Infor Distributions A+ User Security User Guide

Version 11.00.01

Publication Information

Release: Infor Distributions A+ User Security User Guide

Publication date: October 7, 2025

Contents

About this guide

This guide describes workflow, concepts and procedures for using the Infor Distribution A+ User Security module.

Related documentation

You can find related documentation at Infor Documentation Central (docs.infor.com). We recommend that you check this website periodically for updated documentation.

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1 User Security Overview

User Security provides you with a flexible and robust security system comprised of three major categories: Application Function Security, Company, Warehouse & Salesrep Security and Application Action Security.

This overview provides a summary of the security design, company, warehouse & salesrep security and application action security, as well as the functionality provided by the features of the security system. Topics include:

- Company, Warehouse & Salesrep Security
- Application Action Security
- Cross Application File Maintenance Menu
- Security Menu
- Company, Warehouse & Salesrep Authority Checking Hierarchy
- Application Function Security Database Structure and Security Checking Logic
- Action Authority Security Database Structure and Security Checking Logic
- Security Infrastructure Redesign

Company, Warehouse & Salesrep Security

The Company, Warehouse & Salesrep Security functionality supports access authority based on company, warehouse and salesrep. Company, warehouse and salesrep security includes all of the necessary structure to restrict all processing, maintenance, inquiry and reporting function to the companies, warehouses and salesreps that a user has been given authority. The system will perform a security check (for many programs that use company, warehouse and salesrep) to determine for that company, warehouse and salesrep if the particular user can perform the function.

Application Action Security

Application Action Security is an infrastructure feature that is used to create a single place from which you can define security functions. Having security in one place, simplifies security setup and improves the ability to audit the application.

The feature name, Application Action Security, is derived from the intention to provide you with a level of security that is within the Distribution A+ menu structure (application security). Once you access a menu option, you then perform an action (e.g., enter an order). It is at this application action level that you may add an additional level of security.

Application Action Security is internally defined using the following four attributes:

1. Action Identifier: The action to perform (for example, Release, Change, Delete, etc.). If the application action allows a user to “Release an Order from Credit Hold,” the Action Identifier is **Release**.
2. Object Identifier: The object on which the action is performed (for example, Picklist, Cost, Order, etc.). If the application action allows a user to “Release an Order from Credit Hold,” the Object Identifier is **Order**.
3. Instance Identifier: Further defines the application object on which the action is performed (for example, if the application action allows a user to “Release an Order from Credit Hold,” the Instance Identifier is **Hold Code**).
4. Extended Instance Identifier (when appropriate): The feature that allows an instance of an action to be extended based on a defined application value. If the application action allows a user to “Release an Order from Credit Hold,” the Extended Instance is **CR** - this would be a valid hold code for orders on credit hold. The Extended Instance will allow some users to be authorized to release orders from Credit Hold, while different users could be authorized to release orders from Gross Margin hold.

These internal attributes are used to define authorities and are used by the system to access the specific authorities set up for an application action. An application action is a sub-task of a function. For example, a function is Enter, Change & Ship Orders (MENU OEMAIN), which provides you with the ability to create new orders, change existing orders and to perform shipping confirmation on an order (all of which are sub-tasks of the function). These orders could be regular customer orders, return orders, special orders or invoices (to name a few examples). You can sub-divide the features and define authority to these sub-divisions, giving some users authority to enter new customer orders and other users the authority to enter returns, etc.

Note: For a complete list of application actions, refer to APPENDIX C: Application Action Authorities. To review the original security options that have been replaced with application actions, refer to the Application Action Security Conversion section.

Using Application Action Authority Maintenance (MENU XASCTY), you define which users will have access to perform a given application action. For each application action available for each company defined to the system, you select the users and/or user groups that will be authorized to perform or access the given action. You will have the option to designate the application action to be available to all users, no users, only master users or selected users and/or user groups.

Cross Application File Maintenance Menu

To support User Security, the following fields are provided through System Options Maintenance (MENU XAFILE) on the Cross Application File Maintenance Menu:

- Activate Company Security: To allow you to determine if you want security for application functions based on company. If you select to activate security for a company, the system will perform a security check and see if a user is allowed to perform the function for the indicated company.
- Activate Warehouse Security: To allow you to determine if you want security for application functions based on warehouse. If you select to activate security for a warehouse, the system will perform a security check and see if a user is allowed to perform the function for the indicated warehouse.
- Activate Salesrep Security: To allow you to determine if you want security for application functions based on salesrep. If you select to activate security for a salesrep, the system will perform a security check and see if a user is allowed to perform the function for the indicated salesrep.

  Note: Regardless of security fields, if a user is a “Master” user they will always have access to all functions (that is, menu options) for all companies, warehouses, and sales reps. However, additional Application Action Authority edits may prohibit the Master user access to certain application actions.

Distribution A+ Security Menu

To provide you with a security system that resides in a single place and to simplify security setup, the Distribution A+ Security Menu (MENU XASCTY) was created. A brief description of each menu option is described below.

- Option 1 - User Maintenance: Used to define the users that will have access to Distribution A+ menu functions. If user and menu security features are active, a user must be defined through this option in order to obtain access to any menu options.
- Option 2 - User Group Maintenance: Used to define Distribution A+ User Groups and to assign users to these groups. User groups are a security feature that allow you to assign certain authorities to groups of users simplifying the effort required to define application authorities. By giving an authority to a user group you in effect provide that authority to all users that are defined within that group. Uses of a user group might include: authorizing access to menu functions, providing authority to General Ledger accounts, authorizing use of secured features (such as releasing orders), and authority to view and/or change secured values (such as cost and profit).
- Option 3 - Authority Profile Maintenance: Used to define “Public” authority profiles. Authority profiles are used to define general authority access parameters that determine a user's authority levels. By defining “Public” profiles you can establish these parameters and assign this profile to the users that you want to have the same authority without having to duplicate it multiple times. Through this menu option, you assign Master User Authority, General Ledger and Account Number Authority, Company, Warehouse & Salesrep Authority, and Default Company and Warehouse.
- Option 4 - Application Authority Maintenance: Used to define application access (or menu option) authority to your various users and user groups. This option provides various methods for assigning these authorities. You can select a user and then select the functions that user is authorized. You can select a user group and select the functions that users in this group are

authorized, or you can select an application function and check off which users/user groups will be authorized to the selected function. This option also provides the ability to add custom menus and options to Distribution A+ security checking.

- Option 5 - Company/Warehouse/Salesrep Authority Maintenance: Used to define the Company, Warehouse and/or Salesrep Authority feature of Distribution A+ security. Once the Company, Warehouse and/or Salesrep Authority feature is activated, all users that are not Master users or have not chosen to bypass company, warehouse and/or salesrep security in the Authority Profile will be subject to the company, warehouse and salesrep authority check. This option will provide you with the ability to determine on the application function, user/application function and user group/ application function level if the company, warehouse or salesrep authority check will be bypassed.
- Option 6 - Application Action Authority Maintenance: Used to define which users will have access to perform a given application action by selecting users and/or user groups for each application action available for each company defined to the Distribution A+ system. You will have the option to designate the function to be available to all users, no users, only master users or selected users and/or user groups. See Application Action Security for further details.
- Option 7 - Authorization Codes Maintenance: Used to define authorization codes that you can associate with particular application actions. Authorization codes provide an alternate method for providing access to a secured application action. When you define authorization codes, you are creating codes that are used to permit overrides in specific situations, such as to authorize the cancellation of an order for a clerk who does not have authority to cancel an order. If a user is attempting to perform an action that he/she is not authorized to perform, and an authorization code has been set up for the particular action, an Authorization pop-up window will display prompting the user to enter a valid authorization code to continue. If the user is aware of the code, he/she will be granted authority to the secured action. Authorization codes can be defined using either the Distribution A+ Security Menu (MENU XASCTY) or the Point of Sale File Maintenance Menu (MENU PSFILE).
- Option 30 - Security Audit Inquiry: Used to view access rights for a user or user group, a particular application function (menu option), or an application action. You can also use this menu option to print reports detailing the security audit.

Company, Warehouse & Salesrep Authority Checking Hierarchy

In order to provide you with the greatest amount of flexibility, multiple levels of authority checking have been built into the new security features. The multiple levels of authority were designed to provide for any authority exceptions to meet the needs of the different level of users accessing Distribution A+ application functions. The different levels are defined as:

- System
- Authority Profile
- Application Function
- User Group/Application Function

Note: Regardless of the different security levels, if a user is a “Master” user they will always have access to all functions (that is, menu options) for all companies, warehouses, and sales reps. However, additional Application Action Authority edits may prohibit the Master user access to certain application actions.

System Level

On the system level, as previously stated in this overview, System Options Maintenance (MENU XAFILE) includes the following tailoring options:

1 **Activate Company Security**

2 **Activate Warehouse Security**

3 **Activate Salesrep Security**

Selecting a ‘**Y**’ to these options activates the company, warehouse and/or salesrep authority checking features.

Authority Profile Level

Once the system level feature(s) is/are activated, by default all users are subject to the company, warehouse and/or salesrep authority checking logic. If a user (or group of users) is not to be subject to these authority verifications, then you can choose to exclude that user (or group of users) from this logic by selecting to omit the following authority verification options on the authority profile level through Authority Profile Maintenance (MENU XASCTY):

1 **Bypass Company Security**

2 **Bypass Warehouse Security**

3 **Bypass Salesrep Security**

Application Function Level

Once the system level options have been activated, all application functions (menu options) are subject to company, warehouse and/or salesrep authority checking. If there are some functions that do not need to prevent users from accessing information or performing functions on companies, warehouses and/or salesreps that the users are not normally authorized, those functions can be omitted from the authority checking logic. To omit certain functions, select to omit the following authority verification options on the application function level through Application Authority Maintenance (MENU XASCTY):

1 **Bypass Company Security**

2 **Bypass Warehouse Security**

3 Bypass Salesrep Security

User Group/Application Function Level

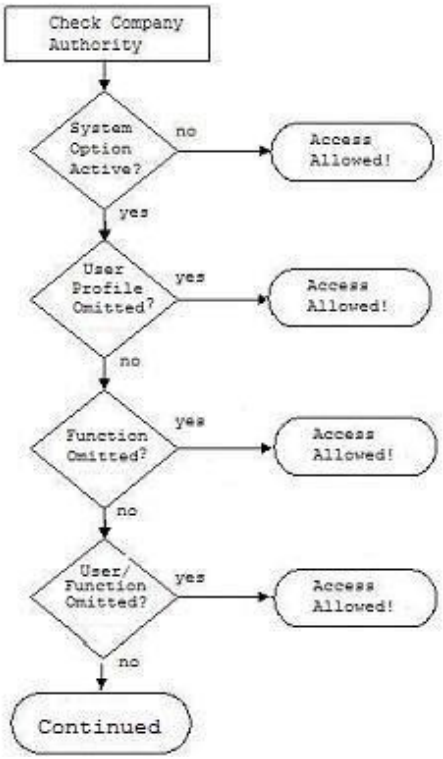
To provide the ultimate flexibility, the final level of authority checking omissions are on the user group/application function level through Application Authority Maintenance (MENU XASCTY). A specific user may be limited to performing certain application functions only for companies, warehouses and/or salesreps that they are authorized, but may need access to all companies/ warehouses/salesreps when they perform other application functions. Omitting the following authority checking options at this level will provide them with access to necessary functions:

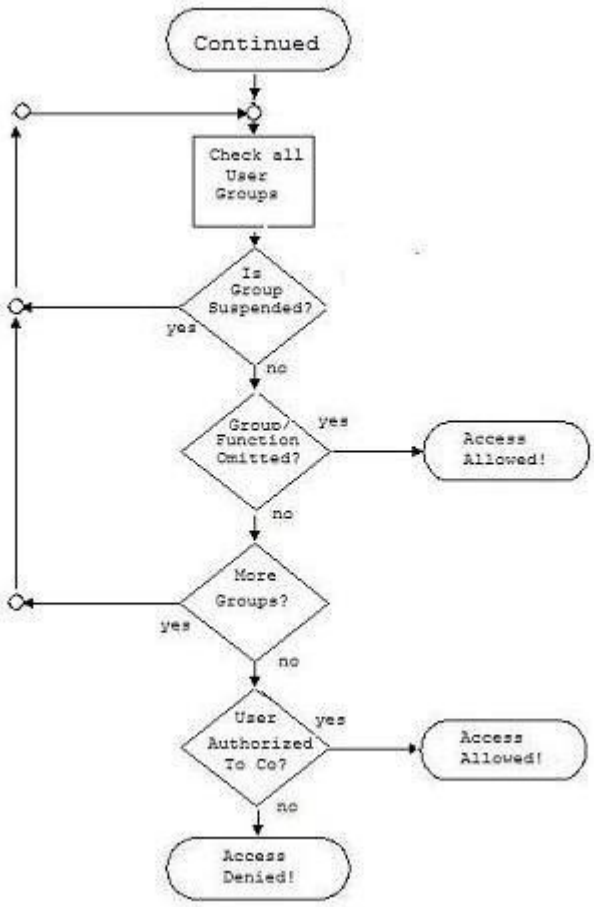
1 Bypass Company Security

2 Bypass Warehouse Security

3 Bypass Salesrep Security

Application Authority Checking Logic Flow





Application Function Security Database Structure and Security Checking Logic

To facilitate the security features and to provide a structure to simplify the security audit process, a set of database files have been introduced:

- Function Master File (**FNCMST**)
- Function Application File (**FNCAPP**)
- Function Menu File (**FNCMNU**)
- Job Function File (**JOBFNC**)
- User Master File (**USRMST**)
- Group Master File (**GRPMST**)

- Menu Master File (**MNUMST**)
- Authority Master File (**AUTMST**)
- Group/User File (**GRPUSR**)
- Application Function Authority File (**FNCAUT**)
- Company Authority File (**COAUT**)
- Warehouse Authority File (**WHAUT**)
- SalesRep Authority File (**RPAUT**)

Function Master, Function Application, Function Menu, and User Master Files

These files are used to provide the foundation for application authority and define the values used to determine what application functions (menu options) a user has authority to access. The Function Master (**FNCMST**), Function Application (**FNCAPP**) and Function Menu (**FNCMNU**) files are shipped with the programs and provide the values necessary to define each of the application interface functions or menu options and provide a framework to assist users in their security definition. They contain one record for each application function or unique menu option. Custom user created application functions can be added to these files to provide the same security features to custom processes as are available to the Distribution A+ functions.

Note: These are the same entries that were previously stored in the application program XASECM and displayed from the Security Option on MENU XASCTY.

Each user that will have access to these application functions must be defined in the User Master File (**USRMST**) and must be a valid IBM i user profile.

Authority Master File

The Authority Master File (**AUTMST**) contains the general security parameters. Through the use of this file, you are able to define these general security parameters either:

- on the user level by creating a personal authority profile that is the same as the user, or
- you can define a public authority profile that can be shared by multiple users by referencing that public authority profile in the user master definition.

User Group Master and Group User Assignment Files

User groups are defined in two files: the User Group Master File (**GRPMST**) and the Group User Assignment File (**GRPUSR**). The User Group Master File contains one record for each user group defined; this file simply defines the group. Users that are assigned to the group are contained in the

separate Group User Assignment File. This simplifies the user group definition process and helps to improve the audit ability of user groups.

Function Authority File

The Function Authority File (**FNCAUT**) provides a record for each application function that a user is authorized to. Additionally, these authorities can be defined on the user group level, allowing access to application functions to be defined by group as well as by an individual user.

Example: Define a user group called "**CUSTSERV**". You could then assign all of the customer service representatives to that user group. Then, using Application Authority Maintenance, you could provide access to all of the necessary application functions (or menu options) needed by a customer service representative (Enter, Change or Ship Orders, Open Order Inquiry, Customer Inquiry, etc.) by authorizing those functions to the user group "**CUSTSERV**," as opposed to each of the customer service users. All of the customer service representatives that are part of the "**CUSTSERV**" user group will have access to all of the necessary application functions to perform their job. If you then wanted to give the authority to release held orders to just the lead representative, you could provide access to the Order Release function to just that lead representative by using their User ID.

This simple example illustrates some of the flexibility that is available with the security infrastructure. The ability to define application function authorities on both the user and user group level and the addition of public authority profiles reduce the task load for adding and maintaining user security and improves the audit ability due to a structured database design.

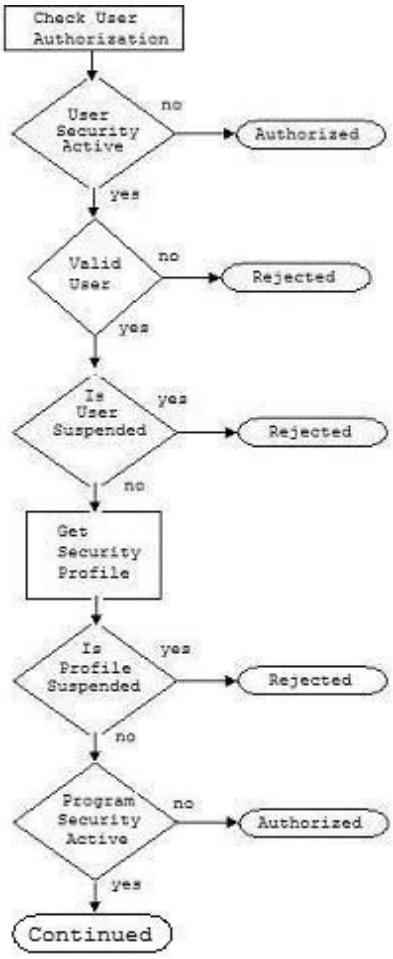
Company and Warehouse Authority File

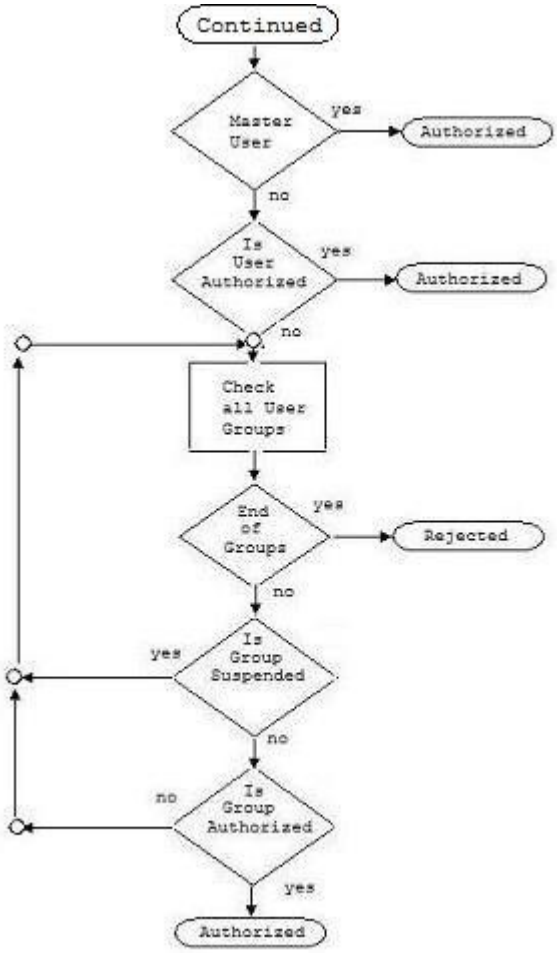
The Company Authority File (**COAUT**) and Warehouse Authority File (**WHAUT**) contains a record for every company and warehouse that a user has authority to access.

Salesrep Authority File

The Salesrep Authority File (**RPAUT**) contains the users and user groups that are authorized to a specific sales rep. This file is maintained by Application Authority Maintenance (MENU XASCTY).

User Authority Checking Logic Flow





Application Action Authority Security Database Structure and Security Checking Logic

The following set of database files are for application action authority security:

- Application Action Security Master File (**ACTMST**)
- Application Action Security Definition File (**ACTDEF**)
- Application Action Security Authorization File (**ACTAUT**)
- Salesrep Authority File (**RPAUT**)
- Clerk Group Master File (**CGPMST**)
- Clerk Group Association File (**CGPCLK**)
- Authorization Code Master File (**ACDMST**)
- Action Authorization Code File (**ACTACD**)

Application Action Security Master File

The Application Action Security Master File (**ACTMST**) defines the application actions and contains the control values that affect how the action is used. The data for this file is shipped with the software and cannot be maintained.

Application Action Security Definition File

The Application Action Security Definition File (**ACTDEF**) contains the company and store level (Point of Sale) determined user authority settings selected for an application action. This file is maintained through Application Action Authority Maintenance (MENU XASCTY).

Application Action Security Authorization File

The Application Action Security Authorization File (**ACTAUT**) contains the user, clerk, user groups and clerk groups that are authorized to a specific application action. This file is maintained through Application Action Authority Maintenance (MENU XASCTY).

Clerk Group Master File

The Clerk Group Master File (**CGPMST**) contains the definition of clerk groups, which are used to logically group clerks for the purpose of defining clerk authorities. It contains a record for each clerk group defined using Clerk Group Maintenance (MENU PSFILE).

Clerk Group Association File

The Clerk Group Association File (**CGPCLK**) contains the clerks that make up a specific clerk group. Clerks are added to a clerk group using Clerk Maintenance (MENU PSFILE) or Clerk Group Maintenance (MENU PSFILE).

Authorization Code Master File

The Authorization Code Master File (**ACDMST**) contains the definition of authorization codes. Authorization codes are used to provide access to certain application actions by allowing the user (or clerk) to authorize them to a specific action on demand. This file is maintained through Authorization Codes Maintenance (MENU XASCTY / MENU PSFILE).

Action Authorization Code File

The Action Authorization Code File (**ACTACD**) contains the authorization codes that are valid to provide access to a specific application action. This file associates authorization codes to application actions. These associations are currently restricted to POS actions and maintained through Authorization Codes Maintenance (MENU XASCTY / MENU PSFILE).

Security Infrastructure Redesign

The Security Infrastructure Redesign replaces the original user security infrastructure, providing you with more robust features and easier maintenance and review of user authorities. Features include a flexible user friendly security maintenance program, expanded use of user groups for application authorities (security for all users will not be required and authority can be defined at the group level), and improved user authority audit capabilities. By restructuring the existing security, you can now query information you want to review and quickly access information you need to analyze for audit purposes.

Important:

When this enhancement is initially installed in a software update, the conversion process is intended to duplicate the previous security profile. You can then take advantage of the new security features by defining new security profiles and changing user security definitions. Additionally, when you update to Version 6.0, ONLY those users that were master users before the update will have access to the menu options on MENU XASCTY. If you were not a master user and had access before, you will need to be reauthorized. Finally, due to this enhancement, security menu options on MENU APFIL2 and GLFIL2 are no longer available. Security maintenance is performed through MENU XASCTY.

Note: For Version 6.0 Cumulative 8, additional conversion programs run which will populate the Application Action Definition File from various Order Control file options.

Security Files

Unlike the predecessor Security File (**SECTY**), the new User Master File (**USRMST**) will only contain basic user definition information. The general security information that was previously stored in the Security File has been moved to other files to provide both improved flexibility and additional features and functions.

User groups, which were previously defined in the User Group File (**USERG**) have been moved to two new files: the User Group Master File (**GRPMST**) and the Group User Assignment File (**GRPUSR**).

Important

Beginning with Version 6.0 Cumulative 5, the **User Group** field has been increased from five to ten characters for Distribution A+ User Security. For menu/option access, feel free to use the complete ten character field if necessary. For example, User Group CST- SERVICE might be created for your users in the Customer Service area and you may choose to give them access to all the Order Entry menu options. However, User Group INQUIRY may be created for users that only have inquiry access and you would then only select the inquiry menu options for menu/option access.

For version releases Version 6.0 Cumulative 5 through Version 6.0 Cumulative 7, five character User Group names must still be adhered to in areas in the Distribution A+ system. Groups that are currently used to secure GL account numbers and to control certain detailed application functions (such as releasing orders and displaying costs) are five characters maximum for the indicated version releases. As of Version 6.0 Cumulative 8, all areas in Distribution A+ support the new ten character User Group names.

The Function Authority File (**FNCAUT**) replaces the security string field that was contained in the predecessor Security File (**SECTY**).

Chapter 2 User Security Setup, Planning & Implementation

This chapter explains how to:

- Plan for conversion
- Simplify User Security functionality by performing various set up steps

  Note: Installation instructions are explained in a stand alone supplement.

Getting Started - The Importance of Setup

Prior to using Distribution A+, you must make procedural decisions and provide operational-related information required by the system in order for it to run properly. You will have to make decisions in the areas of business operations on the Cross Applications File Maintenance Menu (MENU XAFILE), Distribution A+ Configuration Menu (MENU XACFIG) and Distribution A+ Security Menu (MENU XASCTY). The decisions you make and the responses you provide are based on the manner in which you do business and therefore allow you to tailor Distribution A+ to meet your needs.

The sections in this chapter outline the Cross Application steps required to derive, at a high level, the procedural and operational data needed; focus on software update and planning and implementation; and, the steps you can optionally take to maximize your security process.

User Security Setup

Note: The steps in this section apply only if you are converting from a release of Distribution A+ prior to Version 6 Cumulative 5. If you are a new install, skip this section and refer to User Security Planning.

This section is used to plan for the implementation process that occurs for User Security functionality that is installed with Version 6.0 Cumulative 5 or later.

When the security functionality is initially installed, the conversion process is intended to duplicate the previous security profile. You are not required to perform any of the following setup steps; these

steps are included in this section only if you want to take advantage of the new security features by defining new security profiles and changing user security definitions. We recommend that you review the setup steps in this section before you begin the installation of Distribution A+ Version 6.0 Cumulative 5 or later.

Important

When Version 6.0 Cumulative 5 or later is installed, all current user security settings and data will be converted into the advanced security database. This conversion will make some assumptions based on the current security setup. Because of this, we suggest that you review your existing security definitions and, if possible, make some adjustments prior to the installation of this new security program.

A few security definitions in particular that we recommend you review are:

- Your current use of companies keyed into any of the ten authorized company fields on the User Information Screen in the Security definition (MENU XASCTY). These authorized companies are used exclusively by the General Ledger (GL) and Accounts Payable (AP) applications to limit access to certain sensitive data. If these company values have been entered for users that are not GL or AP users, or for users that are defined as Master users, unnecessary data will be generated by the conversion process. This data may make later use of the new security features slightly more involved. Therefore, although it is not required that this review occur, if these companies are filled in erroneously, we suggest that they be removed prior to the upgrade.
- Your existing and converted security tailoring options. Due to Application Action Security, a conversion occurs from the tailoring options records to the Action Security Database. For a list of the existing security options that have been removed and what security options replaced them, refer to the Application Action Security Conversion.

User Security Setup Steps

1 Verify IBM i User Profiles

a The Distribution A+ user data will be verified against the existing IBM i User Profiles. Any user that does not have a corresponding IBM i User Profile will not be converted into the User Master File (**USRMST**) or Authority Master File (**AUTMST**).

b The **User Name**, when displayed anywhere, will now be extracted from the IBM i User Profile. There will no longer be duplication of effort for typing a user's name.

c The User Master File (**USRMST**) and Authority Master File (**AUTMST**) contain 10 character user fields. All 8 character users will be converted to a matching 10 character user if one exists. For example, for employee M. Richardson, MRICHARD is the Distribution A+ user; however, the IBM i User Profile is MRICHARDSO. The User Master File and Authority Master File will be created with MRICHARDSO as the user.

d Remove any IBM i User Profiles that are no longer employed by your company.

2 Verify Distribution A+ Users

a Remove any users that are no longer employed by your company.

b Review existing records for accuracy of data:

- Per user, there are currently 10 authorized company fields that are used only for General Ledger and Accounts Payable access. If your users have data in these fields erroneously, clear out that data so the new security tailoring options will be set correctly. There should ONLY be an authorized company field if a user is a General Ledger or Accounts Payable user that is restricted to that specific company.
- Determine the accuracy of the **Master User** Y/N field in Authority Profile Maintenance (MENU XASCTY). With User Maintenance (MENU XASCTY) and Authority Profile Maintenance (MENU XASCTY) security, this field is particularly important because it grants total access without exception.

3 Warning Note

a Be advised that the original Security File (**SECTY**) and User Group File (**USERG**) will NOT be used with User Security. The data in the Security File will be converted into the User Master File (**USRMST**) and Authority Master File (**AUTMST**), and the data in the User Group File will be converted into the Group Master File (**GRPMST**) and Group User File (**GRPUSR**). All default values will be copied from the original files.

Checklist: User Security Setup

What To Do	Menu and Option
☐ Verify IBM I User Profile	N/A
☐ Verify Distribution A+ Users	User Maintenance (MENU XASCTY)

User Security Planning

This section describes setup steps that you can optionally take in order to simplify user security functionality.

User Security Planning Steps

1 Access to the Security Menu (MENU XASCTY)

a For existing installs prior to Version 6 Cumulative 5

All options on the Infor Distribution A+ Security Menu (MENU XASCTY) have changed. Due to the rewrite of the Infor Distribution A+ Security menu options, access to any of the new menu options will only be allowed to “Master” users (i.e. users defined in the installation as

Master users) once the conversion process has taken place. While you are signed on as a Master user, you will need to access Application Authority Maintenance (MENU XASCTY) and grant the appropriate users access to the options on the Infor Distribution A+ Security Menu.

b For new installs

Any users that you created as Master users during the installation process will have access to the menu options on the Infor Distribution A+ Security Menu (XASCTY).

2 Determine Public Authority Profiles

a Determine how many Public Authority Profiles will be needed to organize your users. Authority Profile Maintenance (MENU XASCTY) contains the following information:

- master user
- default company
- default warehouse
- maintain help text
- password required
- G/L security options
- A/P security options
- bypass company security
- bypass warehouse security
- bypass salesrep security

By creating Public Authority Profiles, you can easily establish consistent access for your existing users as well as setting the basis for easily adding new employees. For example, Public Authority Profile CO1WH3 might be created and assigned to users that should have access to only company 01 and only warehouse 3.

3 Determine User Groups

a Determine how many User Groups will be needed to organize your users. Menu/Option access can be established by User or User Group. By creating User Groups based on the types of job functions at your company, you can easily set up your users with consistent access to the menu/ options needed to perform their jobs.

Important: The User Group field is 10 characters for Distribution A+ User Security. For menu/option access, feel free to use the complete 10 character field if necessary. For example, User Group CSTSERVICE might be created for your users in the Customer Service area and you may choose to give them access to all the Order Entry menu options. However, User Group INQUIRY may be created for users that only have inquiry access and you would then only select the inquiry menu options for menu/option access.

4 Verify System Options Maintenance Tailoring Options

a There are new tailoring options in System Options Maintenance (MENU XAFILE): **Activate Company Security, Activate Warehouse Security**, and **Activate Salesrep Security**. Based on the setup of the existing data in your files, the system will determine how to set the System Tailoring Options. It will set the options to the values that match how your users are

currently established, so there should not be any disruption in daily activity while you create and implement the new security values.

5 Authorized Companies in the Security File (SECTY)

a For existing installs

If your users have any Authorized Companies in the Security File (SECTY), the conversion will create bypass company, bypass warehouse and bypass salesrep records that you will have to remove for each function as you begin your implementation.

b For new installs

Not applicable for new users.

6 Review Application Action Authorities

Note: For details about action authorities, refer to Application Action Security.

a For existing installs prior to Version 6 Cumulative 5

Due to Application Action Security, a conversion occurs from select tailoring options records to the Action Security Database and various security options are removed and replaced with new application actions on the Infor Distribution A+ Security Menu (MENU XASCTY). For a list of the existing security options that have been removed and what security options (application actions) replaced them, refer to the Application Action Security Conversion.

b For new installs

Review the application actions through Application Action Authority Maintenance (MENU XASCTY) to determine types of authorities you need to define.

Checklist: User Security Planning Steps

What To Do	Menu and Options
☐ Access to Menu Security	Application Authority Maintenance (MENU XASCTY)
☐ Determine Public Authority Profiles	Authority Profile Maintenance (MENU XASCTY)
☐ Determine User Groups	User Group Maintenance (MENU XASCTY)
☐ Verify System Options Maintenance Tailoring Options	System Options Maintenance (MENU XAFILE)
☐ Remove records - Authorized Companies in the Security File	Company/Warehouse/Salesrep Authority (MENU XASCTY)
☐ Review Application Action Authorities	Application Action Authority Maintenance (MENU XASCTY)

User Security Implementation

This section describes the setup steps you take in order to implement User Security.

User Security Implementation Steps

1 Determine Implementation Methodology

a Determine your implementation methodology: company, warehouse, and/or salesrep security, departments, users, authority profiles, and user groups. At this point, do not perform any steps other than determining what your method will be.

2 Create Public Authority Profiles

a Create the needed Public Authority Profiles establishing default values and authorized company and warehouse values and know what users will have these Public Authority Profiles assigned to them.

3 Create Users

a Define the users that will have access to Distribution A+ menu functions. If the user and menu security features are active, then a user must be defined in order to gain access to menu options. Assign the appropriate authority profile to the users.

4 Create User Groups

a Create User Groups and then assign users to the User Groups. Keep a list of what users have been assigned to what user groups.

5 Assign Public Authority Profiles

a Assign the Public Authority Profiles to users in manageable numbers to troubleshoot any questions that may arise.

b Validate users have access to the correct companies and warehouses and are denied access to appropriate companies and warehouses. This step can only be performed after you select System Options Maintenance (MENU XAFILE) and activate company and warehouse security.

6 Assign Application Authority

a Based on your lists of users and user groups, grant access to appropriate menu options.

7 Assign Company/Warehouse/Salesrep Authority

a Setup overrides to other company, warehouse, and salesrep security levels by User, User Group, and/or Function.

b Remove the application function level bypass company, bypass warehouse and bypass salesrep values for the application menu options that you are ready to now utilize for the company, warehouse and/or salesrep security.

8 Activate Security

a Select System Options Maintenance (MENU XAFILE) and activate Company, Warehouse, and/ or Salesrep Security.

9 Verify or Define Application Action Authorities

a If you are a current user, select Application Action Authority Maintenance (MENU XASCTY) to verify existing authorities. If you are a new user, set up authorities for application actions for each company using Distribution A+.

10 Verify User Security

a Select the Security Audit Inquiry (MENU XASCTY) to verify your security setup for both application functions and application actions.

Checklist: User Security Implementation Steps

What To Do	Menu and Option
☐ Determine Implementation Methodology	N/A
☐ Create Public Authority Profiles	Authority Profile Maintenance (MENU XASCTY)
☐ Create Users	User Maintenance (MENU XASCTY)
☐ Create User Groups	User Group Maintenance (MENU XASCTY)
☐ Assign Application Authority	Application Authority Maintenance (MENU XASCTY)
☐ Assign Company/Warehouse/Salesrep Authority	Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY)
☐ Activate Security	System Options Maintenance (MENU XAFILE)
☐ Verify or Define Application Action Authorities	Application Action Authority Maintenance (MENU XASCTY)
☐ Verify User Security	Security Audit Inquiry (MENU XASCTY)

Chapter 3 User Maintenance/Listing

Maintaining Users is performed through the Distribution A+ Security Menu (MENU XASCTY). User maintenance allows you to define the users that will have access to Distribution A+ menu functions. If the user and menu security features are activated through System Options Maintenance (MENU XAFILE), then a user must be defined through this option in order for them to access Distribution A+ menu options.

This is the starting point for all security features. Before any security features can be defined through this option for a user, the user must first be identified to the system, by receiving a valid IBM i user profile, and must be registered as a Distribution A+ user. A user can be manually registered through Register A+ User IDs on the A+ Configuration Menu (MENU XACFIG), or, if you are copying user security settings from an existing user through this option, an initial registration record will be automatically created when the system detects that one did not already exist for the new user you are adding.

We recommend that you carefully plan the types of users in your organization and create Authority Profiles for the company, warehouse, and sales rep assignments and User Groups for access to menu options and functionality within the menu options a user has been granted access to.

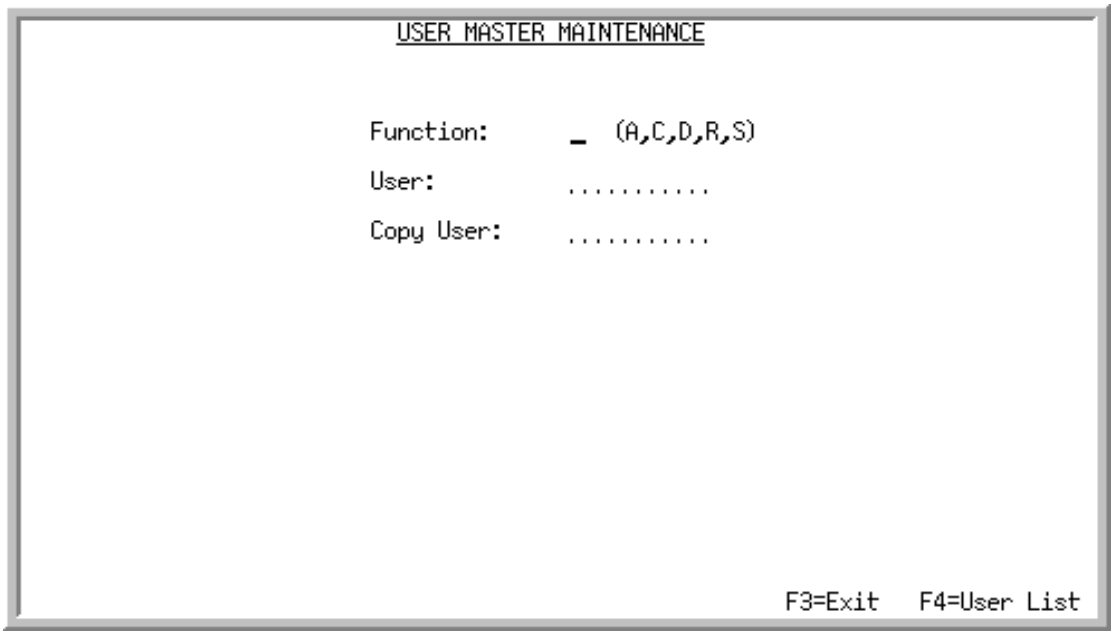
User Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
User Master Maintenance Screen	Used to add, change, delete, reinstate, and suspend valid users, already identified to the system through Register A+ User IDs (MENU XACFIG).
User List Screen	Used to display users (users in the Distribution A+ User File in the current base) and environment users (users in the User Master File in the current environment, previously defined through this menu option with a user master definition).

Title	Purpose
User Master Definition Screen	Used to set up and maintain a user authority profile for the indicated user. User authority profiles are used to define a user's general access authorities.
Authority Profile Definition Screen	Refer to Authority Profile Maintenance for an explanation of this screen.
Authority Profile List Screen	Refer to Authority Profile Maintenance for an explanation of this screen.
User Group List Screen	Used to assign the current user to a user group or multiple groups.

User Master Maintenance Screen



Use this screen to add, change, delete, reinstate, and suspend a user master definition for a valid Distribution A+ user. A user master definition must be set up for new and existing users that will have access to certain menu functions and additional security features.

