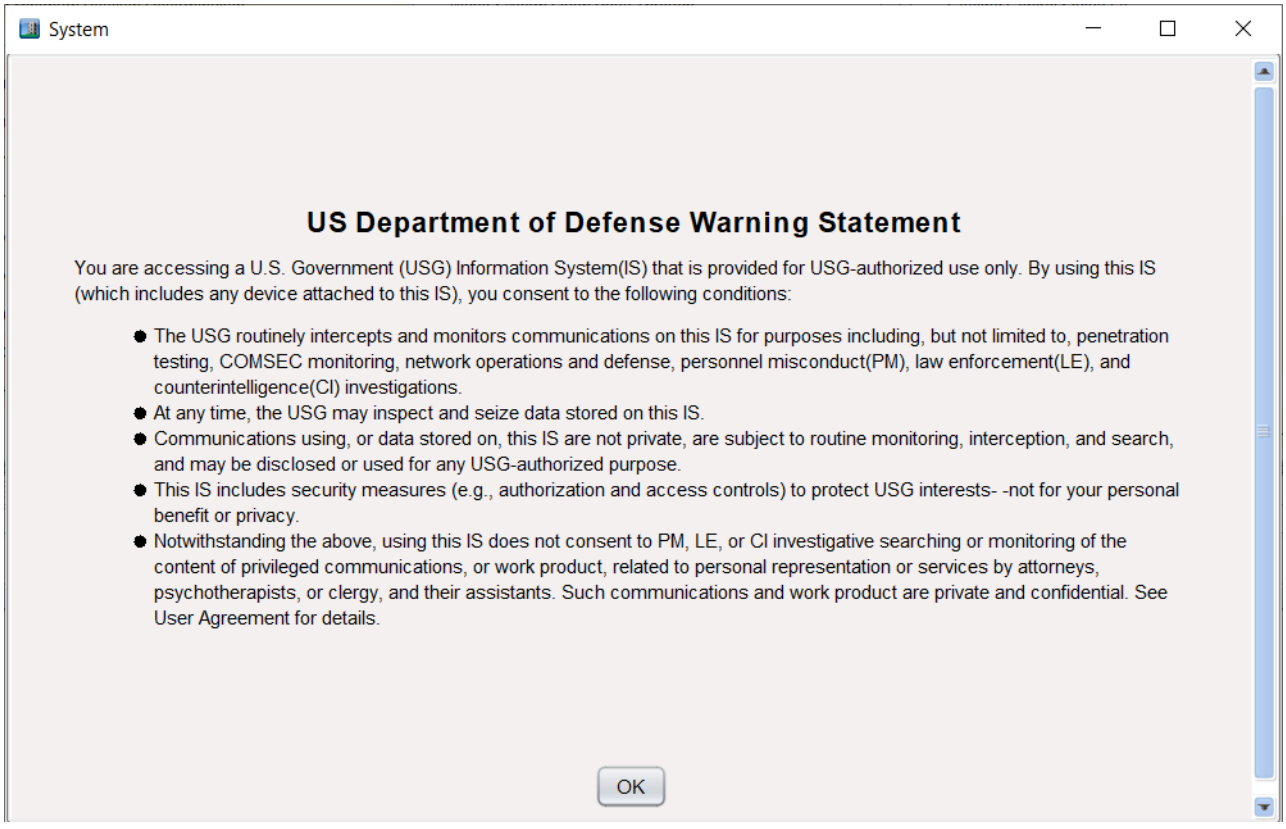


Figure 2: U.S. General Services Administration (GSA) Warning Banner

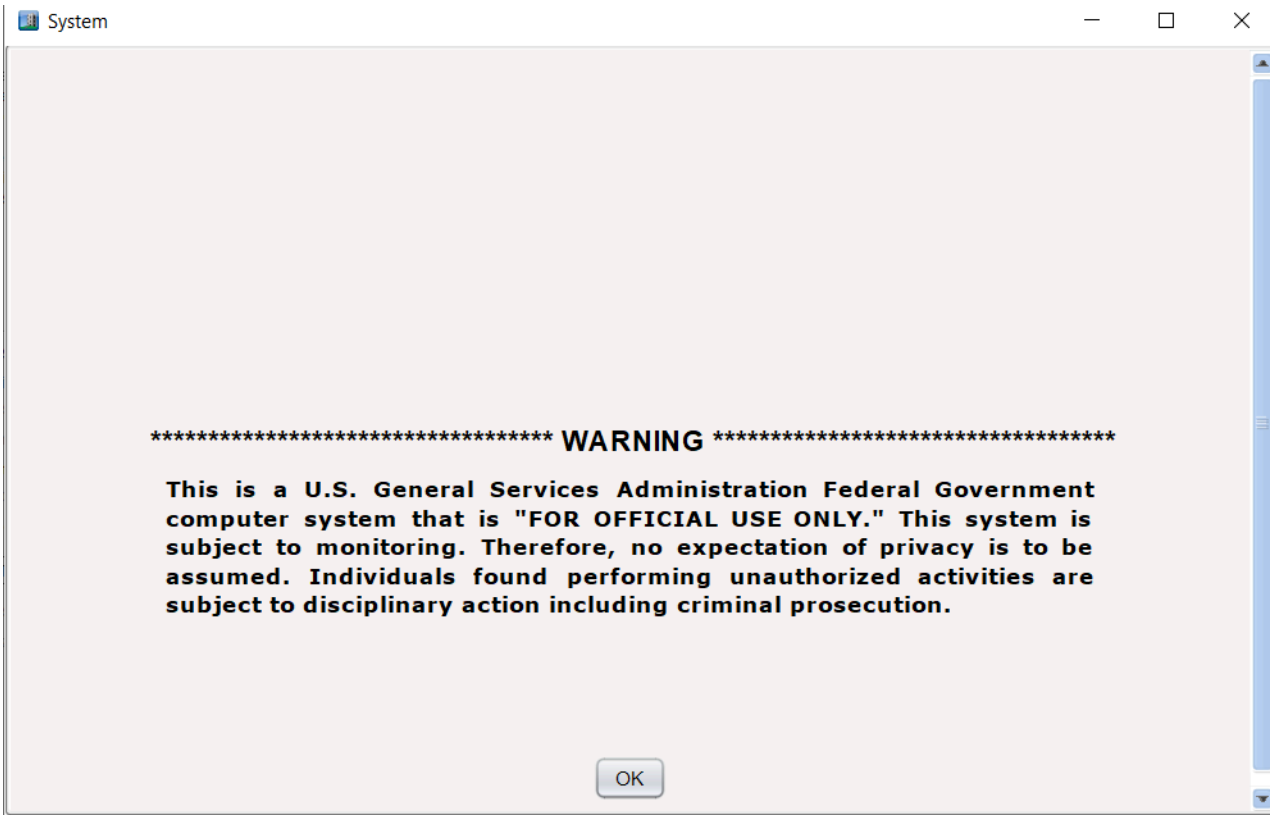
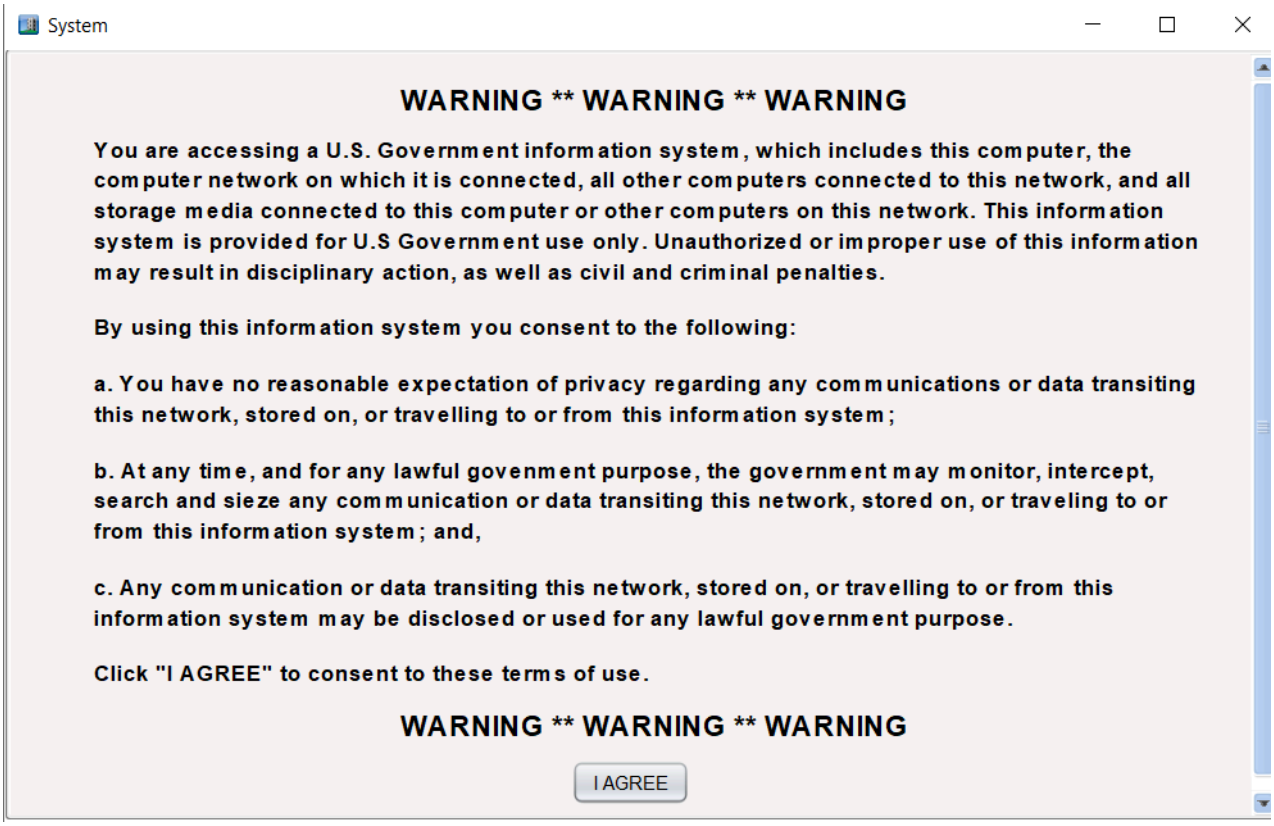


Figure 3: U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) Warning Banner



Privileges Overview

Privileges allow users to perform certain tasks within the Metasys system. Administrators set up privileges to determine which actions each user is authorized to perform. A privilege is a group of related user actions. For example, the Intervene privilege includes actions such as disable, enable, release, and reset.

Privileges are divided into two types: category-based and system-based. Category-based privileges apply only to the categories of the Metasys system items or objects for which the user is explicitly authorized such as General, Security, and Lighting. System privileges apply to the Metasys system as a whole and include actions such as discard events and manage audit history.

Any privileges that are assigned to a role can also be assigned to either a Metasys local user or an Active Directory service user. A role is like a template of privileges that, once created, is applied to multiple users. When you assign users to a role, they are granted the privileges associated with that role, in addition to their specific user privileges, if any. Assign roles to centralize administration of users.

Note:

- Assign privileges by going to **Tools>Administrator** in SCT.
- Changes to privileges do not take effect until the next time the user logs in to the system. For example, if users are currently logged in, the changes you make to their accounts do not affect their privileges until the users log out and log in again.

Authorization Category Assignment

When adding devices, objects, and other items to the All Items view (that is, when inserting an object into the system so that the object appears in the All Items tab), you can assign a single category to each object on the All Items navigation tree except the Site. Use the Authorization Category menu in the configuration wizard to select a category to assign to the specific object. Figure 4 shows the selection process for assigning object categories. Also, authorized users can change assigned categories after the you create the object.

Figure 4: Assigning Authorization Categories

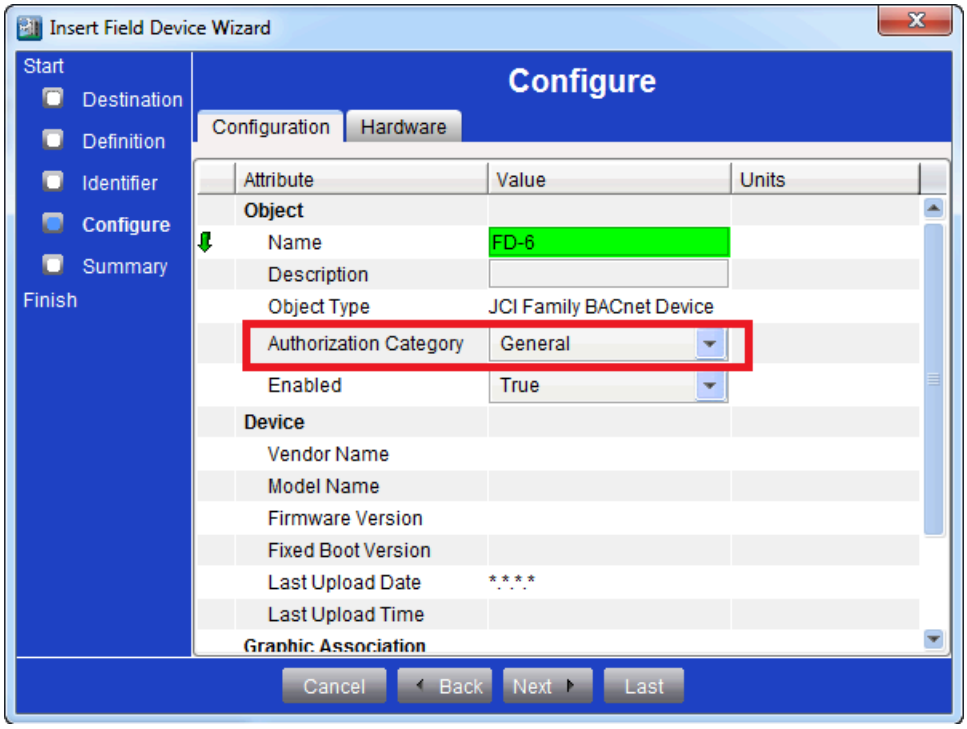
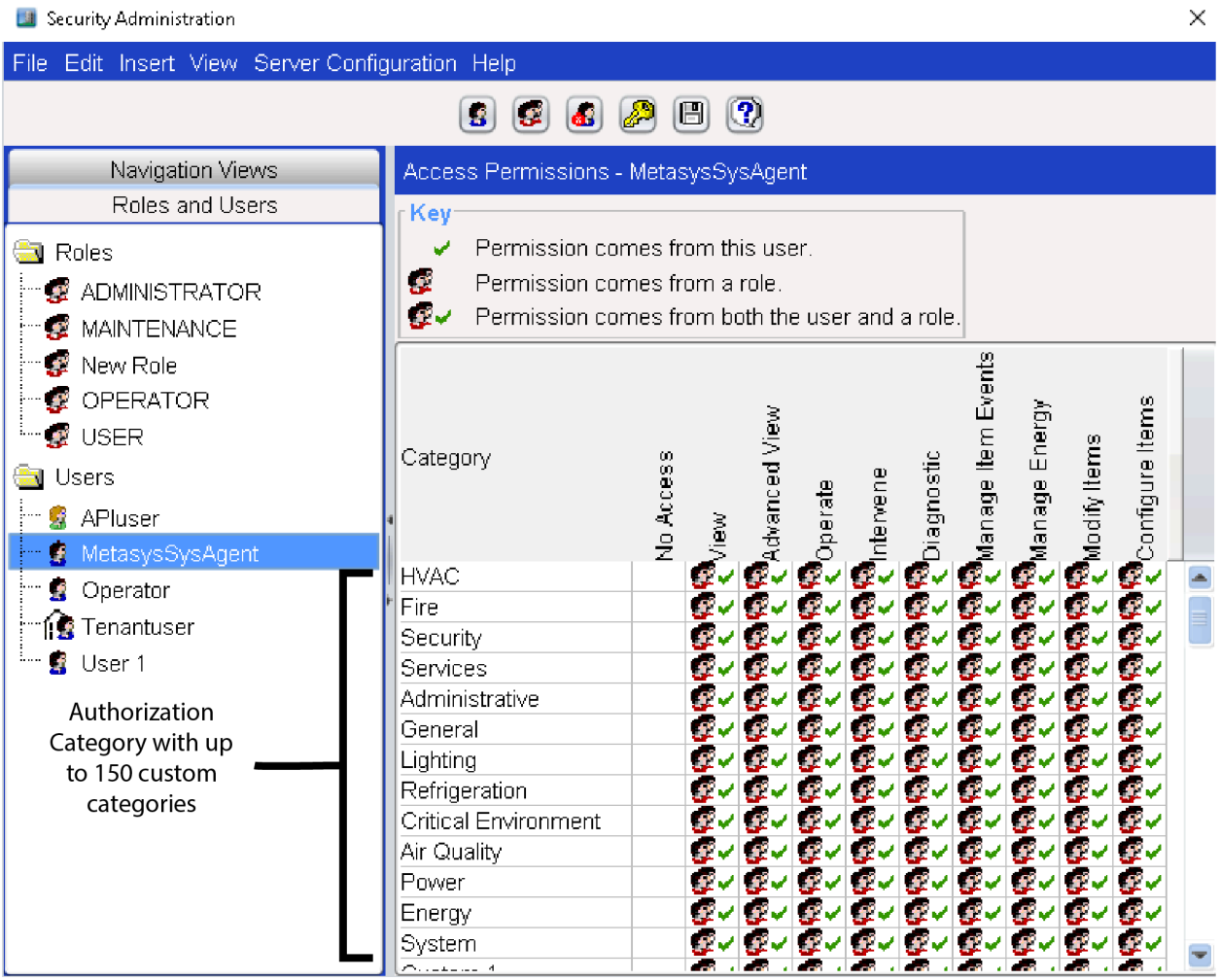


Figure 5 shows the authorization categories as they appear in the Security Administrator System and how the authorization category-based privileges are assigned to each authorization category. The Active Directory Users folder shown in the left pane appears only if Active Directory service is enabled for the site. See Table 2 for detailed descriptions of the authorization category-based privileges.

Figure 5: Authorization Categories

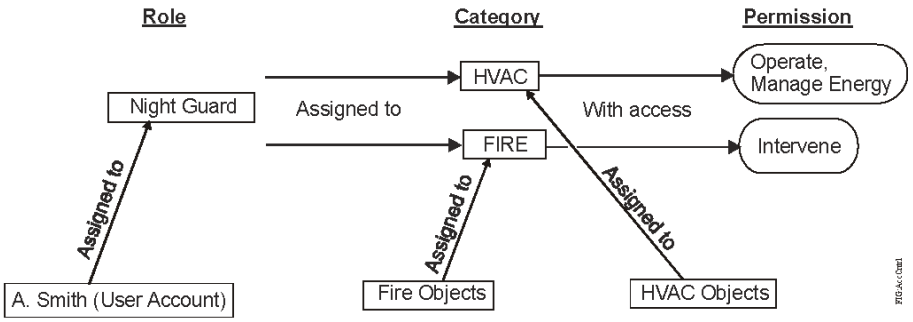


ⓘ **Note:** The Security Administration system in Metasys Release 5.2 or later provides up to 150 custom categories. However, if you set up your user profile prior to Metasys system Release 5.2, then you are limited to the 12 custom categories.

Authorization Category-Based Privileges Assignment Example

Figure 6 shows a user assigned to a role. Based on the role setup, the user has permission privileges over certain categories of authorization. See Figure 10 for the Access Permissions screen that matches the example in Figure 6.

Figure 6: Access Control Assignment Example



In the example, an administrator created the Night Guard role with Operate and Manage Energy privileges over the authorization category HVAC. The role also has Intervene privileges over the Fire category. Assigning Smith (User A) to the Night Guard role gives Smith all access permissions defined by the particular role; therefore, Smith has access to all HVAC objects (items) using the actions defined by the privileges Operate and Manage Energy, as well as the Intervene privilege with Fire objects.

Authorization Category-Based Privileges

Category-based privileges apply to specific categories of Metasys system objects. When you assign users a category-based privilege, they can perform the actions associated with that privilege only on specific categories of objects for which that privilege is granted. The Security System has a predefined set of categories available (for example, HVAC and Fire).

If you do **not** assign users **View** access permission to a particular category of items, they cannot see the details of those items in the View panel, limiting user access to items (objects, trends, and schedules) within the navigation tree.

Table 2 describes all the predefined authorization category-based privileges.

Table 2: Authorization Category-Based Privileges

Permission	Permission Privileges
No Access	Designates that the user has no access to the items in the specified category.
View	Gives the user the following privileges: view event, snooze event, focus view in panel, view item value, view item on graphic, view item in report, summary view in panel, user navigation views (display panel only), view all extensions in panel, hyperlink from graphic, and view the list of attribute commands (generic integration object). ⓘ **Note:** To snooze an alarm in the alarm bar, the user must have View permission and Manage Item Events permission. To display the Audit Viewer, the user must have View permission and View Metasys Status permission.
Advanced View	Gives the user the same privileges as the View permission, in addition to the capability of editing the advanced attributes for users with edit privileges. When not selected, the Advanced option in all item views (for example, Focus view) is disabled.
Operate	Gives the user the following privileges: Adjust commands; State commands based on States Text – BV, BO, MV, MO; Setpoint; Route (Trend); Execute (Trend); Re-command (Interlock); Set State.

Table 2: Authorization Category-Based Privileges

Permission	Permission Privileges
Intervene	Gives the user the following privileges: Release; Release All; Operator Override; Release Operator Override; Timed Operator Override (TOO); Enable; Disable; Preset Counter; Reset – Pulse Meter, Analog Object, Totalization, Optimal Start (OST); Add Recipient Command and Remove Recipient Command (Notification); Cancel Delay Time (Analog Alarm); Cancel Report Delay (Multistate Alarm); and Clear (Trend).
Diagnostic	Gives the user the following privileges: Latch/Clear Statistics; Analyze Field Bus; Out-of-Service; In Service; Timed Out of Service (TOS).
Manage Item Event	Gives the user the following privileges: Acknowledge, Annotate. Applies to category-based events and allows the user to display an alarm in the Alarms Window (also referred to as Metasys - Events and Alarm Bar).
Manage Energy	Gives the user the following privileges: • OST Commands: Start/Stop Meter, Cancel Prestart/Prestop • Load Commands: Shed, Release Load, Comfort Override, Release Comfort Override, Lock, Unlock • DLLR Commands: Set Mode, Set Target, Reset Profile, Reset Interval, Reset Initialization Parameters
Modify Items	Gives the user the following privileges: Modify Item (cannot add or delete). Commands included: Use GIO to Change Name, Change Units, and Change Display Precision When users modify items, they can only set the Authorization Category property of a modified object to a category for which they have modify access permissions.
Configure Items	Gives the user the following privileges: Add, Modify, or Delete an Item. When users create objects, they can only set the Authorization Category property to a category for which they have configuration access permission.

System Access Privileges

The System Access Privileges have two dialog boxes: one for the role assignment and one for the user assignment. Administrators assign System Privileges directly to a user or role. System Access Privileges apply to the system as a whole, not to individual categories of objects or items. Table 3 describes all the predefined privileges for System Access Permission.

Table 3: System Access-Based Privileges

Permissions	Permission Privileges
Discard All Events	Gives the user permission to discard all events. Applies to all events a user can manage through the Manage Item Events action set. Use this action set carefully because it is a system-wide discard.
Manage Devices & Sites	Gives the user the following privileges: Reset Device, Archive Device, Set Date, Set Time, Force Archive of Local Repository (audits and trends), Change Audit Enabled Level, and Remove from Site (offline devices and servers). Handles non category-based configuration actions. **Note:** To disable the All Items Organizer for a user, you must remove the Manage Devices & Sites privilege from the available privileges for the user.
View Metasys Status [1]	Gives the user permission to display and use the Audit Viewer. To display the Audit Viewer, the user must have View permission and View Metasys Status permission. Also, the audit data visible in the Audit Viewer depends on the categories for which the user has View privileges.
Manage Audit History[1]	Gives the user permission to annotate audit entries.
Clear Audit History[1]	Gives the user permission to clear the audit log.
Discard Acknowledged Events	Gives the user permission to discard acknowledged events. Applies to all events a user can manage through the Manage Item Events action set. See the Discard All Events permission description for information on discarding all events. A user who has the Discard Acknowledged Events permission can discard any event that the user has permission to acknowledge, even if it has already been acknowledged. The Discard Acknowledged Events permission provides a one-step shortcut for the two-step process of acknowledging the event and then discarding the event afterward.
Advanced Reporting[1]	Gives users with Standard Access permission to access the Metasys Advanced Reporting System. In the Advanced Reporting system, users can run reports to view on a web browser. The Advanced Reporting privilege appears in the list of permission privileges only if Metasys Advanced Reporting System is installed. For more information, refer to the *Metasys Advanced Reporting System and Energy Essentials Help (LIT-12011312)*.
Schedule Reports[1]	Gives the user permission to create new Scheduled Reports (Query menu), and to run, modify, reschedule, or delete scheduled reports using the Scheduled Reports Viewer. All users, including those without this privilege, may use the Scheduled Reports Viewer to monitor the status of scheduled reports.

Table 3: System Access-Based Privileges

Permissions	Permission Privileges
Snooze All Events	Applies to all events a user can manage by using the Manage Item Events action set. This action set should be used carefully because it is a system-wide snooze.
System Configuration Tool	Gives users with Standard Access at releases earlier than 7.0 the following privileges: Access to SCT, Configure and Simulate using the SCT, and Import Integration. Tenant Access users do not have access to the SCT. ⓘ **Note:** • For a unified ADS, ADX, OAS, or ODS with SCT, the SCT system privilege does not provide the user access to SCT when assigned using the ADS, ADX, OAS, or ODS Security Administration window. Instead, assign the user to the System Configuration Tool system privilege using the Security Administration window in SCT.

1 This privilege does not apply to users with Tenant Access, and does not appear in the System Privileges for Role/User dialog box for Tenant Access accounts (Figure 7). See Access Type for more information.