Security settings can be entered for a user manually by accessing and completing all the screens in this option, or automatically, by simply copying the user security from an existing user to the new user you are adding. If you are adding a user manually and not copying security from another existing user, you must also remember to define this user as a registered Distribution A+ user. If you are adding a user and copying user security from an existing user, the system will completely copy all of the user security and will also check if a registration record exists. If one exists, that registration record will remain the same and not be updated. If one does not exist, the system will automatically create an initial user registration structure by copying most of the information from the existing user.

Since some information pertaining to the registration needs to be unique to the new user, certain data, such as the email address, copy to email (Workflow), and MOE User Number, will not be included in the copy. You can easily update or modify this information, as needed. This Copy User functionality will help eliminate repetitive steps of registering and entering user security among several options.

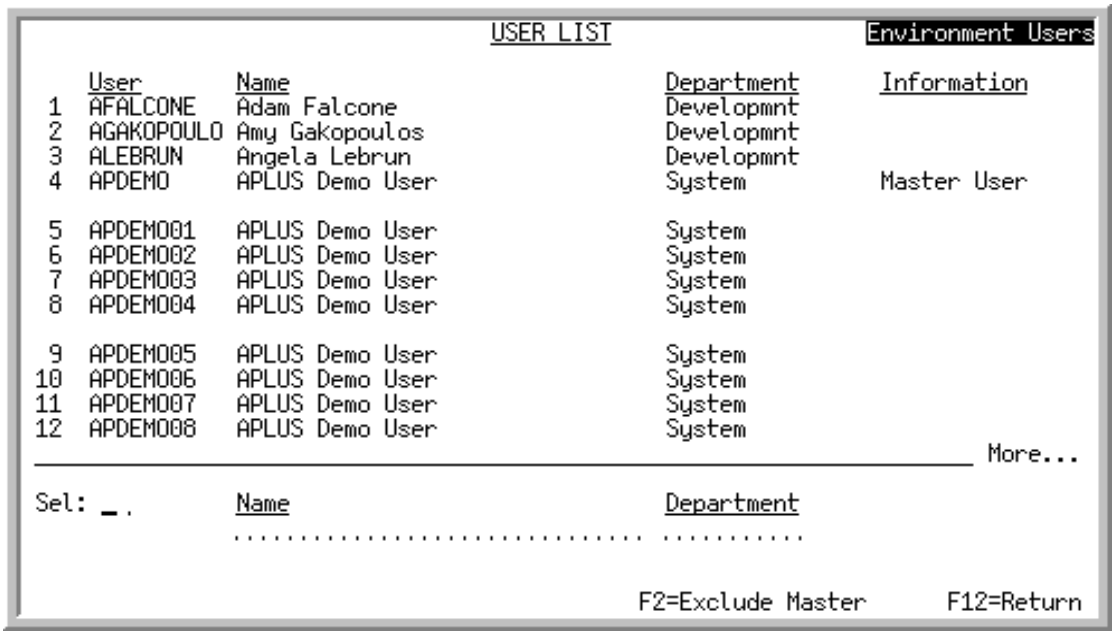
User Master Maintenance Screen Fields and Function keys

Field/Function Key	Description
Function	Use this field to add, change, delete, reinstate or suspend a user master definition for a valid Distribution A+ user. Key **A** to create a user master definition in the current environment for the user ID you key in the **User** field. Key **C** to change a user master definition in the current environment for the user ID you key in the **User** field. Key **D** to delete a user from the Distribution A+ user master definition. You will be prompted to confirm deletion when you key this option. Key **R** to reinstate a user master definition that has been suspended. You will be prompted to confirm action when you key this option. Key **S** to suspend a user master definition. The indicated user will be denied access to the system. You will be prompted to confirm action when you key this option. (A 1) Required
User	Use this field to identify the IBM i user profile for whom security options are being added, changed, deleted, reinstated, or suspended. Key the user's ID. **Note:** A valid user profile must be defined on the IBM i for the User ID you key in this field, and, with exception during the initial add function, the User ID must also be defined as a registered user through Register A+ User IDs (MENU XACFIG). **Valid Values:** A valid user profile defined on the IBM i. (A 10) Required

Field/Function Key	Description
Copy User	This field applies only if you are adding a new Distribution A+ user with a valid IBM i user profile. That is, the **Function** field contains an **A**, and the **User** field contains the ID of the new user you are adding. Use this field to enter a registered Distribution A+ user ID for which user security/authority records of this existing user will be copied to the new user you are adding (in the **User** field). Key the existing user's ID. **Note:** When adding a new user and copying user security/authority records from an existing user, the appropriate security and/or registration files are updated immediately and the remainder of the screens in this option are bypassed. You can still, however, access the screens on demand to maintain the data (modify user security), if needed. **Valid Values:** A valid user profile defined on the IBM i, and registered through Register A+ User IDs (MENU XACFIG). (A 10) Required
F3=Exit	Press **`F3=EXIT`** to exit this menu option and return to MENU XASCTY.
F4=User List	Press **`F4=USER LIST`** to access the User List Screen, which displays existing registered Distribution A+ users.

Field/Function Key	Description
Enter	Press **ENTER** to confirm your selections and proceed to the User Master Definition Screen. If you are adding a new user and selected to copy user security/authority records from an existing user, when you press **ENTER** to confirm your selections, the appropriate security and/or registration files are immediately updated. The screen will then redisplay with the 'Last Function' detail of the new user copied from the existing user (for example, **Add** JohnS; **Copied** SarahP), and an added detail line of what files were updated will be shown (for example, ****Security Options & Registration Copied**** or ****Security Options Copied****). If the new user was not previously registered and registration files were copied to the new user from the copy user, an initial user registration structure was provided. However, since some information pertaining to the registration needs to be unique to the new user, certain data, such as the email address, copy to email (Workflow), and MOE User Number, was not included in the copy. You can easily update or modify this information, as needed. If registration for the new user already existed (since it was previously entered), then it remained the same and was not modified when **ENTER** was pressed. As for the user security options that were copied when **ENTER** was pressed, they were completely copied from the copy user to the new user.

User List Screen



This screen displays users (users in the Distribution A+ User File in the current base) and environment users (users in the User Master File in the current environment, previously defined through this menu option). The top portion of the screen includes the user ID, name of the user, department the user resides in, and information about the user (whether that user is a "Master" user or suspended). The lower portion of the screen provides filters allowing you to display only users that match the user name criteria you enter.

You can select a user by entering the user's selection number in the **Sel** field, or you can limit the screen to show users that match the criteria you key in the Name and/or Department fields. You can also use the **F2=ENVIRONMENT USERS / F2=ALL USERS** key to display all users or environment users only.

Note: Depending on where you access this screen from, **F2=EXCLUDE MASTER** may display and will then allow you to toggle between including or excluding "Master" users.

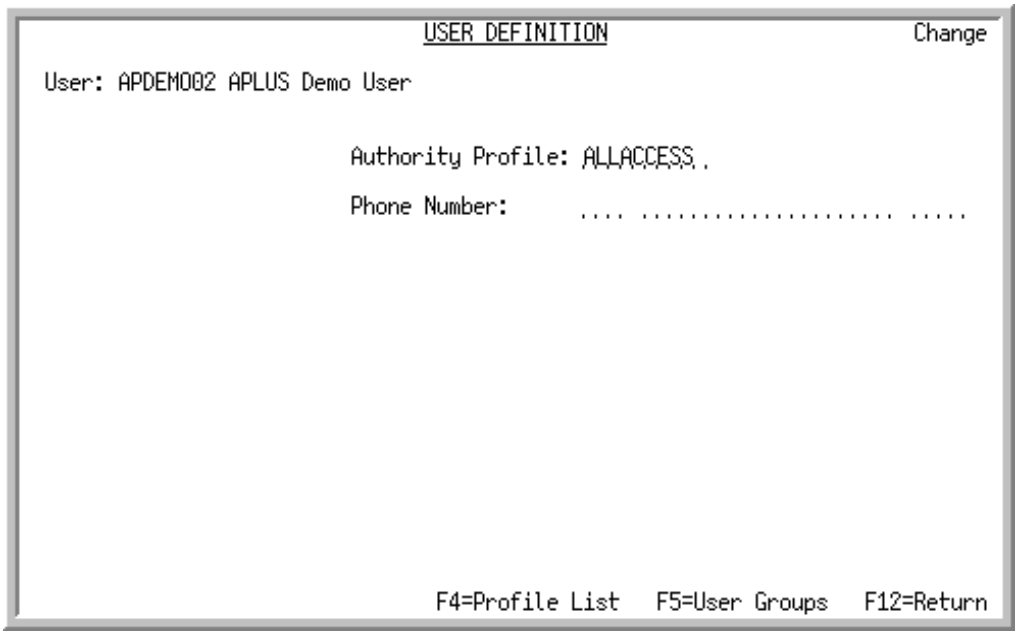
User List Screen Fields and Function keys

Field/Function Key	Description
(Reference Number)	Use the number in this field to select a user ID to change or delete. Display
User	The IBM i User ID of the user to be changed or deleted. Display
Name	The name of the user ID as recorded for the IBM i User Profile. Display

Field/Function Key	Description
Department	The optional department name in which this user works as identified in Register A+ User IDs (MENU XACFIG). This name is not validated and is for informational purposes only to help distinguish this user. Display
Information	This field displays special information about the user. If a user is suspended, this column will show **Suspended User**. The column will show as **Master User** when: • the user is a Transaction Processor Job • Distribution A+ Security is not active • the user is the Distribution A+ Master User from System Options (MENU XAFILE) • the user is the Authorized User ID from Company Name Maintenance (MENU XAFILE) Display
Sel	Use this field to select an existing user. Key the corresponding selection number of the user you want to select and press ENTER to proceed to the next screen. (N2,0) Optional
Name	Use this field to limit the screen to only those users whose names match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display users, if any, matching the name criteria you entered. **Note:** This is a character string search and will display users that match the data anywhere in the **Name** field. (A 30) Optional
Department	Use this field to limit the screen to only those users whose departments match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display users, if any, that reside in the department you entered. **Note:** This is a character string search and will display departments that match the data anywhere in the **Department** field. (A 10) Optional

Field/Function Key	Description
F2=Environment Users/Exclude Master	Use this **F2=ENVIRONMENT USERS / F2=ALL USERS** toggle key to include or exclude environment users on this screen. Environment users are those users set up with user master definitions through this menu option and reside in the User Security Master File. All users are Distribution A+ users that reside in the Distribution A+ User File. Depending on where you access this screen from, **F2=EXCLUDE MASTER** may display. The **F2=EXCLUDE MASTER/ F2=INCLUDE MASTER** toggle will allow you to include or exclude Master users on this screen.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	Press **ENTER** to confirm your selection and proceed to the next screen. If you keyed criteria in the **Name** and/or **Department** field, the screen refreshes and displays the users that match the criteria entered.

User Master Definition Screen



Use this screen to set up and maintain a user authority profile for the indicated user. User authority profiles are used to define a user's general access authorities. You would create profiles for users to organize a user's default company, default warehouse, authorized company/warehouse/salesrep, and so on. The user's ID you keyed on the User Master Maintenance Screen displays in the **User** field. The user's name, extracted by the system from the IBM i User Profile, displays below the user's ID.

You have the option to set up a personal authority profile (the **User** field and **Authority Profile** field are the same and the profile cannot be shared with other users) or a public authority profile (the **User** field and **Authority Profile** field are different and the profile can be shared by multiple users, providing the ability to group users into categories). You would set up a public authority profile when you want to define multiple users with the same authority profile. For example, you could create an authority profile CO01WH3, indicating users with this profile will only have access to Company 01 and Warehouse 3.

From this screen, you can also access the Authority Profile List Screen and User Group List Screen.

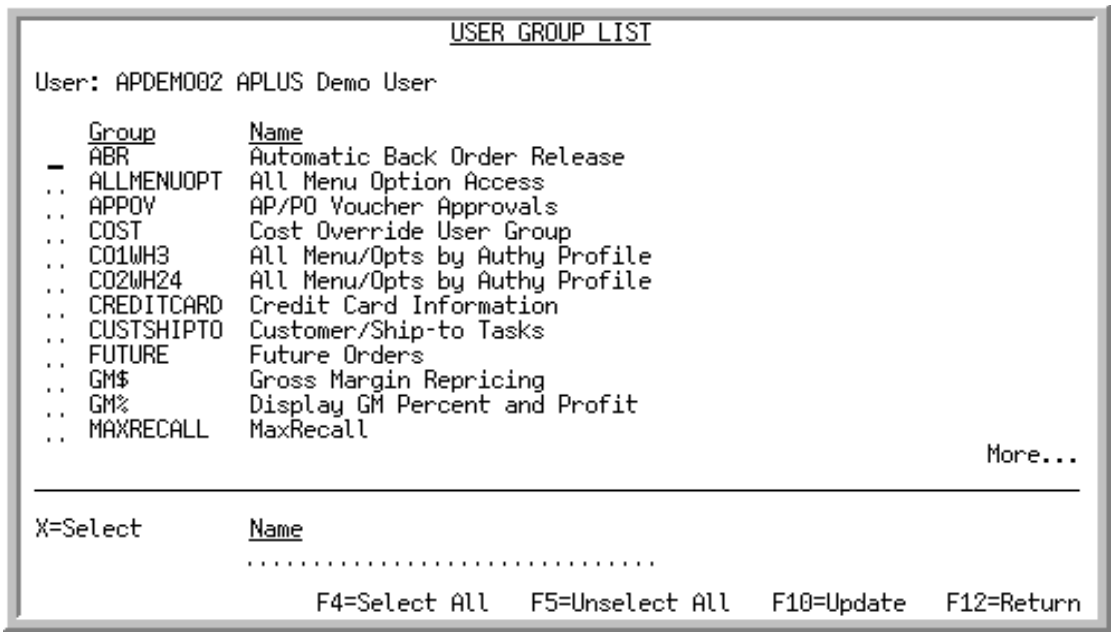
Note: A Master user can access all menu options. For those users that are not master users, you can determine through this menu option what the user's authority level will be.

User Master Definition Screen Fields and Function keys

Field/Function Key	Description
Authority Profile	Use this field to select a personal (not shared with other users) or public (shared with other users) user authority profile for the indicated user. To set up a personal (non-generic private) profile that cannot be shared with other users, key the same user ID that exists in the User field on this screen. When both the User field and this field are the same, you are creating a personal authority profile. To set up a public (generic) profile that can be shared with other users, key an existing authority profile that is different than the ID that exists in the **User** field on this screen. When the **User** field and this field are different, you are assigning a public authority profile to this user. If you key an authority profile that does not already exist and that is different than the user ID being added, a message displays informing you that the authority profile does not exist and press F6 to add the profile. F6 provides access to the Authority Profile Maintenance option (MENU XASCTY). (A 10) Required
Phone Number	Use this field to enter the user's contact information. Key the user's telephone number, which includes a 3-character country access code followed by the area code and telephone number, and telephone extension. **Valid Values:** Numerals and the symbols: - ( ) . / Blank spaces are allowed between numerals only if **Allow Blank Phone Delimiters** is **Y** in System Options Maintenance (MENU XAFILE). (N3,0/N20,0/N4,0-O) Optional
F4=Profile List	Press **F4=PROFILE LIST** to access the Authority Profile List Screen, which displays existing group (public) profiles. Personal profiles will not be shown on the Authority Profile List Screen.
F5=User Groups	Press **F5=USER GROUPS** to access the User List Screen, which displays existing user group information. From the User List Screen, you can assign the indicated user to an available user group.

Field/Function Key	Description
F6=Add Profile	This function key is non-display. When adding a new user with a public authority profile and the user and authority profile are different, after pressing **ENTER**, a message displays: **This Authority Profile does not exist. Press F6 to add profile.** Press **F6=ADD PROFILE** to launch into Authority Profile Maintenance (MENU XASCTY), the Authority Profile Definition Screen will display.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	Press **ENTER** to confirm your selections. When adding a new user with a personal authority profile (user and authority profile are the same ID) or when maintaining a user with an existing personal authority profile, after you press **ENTER**, the Authority Profile Definition Screen will display. When maintaining a user with an existing public authority profile, after you press **ENTER**, you are returned to the User Master Definition Screen. The Authority Profile Definition Screen is bypassed. You must access Authority Profile Maintenance (MENU XASCTY) to maintain public profiles.

User Group List Screen



This screen displays existing user groups. The top portion of this screen displays the user group and the name of the user group. The lower portion of this screen allows you to limit the screen to show only user groups that match the criteria you key in the **Name** field.

Use this screen to assign the current user to a user group or multiple groups by keying **X** next to the groups to which this user will be assigned.

User Group List Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to assign the current user to the indicated user group(s). On the top portion of the screen, key **X** in the column corresponding to the user groups you want to select and press **F10=UPDATE**. A message will display informing you that the indicated user will be assigned to the user groups you selected. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To deselect any user groups to which you assigned the current user, simply blank out the X next to the group you no longer want the user assigned to. (A 1) Optional

Field/Function Key	Description
Name	Use this field to limit the screen to only those user groups that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display user groups, if any, matching your criteria. **Note:** This is a character string search and will display user group names that match the data anywhere in the **Name** field. (A 30) Optional
F4=Select All	Press **F4=SELECT ALL** to select to assign the current user to all user groups. An will appear in the left column before all Group IDs. If you want the user assigned to most groups but want to exclude one or a few, simply blank out the **X** in the column before the Group ID(s) you do not want to include. To Unselect all user groups, see **F5=UNSELECT ALL**. **Note:** The Select All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your list of user group names. You would filter to the word 'credit' and press **F4=SELECT ALL** to Select All. When then pressing **F10=UPDATE**, the confirmation list will show the user groups selected based on the credit filter. If you want to ensure that you have selected ALL user groups, verify that there is no data filter active in the **Name** field.
F5=UnSelect All	Press **F5=UNSELECT ALL** to unselect all groups to which you assigned the current user. All X's will disappear in the left column before all Group IDs. If you want to include only a few groups to which the current user will be assigned, simply key **X** in the column before the Group ID(s) you want to assign the user to. To select all user groups to which the user will be assigned, see **F4=SELECT ALL**. **Note:** The Unselect All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your list of user group names. You would filter to the word 'credit' and press **F5=UNSELECT ALL** to Unselect All. When then pressing **F10=UPDATE**, your confirmation list will show the user groups remaining based on the credit filter. If you want to ensure that you have Unselected ALL user groups, verify that there is no data filter active in the **Name** field.

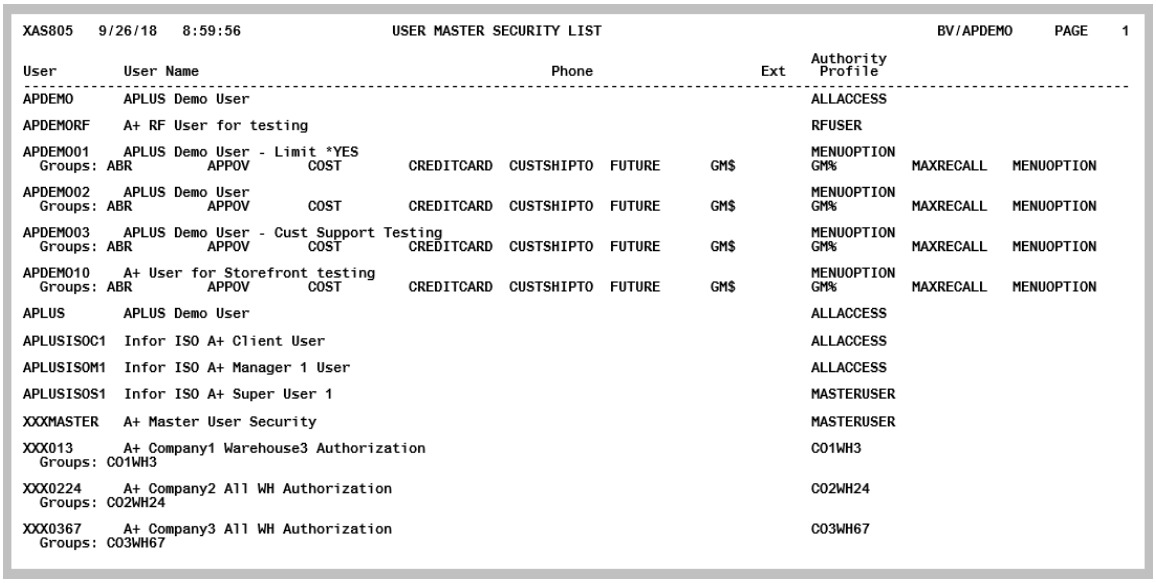
Field/Function Key	Description
F10=Update	After you have selected the groups to which you want this user assigned, press **F10=UPDATE** to confirm your selections. Once **F10=UPDATE** is pressed, only the user groups you selected are shown on the screen and a message displays informing you that the user will be assigned to the indicated user groups. You will have the option to confirm your selections by pressing Enter or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	After keying filter criteria in the **Name** field, press **ENTER**. The screen will refresh and display user groups, if any, matching your criteria.

User Listing

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
User Master Security List	Used to print users that will have access to Distribution A+ menu functions, and their authority profile.

User Master Security List



```
XAS805   9/26/18   8:59:56                USER MASTER SECURITY LIST                                    BV/APDEMO     PAGE    1

User        User Name                                          Phone                  Ext    Authority Profile
-------------------------------------------------------------------------------------------------------------------------------
APDEMO      APLUS Demo User                                                                  ALLACCESS

APDEMORF    A+ RF User for testing                                                           RFUSER

APDEMO01    APLUS Demo User - Limit *YES                                                     MENUOPTION
  Groups: ABR          APPOV       COST        CREDITCARD  CUSTSHIPTO  FUTURE      GM$     GM%          MAXRECALL    MENUOPTION

APDEMO02    APLUS Demo User                                                                  MENUOPTION
  Groups: ABR          APPOV       COST        CREDITCARD  CUSTSHIPTO  FUTURE      GM$     GM%          MAXRECALL    MENUOPTION

APDEMO03    APLUS Demo User - Cust Support Testing                                           MENUOPTION
  Groups: ABR          APPOV       COST        CREDITCARD  CUSTSHIPTO  FUTURE      GM$     GM%          MAXRECALL    MENUOPTION

APDEMO10    A+ User for Storefront testing                                                   MENUOPTION
  Groups: ABR          APPOV       COST        CREDITCARD  CUSTSHIPTO  FUTURE      GM$     GM%          MAXRECALL    MENUOPTION

APLUS       APLUS Demo User                                                                  ALLACCESS

APLUSISOC1  Infor ISO A+ Client User                                                         ALLACCESS

APLUSISOM1  Infor ISO A+ Manager 1 User                                                      ALLACCESS

APLUSISOS1  Infor ISO A+ Super User 1                                                        MASTERUSER

XXXMASTER   A+ Master User Security                                                          MASTERUSER

XXX013      A+ Company1 Warehouse3 Authorization                                             CO1WH3
  Groups: CO1WH3

XXX0224     A+ Company2 All WH Authorization                                                 CO2WH24
  Groups: CO2WH24

XXX0367     A+ Company3 All WH Authorization                                                 CO3WH67
  Groups: CO3WH67
```

This listing prints after selecting option **11** - User Listing on the A+ Security Menu (MENU XASCTY). This listing prints users that will have access to Distribution A+ menu functions, and their authority profile (**Private**, indicating that their profile is not shared with other users, or **Public**, indicating that their profile is shared with other users).

Use this listing to view the users that have been added to Distribution A+.

Chapter 4 User Group Maintenance/Listing

Maintaining User Groups is performed through the Distribution A+ Security Menu (MENU XASCTY). User Group Maintenance allows you to define user groups and to assign users to these groups.

User groups are a security feature that allow you to assign certain authorities to groups of users simplifying the effort required to define application authorities. By giving an authority to a user group you in effect provide that authority to all users that are defined within that group.

Some of the uses of a user group include:

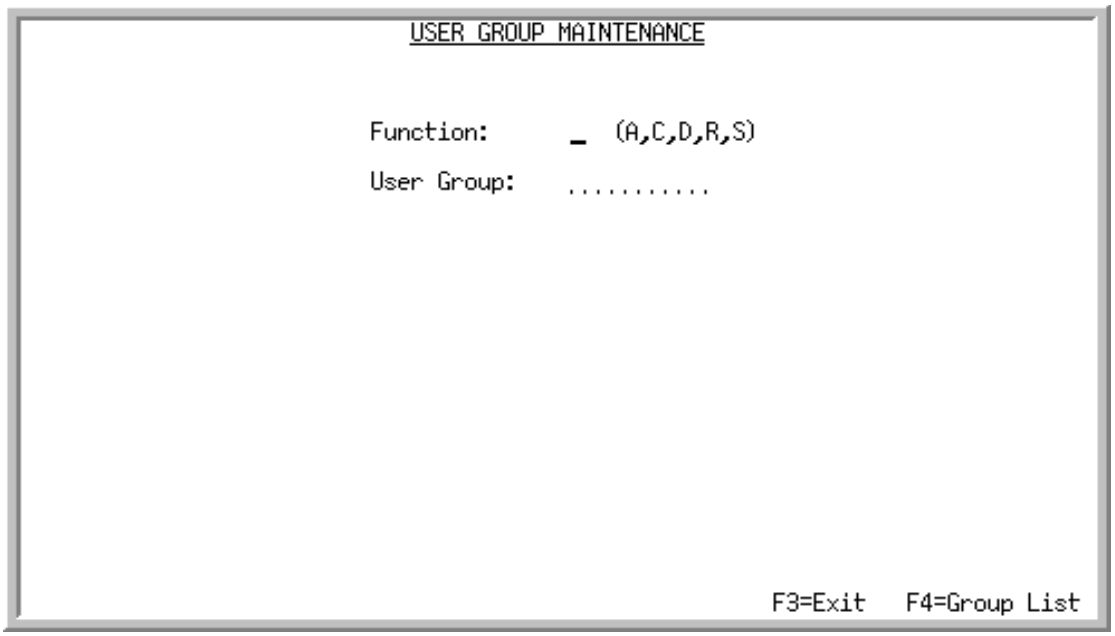
- Authorizing access to menu functions
- Providing authority to GL accounts
- Authorizing use of secured features, such as releasing orders
- Authority to view and/or change secured values, such as cost and profit

User Group Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
User Group Maintenance Screen	Used to add, change, delete, reinstate, and suspend User Groups.
User Group List Screen	Used to review and select existing user groups to maintain.
User Group Definition Screen	Used to enter a description for the user group you are creating, or to change a description for an existing user group.
Assign Users Screen	Used to select the users you want to include in the indicated user group (if this screen is accessed from this menu option) or assign to the indicated action (if this screen is access from Application Action Authority Maintenance).

User Group Maintenance Screen



Use this screen to add, change, delete, reinstate, and suspend User Groups. A User Group consists of one or more users who are authorized to access functions in Distribution A+ that normally only have one authorized user. This is useful if you want to limit access to functions to a group of users with a common level of authority, such as managers. This also provides you with the ability to create user groups for specific menu/option functions and easily give multiple users access to exactly the same functions.

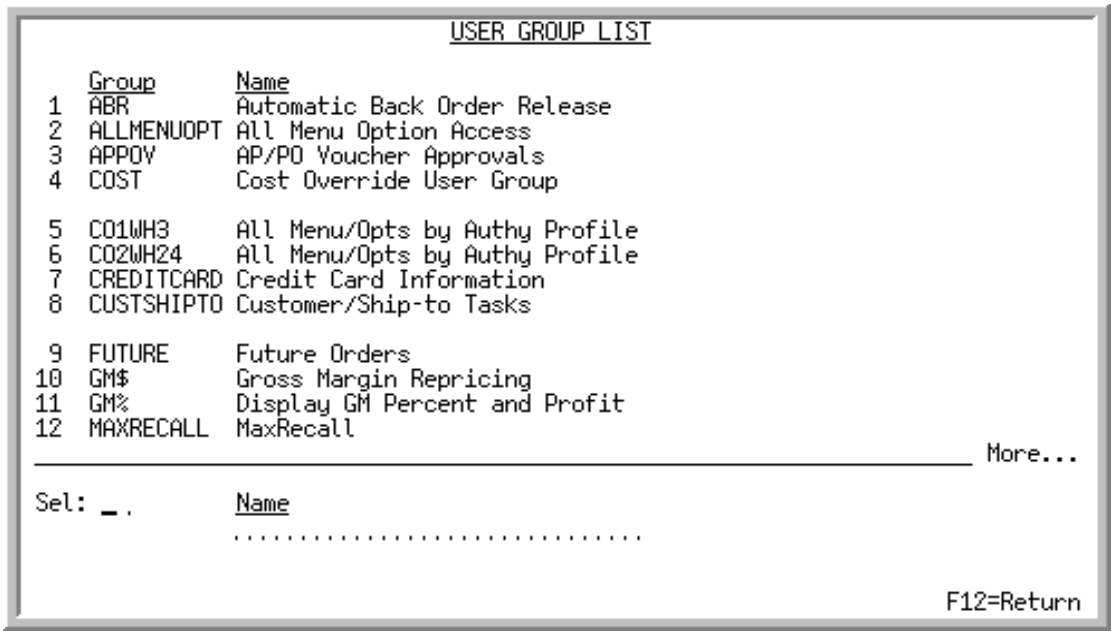
Once a group has been created, you can add or delete users from that group.

Important: A single User Group may be added to a list of authorized users (as the first in the list) who are allowed to perform order entry functions of entering returns or removing a single hold code. For each hold code, you should create a separate User Group and establish a separate list of authorized users with that User Group as the first authorized user. Authorized User IDs are defined through MENU OEMAST.

User Group Maintenance Screen Fields and Function keys

Field/Function Key	Description
Function	Use this field to add, change, delete, reinstate or suspend a user group. Key **A** to create a user group. Once you have created a user group, you can then add/remove users to/from that group Key **C** to change a user group. The description of the user group may be changed as well as user assignments in that group. Key **D** to delete a user group. You cannot delete a user group if users exist in that group. You will be prompted to confirm deletion when you key this option. Key **R** to reinstate a user group that has been suspended. You will be prompted to confirm action when you key this option. Key **S** to suspend a user group. Users in that group will be denied access to any system function the group is assigned to. You will be prompted to confirm action when you key this option. (A 1) Required
User Group	Use this field to identify the user group you are adding, changing, deleting, reinstating or suspending. This is the user group to which users will be added or deleted. Key up to 10 characters for the description of this group. (A 10) Required
F3=Exit	Press **F3=EXIT** to exit this menu option and return to MENU XASCTY.
F4=Group List	Press **F4=GROUP LIST** to access the User Group List Screen, which displays existing user groups.
Enter	Press **ENTER** to confirm your selections and proceed to the User Group Definition Screen.

User Group List Screen



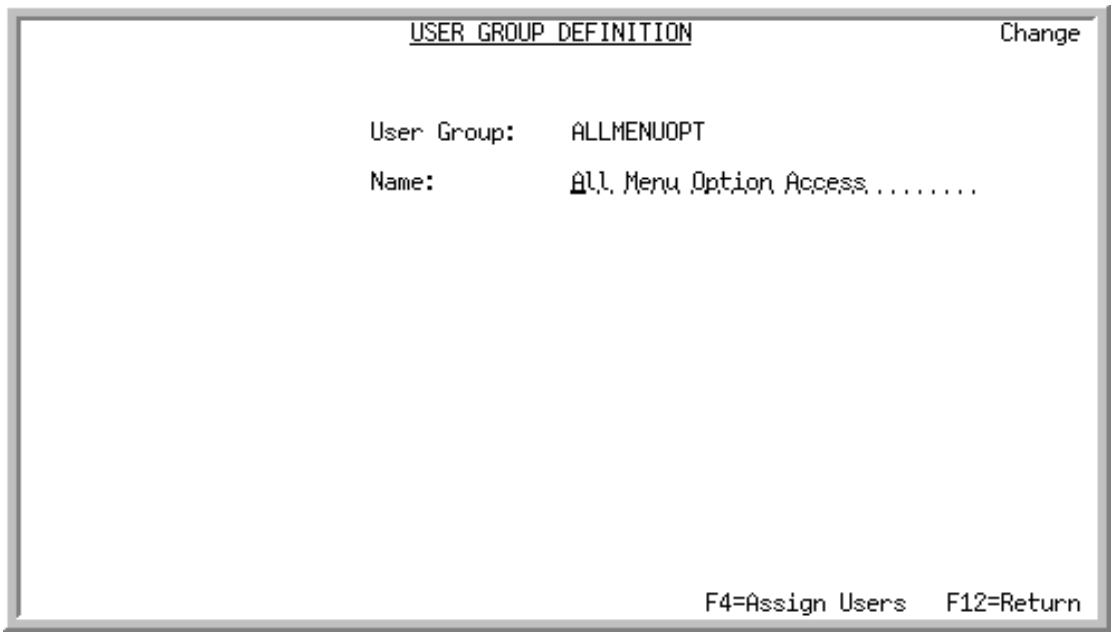
This screen displays existing user groups. The top portion of this screen displays the user group and the name of the user group. On the lower portion of this screen, you can select a user group to maintain by entering the group's selection number in the **Sel** field. You can also limit the screen to show only user groups that match the criteria you key in the **Name** field.

User Group List Screen Fields and Function keys

Field/Function Key	Description
Sel	Use this field to select an existing user group to maintain. Key the corresponding selection number of the group you want to maintain and press **ENTER**. (N2,0) Optional
Name	Use this field to limit the screen to only those user groups that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display user groups, if any, matching your criteria. **Note:** This is a character string search and will display users that match the data anywhere in the **Name** field. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without confirming your entries.

Field/Function Key	Description
Enter	Press **ENTER** to confirm your selection and proceed to the next screen. If you keyed criteria in the **Name** field, the screen refreshes and displays the user groups that match the criteria entered.

User Group Definition Screen

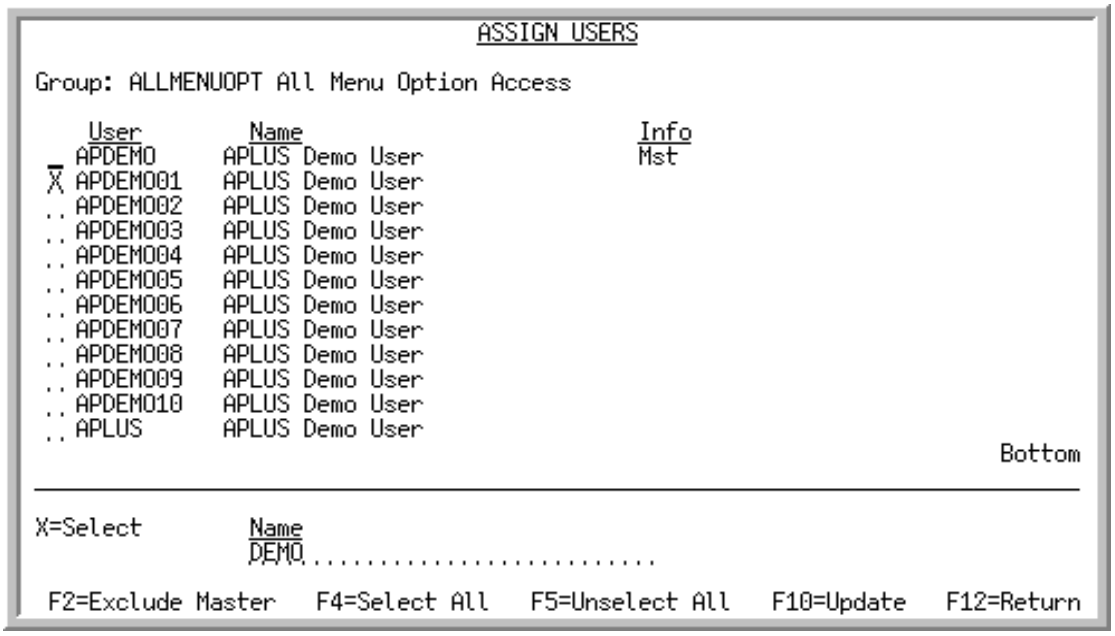


Use this screen to enter a description for the user group you are creating, or to change a description for an existing user group. This screen also provides access to the Assign Users Screen, where you can add/remove users to/from the user group.

User Group Definition Screen Fields and Function keys

Field/Function Key	Description
Name	Use this field to enter a description for the user group. (A 30) Required
F4=Assign Users	Press **F4=ASSIGN USERS** to access the Assign Users Screen, where you select which users will be in the indicated user group.
F12=Return	Press **F12=RETURN** to return to the User Group Maintenance Screen without saving your entry.
Enter	Press **ENTER** to confirm your entry and return to the User Group Maintenance Screen.

Assign Users Screen



This screen displays all valid users in the User Master File defined in the system. The top portion of the screen includes the user ID, name of the user, and information about the user (whether that user is a "Master" user or suspended). The lower portion of the screen provides a filter allowing you to display only users that match the criteria you enter.

This screen can be accessed from this menu option or Application Action Authority Maintenance (MENU XASCTY). If accessed from this menu option, the **Group** is identified on the top portion of this screen. If accessed from Application Action Authority Maintenance, the **Company** and **Action** are identified on the top portion of this screen.

Use this screen to select the users you want to include in the indicated user group [if this screen is accessed from this menu option] or assign to the indicated action [if this screen is access from Application Action Authority Maintenance (MENU XASCTY)].

You can also deselect users previously assigned to the group or action and exclude "Master" users from the selection.

Assign Users Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to assign users to the indicated user group or action, depending on where this screen is being accessed from. On the top portion of the screen, key **X** in the column corresponding to the user(s) you want to select and press **F10=UPDATE**. A message will display informing you that the indicated users will be assigned to the group or action. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To deselect any user(s) previously included in the user group or assigned to the action, simply blank out the **X** next to the user you no longer want included. (A 1) Optional
Name	Use this field to limit the screen to only those users that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display users, if any, matching your criteria. **Note:** This is a character string search and will display users that match the data anywhere in the **Name** field. (A 30) Optional
F2=Exclude Master/ Include Master	Use this **F2=EXCLUDE MASTER / F2=INCLUDE MASTER** toggle key to include or exclude "Master" users on this screen. Press **F2=EXCLUDE MASTER / F2=INCLUDE MASTER** to exclude users defined as "Master" users (based on the authority profile) from displaying on this screen. Press **F2=EXCLUDE MASTER / F2=INCLUDE MASTER** again to include "Master" users on this screen.

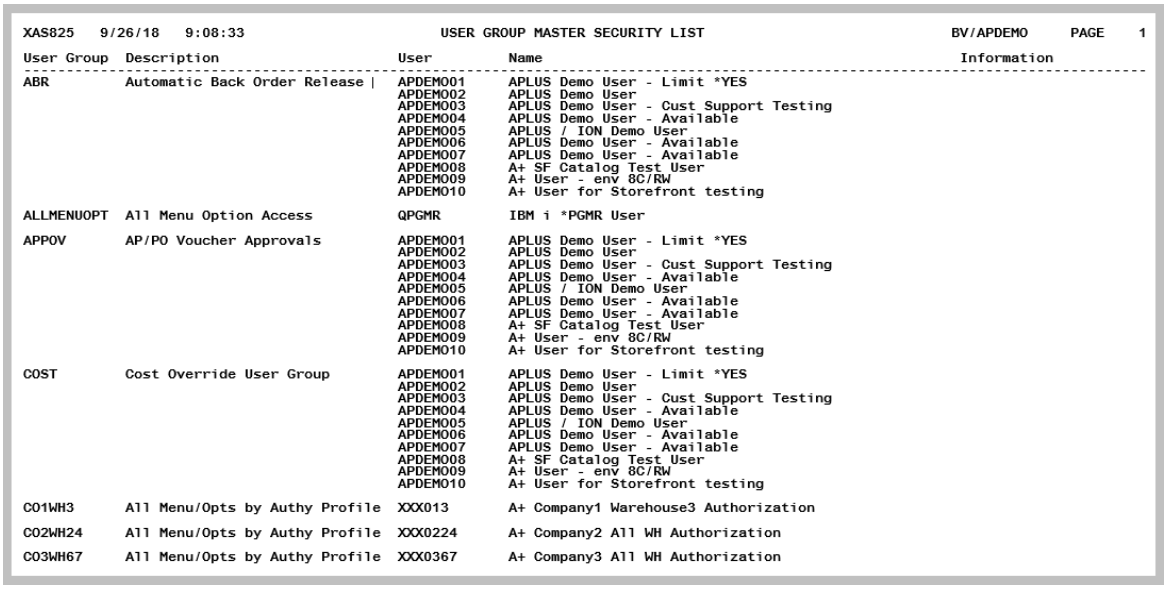
Field/Function Key	Description
F4=Select All	Press **F4=SELECT ALL** to select all users to be included in the indicated user group or assigned to the action. An **X** will appear in the left column before all users. If you want most users included in the group or assigned to the action and want to exclude only one or a few, simply blank out the **X** in the column before the users you do not want to include and press **F10=UPDATE** to Update. **Note:** The Select All option is based on the data filter information in the **Name** field. For example, assume you have multiple users named Joe in your list of user names. You would filter to the word 'Joe' and press **F4=SELECT ALL** to Select All. When you then press **F10=UPDATE**, your confirmation list will show the users you selected based on the Joe filter. If you want to ensure that you have selected ALL users, verify that there is no data filter active in the **Name** field.
F5=Unselect All	Press **F5=UNSELECT ALL** to unselect all users from being included in the indicated user group or assigned to the action. All **X**'s will disappear in the left column before all user IDs. If you want to include only a few users in the group or assigned to the action, simply key **X** in the column before the user IDs you want to include and press **F10=UPDATE** to update. **Note:** The Unselect All option is based on the data filter information in the **Name** field. For example, assume you have multiple users named Joe in your list of user names. You would filter to the word 'Joe' and press **F5=UNSELECT ALL** to Unselect All. When you then press **F10=UPDATE**, your confirmation list will show the users remaining based on the Joe filter. If you want to ensure that you have unselected ALL users, verify that there is no data filter active in the **Name** field.
F10=Update	After you have selected the users you want included in the user group or want assigned to the action, press **F10=UPDATE** to confirm your selections. Once **F10=UPDATE** is pressed, the users you selected are shown on the screen and a message displays informing you that the indicated users will be assigned to the group or action. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	After entering criteria in the **Name** field, press **ENTER** to refresh the screen and display users that match the criteria you entered.

User Group Listing

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
User Group Master Security List	Used to print User Groups created through User Group Maintenance and the users assigned to the group.

User Group Master Security List



XAS825 9/26/18 9:08:33 USER GROUP MASTER SECURITY LIST BV/APDEMO PAGE 1

User Group	Description	User	Name	Information
ABR	Automatic Back Order Release |	APDEMO01	APLUS Demo User - Limit *YES	
		APDEMO02	APLUS Demo User	
		APDEMO03	APLUS Demo User - Cust Support Testing	
		APDEMO04	APLUS Demo User - Available	
		APDEMO05	APLUS / ION Demo User	
		APDEMO06	APLUS Demo User - Available	
		APDEMO07	APLUS Demo User - Available	
		APDEMO08	A+ SF Catalog Test User	
		APDEMO09	A+ User - env 8C/RW	
		APDEMO10	A+ User for Storefront testing	
ALLMENUOPT	All Menu Option Access	QPGMR	IBM i *PGMR User	
APPOV	AP/PO Voucher Approvals	APDEMO01	APLUS Demo User - Limit *YES	
		APDEMO02	APLUS Demo User	
		APDEMO03	APLUS Demo User - Cust Support Testing	
		APDEMO04	APLUS Demo User - Available	
		APDEMO05	APLUS / ION Demo User	
		APDEMO06	APLUS Demo User - Available	
		APDEMO07	APLUS Demo User - Available	
		APDEMO08	A+ SF Catalog Test User	
		APDEMO09	A+ User - env 8C/RW	
		APDEMO10	A+ User for Storefront testing	
COST	Cost Override User Group	APDEMO01	APLUS Demo User - Limit *YES	
		APDEMO02	APLUS Demo User	
		APDEMO03	APLUS Demo User - Cust Support Testing	
		APDEMO04	APLUS Demo User - Available	
		APDEMO05	APLUS / ION Demo User	
		APDEMO06	APLUS Demo User - Available	
		APDEMO07	APLUS Demo User - Available	
		APDEMO08	A+ SF Catalog Test User	
		APDEMO09	A+ User - env 8C/RW	
		APDEMO10	A+ User for Storefront testing	
CO1WH3	All Menu/Opts by Authy Profile	XXX013	A+ Company1 Warehouse3 Authorization	
CO2WH24	All Menu/Opts by Authy Profile	XXX0224	A+ Company2 All WH Authorization	
CO3WH67	All Menu/Opts by Authy Profile	XXX0367	A+ Company3 All WH Authorization	

Use this listing to show the User Groups created through User Group Maintenance (MENU XASCTY) and the users assigned to the group. It also indicates if the user in the group is a Master user.

Chapter 5 Authority Profile Maintenance/ Listing

Maintaining Authority Profiles is performed through the Distribution A+ Security Menu (MENU XASCTY). Authority Profile Maintenance allows you to define "Public" authority profiles. Authority profiles are used to define general authority access parameters that determine a user's authority levels. By defining "Public" profiles you can establish these parameters and assign this profile to the users that you want to have the same authority without having to duplicate it multiple times.

Through Authority Profiles you assign the following authorities:

- Master User Authority
- GL and Account Number Authority
- Company, Warehouse, and Salesrep Authority
- Default Company and Warehouse

The company, warehouse, and salesrep authority assigned here will be utilized when those levels of security are activated through Systems Options (MENU XAFILE) selections to **Activate Company Security**, **Activate Warehouse Security**, **Activate Salesrep Security** are set to **Y**.

Authority Profile Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Authority Profile Maintenance Screen	Used to add, change, delete, reinstate or suspend an authority profile.
Authority Profile List Screen	Use to select an authority profile for maintenance.
Authority Profile Definition Screen	Used to define general authority security options for user(s) in the current authority profile.

Title	Purpose
Select Authorized Companies Screen	Used to select the companies that the users in this authority profile will be authorized to use when performing Distribution A+ functions.
Select Authorized Warehouses Screen	Used to select the warehouse that the users in this authority profile will be authorized to use when performing Distribution A+ functions.
Select Authorized SalesReps Screen	Used to select the salesreps that the users in this authority profile will be authorized to use when performing Distribution A+ functions.

Authority Profile Maintenance Screen

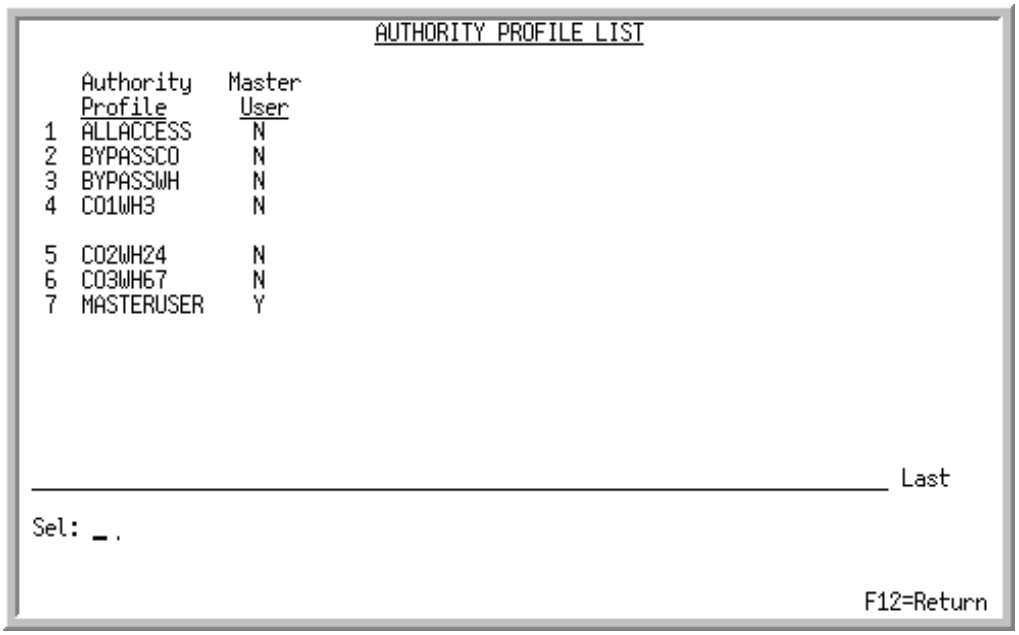
Use this screen to add, change, delete, reinstate or suspend a public authority profile. A public authority profile can be shared with other users, providing the ability to group users into categories. General security options are maintained within authority profiles including company and warehouse security authorities. You would set up a public authority profile when you want to define multiple users with the same authority profile, such as Managers. You can create a personal authority profile, which cannot be shared with other users, through User Maintenance (MENU XASCTY). Public authority profiles can also be initially created there as well but once established they must be maintained through this menu option.

You can also access the Authority Profile List Screen to view a list of existing group (public) authority profiles.

Authority Profile Maintenance Screen Fields and Function keys

Field/Function Key	Description
Function	Use this field to add, change, delete, reinstate or suspend a public authority profile. The public authority profile you add cannot be an existing IBM i User Profile Name. Key **A** to add a public authority profile. Key **C** to change an existing public authority profile. Key **D** to delete an existing public authority profile. You will be prompted to confirm deletion when you key this option. Key **R** to reinstate a public authority profile that has been suspended. You will be prompted to confirm action when you key this option. Key **S** to suspend a public authority profile. The public authority profile will be denied access to the system. You will be prompted to confirm action when you key this option. (A 1) Required
Authority Profile	Use this field to enter the public authority profile you are adding, changing, deleting, reinstating, or suspending. Key the authority profile which is or will be shared by multiple users with the same authority profile. The authority profile entered cannot be an IBM i User Profile name. An example of an authority profile you might enter is CO01WH3, indicating users with this authority profile will only have access to Company 01 and Warehouse 3. You would then assign that authority profile to users (through **User Maintenance**, MENU XASCTY), allowing you to determine the general access authorities for this group of users. (A 10) Required
F3=Exit	Press **F3=EXIT** to exit this menu option and return to MENU XASCTY.
F4=Profile List	Press **F4=PROFILE LIST** to access the Authority Profile List Screen, which displays existing public profiles. Personal profiles will not be shown on the Authority Profile List Screen.
Enter	Press **ENTER** to confirm your selections and access the Authority Profile Definition Screen.

Authority Profile List Screen



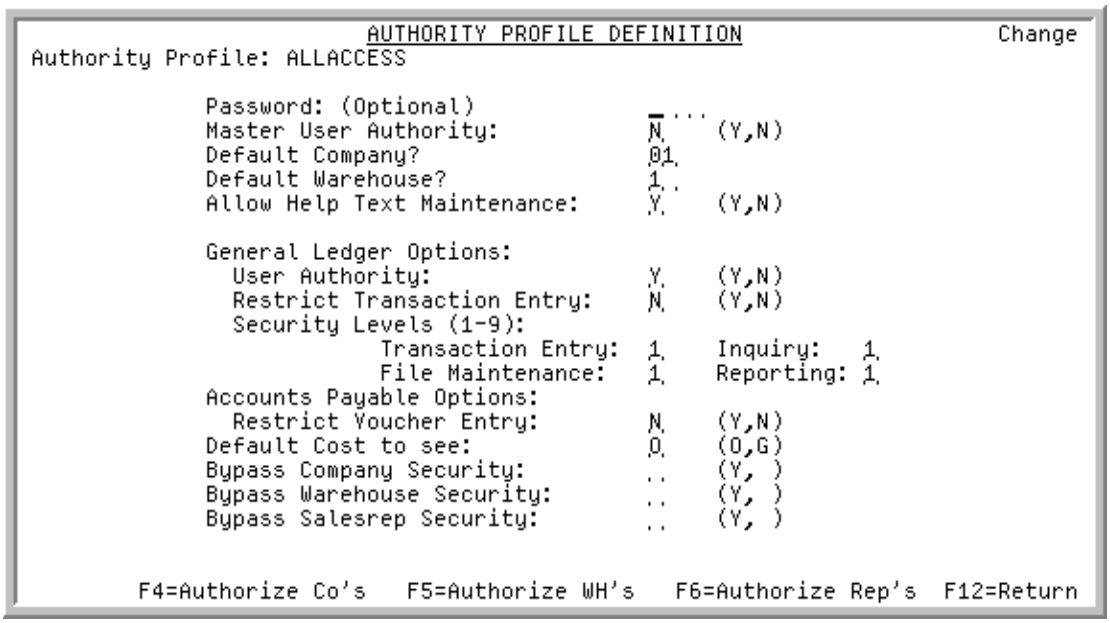
This screen displays a list of existing public authority profiles, and indicates whether or not the public authority profile has "Master" user authority. Personal profiles are not shown on this screen.

Use this screen to select a public authority profile to maintain.

Authority Profile List Screen Fields and Function keys

Field/Function Key	Description
Sel	Use this field to select an existing public authority profile you want to maintain. Key the corresponding selection number of the public profile you want to choose and press **Enter** to return to the previous screen. (N2,0) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without selecting a group profile.
Enter	Press **ENTER** to confirm your selections.

Authority Profile Definition Screen



This screen is used to define general authority security options for user(s) in the current authority profile. If you are adding a new user with a personal authority profile (user and authority profile are the same ID) or if you are maintaining a personal authority profile, values on this screen pertain to that user profile only. If you are adding a new user with a public authority profile (user and authority profile are different) or if you are maintaining a public authority profile, values on this screen pertain to all user(s) in that public authority profile.

To be able to use this screen, you must be a Master user or a user that has access to this function as defined through Application Authority Maintenance (MENU XASCTY).

This screen also allows you to select what companies, warehouses, and salesreps the user(s) in this profile are authorized to use via the **F4=AUTHORIZE CO'S, F5=AUTHORIZE WH'S, and F6=AUTHORIZE REP'S** function keys.

Note: This screen displays through User Maintenance (MENU XASCTY) or Authority Profile Maintenance (MENU XASCTY). When maintaining a user with an existing public authority profile, this screen is bypassed in User Maintenance. You must access this screen through this menu option to maintain public profiles.

Authority Profile List Screen Fields and Function keys

Field/Function Key	Description
Password	Key the password for this public authority profile. Prior to accessing Distribution A+ menu functions, users with this authority profile will be required to enter the password you select in this field. The user will be given three chances to key the correct password. If a fourth incorrect password is attempted, the user will be signed off the IBM i. The password you key in this field may be changed at any time. (A 4) Optional
Master User Authority	Use this field to specify whether this authority profile will have "Master" user authority. Key **Y** if you want users with this profile to have master user authority. In addition to by-passing all security checks, a master user has other privileges. For example, a master user can access all menus, all menu options, and general ledger accounts. A master user also has access to all functions for all companies, warehouses and salesreps. Key **N** if you do not want users with this profile to have master user authority. Users that are not master users do not by-pass security checks and will be permitted or denied access to various functions of Distribution A+ as designated. **Default Value:** N (A 1) Required

Field/Function Key	Description
Default Company	This field indicates the default company number that will appear on many screens throughout Distribution A+ for users with this authority profile. When a new user is set up with security, the default company will appear as the system default company and may be accepted or overridden. When the default company is being determined for prompt screens, it will first try to find a default company for the user requesting the job. If the user has not been set up with a default company, the prompt screen will then display the system default company defined in System Options Maintenance (MENU XAFILE). **Note:** If company security options are activated in System Options Maintenance (MENU XAFILE) and you key a default company that is not authorized, an error message appears informing you that the default company you entered must be authorized. Press **F4=AUTHORIZE CO'S** to authorize the company you want to enter as the default. **Default Value:** The default company defined in Authority Profile Maintenance (MENU XASCTY) if one has been defined; otherwise, this is the default company defined through System Options Maintenance (MENU XAFILE) **Valid Values:** A valid company number defined through Company Name Maintenance (MENU XAFILE) which you are authorized to access through Authority Profile Maintenance (MENU XASCTY). (N2,0) Required

Field/Function Key	Description
Default Warehouse	This field indicates the default warehouse number that will appear on many screens throughout Distribution A+ for users with this authority profile. When a new user is set up with security, the default warehouse will appear as the default warehouse for the system default company. When the default warehouse is being determined for prompt screens, the system will first try to find a default warehouse for the user requesting the job. If the user has not been set up with a default warehouse, the prompt screen will then display the default warehouse of the system default company as defined through System Options Maintenance (MENU XAFILE). **Note:** If warehouse security options are activated in System Options Maintenance (MENU XAFILE) and you key a default warehouse that is not authorized, an error message appears informing you that the default warehouse you entered must be authorized. Press **F5=AUTHORIZE WH'S** to authorize the warehouse you want to enter as the default. **Default Value:** The default warehouse defined in Authority Profile Maintenance (MENU XASCTY) if one has been defined; otherwise, this is the **Default Warehouse** defined through Company Name Maintenance (MENU XAFILE). **Valid Values:** A valid warehouse number defined through Warehouse Numbers Maintenance (MENU IAFILE) which you are authorized to access through Authority Profile Maintenance (MENU XASCTY) (A 2) Required
Allow Help Text Maintenance	This field indicates if users with this authority profile will be allowed to create and maintain help text from the help text window. Key **Y** to allow user(s) to maintain help text from the help text window. Key **N** to not allow user(s) to access help text maintenance. **Default Value:** N **Valid Values:** Y or N; must be Y if this authority profile is defined as a master user (i.e., **Master User Authority** field on this screen is **Y**). (A 1) Required

Field/Function Key	Description
GL: User Authority	This field is used to identify the authority profile as a valid profile of Distribution A+ General Ledger. Key **Y** if this authority profile is authorized to use the General Ledger application. Key **N** if this authority profile is not authorized to use the General Ledger Application. **Note:** If user security is activated through G/L Options Maintenance (MENU GLFIL2), only profiles with a **Y** in this field will be able to access a G/L program from any menu. **Default Value:** N **Valid Values:** Y or N; must be Y if master user (A 1) Required
GL: Restrict Transaction Entry	This field is used to restrict G/L transaction entry for users with this authority profile. Restricted transaction entry allows a user to enter transactions through Transaction Entry (MENU GLMAIN), but the account's description will not be displayed, the search will not be available, and the account description will not appear on the Transaction Edit List. Key **Y** in this field to only allow a restricted version of GL transaction entry. Key **N** in this field if users with this authority profile will not have a restricted version of GL transaction entry. **Default Value:** N **Valid Values:** Y or N; must be N if master user (A 1) Required

Field/Function Key	Description
GL: Security Levels	These fields are used to assign account access security levels for the current public authority profile. Account access security levels are assigned to provide or deny access to one or many G/L accounts. Each G/L account has four different access levels based on the type of function being performed: Transaction Entry, Inquiry, File Maintenance, and Reporting. When setting up the chart of accounts through G/L Accounts Maintenance (MENU GLFILE), each account is assigned an account access security level from 1 (most secure) to 9 (least secure) for each of the four types of functions. For each type of function, assign a security level by keying a value of 1 through 9. A 1 will allow users in the authority profile to have maximum access while a 9 will allow minimum access to GL accounts. A user will be given access to an account only if the account access security level (specified in these fields) is less than or equal to the access level assigned to the G/L account through G/L Accounts Maintenance (MENU GLFILE) for the respective type of function (transaction entry, inquiry, file maintenance and reporting). **Note:** Access level security is optional for each company and is turned on or off in GL Options Maintenance. **Default Value:** 9 **Valid Values:** 1-9; all security fields must be 1 if master user (N1,0) Required
AP: Restrict Voucher Entry	This field is used to restrict A/P Voucher Entry for users assigned with this authority profile. Restricted voucher entry allows a user to key a voucher group through Voucher Entry (MENU APMAIN), but GL account descriptions are not displayed, and GL account searches are not available. The user may print the Voucher Edit Report and Voucher Error Report without GL account descriptions. Key **Y** to have a restricted Voucher Entry. Key **N** if you do not want to restrict the use of Voucher Entry. **Default Value:** N **Valid Values:** Y or N; must be N for a master user (A 1) Required

Field/Function Key	Description
Default Cost to see	This field determines the default cost (OE or GL) to display in inquiries throughout Distribution A+. Key **O** to display the Order Entry (OE) cost as the default in inquiries. Key **G** to display the General Ledger (GL) cost as the default in inquiries. If a user does not have authority to either the **Display OE Cost and Profit (OE, SA, AR, some PO)** or **Display GL Cost and Profit (OE, SA, AR, some PO)** security options in Application Action Authority Maintenance (MENU XASCTY), then no cost will be shown in the inquiries. If a user has authority to only one of the security options, the opposite cost will not be available and therefore the toggle function key that displays in various inquiries to switch back and forth between the two costs (OE or GL cost), will not be displayed. Note that the description of the toggle key will vary depending on where the option is located to display both costs. (A 1) Required
Bypass Company Security	Use this field if the authority profile does not have master user authority (i.e., **Master User Authority** field is **N** on this screen) but you want to bypass company security checks for all functions. **Note:** Master users (**Master User Authority** field is **Y** on this screen) bypass any security checks and this field is ignored for master user authority. Key **Y** to bypass company security checks for this authority profile. Leave this field blank if you do not want to bypass company security checks for users with this authority profile or if the profile has Master User Authority. **Default Value:** Blank (A 1) Optional

Field/Function Key	Description
Bypass Warehouse Security	Use this field if the authority profile does not have master user authority (i.e., **Master User Authority** field is **N** on this screen) but you want to bypass warehouse security checks for all functions. **Note:** Master users (**Master User Authority** field is **Y** on this screen) bypass any security checks and this field is ignored for master user authority. Key **Y** to bypass warehouse security checks for this authority profile. Leave this field blank if you do not want to bypass warehouse security checks for users with this profile or if the profile has Master User Authority. **Default Value:** Blank (A 1) Optional
Bypass Salesrep Security	Use this field if the authority profile does not have master user authority (i.e., **Master User Authority** field is **N** on this screen) but you want to bypass salesrep security checks for all functions. **Note:** Master users (**Master User Authority** field is **Y** on this screen) bypass any security checks and this field is ignored for master user authority. Key **Y** to bypass salesrep security checks for this authority profile. Leave this field blank if you do not want to bypass salesrep security checks for users with this profile or if the profile has Master User Authority. **Default Value:** Blank (A 1) Optional
F4=Authorize Co's	You cannot use this function if the **Bypass Company Security** field is **Y** on this screen. If you do not want to bypass company security checks (**Bypass Company Security** field is blank), use this function key to select the companies for which users in this authority profile will be authorized to use. Press **F4=AUTHORIZE CO'S** to access the Select Authorized Companies Screen.
F5=Authorize WH's	You cannot use this function if the **Bypass Warehouse Security** field is **Y** on this screen. If you do not want to bypass warehouse security checks (**Bypass Warehouse Security** field is blank), use this function key to select the warehouses for which users in this authority profile will be authorized to use. Press **F5=AUTHORIZE WH'S** to access the Select Authorized Warehouses Screen.

Field/Function Key	Description
F6=Authorize Rep's	You cannot use this function if the **Bypass Salesrep Security** field is **Y** on this screen. If you do not want to bypass salesrep security checks (**Bypass Salesrep Security** field is blank), use this function key to select the salesreps for which users in this authority profile will be authorized to use. Press **F6=AUTHORIZE REP'S** to access the Select Authorized SalesReps Screen.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	Press **ENTER** to confirm your selections and return to the previous screen.

Select Authorized Companies Screen

This screen displays all valid companies defined through Company Name Maintenance (MENU XAFILE). The top portion of the screen includes the Authority Profile, company number and name of company. The lower portion of the screen provides a filter allowing you to display only company numbers that match the criteria you enter in the **Company Name** field.

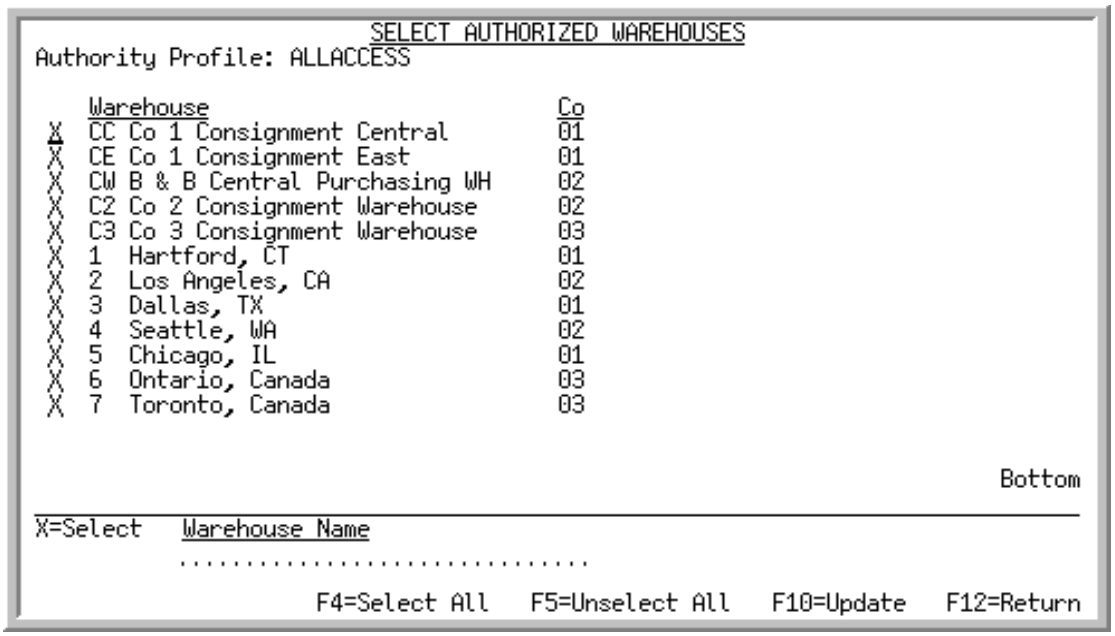
Use this screen to select the companies that the users in this authority profile will be authorized to use when performing Distribution A+ functions.

Select Authorized Companies Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to select which companies users with this authority profile will be authorized to use when performing Distribution A+ functions. On the top portion of the screen, key **X** in the column corresponding to the companies you want to select and press **F10=UPDATE** to update. A message will display informing you that the indicated companies will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To deselect any companies previously authorized, simply blank out the **X** next to the company you no longer want authorized. (A 1) Optional

Field/Function Key	Description
Company Name	Use this field to limit the screen to only those companies that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display companies, if any, matching your criteria. **Note:** This is a character string search and will display companies that match the data anywhere in the **Name** field. (A 30) Optional
F4=Select All	Press **F4=SELECT ALL** to select all companies (that are displayed on the screen based on filters) to be authorized for users with the current authority profile. An **X** will appear in the left column before all company numbers. If you want most companies authorized but want to exclude one or a few, simply blank out the X in the column before the companies you do not want authorized. The Select All option is based on the data filter information in the **Company Name** field. For example, filter to a common word in the names of some of your companies and press **F4=SELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the companies you selected based on the common word filter. If you want to ensure that you have selected ALL companies, verify that there is no data filter active in the **Company Name** field.
F5=Unselect All	Press **F5=UNSELECT ALL** to unselect all companies (that are displayed on the screen based on filters) from being authorized. All **X**'s will disappear in the left column before all company numbers. If you want to include only a few companies, simply key **X** in the column before the companies you want to authorize. **Note:** The Unselect All option is based on the data filter information in the **Company Name** field. For example, filter to a common word in the names of some of your companies and press **F5=UNSELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the companies remaining based on the common word filter. If you want to ensure that you have Unselected All companies, verify that there is no data filter active in the **Company Name** field.
F10=Update	After you have selected the companies, you want authorized, press **F10=UPDATE** to confirm your selections and update the Company Authority Assignment File (**COAUT**). Once **F10=UPDATE** is pressed, the companies you selected are shown on the screen and a message display informing you that the indicated companies will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.

Select Authorized Warehouses Screen



This screen displays all valid warehouses defined through Warehouse Numbers Maintenance (MENU IAFILE). The top portion of the screen includes the Authority Profile, warehouse number, name of warehouse, and company number associated with the warehouse. The lower portion of the screen provides a filter allowing you to display only warehouse numbers that match the criteria you enter in the **Warehouse Name** field.

Use this screen to select the warehouses that the users in this authority profile will be authorized to use when performing Distribution A+ functions.

Select Authorized Warehouses Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to select which warehouses users with this authority profile will be authorized to use when performing Distribution A+ functions. On the top portion of the screen, key **X** in the column corresponding to the warehouses you want to select and press **F10=UPDATE**. A message will display informing you that the indicated warehouses will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=REUTRN**. To deselect any warehouses previously authorized, simply blank out the **X** next to the warehouse you no longer want authorized. (A 1) Optional

Field/Function Key	Description
Warehouse Name	Use this field to limit the screen to only those warehouses that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display warehouses, if any, matching your criteria. This is a character string search and will display warehouses that match the data anywhere in the **Warehouse Name** field. (A 30) Optional
F4=Select All	Press **F4=SELECT ALL** to select all warehouses (that are displayed on the screen based on filters) to be authorized for users with the current authority profile. An **X** will appear in the left column before all warehouse numbers. If you want most warehouses authorized but want to exclude one or a few, simply blank out the **X** in the column before the warehouses you do not want authorized. **Note:** The Select All option is based on the data filter information in the **Warehouse Name** field. For example, filter to a common word in the names of some of your warehouses and press **F4=SELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the warehouses you selected based on the common word filter. If you want to ensure that you have selected All warehouses, verify that there is no data filter active in the **Warehouse Name** field.
F5=Unselect All	Press **F5=UNSELECT ALL** to unselect all warehouses (that are displayed on the screen based on filters) from being authorized. All **X**'s will disappear in the left column before all warehouse numbers. If you want to include only a few warehouses, simply key **X** in the column before the warehouses you want to authorize. **Note:** The Unselect All option is based on the data filter information in the **Warehouse Name** field. For example, filter to a common word in the names of some of your warehouses and press **F5=UNSELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the warehouses remaining based on the common word filter. If you want to ensure that you have Unselected ALL warehouses, verify that there is no data filter active in the **Warehouse Name** field.
F10=Update	After you have selected the warehouses, you want authorized, press **F10=UPDATE** to confirm your selections and update the Warehouse Authority Assignment File (**WHAUT**). Once **F10=UPDATE** is pressed, the warehouses you selected are shown on the screen and a message displays informing you that the indicated warehouses will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.

Field/Function Key	Description
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.

Select Authorized Salesreps Screen

The salesreps that display on this screen are based on the companies that the user(s) in this authority profile are authorized to, as determined on the Select Authorized Companies Screen. Salesreps for companies that user(s) in the authority profile are not authorized to use, will not display on this screen.

The top portion of the screen includes the Authority Profile, company number, and number and name of the salesrep. The lower portion of the screen provides a filter allowing you to display only salesreps that match the criteria you enter in the **Co** and/or **Salesrep Name** fields.

Use this screen to select the salesreps that the users in this authority profile will be authorized to use when performing Distribution A+ functions.

Select Authorized Salesreps Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to select which salesreps users with this authority profile will be authorized to use when performing Distribution A+ functions. On the top portion of the screen, key **X** in the column corresponding to the salesreps you want to select and press **F10=UPDATE**. A message will display informing you that the indicated salesreps will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To deselect any salesreps previously authorized, simply blank out the **X** next to the salesreps you no longer want authorized. (A 1) Optional
Co	Use this field to limit the screen to only those salesreps associated with the company number you key in this field. Key the company number and press **ENTER**. The screen will refresh and display salesreps, if any, matching your criteria. (N 2,0) Optional
Salesrep Name	Use this field to limit the screen to only those salesreps that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display salesreps, if any, matching your criteria. This is a character string search and will display salesreps that match the data anywhere in the **Salesrep Name** field. (A 30) Optional
F4=Select All	Press **F4=SELECT ALL** to select all salesreps (that are displayed on the screen based on filters) to be authorized for users with the current authority profile. An **X** will appear in the left column before all salesrep numbers. If you want most salesreps authorized but want to exclude one or a few, simply blank out the **X** in the column before the salesreps you do not want authorized. **Note:** The Select All option is based on the data filter information in the **Co** and **Salesrep Name** fields. For example, filter to a common word in the names of some of your salesreps and press **F4=SELECT ALL** to Select All. When you then press **F10=UPDATE**, your confirmation list will show the salesreps you selected based on the common word filter. If you want to ensure that you have selected All salesreps, verify that there is no data filter active in the **Co** and **Salesrep Name** fields.

Field/Function Key	Description
F5=Unselect All	Press **F5=UNSELECT ALL** to unselect all salesreps (that are displayed on the screen based on filters) from being authorized. All **X**'s will disappear in the left column before all salesrep numbers. If you want to include only a few salesreps, simply key **X** in the column before the salesreps you want to authorize. **Note:** The Unselect All option is based on the data filter information in the **Co** and **Salesrep Name** fields. For example, filter to a common word in the names of some of your salesreps and press **F5=UNSELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the salesreps remaining based on the common word filter. If you want to ensure that you have Unselected ALL salesreps verify that there is no data filter active in **Co** and **Salesrep Name** fields.
F10=Update	After you have selected the salesreps you want authorized, press **F10=UPDATE** to confirm your selections and update the Sales Rep Authority File (**RPAUT**). Once **F10=UPDATE** is pressed, the salesreps you selected are shown on the screen and a message display informing you that the indicated salesreps will be authorized to the current profile. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.

Authority Profile Listing

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Authority Profile Listing Screen	Used to specify the criteria for which options defined through Authority Profile Maintenance (MENU XASCTY) will print.
Authority Profile Listing	Used to print Authority Profiles defined through Authority Profile Maintenance (MENU XASCTY).

Authority Profile Listing Screen

Use this screen to specify the criteria for which options defined through Authority Profile Maintenance (MENU XASCTY) will print. The Authority Profile Master Listing will print information for Personal, Public, or both types of profiles.

You will also be able to select to print authorized companies, warehouses, or salesreps for the indicated types of profiles.

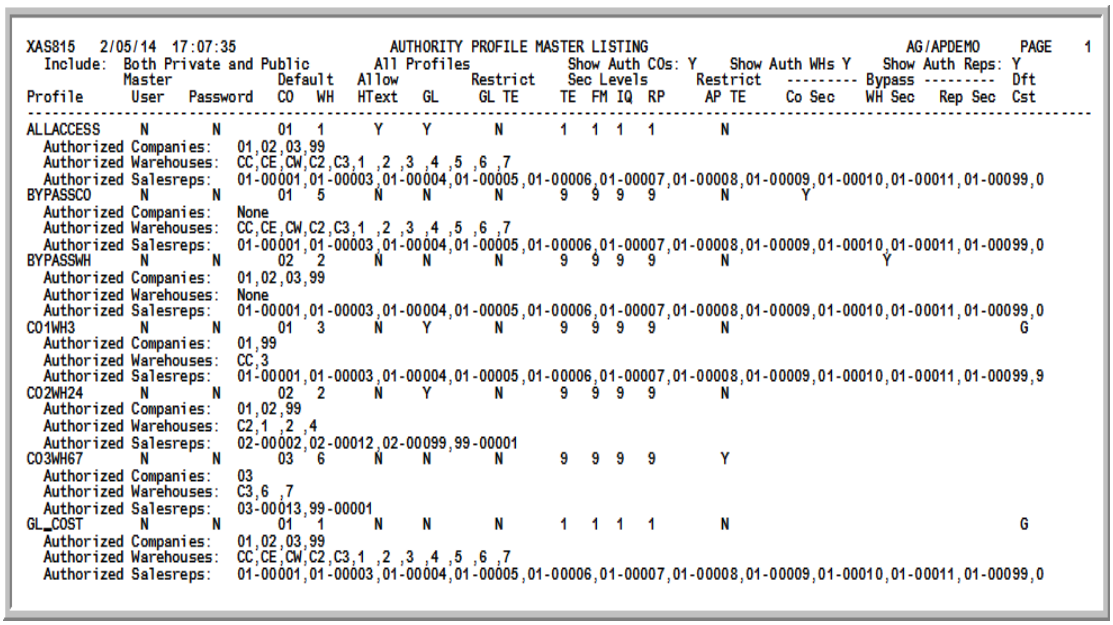
Authority Profile Listing Screen Fields and Function keys

Field/Function Key	Description
Include	Use this field to select the type of profile you want included on the Authority Profile Master Listing. You have the option to print information for Personal Profiles, Public Profiles, or both types of profiles. Personal profiles are set up through User Maintenance (MENU XASCTY) and cannot be shared with other users. Public profiles are set up through Authority Profile Maintenance and can be shared with other users. Public profiles can also initially be set up through User Maintenance, but once defined the profile must then be maintained through Authority Profile Maintenance. Key **1** to include personal profiles on the listing. Key **2** to include public profiles on the listing. Key **3** to include both personal and public profiles on the listing. (N 1,0) Required

Field/Function Key	Description
Profile	Use this field to key the range of profiles you want included on the Authority Profile Master Listing. **Valid Values:** Personal or Public profiles defined through User Maintenance (MENU XASCTY) or Authority Profile Maintenance (MENU XASCTY) (2@A10) Optional
Show Authorized Companies	Use this field to select if authorized companies will be included on the Authority Profile Master Listing for the indicated profiles. Key **Y** if you want the companies the profile is authorized to access printed on the listing. For each profile type you select to print, the authorized companies for that profile will be shown. For example, if you set up an individual profile of SMITH who had authority to work with companies 1, 2, and 99, and selected to print SMITH's profile and keyed **Y** in this field, the listing would show: SMITH Authorized Companies: 1, 2, 99 Key **N** if you do not want to include authorized companies on the listing. (A1) Required
Show Authorized Warehouses	Use this field to select if authorized warehouses will be included on the Authority Profile Master Listing for the indicated profiles. Key **Y** if you want the warehouses the profile is authorized to access printed on the listing. For each profile type you select to print, the authorized warehouses for that profile will be shown. For example, if you set up an individual profile of SMITH who had authority to work with warehouses 1, 2, and 99, and selected to print SMITH's profile and keyed **Y** in this field, the listing would show: SMITH Authorized Warehouses: 1, 2, 99 Key **N** if you do not want to include authorized warehouse on the listing. (A1) Required

Field/Function Key	Description
Show Authorized Salesreps	Use this field to select if authorized salesreps will be included on the Authority Profile Master Listing for the indicated profiles. Key **Y** if you want the salesreps the profile is authorized to access printed on the listing. For each profile type you select to print, the authorized salesreps for that profile will be shown. For example, if you set up an individual profile of SMITH who had authority to work with salesreps 1, 2, and 3, and selected to print SMITH's profile and keyed **Y** in this field, the listing would show: SMITH Authorized Salesreps: 1, 2, 3 Key **N** if you do not want to include authorized salesreps on the listing. (A1) Required
F3=Cancel	Press **F3=CANCEL** to cancel the listing and return to the menu.
F4=Profile List	Press **F4=PROFILE LIST** to access the Authority Profile List Screen which displays existing public profiles. Personal profiles will not be shown on the Authority Profile List Screen.
Enter	Press **ENTER** to confirm your entries. The Report Options Screen displays.