Role/User Assigned Tab

The Role/User Assigned tab in the **System Privileges for User Operator** dialog box shows only those system level permissions directly assigned to the role or user.

Figure 7: System Privileges User Assigned Dialog Box

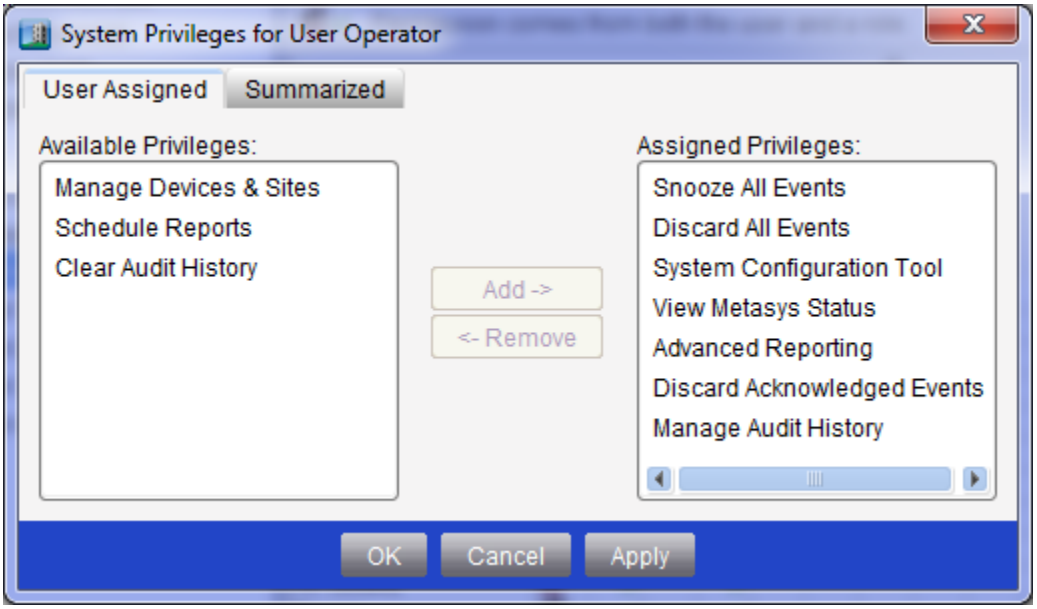


Table 4: Role/User Assigned Tab Parameters

Field	Description	Default Value
Available Privileges	Displays the available System Privileges that may be assigned to a user or role.	All Available Privileges
Assigned Privileges	Displays the System Privileges assigned to the user or role. ⓘ **Note:** For Metasys Release 7.0 or later, assigning the **System Configuration Tool** privilege through the SMP does not grant the user access to the application. The SCT user system privileges are maintained and accessed separately through the SCT UI.	—
Add	Moves the selected Privileges from the **Available (System) Privileges** list box to the **Assigned (System) Privileges** list box. Privileges are then assigned to the user or role.	—
Remove	Moves the selected Privileges from the **Assigned (System) Privileges** list box to the **Available (System) Privileges** list box. Privileges are then removed from the user or role.	—

Summarized Tab

When you are viewing user system privileges, select the **Summarized** tab to view all system privileges assigned to the user either directly or by a role. This tab includes the same information as the **Role/User Assigned** tab, but you cannot add or remove privileges by using the **Summarized** tab. This tab does not appear when viewing role system privileges.

Actions for Metasys UI Users

Table 5 lists the actions that users can perform in the Metasys UI with the corresponding required privileges for those actions. For all of the below actions, you must have authorization category permission.

Table 5: Actions and Corresponding Privileges for Metasys UI Users

Metasys UI Action	Authorization Permission Required
Adjust	Operate Permission (Authorization Category-Based) You must have authorization category permission for the point that you are adjusting.
Override	Intervene Permission (Authorization Category-Based) You must have authorization category permission for the point you are overriding.
Release	Intervene Permission (Authorization Category-Based) You must have authorization category permission for the point you are releasing.
Take Out of Service Put Back in Service	Diagnostic Permission (Authorization Category-Based) You must have authorization category permission for the point you are taking out of service or putting back in service.

Security Scenarios

Intracomputer Password

The intracomputer password, used for authentication in inter-device communication, was removed from the following devices as of Metasys Release 10.0 and above:

- Network engines
- SCT
- Metasys UI
- NAE Update Tool
- LIP

> ⓘ **Note:** Use the intracomputer password continues for communications between devices prior to Release 10.0.

Starting with Release 10.0 and above, each device has its own unique Device Key, which is generated during the pairing process. The Site Director stores its own individual device secure key and maintains the keys of all child devices. This transition affects the pairing process between network engines and Site Director from this release onwards. For further information, refer to the *Pair NxE with Site Director* section in *Metasys SCT Help (LIT-12011964).*

Advanced Security Enabled

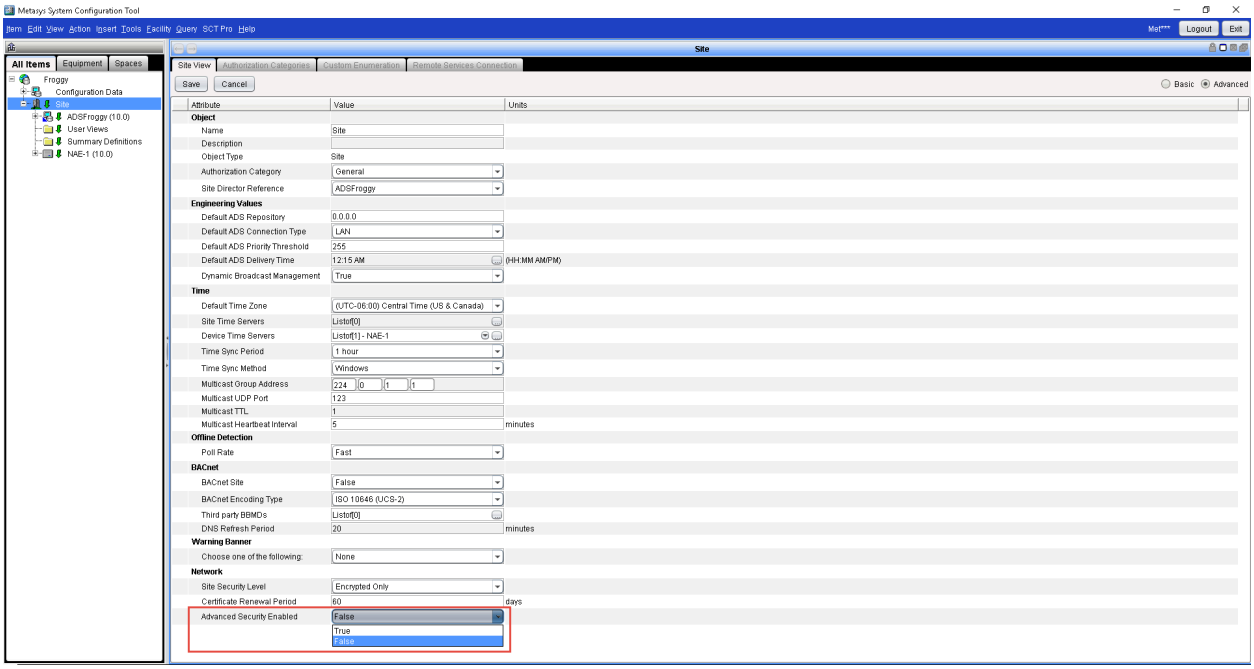
The **Advanced Security Enabled** setting in the Site object indicates if the site uses the advanced security settings. This attribute provides an improved layer of security between Metasys Site Directors and devices. With this attribute set to **True**, backward-compatible methods of communication between the Site Director and its network engines are **disabled**, which means a Site Director at Release 10.0 or later discards all communication attempts from network engines prior to Release 10.0.

Starting at Release 10.1 and later, the **Advanced Security Enabled** attribute will be set to **True** by default. At Release 10.0, this attribute is set to **False** by default. This setting applies to the entire site, so keep this attribute set to **False** if you have any network engines on the site that are running a Metasys release prior to Release 10.0. When you change this attribute to **True**, a user message appears to indicate that all network engines prior to Release 10.0 remain online, but are disconnected from the site because they no longer communicate with the Site Director.

If this message appears, click **OK** to continue and set the attribute to **True**, or **Cancel** to keep the attribute set to **False**.

You can change the Advanced Security Enabled attribute of the site object that offline using SCT or online via SMP or Metasys UI. For further information, refer to the *Metasys® SMP Help (LIT-1201793)*, *Metasys® SCT Help (LIT-12011964)*, and *Metasys® UI Help (LIT-12011953)*.

Figure 8: Advanced Security Enabled Attribute in SCT



Overview of Active Directory Service Implementation on the Metasys System

The Active Directory service used by the Metasys system is an LDAP integration. It provides an IT standard integration of the Metasys system into a customer's existing Active Directory service infrastructure for authentication purposes. This optional component provides the convenience of SSO, a capability that permits users to log in to multiple, secured application UIs without re-entering their usernames and passwords.

The Active Directory service infrastructure includes Microsoft network operating technologies that enable IT administrators to manage enterprise-wide information from a central repository. This information includes data center policy compliance and identity management (user login accounts), which are used for both Microsoft Windows OS authentication (log in to the Windows OS) and network resource authentication (log in to enterprise-wide secured applications such as email and the Metasys system). At Release 8.1 and later, the User Principal Name (UPN) authentication support for the Metasys system is now in compliance with Microsoft Office 365 authentication. For instructions on enabling the new UPN format, see the Steps to Enable Exact UPN Format section.

Note: The Metasys system does not require any particular Active Directory service structure.

Authentication Process

Without Active Directory service integration, authentication is performed through an internal Metasys login process against a local Security database. With Active Directory service integration, authentication is performed for Active Directory service users against an Active Directory service authority called a Domain Controller. If you are logged in to the operating system with an Active Directory service user account that is privileged on the Metasys system, you proceed directly to the main Metasys SMP UI screen without stopping at the login screen. The Metasys system provides this SSO function for any Active Directory service user who is also a Metasys system user, regardless of how they accessed the Site Director (either locally at the Site Director computer itself or remotely from a client machine that is directly addressable on the network).

Situations When Metasys System Login Screen Appears

The following situations cause the Active Directory service user to be presented with the Metasys system login screen:

- when you log out of the Metasys SMP UI (either manually or when a user session ends)
- if Active Directory service authentication fails for any reason
- when you are logged in to the Windows OS with an Active Directory service user account that is not privileged within the Metasys system
- if the Active Directory service Domain Controller is unavailable
- when you are logged in to the Windows OS using a local Windows account and not an Active Directory service user account
- when access to Active Directory service is restricted at login time because of an Active Directory service time sheet (known as Logon Hours) or access is restricted to the Metasys system via the Metasys time sheet. Active Directory service Logon Hours takes precedence, so if you are restricted from operating system access, but not restricted by a Metasys time sheet, access to the Metasys system as an Active Directory service user is not granted.
- if your Active Directory service user account is locked-out or disabled
- if your Active Directory service user account is enabled, but overridden to disabled with the Metasys Access Suspended property within Metasys Security Administration User Properties
- if Active Directory service authentication is disabled for the Metasys site
- if you log in to a Metasys device such as an NAE, SNC or SNE
- if Metasys authorization fails for any reason, such as when a user without SCT permissions attempts to log in to SCT
- if SSO access is disabled for the site (that is, Windows Workstation SSO is set to disabled)

When the Metasys SMP UI login window appears, and the site has Active Directory service authentication enabled, a list of available domains appears.

Figure 9: Metasys Login Screen with Active Directory Service Domain List

From the Metasys login screen, you have the following options:

- Enter an Active Directory service username and password, and click a domain in a drop-down list.
- Enter an Active Directory service username in the form of domain\username (sometimes called the pre-Windows 2000 format) and an Active Directory service password. (The **Login to** drop-down list becomes disabled.)
- Enter a fully qualified Active Directory service username in the form of **user login name@domain specifier** and an Active Directory service password. (The **Login to** drop-down list becomes disabled.) The domain specifier name must be the fully qualified domain name at the domain level for hybrid UPN authentication users or the forest level domain name for exact UPN authentication users. For more information on hybrid UPN and exact UPN authentication, see the Username Semantics section.
- Enter a Metasys local username and password and click **Metasys Local** in the **Login to** drop-down list.

  ⓘ **Note:**
  - If you select **Metasys Local**, you should enter your local user credentials, not your Active Directory service user credentials. Otherwise, authentication fails.
  - Usernames are obscured at login for local and Active Directory accounts. After login, usernames are partially obscured (for example, JSmith appears as JSm***).
  - The Metasys system only allows active user accounts to log in from this screen. Dormant or locked accounts are not accessible.

The user credentials are strongly encrypted before being transmitted over the network for authentication. (For details on the encryption process used, refer to the *Network Message Security* section of the *Network and IT Guidance Technical Bulletin (LIT-12011279)*. These credentials are active for the entire Metasys SMP UI session until you log out or the user session terminates.

If the Metasys Device Manager has not fully started, and you try to log in to the Metasys server, a runtime status error occurs and the Metasys login screen appears. In this case, the Metasys login screen does not display the Active Directory service domain drop-down list and you are not able to log in with an Active Directory service user account.

To log in as an Active Directory service user, you must close the login screen, wait a few moments for the Metasys Device Manager to fully start, then navigate again to the Metasys server. If you remain at the login screen following the startup error and do not close it, then log in with a Metasys local user account, all Active Directory service menu options and functions are unavailable. To restore Active Directory service options and functions, you must close the browser and navigate to the Metasys server again, then specify your Active Directory service credentials.

Domain List Rules

The list of domains that appear on the Metasys login screen depends on the following:

- If more than one service account is defined, the domain list displays the domains of the service accounts.
- If only one service account is defined, the domain list is based on the list of users added to the Metasys system. In other words, the domain list changes as users from different domains are added and removed from the Metasys system.

Authorization Process

After you have passed through the authentication process, the authorization step is next. Authorization is the process of verifying that a known, authenticated user has the authority to perform a certain operation. Within this process, you determine your access rights by looking up your permissions in the Metasys Security database. You may assign Active Directory service user permissions directly or through Metasys roles. You determine permissions in the same manner as for a Metasys local user.

If authorization is successful, the Metasys SMP UI appears. If either authentication or authorization fails, or if SSO is disabled, the Metasys SMP UI login screen reappears and you must continue the login process by entering either your Active Directory service or Metasys local credentials.

Table 6 lists scenarios that may occur when you log in.

Table 6: Login Scenarios for Active Directory Service Users

Are You Logged in to OS as Active Directory Service User?	Does Active Directory Service User Account Exist in the Metasys System?	Action When You Attempt SSO Login
Yes	Yes	SSO login permitted. Metasys login screen does not appear.

Yes	No	SSO login not permitted. Login screen appears with message:
		`Unable to authorize Active Directory user.`
		If you try to log in with your Active Directory service credentials, the following message appears:
		`User Access Denied.`

Yes	Yes	SSO login not permitted. Login screen appears with message: `Unable to Login. Unexpected error.` If you try to log in with your Active Directory service credentials, system access is permitted.

Yes	No	SSO login not permitted. Login screen appears with message:
		`Unable to authorize Active Directory user.`
		If you try to log in with your Active Directory service credentials, this message appears:
		`User Access Denied.`

No	Yes	SSO login not permitted. Login screen appears with message: `Unable to authorize Active Directory user.` If you try to log in with your Active Directory service credentials, system access is permitted.

Table 6: Login Scenarios for Active Directory Service Users

Are You Logged in to OS as Active Directory Service User?	Does Active Directory Service User Account Exist in the Metasys System?	Action When You Attempt SSO Login

No	No	SSO login not permitted. Login screen appears with message:
		`Unable to authorize Active Directory user.`
		If you try to log in with your Active Directory service credentials, this message appears:
		`User Access Denied.`

No	Yes	SSO login not permitted. Login screen appears with message: `Unable to authorize Active Directory user.` If you try to log in with your Active Directory service credentials, system access is permitted.

No	No	SSO login not permitted. Login screen appears with message:
		`Unable to authorize Active Directory user.`
		If you try to log in with your Active Directory service credentials, this message appears:
		`User Access Denied.`

To log out, click the **Logout** button on the SMP UI of the Metasys server. This action returns you to the Metasys login screen or Warning Banner screen, if enabled, but does not log you out of Microsoft Windows or the Active Directory service. The login screen or the Warning Banner screen, if enabled also appears if your session becomes inactive and times out.

If you exit the Metasys system by closing the Metasys SMP UI window, you are logged out, but the Metasys login screen does not appear.

Active Directory service passwords are not maintained or cached within the Metasys Security database; therefore, they cannot be changed using the Metasys SMP UI. The Security Administrator system maintains passwords for Metasys local accounts.

Active Directory Service - User Administration

Use the Metasys Security Administrator System available on the Metasys server or SCT to add existing Active Directory service users to the Metasys system. The Security Administrator System does not create or maintain user accounts in Active Directory service, it uses existing Active Directory service user accounts. Active Directory service tools handle any changes to Active Directory service user accounts such as password changes or resets. For details on adding Active Directory service users, see User Account Rules.

The system creates a Metasys system audit record whenever you add or remove an Active Directory service user from the Metasys system. Use the Security Administrator system to assign Metasys privileges to Active Directory service users that you have added to the Metasys system. These privileges include those based on system, category, feature, and property.

You assign and maintain all privileges for Active Directory service users in the same way as for Metasys local users. You can use the same windows, menu options, and tabs that you use when

you administer a Metasys local user. However, some UI screens display a combination of Metasys specific data and Active Directory service data, whereas other screens display some options unavailable. For example, the telephone number and email address properties for Active Directory service users appear but you cannot edit them because these are properties under the control of Active Directory service. The dimmed label Active Directory precedes such properties.

Any Standard Access administrator can assign permissions to any Active Directory service user that you have added to the Metasys system. You can assign privileges directly to the Active Directory service user or assign the user to a Metasys role. Also, Standard Access Administrators have full control to add, remove, update, and assign permission operations for any Metasys Active Directory service user.

User Name Synchronization in the Metasys System

To ensure that current Active Directory service user information appears in the Security Administrator system, you can use an automatic synchronization process. You initiate this process whenever you click a user's name in the Active Directory folder. Any changes to the user's account recorded in that user's properties are refreshed. If you cannot read a particular user property from Active Directory services or if the Metasys system cannot successfully use the service account for Active Directory services. For example, if the specified service account password is invalid. A question mark icon ( ) appears to the left of the property's name. Any property value the UI shows reflects its value from the last successful synchronization with the Active Directory service.

If an Active Directory service attribute shows no value in the Security Administrator system, make sure that the attribute has a value on the Active Directory service domain server. Such attributes include Active Directory Description, Phone Number, Full Name, and E-mail. The synchronization process cannot determine whether a particular attribute is unspecified or cannot be read from the Active Directory service domain server.

If you delete an Active Directory service user from Active Directory service, the account becomes disabled in the Metasys system, the user's properties and privileges in the Metasys SMP UI become read-only, and the Metasys Access Suspended property is enabled. A small red X appears next to that user's icon in the Active Directory Users list see Figure 11. See Table 7 for the icons that indicate the current Active Directory service and Metasys access status for a user.

Table 7: Icons that indicate Active Directory service user status

Standard Access icon	API Access icon	Tenant Access icon	Description
			• Metasys access is enabled • Active Directory service access is enabled • Metasys Access Suspended property is cleared
			• Metasys access is suspended • Metasys Access Suspended property is selected
			• User is disabled in Active Directory service • Metasys Access Suspended property is cleared

An Active Directory service user is also marked as deleted if the synchronization process fails to return any attributes for the user. The synchronization process cannot determine the cause of this behavior. Once the error condition is resolved, the user is re-enabled in the Metasys system the next time the user is synchronized.

When a user is removed from Active Directory service, the Metasys system continues to store privileges for a user until a Metasys administrator manually removes the user from the Metasys system.

User Account Rules

When inserting an Active Directory service user with the Metasys Security Administrator tool, note the following rules:

- For each user account, use the User Principal Name (UPN) format for the username. If you have enabled the exact UPN format at Release 8.1 or later, you do not need to provide the Fully Qualified Domain Name (FQDN). For example, you can use **myUser@corp.com** instead of **myUser@my.corp.com**. For more information on enabling the exact UPN format, see the Steps to Enable Exact UPN Format section.

  ⓘ **Note:** Users who have not enabled the exact UPN format must provide the FQDN. For example, specify **myUser@my.corp.com** instead of **myUser@corp.com** even though the latter is a valid form of the username. Figure 10 shows the screen for adding an Active Directory service user.

  The fully qualified username is used to identify the currently logged in user on the main Metasys SMP UI screen (Figure 11). The name also appears as the username on Metasys reports and logs (Figure 11). For more details on how to specify an Active Directory service user name, see Username Semantics.

- Each user you specify must exist and be enabled in Active Directory service. Properties of the user, such as the phone number and email address, are read when you add the user to the Metasys system. The Metasys SMP UI displays these items under User Properties. For details, see Information Obtained from Active Directory Services.

Figure 10: Adding an Active Directory Service User

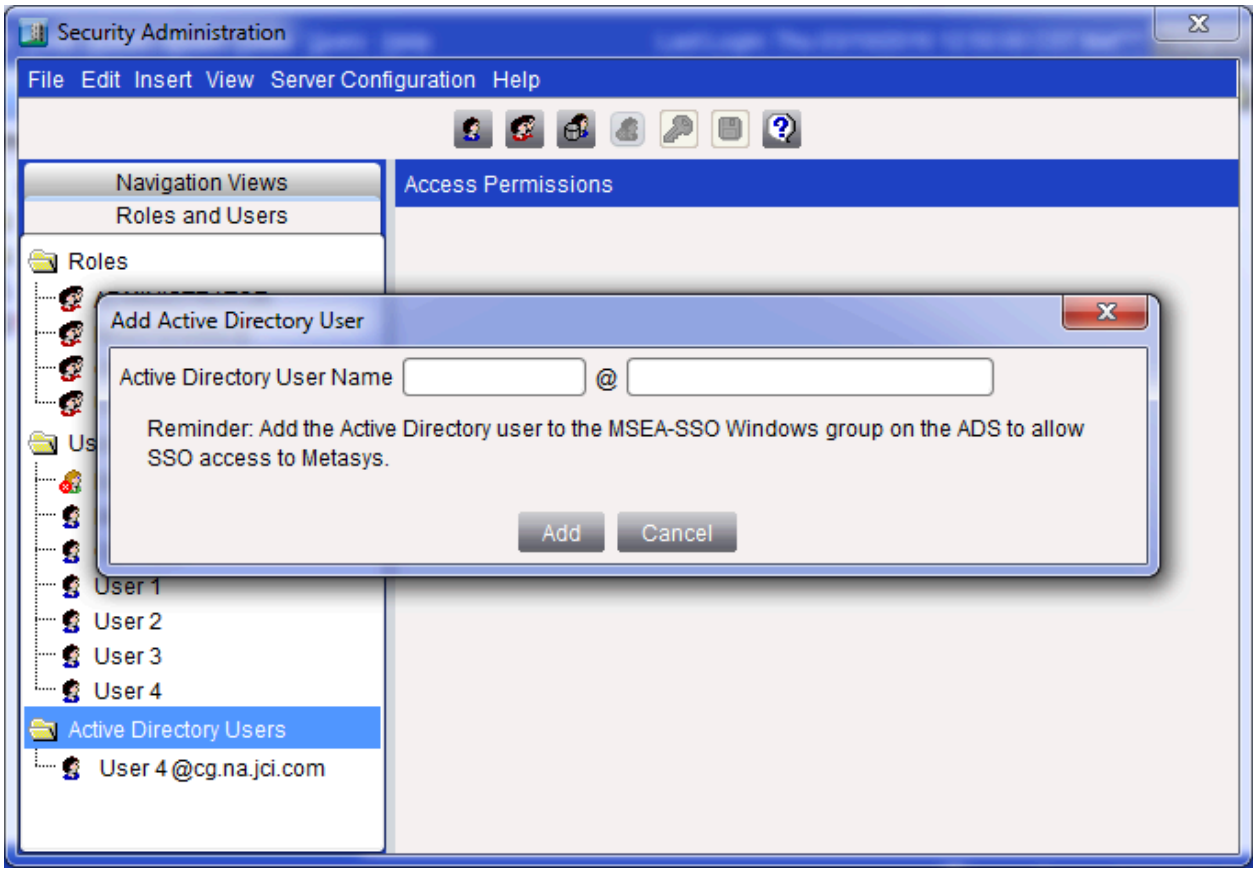
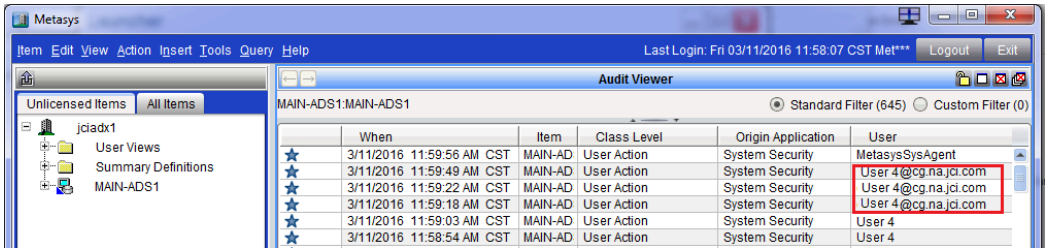


Figure 11: Identifying Active Directory Service User



- If the username for an Active Directory service user changes, you do not need to specify the new name with the Metasys System Administrative tool. Before the user can log in again, update the username with the Security Administrator tool by clicking the Active Directory service user account. For details, see User Name Synchronization in the Metasys System.