Authority Profile Master Listing



```
XAS815   2/05/14  17:07:35                AUTHORITY PROFILE MASTER LISTING                                  AG/APDEMO     PAGE    1
  Include:  Both Private and Public       All Profiles          Show Auth COs: Y    Show Auth WHs Y    Show Auth Reps: Y
            Master            Default   Allow        Restrict    Sec Levels      Restrict   --------- Bypass ---------  Dft
Profile      User   Password   CO   WH   HText   GL    GL TE     TE  FM IQ  RP     AP TE     Co Sec    WH Sec   Rep Sec  Cst
-------------------------------------------------------------------------------------------------------------------------------
ALLACCESS     N        N       01   1      Y     Y       N       1   1  1   1       N
  Authorized Companies:   01,02,03,99
  Authorized Warehouses:  CC,CE,CW,C2,C3,1 ,2 ,3 ,4 ,5 ,6 ,7
  Authorized Salesreps:   01-00001,01-00003,01-00004,01-00005,01-00006,01-00007,01-00008,01-00009,01-00010,01-00011,01-00099,0
BYPASSCO      N        N       01   5      N     N       N       9   9  9   9       N          Y
  Authorized Companies:   None
  Authorized Warehouses:  CC,CE,CW,C2,C3,1 ,2 ,3 ,4 ,5 ,6 ,7
  Authorized Salesreps:   01-00001,01-00003,01-00004,01-00005,01-00006,01-00007,01-00008,01-00009,01-00010,01-00011,01-00099,0
BYPASSWH      N        N       02   2      N     N       N       9   9  9   9       N                    Y
  Authorized Companies:   01,02,03,99
  Authorized Warehouses:  None
  Authorized Salesreps:   01-00001,01-00003,01-00004,01-00005,01-00006,01-00007,01-00008,01-00009,01-00010,01-00011,01-00099,0
CO1WH3        N        N       01   3      N     Y       N       9   9  9   9       N                                 G
  Authorized Companies:   01,99
  Authorized Warehouses:  CC,3
  Authorized Salesreps:   01-00001,01-00003,01-00004,01-00005,01-00006,01-00007,01-00008,01-00009,01-00010,01-00011,01-00099,9
CO2WH24       N        N       02   2      N     Y       N       9   9  9   9       N
  Authorized Companies:   01,02,99
  Authorized Warehouses:  C2,1 ,2 ,4
  Authorized Salesreps:   02-00002,02-00012,02-00099,99-00001
CO3WH67       N        N       03   6      N     N       N       9   9  9   9       Y
  Authorized Companies:   03
  Authorized Warehouses:  C3,6 ,7
  Authorized Salesreps:   03-00013,99-00001
GL_COST       N        N       01   1      N     N       N       1   1  1   1       N                                 G
  Authorized Companies:   01,02,03,99
  Authorized Warehouses:  CC,CE,CW,C2,C3,1 ,2 ,3 ,4 ,5 ,6 ,7
  Authorized Salesreps:   01-00001,01-00003,01-00004,01-00005,01-00006,01-00007,01-00008,01-00009,01-00010,01-00011,01-00099,0
```

This listing prints Authority Profiles defined through Authority Profile Maintenance (MENU XASCTY). You will be able to print both Private and Public Authority Profiles, select which profiles you want to include and select to include or exclude authorized companies, warehouses, and salesreps.

Chapter 6 Application Authority Maintenance/ Listing

Maintaining Application Authorities is performed through the Distribution A+ Security Menu (MENU XASCTY). Application Authority Profile Maintenance allows you to define application access (or menu option) authority to your various users and user groups.

This option provides various methods for assigning these authorities. You can select a user and then select the functions that user is authorized. You can select a user group and select the functions that users in this group are authorized, or you can select an application function and check off which users/ user groups will be authorized to the selected function.

Filter fields and function keys are available to assist in your selection of the application functions to provide authorization.

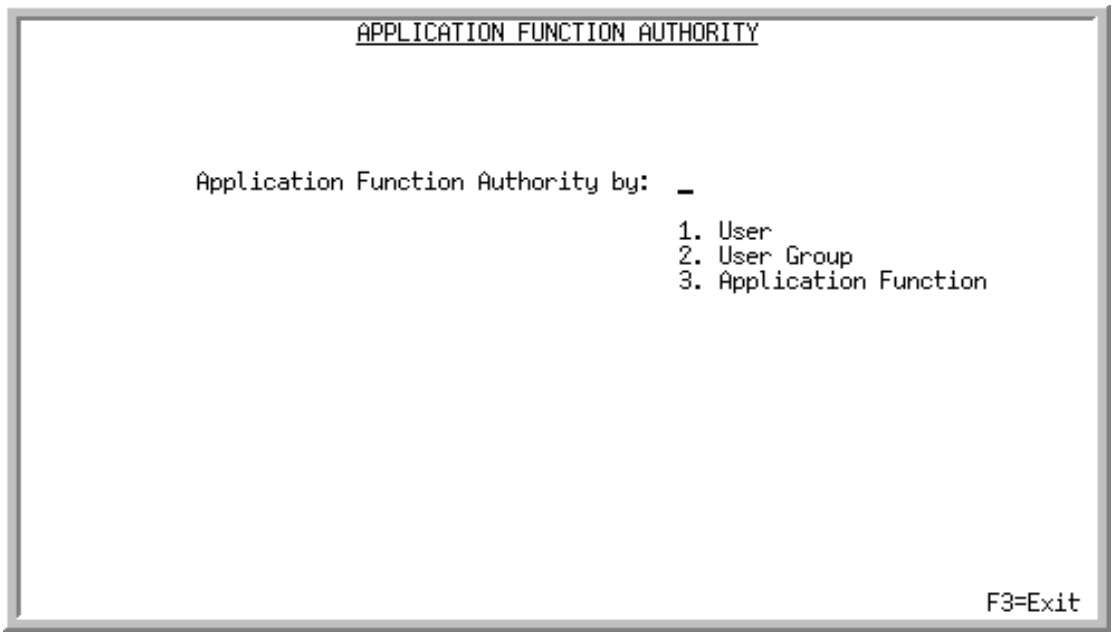
Application Authority Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Application Function Authority Screen	Used to determine which application functions (menu options) users will be authorized to perform.
User Selection or User Group Selection Screen	Used to select the User or User Groups for which you are defining application function authority.
User List Screen	Used to display users in the Distribution A+ User File for in the current base and environment users in the User Master File in the current environment, previously defined through this menu option with a user master definition). See User List Screen in the User Maintenance chapter for an explanation of this screen.

Title	Purpose
User Group List Screen	Used to assign the current user to a user group or multiple groups. See User Group List Screen in the User Maintenance chapter for an explanation of this screen.
Function Authorization Screen	Used to select the application functions for which you want to define application authorities based on user or user group.
Application Functions Screen	Used to select the application functions for which you want to define application authorities for all users based on application function.
Application Function Definition Screen	Used to review the application function definition, maintain the custom application function definition or to add, change or delete a custom application function definition.
User/User Group Authorization Screen	Used to select the User or User Groups you want authorized to use the selected function.

Application Function Authority Screen



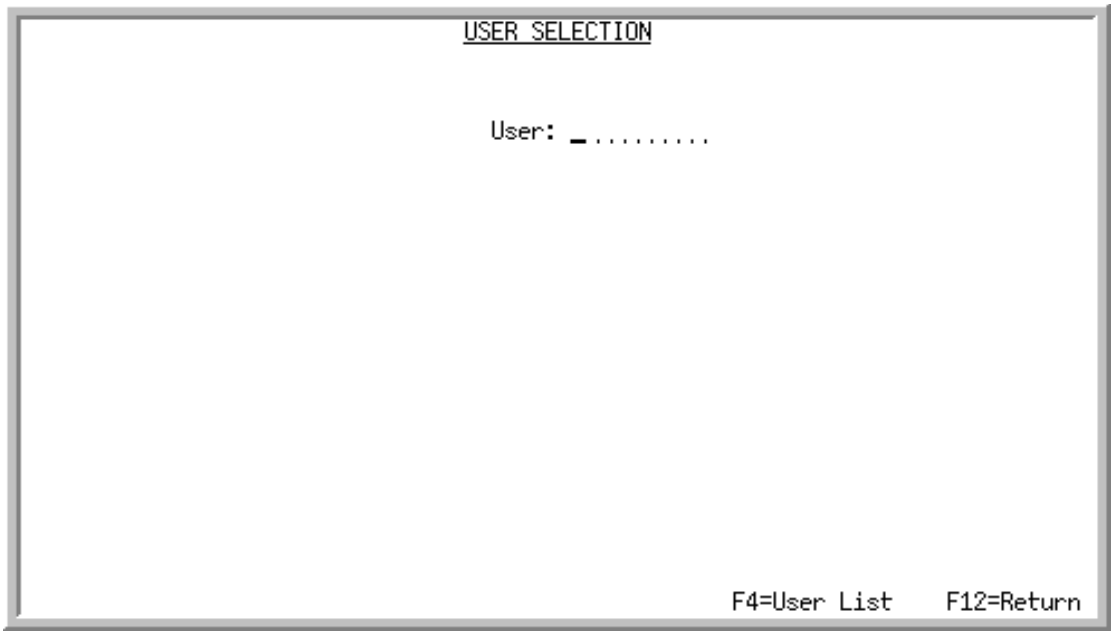
Use this screen to determine which application functions (menu options) users will be authorized to perform. You have the option to set up application authorities based on a particular User, User Group (for all users in that group), and Application Function (for specified menu options for any user).

Application Function Authority Screen Fields and Function keys

Field/Function Key	Description
Application Function Authority by	Use this field to determine which application functions (menu options) users will be authorized to perform. You have the option to set up application authorities based on a particular User, User Group, or Application Function. Key **1** if you want to set up application function authority for a particular User. Key **2** if you want to set up application function authority for users in a particular User Group. Key **3** if you want to set up application function authority for specified menu options for any user. (N1,0) Required
F3=Exit	Press **F3=EXIT** to exit this menu option and return to MENU XASCTY.

Field/Function Key	Description
Enter	Press **ENTER** to confirm your selection. If you keyed **1**, the User Selection or User Group Selection Screen appears. If you keyed **2**, the User Selection or User Group Selection Screen appears. If you keyed **3**, the Application Functions Screen appears.

User Selection or User Group Selection Screen



Use this screen to select the User or User Group for which you are defining application function authority. You can also access the User List Screen with **F4=USER LIST** or the User Group List Screen with **F4=GROUP LIST** to display a list of existing users or user groups.

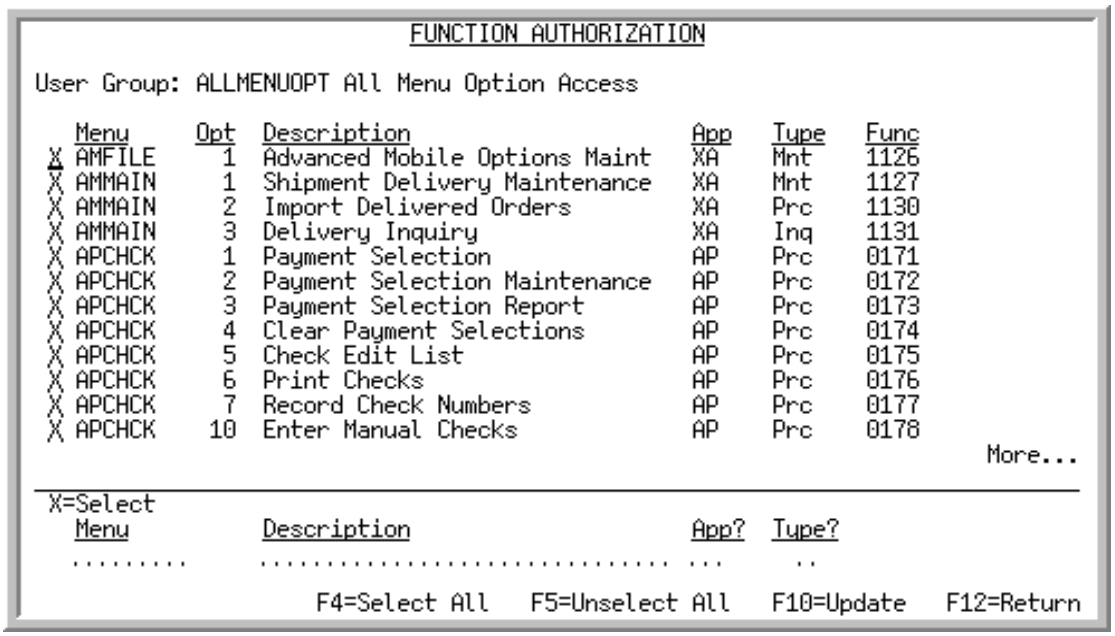
If you keyed 1 (User) on the Application Function Authority Screen, the title of this screen is User Selection Screen. If you keyed 2 (User Group), the title of this screen is User Group Selection Screen.

User Selection or User Group Selection Screen Fields and Function keys

Field/Function Key	Description
User / User Group	If you keyed **1** for User on the Application Function Authority Screen, use this field to identify the User for whom you are defining application function authorities. If you keyed **2** for User Group on the Application Function Authority Screen, use this field to identify the User Group for whom you are defining application function authorities. Key the user or user group. The user must be a valid user defined in the Distribution A+ User Master File; the user group must be a valid group created through User Group Maintenance (MENU XASCTY). Press **F4=USER LIST** to display a list of existing users. Press **F4=GROUP LIST** to display a list of existing user groups. (A 10) Required

Field/Function Key	Description
F4=User List / Group List	Press **F4=USER LIST / F4=GROUP LIST** to access the User List Screen, which displays existing users or User Group List Screen, which displays existing user groups. If you keyed **1** (User) on the Application Function Authority Screen, **F4=USER LIST** displays. If you keyed **2** (User Group), **F4=GROUP LIST** displays.
F12=Return	Press **F12=RETURN** to return to the Application Function Authority Screen without saving your selection.
Enter	Press **ENTER** to confirm your selection and proceed to the Function Authorization Screen.

Function Authorization Screen



Use this screen to select the application functions for which you want to define application authorities based on user or user group (depending on your selection on the Application Function Authority Screen. Application authorities can also be defined for application functions for all users by selecting **3** in the **Application Function Authority by** field on the Application Function Authority Screen.

If you are setting up application authority based on User, application authorities for the selected functions will be for this user only. If you are setting up application authorities based on User Group, application authorities for the selected functions will be for all users in this user group.

When paging through the list of menu options, each function is listed based on the menus it is assigned to. For example, the Item Inquiry is available on nine menus but has only one function number, and is assigned to application IA. If you filter to the **Description** of **Item Inquiry**, it will display just once. However, if you filter to a menu where the Item Inquiry exists, it will display in that menu specific list.

The lower portion of this screen provides filters that allow you to limit the criteria on the screen based on menu, description, application, and type.

Function Authorization Screen Fields and Function keys

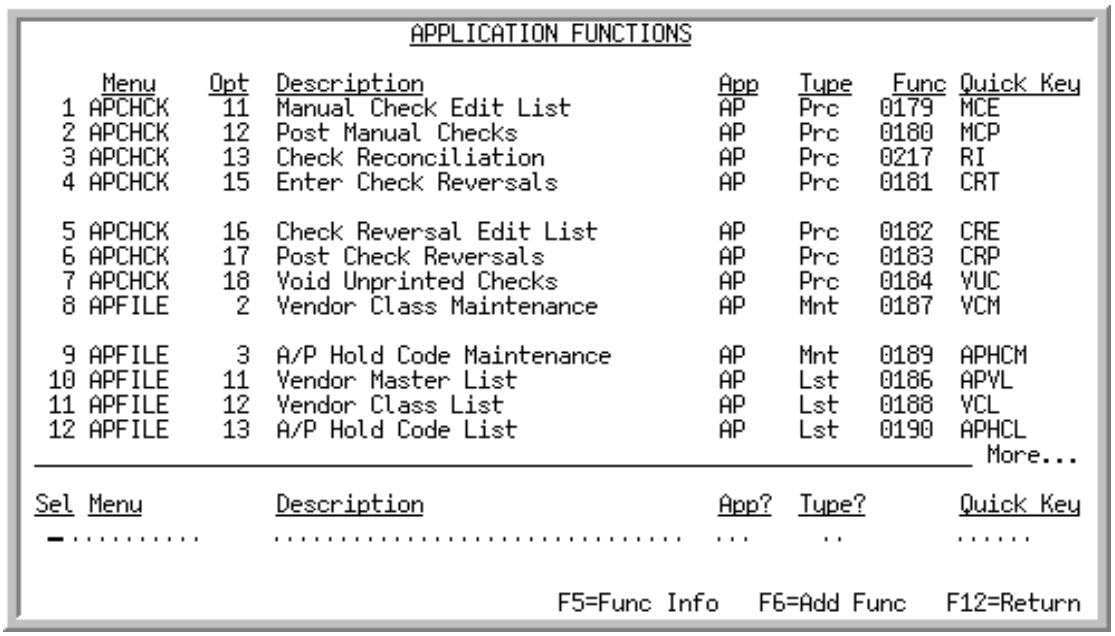
Field/Function Key	Description
User / User Group	If you keyed **1** for User on the Application Function Authority Screen, this is the User ID and Name of the user for whom you are defining application function authorities. If you keyed **2** for User Group on the Application Function Authority Screen, this is the User Group and Description for whom you are defining application function authorities.
X=Select	Use this field to select the application functions for which you are defining application authorities for the indicated user or user group. On the top portion of the screen, key **X** in the column corresponding to the functions you want to select and press **F10=UPDATE**. A message will display informing you that the indicated user or user group will be assigned to these functions. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To deselect any functions previously flagged, simply blank out the X next to the application functions you no longer wanted flagged. You can also use **F4=SELECT ALL** or **F5=UNSELECT ALL** to select or unselect all application functions. (A 1) Optional
Menu	The menu the function resides on (APCHCK, OEFILE, etc.). Display
Opt	The option number associated with the function on the specific menu. Display
Description	The description of the function as it appears on the menu. Display
App	The primary application the function is associated with (AP, OE, etc.). Display
Type	The type of function (reporting, processing, maintenance, etc.). Display
Func	The unique function number assigned to the specific program. Display

Field/Function Key	Description
Menu	Use this field to limit the screen to only those menus that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display menus, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 6) Optional
Description	Use this field to limit the screen to only those functions that match the description you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display those functions, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays limited information. **Note:** This is a character string search and will display descriptions that match the data anywhere in the **Description** field. (A 30) Optional
App	Use this field to limit the screen to the application you key in this field. Key the application ID and press **ENTER**. The screen will refresh and show only those functions associated with this application ID, if any. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 2) Optional
Type	Use this field to limit the screen to the type of function you key in this field. Key the first letter of the function type and press **ENTER**. The screen will refresh and show only those functions associated with this type of function. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** P-Processing, I-Inquiry, R-Report, M-Maintenance, L-List **Note:** The **Type** field value of **U** for Menu is not a valid selection for this screen because individual menus are not presented for security; the specific menu options are presented. (A 1) Optional

Field/Function Key	Description
F4=Select All	Press **F4=SELECT ALL** to select all application functions for which you are defining function authorities for the selected user or user group. An **X** will appear in each field corresponding to the application function indicating that all functions are flagged for assignment for this user or user group. If you want most functions flagged for application authority but want to exclude one or a few, simply blank out the **X** corresponding to the function you do not want flagged. **Note:** The **F4=SELECT ALL** option is based on the data filter information in the available filter fields on the lower portion of this screen. Use multiple combinations of filters to quickly and easily mark several items in the list. For example, filter to MENU OEMAIN and press **F4=SELECT ALL** to Select All and then filter to MENU ARMAIN and press **F4=SELECT ALL** to Select All. When you then press **F10=UPDATE** to Update, your confirmation list will show all the options on these menus. If you want to ensure that you have selected ALL application functions, verify that there is no data filter active in any of the available filter fields. To unselect all application functions, see **F5=UNSELECT ALL**.
F5=Unselect All	If you have previously flagged application functions for application authority definitions and no longer want certain or all functions flagged, press **F5=UNSELECT ALL** to unselect all application functions. **X** will disappear in each field corresponding to the application function that was previously flagged. **Note:** The **F5=UNSELECT ALL** option is based on the data filter information in the available filter fields on the lower portion of this screen. Use multiple combinations of filters to quickly and easily mark several items in the list. For example, filter to MENU OEMAIN and press **F5=UNSELECT ALL** to Unselect All and then filter to MENU ARMAIN and press **F5=UNSELECT ALL** to Unselect All. When you then **F10=UPDATE** to Update, your confirmation list will show all the options remaining when these menu options are removed. If you want to ensure that you have unselected ALL application functions, verify that there is no data filter active in any of the available data filter fields. To select all application functions, see **F4=SELECT ALL**.

Field/Function Key	Description
F10=Update	After you have selected which functions you want to flag for application authority for the indicated user or user group, press **F10=UPDATE** to confirm your selections. Once **F10=UPDATE** is pressed, the screen refreshes and displays the functions that will be assigned to the indicated user or user group. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the User Selection or User Group Selection Screen without saving your selections.

Application Functions Screen



Use this screen to select the application functions for which you want to define application authorities for all users based on application function (you selected **3** on the Application Function Authority Screen).

Note: This screen can also be accessed from the Security Audit Inquiry after pressing **F4=FUNCTIONS** on the Audit Access By Application Function Screen. If this screen is accessed from the inquiry mode, you will be presented with a list of options available for the menu you selected on the Audit Access By Application Function Screen, if you selected a menu. Otherwise, all menu options are displayed on this screen.

The lower portion of this screen provides filters that allow you to limit the criteria on the screen based on menu, description, application, type, and quick key.

From this screen, you can also review an application function or maintain a custom application function definition via **F5=FUNC INFO** or add a custom application function definition via **F6=ADD FUNC**. Additionally, from this screen, you will be able to access the User/User Group Authorization Screen where you can select users/user groups for authorization to the selected application function. Note that if you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, this functionality does not apply and the **F5=FUNC INFO** and **F6=ADD FUNC** keys will not be displayed on this screen.

When paging through the list of functions, each function is listed once based on the primary application it is assigned to. For example, the Item Inquiry is available on nine menus but has only one function number, and is assigned to application IA. If you filter to the **Description** of **Item Inquiry**, it will display just once. However, if you filter to a menu where the Item Inquiry exists, it will display in that menu specific list.

Application Functions Screen Fields and Function keys

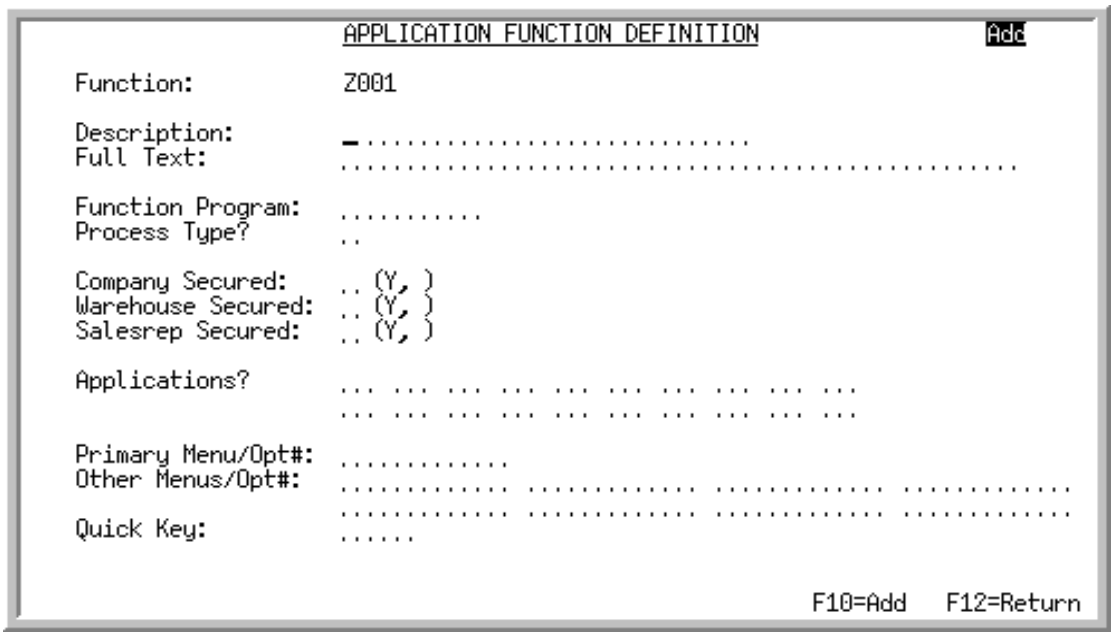
Field/Function Key	Description
(Reference Number)	The reference number of the application function authorities displayed on this screen. This number is 1 through 12 for the twelve functions that may display. When rolling forward or backward, the reference numbers do not change. Key this number in the **Sel** field to select it for further action. Display
Menu	The menu the function resides on (APCHCK, OEFILE, etc.). Display
Opt	The option number associated with the function on the specific menu. Display
Description	The description of the function as it appears on the menu. Display
App	The primary application the function is associated with (AP, OE, etc.). Display
Type	The type of function (reporting, processing, maintenance, etc.). Display
Func	The unique function number assigned to the specific program. Display
Quick Key	The quick key associated with the function to be used as one method available to launch the program from A+ WEB. Display
Sel	Use this field to select an application function for which you want to assign user/user group authorizations for that function, review application function definitions, or maintain custom application function definitions. Key the corresponding reference number of the function you want to select and press **ENTER** or **F5=FUNC INFO**, depending on the process you want to perform. **Note:** If you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, after selecting an application function and pressing **ENTER**, you are returned to the Audit Access By Application Function Screen. (N2,0) Optional

Field/Function Key	Description
Menu	Use this field to limit the screen to only those menus that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display menus, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Note:** If you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, this field displays the menu name you keyed on that screen, if one was keyed. (A 6) Optional/Display
Description	Use this field to limit the screen to only those functions that match the description you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display those functions, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays limited information. **Note:** This is a character string search and will display descriptions that match the data anywhere in the **Description** field. (A 30) Optional
App	Use this field to limit the screen to the application you key in this field. Key the 2 character application ID and press **ENTER**. The screen will refresh and show only those functions associated with this application ID, if any. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 2) Optional

Field/Function Key	Description
Type	Use this field to limit the screen to the type of function you key in this field. Key the first letter of the function type and press **ENTER**. The screen will refresh and show only those functions associated with this type of function. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** P-Processing, I-Inquiry, R-Report, M-Maintenance, L-List **Note:** The **Type** field value of **U** for Menu is not a valid selection for this screen because individual menus are not presented for security; the specific menu options are presented. (A 1) Optional
Quick Key	Use this field to limit the screen to the functions with quick keys that match the data anywhere in the quick key field. Key the criteria and press **ENTER**. The screen will refresh and display those functions, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 5) Optional
F5=Func Info	**Note:** If you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, this function key is not applicable and therefore does not display. After keying a selection number in the **Sel** field for the function you want to select, press **F5=FUNC INFO** to review an application function definition. The Application Function Definition Screen will appear and you will be able to review the application function definition. Fields will be display-only. If you selected a 'custom' application definition, when you press **F5=FUNC INFO**, fields will not be display-only and you will be able to maintain or delete that definition. To add a custom application definition, press **F6=ADD FUNC**.
F6=Add Func	**Note:** If you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, this function key is not applicable and therefore does not display. Press **F6=ADD FUNC** to add a custom application function definition. The Application Function Definition Screen will appear, where you can add a custom application function definition.
F12=Return	Press **F12=RETURN** to return to the Application Function Authority Screen without saving your selections.

Field/Function Key	Description
Enter	After keying a selection number in the Sel field for the function you want to select, press **ENTER** to confirm your selection. The User/User Group Authorization Screen will display, allowing you to select the users and user groups that you want authorized to this application functions. If you entered criteria in the filter fields on the lower portion of the screen, press **ENTER** to refresh the screen and display those functions that match the criteria you entered. **Note:** If you accessed this screen from the Audit Access By Application Function Screen, during the Security Audit Inquiry, after selecting an application function and pressing **ENTER**, you are returned to the Audit Access By Application Function Screen.

Application Function Definition Screen



If you pressed **F5=FUNC INFO** on the Application Functions Screen, after selecting an application function, use this screen to review the application function definition. Fields are display-only for base application functions.

If you pressed **F5=FUNC INFO** on the Application Functions Screen, after selecting a particular custom function, use this screen to maintain or delete the custom application function definition.

If you pressed **F6=ADD FUNC** on the Application Functions Screen, use this screen to add a custom application function definition.

Note: Custom functions are identified by the system generating a Function number starting with the letter 'Z' (e.g., Function: Z001).

Application Function Definition Screen Fields and Function keys

Field/Function Key	Description
Function	**Display Mode** The system function number that was generated during an addition of an application function definition. **Maintenance Mode** This field displays the system generated function number. It starts with 'Z' indicating that you are adding a "custom" application function definition. Display

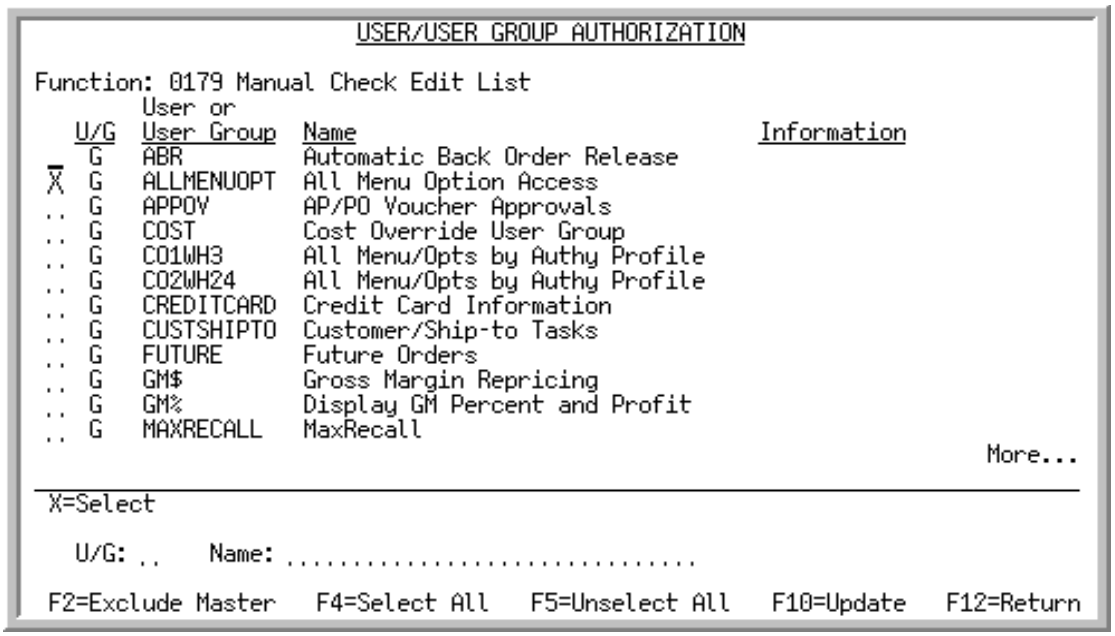
Field/Function Key	Description
Description	**Display Mode** The description of the function to perform on the primary menu. **Maintenance Mode** Use this field to key the description of the function to perform as it will appear on the primary menu. For example, a description might be "Payment Processing". (A 30) Required
Full Text	The full text of the menu option for descriptive purposes. (A 50) Optional
Function Program	**Display Mode** The system program number associated with the particular application function that will be called from the menu. **Maintenance Mode** Use this field to key the system program number associated with the particular application function that will be called when the menu option is selected. (A 10) Optional
Process Type	Display Mode The type of process the function is, such as reporting, processing, maintenance, etc. Maintenance Mode Use this field to key the type of process associated with this function. **Type U** for menus is used to show menu names on the module tabs. The quick key value is coded in Distribution A+ GUI panel and is passed to the Attention Menu to update the active task with the menu's name. Additionally, it is used to build the drop down navigation menus for non-command line access users. Key one of the following: • **I** for Inquiry • **L** for List • **M** for Maintenance • **P** for Processing • **R** for Report • **U** for Menu (A 1) Required

Field/Function Key	Description
Company Secured	**Display Mode** The system displays **Y** if this function is flagged for company security checks. **Maintenance Mode** Use this field to indicate that company security is available to this function. For custom functions being added here, logic will need to be added to the program behind this option to perform the company authority checking logic. Key **Y** to indicate that company security is available to this function. This function (menu option) will then display on the Company/Warehouse/ Salesrep Authority screens in Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) and be available for additional tailoring. Leave this field blank to indicate that company security is not available to this function. (A 1) Optional
Warehouse Secured	**Display Mode** The system displays **Y** if this function is flagged for warehouse security checks. **Maintenance Mode** Use this field to indicate that warehouse security is available to this function. For custom functions being added here, logic will need to be added to the program behind this option to perform the warehouse authority checking logic. Key **Y** to indicate that warehouse security is available to this function. This function (menu option) will then display on the Company/Warehouse/ Salesrep Authority screens in Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) and be available for additional tailoring. Leave this field blank to indicate that warehouse security is not available to this function. (A 1) Optional

Field/Function Key	Description
Salesrep Secured	**Display Mode** The system displays **Y** if this function is flagged for salesrep security checks. **Maintenance Mode** Use this field to indicate that salesrep security is available to this function. For custom functions being added here, logic will need to be added to the program behind this option to perform the salesrep authority checking logic. Key **Y** to indicate that salesrep security is available to this function. This function (menu option) will then display on the Company/Warehouse/ Salesrep Authority screens in Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) and be available for additional tailoring. Leave this field blank to indicate that salesrep security is not available to this function. (A 1) Optional
Applications	**Display Mode** The 2-character ID(s) of the application(s) the function is performed through. **Maintenance Mode** This field represents the application(s) that the function is performed through. At least one application must be entered. Key the 2-character ID(s) of the application(s) for which you can perform this function. (20 @ A 2) Required
Primary Menu/Opt #	**Display Mode** The primary menu the function resides on, followed by the option number on the menu. **Maintenance Mode** Key the primary menu that the function resides on, followed by the option number of the function. (A 6/N3,0) Required
Other Menus/Opt #	**Display Mode** The other menus the function can be performed through, followed by the option number on the menu. **Maintenance Mode** Key the other menus that the function resides on (other than the primary menu), followed by the option number of the function. (8 @ A 6/N3,0) Optional

Field/Function Key	Description
Quick Key	**Display Mode** The unique quick key identifier assigned to this menu option. **Maintenance Mode** Quick keys may be defined to provide you with direct access into a particular function when working within Distribution A+. Key the quick key that will be associated with this custom application function. Upon pressing **F10=ADD**, the **Quick Key** field in the Application Function Master File (**FNCMST**) will be updated. **Valid Values:** A quick key that has not yet been defined for another function (A 5) Optional
F10=Add / F10=Update	The **F10=ADD / F10=UPDATE** function key does not display if you selected an application function and pressed **F5=FUNC INFO** on the Application Functions Screen. If you selected a particular 'custom' application function definition and pressed **F5=FUNC INFO**, or simply pressed **F6=ADD FUNC** to add a new application function definition, this key will be displayed. If you are adding a new custom application function definition, this function key displays as **F10=ADD**. If you are changing an existing custom application function definition, this function key displays as **F10=UPDATE**. Press **F10=ADD / F10=UPDATE** to add the new custom application function definition, or to update an existing custom application function definition with your changes. You will be returned to the Application Functions Screen.
F12=Return	If you are in the display-only mode (you selected an application definition and pressed **F5=FUNC INFO** on the Application Functions Screen), after reviewing the function definition information, press **F12=RETURN** to return to the previous screen. If you are adding/maintaining an existing custom application function definition, press **F12=RETURN** to return to the previous screen without saving your changes.
F24=Delete	The **F24=DELETE** function key appears only if you are maintaining an existing custom application function definition. Press **F24=DELETE** to delete the custom application function definition. You will be prompted to confirm deletion by keying **Y** or **N**.

User/User Group Authorization Screen



This screen displays after selecting an application function on the Application Functions Screen. Use this screen to select the User or User Groups to be authorized to use the selected function.

Filters are also provided at the lower portion of this screen to allow you to limit the screen to Users or User Groups that match the criteria you enter.

User/User Group Authorization Screen Fields and Function keys

Field/Function Key	Description
X=Select	Use this field to assign users or user groups to the indicated function. On the top portion of the screen, key **X** in the column corresponding to the users or user groups you want to select and press **F10=UPDATE**. A message will display informing you that the indicated users or user groups will be assigned to the function. You will have the option to confirm your selections by pressing Enter or make more changes by pressing **F12=RETURN**. To deselect any users or user groups previously assigned to the function, simply blank out the **X** next to the user or user group you no longer want included. (A 1) Optional
Function	The function number and name of the selected menu option. Display

Field/Function Key	Description
U/G	Displays as **U** for User or **G** for User Group to identify the value in the User or User Group column. Display
User or User Group	The User or User Group as identified in the **U/G** column. Users are defined in the Distribution A+ User Master File. User groups are created through User Group Maintenance (MENU XASCTY). Display
Name / Information	The Username or User Group description, and information identifying if the user is a Master User or is a Suspended user. Display
U/G	Use this field to limit the screen to users OR user groups only. Key **U** to limit the screen to users only. Key **G** to limit the screen to user groups only. After you press **ENTER**, the screen will refresh and display users or user groups matching the criteria you entered. (A 1) Optional
Name	Use this field to limit the screen to only those users or user groups that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display users or user groups, if any, matching your criteria. (A 1) Optional
F2=Exclude Master	Use this **F2=EXCLUDE MASTER** toggle key to include or exclude Master users on this screen. Press **F2=EXCLUDE MASTER** to exclude users defined as Master users from displaying on this screen. Press **F2=EXCLUDE MASTER** again to include users defined as Master users. (A 2) Optional

Field/Function Key	Description
F4=Select All	Press **F4=SELECT ALL** to select all users or user groups to be assigned to the indicated function. An **X** will appear in the left column before all displayed users or user groups. If you want most users or user groups assigned to the function but want to exclude one or a few, simply blank out the **X** in the column before the users or user groups you do not want to include. **Note:** The Select All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your list of user/user group names. You would filter to the word 'credit' and press **F4=SELECT ALL** to Select All. When you press **F10=UPDATE** to Update, your confirmation list will show the user/user groups you selected based on the credit filter. If you want to ensure that you have selected ALL user/user groups, verify that there is no data filter active in the **U/G** and **Name** fields. To unselect all users or user groups, see **F5=UNSELECT ALL**. (A 1) Optional
F5=Unselect All	Press **F5=UNSELECT ALL** to unselect all users or user groups from being assigned to the function. All X's will disappear in the left column before all users and user groups. If you want to assign only a few users or user groups to the function, simply key **X** in the column before the users or user groups you want to include. **Note:** The Unselect All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your list of user/user group names. You would filter to the word 'credit' and press **F5=UNSELECT ALL** to Unselect All. When you then press **F10=UPDATE** to update, your confirmation list will show the user/user groups remaining based on the credit filter. If you want to ensure that you have unselected ALL user/user groups, verify that there is no data filter active in the **U/G** and **Name** fields. To select all users or user groups, see **F4=SELECT ALL**.
F10=Update	After you have selected the users or user groups you want assigned to the indicated function, press **F10=UPDATE** to confirm your selections and update the User Group Assignment File. Once **F10=UPDATE** is pressed, the users or user groups you selected are shown on the screen and a message display informing you that the indicated users or user groups will be assigned to the function. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.