- If an Active Directory service user is deleted from the Active Directory service database, delete that user from the Metasys system as well. If you add an Active Directory service user with the same username to the Active Directory service database, but you did not delete this user from the Metasys system, you cannot add the new user to the Metasys system until the original user is deleted.
- If you disable an Active Directory service user in the Active Directory service database, the Metasys Access Suspended property check box in the user's Properties window becomes selected. Once you re-enable the Active Directory service user, a Metasys Administrator must manually clear the Metasys Access Suspended property check box before the user can log in again.
- The Metasys system follows the text case format dictated by Active Directory services. In other words, if you add a user called **MYUSER@my.corp.com,** and the Active Directory service format uses all lowercase characters, the username adjusts to **myuser@my.corp.com** when added, because the user name is not case sensitive.
- At least one defined service account for Active Directory service must have the privilege to read the user's Active Directory service attributes. For more details, see Information Obtained from Active Directory Services and Service Account.

Username Semantics

An Active Directory service fully qualified username consists of three parts: the user login name, an at sign (@), and the domain specifier:

{User Login Name}@{Domain Specifier}

Note: Active Directory usernames cannot be the same as a local Metasys username.

The user login name must be an existing name that is a member of the Active Directory service, and the domain specifier can be either at the domain level or at the forest level depending on your `web.config` file **appSettings** section. For more information, see the Steps to Enable Exact UPN Format section.

At Release 8.1 and later, you can enable authentication for an exact UPN format that complies with Microsoft Office 365 authentication in which the **domain specifier** is at the forest level. For example, you can have company.com instead of division.company.com.

If the hybrid UPN format is the only UPN format available, the **domain specifier** must be a fully qualified domain name (FQDN). For example, division.company.com instead of company.com.

If you rename the user's login name, the Metasys Administrator must synchronize the user with Active Directory service before the rename is recognized in the Metasys system. The user cannot use SSO login-free access to the Metasys system until the synchronization occurs. For synchronization details, see User Name Synchronization in the Metasys System. If you change the domain specifier for the user, that is, move the user to another domain, you must delete the original user, then re-add the user to the Metasys system using the new domain name.

You can add an Active Directory service user with any of these methods see Figure 28:

- In the toolbar section of the Security Administration screen, click the **Add Active Directory User** icon.
- On Security Administrator screen, click the **Insert > Insert Active Directory User** menu option.
- In the **Roles and Users** tab, right-click the **Active Directory Users** folder.

You can change a Metasys system user account from a Metasys local account to an Active Directory service user account. However, since the Metasys system does not provide a method to convert the user directly, choose on of the following options:

- Keep the Metasys local user account active as a backup account in case the Active Directory service becomes temporarily unavailable. Remember that the new Active Directory service user account is not linked in any way to the Metasys local account. This means that, the local account remains under the control of the existing Metasys system tools, including password changes.
- Disable the Metasys local account after you are sure that you have correctly set up the user's Active Directory service user account in the Metasys system.
- Delete the Metasys local account after you are sure that you have correctly set up the user's Active Directory service user account in the Metasys system.

Under normal circumstances, each user needs one account to access the Metasys system.

Information Obtained from Active Directory Services

The Active Directory service used by the Metasys system reads a set of information from the Active Directory service database and populates or updates the user's Properties based on those values. The following information is read, with the actual Active Directory service attribute names in parentheses:

- User name (samAccountName, userPrincipalName, CanonicalName)
- Description (Description)
- Full name (displayName)
- Email (mail)
- Phone number (telephoneNumber)
- Account disabled (UserAccountControl)

In addition, the Active Directory service database provides the Security Identifier (ObjectSID), which is used internally to uniquely identify the Metasys user.

Service Account

The Metasys system requires a service account in Active Directory service consisting of an Active Directory service username and password. The feature uses this service account when querying Active Directory service. The system allows for the use of one service account to access all domains, or one service account per domain. For details, see Service Account Rules.

The customer's IT department defines the service account username and password. You should create this user with a non-expiring password. If the IT department requires the modification of the service account password on a periodic basis, you must define a Metasys system work process to update the password in the Security Administrator System at the time it is changed in Active Directory service. If the service account password in the Metasys system does not match the service account password in Active Directory service, Active Directory service users cannot access the Metasys system.

Service Account Rules

When specifying a service account with the Metasys Security Administrator tool, apply the following rules:

- For each service account, use the UPN format for the username and provide the domain specifier. For example, use **metasys.service@my.corp.com** for the hybrid UPN formats and use **metasys.service@corp.com** for exact UPN formats.

  ⓘ **Note:** Starting at Release 8.1 and SCT 11.1 and later, to enable the email UPN authentication format, manually edit the web.config files.

- The tool does not allow a blank password for a service account.
- Whenever you change the domain or username of the service account with the Metasys Security Administrator tool, you must also enter the password.
- You can specify more than one service account. You only need to specify more than one service account if an Active Directory service trust does not exist between the domain in which the service account is created and all other domains where Metasys users reside. In this case, specify one service account per domain where the Metasys users reside.
- You should configure the service account with a non-expiring password; however, if the password is set to expire, you need to reset it in the Metasys Security Administration system tool each time you reset it on the Active Directory service domain.

Service Account Permissions

The Metasys system requires that the service account for Active Directory service allows for a minimal set of permissions. This section lists these permissions but does not dictate how they should be applied; the customer's IT department determines how they should be applied when the permissions are created. The permissions are as follows:

- Read-only access to the domain object of each domain that includes Active Directory service users who are Metasys system users.
- Read-only access to the each organizational unit that includes Active Directory service users who are Metasys system users.
- Read-only access to the attributes of each Active Directory service User Object that are Metasys system users or read access to only the following individual attributes on those user objects (if full read access is not allowed):
  - objectSID
  - sAMAccountName
  - displayName
  - description
  - mail
  - userPrincipalName
  - telephoneNumber
  - userAccountControl
- Non-expiring service account password (see Service Account Rules).
- The service account must be able to access all domains with Metasys system users to do LDAP queries. For example, accounts cannot be denied access to the domain controller by the domain's security policy.

Restrictions

The Active Directory service on the Metasys system has the following restrictions:

- The Active Directory service for use by the Metasys system with SSO login-free access and login access is available for the Metasys server and SCT; it is not available when you log in to an NAE, NCE, SNC, or SNE directly.
- The **Change Password** menu option is disabled for an Active Directory service user. An Active Directory service user may not change their Active Directory service user account password through the Metasys system SMP UI.
- Metasys Active Directory service users cannot log in as Metasys local users. They must use their Active Directory service username, password, and domain name to log in.
- Existing Metasys local users must not use the reserved characters of @ or \ in their usernames. This restriction is necessary to avoid collision with fully qualified Active Directory service usernames.

Active Directory and SSO Logins with Metasys Applications

Table 8 summarizes which Metasys system application UIs support Active Directory username and password logins and the SSO capability. If the application supports Active Directory username and password login, then the Metasys application can use an Active Directory username and password at the login screen for authentication purposes. If the application supports SSO, then the application can authenticate based on the Active Directory user currently logged in to the Windows desktop without the user reentering the Active Directory username and password again at the Metasys login screen.

Table 8: Products That Support Active Directory Logins and SSO

Application	Active Directory Username/ Password Logins Supported	SSO Supported
ADS SMP UI	Yes	Yes
ADX SMP UI	Yes	Yes
OAS SMP UI	Yes	Yes
ODS SMP UI	Yes	Yes
SCT UI	Yes	Yes
Metasys Advanced Reporting System	No	No
Metasys for Validated Environment (MVE)	Yes	No
Metasys UI and Metasys UI Offline	Yes (Computer) Yes (Mobile Phones and Tablets)	No
NAE/NCE	No	No
NIE	No	No
SNC	No	No
SNE	No	No

The following important aspects relate to Active Directory:

- If you are using Metasys Advanced Reporting System UI on anMetasys server, you still can use the SSO or Active Directory username and password login capability to log in to the server UI. For example, if you have an ADX with the Metasys Advanced Reporting System, you can use SSO to log in to the ADX UI but you must enter your Metasys system username and password pair to log in to the Metasys Advanced Reporting System UI.
- The NAE/SNC/SNE UIs do not currently support authentication with Active Directory service. However, if you have an Metasys server Site Director, you can log in to the server UI using SSO or Active Directory username and password and access system information for the entire site, including details on the NAE/NIE.
- If you are using the Metasys for Validated Environments (MVE), the SSO login-free access is supported for the SCT but is not supported for the Metasys SMP UI. Active Directory users can still select a domain and use their Active Directory user names and passwords on the SMP login screen if the Active Directory feature is enabled and configured.
- If you are using an SMP UI with the Warning Banner enabled, Active Directory users must agree to the conditions on the warning statement before SSO login-free access is granted.

Active Directory Service with SCT

Even if you are logged in to SCT with an Active Directory user account, you must provide a Metasys local account to perform upload, download, and synchronize tasks with a target device at the Site Login screen of the wizard. To indicate this requirement, the Manage Archive Wizard's Site Login screen displays the text `Active Directory users may not be used to log into the site`. Another option is to log in to SCT with a Metasys local user account with appropriate privileges, which populates the log in information for you.

Steps to Enable Active Directory Service for Use by the Metasys System

By default, the Active Directory service for use by the Metasys system on the *Metasys* server or SCT computer is disabled. You must perform a number of required actions to enable the Active Directory service for use by the Metasys system. Different individuals within the organization sometimes perform these actions. Table 9 provides an overview of these actions. If any of these steps are specific to the Metasys product, they are further described in the sections that follow.

Table 9: Overview of Actions Required for Enabling Active Directory Service for Use by the Metasys System

Step	Action	Who Is Responsible	Comments/Literature Reference
1	Configure the Domain Name System (DNS) on the Metasys Site Director.	Microsoft Windows Administrator	Accomplished by using standard Microsoft Windows network configuration tools. Refer to Microsoft Windows networking documentation. ⓘ **Note:** Active Directory services rely on DNS functionality.
2	Add Metasys Site Director to an Active Directory service Domain.	Active Directory Service Administrator	Accomplished by using any available method. Refer to appropriate vendor documentation.

Table 9: Overview of Actions Required for Enabling Active Directory Service for Use by the Metasys System

Step	Action	Who Is Responsible	Comments/Literature Reference
3	Within the Active Directory service, create one or more service accounts the Metasys application can use. If more than one account is assigned, use only one account for each domain.	Active Directory Service Administrator	Accomplished by using an Active Directory service user administrative tool. The Metasys application uses these credentials when making requests to Active Directory services. Refer to the following sections: Service Account, Service Account Rules, Service Account Permissions. Also, refer to *Appendix: Active Directory Service* in the *Network and IT Guidance for the BAS Professional Technical Bulletin (LIT-12011279)* and to the Active Directory service documentation available from Microsoft Corporation.
4	Communicate the service account credentials created in Step 3 to the Metasys Security Administrator.	Active Directory Service Administrator	User name login, domain specifier, and password are communicated for each account created.
5	Enable Active Directory service authentication for the Metasys site.	Metasys Administrator	Accomplished by using the Metasys Security Administrator Tool. See Enabling Active Directory Service Integration for Metasys server or SCT Software.
6	Enter the domain, username, and password for assigned Active Directory service user accounts (received from the Active Directory Service Administrator in Step 4).	Metasys Administrator	Accomplished by using the Metasys Security Administrator Tool. See Enabling Active Directory Service Integration for Metasys server or SCT Software.
7	Add each existing Active Directory service user to Metasys and authorize each to access Metasys functions. (This is an ongoing task.)	Metasys Administrator	Assumes that the Active Directory service users have already been created in Active Directory service by an Active Directory Service Administrator. This step is revisited each time changes occur to the set of Active Directory service users, and therefore, is part of ongoing user administration.
8	Select the default domain to be displayed in the domain list box located on the Metasys Login screen. (This is optional.)	Metasys Administrator	Accomplished by using the Metasys Security Administrator Tool. See Enabling Active Directory Service Integration for Metasys server or SCT Software.

Steps to Enable Exact UPN Format

About this task:
Prior to Metasys Release 8.1, a hybrid UPN format that uses a username with the FQDN was the only UPN option available. An example of this hybrid UPN format is myUser@my.corp.com.

Starting at Metasys Release 8.1 and SCT 11.1 and later, you can enable an exact UPN name authentication that does not require the FQDN. An example of this exact UPN format is myUser@corp.com.

Follow these steps to enable this authentication method:

1. Open Notepad by right-clicking and selecting **Run as Administrator**.
2. In Notepad, click **File** > **Open**.
3. Browse to `C:\Program Files\Johnson Controls\MetasysIII\ws` and right-click on the `web.config` file.

   ⓘ **Note:** By default, the Metasys software and databases are installed to the C: drive. If you have customized the installation location, specify the location. For example, if you installed on drive E, use E:\.
4. Click **Open**.
5. Modify the following key under the<configuration><appSettings> section from false to **true**:
   <! --Whether to validate onexact UPN for Office365 style ActiveDirectory --
   ><addkey="enableOffice365StyleActiveDirectoryAuthentication"value="**true**"></add>
6. Save and close the `web.config` file.
7. If SCT **is not** installed on the same computer as the Metasys server, restart the target server.
   If SCT **is** installed on the same computer as the as the Metasys server, continue to Step 7a.

   a. Open Notepad by right-clicking and selecting **Run as Administrator**.
   b. In Notepad, click **File** > **Open**.
   c. Browse to `C:\Program Files\Johnson Controls\MetasysIII\Tool` and right-click on the `web.config` file.

      ⓘ **Note:** By default, the Metasys software and databases are installed to the C: drive. If you have customized the installation location, specify the location. For example, if you installed on drive E, use E:\.
   d. Modify the following key under the<configuration><appSettings> section from false to **true**:
      <! --Whether to validate onexact UPN for Office365 style ActiveDirectory --
      ><addkey="enableOffice365StyleActiveDirectoryAuthentication"value="**true**"></add>
   e. Save and close the `web.config` file.
   f. Restart the target server.
8. After editing the `web.config` files, you can begin adding Active Directory users with exact UPN usernames to the Metasys system using the Security Administrator System.

Site Director Demotion

If you demote a supervisory controller from a Site Director to a child device on the site, all local and Active Directory service user accounts that you added to the device while it was a Site Director remain in the Security Database unless you manually remove them. If you do not manually remove

them, any user with an active (enabled) account in the Security Database may locally log in to the demoted device.

Also, user accounts from the demoted device are not synchronized with user accounts on the new Site Director. This feature prevents you from maintaining the user accounts from the demoted sites. For example, if you change the privileges of a user account at the Site Director, these changes do not propagate to the demoted device. For details on how to manually remove a user account from a demoted Site Director, refer to the *NAE Commissioning Guide (LIT-1201519)*, *SNC Commissioning Guide (LIT-12013295)*, *SNE Commissioning Guide (LIT-12013352)*, the *ADS/ADX Commissioning Guide (LIT-1201645)*, *ODS Commissioning Guide (LIT-12011944)* and the *Open Application Server (OAS) Commissioning Guide (LIT-12013243).*

Security Menu Options

The following menus are available in the Security Administrator.

Table 10: Security Menu Options

Menu	Selection	Description
File	Exit	Closes the Security Administrator.
	Save	Saves the modified permissions in the security grid.
Edit	Delete	Deletes a user-defined role or a user-defined user. Prompts for confirmation before deleting.
	Properties	Opens the **Role Properties** or **User Properties** window.
	System Access Permissions	Opens the **System Privileges** dialog box.
	Account Disabled	Marks the selected user account as disabled. The next time the user attempts to log in to the system, an account disabled message appears. An administrator must enable the user account through the User Properties. ⓘ **Note:** This option is not available to Active Directory service users.
Insert	New User	Adds a new user to the **Roles and Users** tree. The **User Properties** dialog box appears.
	New Role	Adds a new role to the **Roles and Users** tree. The **Role Properties** dialog box appears.
	Copy of User	Inserts a copy of the selected user into the **Roles and Users** tree. The **User Properties** dialog box appears. You can edit the copied user's properties.
	Copy of Role	Inserts a copy of the selected role into the **Roles and Users** tree. The **Role Properties** dialog box appears. You can edit the copied roles.
	Insert Active Directory User	Adds a new Active Directory service user to the Roles and Users tree. The **User Properties** dialog box appears. ⓘ **Note:** This option is only available if the Active Directory Service is enabled.
View	Tool Bar	Displays the Security Administrator toolbar.
	User Preferences File Names	The MetasysSysAgent administrator can view the name of the user preferences file for each account. You view file names to manage user and system preferences files on the device. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*, the *NAE Commissioning Guide (LIT-1201519)*, the *ODS Commissioning Guide (LIT-12011944)* or the *Open Application Server (OAS) Commissioning Guide (LIT-12013243)* for details.
Server Configuration	Active Directory	Configures Active Directory service for use by Metasys system users. The **Configure Active Directory** dialog box appears.

Table 10: Security Menu Options

Menu	Selection	Description
Help	Help Topics	Opens the *Metasys Site Management Portal Help (LIT-1201793)*. There is no Help system for the Security Administrator system. Information about the Security Administrator system is located only in this document. ⓘ **Note:** A **File Download** dialog box may appear. To open the Help system, click **Open**.
	About Metasys	Opens the **About Metasys** pop-up box that displays the system name, installed version, version number, graphics version, and copyright stamp. Click **Terms & Conditions** for terms and conditions of use information.

Security Toolbar and User Access Icons

Table 11 describes the Security toolbar options, and Table 12 provides descriptions of the icons that appear next to a username.

Table 11: Security Toolbar

Icon	Description
	Adds a new user to the **Roles and Users** tree. The **User Properties** dialog box appears.
	Adds a new role to the **Roles and Users** tree. The **Role Properties** dialog box appears.
	Adds a new Active Directory service user to the **Roles and Users** tree. The **Add Active Directory User** dialog box appears.
	Marks the standard user account as disabled. Next time the user attempts to log in to the system, an account disabled message appears. An administrator must enable the account through the User Properties. ⓘ **Note:** Active Directory service users cannot be disabled in this manner. Active Directory Service administrator manages account accessibility.
	Opens the **System Privileges** window. ⓘ **Note:** If you select apredefined role or predefined user, the System Access Permissions are read-only.
	Saves the category-based permissions information.
	Opens the *Metasys Site Management Portal Help (LIT-1201793)*, *Metasys SCT Help (LIT-12011964)*, *Open Application Server (OAS) Commissioning Guide (LIT-12013243)*, or the *Open Data Server (ODS) Help (LIT-12011942)*. There is no Help system for the Security Administrator system. Information on the Security Administrator system is located only in *Security Administrator System Technical Bulletin (LIT-1201528)* (this document). ⓘ **Note:** A **File Download** dialog box may appear. To open the Help system, click **Open**.

Table 12: Icons That Indicate User Accessibility

Icon	Description
	Standard access user account is enabled.
	API Access account is enabled.
	Tenant access user account is enabled.
	Standard access Metasys user account is disabled (**Account Disabled** property check box selected). Metasys system access is suspended for standard access Active Directory service user. (**Metasys Access Suspended** property check box is selected).
	Standard access Active Directory service user account is disabled in Active Directory service (**Metasys Access Suspended** property check box is cleared).
	API Access Metasys local user account disabled (**Account Disabled** property selected). API access Active Directory service user account has Metasys system access suspended (**Metasys Access Suspended** property check box is selected).
	API access Active Directory service user account is disabled in Active Directory service (**Metasys Access Suspended** property check box is cleared).
	Tenant access Metasys local user account disabled (**Account Disabled** property selected). Tenant access Active Directory service user account has Metasys system access suspended (**Metasys Access Suspended** property check box is selected).
	Tenant access Active Directory service user account is disabled in Active Directory service (**Metasys Access Suspended** property check box is cleared).

Access Type

The Security Administrator system provides three types of access for user accounts: Standard Access, Tenant Access and API Access.

- **Standard Access**: The Metasys local system user or Active Directory service user can access all authorized features of the online SMP UI and the SCT. Users can also access the Metasys UI.

  ⓘ **Note:** If you have Standard Access and the Advanced Reporting privilege, you can use the Metasys Advanced Reporting System.

- **Tenant Access**: The Metasys local system user or Active Directory service user can access all authorized features of the Metasys UI.
- **API Access**: The Metasys local system user or Active Directory user can access the API, as well as all authorized features of the Metasys UI. API Access users can also access limited features of the SMP UI.

Administrators can assign access types for users on the **User Properties** tab of the **Properties of User Operator** dialog box. See Figure 14 and User Properties Tab – Metasys Local User.

Access types must meet the following requirements:

- Each user account can have only one type of access to the Metasys system.
- Users requiring Standard Access, Tenant Access, and API Access must have a separate user account for each access type with different user names.
- A user who wants both a Metasys local account and an Active Directory service user account must have separate user accounts for each.

- You can use a user account with Standard Access to log in to the online SMP UI, and the SCT.
- When upgrading the Security Database from a version prior to Release 2.0, each user account defaults to the Standard Access type.
- A user with a Metasys local account must select the Metasys Local option on the login screen for the SMP UI or the SCT. A user who is an Active Directory service user must select the appropriate domain name on the login screen.
- Tenant users cannot be Metasys system administrators and cannot have any of the following system-level privileges:
    - System Configuration Tool (SCT)
    - Advanced Reporting (Metasys Advanced Reporting system)
    - Clear Audit History (clear audit log)

Administrators

The Security Administrator system provides predefined administrators for user account: MetasysSysAgent.

MetasysSysAgent (Standard Administrator)

MetasysSysAgent (Standard Administrator) is a user account with the ADMINISTRATOR role and the Standard Access type assigned. All Standard administrators can access the full Security Administrator system by using the Metasys system online user interface and the SCT. The initial login username is MetasysSysAgent and it is not case sensitive. For the MetasysSysAgent default password, contact your local Johnson Controls® representative.

ⓘ **Note:** You must change the default password for the Metasyssysagent user account on new or reimaged devices. If you use SCT to download the archive database to a device that still has the factory default password, you can log in to SCT with the default password, but prompts you to immediately change this password before you can perform the download. This action helps ensure the safety of the system. After you successfully change the password, SCT proceeds with the archive download and updates the security database on the device with the new password.

Standard administrators can change the access type for any account except MetasysSysAgent to Standard Access, API Access or Tenant Access.

All Metasys local system users and Active Directory service users who are Standard Access administrators can administer other Standard Access Metasys local system and Active Directory service users.

API Access

API access is required for to use the Metasys Application Programming Interface (API) and for API calls to function. With API Access, users can retrieve information from the Metasys system network. Use API Access to read and write Metasys system data from a custom application with the same high level of security as when you access system data through the SMP UI.

To use the Metasys APIs to perform a data request using a custom application, you need a Metasys user account, such as local or Active Directory, with the API access type and the appropriate Metasys permissions and privileges assigned. Metasys user accounts with the Standard or Tenant access type cannot use the Metasys APIs.

Metasys users with API access type can also login to Metasys using the SMP UI and the Metasys UI. API users have limited functionality in the SMP UI, but full functionality in the Metasys UI depending on their assigned permissions and privileges.

We do not recommend that users with the API access type are given the ADMINISTRATOR role. If a user with the API access type is given the ADMINISTRATOR role, that user will have full administrator rights in the Metasys UI, and limited administrator rights in the SMP UI. In the SMP UI, an API user with administrator rights can create, view, and modify user accounts with the API access type, but cannot affect any other users. In the Metasys UI, an API user with administrator rights has the same capabilities as an administrator with the Standard access type and can manage all user accounts.

Roles and Users Tab

The Roles and Users tab appears in the left pane of the Security Administrator system screen. See Figure 10.

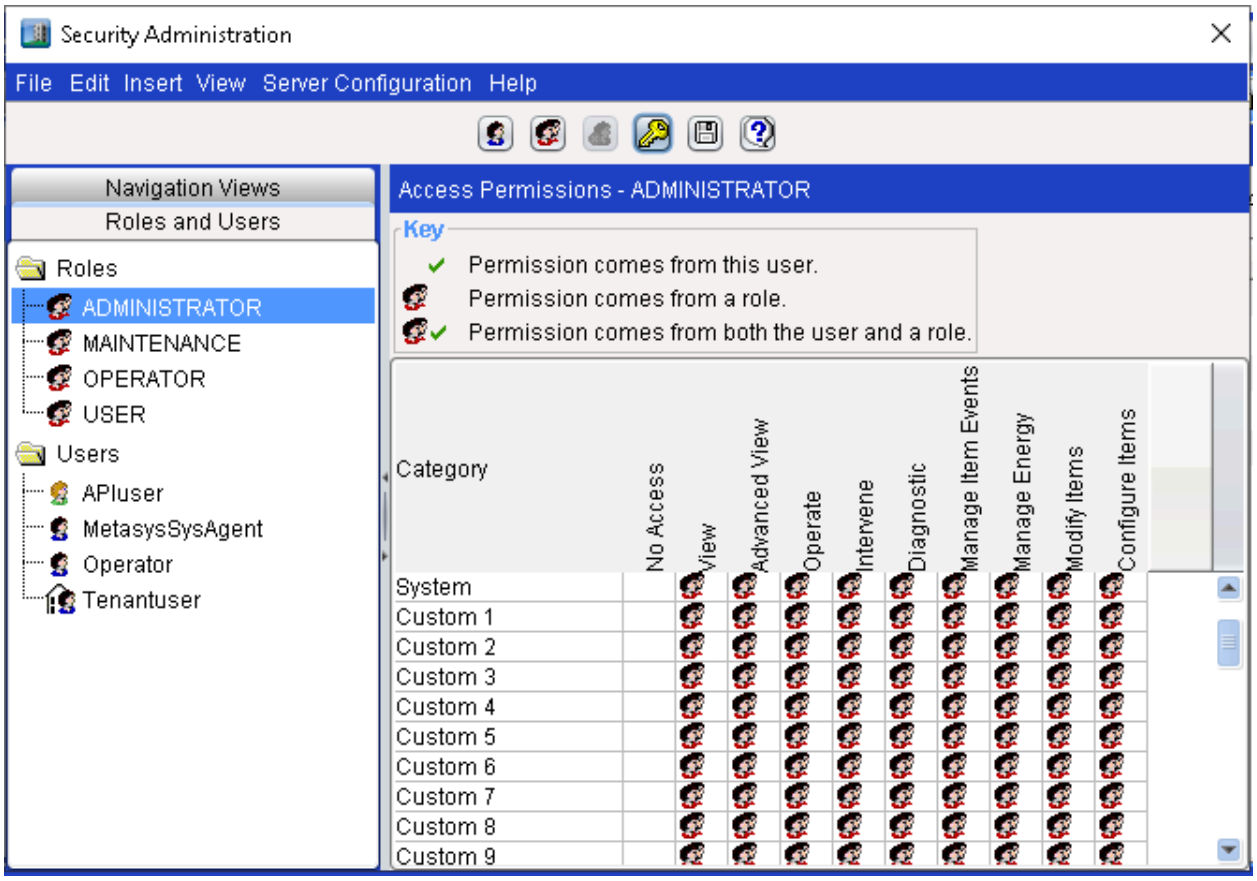
When you select a user or role on the **Roles and Users** tab, the category-based permissions appear in the right pane. To provide more capabilities to the user or role, see Assigning Category-Based Permissions to a User or Role and System Access Privileges.

Consider the following when creating user accounts and assigning roles:

- The users must have one or more roles in the system. The default role for a new user is USER. The USER role is granted read-only access (View Action set) to the General category.
- You cannot delete or rename the predefined set of users. However, you can add or remove the predefined users, except the MetasysSysAgent, to or from roles and copy the users. You can view the Access Permissions and Properties of the predefined users but you cannot edit them.
- You cannot delete or rename the predefined set of roles; however, Standard administrators can add or remove users, except the MetasysSysAgent, to or from the roles and copy the roles. You can view the Access Permissions on the predefined roles but you cannot edit them.
- You cannot delete the ADMINISTRATOR role. You cannot delete or remove the MetasysSysAgent administrator account from the system.
- You can copy and then modify the OPERATOR, ADMINISTRATOR, USER, and MAINTENANCE roles. When you copy these roles, the permissions for those roles are copied as well.

Figure 10 shows a summarized view of a user's permissions, indicating the permissions provided by roles and the permissions directly assigned to the user. The two-headed icon indicates the permission is from the role level. The green check mark indicates that the permissions are from the user level. Figure 6 shows the relationship between role and user for the user shown in Figure 10.

Figure 12: Access permissions (Active directory not enabled)



Roles and Users Pop-up Menus

When you right-click a role or user, the **Roles and Users** pop-up menu appears (Table 13).

Table 13: Roles and Users Pop-up Menu

Menu Option	Description
Delete	Deletes the selected role or user information. ⓘ **Note:** You cannot delete predefined roles and users.
Copy of	Creates a copy of the selected role or user. Not available to Active Directory service users.
Properties	Opens the **Role Properties** or **User Properties** dialog box.
System Access Permissions.	Opens the **System Privileges** dialog box. ⓘ **Note:** If a predefined role or predefined user is selected, the System Access Permissions are read-only.

If you right-click the **Users**, **Active Directory Users**, or **Roles folder** and click **Insert** on the menu, you create a New User, Active Directory service user, or Role. See Creating a Metasys local user account and Creating a new role for details.

Navigation Views Tab

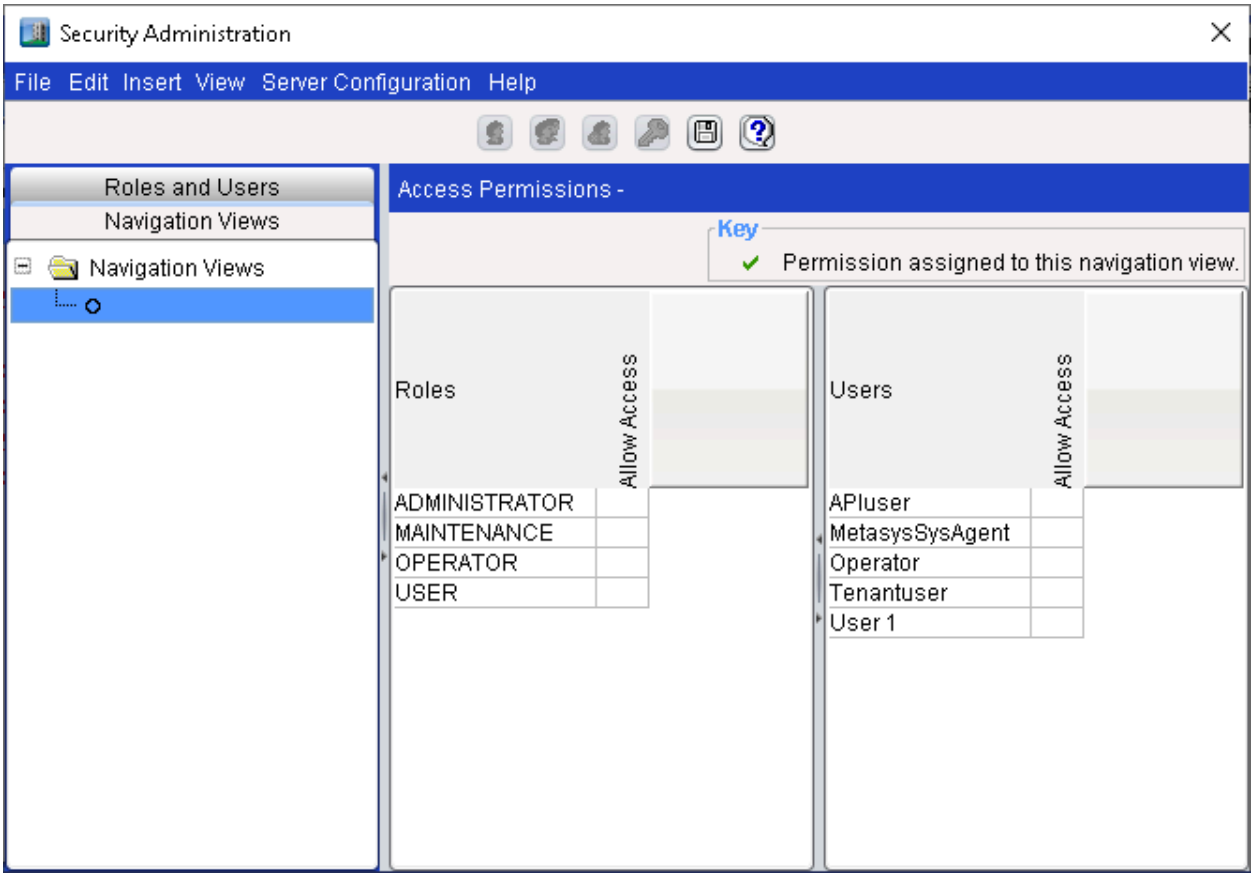
In addition to authorization category-based privileges, administrators can limit a user's access to objects by controlling which user views appear in the user's navigation frame. When users log in to a Metasys system, only their assigned user views appear in the navigation pane. User views not assigned to a particular user do not appear in the navigation pane, regardless of the authorization category assigned to the user view. This scenario allows you to limit user access to only those items in their assigned user views.

If users have access to a user navigation view, but do not have View Access to items referenced by that view due to assigned authorization category-based privileges, they can see the items in the user navigation view but cannot see the details of those items in the View panel. Users must have both user navigation View Access and authorization category View Access to see such item details.

When you create a new user view using the SMP UI, you (the creator) are automatically assigned access to the new user view; however, any user views you create in the SCT are not yet assign to any users, and an administrator must manually assigned the users views to users after downloading the views to the site.

The **Navigation Views** tab appears in the left pane of the Security Administrator system's Security Administration screen. This tab is disabled in the SCT. See Figure 13.

Figure 13: Navigation Views



The left pane lists all available user navigation views. When you assign at least one user or role to a user navigation view, the circle next to it in the list appears solid. If you do not assign users or roles to the view, the circle appears empty. The right pane shows a summary of the roles and users and their access to each user navigation view. Both Metasys local system and Active Directory service users are shown.

You also can assign access to user navigation views on the **Navigation** tabs of the **User Properties** and **Role Properties** dialog boxes. See User Properties and Role Properties.

User Properties

The **User Properties** dialog box defines users within the system. The tabs include User Properties, User Profile, Roles, Time Sheet, Account Policy, and Navigation. See Creating a Metasys local user account.

User Properties Tab – Metasys Local User

The **User Properties** tab defines the general information about the user: username, type of account, and password information (Figure 14). You can set these user properties for any new user you define. However, you cannot modify some or all of the user properties for thepredefined system user: MetasysSysAgent. This restriction is according to design. For an Active Directory service user, see User Properties Tab – Active Directory Service User.

Figure 14: User Properties Tab – Metasys Local User

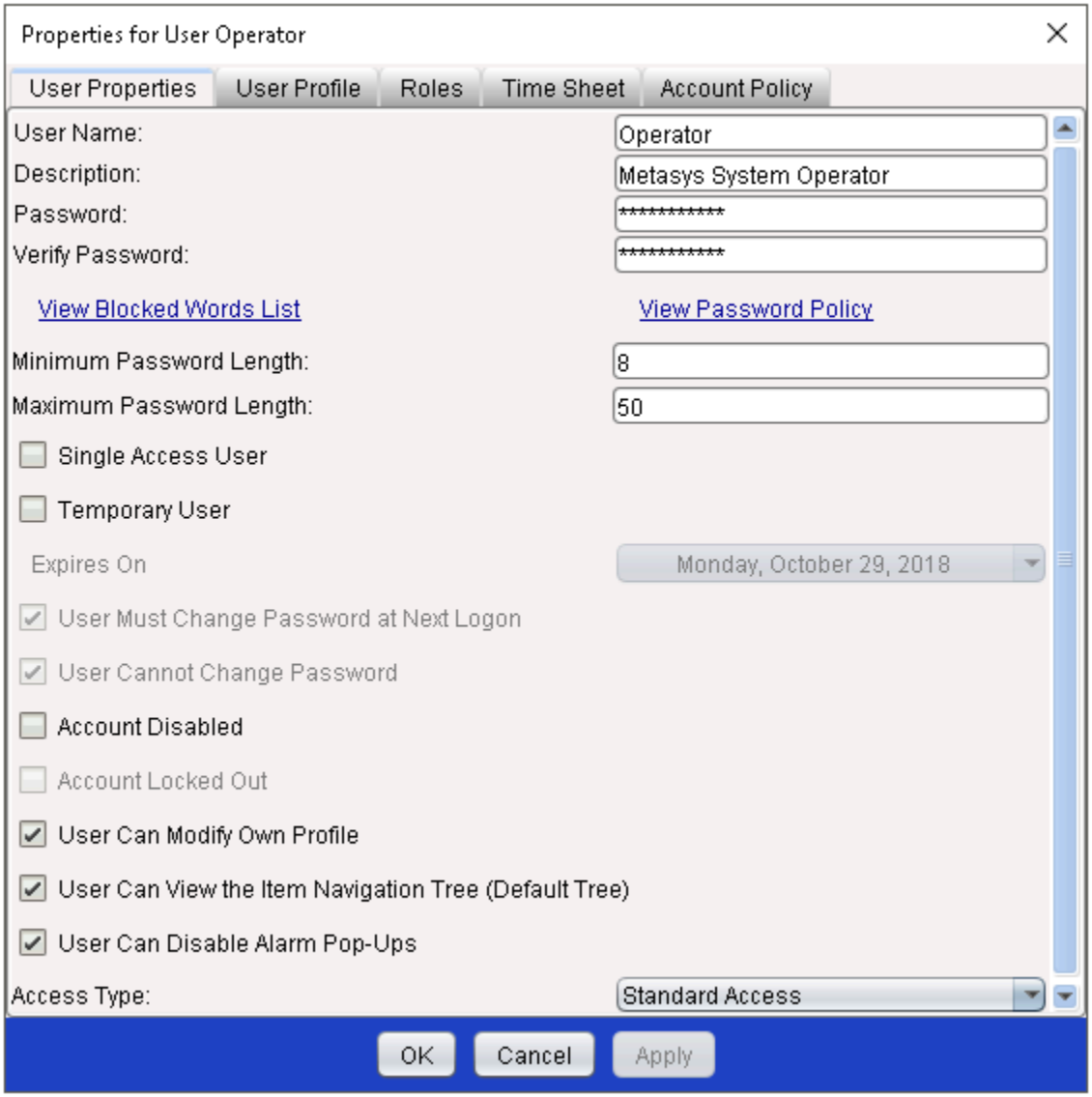


Table 14: User Properties Tab Parameters – Metasys Local User

Field	Description	Default Value	Required
User Name	Displays the login name of the user. The default name in the **User Name** field when creating a new user is New User. The default name when creating a copy of a user is **Copy of <username>**, where <username> is the name of the user being copied. ⓘ **Note:** • This login name is a Metasys system username; it is not the Microsoft Windows operating system username. However, for the MetasysSysAgent account, the username is both a Metasys system name and a Windows operating system username on the NAE/SNC/SNE platforms, excluding the server-based NAE/SNC/SNE. • Do not use extended ASCII characters to create usernames. • Do not use the @ and \ characters. These characters are reserved characters for Active Directory service usernames and cannot be used within a Metasys local username.	User Name	Yes
Description	Displays a description of the user.	---	No
Password	Displays the password entered for the user. Metasys server and engine platforms require complex passwords. For more information, see Password Rules and Password Complexity. ⓘ **Note:** For the MetasysSysAgent user only, the **Password** field cannot be edited. To change the password for the MetasysSysAgent user, select the **Tools** > **Change Password** menu option.	---	Yes
Verify Password	Confirms the letters, numbers, and symbols typed into the **Password** box. ⓘ **Note:** For the MetasysSysAgent user only, the **Verify Password** field cannot be edited. To change the password for the MetasysSysAgent user, select the **Tools** > **Change Password** menu option.	---	Yes
View Blocked Words List	Displays the Blocked Words List.		

Table 14: User Properties Tab Parameters – Metasys Local User

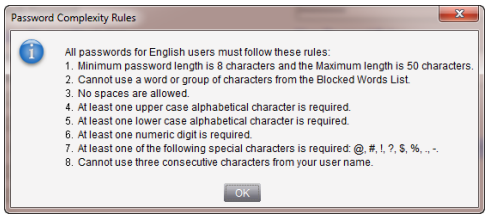
Field	Description	Default Value	Required
View Password Policy	Displays the rules for password complexity which varies for English and non-English users. For further information see Password Rules. **Figure 15: View Password Policy Window** 		
Minimum Password Length	Allows the user to set the minimum character length for the password. The default minimum character length is 8. You cannot set the minimum character length below 8 characters.		
Maximum Password Length	Allows the user to set the maximum character length for the password. The default maximum character length is 50. You cannot set the maximum character length above 50 characters.		
Single Access User	Allows the user to log in to the account once. After logging on once, the account becomes disabled.	Cleared	No
Temporary User	Allows the user to access the system as a temporary user. The user can access the account as long as it has not expired. When expired, the user is logged out of the system.	---	No

Table 14: User Properties Tab Parameters – Metasys Local User

Field	Description	Default Value	Required
Expires On	Allows the administrator to specify the date on which a temporary user's account expires. The account expires at the end of the specified date (midnight), after which the user can no longer access the system. ⓘ **Note:** If a user account is created when the Site Director is set to an incorrect future date and time and the user account password is later set to expire after some number of days, the password may not expire until the incorrect future date and time. The user account stores a timestamp for when the user's password was last changed, and the system does not expire the password until the number of days after the stored value. For example, suppose that you create a user account on Monday, November 4, 2013. However, the Site Director date is set to Monday, May 4, 2015. If you then set the user account's password to expire in 30 days, the password does not expire 30 days from Monday, November 4, 2013. To resolve this issue, ensure you select the **User Must Change Password at Next Login** option when you set a user account password to expire after a period of time. Doing so forces the user to create a new password at the next login and again after the time period has elapsed. To prevent this issue, ensure that your Site Director is always set to the current date and time.	The default value is the current date.	Yes, if temporary user selected.
User Must Change Password at Next Logon	Requires that the users change their passwords the next time they log in to the system.	Selected	No
User Cannot Change Password	Disables the ability to change the password.	Cleared	No
Account Disabled	Disables the user account	Cleared	No
Account Locked Out	Allows the administrator to reset a locked out user account.	Cleared	No
User Can Modify Own Profile	Allows the users to update their own profile information. The administrator can also change or update the profile information by using the **User Profile** tab.	Selected	No
User Can View the Item Navigation Tree (Default Tree)	Designates that a user can view the All Items navigation tree.	Selected	No

Table 14: User Properties Tab Parameters – Metasys Local User

Field	Description	Default Value	Required
User Can Disable Alarm Pop-ups	Allows the user to disable or enable alarm windows.	Selected	No
Access Type	Specifies the type of access the user has to the system. Selections are Standard Access and Tenant Access. Metasys for Validated Environment (MVE) sites do not support API Access user accounts and Tenant Access user accounts. MVE sites support Standard Access only.	Standard	Yes

User Properties Tab – Active Directory Service User

The **User Properties** tab for an Active Directory service user defines general information about the user. The Active Directory service domain server sets and controls the fields that appear as read-only (Figure 16). The Metasys system controls all other fields, which are user modifiable and do not affect the account since it is maintained by the Active Directory service domain server.

Figure 16: User Properties Tab – Active Directory Service User

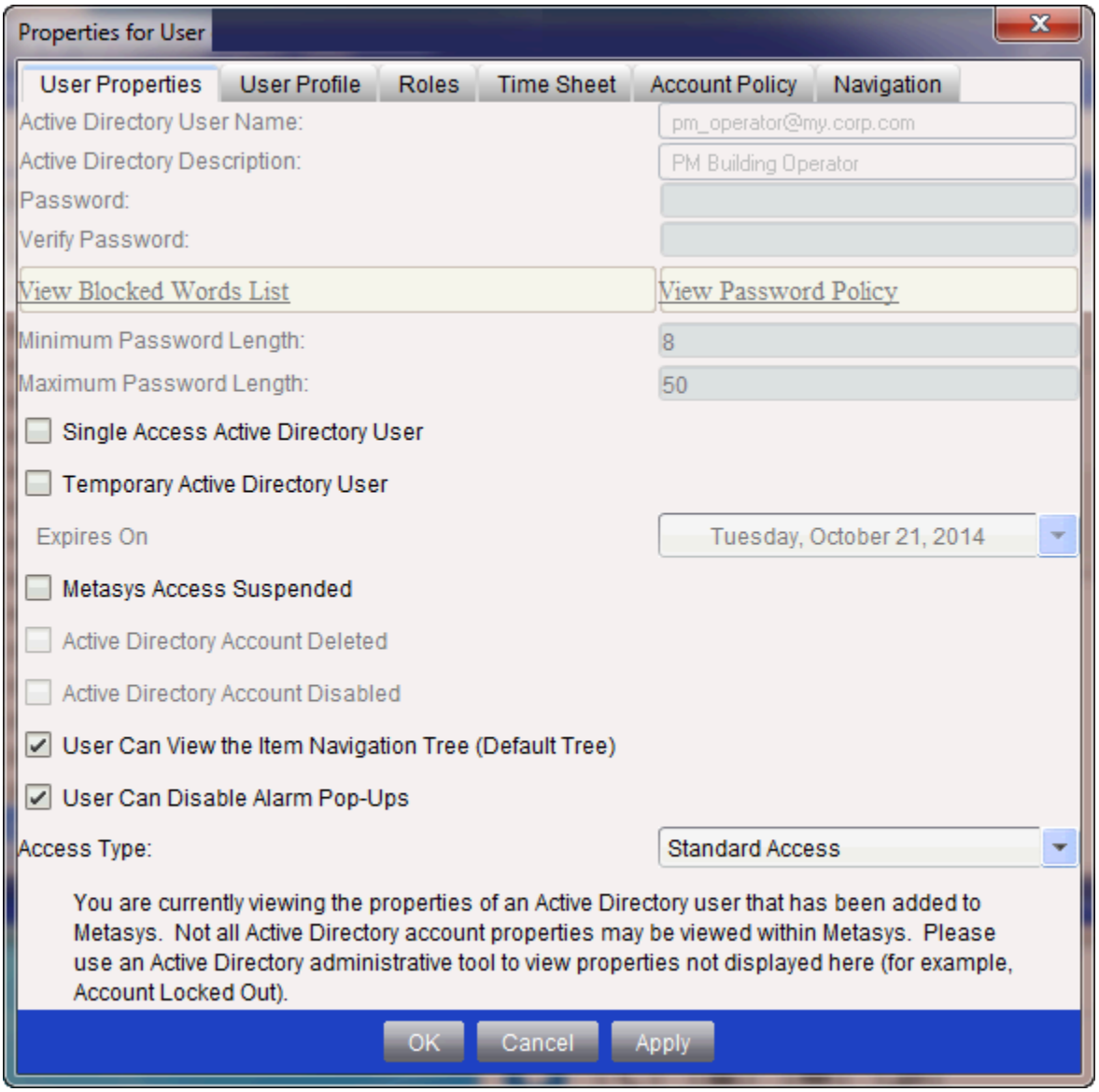


Table 15: User Properties Tab Parameters – Active Directory Service User

Field	Description	Default Value	Required
Active Directory User Name	Displays the login name of the Active Directory service user. This is a read-only field.	—	Yes
Active Directory Description	Displays a description of the Active Directory service user. This is a read-only field.	—	No
Password	Displays a dimmed field because the password is defined and maintained with Active Directory services.	—	—

Table 15: User Properties Tab Parameters – Active Directory Service User

Field	Description	Default Value	Required
Verify Password	Displays a dimmed field because the password is defined and maintained with Active Directory services.	—	—
View Blocked Words List	Displays a dimmed View Blocked Words List link.	—	—
View Password Policy	Displays a dimmed link to the rules for password complexity.	—	—
Minimum Password Length	Displays a dimmed field because the password is defined and maintained with Active Directory services.	—	—
Maximum Password Length	Displays a dimmed field because the password is defined and maintained with Active Directory services.	—	—
Single Access Active Directory User	Allows the Active Directory service user to log in to the account once. After logging in once, the account becomes disabled.	Cleared	No
Temporary Active Directory User	Allows the Active Directory service user to access the system as a temporary user. The user can access the account as long as it has not expired. When expired, the user is logged out of the system.	—	No
Expires On	Allows the administrator to specify the date on which a temporary user's account expires. The account expires at the end of the specified date (midnight), after which the user can no longer access the system.	The default value is the current date.	Yes, if temporary user selected.
Metasys Access Suspended	Allows the administrator to suspend an Active Directory service user account from accessing the Metasys system. This option becomes selected automatically if the Active Directory service user is disabled or deleted from Active Directory services. ⓘ **Note:** If the Active Directory service user's account is enabled again or re-added, you must manually clear the **Metasys Access Suspended** check box.	Cleared	No
Active Directory Account Deleted	Displays a dimmed field because this property is controlled by Active Directory service. If this option is selected, the Active Directory service user account cannot be found and may have been deleted.	Cleared	No
Active Directory Account Disabled	Displays a dimmed field because this property is controlled by Active Directory services. If this option is selected, the Active Directory service user account has been disabled within Active Directory services.	Cleared	No

Table 15: User Properties Tab Parameters – Active Directory Service User

Field	Description	Default Value	Required
User Can View the Item Navigation Tree (Default Tree)	Designates that a user can view the All Items navigation tree.	Selected	No
User Can Disable Alarm Pop-ups	Allows the user to disable or enable alarm windows.	Selected	No
Access Type	Specifies the type of access the user has to the system.	Standard	Yes

Password Rules

The following table lists the password rules enforced by the Metasys system user's language_locale setting.

Table 16: Metasys System Password Rules

Supported Language_Locale	Enforced Password Rules
English (en_us)	• The password must include a minimum of 8 characters and a maximum of 50 characters. • The password cannot include spaces or include a word or phrase that is in the Blocked Words list. • The password and the username cannot share the same three consecutive characters. • The password must meet the four following conditions: - Include at least one number (0–9) - Include at least one special character (-, ., @, #, !, ?, $, %) ⓘ **Note:** Only the special characters listed above can be used; all other special characters are invalid. - Include at least one uppercase character - Include at least one lowercase character
Czech (cs_cz) German (de_de) Spanish (es_es) French (fr_fr) Hungarian (hu_hu) Italian (it_it) Norwegian (nb_no) Dutch (nl_nl) Polish (pl_pl) Portuguese (Brazilian) (pt_br) Russian (ru_ru) Swedish (sv_se) Turkish (tr_tr)	• The password must include a minimum of 8 characters and a maximum of 50 characters. • The password cannot include spaces or include a word or phrase that is in the Blocked Words list. • The password and the username cannot share the same three consecutive characters. • The password must meet three of the following conditions: - Include at least one number (0–9) - Include at least one special character (-, ., @, #, !, ?, $, %) - Include at least one uppercase character - Include at least one lowercase character - Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase
Chinese Simplified (zh_cn) Chinese Traditional (zh_tw) Japanese (ja_jp) Korean (ko_kr)	• The password must include a minimum of 8 characters and a maximum of 50 characters. • The password cannot include spaces or include a word or phrase that is in the Blocked Words list. • The password and the username cannot share the same three consecutive characters. • The password must meet two of the following conditions: - Include at least one number (0–9) - Include at least one special character (-, ., @, #, !, ?, $, %) - Include at least one uppercase character - Include at least one lowercase character - Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase

Password rules are not applicable to Active Directory users. These users are handled by the domain controller and not by the Metasys system.

Password Complexity

All valid passwords are considered complex for Metasys server and all engine platforms on Metasys local system accounts. This feature does not apply to Active Directory service users whom you have added to the Metasys system because password complexity is controlled by Active Directory services.

ⓘ **Note:** Metasys network engines do not support Active Directory.

User Profile Tab

The **User Profile** tab includes more details about the user. The administrator sets the language and the default navigation view that the user sees when logging in to the system (Figure 17). For the User Profile of an Active Directory service user, the first three properties appear dimmed because they are read from and maintained by Active Directory services.