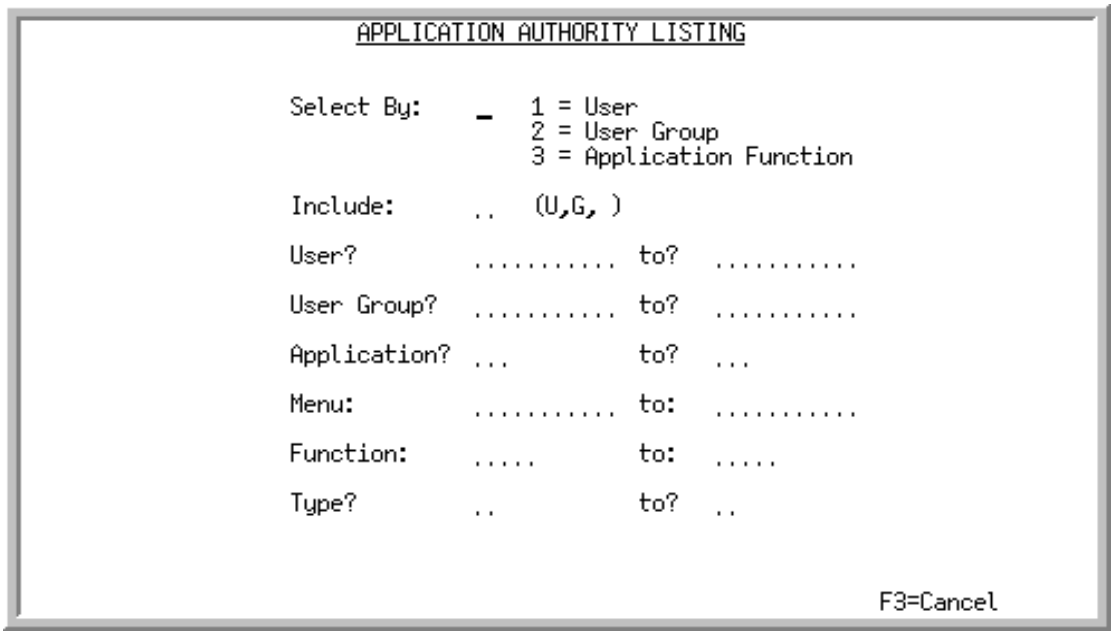
Field/Function Key	Description
Enter	After entering criteria in the **U/G** or **Name** field, press **ENTER** to refresh the screen and display users or user groups that match the criteria you entered.

Application Authority Maintenance Listing

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Application Authority Listing Screen	Used to specify the criteria for which options defined through Application Authority Maintenance (MENU XASCTY) will print.
Application Authority Listing	Used to print information by User, User Group, or Application Function to determine who has access to what menu options.

Application Authority Listing Screen



Use this screen to specify the criteria for which options defined through Application Authority Maintenance (MENU XASCTY) will print. The Application Authority List will print information by User, User Group, or Application Function to determine who has access to what menu options. You will be able to enter selection criteria to limit the information to print based on: User, User Group, Application, Menu, Function, and Type. You can also select to include Users only, User Groups only, or both types on the list.

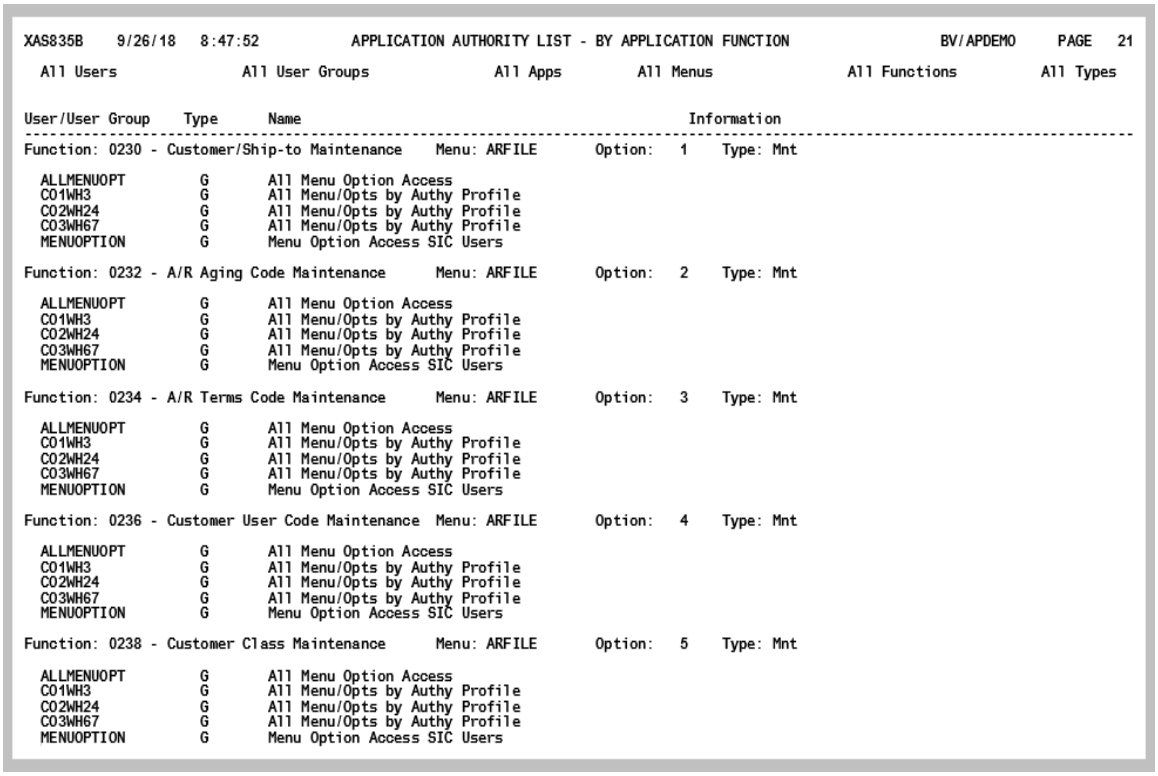
Application Authority Listing Screen Fields and Function keys

Field/Function Key	Description
Select By	Use this field to select to print application authorities defined through Application Authority Maintenance (MENU XASCTY) by User, User Group, or Application Function. Key **1** to print the application functions (menu options) a particular user or range of users have authority to use. Key **2** to print the application functions (menu options) a particular user group or range of user groups have authority to use. Key **3** to print each application function (menu option) and the user(s) and/or user group(s) that have authority to use the particular function. (N 1,0) Required

Field/Function Key	Description
Include	If you selected to print the listing by Application Function (the Select By field = 3), use this field to include Users only, User Groups only, or both types for each function (menu option) listed. Key **U** to include Users only. For each application function, the list will print the users that have access to that function. Key **G** to include User Groups only. For each application function, the list will print the user groups that have access to that function. Leave this field blank to include both Users and User Groups. For each application function, the list will print the users and user groups that have access to that function. Functions that are not assigned any user access will not print. (A1) Required
User	If you selected to print the listing by User (the Select By field = 1), use this field to limit the listing to one or more users for which application authorities will print. Key the user or range of users to be included on the listing. (2 @ A10) Optional
User Group	If you selected to print the listing by User Group (the Select By field = 2), use this field to limit the listing to one or more user groups for which application authorities will print. Key the user group or range of user groups to be included on the listing. (2 @ A10) Optional
Application	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the application or range of applications you select. Key the application ID or range of application IDs to be included on this listing. For example, if you want only Accounts Payable authority information printed, key AP in this field. (2 @ A2) Optional
Menu	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the menu or range of menus you select. Key the menu or range of menus to be included on this listing. For example, if you want only Accounts Payable check processing information printed, key APCHCK (for MENU APCHCK options) in this field. (2 @ A6) Optional

Field/Function Key	Description
Function	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the function number or range of function numbers you select. Key the function number or range of functions numbers to be included on this listing. For example, if you want only function number 0134 included on this listing, key that number in this field. (2 @ A4) Optional
Type	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the function type or range of function types you select. Key the function type or range of function types to be included on this listing. **Valid Values:** P-Processing, I-Inquiry, R-Report, M-Maintenance, L-List **Note:** The **Type** field value of **U** for Menu is not a valid selection for this screen because individual menus are not presented for the listing. (2 @ A1) Optional
F3=Cancel	Press **F3=CANCEL** to cancel the listing and return to the menu.
Enter	Press **ENTER** to confirm your entries. The Report Options Screen displays.

Application Authority Listing



```
XAS835B    9/26/18   8:47:52          APPLICATION AUTHORITY LIST - BY APPLICATION FUNCTION                BV/APDEMO     PAGE   21
  All Users              All User Groups              All Apps         All Menus               All Functions          All Types

User/User Group    Type      Name                                                 Information
-------------------------------------------------------------------------------------------------------------------------------
Function: 0230 - Customer/Ship-to Maintenance    Menu: ARFILE       Option:   1    Type: Mnt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0232 - A/R Aging Code Maintenance      Menu: ARFILE       Option:   2    Type: Mnt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0234 - A/R Terms Code Maintenance      Menu: ARFILE       Option:   3    Type: Mnt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0236 - Customer User Code Maintenance  Menu: ARFILE       Option:   4    Type: Mnt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0238 - Customer Class Maintenance      Menu: ARFILE       Option:   5    Type: Mnt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users
```

Use this listing to determine information by User, User Group, or Application Function to see who has access to what menu options.

On the Application Authority Listing Screen, you will be able to enter selection criteria to limit the information to print based on: User, User Group, Application, Menu, Function, and Type. You can also select to include Users only, User Groups only, or both types on the list.

Chapter 7 Company/Warehouse/Salesrep Authority Maintenance/Listing

Maintaining Company/Warehouse/Salesrep Authorities is performed through the Distribution A+ Security Menu (MENU XASCTY). If security is activated and you selected not to bypass company, warehouse, and salesrep security in Authority Profile Maintenance (MENU XASCTY), you can use the Company/Warehouse/Salesrep Authority Maintenance option to determine if company, warehouse, and/or salesrep authority checking will be performed based on certain criteria. You will have the option to override security checks based on the user/application function, user group/application function level, and application function.

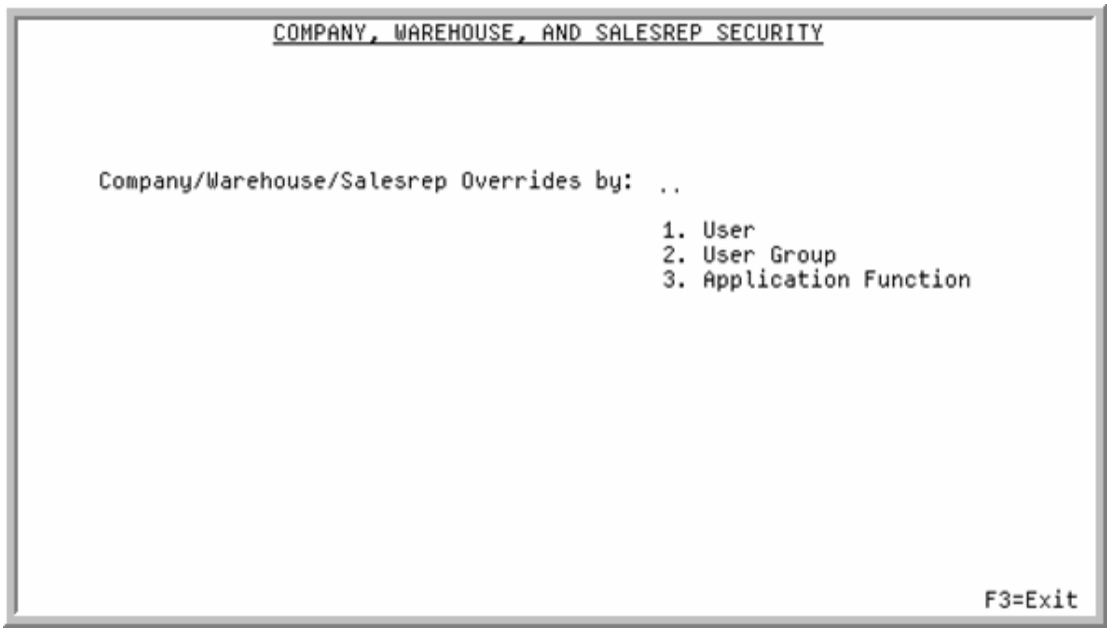
This option assumes that company, warehouse, and/or salesrep security options have been activated through System Options Maintenance (MENU XAFILE) and authorization has been set up through Application Action Authority (MENU XASCTY).

Company/Warehouse/Salesrep Authority Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Company, Warehouse, and Salesrep Security Screen	Used to specify the type of authority override you want to create.
User or User Group Selection Screen	Used to specify the user for whom or the user group for which you are creating an override.
Application Function Overrides Screen	Used to select the application functions that will be bypassed for company, warehouse, and/or salesrep security.

Company, Warehouse, and Salesrep Security Screen



Use this screen to select the method by which you want to create company/warehouse/salesrep authority overrides. You can create override security checks based on the user/application function, user group/application function level, and application function.

Company, Warehouse, and Salesrep Security Screen Fields and Function Keys

Field/Function Key	Description
Company/Warehouse/ Salesrep Overrides by	Use this field to omit company, warehouse, and/or salesrep authority security checks for the override type you key in this field. Key **1** if you want to set up company, warehouse, and/or salesrep authority overrides by User. Key **2** if you want to set up company, warehouse, and/or salesrep authority overrides by User Group. Key **3** if you want to set up company, warehouse, and/or salesrep authority overrides by Application Function. (N 1,0) Required
F3=Exit	Press **F3=EXIT** to exit this screen and return to MENU XASCTY.
Enter	Press **ENTER** to confirm your selection. If you keyed **1** or **2**, the User or User Group Selection Screen appears. If you keyed **3**, the Application Function Overrides Screen appears.

User or User Group Selection Screen

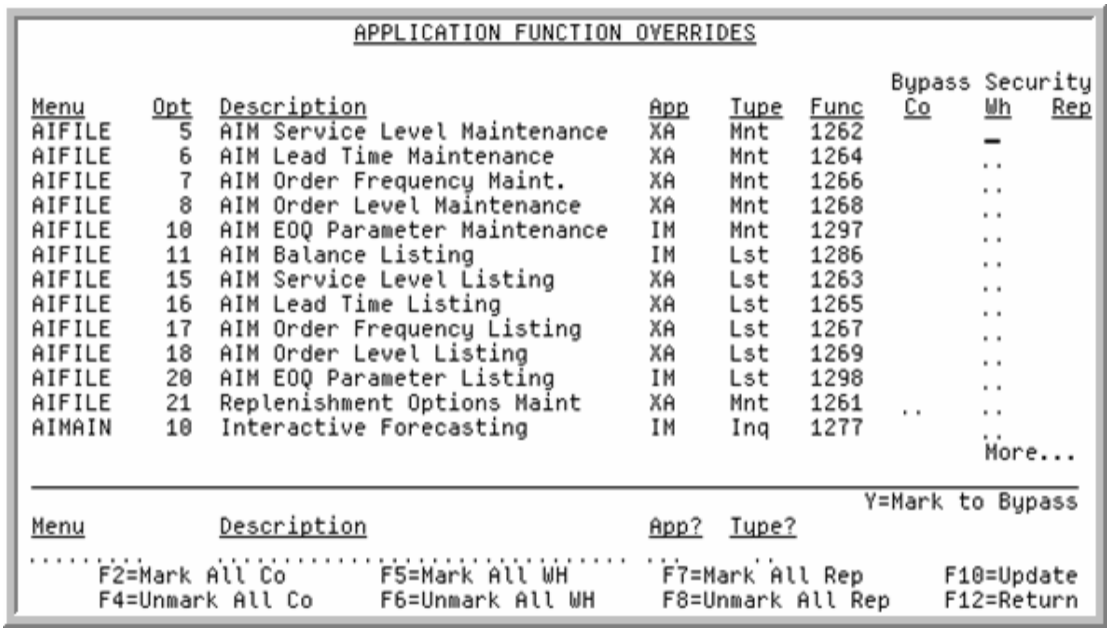
Use this screen to select the Users or User Groups for which company/warehouse/salesrep authority checks will be omitted. You can also access the User List Screen or User Group List Screen with **F4=USER LIST / F4=GROUP LIST** to display a list of all existing users or user groups.

If you keyed **1** (User) on the Company, Warehouse, and Salesrep Security Screen, the title of this screen is User Selection Screen and the field is **User** and the function key is **F4=USER LIST**. If you keyed **2** (User Group), the title of this screen is User Group Selection Screen and the field is **User Group** and the function key is **F4=GROUP LIST**.

User or User Group Selection Screen Fields and Function Keys

Field/Function Key	Description
User/User Group	If you keyed **1** for User on the Company, Warehouse, and Salesrep Security Screen, use this field to identify the user for whom company, warehouse and salesrep authority checks are being omitted. Press **F4=USER LIST** to display a list of existing users. If you keyed **2** for User Group on the Company, Warehouse, and Salesrep Security Screen, use this field to identify the user group for whom company, warehouse and salesrep authority checks are being omitted. Press **F4=GROUP LIST** to display a list of existing user groups Key the user or user group. **Valid Values:** The user must be a valid user defined in the Distribution A+ User Master File; the user group must be a valid group created through User Groups (MENU XASCTY). (A 10) Required
F4=User List/ F4=Group List	Press **F4=USER LIST** to access the User List Screen, which displays existing users, or press **F4=GROUP LIST** to access the User Group List Screen, which displays existing user groups.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your selection.
Enter	Press **ENTER** to confirm your selection and proceed to the next screen.

Application Function Overrides Screen



Use this screen to select the application functions that will be bypassed for company, warehouse, and/ or salesrep security checks based on user, user group or application function (depending on your selection on the Company, Warehouse, and Salesrep Security Screen).

If you are setting up overrides based on **User** (the **User** name displays on the top of this screen), company, warehouse, and/or salesrep security checks will be bypassed for this user only for the application functions you select on this screen.

If you are setting up overrides based on **User Group** (the **User Group** name displays on the top of this screen), company, warehouse, and/or salesrep security checks will be bypassed for all users in this User Group for the application functions you select on this screen.

If you are setting up overrides based on **Application Function**, company, warehouse, and/or salesrep security checks will be bypassed for any user for the application functions you select on this screen.

If you are setting up overrides for Application Functions, only functions that are subject to company, warehouse, and/or salesrep authority checking are displayed on this screen. If you are setting up overrides for Users or User Groups, only functions that the user or user group have access authorization to are displayed on this screen. An entry field in the **Bypass Security Company**, **Warehouse**, and **Salesrep** fields on the top portion of this screen is only provided if that particular function has company, warehouse, and/or salesrep logic associated with it.

The top portion of this screen displays the:

- menu the function resides on (apchck, oefile, etc.)
- option number associated with the function

- description of the function
- application the function is associated with (AP, OE, PO, etc.)
- type of function (reporting, processing, maintenance, etc.)
- function number
- **Bypass Security Co, Bypass Security Wh**, and **Bypass Security Rep** fields

You will be able to key **Y** in the **Bypass Security Co**, **Bypass Security Wh**, and/or **Bypass Security Rep** column for those functions that will not be subject to company, warehouse, and/or salesrep authority checking, or (on the lower portion of this screen) you can press **F2=MARK ALL CO, F5=MARK ALL WH**, or **F7=MARK ALL REP** to mark all companies, warehouses, and salesreps. You can use **F4=UNMARK ALL CO, F6=UNMARK ALL WH**, or **F8=UNMARK ALL REP** to unmark all companies, warehouses, and salesreps previously selected for security check omission. The lower portion of this screen also provides filters that allow you to limit the criteria on the screen based on menu, description, application, and type.

Application Function Overrides Screen Fields and Function Keys

Field/Function Key	Description
Bypass Security Co	Use this column to select the functions that will not be subject to company authority checking based on user, user group, or application function (as determined on the Company, Warehouse, and Salesrep Security Screen). Key **Y** next to those functions that will be omitted from company authority checking. You can also press **F2=MARK ALL CO** to mark all companies or **F4=UNMARK ALL CO** to unmark all companies. **Note:** You will notice that not every function has an entry field available. An entry field is provided only if that particular function has company, warehouse, and/or salesrep logic associated with it. (A 1) Optional
Bypass Security Wh	Use this column to select the functions that will not be subject to warehouse authority checking based on user, user group, or application function (as determined on the Company, Warehouse, and Salesrep Security Screen). Key **Y** next to those functions that will be omitted from warehouse authority checking. You can also press **F5=MARK ALL WH** to mark all warehouse or **F6=UNMARK ALL WH** to unmark all warehouses. **Note:** You will notice that not every function has an entry field available. An entry field is provided only if that particular function has company, warehouse, and/or salesrep logic associated with it. (A 1) Optional

Field/Function Key	Description
Bypass Security Rep	Use this column to select the functions that will not be subject to salesrep authority checking based on user, user group, or application function (as determined on the Company, Warehouse, and Salesrep Security Screen). Key **Y** next to those functions that will be omitted from salesrep authority checking. You can also press **F7=MARK ALL REP** to mark all salesreps or **F8=UNMARK ALL REP** to unmark all salesreps. **Note:** You will notice that not every function has an entry field available. An entry field is provided only if that particular function has company, warehouse, and/or salesrep logic associated with it. (A 1) Optional
Menu	Use this field to limit the screen to only those menus that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display menus, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 6) Optional
Description	Use this field to limit the screen to only those functions that match the description you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display those functions, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays limited information. **Note:** This is a character string search and will display menus that match the data anywhere in the **Description** field. (A 30) Optional
App	Use this field to limit the screen to the application you key in this field. Key the application ID and press **ENTER**. The screen will refresh and show only those functions associated with this application ID, if any. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 2) Optional
Type	Use this field to limit the screen to the type of function you key in this field. Key the first letter of the function type and press **ENTER**. The screen will refresh and show only those functions associated with this type of function. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** P-Processing, I-Inquiry, R-Report, M-Maintenance, L-List (A 1) Optional

Field/Function Key	Description
F2=Mark All Co	Press **F2=MARK ALL CO** to bypass company security checks for all application functions for the indicated user, user group or application function (all users). A **Y** will appear in each **Bypass Security Co** field indicating that all functions are marked for omission of company authority checking. If you want most functions marked for omission of company security checks but want to exclude one or a few, simply blank out the **Y** corresponding to the function you do not want marked. **Note:** The **F2=MARK ALL CO** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have marked ALL application functions, verify that there is no data filter active in any of the available filter fields.
F4=Unmark All Co	If you have previously marked to bypass company security checks for application functions and no longer want to omit the security check, press **F4=UNMARK ALL CO** to unmark all companies. **Y** will disappear in each **Bypass Security Co** field. **Note:** The **F4=UNMARK ALL CO** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have unmarked ALL application functions, verify that there is no data filter active in any of the available data fields.
F5=Mark All WH	Press **F5=MARK ALL WH** to bypass warehouse security checks for all application functions for the indicated user, user group or application function (all users). A **Y** will appear in each **Bypass Security WH** field indicating that all functions are marked for omission of warehouse authority checking. If you want most functions marked for omission of warehouse security checks but want to exclude one or a few, simply blank out the **Y** corresponding to the function you do not want marked. **Note:** The **F5=MARK ALL WH** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have marked ALL application functions, verify that there is no data filter active in any of the available filter fields.
F6=Unmark All WH	If you have previously marked to bypass warehouse security checks for application functions and no longer want to omit the security check, press **F6=UNMARK ALL WH** to unmark all warehouses. **Y** will disappear in each **Bypass Security WH** field. **Note:** The **F6=UNMARK ALL WH** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have unmarked ALL application functions, verify the there is no data filter active in any of the available data fields.

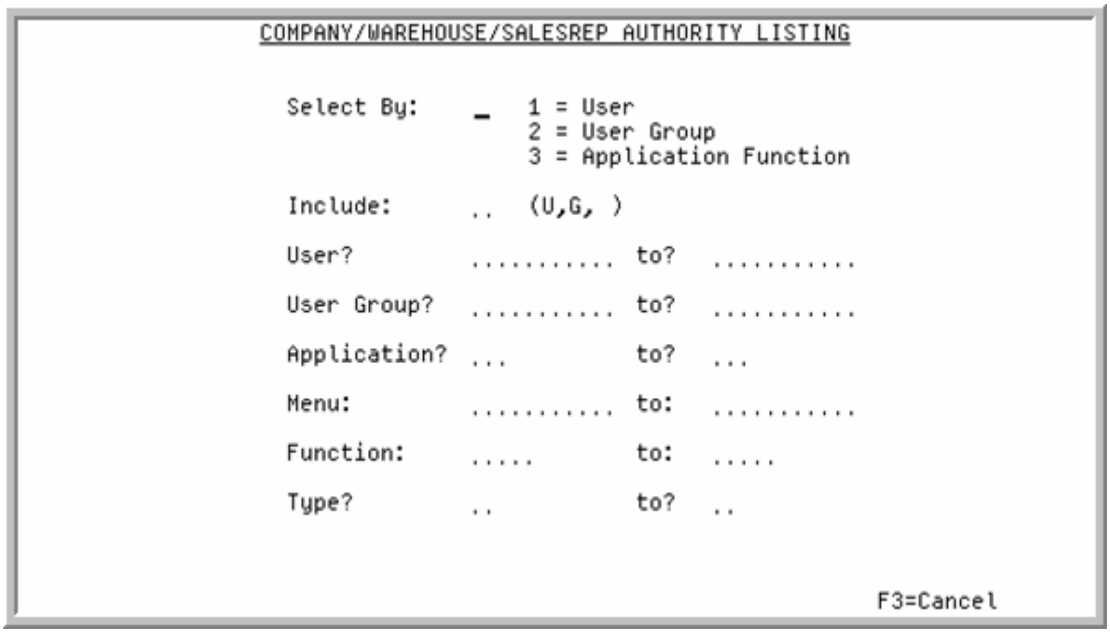
Field/Function Key	Description
F7=Mark All Rep	Press **F7=MARK ALL REP** to bypass salesrep security checks for all application functions for the indicated user, user group or application function (all users). A **Y** will appear in each **Bypass Security Rep** field indicating that all functions are marked for omission of salesrep authority checking. If you want most functions marked for omission of salesrep security checks but want to exclude one or a few, simply blank out the Y corresponding to the function you do not want marked. **Note:** The **F7=MARK ALL REP** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have marked ALL application functions, verify that there is no data filter active in any of the available filter fields.
F8=Unmark All Rep	If you have previously marked to bypass salesrep security checks for application functions and no longer want to omit the security check, press **F8=UNMARK ALL REP** to unmark all salesreps. **Y** will disappear in each **Bypass Security Rep** field. **Note:** The **F8=UNMARK ALL REP** option is based on the data filter information in the available filter fields on the lower portion of this screen. If you want to ensure that you have unmarked ALL application functions, verify the there is no data filter active in any of the available data fields.
F10=Update	After you have selected which functions you want to bypass company, warehouse, and/or salesrep security, press **F10=UPDATE** to confirm your selections. Once **F10=UPDATE** is pressed, the screen refreshes and displays the functions for which company, warehouse, and/or salesrep security will be bypassed. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your selections.

Company/Warehouse/Salesrep Authority Listing

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Company/Warehouse/Salesrep Authority Listing Screen	Used to specify the criteria for which options defined through Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) will print.
Company/Warehouse/Salesrep Authority List	Prints information defined through Company/ Warehouse/Salesrep Authority Maintenance (MENU XASCTY) by User, User Group, or Application Function.

Company/Warehouse/Salesrep Authority Listing Screen



Use this screen to specify the criteria for which options defined through Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) will print.

The Company/Warehouse/Salesrep Authority List will print information by User, User Group, or Application Function. You will be able to enter selection criteria to limit the information to print based on: User, User Group, Application, Menu, Function, and Type. You can also select to include Users only, User Groups only, or both types on the list.

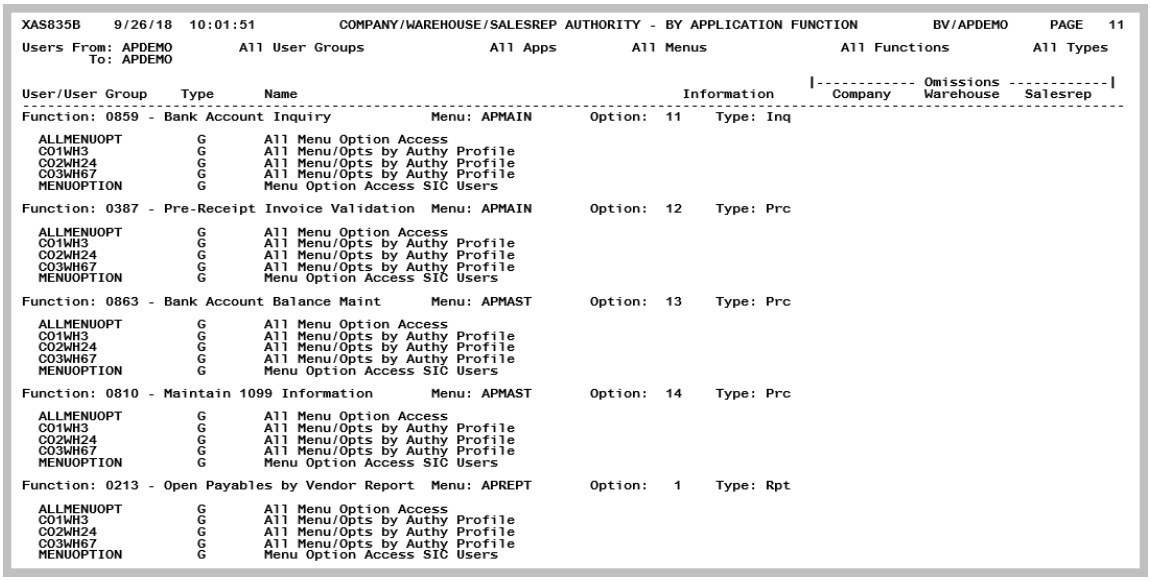
Company/Warehouse/Salesrep Authority Listing Screen Fields and Function Keys

Field/Function Key	Description
Select By	Use this field to select to print company/warehouse/salesrep authorities defined through Company/Warehouse/Salesrep Authority Maintenance (MENU XASCTY) by User, User Group, or Application Function. Key **1** to print the company/warehouse/salesrep authorities profiles a particular user or range of users have authority to use. Key **2** to print the company/warehouse/salesrep authorities profiles a particular user group or range of user groups have authority to use. Key **3** to print each application function (menu option) and the user(s) and/or user group(s) that have authority to use the particular function based on company/warehouse/salesrep authority. (N 1,0) Required

Field/Function Key	Description
Include	If you selected to print the listing by Application Function (the **Select By** field is **3**), use this field to include Users only, User Groups only, or both types for each function (menu option) listed. Key **U** to include Users only. For each application function, the list will print the users that have access to that function. Key **G** to include User Groups only. For each application function, the list will print the user groups that have access to that function. Leave this field blank to include both Users and User Groups. For each application function, the list will print the users and user groups that have access to that function. (A1) Required
User	If you selected to print the listing by User (the **Select By** field is **1**), use this field to limit the listing to one or more users for which company/warehouse/ salesrep authorities will print. Key the user or range of users to be included on the listing. (2@A10) Optional
User Group	If you selected to print the listing by User Group (the **Select By** field is **2**), use this field to limit the listing to one or more user groups for which company/warehouse/salesrep authorities will print. Key the user group or range of user groups to be included on the listing. (2@A10) Optional
Application	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the application or range of applications you select. Key the application ID or range of application IDs to be included on this listing. For example, if you want only Accounts Payable company/ warehouse/salesrep information printed, key AP in this field. (2@A10) Optional
Menu	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the menu or range of menus you select. Key the menu or range of menus to be included on this listing. For example, if you want only payment check information printed, key APCHCK (for MENU APCHCK options) in this field. (2@A6) Optional

Field/Function Key	Description
Function	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the function number or range of function numbers you select. Key the function number or range of functions numbers to be included on this listing. For example, if you want only function number 0134 included on this listing, key that number in this field. (2@A4) Optional
Types	Regardless of how you selected to print this listing (by User, User Group, or Application Function), use this field to limit the listing to the function type or range of function types you select. Key the function type or range of function types to be included on this listing. For example, if you want only inquiry function types printed, key I (I=Inquiry) in this field. (2@A1) Optional
F3=Cancel	Press **F3=CANCEL** this key to cancel the listing and return to the menu.
Enter	Press **ENTER** to confirm your entries. The Report Options Screen display

Company/Warehouse/Salesrep Authority List



```
XAS835B    9/26/18  10:01:51          COMPANY/WAREHOUSE/SALESREP AUTHORITY - BY APPLICATION FUNCTION          BV/APDEMO     PAGE   11

Users From: APDEMO        All User Groups              All Apps         All Menus               All Functions          All Types
        To: APDEMO

                                                                                                |------------ Omissions ------------|
User/User Group    Type      Name                                                  Information      Company    Warehouse   Salesrep
-------------------------------------------------------------------------------------------------------------------------------------
Function: 0859 - Bank Account Inquiry            Menu: APMAIN       Option:  11    Type: Inq

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0387 - Pre-Receipt Invoice Validation  Menu: APMAIN       Option:  12    Type: Prc

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0863 - Bank Account Balance Maint      Menu: APMAST       Option:  13    Type: Prc

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0810 - Maintain 1099 Information       Menu: APMAST       Option:  14    Type: Prc

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users

Function: 0213 - Open Payables by Vendor Report  Menu: APREPT       Option:   1    Type: Rpt

  ALLMENUOPT         G       All Menu Option Access
  CO1WH3             G       All Menu/Opts by Authy Profile
  CO2WH24            G       All Menu/Opts by Authy Profile
  CO3WH67            G       All Menu/Opts by Authy Profile
  MENUOPTION         G       Menu Option Access SIC Users
```

The listing prints information by User, User Group, or Application Function. On the Company, Warehouse, and Salesrep Security Screen, you will be able to enter selection criteria to limit the information to print based on: User, User Group, Application, Menu, Function, and Type.

Use this listing to view what users may be coded for company, warehouse, and/or salesrep security bypasses.

Chapter 8 Application Action Authority Maintenance/Listing

This option allows you to define authorization for specific application actions. Application action authorities are sub-tasks of a function. For example, a function is Enter, Change & Ship Orders (MENU OEMAIN), which provides you with the ability to create new orders, change existing orders and to perform shipping confirmation on an order (all of which are sub-tasks of the function). These orders could be regular customer orders, return orders, special orders or invoices (to name a few examples). Through this option you can sub-divide the features and define authority to these sub-divisions, giving some users authority to enter new customer orders and other users the authority to enter returns, etc.

Use this option to define which users will have access to perform a given application action by selecting users and/or user groups for each application action available for each company defined to the Distribution A+ system. You will have the option to designate the function to be available to all users, no users, only master users or selected users and/or user groups.

Application action authorities are defined through Application Action Authority Maintenance on the Distribution A+ Security Menu (MENU XASCTY).

For a description of the application actions, see APPENDIX C: Application Action Authorities.

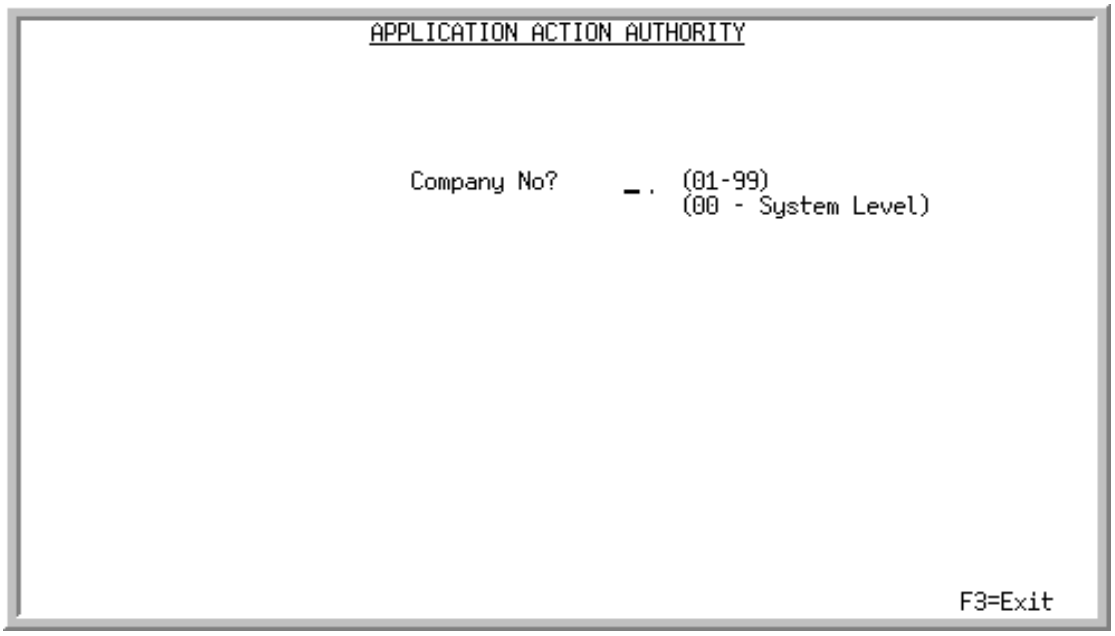
Application Action Authority Maintenance

The screens and/or reports in this option and a brief description of their purpose are listed in the following table. A complete description of each is provided in this section.

Title	Purpose
Application Action Authority Screen	Use to specify the company number for which you are creating/maintaining company level application action authorities, or to create/maintain system level application action authorities.
Application Action Authority Selection Screen	Used to review a list of available application actions from which you can select to define authorities for the application actions.

Title	Purpose
Define Application Action Authority Screen	Used to define authorities for the indicated application action.
Assign Users Screen	Used to assign users to the indicated application action. This screen is shown in User Group Maintenance (MENU XASCTY). Refer to the Assign Users Screen in that chapter for details.
Assign User Groups Screen	Used to assign user groups to the indicated application action.
Application Action Instances Screen	Used to select the extended instance available for the application action, if one is available.
Define Extended Instance Screen	Used to set up extended instances for a particular application action.