ⓘ **Note:** Other languages are available only when the associated language files are installed on the server or supervisory device. Multiple languages can be installed on the Metasys server and SCT. Only a single language can be installed on the NAE/NCE, including the NAE85.

Figure 17: User Profile Tab - Metasys Local User

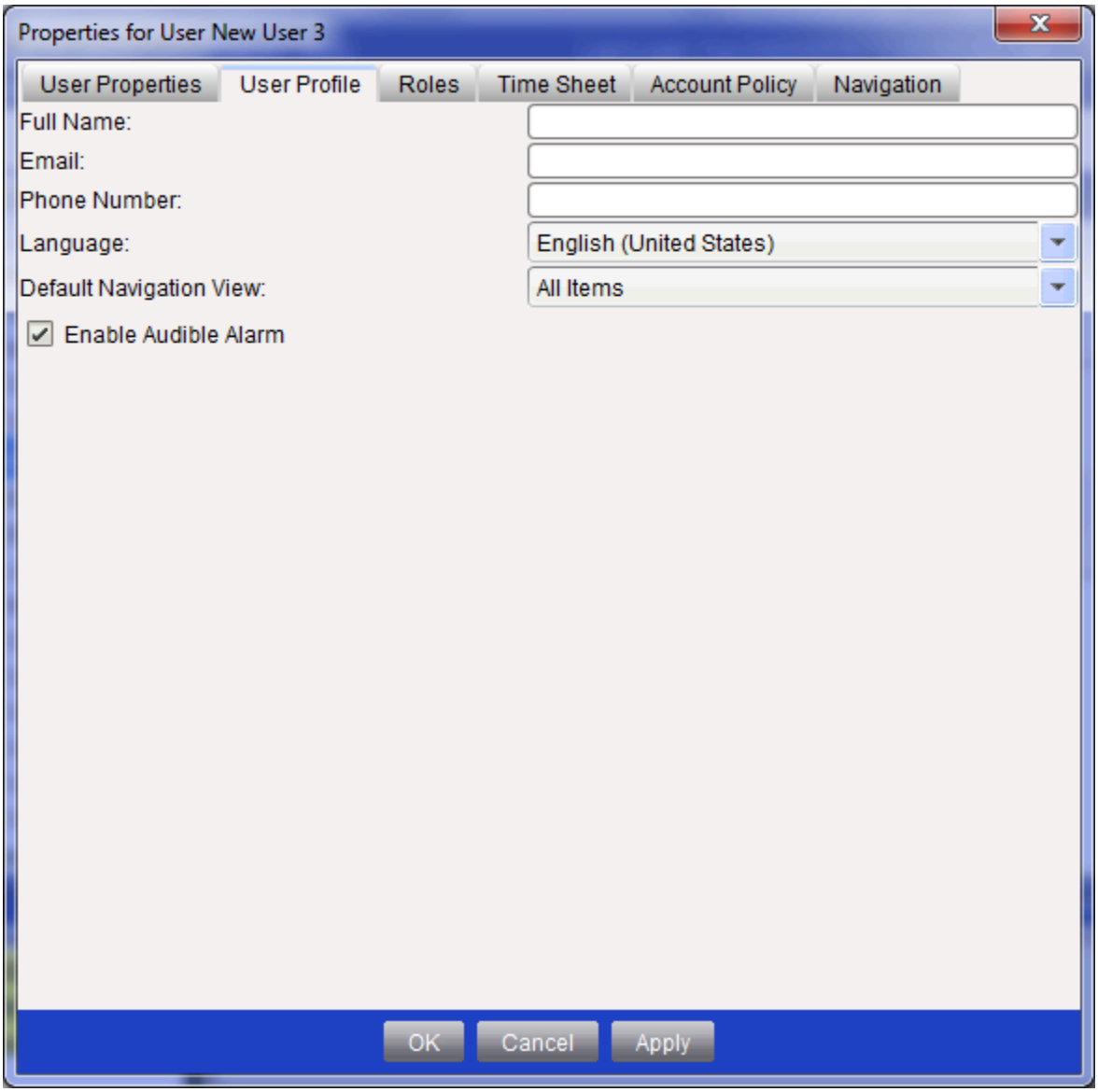


Table 17: User Profile Tab Parameters

Field	Description	Default Value	Required
Full Name [1]	Displays the full name of the user.	—	No
Email[1]	Displays the email address of the user.	—	No
Phone Number[1]	Displays the telephone number of the user.	—	No

Table 17: User Profile Tab Parameters

Field	Description	Default Value	Required
Language	Displays a drop-down list of the site supported languages. ⓘ **Note:** Each time you change the language, you are required to change your password the next time you log in so that the new password you define is verified against the requirements of the new language.	English (United States)	Yes
Default Navigation View	Displays a drop-down list of available navigation views. The selected view is the initial view used upon logging on to the account.	All Items Navigation Tree	Yes
Enable Audible Alarm	Allows user to hear a sound when an alarm occurs.	Selected	No

1 For an Active Directory service user, this field is read-only and the following text is appended to its property name from Active Directory.

Roles Tab

The **Roles** tab allows administrators to provide access privileges to a group of users without editing each individual profile. Administrators assign a user to one or more roles (Figure 18). The **Roles** tab is the same for both the Metasys local system user and the Active Directory service user.

Figure 18: Roles Tab

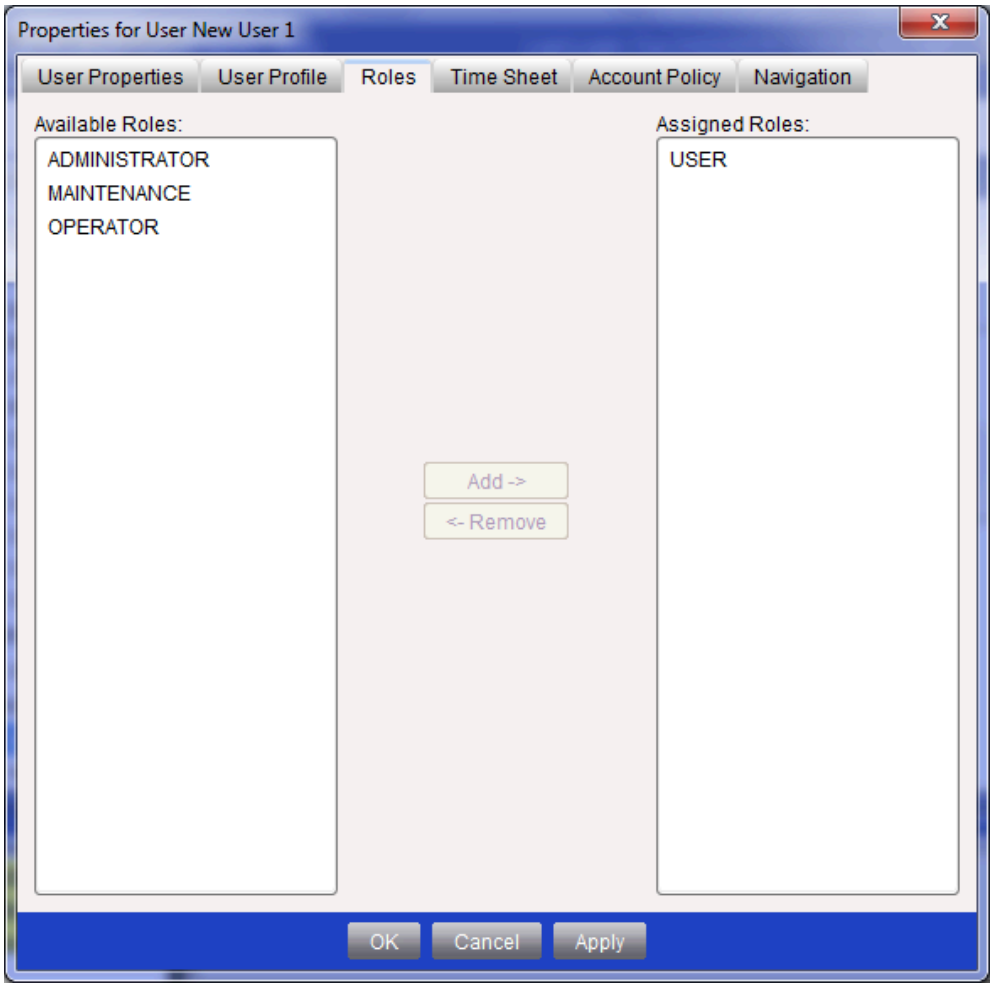


Table 18: Roles Tab Parameters

Field	Description	Default Value	Required
Available Roles	Displays the roles to which the selected user is not assigned.	All available roles, minus the USER role	—
Assigned Roles	Displays the roles to which the selected user is assigned. All users must be assigned to at least one role.	USER	At least one role
Add	Moves the roles from the Available Roles list box to the Assigned Roles list box.	—	—
Remove	Moves the roles from the Assigned Roles list box to the Available Roles list box. Also removes all associated access privileges.	—	—

Time Sheet Tab

The **Time Sheet** tab allows administrators to place time-of-day restrictions on user login. Users may log in to the system during any of the selected hours. Users are denied access when they try to log in during unselected hours (Figure 19). The **Time Sheet** tab is the same for both the Metasys local system user and the Active Directory service user. User access for an Active Directory service user is also controlled by an Active Directory service property called **Logon Hours**. See Authentication Process.

Figure 19: Time Sheet Tab

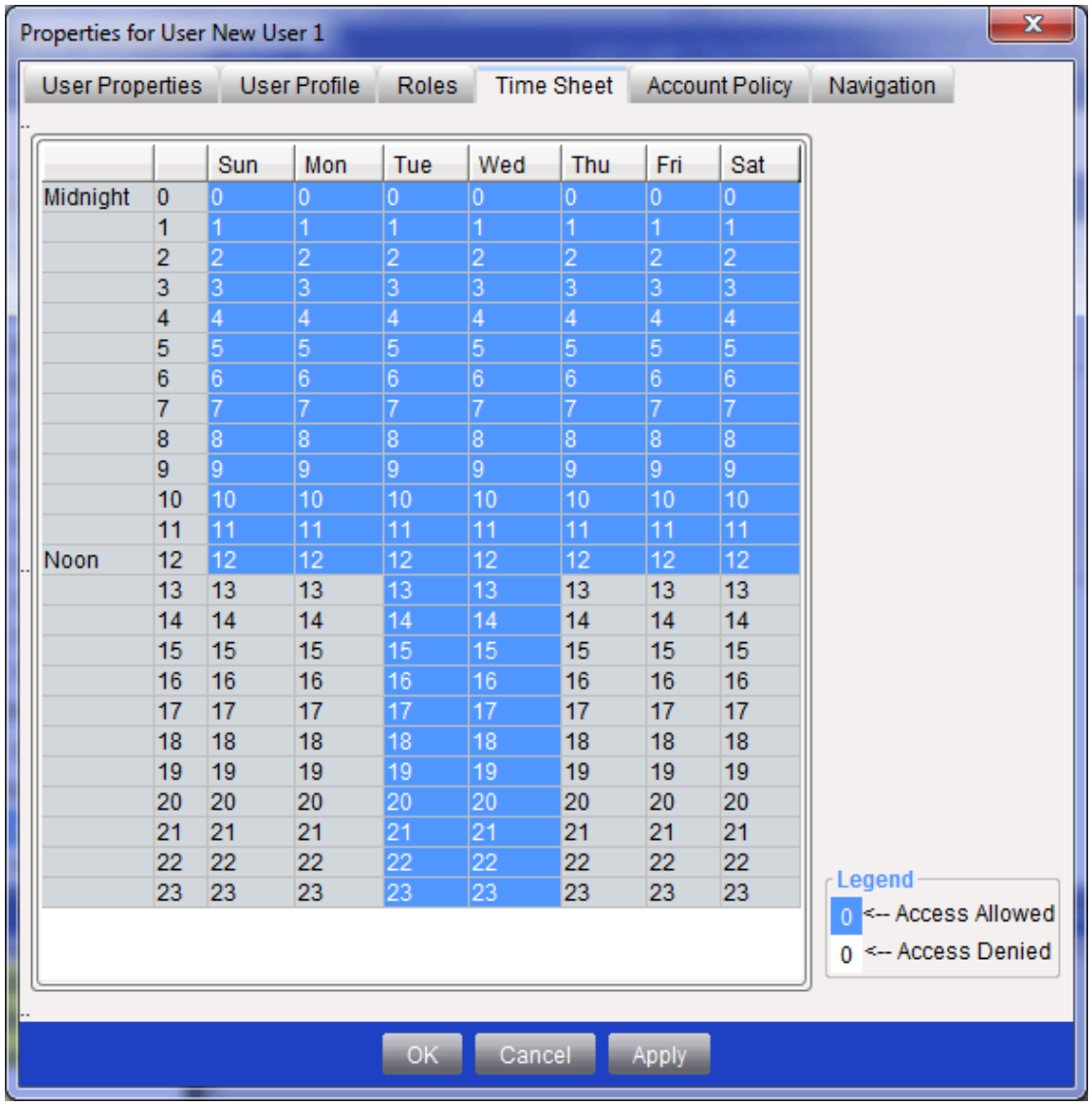


Table 19: Time Sheet Tab Parameter

Field	Description	Default Value	Required
Time of Day	Allows administrators to select times when users can access the system.	All hours selected	Yes

Account Policy Tab

The **Account Policy** tab controls how passwords are used by the user account, the account lockout policy, and the inactive session policy (Figure 20).

By default, the passwords for all user accounts are set to expire in 60 days, including the MetasysSysAgent account. The Maximum Password Age, Password Uniqueness, and Account Lockout properties are not configurable for Active Directory users.

Figure 20: Account Policy Tab – Metasys Local User

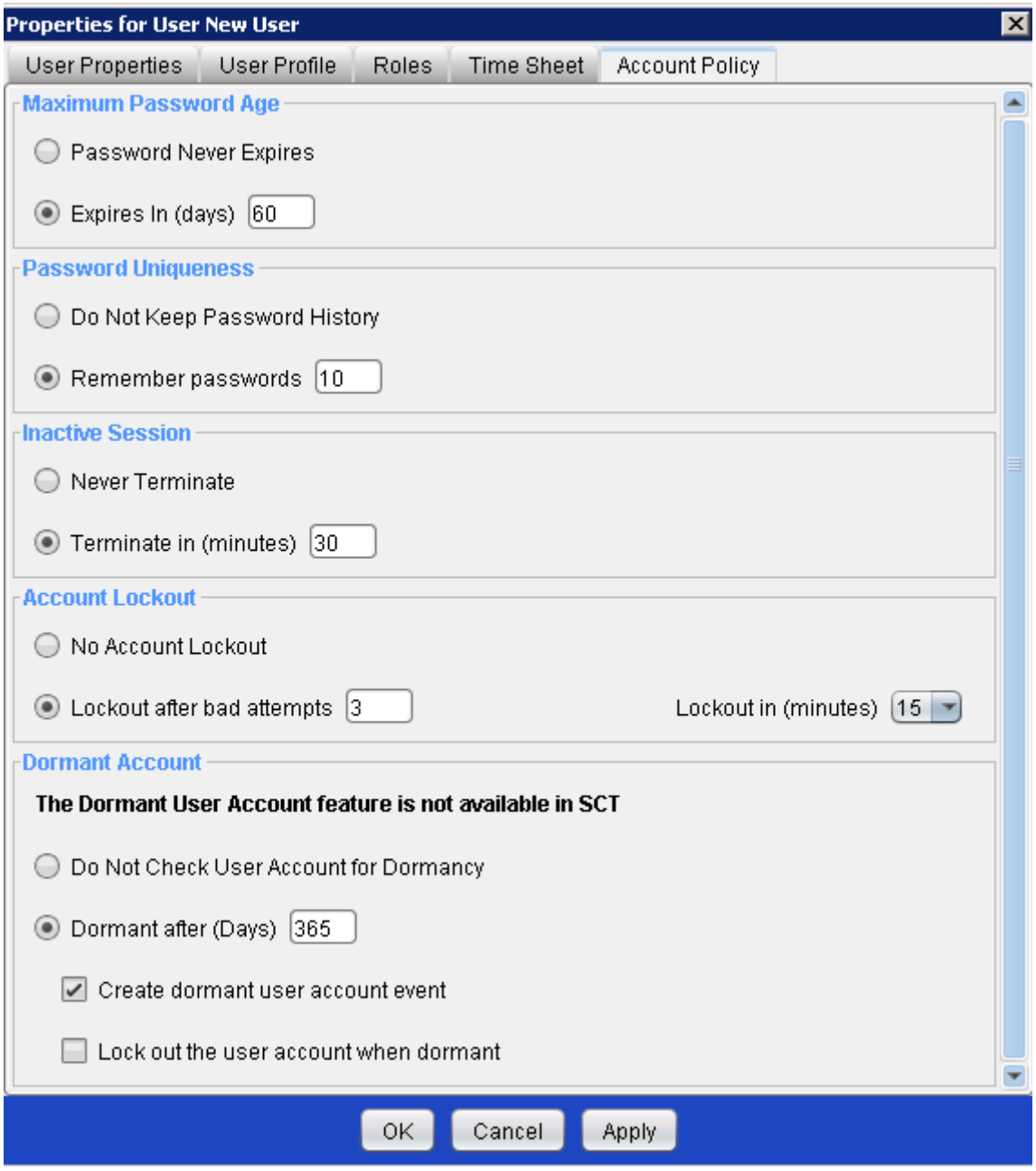


Table 20: Account Policy Tab Parameters – Metasys Local User

Field	Description	Default Value
Password Never Expires	When selected, the password never expires.	Unselected
Expires In (days)	When selected, the user must enter the number of days until the password expires.	Selected (60 days for Users) Selected (90 days for MetasysSysAgent user only)
Do Not Keep Password History	When selected, the system does not remember the password history.	Unselected
Remember passwords	When selected, the system remembers the number of passwords indicated. The system does not allow the user to repeat the same password.	Selected (10 previous passwords)
Never Terminate	When selected, the session never terminates. The session does not terminate as long as the operating system hosting the Metasys system is not suspended or terminated by shutting down, sleeping, or hibernating. Make sure the options for suspending the operating system are disabled. ⓘ **Note:** For more information on how to set up your system so that sessions do not terminate, refer to the *Network and IT Guidance Technical Bulletin (LIT-112011279).*	Unselected
Terminate in (minutes)	When selected, the amount of time the system allows the user to remain inactive before the session terminates and automatically logs the user off from the Metasys system.	Selected (30 minutes)
No Account Lockout	When selected, the account does not lock out.	Unselected
Lockout after bad attempts	When selected, the account locks out after the designated number of sequential failed login attempts. ⓘ **Note:** Both User and MetasysSysAgent user accounts can be unlocked by an administrator. Once the number of failed login attempts have been exceeded, MetasysSysAgent users will also be presented with an opportunity to re-enter	Selected (3 failed login attempts for Users) Selected (10 failed login attempts for MetasysSysAgent users)
Lockout in (minutes)	When selected, the account locks out after the designated number of sequential failed login attempts within the designated time frame. Users will be presented with the opportunity to re-enter their password once every five minutes thereafter. This property also applies to the MetasysSysAgent user. ⓘ **Note:** Both User and MetasysSysAgent user accounts can be unlocked by an administrator.	Selected (15 minutes)

Table 20: Account Policy Tab Parameters – Metasys Local User

Field	Description	Default Value
Do Not Check User Account for Dormancy	When selected, the account never becomes dormant. The user has access to the account regardless of the number of days after the last login.	Unselected
Dormant after (Days)	When selected, the account becomes dormant after the designated number of days after the last login.	Selected (365 days)
Create dormant user account event	When selected, an event message displays alerting the administrator that the dormant user account has not been accessed in the designated number of Dormant After (Days). ⓘ **Note:** For a report of all accounts dormancy settings and status, go to **Query > Dormant User Account Report** in SMP. Dormant user account events are also included in the Audit Viewer and the Event Viewer. On a Metasys server, you can schedule the generation of Dormant User Account Reports. For more information, refer to the product's help system.	Selected
Lock out user account when dormant	When selected, the account locks out after the designated number of Dormant After days.	Unselected

Figure 21: Account Policy Tab – Active Directory User

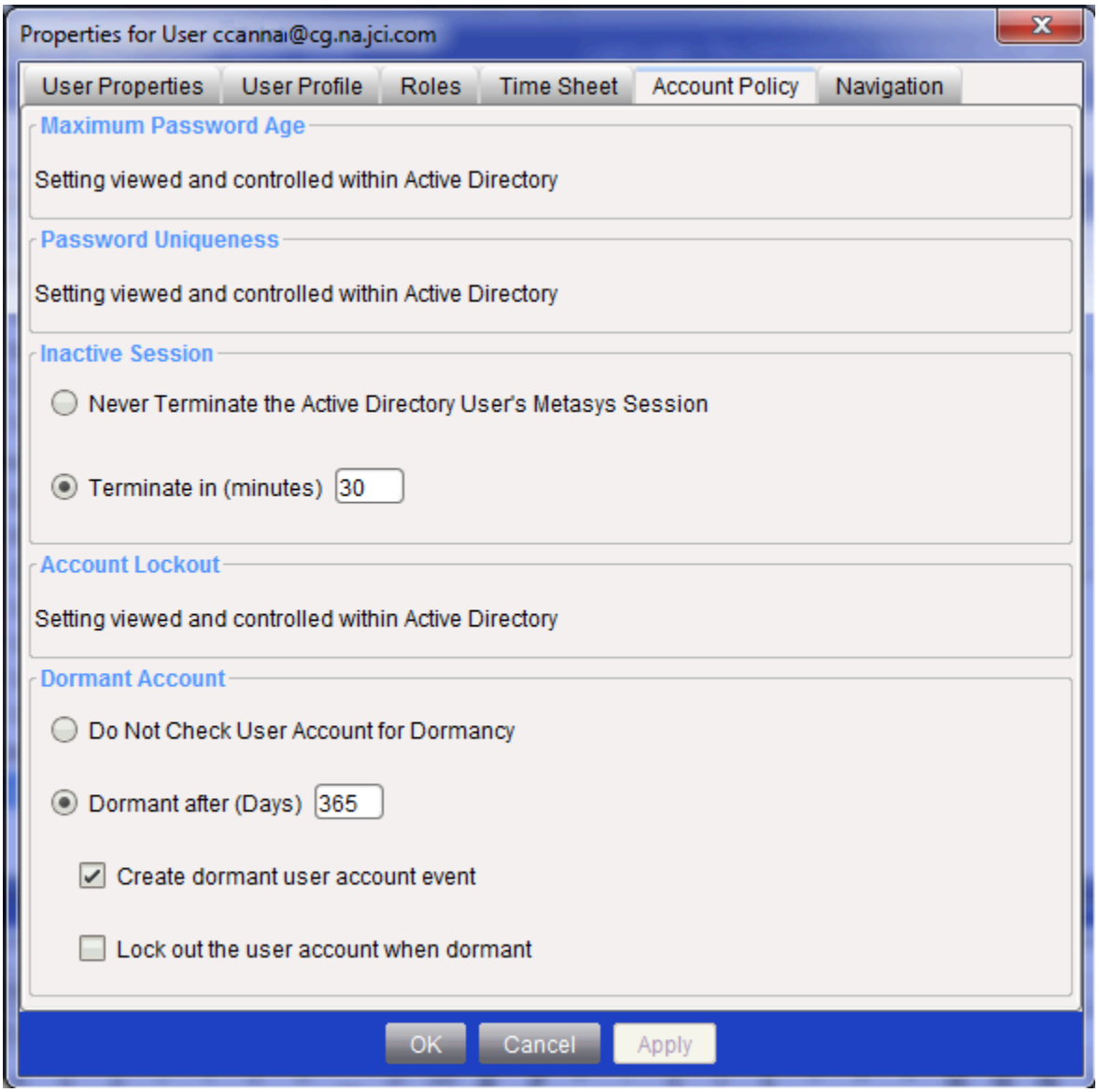


Table 21: Account Policy Tab Parameters – Active Directory User Account

Field	Description	Default Value
Maximum Password Age	View and control this setting within Active Directory service.	—
Password Uniqueness	View and control this setting within Active Directory service.	—

Table 21: Account Policy Tab Parameters – Active Directory User Account

Field	Description	Default Value
Never Terminate the Active Directory User's Metasys Session	When selected, the session never terminates. The session does not terminate as long as the operating system hosting the SMP UI is not suspended or terminated by shutting down, sleeping, or hibernating. Make sure the options for suspending the operating system are disabled. ⓘ **Note:** For more information on how to set up your system so that sessions do not terminate, refer to the *Network and IT Considerations for the IT Guidance Technical Bulletin (LIT-12011279).*	Unselected
Terminate in (minutes)	When selected, the administrator must enter the amount of time the system allows the user to remain inactive before the session terminates and automatically logs the user out of the system.	Selected (30 minutes)
Account Lockout	This setting is viewed and controlled within Active Directory service.	—
Do Not Check User Account for Dormancy	When selected, the account never becomes dormant. The user has access to the account regardless of the number of days after the last login.	Unselected
Dormant after (Days)	When selected, the account becomes dormant after the designated number of days after the last login.	Selected (365 days)
Create dormant user account event	When selected, an event message displays alerting the administrator that the dormant user account has not been accessed in the designated number of Dormant after (Days).	Selected
Lock out user account when dormant	When selected, the account locks out after the designated number of Dormant after (Days).	Unselected

Navigation Tab

The **Navigation** tab allows administrators to specify which user navigation views a user can access (Figure 22). This tab is the same for both the Metasys local system user and the Active Directory service user, but is disabled in the SCT.

Figure 22: Navigation Tab - User

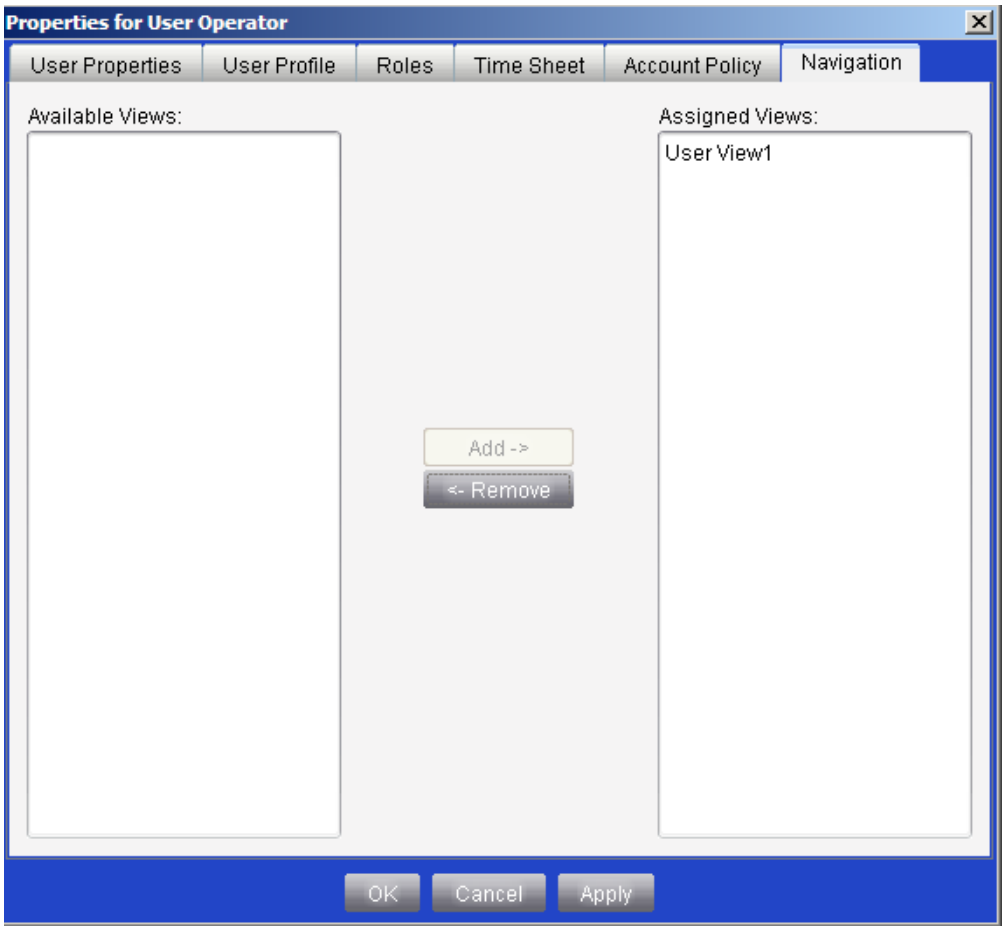


Table 22: Navigation Tab Parameters

Field	Description	Default Value
Available Views	Displays the user navigation views to which the selected user is not assigned.	All available views
Assigned Views	Displays the user navigation views to which the selected user is assigned.	—
Add	Moves the user navigation views from the **Available Views** list box to the **Assigned Views** list box.	—
Remove	Moves the user navigation views from the **Assigned Views** list box to the **Available Views** list box.	—

Role Properties

The **Role Properties** tab defines the roles of users within the system. Assigning users to a role gives the users all access privileges that are assigned to the role in addition to their user-assigned privileges. Roles can be assigned on the **Users** tab of the **Role Properties** dialog box or on the **Role Properties** tab of the **User Properties** dialog box. See Creating a new role.

Role Properties Tab

The **Role Properties** tab defines the general information about the **Role Users** tab (Figure 23).

Figure 23: Role Properties Tab

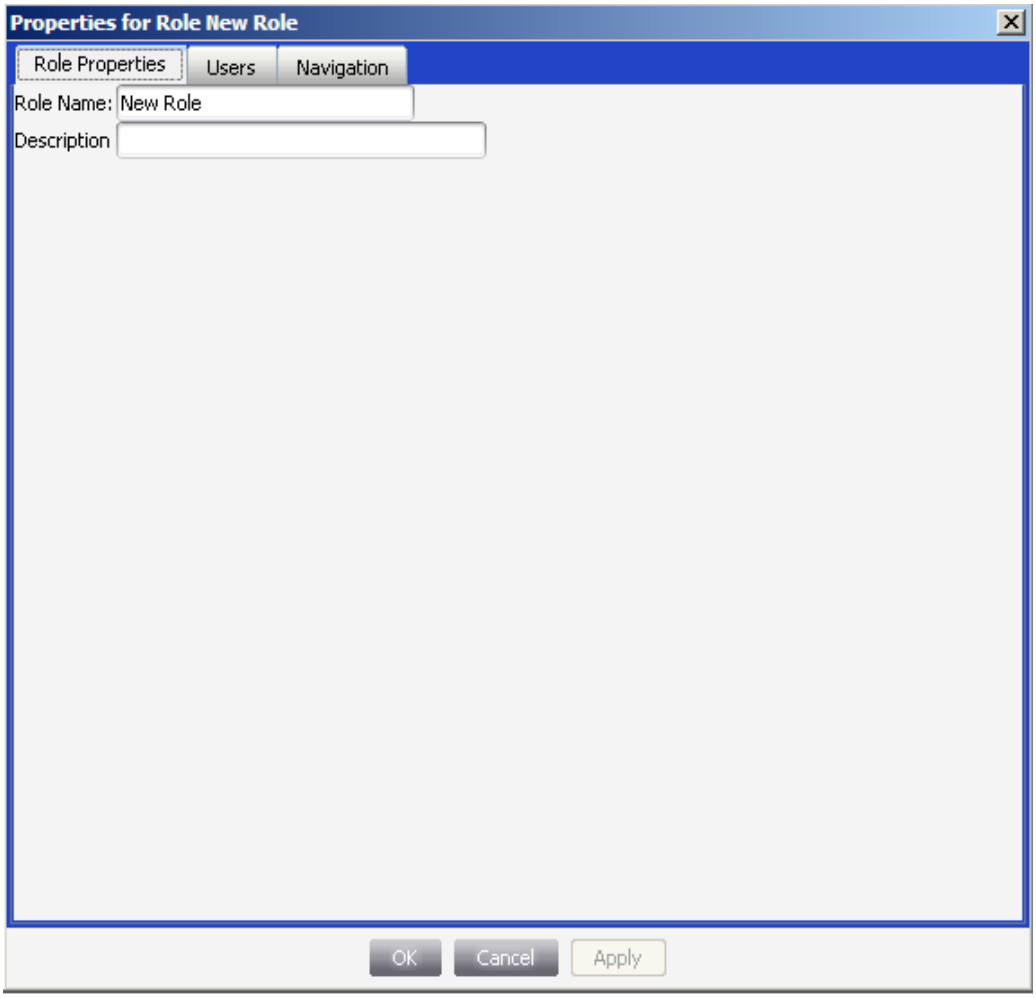


Table 23: Role Properties Tab Parameters

Field	Description	Default Value	Required
Role Name	Displays a unique name for the role.	Role Name	Yes
Description	Displays a description for the role.	---	No

Users Tab

The **Users Tab** allows administrators to assign users specific roles (Figure 24). The following example shows that Active Directory service for use by the Metasys system is enabled with a defined set of Metasys local system users and Active Directory service users.

Figure 24: Users Tab

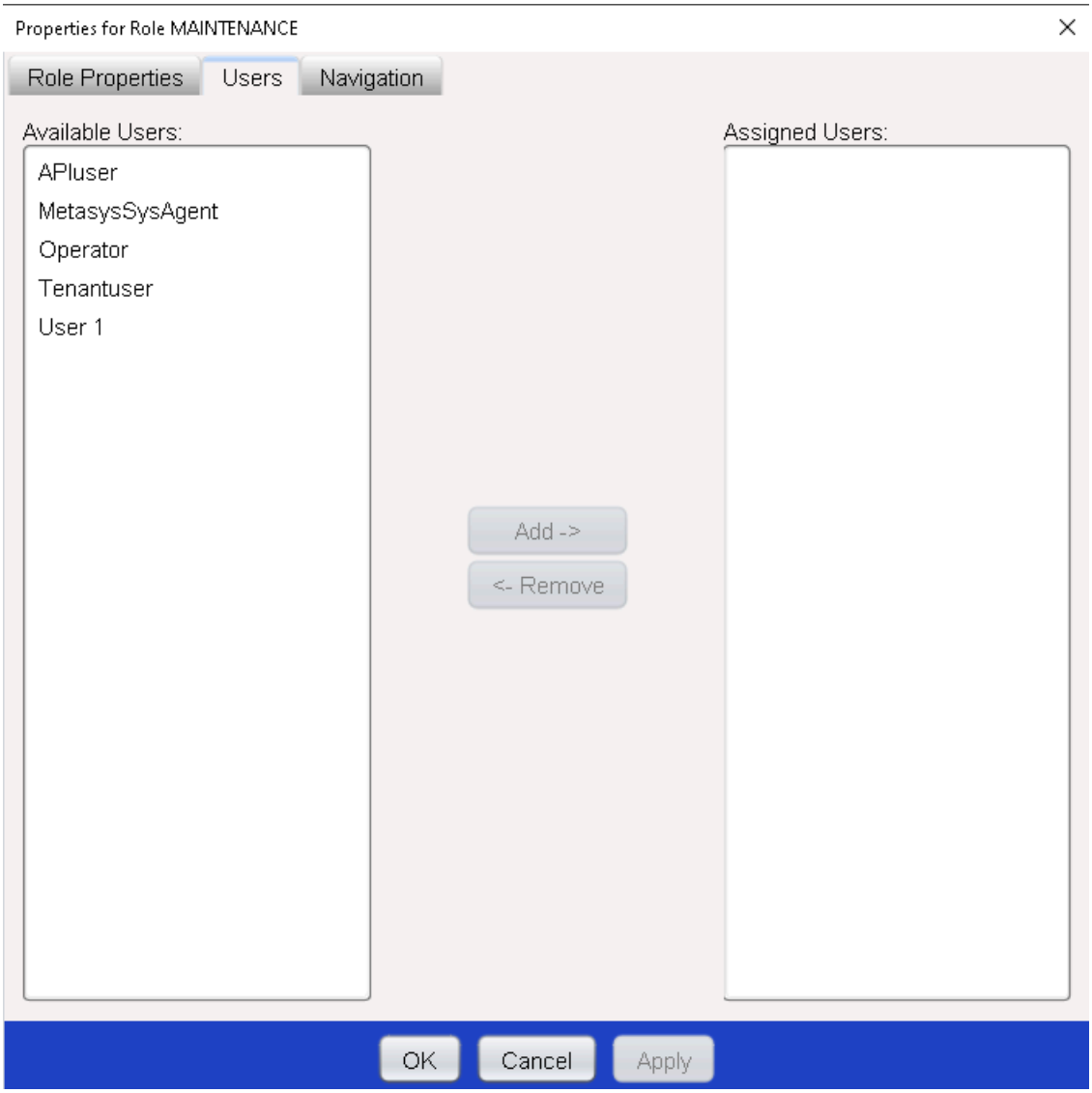


Table 24: Users Tab Parameters

Field	Description	Default Value
Available Users	Users Not Assigned to the Role	All Available Users
Assigned Users	Users Assigned to the Role	—

Table 24: Users Tab Parameters

Field	Description	Default Value
Add	Moves the users from the **Available Users** list box to the **Assigned Users** list box. Once in the **Assigned Users** list box, the role access privileges are granted.	—
Remove	Moves the users from the **Assigned Users** list box to the **Available Users** list box. Once in the **Available Users** list box, the role access privileges are removed. **Note:** You cannot remove the MetasysSysAgent user from the ADMINISTRATOR role.	—

Navigation Tab

The **Navigation** tab allows administrators to specify which user navigation views users in a specific role can access (Figure 25). This tab is disabled in the SCT.

Figure 25: Navigation Tab - Role

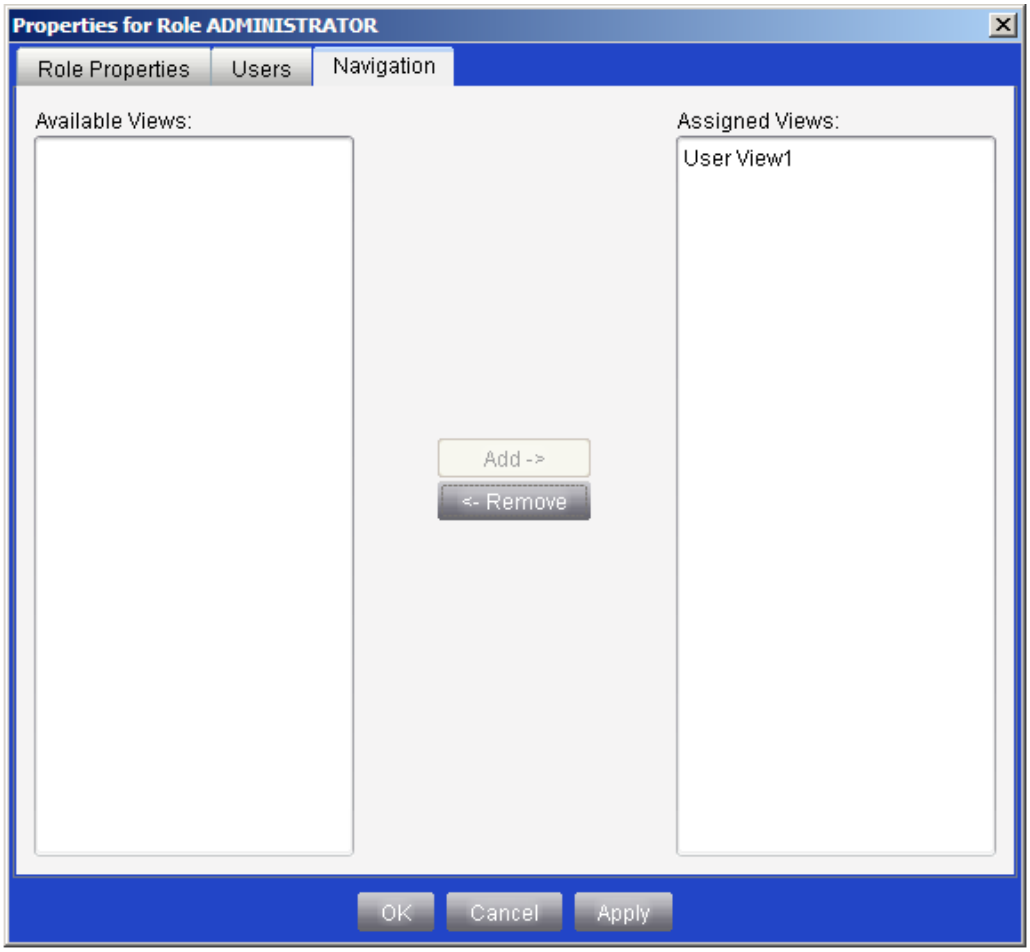


Table 25: Navigation Tab Parameters

Field	Description	Default Value
Available Views	Displays the user navigation views to which the selected role is not assigned.	All available views
Assigned Views	Displays the user navigation views to which the selected role is assigned.	—
Add	Moves the user navigation views from the **Available Views** list box to the **Assigned Views** list box.	—
Remove	Moves the user navigation views from the **Assigned Views** list box to the **Available Views** list box.	—

Security Database Backup and Restore

Use the Manage Archive wizard, available only in the SCT, to back up Metasys Security System databases of Site Directors and other supervisory devices. Beginning at Release 6.0, the archive database upload and download process includes the Security System database. The Security Database Backup/Restore wizard is no longer available in SCT. Use the Security Copy function in SCT to restore Metasys Security System databases of Site Directors and other supervisory devices. For the Metasys server, back up and restore Metasys system local users, Active Directory service users, and the Active Directory service configuration for the Metasys system, but only back up and restore Metasys local users for network engines. (For details, see Active Directory Service - Security Database Backup and Restore.)

If you need to change Site Directors, use the Manage Archive wizard to upload the archive database before changing Site Directors to ensure you have the most updated Security System database. Then, use the Security Copy wizard to copy the Security System database from one Site Director to another.

ⓘ **Note:** If the factory-default password of a supervisory engine at Release 6.5 has never been changed and the archive database is uploaded with SCT, then use Security Copy to copy its Security Database to an engine at Release 5.2, the MetasysSysAgent user account becomes locked out for the Release 5.2 engine. When you try to log in to the Release 5.2 engine with the MetasysSysAgent user, the message `Invalid name or password entered` appears. To correct this issue, change the default password of the Release 6.5 engine, then perform a Security Copy from the Release 6.5 engine to the Release 5.2 engine.

When you change the Security System database for small-capacity network engines (NAE35, NAE45, NCE25, NIE29, NIE39, NIE49, SNC and SNE), you must issue the **Reset Device** command to ensure that the Security Database is archived to permanent memory. This step **is not** required for NAE55s. If you do not perform this step for a network engine that has a poor or dead battery, and that engine loses power, the latest changes to the Security System database are lost.

You must rename a Metasys local username that includes the reserved characters @ or \ after a Security Database restore if:

- the user was added to the Metasys system before Release 4.0; and
- the username is intended for login after the Security Database is restored to a Release 4.0 or later system.

This user cannot login to the Metasys system until the @ and \ characters are removed from the username. Also, any change to a user's property that currently includes either of these reserved characters forces the administrator to rename the user.

Active Directory Service - Security Database Backup and Restore

The Security Database stores Active Directory service users that are configured in the Metasys system along with Metasys local users and roles.

Security Database Backup and Restore for Metasys server

Backing up and restoring the Security Database with SCT backs up and restores the Active Directory service users, Metasys local users, and roles for a Metasys server.

The following Metasys Active Directory service configuration information is stored in the Security Database and backed up or restored along with other Security data:

- Active Directory Service Authentication Enabled or Disabled
- Windows Workstation SSO Enabled or Disabled
- Login Page Default Domain Selection
- Active Directory Service Service Accounts

Settings from the backup replace existing settings on the targeted device during a restore operation.

Security Database Backup and Restore for Network Engines

For NAE and SNE series network engines, a Security Database that is backed up from a *Metasys* server may include a mixture of Metasys local users and roles with Active Directory service users. The Download To Device function only restores local users and roles to the device because network engines do not support Active Directory service authentication and authorization, even if the NxE is a Site Director. The Download To Device function informs the user if Active Directory service users exist within the Security Database but are not restored because the target device does not support Active Directory service authentication and authorization. The message that appears in the Completed Actions screen of ActionQ is: `OK - Restore to non-Active Directory Device (616).`

Security Copy

The Security Copy function in the SCT allows you copy the user store to a device that is at the same release or lower than the source system. For example, if you make changes to your Security Database on the Site Director, you can copy the Security Database with your changes to other devices in your site. Security Copy is located on the Tools menu of SCT. For more details, refer to the *Metasys SCT Help (LIT-12011964)*

Note: If the factory-default password of a supervisory engine at Release 6.5 has never been changed, and you upload its archive database with SCT, then use Security Copy to copy its Security Database to an engine at Release 5.2, the MetasysSysAgent user account becomes locked out for the Release 5.2 engine. When you try to log in to the Release 5.2 engine with the MetasysSysAgent user, the message `Invalid name or password entered` appears. To correct this issue, change the default password of the Release 6.5 engine, then perform a Security Copy from the Release 6.5 engine to the Release 5.2 engine.

Detailed Procedures

Changes made to user accounts in the Security Administrator system no longer affect all Metasys system components that reside on the same computer. For example, on a computer that has both

an ADS and SCT installed, changes you made in the Security Administrator system do NOT affect both the ADS and the SCT.

For more information on Security Databases at Release 7.0, refer to the *Metasys SCT Help (LIT-12011964)*.

ⓘ **Note:** Some of the procedures in the following sections apply only to networks that have the Microsoft Active Directory service technology implemented at the site. If you are enabling the Active Directory service for use by the Metasys system, see Configuring Active Directory Service for Metasys System Use.

Creating a Metasys local user account

1. Log in to the Metasys server or SCT with a Metasys Administrator account.
2. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears (Figure 5).
3. On the **Insert** menu, click **New User**. The **User Properties** tab of the **User Properties** dialog box appears. See Figure 14.
4. Fill in the information and click **OK**. The New User appears in the **Roles and Users** tab.
5. Set the other properties and define System Access Permissions for each Metasys local User. For details, see the Detailed Procedures sections that follow, then see System Access Privileges.
6. Close the Security Administration window.

Creating a local user account in Metasys UI

From release 10.1, you can also create users in Metasys UI. To create a new user in Metasys UI, complete the following steps:

1. Open **User Management**.
2. In the default tab (**Users**), tap or click **+ USER**. The **Create New User** window opens.

   ⓘ **Note:** On a smartphone, tap **+** to create a new user.
3. Select the user type from the **Type** list. Selectable user types include Metasys, and Active Directory users.
4. Enter a user name in the mandatory **Username** field.
5. Enter a password in the mandatory **Password** field. Review the password rules listed on the right of the **Create New User** window.

   ⓘ **Note:** On a smartphone, tap the information icon next to **Password** to review the password rules.
6. Confirm the password in the **Confirm Password** field.
7. Select a user role from the **Role** list.

   ⓘ **Note:** You must assign at least one role to a user.
8. Tap or click **CREATE AND EDIT** to create the user and edit the user details. To create the user with the details you entered, tap or click **CREATE AND CLOSE**.

Creating a new role

1. On the **Insert** menu, click **New Role**. The **Role Properties** tab of the **New Role** dialog box appears (Figure 23).

2. On the **Role Properties** tab, fill in the information. See Table 23.
3. On the **Users** tab, assign users to the new role using the **Add** button. See Figure 24.
4. On the **Navigation** tab, assign access to user navigation views using the **Add** button. See Figure 25.
5. Click **OK**.
   The New Role appears in the **Roles and Users** tab.

Creating a new role in Metasys UI

Starting at Release 10.1, users can also be created in Metasys UI. To create a new role in Metasys UI, complete the following steps:

You can create a new role on desktop platforms only.

1. Open **User Management**.
2. In the **Roles** tab, tap or click **+ ROLE**. The **Create New Role** window opens.
3. Enter a role name in the mandatory **Role Name** field.

   ⓘ **Note:** The following two special characters are not supported in a role name: at sign (@) and backslash (\).
4. Enter a description in the **Description** field.
5. Search for and select a user you want to assign to this new role from the **Available** section.
6. After a user is selected, tap or click the right-arrow to add the user to the **Assigned Users** section.

   ⓘ **Note:** You can select multiple users at once by using the keyboard shortcuts Ctrl or Shift. You can also click and drag the mouse over the users to select multiple users.
7. Tap or click **CREATE AND EDIT** to create the role and further edit the role details. Or, tap or click **CREATE AND CLOSE** to create the role with the details you entered.

ⓘ **Note:** For further information, refer to the User Management section in *Metasys® UI Help (LIT-12011953)*.

Configuring a User Profile

1. Select the user to configure.
2. On the **Edit** menu, click **Properties**. The **User Properties** dialog box appears (Figure 14).
3. Select the **User Profile** tab (Figure 17).
4. Modify the user information using Table 17.
5. Click **OK**.

Placing Time-of-Day Restrictions

1. Select the user to configure.
2. On the **Edit** menu, click **Properties**. The **User Properties** dialog box appears. See Figure 14.
3. Select the **Time Sheet** tab. See Figure 19.
4. Select the times when users can access the system by clicking time slots to toggle between **Access Allowed** (blue highlight with white text) and **Access Denied** (no highlight with black text). See Table 19.
5. Click **OK**.

Setting Password Account Policies

1. Select the user to configure.
2. On the **Edit** menu, click **Properties**. The **User Properties** dialog box appears. See Figure 14.
3. Select the **Account Policy** tab.
4. Select options using Table 20 (Metasys local users) or Table 21 (Active Directory service users).
5. Click **OK**.

Assigning All Items Navigation View Permissions

About this task:
Users can navigate with any user navigation view for which they have been assigned access rights; however, permission to view the All Items navigation view is assigned separately.

1. Select the user.
2. On the **Edit** menu, click **Properties**. The **User Properties** tab of the **User Properties** dialog box appears. See Figure 14.
3. Click to select the **User Can View the Item Navigation Tree (Default Tree)** check box.
4. Click **OK**.

Assigning User Navigation View Access

Perform this procedure in the SMP UI. The Navigation and Navigation Views tabs are disabled in the SCT.

Assigning Access by Using the User Properties or Role Properties Dialog Boxes

1. Select the user or role.
2. On the **Edit** menu, click **Properties**. The **User Properties** tab of the **User Properties** dialog box appears (see Figure 14) or the **Role Properties** tab of the **Role Properties** dialog box appears (Figure 23).
3. Select the **Navigation** tab (Figure 22 for user or Figure 25 for role).
4. In the **Available Views** list, click one or more user views to assign.
5. Click **Add**.

   ⓘ **Note:** To remove user Navigation View Permissions from the user or role, click one or more user views in the Assigned Views list and then click **Remove**.

6. Click **OK**.

Assigning Access by Using the Navigation Views Tab

1. Select the **Navigation Views** tab (Figure 13). The available views appear in the **Navigation Views** folder.
2. Click the view to assign access permissions. The **Roles and Users Access Permissions** tables appear in the right pane.
3. Assign access to Roles in the **Roles Access Permissions** table:
   a. Click the **Allow Access** column header to assign access to all roles. If all roles are already assigned permission, clicking the column header removes all selections. If one or more roles are not currently assigned permission to the view, clicking the column header selects and assigns access to all roles.
   b. Click individual rows or cells to assign access to particular roles. Click to select or

remove selections as desired.

4. Assign access to users in the **Users Access Permissions** table:
   a. Click the **Allow Access** column header to assign access to all users. If you have already assigned all users permission, clicking the column header removes all selections. If you have not currently assigned one or more users permission to the view, clicking the column header selects and assigns access to all users.
   b. Click individual rows or cells to assign access to particular users. Click to select or remove selections as desired.
5. In the **File** menu, click **Save**. The circle icon next to the view name in the left pane updates to reflect the changes (filled = at least one role or user assigned, empty = no roles or users assigned).
6. Repeat Steps 2 through 5 to assign access to other available user navigation views.