Application Action Authority Screen

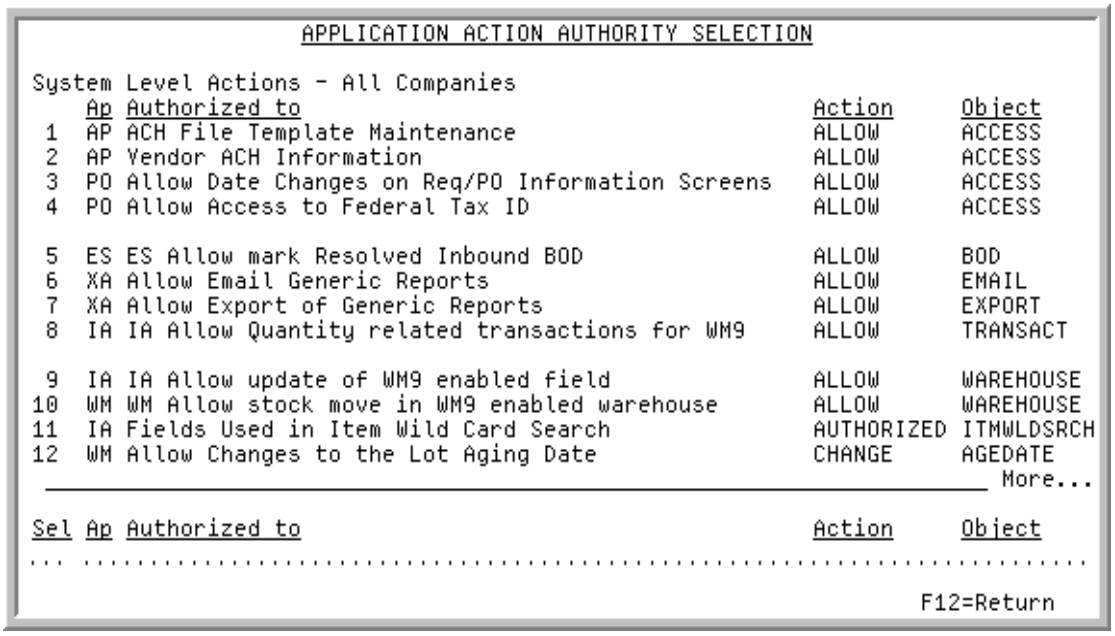


This screen displays after selecting Application Action Authority Maintenance from MENU XASCTY. Use this screen to specify the company number for which you are creating/maintaining system or company level application action authorities.

Application Action Authority Screen Fields and Function Keys

Field/Function Key	Description
Company No	This field is used to specify the level (company or system), of the application action authorities to be created or maintained. Key the company number for which you are creating/maintaining company level application action authorities. Leave this field blank or key **00** to create/maintain system level application action authorities. **Valid Values:** 00 or blank for system level application action authorities; a valid company number defined through Company Name Maintenance (MENU XAFILE) which you are authorized to access through Authority Profile Maintenance (MENU XASCTY). (N 2,0) Required/Optional
F3=Exit	Press **F3=EXIT** to exit from this screen.
Enter	Press **ENTER** to confirm your entry and proceed to the Application Action Authority Selection Screen.

Application Action Authority Selection Screen



This screen displays after entering a company number or specifying system level options on the Application Action Authority Screen. The application actions that display on this screen are different depending on if you are creating/maintaining company level or system level application action authorities.

Use this screen to define authorization for the application action you select. Once you select an application action, the Define Application Action Authority Screen displays, where you can designate who will be authorized to use the application action (all users, master users only, selected users, or no users). For a description of the application actions, see APPENDIX C: Application Action Authorities.

You can also limit this screen to particular application actions based on filter criteria you enter in the **Ap**, **Authorized to**, **Action** and **Object** filter fields on the lower portion of this screen.

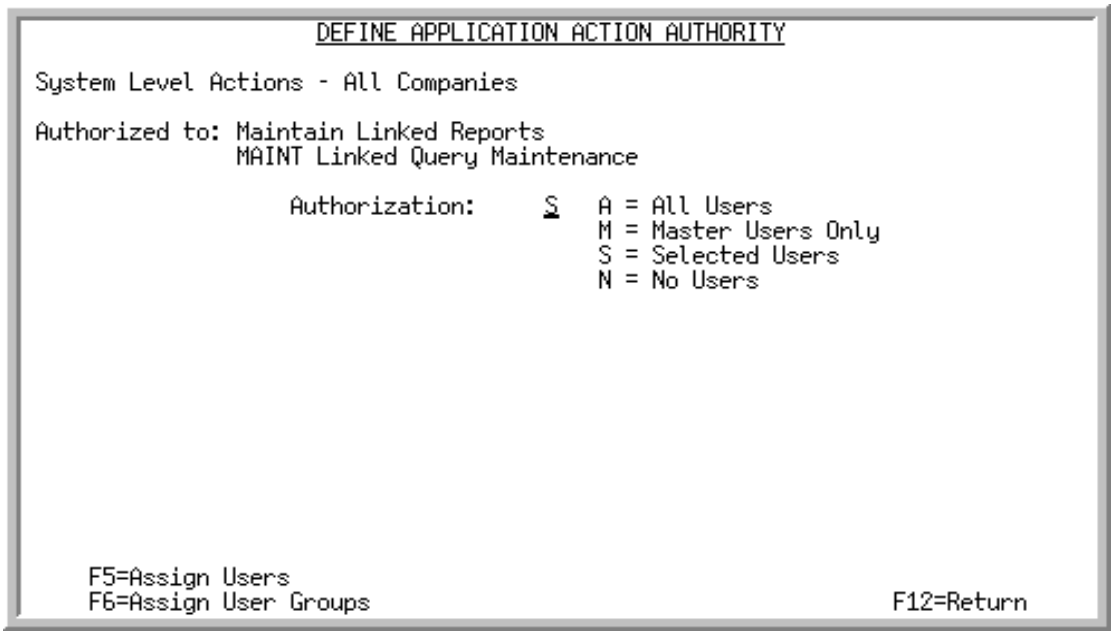
Application Action Authority Selection Screen Fields and Function Keys

Field/Function Key	Description
(Level)	If you entered a company number on the Application Action Authority Screen, the selected company number and name is displayed on the top left corner of this screen. If you entered **00** or left the company number field blank on the Application Action Authority Screen, **System Level Actions - All Companies** is displayed on the top left corner of this screen. Display

Field/Function Key	Description
(Reference Number)	The reference number of the application actions authorities displayed on this screen. This number is **1** through **12** for the twelve authorities that may display. When rolling forward or backward, the reference numbers do not change. Display
Ap	The 2-position common abbreviation for the Distribution A+ application module (e.g. OE for Order Entry). Display
Authorized To	The application action for which you are defining authorities. Display
Action	The specific action that this authorization enables (e.g., Enter). Display
Object	The object that this authorization reflects (e.g., Order). Display
Sel	Use this field to select an existing application action you want to create/ maintain authorizations for. Key the corresponding **Reference Number** of the application action you want to choose, and press **ENTER** to proceed to the next screen. (N 2,0) Optional
Ap	Use this field to limit the screen to only those application actions associated with the application ID you key in this field. To limit the screen to only application actions associated with a particular application, key the ID of the application and press **ENTER**. The screen will refresh and display application actions, if any, matching the application you entered. For example, to display only application actions associated with the Order Entry application, key OE in this field. **Valid Values:** AR, EP, IA, OE, PO, XA, WO (A 2) Optional
Authorized to	This is a description of the application action. Use this field to limit the screen to only those application actions that match the authority criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display application actions, if any, matching your criteria. **Note:** This is a character string search and will display application actions that match the data anywhere in the **Authorized to** field. (A 40) Optional

Field/Function Key	Description
Action	Use this field to limit the screen to only those application actions that match the criteria you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those application actions that pertain to release functions, key release in this field. The screen will refresh and display application actions, if any, matching your criteria. **Valid Values:** Add, Allow, Authorized, Change, Copy, Delete, Display, Enter, Maintain, Override, Release, Reprice, Reprint, Return, Run, Shpconfirm, Work. (A 10) Optional
Object	Use this field to limit the screen to only those application actions that match the object ID you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those application actions that pertain to an order, key **ORDER** in this field. The screen will refresh and display application actions, if any, matching your criteria. **Valid Values:** COMPANY LEVEL: abr, altstore, ccauthmode, ccinquiry, ccnbrinq, ccstatus, comments, contrcalc, cost, costloadw, credlim, cstprf, customer, deposit, droppull, dropship, epmaintacc, epmaintcc, gm, header, invoice, line, nosale, oeord, order, origorder, override, pickdel, picklist, price, pricelist, priority, qtyord, qtyovr, quantity, quickpay, rbtdsp, return, rushpo, shipto, shpdate, slowpay, sochgreq, specord, storecred, threads, voucher, willcall. SYSTEM LEVELL: access, agedate, bod, ccinquiry, dayend, email, export, itmwldsrch, linked, maxrecall, rebate. (A 10) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display application actions, if any, matching your criteria. After entering a **Reference Number** of an application action in the **Sel** field, press **ENTER** to confirm your entry. The Define Application Action Authority Screen displays, where you can designate who will be authorized to use the application action (all users, master users only, selected users, or no users).

Define Application Action Authority Screen



This screen displays after entering a **Reference Number** in the **Sel** field and pressing **ENTER** on the Application Action Authority Selection Screen or from Application Action Instances Screen.

Use this screen to create/maintain user authorization for the selected application action shown in the **Authorized to** field on the top portion of this screen. Only the users and/or user groups you designate will be authorized to perform the application action shown on this screen. If an extended instance exists for the application action, it will display below the application action. For a description of the application actions and extended instances, see APPENDIX C: Application Action Authorities.

You can assign both users and user groups simultaneously to an application action. To assign specific users and/or user groups, use the **F5=ASSIGN USERS** or **F6=ASSIGN USER GROUPS** function key when the **Authorization** type is set to **S**.

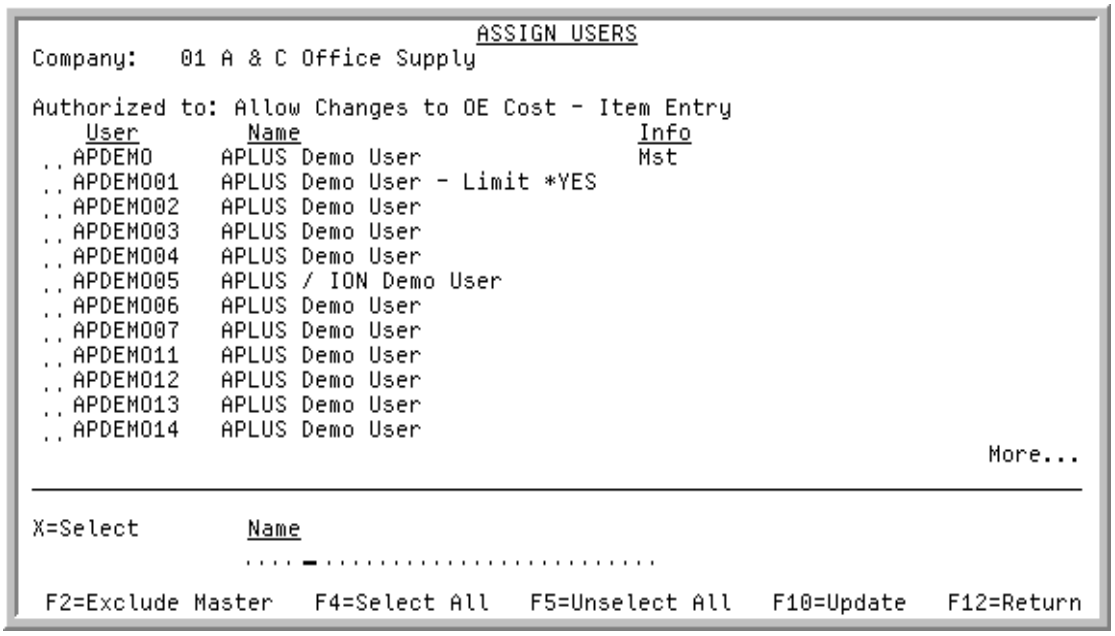
Important: If you key **S** in the **Authorization** field on this screen and press **ENTER** (without pressing **F5=ASSIGN USERS** or **F6=ASSIGN USER GROUPS**), only Master users will be authorized to this application action. If you previously keyed **S** in the **Authorization** field and pressed **F5=ASSIGN USERS** and/or **F6=ASSIGN USER GROUPS** to assign users and/or user groups, then you changed the **Authorization** field to **A** (for All Users), **M** (for Master Users Only), or **N** (for No Users), and then you change the **Authorization** field back to **S** (for Selected Users), you do not need to reselect **F5=ASSIGN USERS** and/or **F6=ASSIGN USER GROUPS** since the users/user groups you previously selected still exist.

Define Application Action Authority Screen Fields and Function keys

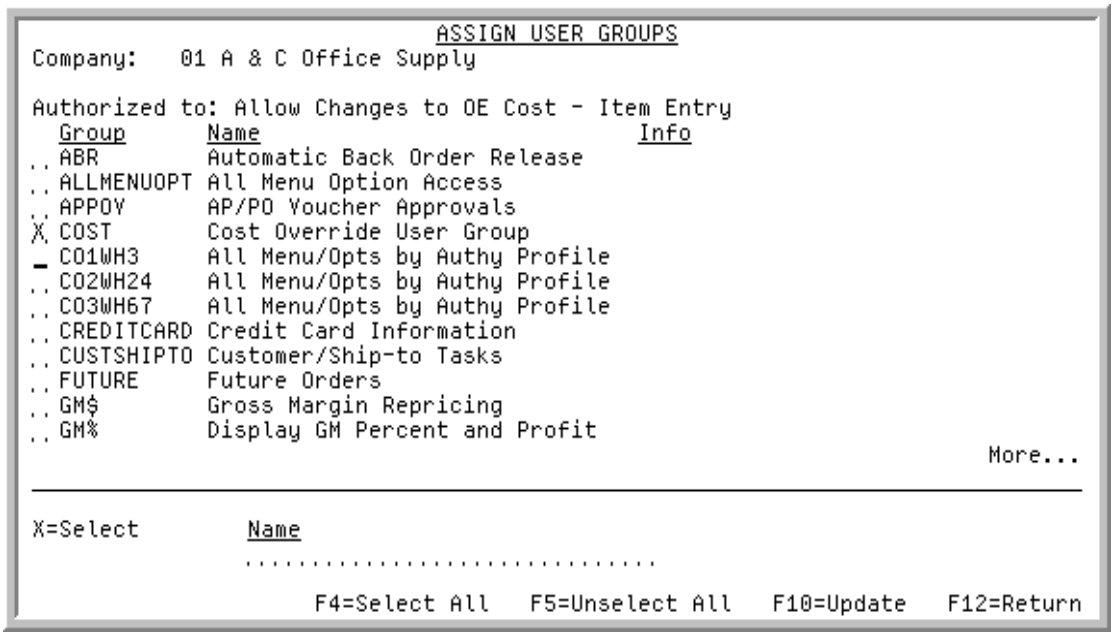
Field/Function Key	Description
Authorization	Use this field to determine who will be allowed access to the indicated application action. This field can be changed at a later date, if you need to reset authorizations. Key **A** if you want all users that reside in the Distribution A+ User File to have access to the application action. Users are defined through User Maintenance (MENU XASCTY). Key **M** if you want only users defined as Master users to to have access to the application action. Users are defined as Master users through User Maintenance (MENU XASCTY) or Authority Profile Maintenance (MENU XASCTY). Key **S** if you want to select specific users and/or user groups to have access to the application action. To select users, after keying **S**, press **F5=ASSIGN USERS** to assign the users. To select user groups, after keying **S**, press **F6=ASSIGN USER GROUPS** to assign the groups. **Note:** If you select **S**, Master users will also have authority to perform the application action, even if they were not selected via the **F5=ASSIGN USERS** and/or **F6=ASSIGN USER GROUPS** function keys. Key **N** if you do not want anyone (not even a Master user) to have access to the application action. For example, if you do not want to use the Gross Margin Pricing functionality, and you chose that as the application action for which you are creating/maintaining authorizations, key **N** in this field. The application action will be disabled, and no one will be able to perform the functionality, so be sure you consider your business needs prior to keying **N** in this field. (A 1) Required
F5=Assign Users	After keying **S** in the **Authorization** field, press **F5=ASSIGN USERS** to access the Assign Users Screen, which displays existing user information. From the Assign Users Screen, you can select the users you want assigned to the application action. In addition to any user groups assigned via **F6=ASSIGN USER GROUPS** and any Master users, the users you select on the Assign Users Screen will be authorized.

Field/Function Key	Description
F6=Assign User Groups	After keying **S** in the **Authorization** field, press **F6=ASSIGN USER GROUPS** to access the Assign User Groups Screen, which displays existing user group information. From the Assign User Groups Screen, you can select the user groups you want assigned to the application action. In addition to any users assigned via **F5=ASSIGN USERS** and any Master users, users in the user groups you select on the Assign User Groups Screen will be authorized.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entry.
Enter	Press **ENTER** to confirm your entry and proceed to the next screen.

Assign Users Screen



Assign User Groups Screen



The Assign Users Screen displays when you press **F5=USERS** on the Define Application Action Authority Screen. The Assign User Groups Screen displays when you press **F6=USER GROUPS** on the Define Application Action Authority Screen.

The lower portion of this screen allows you to limit the screen to show only user/user groups that match the criteria you key in the **Name** field.

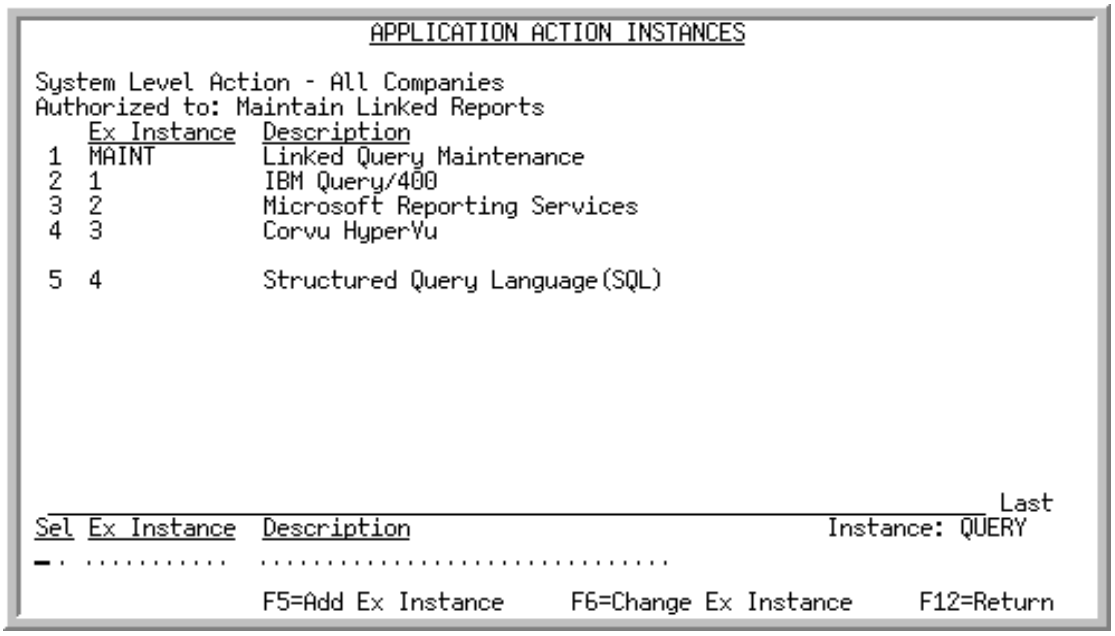
Assign Users and Assign User Groups Screen Fields and Function keys

Field/Function Key	Description
Company	If you entered a company number on the Application Action Authority Screen, the selected company number and name is displayed on the top left corner of this screen. If you entered **00** or left the company number field blank on the Application Action Authority Screen, **System Level Actions - All Companies** is displayed on the top left corner of this screen. Display
Authorized To	This is a description of the selected application action. Display
User or Group	The user ID or the user group selected. Display
Name	The name assigned to the User ID or the description of the user group. Display
Info	For users that are identified as master users (**Master User Authority** field is **Y**), **Mst** displays in this column. Displayed
X=Select	Use this field to assign user group(s) to the indicated application action. On the top portion of the screen, key **X** in the column corresponding to the user groups you want to select and press **F10=UPDATE** to update. A message will display informing you that the indicated user groups will be authorized to the application action. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**. To unselect any user groups assigned to the application action, simply blank out the **X** next to the group you no longer want assigned to the application action and press **F10=UPDATE** to update. (A 1) Optional

Field/Function Key	Description
Name	Use this field to limit the screen to only those user groups that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display user groups, if any, matching your criteria. **Note:** This is a character string search and will display user group names that match the data anywhere in the **Name** field. (A 30) Optional
F4=Select All	Press **F4=SELECT ALL** to assign all user groups to the current application action. An **X** will appear in the left column before all Group IDs. If you want to assign most user groups to the application action and want to exclude only one or a few, after selecting all, you can then simply blank out the **X** in the column before the Group ID(s) you do not want to include. **Note:** The Select All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your **list** of user group names and you wanted only these two groups to be authorized to this application action. You would filter to the word 'credit' and then press **F4=SELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the user groups you selected based on the 'credit' filter. If you want to ensure that you have selected ALL user groups, verify that there is no data filter active in the **Name** field before using this key.
F5=UnSelect All	Press **F5=UNSELECT ALL** to unselect all user groups from the current application action. All **X**'s will disappear in the left column before all Group IDs. If you want to assign only a few user groups to the application action, after unselecting all, you can then simply key **X** in the column before the Group ID(s) you want to assign to the application action. **Note:** The Unselect All option is based on the data filter information in the **Name** field. For example, assume you have two user groups labeled credit hold and credit warning in your list of user group names and wanted to remove authorization to the application action from only these two groups. You would filter to the word 'credit' and then press **F5=UNSELECT ALL**. When you then press **F10=UPDATE**, your confirmation list will show the user groups remaining based on the credit filter. If you want to ensure that you have Unselected ALL user groups, verify that there is no data filter active in the **Name** field before using this key.

Field/Function Key	Description
F10=Update	After you have selected the groups to assign to the application action, press **F10=UPDATE** to confirm your selections. Once **F10=UPDATE** is pressed, only the user groups you selected are shown on the screen and a message displays informing you that the groups you selected will be assigned to the application action. You will have the option to confirm your selections by pressing **ENTER** or make more changes by pressing **F12=RETURN**.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	After keying filter criteria in the **Name** field, press **ENTER**. The screen will refresh and display user groups, if any, matching your criteria.

Application Action Instances Screen



This screen only displays if the application action you selected on the Application Action Authority Selection Screen has an extended instance associated with it. Extended instances are set up for an application action on the Define Extended Instance Screen.

This screen displays extended instances that are available for the application action. Use this screen to select an extended instance for the indicated application action, further defining the application action. For example, if the application action is Allow the Release of Held Orders, you will add extended instances for all new user hold codes and then authorize users and/or user groups to those hold code extended instances. This application action would then require that you further define its user authority on the extended instance level (in this example, for each specific hold code).

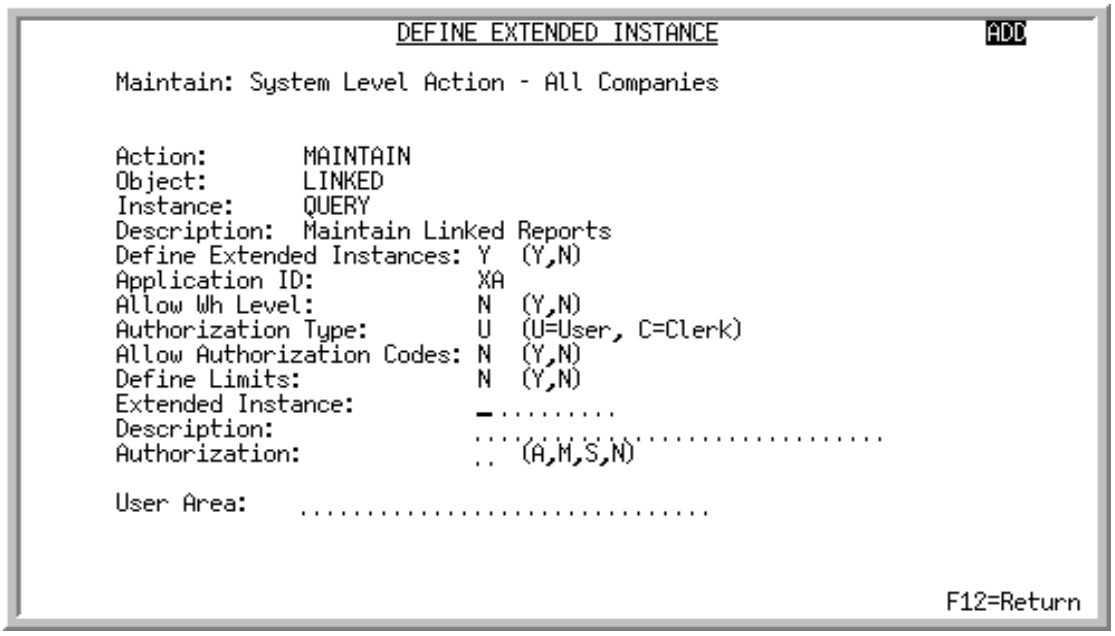
For a list of extended instances that are available for each application action, see APPENDIX C: Application Action Authorities.

Application Action Instances Screen Fields and Function keys

Field/Function Key	Description
(Level)	If you entered a company number on the Application Action Authority Screen, the selected company number and name is displayed on the top left corner of this screen. If you entered **00** or left the company number field blank on the Application Action Authority Screen, **System Level Actions - All Companies** is displayed on the top left corner of this screen.
	Display

Field/Function Key	Description
Authorized To	This is a description of the selected application action. Display
Sel	Use this field to select an existing extended instance. Key the corresponding selection number of the extended instance you want to choose, and press **ENTER** to proceed to the next screen. (N 2,0) Optional
Ex Instance	Use this field to limit the screen to only those extended instances that match the extended instance ID you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display instances, if any, matching your criteria. (A 10) Optional
Description	Use this field to limit the screen to only those extended instances that match the extended instance description you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display instances, if any, matching your criteria. **Note:** This is a character string search and will display instances that match the data anywhere in the **Description** field. (A 30) Optional
Instance	This field displays the instance for this application action, showing you what type of data the extended instances will be. Display
F5=Add Ex Instance	Press **F5=ADD EX INSTANCE** to add a new extended instance for the application action. The Define Extended Instance Screen displays.
F6=Change Ex Instance	After selecting an existing extended instance in the **Sel** field, press **F6=CHANGE EX INSTANCE** to maintain the extended instance defined for the application action. The Define Extended Instance Screen displays.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
Enter	After keying filter criteria on this screen, press **ENTER**. The screen will refresh and display extended instances, if any, matching your criteria.

Define Extended Instance Screen



This screen displays after pressing either **F5=ADD EX INSTANCE** or **F6=CHANGE EX INSTANCE** on the Application Action Instances Screen. Use this screen to set up or maintain extended instances for a particular application action. If you are adding a new extended instance, the **Extended Instance**, **Description**, **Authorization** and **User Area** fields will be available. If you are changing an existing extended instance, the **Description**, **Authorization** and **User Area** fields will be available. **F24=DELETE** is only available in Change mode.

Note: For the company level **Allow the Release of Held Orders** action authority, the six system-generated hold codes (CR, SP, GM, GX, NC, OH) will automatically have Application Action Authority Extended Instances established for Master User access.

Define Extended Instance Screen Fields and Function keys

Field/Function Key	Description
Action	This field displays the authority action. For a list of valid actions, refer to the **Actio**n field on the Application Action Authority Selection Screen. Display
Object	This field displays the authority object. For a list of valid objects, refer to the **Object** field on the Application Action Authority Selection Screen. Display

Field/Function Key	Description
Instance	This field displays the Instance, further describing the application action. For example, if the application action is pertaining to the releasing of a held order, the instance is Hold Code. Display
Description	This field displays the description of the application action for which you are defining/maintaining extended instances. The description of the application action is what you will see through this menu option when you are determining authorities. Display
Define Extended Instances	This field displays **Y** if this application action requires an extended instance to be defined. This field displays **N** if this application action does not require an extended instance to be defined. Display
Application ID	This field displays the 2-character ID of the application the action is associated with. For example, if the application action is performed through Order Entry, OE displays in this field. **Note:** The Application ID is also a filter field in various places and can be used to limit the application actions that display based on the ID you key. Display
Allow WH Level	If authorities for this application action will be allowed on the warehouse level, **Y** displays in this field. If authorities for this application action will not be allowed on the warehouse level, **N** displays in this field. Display
Authorization Type	This field displays **U** if the authorization you are defining is for a User. This field displays **C** if the authorization you are defining is for a Clerk. Display
Allow Authorization Codes	This field displays **Y** if authorization codes will be allowed. For security reasons, authorization codes may be set up for an application action and in addition to user/clerk authorities, authorization codes can provide a user/clerk access to an application action. This field displays **N** if authorization codes will not be allowed. Display

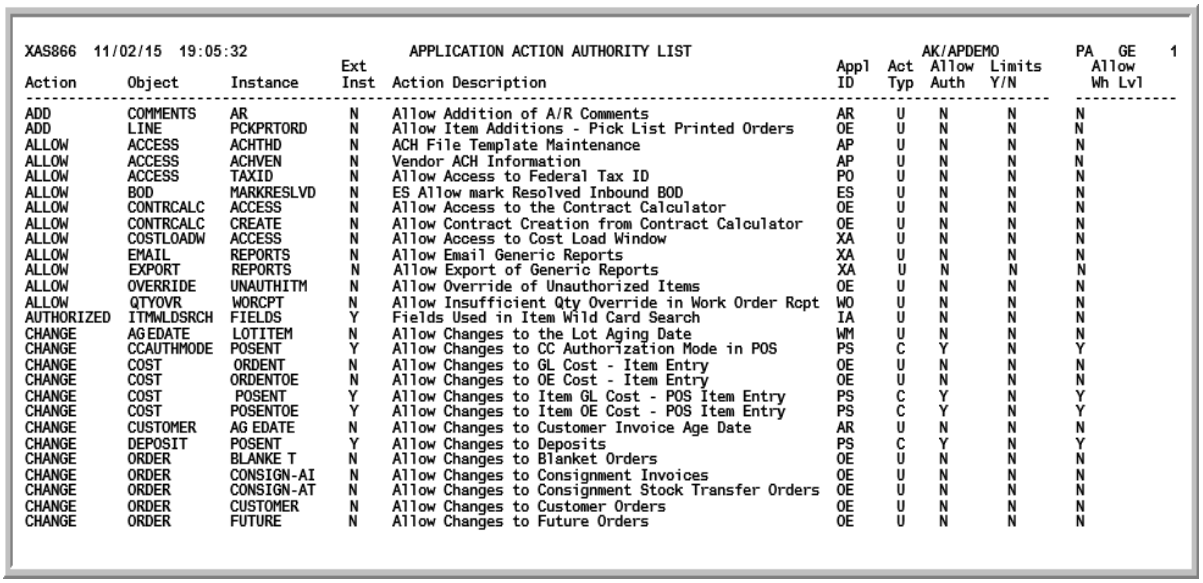
Field/Function Key	Description
Define Limits	Certain application actions may require limits of percentage or currency to the authority of the application action. For example, in Point of Sale you might have the authority to override the price of an item but only for the limit that is defined. If the minimum limit defined is $20.00 and the item costs $100.00, you can override the price down to $80.00. This field displays **Y** if limits can be defined for the application action. This field displays **N** if limits cannot be defined for the application action. Display
Extended Instance	In Change mode, this field is display-only and shows the extended instance previously defined for the application action. You will be allowed to change the **Description**, **Authorization** and **User Area** fields or delete the extended instance using **F24=DELETE**. In Add mode, use this field to key the extended instance you want to define for the application action. For example, if the application action is pertaining to the releasing of a held order, the extended instance might be SP for Slow Pay Hold. Meaning, allow the release of held orders only if they are on slow pay hold. **Note:** The extended instance you add must be a valid value of the actual field that the instance refers to. For example, if the instance is Hold Code, the extended instance must be an actual valid value of the hold codes you already defined. (A 10) Display/Required
Description	Use this field to key (add or change) a description for the extended instance. For example, if the application action is pertaining to the releasing of a held order, the extended instance might be SP, and the description might be Slow Pay Hold. (A 30) Required
Authorization	Use this field to designate if the authorization pertains to All Users (key **A**), Master Users only (key **M**), Selected Users (key **S**), or No Users (key **N**). For further details, refer to the **Authorization** field on the Define Application Action Authority Screen. (A 1) Required
User Area	This space is provided for additional information. Use this field to key any notes that you want associated with the extended instance. (A 30) Optional

Field/Function Key	Description
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entries.
F24=Delete	The **F24=DELETE** function key only displays in the Change mode. Press **F24=DELETE** to delete the extended instance for the application action. You will be returned to the previous screen.
Enter	Press **ENTER** to confirm your entries and return to the previous screen.

Application Action Authority List

Once you have defined your application action authorities, you can print a listing of those action authorities through the Application Action Authority Listing option on the Distribution A+ Security Menu (MENU XASCTY).

Application Action Authority List



XAS866 11/02/15 19:05:32 APPLICATION ACTION AUTHORITY LIST AK/APDEMO PA GE 1

Action	Object	Instance	Ext Inst	Action Description	Appl ID	Act Typ	Allow Auth	Limits Y/N		Allow Wh Lvl
ADD	COMMENTS	AR	N	Allow Addition of A/R Comments	AR	U	N	N		N
ADD	LINE	PCKPRTORD	N	Allow Item Additions - Pick List Printed Orders	OE	U	N	N		N
ALLOW	ACCESS	ACHTHD	N	ACH File Template Maintenance	AP	U	N	N		N
ALLOW	ACCESS	ACHVEN	N	Vendor ACH Information	AP	U	N	N		N
ALLOW	ACCESS	TAXID	N	Allow Access to Federal Tax ID	PO	U	N	N		N
ALLOW	BOD	MARKRESLVD	N	ES Allow mark Resolved Inbound BOD	ES	U	N	N		N
ALLOW	CONTRCALC	ACCESS	N	Allow Access to the Contract Calculator	OE	U	N	N		N
ALLOW	CONTRCALC	CREATE	N	Allow Contract Creation from Contract Calculator	OE	U	N	N		N
ALLOW	COSTLOADW	ACCESS	N	Allow Access to Cost Load Window	XA	U	N	N		N
ALLOW	EMAIL	REPORTS	N	Allow Email Generic Reports	XA	U	N	N		N
ALLOW	EXPORT	REPORTS	N	Allow Export of Generic Reports	XA	U	N	N		N
ALLOW	OVERRIDE	UNAUTHITM	N	Allow Override of Unauthorized Items	OE	U	N	N		N
ALLOW	QTYOVR	WORCPT	N	Allow Insufficient Qty Override in Work Order Rcpt	WO	U	N	N		N
AUTHORIZED	ITMWLDSRCH	FIELDS	Y	Fields Used in Item Wild Card Search	IA	U	N	N		N
CHANGE	AGEDATE	LOTITEM	N	Allow Changes to the Lot Aging Date	WM	U	N	N		N
CHANGE	CCAUTHMODE	POSENT	Y	Allow Changes to CC Authorization Mode in POS	PS	C	Y	N		Y
CHANGE	COST	ORDENT	N	Allow Changes to GL Cost - Item Entry	OE	U	N	N		N
CHANGE	COST	ORDENTOE	N	Allow Changes to OE Cost - Item Entry	OE	U	N	N		N
CHANGE	COST	POSENT	Y	Allow Changes to Item GL Cost - POS Item Entry	PS	C	Y	N		Y
CHANGE	COST	POSENTOE	Y	Allow Changes to Item OE Cost - POS Item Entry	PS	C	Y	N		Y
CHANGE	CUSTOMER	AGEDATE	N	Allow Changes to Customer Invoice Age Date	AR	U	N	N		N
CHANGE	DEPOSIT	POSENT	Y	Allow Changes to Deposits	PS	C	Y	N		Y
CHANGE	ORDER	BLANKET	N	Allow Changes to Blanket Orders	OE	U	N	N		N
CHANGE	ORDER	CONSIGN-AI	N	Allow Changes to Consignment Invoices	OE	U	N	N		N
CHANGE	ORDER	CONSIGN-AT	N	Allow Changes to Consignment Stock Transfer Orders	OE	U	N	N		N
CHANGE	ORDER	CUSTOMER	N	Allow Changes to Customer Orders	OE	U	N	N		N
CHANGE	ORDER	FUTURE	N	Allow Changes to Future Orders	OE	U	N	N		N

This listing prints application action authorities defined through Application Action Authority Maintenance (MENU XASCTY).

Chapter 9 Authorization Codes Maintenance/Listing

Use Authorization Codes Maintenance to define authorization codes that you can associate with particular actions. Authorization codes provide an alternate method for providing access to a secured action. When you define authorization codes, you are creating codes that are used to permit overrides in specific situations, such as to authorize the cancellation of an order for a clerk who does not have authority to cancel an order.

If a user is attempting to perform an action that he/she is not authorized to perform, and an authorization code has been set up for the particular action, an Authorization pop-up window will display prompting the user to enter a valid authorization code to continue. If the user is aware of the code, he/she will be granted authority to the secured action.

Authorization codes are defined through Authorization Codes Maintenance on the Distribution A+ Security Menu (MENU XASCTY) or the Point of Sale File Maintenance Menu (MENU PSFILE).

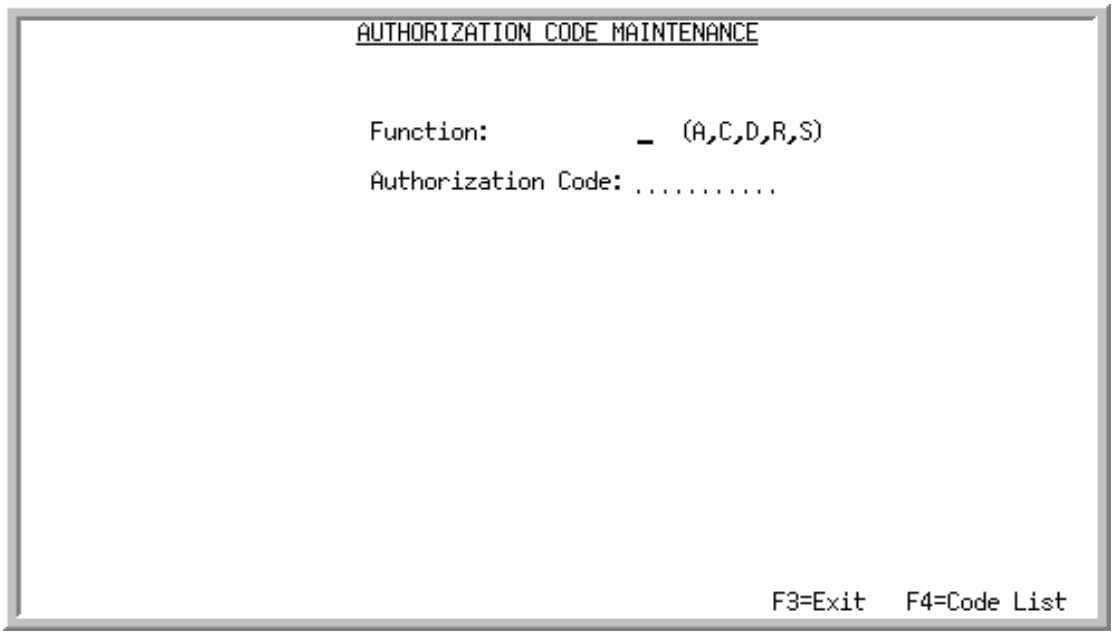
Authorization Codes Maintenance

The screens and/or reports in this option and a brief description are listed in the following table. A complete description of each screen/report is contained in this section.