Copying a User or Role

About this task:

ⓘ **Note:** Active Directory service users cannot be copied. You must add them individually.

1. Select the user or role you wish to copy.
2. On the **Insert** menu, click **Copy of User**. The **Properties for User Copy Of <user or role>** dialog box appears.
3. Make the necessary modifications.
4. Click **OK**.

Deleting a User or Role

About this task:

ⓘ **Note:** Do not use this procedure for deleting an Active Directory service user. See Removing User Access to Active Directory Service from the Metasys System.

1. Select a user or role to delete.
2. On the **Edit** menu, click **Delete**. The **Delete <user or role>** dialog box appears confirming the user or role should be deleted.
3. Click **Yes**.
   Notes:
   - If you cannot delete the selected user or role (for example, a predefined user), the **Delete** menu choice appears dimmed.
   - The following user message appears if you are trying to delete a role that is assigned to an Active Directory service user: `Failed to delete role – some Active Directory users still exist for the role (Active Directory authentication must be enabled within` *`Metasys`* `to see these users in the Administrator Tool). Reenable Active Directory service authentication, remove the role assignment for each Active Directory service user who appears in the Role, then delete the Role. You can disable Active Directory service authentication again.` Re-enable Active Directory service authentication, remove the role assignment for each Active Directory service user who appears in the Role, then delete the Role. You can disable Active Directory service authentication again.

Renaming a User or Role

About this task:

ⓘ **Note:** The Metasys Security Administration tool cannot rename the Active Directory service users because their names are controlled by Active Directory services. If you rename an Active Directory service user, a Metasys System Administrator must synchronize the user before the user can log in to the Metasys system. See Synchronizing an Active Directory Service – User Account.

1. Select the user or role to rename.
2. On the **Edit** menu, click **Properties**. The **User/Role Properties** tab of the **User/Role Properties** dialog box appears.
3. Type a new name in the **User Name** field.
4. Click **OK**.

Unlocking a User Account

About this task:

ⓘ **Note:** Active Directory service user accounts cannot be unlocked by using the Metasys Security Administrator tool. An Active Directory Service Administrator must unlock the account with an Active Directory service tool. MetasysSysAgent user accounts can also be unlocked, but only by another Admin user.

1. Select the user whose account needs to be unlocked.
2. On the **Edit** menu, click **Properties**. The **User Properties** tab of the **User Properties** dialog box appears (see Figure 14).
3. Clear the **Account Locked Out** check box.

   ⓘ **Note:** You cannot select this check box to lock a user account.
4. Click **OK**.
   The user can now log in to the system.

Assigning Category-Based Permissions to a User or Role

1. Select the user or role. The **Access Permission** table for the user or role appears in the right pane.
2. Assign permissions to the user or role in the **Access Permissions** table. Use Table 2 as a reference.
   a. Click column headers to assign a privilege to all authorization categories. Click the column header again to remove the selection.
   b. Click rows to assign all privileges to the authorization category. Click the row again to remove the selection.
   c. Click a cell to assign a single privilege to a single authorization category. Click the cell again to remove the selection.
3. On the **File** menu, click **Save**.

   ⓘ **Note:** No changes are saved and no error messages appear if you update permissions for a user in an Metasys server system when the database is offline. For example, an offline database may be the result of Microsoft SQL Server database not running, or an ADX split configuration network connectivity problem between the web/application server and the database server. To verify your changes, select another user and then reselect the user to which you made changes.

Assigning Users to Roles

Assigning Users to Roles by Using the User Properties Dialog Box

1. Select the user to configure.
2. On the **Edit** menu, click **Properties**. The **User Properties** dialog box appears.

   ⓘ **Note:** To remove a role, select one or more roles from the **Assigned Roles** list and click **Remove**.
3. Select the **Roles** tab.
4. In the **Available Roles** list, click one or more roles.
5. Click **Add**. The selected roles appear in the **Assigned Roles** list.

   ⓘ **Note:** To remove a role, select one or more roles from the **Assigned Roles** list and click **Remove**.
6. Click **OK**. The system displays a two-headed icon for each permission assigned to the role you selected.

Assigning Users to Roles by Using the Role Properties Dialog Box

1. Select the role to configure.
2. On the **Edit** menu, click **Properties**. The **Role Properties** dialog box appears.

   ⓘ **Note:** You can also double-click a role to display the **Role Properties** dialog box.
3. Select the **Users** tab.
4. In the **Available Users** list, click one or more users.
5. Click **Add**. The selected users appear in the **Assigned Users** list.

   ⓘ **Note:** To remove a user, select one or more users in the **Assigned Users** list and click **Remove**.
6. Click **OK**. The system displays a two-headed icon for each permission assigned to the role you selected.

Assigning System Access Permissions

1. Select the user or role.
2. On the **Edit** menu, click **System Access Permissions**. The **System Privileges** dialog box appears.
3. Select an available privilege using Table 4.
4. Click **Add**.
5. Click **OK**.

   The System Access Permissions are assigned to the selected user or role.

   When you are viewing user system privileges, select the **Summarized** tab to view all system privileges assigned to the user either directly or by a role. You cannot add or remove privileges from this tab, and it does not appear when viewing role system privileges.

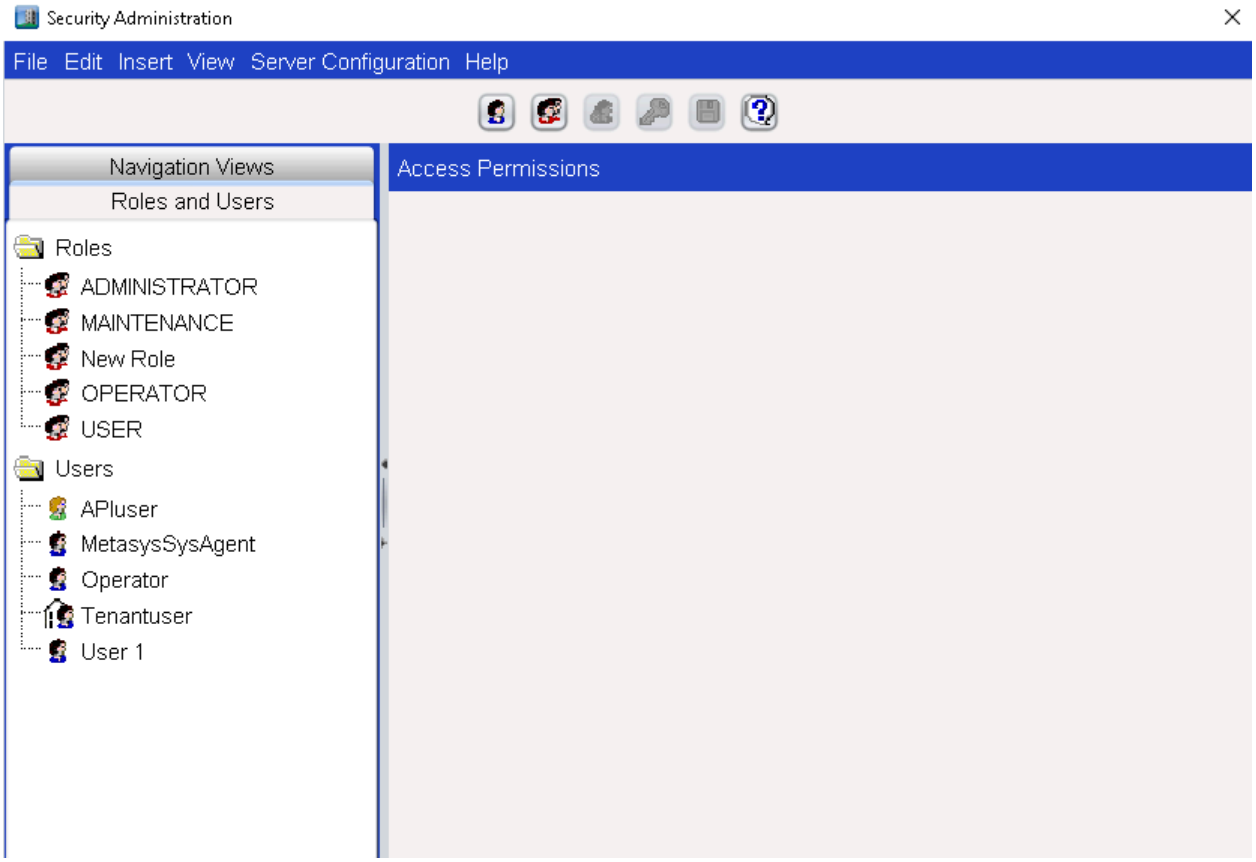
Configuring Active Directory Service for Metasys System Use

To implement the Active Directory service for use by the Metasys system, follow the steps in this section. For general user configuration information, see Table 9.

Enabling Active Directory Service Integration for Metasys server or SCT Software

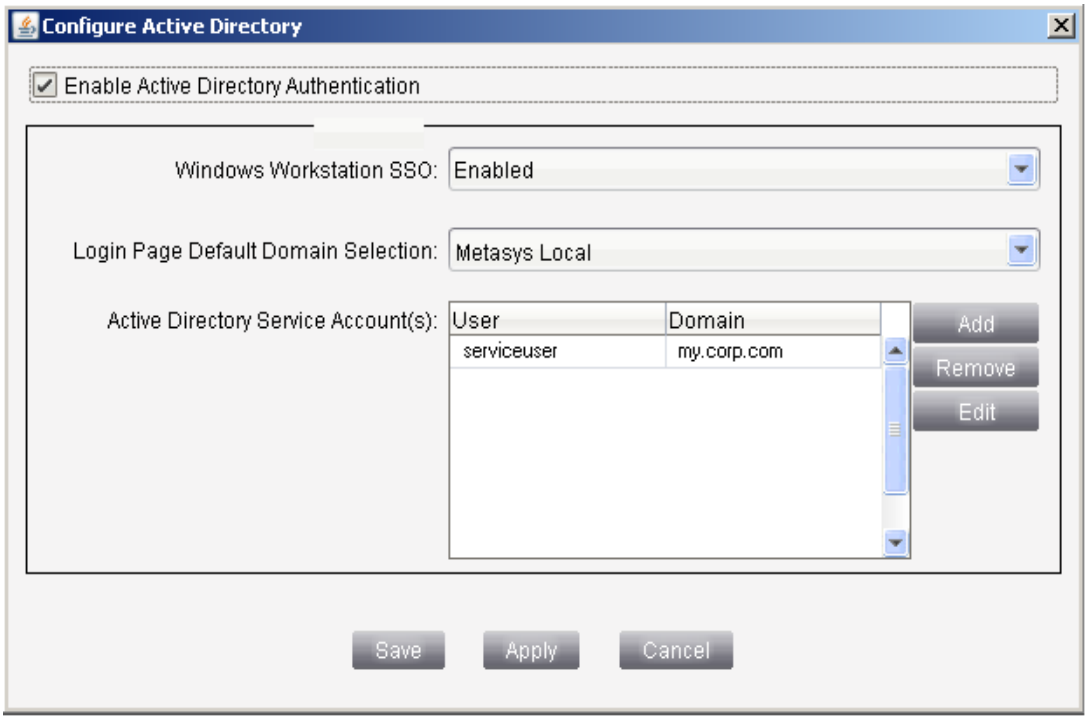
1. Log in to the Metasys server or SCT software with a Metasys Administrator account. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears (Figure 26).

Figure 26: Security Administrator Screen



2. In the Security Administration window, click **Server Configuration** > **Active Directory**. The **Configure Active Directory** dialog box appears.

Figure 27: Configure Active Directory Service

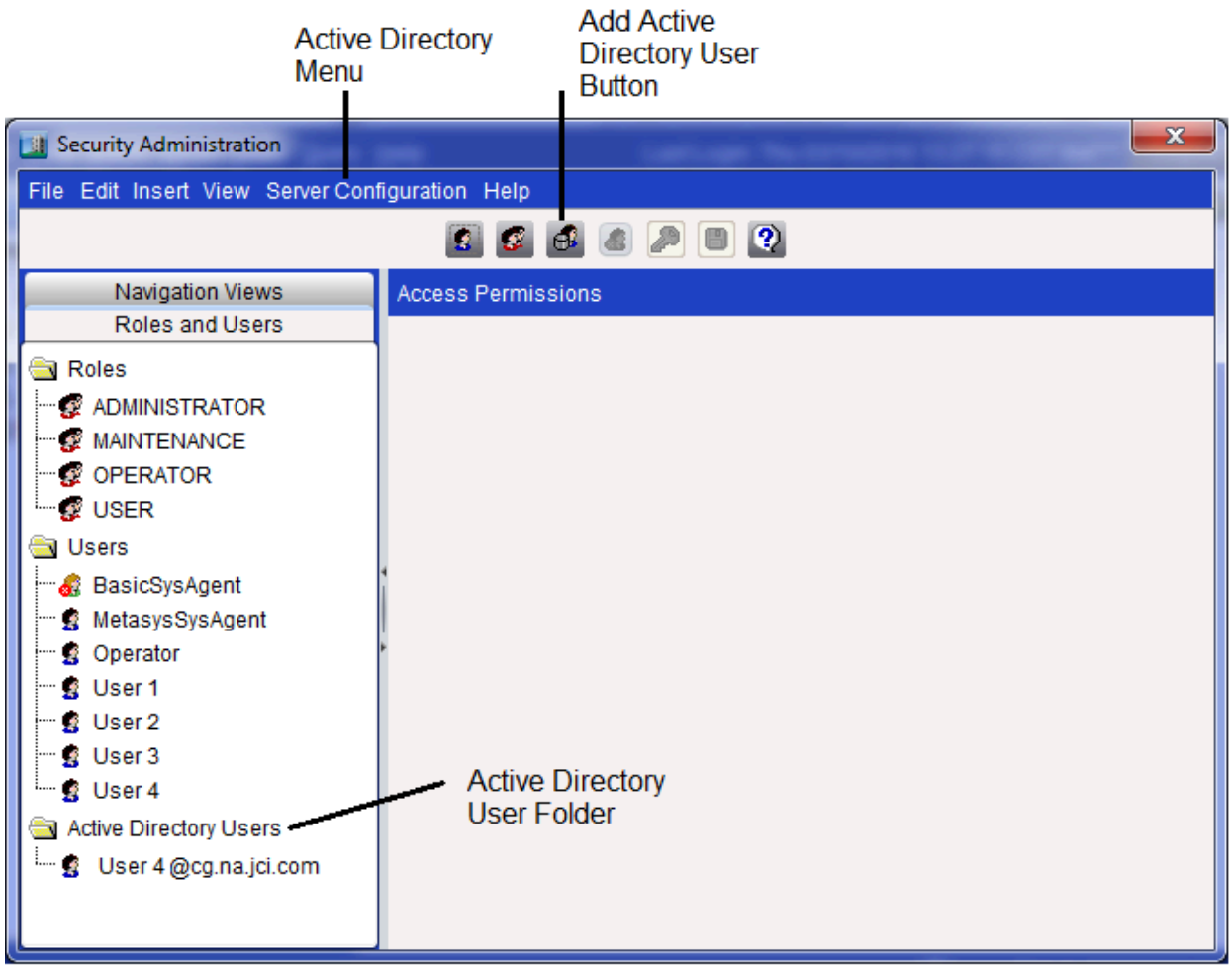


3. Click to select the **Enable Active Directory Authentication** check box. The next three selections become editable.
4. Set **Windows Workstation SSO** to **Enabled** if you want to use the SSO login free access feature. Otherwise, select **Disabled**.
5. Ignore the **Login Page Default Domain Selection** option. You must add the Active Directory service users before you select the default domain (covered in the section Providing Access to Metasys System for Active Directory Service Users).
6. Using the **Active Directory Service Account(s)** option, add one or more service account users who have authentication rights to the Active Directory service users you want to add. A username and password for each service account is required. Also, before you can save or apply these changes, you must specify at least one service account and the service account must currently exist on the Active Directory service domain. (For details on service accounts, see Service Account.)
7. Click **Save** or **Apply** to save your changes. Clicking **Save** returns you to the Administration screen, which now has **Active Directory Users** as a new folder in **Roles and Users**.

Providing Access to Metasys System for Active Directory Service Users

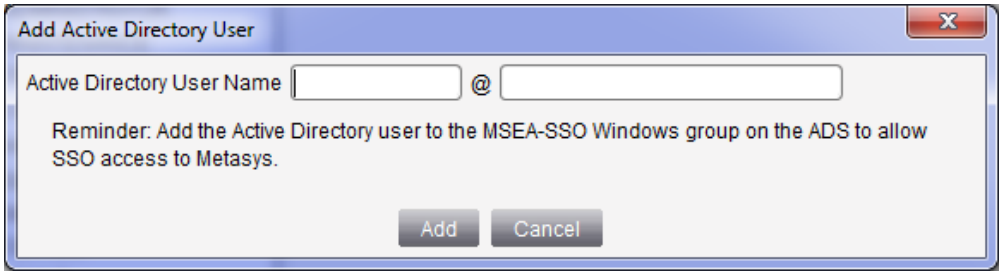
1. Log in to the Metasys server or SCT computer with a Microsoft Windows Administrator account.
2. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears.

Figure 28: Security Administrator Screen



3. On the **Insert** menu, click **Insert Active Directory User**. (You can also click the **Add Active Directory User** icon or right-click the **Active Directory** folder and then click **Insert**.) The **Add Active Directory User** dialog box appears.

Figure 29: Add Active Directory User Dialog Box



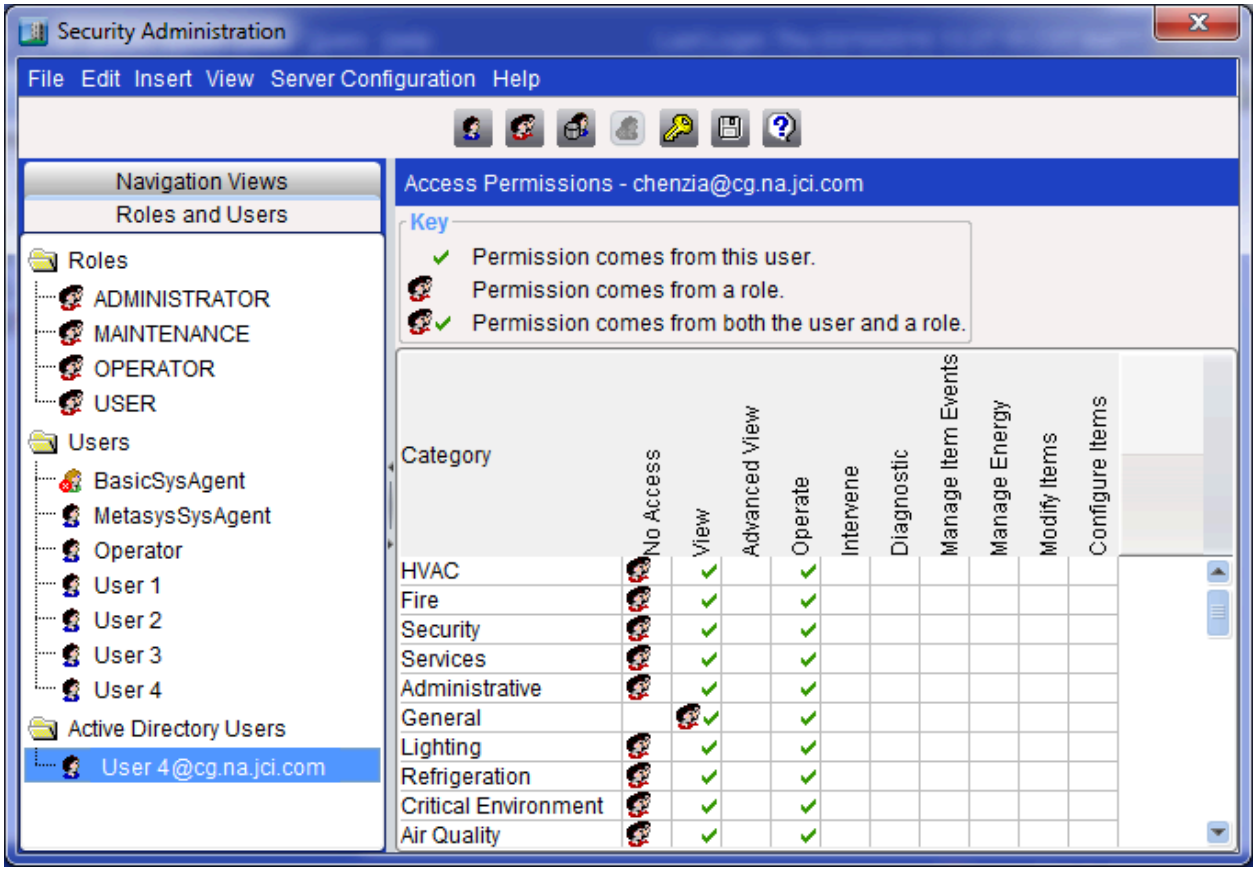
4. Specify the Active Directory User Name using the fully qualified username format (myUser@my.corp.com). Although the dialog reminds you to add the user to the MSEA-SSO Windows group, that is no longer necessary. (For information on this step, see User Account Rules and Username Semantics.)

5. Click **Add**. The Metasys system communicates with Active Directory services to verify this user.
   If the domain provided is not a recognized Active Directory service domain or it is not in the correct format, the message `Active Directory Service Account Authentication Failed` appears.

   If the domain name is correct but the new user cannot be found by Active Directory services, the message `Error encountered: Error in Authenticating Active Directory User` appears.

   If the new user is verified, the new user is added to the Active Directory Users folder in the **Roles and Users** tab (see Figure 30).

Figure 30: Adding Active Directory Service User



6. Open the user properties for the new Active Directory service user, fill in the information using Table 15, and then click **OK**.
7. Assign access permissions to the Active Directory service user in the same manner as you would for a Metasys local system user. For details, see System Access Privileges.

Selecting a Default Domain for Active Directory Service – Users

1. Log in to the Metasys server or SCT with a Metasys Administrator account.
2. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears (Figure 26).
3. On the Security Administration window, click **Server Configuration** > **Active Directory**. The Configure Active Directory dialog box appears (Figure 27).

4. Using the Login Page Default Domain Selection option, select the domain that the Metasys SMP UI presents as the default selection on the Metasys login screen. This default applies to all users, regardless of a particular user's domain; therefore, if multiple domains are used, you may want to select the domain that applies to the majority of users.
5. Click **Save** or **Apply** to save this change. Clicking **Save** returns you to the Security Administration screen.

Removing User Access to Active Directory Service from the Metasys System

1. Log in to the Metasys server or SCT with a Metasys Administrator account. On the Main screen, select **Tools** > **Administrator**. The Security Administration window appears.
2. Select the **Active Directory** service user you want to remove as a Metasys system user. On the Security Administration window, click **Edit**>**Delete**.
3. Click **Yes** to confirm the user deletion. This Active Directory service user is removed as a *Metasys* system user and the **Active Directory User** list is refreshed.

Suspending User Access to Active Directory Service on Metasys System

1. Log in to the Metasys server or SCT with a Metasys Administrator account. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears.
2. Select the **Active Directory** service user whose access to the Metasys system needs to be suspended.
3. On the **Edit** menu, click **Properties**. The **User Properties** tab of the **User Properties** dialog box appears (see Figure 16).
4. Select the **Metasys Access Suspended** check box.

   ⓘ **Note:** If the **Metasys Access Suspended** check box is already selected, this user may have been disabled or deleted by Active Directory services. You can confirm this status by verifying that the Active Directory Account Disabled or Active Directory Account Deleted property (found on the Active Directory Properties sheet) is selected for the user. If the Active Directory service user's account is enabled again or re-added, you must manually clear the **Metasys Access Suspended** check box.

5. Click **OK**.
   The Active Directory service user is prevented from logging in to the system. If the user is currently logged in, theMetasys system terminates the user's session immediately. To re-enable Metasys system access for an Active Directory service user, clear the **Metasys Access Suspended** check box.

Synchronizing an Active Directory Service – User Account

1. Log in to the Metasys server or SCT with a Metasys Administrator account.
2. On the Main screen, click **Tools** > **Administrator**. The Security Administration window appears (Figure 30).
3. In the **Active Directory Users** folder, click the name of the user you want to synchronize. This action initiates the synchronization process with Active Directory services. Any changes to the account are applied.

   ⓘ **Note:**

   - Depending on the Active Directory service refresh rate, immediate changes to a user's properties at the Active Directory service domain server may take a few seconds to propagate to the Metasys system.

- The following message appears the first time you try to synchronize a user who has been deleted as an Active Directory service user, but remains a user in the Metasys system: `This user was deleted from Active Directory but remains in the Metasys System.`

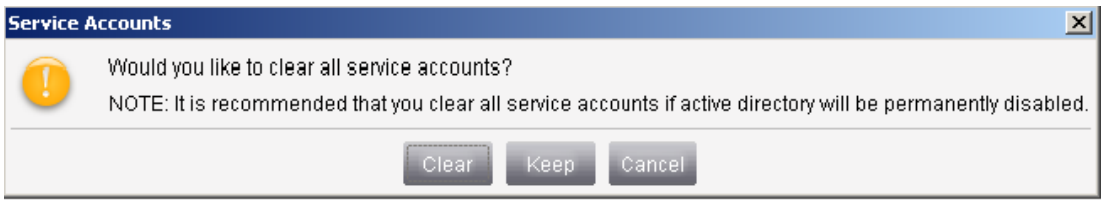
4. Close the Security Administration window.

Disabling Active Directory Service for Metasys System Use

About this task:
To disable Active Directory service for Metasys system use:

1. Log in to the Metasys server or SCT with a Metasys Administrator account. On the Main screen, click **Tools**> **Administrator**. The Security Administration window appears (Figure 26).
2. In the Security Administration window, click **Server Configuration** > **Active Directory**. The **Configure Active Directory** dialog box appears (Figure 27).
3. Clear the **Enable Active Directory Authentication** check box. This step prohibits the three Active Directory service selections from being edited.
4. Click **Save** or **Apply** to save your changes. A dialog box appears asking you if you want to clear all service accounts (Figure 31).