Title	Purpose
Authorization Code Maintenance Screen	Used to specify the authorization code that you want to maintain.
Authorization Code List Screen	Used to select an existing authorization code to maintain.
Authorization Code Definition Screen	Used to define an authorization code.
Authorization Code Action Authority Review Screen	Used to display a list of authority actions that the indicated authorization code is associated with.
Application Action Authority Screen	Used to select an action to be authorized by the indicated authorization code (or clerk or clerk group if this screen is being accessed from Point of Sale).

Title	Purpose
Variance Limits Screen	Used to define limits for the actions selected for the indicated authorization code.

Authorization Code Maintenance Screen



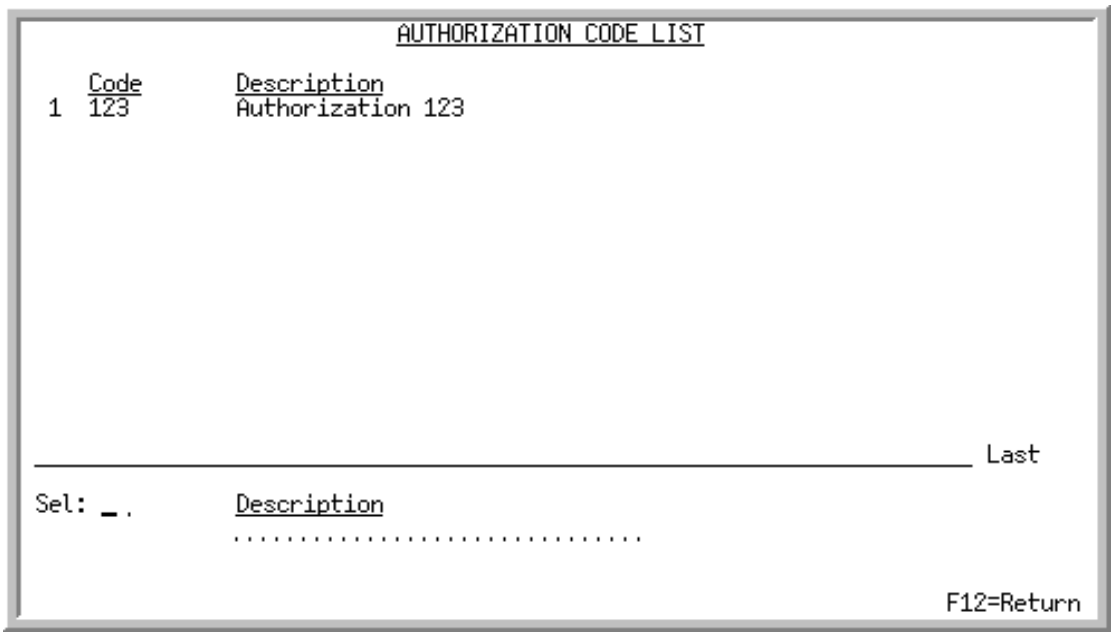
Use this screen to specify the authorization code that you want to maintain. To display a list of existing authorization codes, press **F4=CODE LIST**.

Authorization Code Maintenance Screen Fields and Function Keys

Field/Function Key	Description
Function	Use this field to add, change, delete, reinstate or suspend an authorization code. Key **A** to add an authorization code. Key **C** to change an existing authorization code. Key **D** to delete an existing authorization code (that is not used by any actions). You will be prompted to confirm deletion when you key this option. Key **R** to reinstate an authorization code that has been suspended. You will be prompted to confirm action when you key this option. Key **S** to suspend an authorization code. You will be prompted to confirm action when you key this option. (A 1) Required
Authorization Code	Use this field to enter the authorization code you are adding, changing, deleting, reinstating, or suspending. (A 10) Required

Field/Function Key	Description
F3=Exit	Press **F3=EXIT** to exit from this screen.
F4=Code List	Press **F4=CODE LIST** to access the Authorization Code List Screen, which displays existing authorization codes.
Enter	Press **ENTER** to confirm your entries and proceed to the Authorization Code Definition Screen.

Authorization Code List Screen



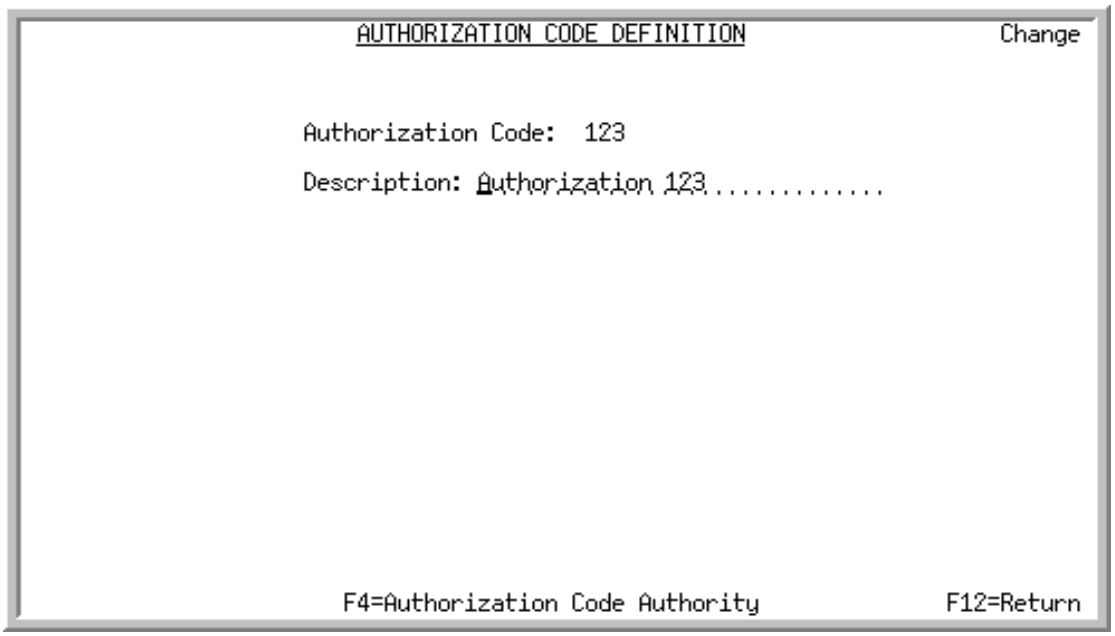
This screen displays existing authorization codes. The top portion of this screen displays the authorization code and the description of the code. On the lower portion of this screen, you can select an authorization code to maintain by entering the code's selection number in the **Sel** field. You can also limit the screen to show only authorization codes that match the criteria you key in the **Description** field.

Authorization Code List Screen Fields and Function keys

Field/Function Key	Description
Sel	Use this field to select an existing authorization code to maintain. Key the corresponding selection number of the code you want to maintain and press **ENTER**. (N2,0) Optional
Description	Use this field to limit the screen to only those authorization codes that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display authorization codes, if any, matching your criteria. **Note:** This is a character string search and will display codes that match the data anywhere in the **Description** field. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without confirming your entries.

Field/Function Key	Description
Enter	Press **ENTER** to confirm your selection and proceed to the next screen. If you keyed criteria in the **Description** field, the screen refreshes and displays the authorization codes that match the criteria entered.

Authorization Code Definition Screen

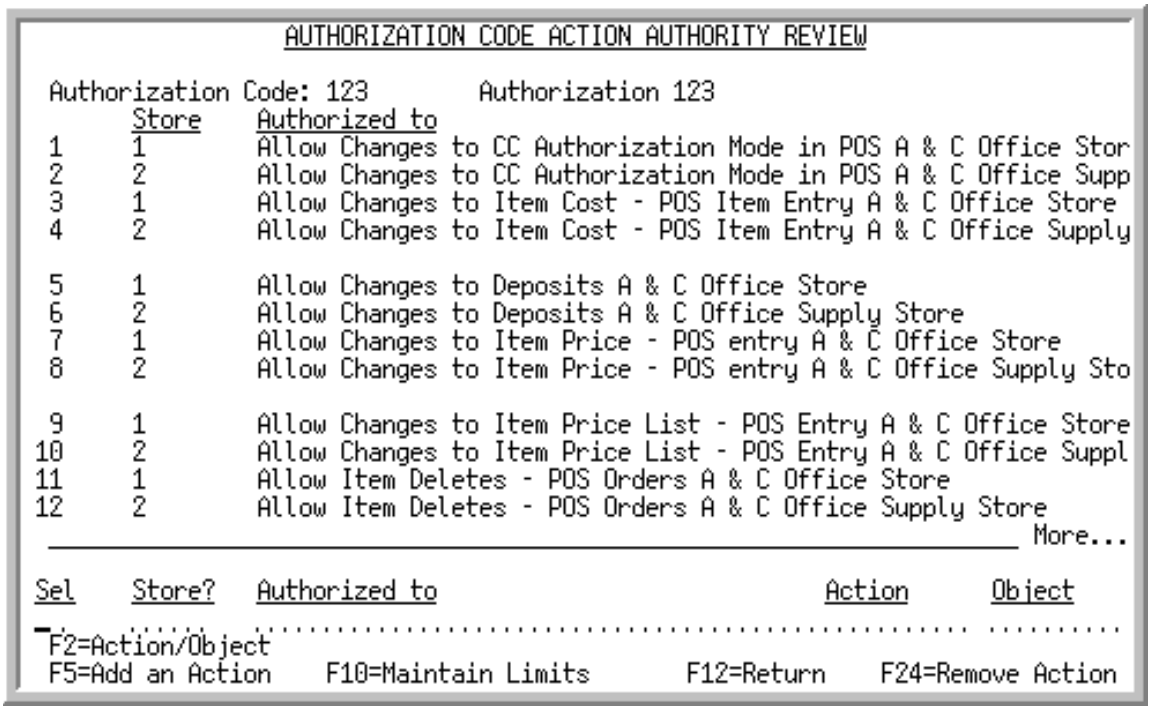


Use this screen to enter a description for the authorization code you are adding or maintaining. This screen also provides access to the Authorization Code Action Authority Review Screen, where you can display a list of application actions that are associated with this authorization code. Refer to the Authorization Code Action Authority Review Screen for further details.

Authorization Code Definition Screen Fields and Function keys

Field/Function Key	Description
Description	Use this field to enter a description for the authorization code. (A 30) Required
F4=Authorization Code Authority	Press **F4=AUTHORIZATION CODE AUTHORITY** to access the Authorization Code Action Authority Review Screen, where you can display a list of application actions that this authorization code provides authority to.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entry.
Enter	Press **ENTER** to confirm your entry and proceed to the next screen.

Authorization Code Action Authority Review Screen



Use this screen to review the various application actions that this authorization code provides authority to. From this screen, you can also choose to:

- associate other actions with this authorization code
- remove current associations with this authorization code
- maintain any limits that may be defined for this authorization code

The top portion of this screen displays the store and the action that the indicated authorization code is associated with. Note that if an extended instance exists (see the Variance Limits Screen), it will display in reverse image following the authority action. Additionally, with the use of the **F2=ACTIONS/OBJECT / F2=DESCRIPTIONS** function key, the top portion of this screen will display descriptions of the Action (e.g., Enter), Object (e.g., Order), Instance (e.g., Return), and Extender (additional information to define the action).

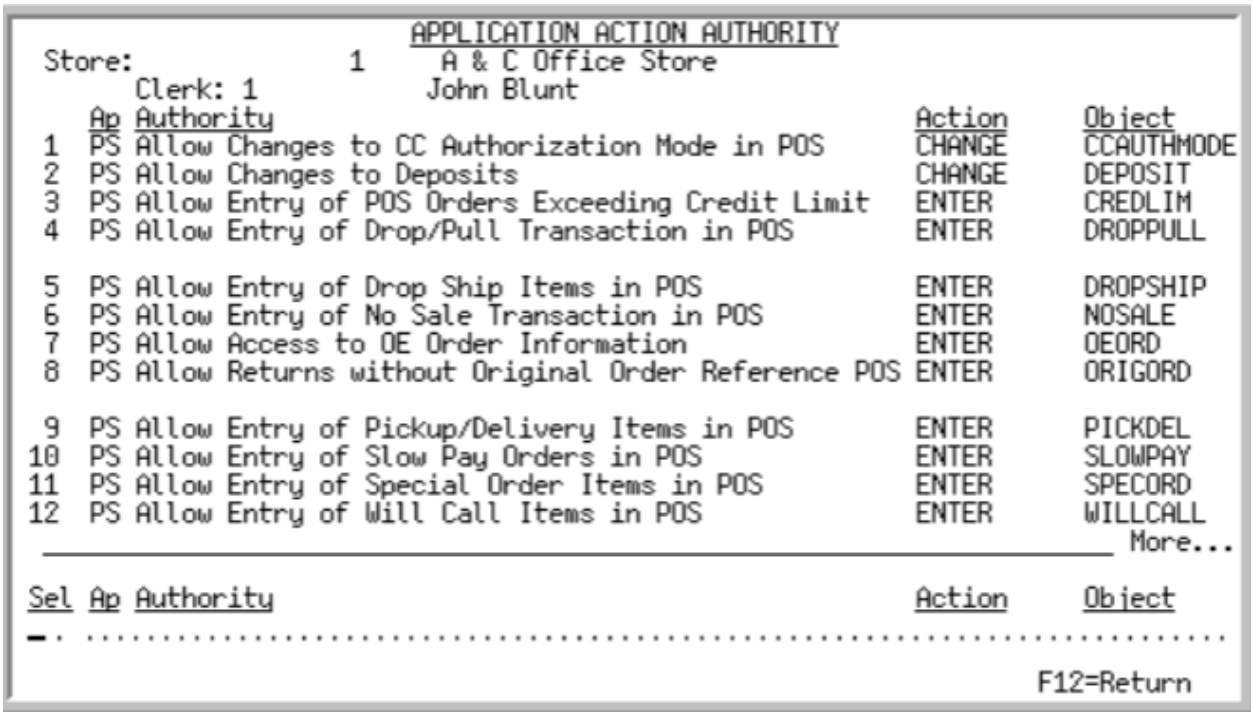
The bottom portion of this screen allows you to select an existing action for which you want to remove the authorization code or limit the screen to particular actions based on filter criteria you enter.

Authorization Code Action Authority Review Screen Fields and Function Keys

Field/Function Key	Description
Sel	Use this field to select an existing action that you want to maintain or for which you want to remove the indicated authorization code. To maintain an action, key the corresponding selection number of the action you want to maintain, and press **F10=MAINTAIN LIMITS**. The Variance Limits Screen displays. To remove the authorization code from a particular action, key the corresponding selection number of the action for which the authorization code will be removed, and press **F24=REMOVE ACTION**. You will be prompted to confirm deletion. (N 2,0) Optional
Store	Use this field to limit the screen to only those actions associated with the store you key in this field or to add limits for this store to the actions selected for this authorization code. To limit the screen to only actions associated with a particular store, key the store and press **ENTER**. The screen will refresh and display actions, if any, matching the store you entered. To add additional actions to this authorization code for a particular store, key the store and press **F5=ADD AN ACTION**. The Application Action Authority Screen will display. **Valid Values:** A store ID created through Stores Maintenance (MENU PSFILE). (A 5) Optional/Required
Authorized to	The Authority is a description of the action. Use this field to limit the screen to only those actions that match the authority criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display actions, if any, matching your criteria. **Note:** This is a character string search and will display actions that match the data anywhere in the **Authorized to** field. (A 40) Optional
Action	Use this field to limit the screen to only those actions that match the criteria you key in this field. Note that the **F2=ACTIONS/OBJECT / F2=DESCRIPTIONS** toggle key displays actions and objects. Key the criteria and press **ENTER**. For example, if you want to display only those actions that pertain to release functions, key **release** in this field. The screen will refresh and display actions, if any, matching your criteria. (A 10) Optional

Field/Function Key	Description
Object	Use this field to limit the screen to only those actions that match the criteria you key in this field. Note that the **F2=ACTIONS/OBJECT / F2=DESCRIPTIONS** toggle key displays actions and objects. Key the criteria and press **ENTER**. For example, if you want to display only those actions that pertain to an order, key **order** in this field. The screen will refresh and display actions, if any, matching your criteria. (A 10) Optional
F2=Actions/Object / F2=Descriptions	Use the **F2=ACTIONS/OBJECT / F2=DESCRIPTIONS** toggle key to display action descriptions. The top portion of this screen will change and show the descriptions for Action (e.g., Enter), Object (e.g., Order), Instance (e.g., Return), and Extender (additional information to define the action).
F5=Add an Action	After entering a store ID, press **F5=ADD AN ACTION** to display the Application Action Authority Screen where you can select an action to be authorized by the indicated authorization code. The store ID will be used for the creation of the Action Authorization Code record.
F10=Maintain Limits	After entering an existing action in the Sel field, press **F10=MAINTAIN LIMITS** to maintain the action. The Variance Limits Screen displays. **Note:** You will only be able to maintain actions that are associated with a variance/price and for which a limit flag exists in the Action Master File. For example, you would be able to select to maintain the action **Allow Changes to Item Price** but would not be able to select to maintain the action **Allow Deletion of Point of Sale Orders.** If you attempt to, an error message displays on screen indicating that the action you selected does not allow limits. The Variance Limits Screen displays only for actions that allow limits.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
F24=Remove Action	After entering an existing action in the **Sel** field for which you want to remove the indicated authorization code, press **F24=REMOVE ACTION**. You will be prompted to confirm deletion.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display actions, if any, matching your criteria.

Application Action Authority Screen



This screen may be accessed from within this menu option (applying to authorization codes) or from Clerks Maintenance (MENU PSFILE) and Clerk Groups Maintenance (MENU PSFILE). The top portion of this screen changes depending on where you access this screen from. It will display the **Authorization Code** if this screen is accessed from this menu option, or **Store** and **Clerk** or **Store** and **Clerk Group** if this screen is accessed from Clerks Maintenance or Clerk Groups Maintenance.

This screen displays a list of available actions (that are not already authorized) for the indicated authorization code, clerk or clerk group, depending on where this screen was accessed from. Use this screen to select an action from the list that you want to be associated with the authorization code, clerk or clerk group. For details about the action, see APPENDIX C: Application Action Authorities.

The top portion of this screen displays the:

- application the action is performed through
- action authority description
- action description (e.g., Enter)
- object description (e.g., Order)

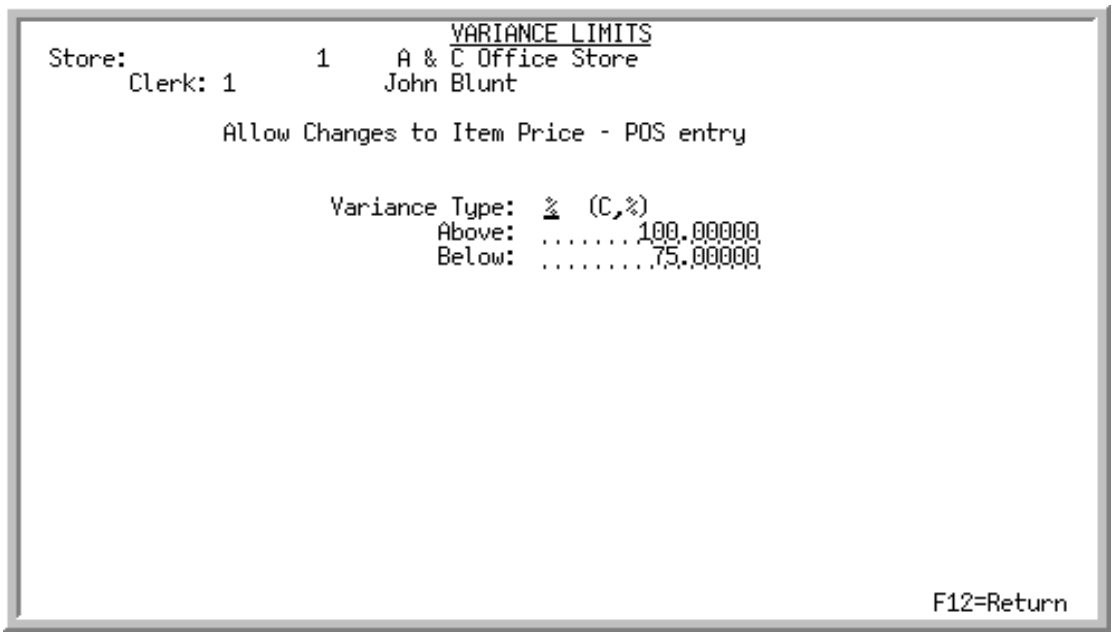
The bottom portion of this screen allows you to select an existing action to be authorized by the indicated type or limit the screen to actions based on filter criteria you enter.

Application Action Authority Screen Fields and Function Keys

Field/Function Key	Description
Sel	Use this field to select an existing action you want to be authorized by the indicated authorization code, clerk or clerk group. Key the corresponding selection number of the action you want authorized, and press **ENTER** to proceed to the next screen. (N 2,0) Optional
Ap	Use this field to limit the screen to only those actions associated with the application ID you key in this field. To limit the screen to only actions associated with a particular application, key the ID of the application and press **ENTER**. The screen will refresh and display actions, if any, matching the application you entered. For example, to display only actions associated with the Point-of-Sale application, key **PS** in this field. (A 2) Optional
Authority	The Authority is a description of the action. Use this field to limit the screen to only those actions that match the authority criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display actions, if any, matching your criteria. **Note:** This is a character string search and will display actions that match the data anywhere in the **Authority** field. (A 40) Optional
Action	Use this field to limit the screen to only those actions that match the criteria you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those actions that pertain to release functions, key **release** in this field. The screen will refresh and display actions, if any, matching your criteria. (A 10) Optional
Object	Use this field to limit the screen to only those actions that match the criteria you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those actions that pertain to an order, key **order** in this field. The screen will refresh and display actions, if any, matching your criteria. (A 10) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.

Field/Function Key	Description
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display actions, if any, matching your criteria. After entering a selection number of an action in the **Sel** field, press **ENTER** to confirm your entry and proceed to the next screen.

Variance Limits Screen



This screen displays only for actions for which a limit flag exists in the Action Master File.

This screen may be accessed from within this menu option (applying to authorization codes) or from Clerks Maintenance (MENU PSFILE) and Clerk Groups Maintenance (MENU PSFILE). The top portion of this screen changes depending on where you access this screen from. It will display the **Authorization Code** if this screen is accessed from this menu option, or **Store** and **Clerk** or **Store** and **Clerk Group** if this screen is accessed from Clerks Maintenance or Clerk Groups Maintenance.

Use this screen to set up variance limits for the indicated action to be associated with the authorization code (if this screen is accessed through this menu option), store/clerk (if accessed through Clerks Maintenance) or store/clerk groups (if accessed through Clerk Groups Maintenance).

Variance Limits Screen Fields and Function Keys

Field/Function Key	Description
Variance Type	Use this field to specify the variance type that will be used for the limits you are defining for this action. Key **C** if the values you are entering in the **Above** and **Below** fields on this screen indicate a currency. Key **%** if the values you are entering in the **Above** and **Below** fields on this screen indicate a percentage. **Note:** If you are using International Currency, the currency used will be the currency of the company for which the store is assigned through Stores Maintenance (MENU PSFILE). (A 1) Optional
Above	Use this field to determine when an override will be allowed for this action. Key the above value that will be used to determine when an override will be allowed. **Example:** If you have an item price of $100.00 and you will allow an override above this price up to $110.00, you would key 10.00 in this field. The Variance Type field would be C. (N 15,5) Optional
Below	Use this field to determine when an override will be allowed for the action. Key the below value that will be used to determine when an override will be allowed. **Example:** If you have an item price of $100.00 and you will allow an override below this price down to $80.00, you would key 20.00 in this field. The Variance Type field would be C. (N 15,5) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
Enter	Press **ENTER** to confirm your entries and return to the previous screen.

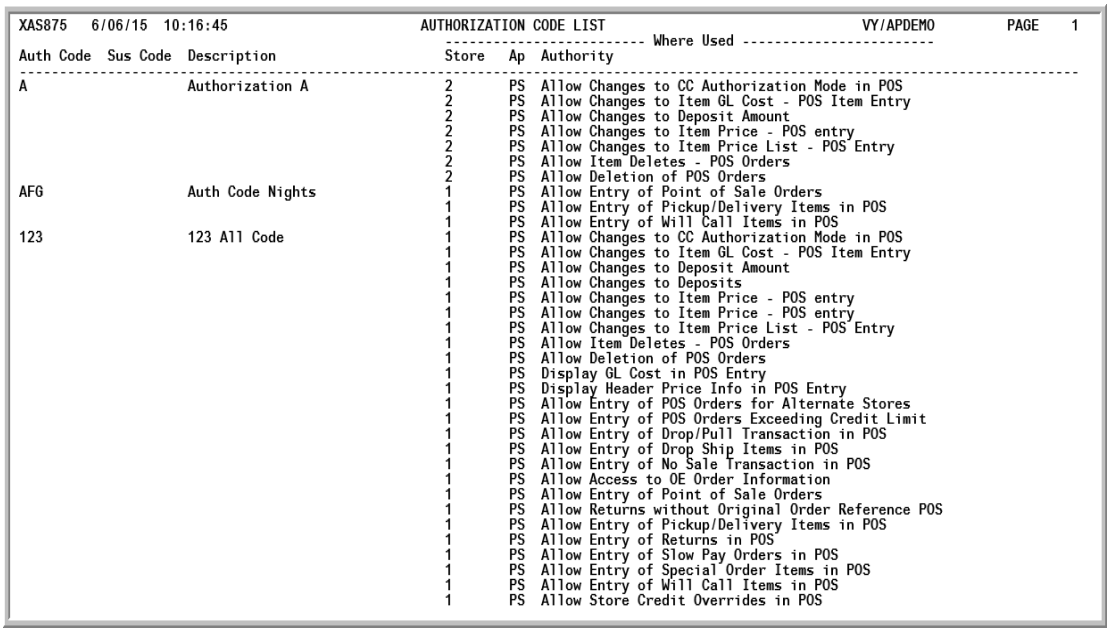
Authorization Codes List

Once you have set up your authorization codes, you can print a listing of those codes through the Authorization Codes Listing option on the Distribution A+ Security Menu (MENU XASCTY) or the Point of Sale File Maintenance Menu (MENU PSFILE).

The screens and/or reports in this option and a brief description are listed in the following table. A complete description of each screen/report is contained in this section.

Title	Purpose
Authorization Codes List	Used to review authorization codes and their settings.

Authorization Codes List



XAS875 6/06/15 10:16:45 AUTHORIZATION CODE LIST VY/APDEMO PAGE 1

Auth Code	Sus Code	Description	Where Used: Store	Ap	Authority
A		Authorization A	2	PS	Allow Changes to CC Authorization Mode in POS
			2	PS	Allow Changes to Item GL Cost - POS Item Entry
			2	PS	Allow Changes to Deposit Amount
			2	PS	Allow Changes to Item Price - POS entry
			2	PS	Allow Changes to Item Price List - POS Entry
			2	PS	Allow Item Deletes - POS Orders
			2	PS	Allow Deletion of POS Orders
AFG		Auth Code Nights	1	PS	Allow Entry of Point of Sale Orders
			1	PS	Allow Entry of Pickup/Delivery Items in POS
			1	PS	Allow Entry of Will Call Items in POS
123		123 All Code	1	PS	Allow Changes to CC Authorization Mode in POS
			1	PS	Allow Changes to Item GL Cost - POS Item Entry
			1	PS	Allow Changes to Deposit Amount
			1	PS	Allow Changes to Deposits
			1	PS	Allow Changes to Item Price - POS entry
			1	PS	Allow Changes to Item Price - POS entry
			1	PS	Allow Changes to Item Price List - POS Entry
			1	PS	Allow Item Deletes - POS Orders
			1	PS	Allow Deletion of POS Orders
			1	PS	Display GL Cost in POS Entry
			1	PS	Display Header Price Info in POS Entry
			1	PS	Allow Entry of POS Orders for Alternate Stores
			1	PS	Allow Entry of POS Orders Exceeding Credit Limit
			1	PS	Allow Entry of Drop/Pull Transaction in POS
			1	PS	Allow Entry of Drop Ship Items in POS
			1	PS	Allow Entry of No Sale Transaction in POS
			1	PS	Allow Access to OE Order Information
			1	PS	Allow Entry of Point of Sale Orders
			1	PS	Allow Returns without Original Order Reference POS
			1	PS	Allow Entry of Pickup/Delivery Items in POS
			1	PS	Allow Entry of Returns in POS
			1	PS	Allow Entry of Slow Pay Orders in POS
			1	PS	Allow Entry of Special Order Items in POS
			1	PS	Allow Entry of Will Call Items in POS
			1	PS	Allow Store Credit Overrides in POS

This listing prints authorization codes and the actions authorized by the codes, as defined through Authorization Codes Maintenance (MENU XASCTY or MENU PSFILE).

Chapter 10 Security Audit Inquiry

Use the Security Audit Inquiry to view access rights for a user or user group, a particular application function (menu option), or an application action. You can also use this menu option to print reports detailing the security audit.

The Security Audit Inquiry can be accessed through the Distribution A+ Security Menu (MENU XASCTY).

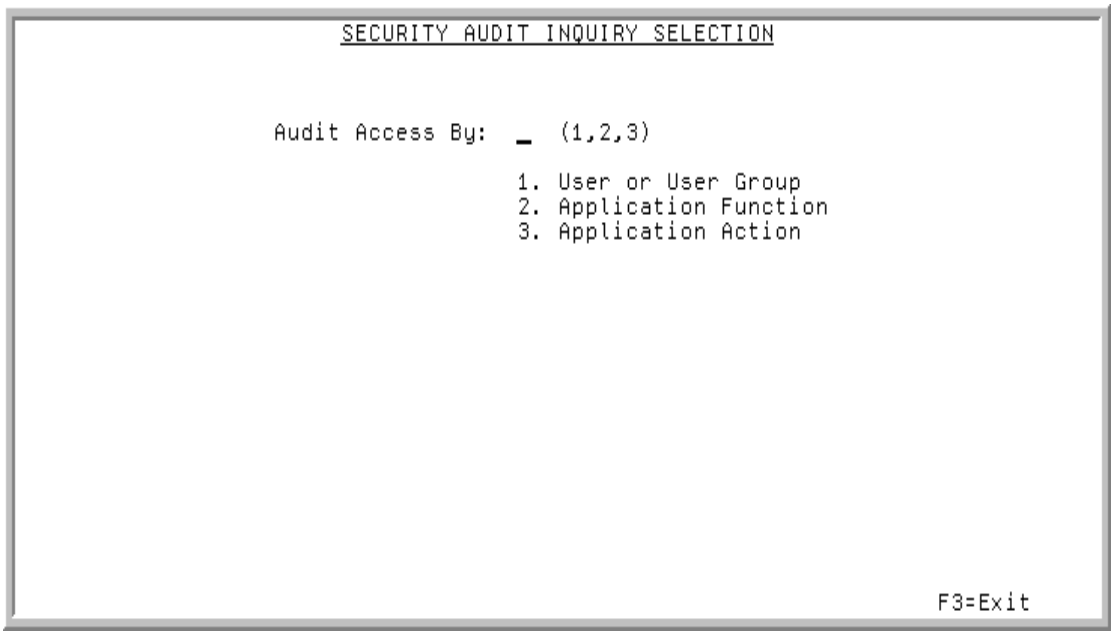
Security Audit Inquiry

The screens and/or reports in this option and a brief description are listed in the following table. A complete description of each screen/report is contained in this section.

Title	Purpose
Security Audit Inquiry Selection Screen	Used to determine the type of audit inquiry you want to perform.
Audit Access By User or User Group Screen	Used to select the user or user group for whom you want to perform an audit inquiry.
Application Action Inquiry Screen	Used to review the application actions to which the user or user group is authorized, or to review the application actions available for the company selected.
User/User Group Action Authority Report	Prints the action authorities for a user or user group.
Action Authority Detail Screen	Used to review general action authority details for the indicated user action.
User/User Group Access Authorities: Functions Screen	Used to review functions, select a function for which you want to display further details, or print the User/ User Group Function Authorities Report.
User/User Group Function Authorities Report	Prints the function authorities for a user or user group.

Title	Purpose
User/User Group Access Full Details Screen	Used to review access authority details for the indicated user or user group. Company, warehouse, and salesrep authority details, as well as the effective authority of a user or user group for a function, will also be displayed for review.
User Authority Detail Screen	Used to review the authority profile information for a specific user.
Authorized Companies Screen	Used to review the companies that the indicated authority profile is authorized to.
Authorized Warehouses Screen	Used to review the warehouses that the indicated authority profile is authorized to.
Authorized SalesReps Screen	Used to review the salesreps that the indicated authority profile is authorized to.
User Group Associations Screen	Used to review the user groups to which the indicated user belongs.
Audit Access By Application Function Screen	Used to inquire into access authorities for a specific application function, allowing you to review the users and user groups that are allowed access to a specific menu option.
Application Function Authorities Screen	Used to review the users and user groups that have access authority to a selected menu option/function.
Application Function Authority Report	Prints the users and user groups that have access authority to a selected menu option/function.
User Group Details Screen	Used to review the users that are included in the selected user group.
Audit Access By Application Action Screen	Used to inquire into application actions for a specific company.
Application Action Authorities Screen	Used to review the users and user groups that have access authority to a selected application action.
Application Action Authority Report	Prints the users and user groups that have access authority to a selected application action.

Security Audit Inquiry Selection Screen



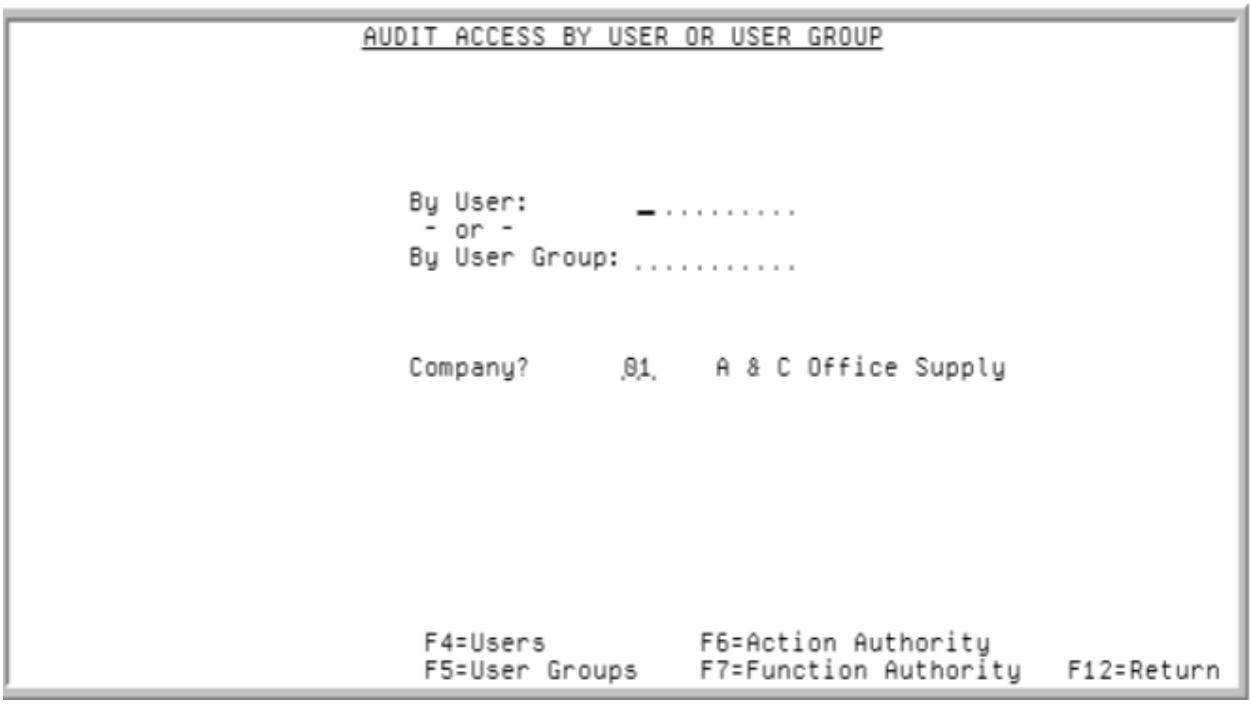
This screen displays after selecting option **30** - Security Audit Inquiry from MENU XASCTY. Use this screen to determine the type of audit inquiry you want to perform. You have the option to access audit information by User or User Group, Application Function, and Application Action.

Security Audit Inquiry Selection Screen Fields and Function Keys

Field/Function Key	Description
Audit Access By	Use this field to determine the type of audit inquiry you want to perform. You have the option to access audit information by User or User Group (for all users in that group), Application Function (for a specified menu option or function ID), and Application Action (e.g., to inquire on authority information regarding a particular action, like changes to blanket orders, changes to item cost, etc.) Key **1** if you want to perform an audit inquiry for a particular User or User Group. Key **2** if you want to perform an audit inquiry for an Application Function. Key **3** if you want to perform an audit inquiry for an Application Action. (N1,0) Required

Field/Function Key	Description
F3=Exit	Press the **F3=EXIT** key to exit from this screen and return to MENU XASCTY.
Enter	Press **ENTER** to confirm your selection. If you keyed **1**, the Audit Access By User or User Group Screen appears. If you keyed **2**, the Audit Access By Application Function Screen appears. If you keyed **3**, the Audit Access By Application Action Screen appears.

Audit Access By User or User Group Screen



This screen displays after keying 1 (User or User Group) in the **Audit Access By** field on the Security Audit Inquiry Selection Screen. Use this screen to select the user or user group for whom you want to perform an audit inquiry. To display a list of existing users or user groups, press **F4=USERS** to access the User List Screen or **F5=USER GROUPS** to access the User Group List Screen. To inquire on the action authorities for a user or user group, select **F6=ACTION AUTHORITY**. To inquiry on the assigned function authority, select **F7=FUNCTION AUTHORITY**.