Figure 31: Clear Service Accounts User Message



5. The following options are available:

   - Click **Clear** if you want to clear all service accounts and intend to permanently disable Active Directory service authentication to the Metasys system. The list of selected service accounts is deleted.

     ⓘ **Note:** Before you disable Active Directory service authentication to the Metasys system, first remove all Active Directory service users from the Metasys system.

   - Click **Keep** if you want to retain all service accounts and intend to temporarily disable Active Directory service authentication to the Metasys system. The list of selected service accounts remains intact.
   - Click **Cancel** to do nothing and return to the previous screen.
   - Clicking **Clear** or **Keep** returns you to the Security Administration screen, which now shows the removal of the Active Directory folder and all Active Directory service users.

     ⓘ **Note:** When you disable the Active Directory service from being used by the Metasys system, the Active Directory service users are not removed from the Security Database. If at some point you re-enable the Active Directory service for use by the Metasys system, the Active Directory service users reappear in the Active Directory service folder of the Security Administration window.

Appendix: Metasys System SQL Server Accounts Connection Configuration

A new Metasys installation creates the predefined SQL Server login accounts and passwords described in SQL Server Login Accounts. The passwords for the SQL Server login accounts are randomly generated and encrypted, to ensure the highest level of security. End users can gain access through various user interfaces and Metasys processes for intercommunication. The end user accounts are described in detail in this document and in *Network and IT Guidance for the IT Professional Technical Bulletin (LIT-1201578)*. This document describes the *Metasys* SQL Server accounts and management of these accounts using the Database Connection Configuration Tool (DBCCT), DBConnectionConfigurationTool.exe. For security reasons, we strongly recommend changing the default passwords after installing the Metasys software.

Note: This document does not apply to SCT, which uses virtual service accounts and Windows authenticated authorization.

SQL Server Login Accounts

SQL Server login accounts are used for communications between the Metasys services and the databases that they rely on. Metasys devices and Metasys users access the Metasys services which make a connection to the databases using the login accounts described in the following tables. These accounts access the databases described in Table 26.

Table 26: Metasys server default user names

User Label	Account Purpose	Default Account Name	Database Name	Database Role Membership
XMS DB User	Read/write site configuration information	ads-user	XMS	db_owner
Historian DB User	Read/write the historical (trend) database	ads-user	JCIHistorianDB	db_owner
Events DB User	Read/write the events database	ads-user	JCIEventsDB	db_owner
Audit DB User	Read/write the audit database	ads-user	JCIAuditTrails	db_owner

Table 26: Metasys server default user names

User Label	Account Purpose	Default Account Name	Database Name	Database Role Membership
Security DB User	Authentication/ authorization service uses to retrieve authentication and authorization information from the security database	g3-AuthUser	MetasysIII	db_owner
Annotation DB User	Annotation database uses to read/write annotations in MVE	ads-user	JCIItemAnnotation	db_owner

Table 27: Additional Default User Names

User Label	Account Purpose	Default Account Name	Database Name	Server Roles
ARS DB User	Reporting component of ADX uses to access the reporting database and the configuration archive	g3-MetasysReportServer [1] ⓘ **Note:** The account name is read-only.	MetasysReporting, MetasysTranslation Dictionary, MetasysValue, MetasysFault, MetasysFaultTriage, and SCTTranslationDictionary	db_datareader, public
Reporting DB User	Access the MUI reporting database	ads-user	SpacesAuthorization database and JCIReportingDB	db_owner

1 In a split ADX configuration, the Advanced Reporting component uses the g3-MetasysReportServer account to access data on the ADX data server through a linked server connection in the ADX database. [1]

Integrated Authentication

The Metasys server services do not use integrated authentication. SCT has two virtual service accounts, IIS APP\MSEA_SCT_APPPOOL and NT SERVICE\MIIISCTAQ, that uses integrated authentication. The access passwords are managed through Windows and the access password can not be changed.

Account Removal During Uninstall

Metasys servers - ADS/ADX/OAS/ODS

When you uninstall a Metasys server, the default SQL server login accounts are removed, even if you choose to retain the databases. This means that you must reset the passwords after you reinstall the server.

SCT

When you uninstall the SCT, the archive database accounts are maintained. There is an option to remove the SCT database and SQL Server login accounts during the SCT uninstall.

Account Reset During Upgrade

When upgrading your Metasys system, the installation program removes the previous version of Metasys software and removes some SQL login accounts. The installation program then creates the default SQL server login accounts. If you previously modified any SQL accounts, the Metasys administrator must update the accounts according to the security policy.

Database Connection Configuration Tool

The Database Connection Configuration Tool (DBCCT) is used to synchronize the SQL server login accounts and passwords embedded in the connection strings used by the Metasys components to connect to their respective SQL Server hosted repositories. The synchronization is necessary when the SQL server accounts are modified in SQL server, typically for security reasons. While you can use different SQL Server login account names, we do not recommend this practice. Using different SQL Server login account names may break other work flows, such as Metasys upgrades. The Metasys system is not tested with modified account names. Use the following workflow to change the accounts after installing the Metasys server.

Note: The ADS uses non-interfering SQL Login accounts and Windows services. Stop the ADS services for the ADS version of DBCCT.

1. Stop the required Metasys services and app pools.

   Table 28: Metasys Services and App Pools

Services to Stop Manually **Control Panel** > **System and Security** > **Administrative Tools** > **Services**	**App Pools to Stop ManuallyControl Panel** > **System and Security** > **Administrative Tools** > **Internet Information Services (IIS) Manager**
Metasys ActionQ	AuthenticationService_AppPool
Metasys Device Manager	ConfigService_AppPool
Metasys.AuditService	EventService_AppPool
Metasys.Config.Ingestion	FaultServiceAppPool
Metasys.EventService	FaultTriageAppPool
Metasys.FaultService	SchedulerService_AppPool
Metasys.LicenseService	TimeSeriesService
Metasys.SchedulerService	UI_AppPool
Metasys.TimeSeriesService	UserService_AppPool
Metasys.Value.DataCollectorService	ValueServiceAppPool

2. Run the DBCCT to update the database connection strings of the components that use the modified accounts.
3. In the SQL Server Management Studio, modify the password of the desired SQL Server login accounts.
4. Reboot the server to restart the system. This is important to ensure that all the services start up again.

See Using the DBCCT for more information about Steps 2 and 3.

Metasys Services

Metasys software installs Windows services. These services include:

- Device Manager (MetasysIII Device Manager)
- ADS/ADX Action Queue (MetasysIII Action Queue)
- Advanced Reporting Cache Refresh (Metasys Report Cache Refresh)

Upon startup, DBCCT checks the status of the Metasys services as shown in Table 29. The tool displays only the tabs and edit fields needed to configure the installed services. You cannot access these fields and tabs until all installed services are stopped. If the tool detects any services running, the editing fields appear as read-only and a message indicates the detected service. We recommend stopping these services before using the DBCCT.

Table 29: DBCCT Verified Services

Application Name	Service or Application Pool Name
ADS\ADX\OAS\ODS	UI_AppPool ActivityService_AppPool Metasys.ActivityService EventService_AppPool Metasys.EventService TimeSeries_AppPool Metasys.TimeSeriesService SchedulerService_AppPool Metasys.SchedulerService AuthenticationService_AppPool HealthService_AppPool ObjectService_AppPool UserService_AppPool Metasys III Device Manager Service Metasys III Action Queue Service Metasys app pool
Advanced Reporting System (ARS)	Metasys Report Cache Refresh
Metasys UI (Release 8.0 and 8.1)	UI_AppPools

Stopping Metasys Services on the ADS

At Metasys 10.0 and later, a batch file can be used for stopping starting, and restarting Metasys Server services. The batch file stops the services in the order listed in Table 29. To run the batch file, do the following:

1. Browse to `C:\ProgramData\Johnson Controls\MetasysIII\Diagnostics\Utilities`.
2. Right-click `stop.bat` and select **Run as Administrator**. Click **Yes** in the **User Account Control** dialog box. A Command Prompt windows appears and displays the status of the services. When the services stop, the Command Prompt window closes.

   Note: You can also use the batch file to restart services on the ADS. For further information, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.

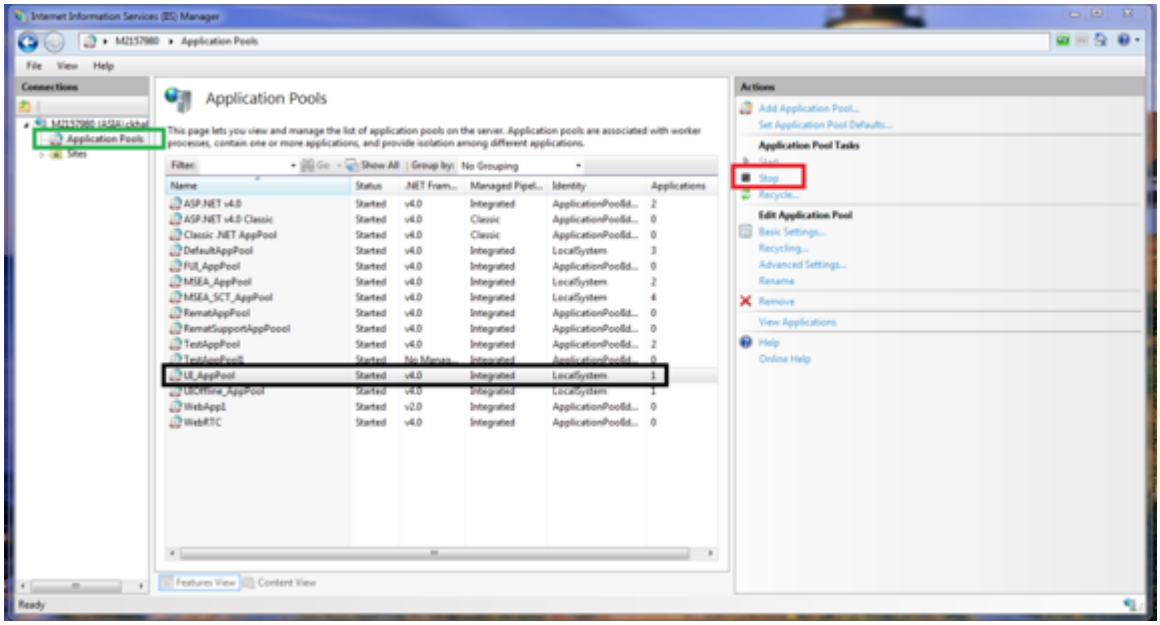
Stopping *Metasys* Services in Metasys UI

About this task:

This procedure must be performed if Metasys UI is installed with Metasys Release 8.0 and 8.1.

1. Open IIS Manager.
2. Select **Application Pools**.

Figure 32: Application Pools



3. Select **UI_AppPool**.
   The Application Pool Tasks pane appears.
4. Click **Stop**.

Using the DBCCT

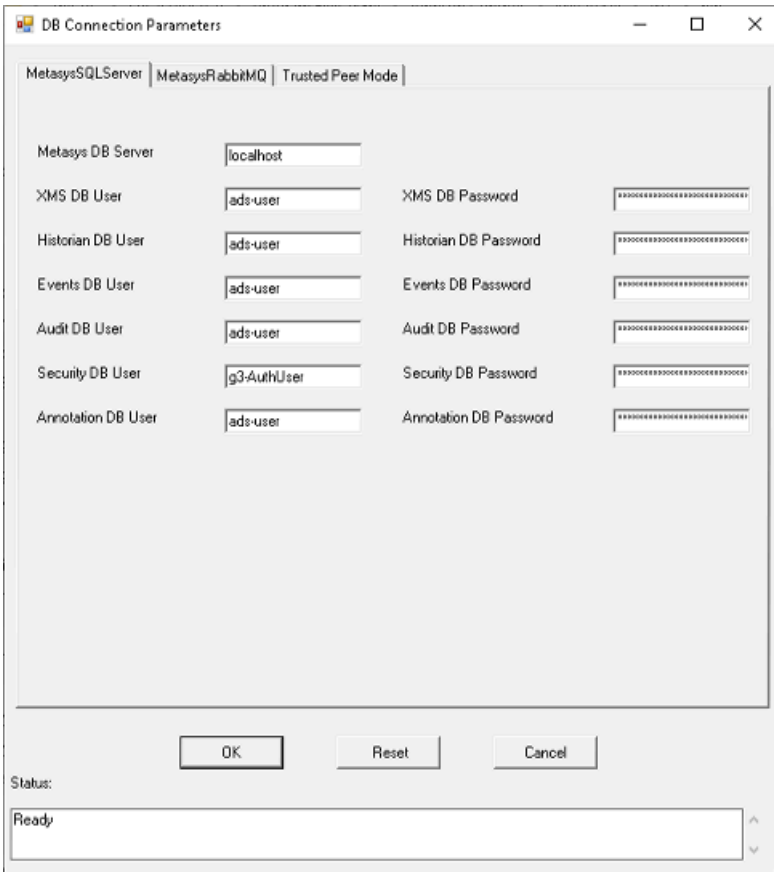
About this task:
The DBCCT is intended for use by administrators only. The ADS version of the tool only operates on the account used within selected tool location.

Note: On a split ADX, run DBCCT from the web server.

The tool is installed in the ADS path: `<Metasys Web Site>\WS\bin\DBConnectionConfigurationtool.exe`

1. Browse to the tool location.
2. Launch the tool.

Figure 33: ADS DB Connection Parameters



3. Change the passwords.

   ⓘ **Note:** An administrator can use the MetasysSQLServer tab to customize the random passwords created at install time for the SQL named accounts which Metasys uses.

   ⓘ **Note:** An administrator can use the MetasysRabbitMQ tab to customize the random passwords created at install time for the RabbitMQ Message bus which Metasys uses for on-box inter-process messaging.

   ⓘ **Note:** From Metasys Release 11.0, an administrator can use the tab for Trusted Peer Mode to customize the random passwords created at install time for on-box inter-Micros Service communication. These are credentials which can be used to retrieve an access token from the authentication service by a micro-service so that it may perform requests against another micro-service's public APIs. These requests are trusted because they do not represent a Metasys user but have the ability to make any public API call.

4. Click **OK**.

   This saves all changes to the configuration files and affects all user names and passwords in the server. **Reset** restores all user names and passwords to their values at the time the tool opened. These values may be different form the installation defaults if DBCCT was previously run. **Cancel** or **X** cancels all pending changes.

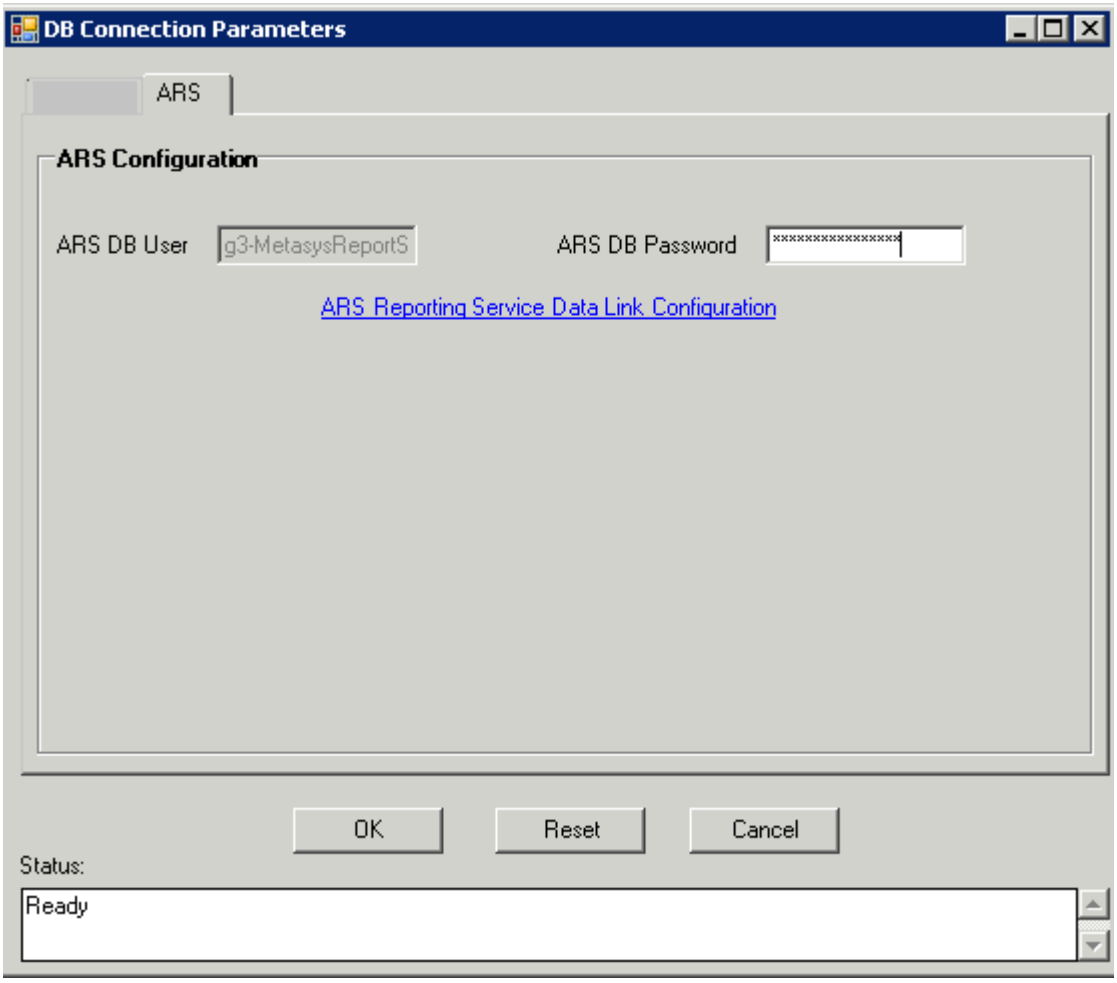
   ⓘ **Note: OK** only saves the connection strings to the configuration file. The Metasys server web services running under IIS still cache the old connection values. You must manually reset IIS after closing the tool. This allows the web services to reload the new connection data.

5. Confirm the change.
   After you confirm the change, a message appears indicating the configuration changes were successful.
6. In SQL Server Management Studio, change the Security Logins passwords to match the server passwords.

Updating the ARS Configuration

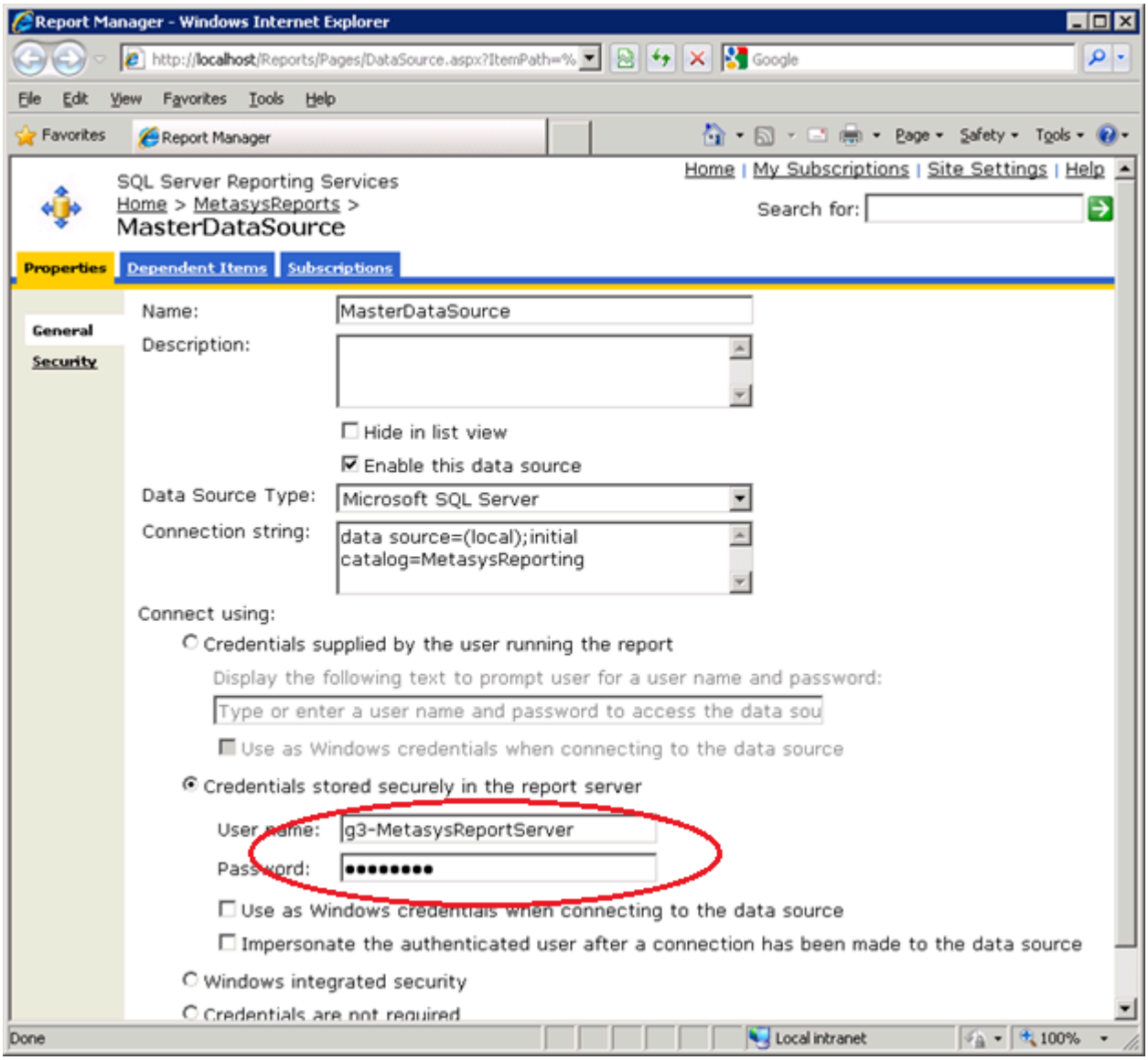
1. Select the **ARS** tab in the DBCCT.

Figure 34: DB Connection Parameters ARS Configuration



2. Update the ARS DB password.
3. Click **ARS Reporting Service Data Link Configuration**.

Figure 35: SQL Reporting Services



4. Update the g3-MetasysReportServer password to match the password you entered in Step 2.
5. Click **OK**.

Changing SQL Passwords

1. Open SQL Server Management Studio.
2. Connect to the server.
3. Expand the **Security** folder.
4. Expand the **Logins** folder.
5. Right-click a user whose password was changed in DBCCT and select **Properties**.
6. Change the password in the **General** tab.
7. Click **OK**.
8. Repeat Steps 5 and 6 for all users whose password was changed.

Server Name

The ADS DB Server field contains the name of the SQL server that hosts the server databases. In a single box ADX, the name is the same as the application server. In a split ADX configuration, this field contains the database server name. This field format is the standard SQL connection string syntax. Metasys supports using SQL Server that has named instances.

Table 30: Server Names

Format	Example	Format with Instance Name	Example with Instance Name
protocol name:server name]	(local) or localhost	protocol name:server name \instance	tcp:localhost\SpecialSqlServer
IP address, port number	159.222.10.194, 1500	IP address\instance name, port number	159.222.10.194\SpecialSqlInstance, 1500

User Names

User names are the login names from the server instance specified in the Server Name field. DBCCT does not validate the user names. You can enter any length name with the exception of the SQL login names, which are limited to 115 characters (SQL Server 2005).

Table 31: DBCCT Dialog Field Details

Field	Description
XMS DB User	The user name used by the ADX to access the site configuration database (XMS).
Historian DB User	The user name used by the data access service to access the historical (trend) database (JCIHistorianDB).
Events DB User	The user name used by the data access service to access the events database (JCIEventsDB).
Audit DB User	The user name used by the data access service to access the audits database.
Security DB User	The user name used by applications to access the security database (MetasysIII), to authenticate and authorize the end-user or calling process.
Annotation DB User	The user who connects to the annotation database (JCIItemAnnotation).
ARS DB User	The database user name impersonated by advanced reporting services (ARS) to obtain access to the databases. This user name is read-only. You cannot change this username.
ARS Reporting Service Data Link Configuration	This link launches the Microsoft SQL Server Reporting Services (SRRS) configuration screen, where you set the reports data source access password. Do not change the user name, only the password. ⓘ **Note:** When you save the password, the change is made even though the DBCCT dialog cancels.

Passwords

Passwords are the SQL Server Login account passwords defined in the server instance that is specified in the **Server name** field. The password length is not limited by DBCCT; however, the maximum password length in SQL Server is 128 characters. DBCCT does not require or prevent the user from entering complex passwords. The complex passwords policy is enforced by SQL Server.

This tool only sets the passwords to match the passwords set in SQL Server for the accounts and connection strings described in Table 26.

Status Messages

Status Messages appear in the DB Connection Parameters Status section.

Table 32: Status Messages

Message	Description
Ready	The tool is ready for action.
Metasys III Device Manager	The device manager is running. You can not update the connection configuration until you stop device manager and relaunch the application.
Error opening/reading configuration file	The connection configuration is locked by another process or missing and can not open for reading.
Error writing to the configuration file	The connection configuration is locked by another user or missing and can not open for writing.

Restarting Services

1. After the DBCCT closes, reboot the system.
2. Verify that the services you stopped in Stopping Metasys Services on the ADS are restarted.

Product warranty

This product is covered by a limited warranty, details of which can be found at www.johnsoncontrols.com/buildingswarranty.

Software terms

Use of the software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at www.johnsoncontrols.com/techterms. Your use of this product constitutes an agreement to such terms.

Patents

Patents: https://jcipat.com

Contact information

Contact your local branch office: www.johnsoncontrols.com/locations

Contact Johnson Controls: www.johnsoncontrols.com/contact-us