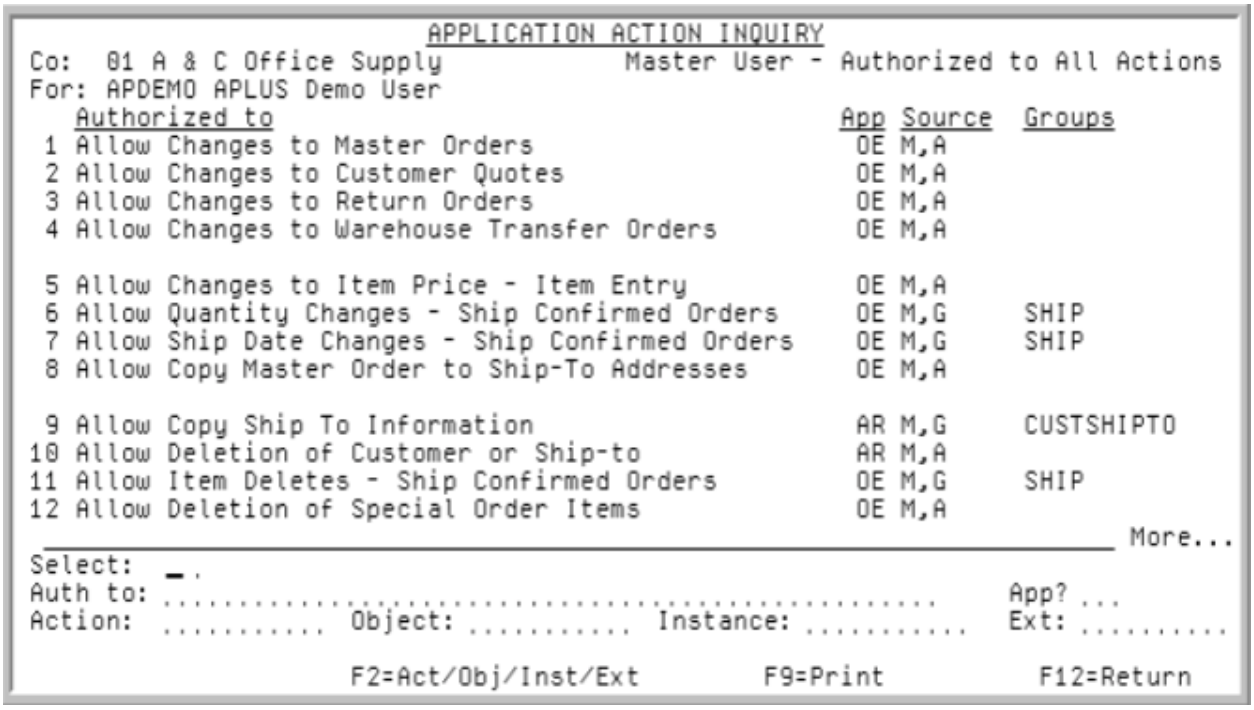
Audit Access By User or User Group Screen Fields and Function keys

Field/Function Key	Description
By User	Use this field to identify the user for whom you want to perform an audit inquiry. You must key a value either in this field or the **By User Group** field; a value cannot be entered in both fields. Key the user ID. Leave this field blank to perform an audit inquiry on a user group. Press **F4=USERS** to display a list of existing users. **Valid Values:** A valid environment user defined in the User Master File (**USRMST**), or a valid Distribution A+ User ID defined in Register A+ User IDs (MENU XACFIG) (A 10) Optional

Field/Function Key	Description
By User Group	Use this field to identify the user group for whom you want to perform an audit inquiry. You must key a value either in this field or the **By User** field; a value cannot be entered in both fields. Key the user group. Leave this field blank to perform an audit inquiry on a particular user. Press **F5=USER GROUPS** to display a list of existing user groups. **Valid Values:** A valid user group defined through User Group Maintenance (MENU XASCTY) (A 10) Optional
Company	This field is protected if **Multi-Company** is **N** in System Options Maintenance (MENU XAFILE). This field is required if you want to inquire on a user's/user group's action authority. Key the company number associated with the user or user group. **Default Value:** The default company defined on the Authority Profile Definition Screen accessed through User or Authority Profile Maintenance on the Distribution A+ Security Menu (MENU XASCTY) if one has been defined; otherwise, this is the default company defined through System Options Maintenance (MENU XAFILE). **Valid Values:** Any valid company number that has been created through Company Name Maintenance (MENU XAFILE). The user or user group entered on this screen must be authorized to the company you key in this field. (N 2,0) Optional/Required
F4=Users	Press **F4=USERS** to access the User List Screen, which displays users in the User Master File for the current environment when accessed from this function key.
F5=User Groups	Press **F5=USER GROUPS** to access the User Group List Screen, which displays existing user groups.
F6=Action Authority	After entering either a user or user group and company, press **F6=ACTION AUTHORITY** to access the Application Action Inquiry Screen to inquire on a user's/user group's action authority.
F7=Function Authority	After entering either a user or user group, press **F7=FUNCTION AUTHORITY** to access the User/User Group Access Authorities: Functions Screen to inquire on a user's/user group's function authority.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving changes made to this screen.

Field/Function Key	Description
Enter	After entering a user or user group, press **Enter** to confirm your selection and proceed to the next screen. If you entered a user, the User Authority Detail Screen appears. If you entered a user group, the User Group Details Screen appears.

Application Action Inquiry Screen



This screen displays after pressing **F6=ACTION AUTHORITY** on the Audit Access By User or User Group Screen or after pressing **ENTER** on the Audit Access By Application Action Screen. The differences will be noted in this section depending on where you accessed this screen from.

Use this screen to review the application actions to which the user or user group is authorized (if you accessed this screen from the Audit Access By User or User Group Screen), or to review the application actions available for the company selected (if you accessed this screen from the Audit Access By Application Action Screen).

If by user and the user is a Master User (authorized to all actions), it will be indicated on the top right portion of this screen.

Note: If you accessed this screen from the Audit Access By User or User Group Screen, all actions will display if either of the following are true:

- **User Security** is **N** in System Options Maintenance (MENU XAFILE)
- You are displaying authorities for a user and the user is set up as a Master User.

The lower portion of this screen provides filters that allow you to limit the criteria on the screen based on authorized to, application, action, object, instance and extended instance.

Application Action Inquiry Screen Fields and Function keys

Field/Function Key	Description
Co	The company number and name of the company selected on the Audit Access By User or User Group Screen or the Audit Access By Application Function Screen. Display
For	This field only displays if you accessed this screen from the Audit Access By User or User Group Screen, The name of the user/user group, which displays only when you are performing an audit access by User or User Group. Display
(Reference Number)	The reference number of the application action authority displayed on this screen. This number is **1** through **12** for the twelve authorities that may display. When rolling forward or backward, the reference numbers do not change. Display
Authorized to	When you access this screen from the Audit Access By User or User Group Screen, this field is the application action the user or user group is authorized to use/access. When you access this screen from the Audit Access By Application Action Screen this field is the application actions available for the selection. Display
Action/Object/Inst/Ext	The action (e.g., ENTER), object (e.g., ORDER), Instance (e.g., HOLDCODE), and extended instance (e.g., SP, CR, etc.) of the selected action. This field toggles with the **F2=APPLICATION / F2=ACT/OBJ/INST/EXT** and **F2=APP AND SOURCE / F2=ACT/OBJ/INST/EXT** keys. Display
App	The application module the action is associated with (e.g. OE for Order Entry). This field toggles with the **F2=APPLICATION / F2=ACT/OBJ/INST/EXT** and **F2=APP AND SOURCE / F2=ACT/OBJ/INST/EXT** keys. Display

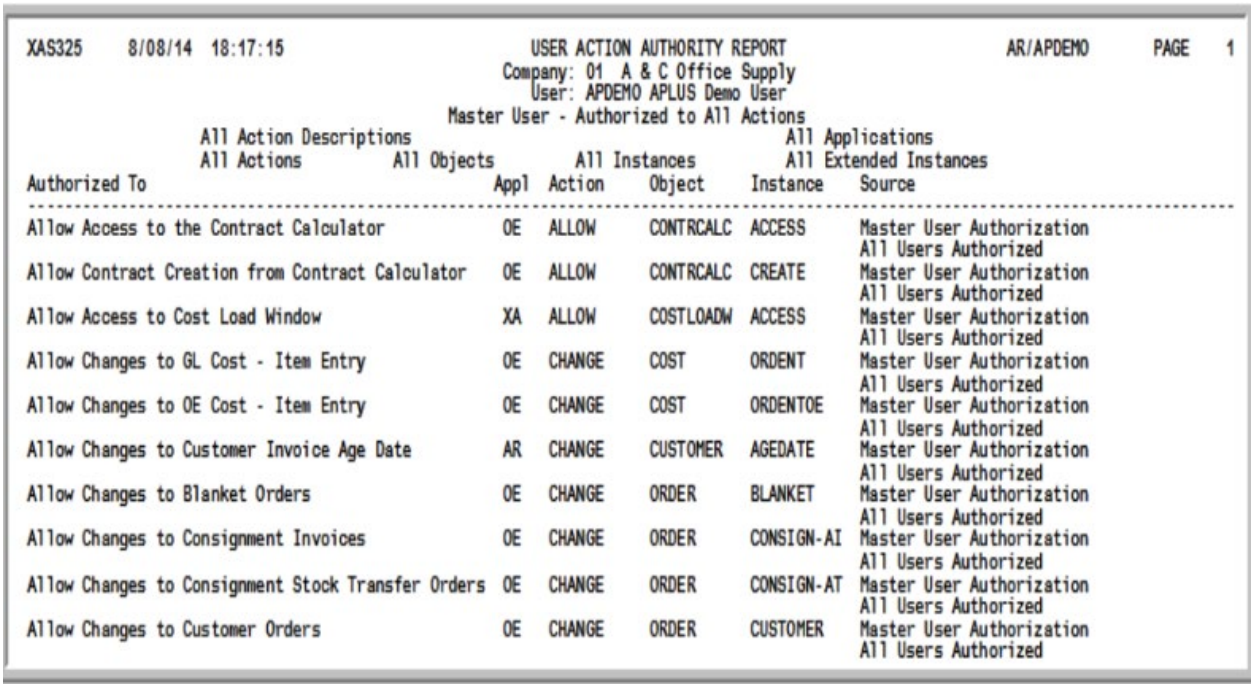
Field/Function Key	Description
Source	This field displays when you access this screen from the Audit Access By User or User Group Screen. The method used to provide the user authorization: • U is By User ID • G is By User Group • A is All Users • M is Master Users. This field toggles with the **F2=APP AND SOURCE / F2=ACT/OBJ/INST/EXT** key. Display
Groups	This field displays when you access this screen from the Audit Access By User or User Group Screen. The groups that this user belongs to that are authorized to the action. If not, all applicable groups can be provided due to space limitations, a '**+**' sign will display in the last position of the **Groups** field. This field toggles with the **F2=APP AND SOURCE / F2=ACT/OBJ/INST/EXT** key. Display
Select	Use this field to select an existing application action for which you want to display further details. Key the corresponding **Reference Number** of the application action you want to choose, and press **ENTER** to proceed to the next screen. (N 2,0) Optional
Auth to	This field represents the description of the application action. Use this field to limit the screen to only those application actions that match the authority criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display application actions, if any, matching your criteria. **Note:** This is a character string search and will display application actions that match the data anywhere in the **Authorized to** field. (A 40) Optional

Field/Function Key	Description
App	Use this field to limit the screen to only those application actions associated with the application ID you key in this field. To limit the screen to only application actions associated with a particular application, key the ID of the application and press **ENTER**. The screen will refresh and display application actions, if any, matching the application you entered. For example, to display only application actions associated with the Order Entry application, key **OE** in this field. (A 2) Optional
Action	Use this field to limit the screen to only those application actions that match the criteria you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those application actions that pertain to release functions, key **RELEASE** in this field. The screen will refresh and display application actions, if any, matching your criteria. For a list of valid actions, refer to the **Action** field on the Application Action Authority Selection Screen. (A 10) Optional
Object	Use this field to limit the screen to only those application actions that match the object ID you key in this field. Key the criteria and press **ENTER**. For example, if you want to display only those application actions that pertain to an order, key **ORDER** in this field. The screen will refresh and display application actions, if any, matching your criteria. For a list of valid objects, refer to the **Object** field on the Application Action Authority Selection Screen. (A 10) Optional

Field/Function Key	Description
Instance	Use this field to limit the screen to only those instances (available for the application action) that match the instance ID you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display instances, if any, matching your criteria. **Valid Values:** blank, or COMPANY LEVEL: access, agedate, ar, avgcst, blanket, bypass, comcst, consign-ai, consign-at, contract, crdrebdupe, create, credit, customer, future, holdcode, invoice, lstcst, master, oe, oecost, ordent, ordentoe, override, pickprtord, po, pocost, posent, posentoe, pospromo, promoitem, quantity, quote, rebateid, return, salesmkt, shipto, shpcmford, so, stdcst, suspcode, tpjob, transfer, unauthitm, unrefed, usrcst, varhold, vicst, wmcost, worcpt SYSTEM LEVEL: achthd, achven, comment, company, fields, item, lotitem, markreslvd, query, reports, shipto, taxid, vendor (A 10) Optional
Ext	Use this field to limit the screen to only those extended instances previously defined for the application action. For example, if the application action is pertaining to the releasing of a held order, the extended instance might be SP for Slow Pay Hold. Meaning, allow the release of held orders only if they are on slow pay hold. (A 10) Optional
F2=Act/Obj/Inst/Ext / F2=App and Source -or- F2=Application / F2=Act/Obj/Inst/Ext	**F2=ACT/OBJ/INST/EXT** toggling to **F2=APP AND SOURCE** display if this screen is accessed from the Audit Access By User or User Group Screen. Press **F2=APP AND SOURCE** to toggle to columns to App, Source, and Group; then press **F2=ACT/OBJ/INST/EXT** to display the combined action, object, instance and extended instance fields. **F2=APPLICATION** toggling to **F2=ACT/OBJ/INST/EXT** display if this screen is accessed from the Audit Access By Application Action Screen. Press **F2=ACT/OBJ/INST/EXT** to display the combined action, object, instance and extended instance fields; then press **F2=APPLICATION** to display the application of the action.
F6=Action Authority	The **F6=ACTION AUTHORITY** function key displays only if you accessed this screen from the Audit Access By Application Action Screen. After entering a reference number in the **Select** field, press **F6=ACTION AUTHORITY** to access the Application Action Authorities Screen. **Note:** If the application action you select is set up with an Authorization of no users (**N**), you will receive a message informing you that the action is disabled.

Field/Function Key	Description
F9=Print	Press **F9=PRINT** to print the User/User Group Action Authority Report. Prior to the report printing, the Report Option Screen displays. On the Report Option Screen, select to print the report interactively (the report cannot be submitted to batch). Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen. **Note:** If the data on this screen is limited by filter criteria you entered, the report will also be limited by that same criteria.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving your entry.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display application actions, if any, matching your criteria. After entering the reference number of an application action in the **Select** field, press **ENTER**. The Action Authority Detail Screen displays.

User/User Group Action Authority Report



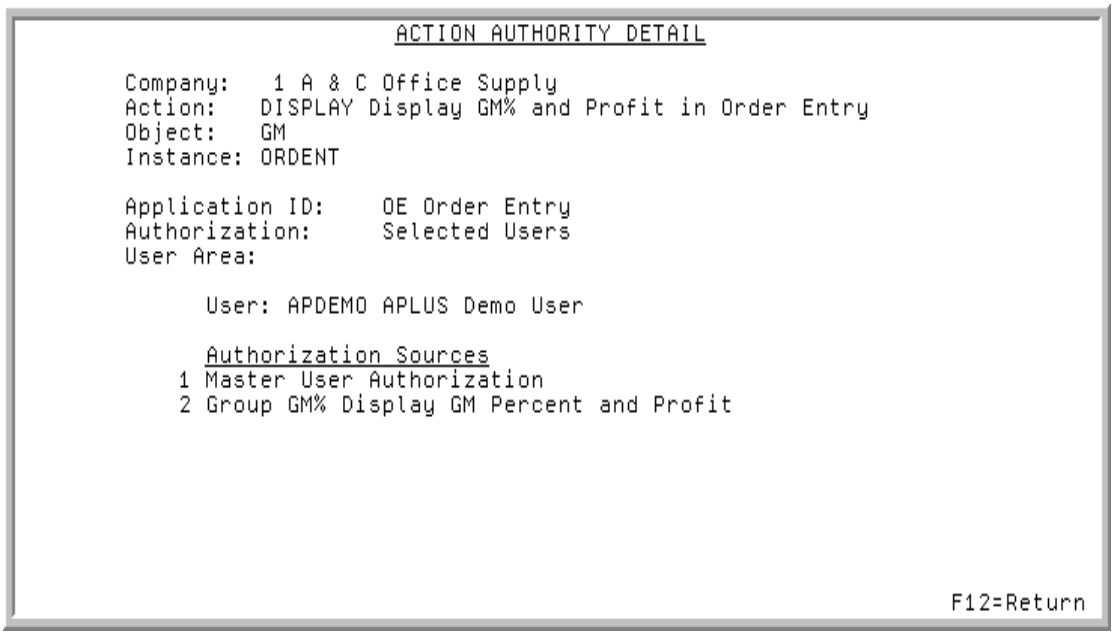
XAS325 8/08/14 18:17:15 USER ACTION AUTHORITY REPORT AR/APDEMO PAGE 1
Company: 01 A & C Office Supply
User: APDEMO APLUS Demo User
Master User - Authorized to All Actions
All Action Descriptions All Applications
All Actions All Objects All Instances All Extended Instances

Authorized To	Appl	Action	Object	Instance	Source
Allow Access to the Contract Calculator	OE	ALLOW	CONTRCALC	ACCESS	Master User Authorization All Users Authorized
Allow Contract Creation from Contract Calculator	OE	ALLOW	CONTRCALC	CREATE	Master User Authorization All Users Authorized
Allow Access to Cost Load Window	XA	ALLOW	COSTLOADW	ACCESS	Master User Authorization All Users Authorized
Allow Changes to GL Cost - Item Entry	OE	CHANGE	COST	ORDENT	Master User Authorization All Users Authorized
Allow Changes to OE Cost - Item Entry	OE	CHANGE	COST	ORDENTOE	Master User Authorization All Users Authorized
Allow Changes to Customer Invoice Age Date	AR	CHANGE	CUSTOMER	AGEDATE	Master User Authorization All Users Authorized
Allow Changes to Blanket Orders	OE	CHANGE	ORDER	BLANKET	Master User Authorization All Users Authorized
Allow Changes to Consignment Invoices	OE	CHANGE	ORDER	CONSIGN-AI	Master User Authorization All Users Authorized
Allow Changes to Consignment Stock Transfer Orders	OE	CHANGE	ORDER	CONSIGN-AT	Master User Authorization All Users Authorized
Allow Changes to Customer Orders	OE	CHANGE	ORDER	CUSTOMER	Master User Authorization All Users Authorized

This report prints after pressing **ENTER** on the Report Option Screen, which displayed after pressing **F9=PRINT** on the Application Action Inquiry Screen. Use this report to review the action authorities for the indicated user or user group.

Note: If the data on the Application Action Inquiry Screen is limited by filter criteria you entered, this report will also be limited by that same criteria.

Action Authority Detail Screen



This screen displays after pressing **ENTER** on the Application Action Inquiry Screen or Application Action Authorities Screen. Use this screen to review general action authority details for the indicated user action. If this action was selected for a particular user, then the different ways in which the user is authorized to the action is displayed on the lower portion of the screen.

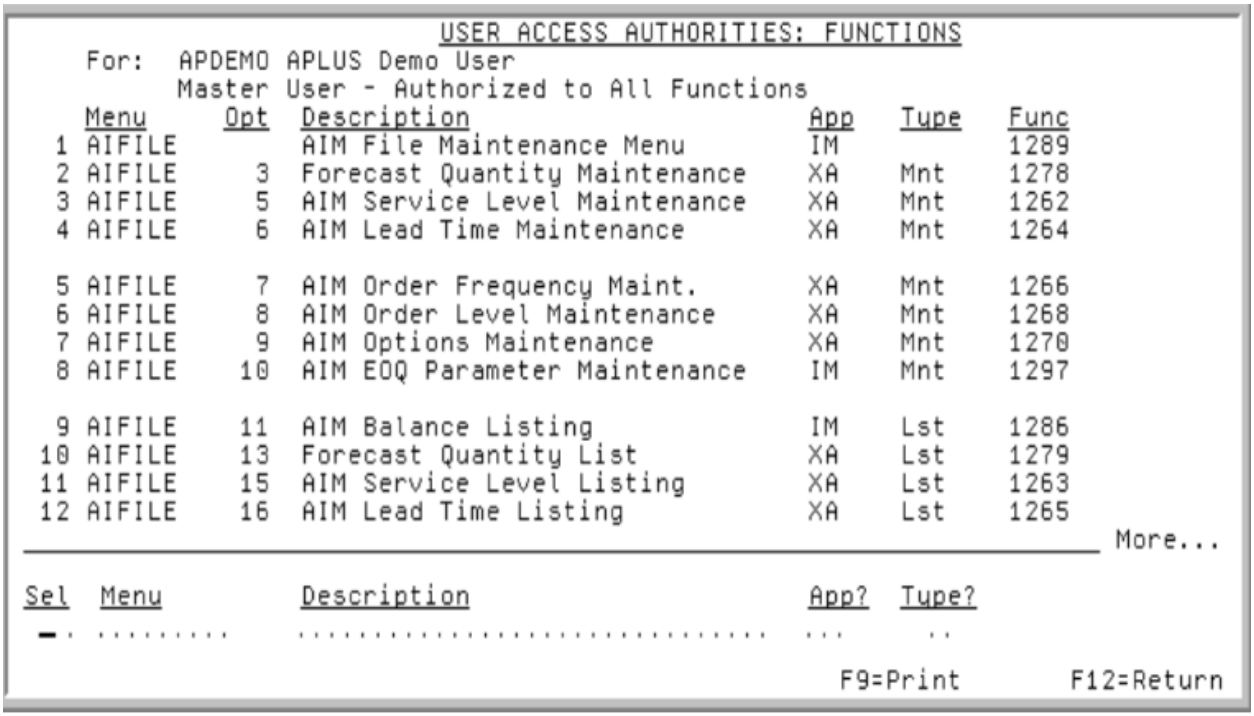
All the fields on this screen are display only and cannot be changed.

Action Authority Detail Screen Fields and Function Keys

Field/Function Key	Description
Company	The company number and name of the company associated with the application action authorities.
Action	The authority action code followed by the description of the selected Application Action Authority. Refer to the Application Action Authority Selection Screen for a list of valid action codes.
Object	The authority object for the selected Application Action Authority. Refer to the Application Action Authority Selection Screen for a list of valid object codes.
Instance	The instance, further describing the application action (e.g., if the application action is pertaining to the releasing of a held order, the instance is Hold Code). Refer to the Application Action Inquiry Screen for valid instances.

Field/Function Key	Description
Application ID	The 2-character ID of the application the action is associated with, followed by the name of the application (e.g., if the action is performed in Purchasing, **PO Purchasing** displays in this field).
Authorization	The authorization pertains to: All Users, Master Users only, Selected Users, or No Users.
User Area	The notes, if any, that are associated with the action.
User	This field displays only if you are inquiring on an action or actions for a particular user. The user for which you are inquiring on an action or actions.
Authorization Sources	This field displays only if you are inquiring on an action or actions for a specific user. The source is the different ways the user is authorized to the action. Values that may be displayed include: • User Level Authorization: this user has been selected for authorization to this action • Master User Authorization: this user is a Master User • All Users Authorized: Indicating that the authorization for this action is 'A' • Group and Description: Any groups that the user belongs to that were selected for authorization to this action.
F12=Return	After viewing the information, press **F12=RETURN** to return to the previous screen.

User/User Group Access Authorities: Functions Screen



This screen displays after pressing **F7=FUNCTION AUTHORITY** on the Audit Access By User or User Group Screen. The application functions that a user or user group is authorized to use/access is displayed on this screen. Use this screen to review the menu option functions, select a function for which you want to display further access details, or print the User/User Group Function Authorities Report including the data currently displayed on this screen.

The lower portion of this screen provides filters that allow you to limit the criteria on the screen based on menu, description, application, type, and source.

Note:

The user or user group is automatically authorized to all functions if any of the following are true:

- **User Security** is **N** in System Options Maintenance (MENU XAFILE)
- **Program Security** is **N** in System Options Maintenance (MENU XAFILE)
- If you are displaying authorities for a user and the user is set up as a Master User

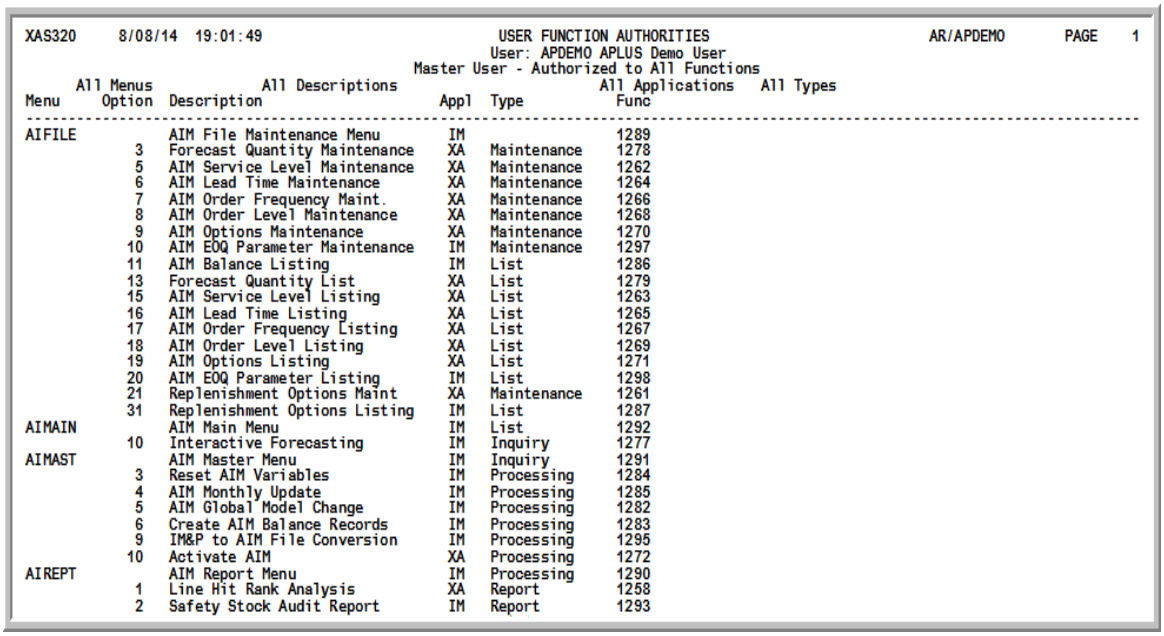
User/User Group Access Authorities: Functions Screen Fields and Function Keys

Table heading	Description
For	The selected user and user name. When the Authority Profile for the user has **Master User Authority** set to **Y**, the text **Master User - Authorized to All Functions** displays on the next line. Display
(Reference Number)	The reference number of the menu function displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
Menu	The primary menu the function resides on (i.e. APCHCK, OEFILE). Display
Opt	The option number associated with the function. Display
Description	Description of the function. Display
App	The primary application the function is associated with (i.e. AP, OE, PO). Display
Type	The type of functionality that the program primarily accomplishes (reporting, processing, maintenance, inquiry, listing). Display
Func	The unique function number assigned to the function in the Function Master File. Display
Source	This column only displays when inquiring by authority for a user that is not a Master User. The source of the function • U - Authorized on the User level - user has been authorized to this function • G - Authorized on the Group level - user belongs to a group that has access to the function. Display

Table heading	Description
Sel	Use this field to select an application function for which you want to display further access details for the indicated user or user group. Key the corresponding reference number of the function you want to select and press **ENTER** to proceed to the User/User Group Access Full Details Screen. (N 2,0) Optional
Menu	Use this field to limit the screen to the menu that matches the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display the menu, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** Must be a valid menu name (A 8) Optional
Description	Use this field to limit the screen to only those functions that match the description you key in this field. Key the description criteria and press **ENTER**. The screen will refresh and display those functions, if any, matching your criteria. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays limited information. **Note:** This is a character string search and will display menus that match the data anywhere in the **Description** field. (A 30) Optional
App	Use this field to limit the screen to the application you key in this field. Key the application ID and press **ENTER**. The screen will refresh and show only those functions associated with this application ID, if any. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. (A 2) Optional
Type	Use this field to limit the screen to the type of function you key in this field. Key the function type and press **ENTER**. The screen will refresh and show only those functions associated with this type of function. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** P-Processing, I-Inquiry, R-Report, M-Maintenance, L-List (A 1) Optional

Table heading	Description
Source	This column only displays when inquiring by authority for a user that is not a Master User. Use this field to limit the screen to the type of source you key in this field. Key the source type and press **ENTER**. The screen will refresh and show only those functions associated with this type of source. Other filter criteria you may select on this screen is also considered when the screen refreshes and displays the limited information. **Valid Values:** U for User level, G for Group level, blank for both (A 1) Optional
F9=Print	Press **F9=PRINT** to print the User/User Group Function Authorities Report. The Report Option Screen displays upon pressing **F9=PRINT** prior to the report printing. Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen. **Note:** If the data on this screen is limited by filter criteria you entered, the report will also be limited by that same criteria.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display functions, if any, matching your criteria. After entering a selection number of a function in the **Sel** field, press **ENTER** to confirm your entry and proceed to the User/User Group Access Full Details Screen.

User/User Group Function Authorities Report



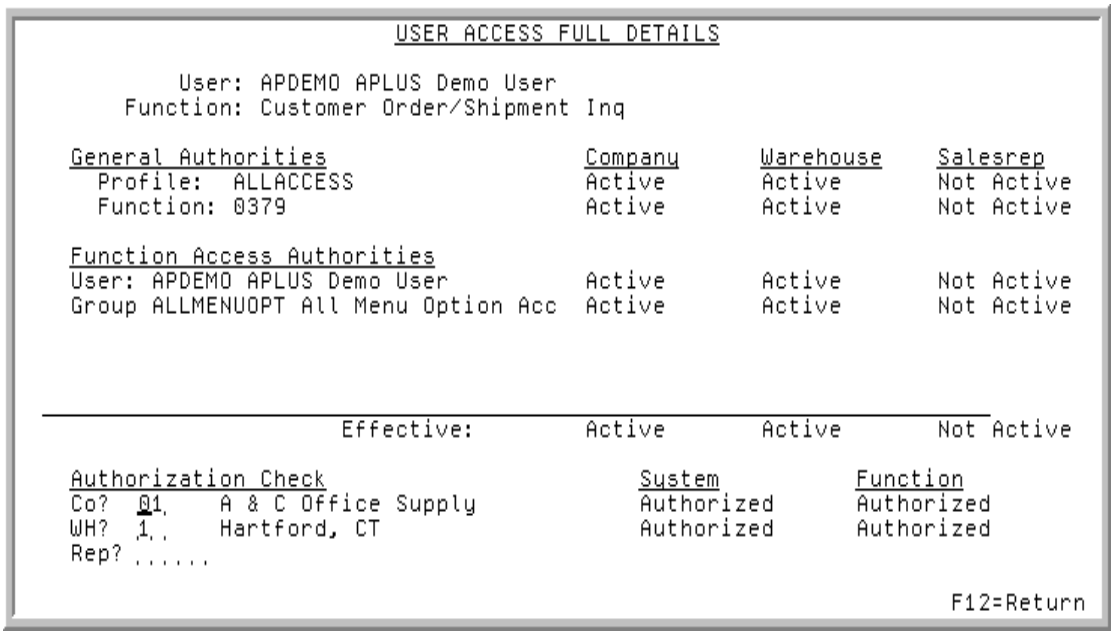
```
XAS320     8/08/14  19:01:49                    USER FUNCTION AUTHORITIES                    AR/APDEMO      PAGE    1
                                                 User: APDEMO APLUS Demo User
                                    Master User - Authorized to All Functions
      All Menus            All Descriptions                          All Applications   All Types
Menu     Option  Description                    Appl  Type           Func
-------------------------------------------------------------------------------------------------------------------
AIFILE           AIM File Maintenance Menu      IM                   1289
              3  Forecast Quantity Maintenance  XA    Maintenance    1278
              5  AIM Service Level Maintenance  XA    Maintenance    1262
              6  AIM Lead Time Maintenance      XA    Maintenance    1264
              7  AIM Order Frequency Maint.     XA    Maintenance    1266
              8  AIM Order Level Maintenance    XA    Maintenance    1268
              9  AIM Options Maintenance        XA    Maintenance    1270
             10  AIM EOQ Parameter Maintenance  IM    Maintenance    1297
             11  AIM Balance Listing            IM    List           1286
             13  Forecast Quantity List         XA    List           1279
             15  AIM Service Level Listing      XA    List           1263
             16  AIM Lead Time Listing          XA    List           1265
             17  AIM Order Frequency Listing    XA    List           1267
             18  AIM Order Level Listing        XA    List           1269
             19  AIM Options Listing            XA    List           1271
             20  AIM EOQ Parameter Listing      IM    List           1298
             21  Replenishment Options Maint    XA    Maintenance    1261
             31  Replenishment Options Listing  IM    List           1287
AIMAIN           AIM Main Menu                  IM    List           1292
             10  Interactive Forecasting        IM    Inquiry        1277
AIMAST           AIM Master Menu                IM    Inquiry        1291
              3  Reset AIM Variables            IM    Processing     1284
              4  AIM Monthly Update             IM    Processing     1285
              5  AIM Global Model Change        IM    Processing     1282
              6  Create AIM Balance Records     IM    Processing     1283
              9  IM&P to AIM File Conversion    IM    Processing     1295
             10  Activate AIM                   XA    Processing     1272
AIREPT           AIM Report Menu                IM    Processing     1290
              1  Line Hit Rank Analysis         XA    Report         1258
              2  Safety Stock Audit Report      IM    Report         1293
```

This report prints after pressing **ENTER** on the Report Option Screen, which displayed after pressing **F9=PRINT** on the User/User Group Access Authorities: Functions Screen. Use this report to review the function authorities for the indicated user or user group.

Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen.

Note: If the data on the User/User Group Access Authorities: Functions Screen is limited by filter criteria you entered, this report will also be limited by that same criteria.

User/User Group Access Full Details Screen



This screen displays after selecting an application function and pressing **ENTER** on the User/User Group Access Authorities: Functions Screenor the Application Function Authorities Screen. The title of this screen is either User Access Full Details or User Group Access Full Details, depending on if you are displaying details for a user or user group. Any screen differences will be noted in this section depending on if you are reviewing information for a user or user group.

Use this screen to review access authority details for the function shown for the indicated user or user group. The company, warehouse, and salesrep authority details, as well as the effective authority of a user or user group for a function, will also be shown on this screen.

User/User Group Access Full Details Screen Fields and Function Keys

Field/Function Key	Description
User	The ID of the user or the user group that has access authority to the selected menu option/function. Display
Function	The description of the unique function number assigned to the function in the Function Master File. Display

Field/Function Key	Description
General Authorities: Profile	This field displays on the screen only if you selected to review access details for a user (instead of a user group). The user's profile displays in this field. If the authority profile has Master User authority, that too will be indicated. Display
General Authorities: Function	The 4 position function ID displays in this field. Display
General Authorities: Company	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the company displays in this field. It indicates if company security is **Active** (company security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (company security has not been activated through System Options Maintenance), or **Bypass** (user is a Master User or the user's profile is set up to bypass company security). Display
General Authorities Function: Company	Authorization details for the company displays in this field. It indicates if company security is **Active** (company security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (company security has not been activated through System Options Maintenance), **Bypass** (the function ID is set up to bypass company security) or **n/a** (the function ID is not company secured). Display
General Authorities: Warehouse	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the warehouse displays in this field. It indicates if warehouse security is **Active** (warehouse security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (warehouse security has not been activated through System Options Maintenance), or **Bypass** (user is a Master User or the user's profile is set up to bypass warehouse security). Display
General Authorities Function: Warehouse	Authorization details for the warehouse displays in this field. It indicates if warehouse security is **Active** (warehouse security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (warehouse security has not been activated through System Options Maintenance), **Bypass** (the function ID is set up to bypass warehouse security) or **n/a** (the function ID is not warehouse secured). Display

Field/Function Key	Description
General Authorities Function: Salesrep	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the salesrep displays in this field. It indicates if salesrep security is **Active** (salesrep security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (salesrep security has not been activated through System Options Maintenance), or **Bypass** (user is a Master User or the user's profile is set up to bypass salesrep security). Display
General Authorities Function: Salesrep	Authorization details for the salesrep displays in this field. It indicates if salesrep security is **Active** (salesrep security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (salesrep security has not been activated through System Options Maintenance), **Bypass** (the function ID is set up to bypass salesrep security) or **n/a** (the function ID is not salesrep secured). Display
Function Access Authorities: User	This field displays on the screen only if you selected to review access details for a user (instead of a user group). The access authorities for the user, if this is a User ID, and function are displayed first. After the access authorities for the user are displayed, any groups that the user belongs to that have authority to this function will then be shown. If more than five lines exist, you will have the ability to scroll down. Display
Function Access Authorities: Company	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the company displays in this field. It indicates if company security is **Active** (company security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (company security has not been activated through System Options Maintenance), **Bypass** (the indicated user or user group is set up to bypass company security for this function ID) or **n/a** (the function ID is not company secured). Display

Field/Function Key	Description
Function Access Authorities: Warehouse	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the warehouse displays in this field. It indicates if warehouse security is **Active** (warehouse security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (warehouse security has not been activated through System Options Maintenance), **Bypass** (the indicated user or user group is set up to bypass warehouse security for this function ID) or **n/a** (the function ID is not warehouse secured). Display
Function Access Authorities: Salesrep	This field displays on the screen only if you selected to review access details for a user (instead of a user group). Authorization details for the salesrep displays in this field. It indicates if salesrep security is **Active** (salesrep security has been activated through System Options Maintenance, MENU XAFILE), **Not Active** (salesrep security has not been activated through System Options Maintenance), **Bypass** (the indicated user or user group is set up to bypass salesrep security for this function ID) or **n/a** (the function ID is not salesrep secured). Display
Effective (Authorities)	Depending on the information displayed on the top portion of this screen, the authority that will be in effect for the user or user group for the company, warehouse, and salesrep will display. The values that display are based on the following hierarchy: **1** **Not Active** displays if the security is not active. **2** **n/a** displays if the function ID is not secured. **3** **Bypass** displays if the profile, function ID, or any of the displayed function authorities for this user is set up to bypass security. **4** **Active** displays if the security for this user and function is activated and will be verified. Display

Field/Function Key	Description
Authorization Check (Co, WH, Rep)	This section displays on this screen only if you are inquiring on access details for a user. If you are inquiring on access details for a user group, this section does not display since a user group is not assigned authorized companies, warehouse, and salesreps. Company, warehouse, and salesrep authorization is on the authority profile level only. **Co**, **WH**, and **Rep** input fields are provided to allow you to check their authorization criteria. Key the company number, warehouse number, and/or salesrep number whose authorizations you want to review. The **System** and **Function** fields displayed to the right of these fields will change accordingly and their authorizations will be shown. **Default Value:** The company and warehouse default values will be the default company and warehouse of the user displayed on this screen; there is no default salesrep value. **Valid Values:** Must be a valid company, warehouse, and/or salesrep; company number cannot be blank if a salesrep is entered. (N2,0 / A2, A5) Optional/Required

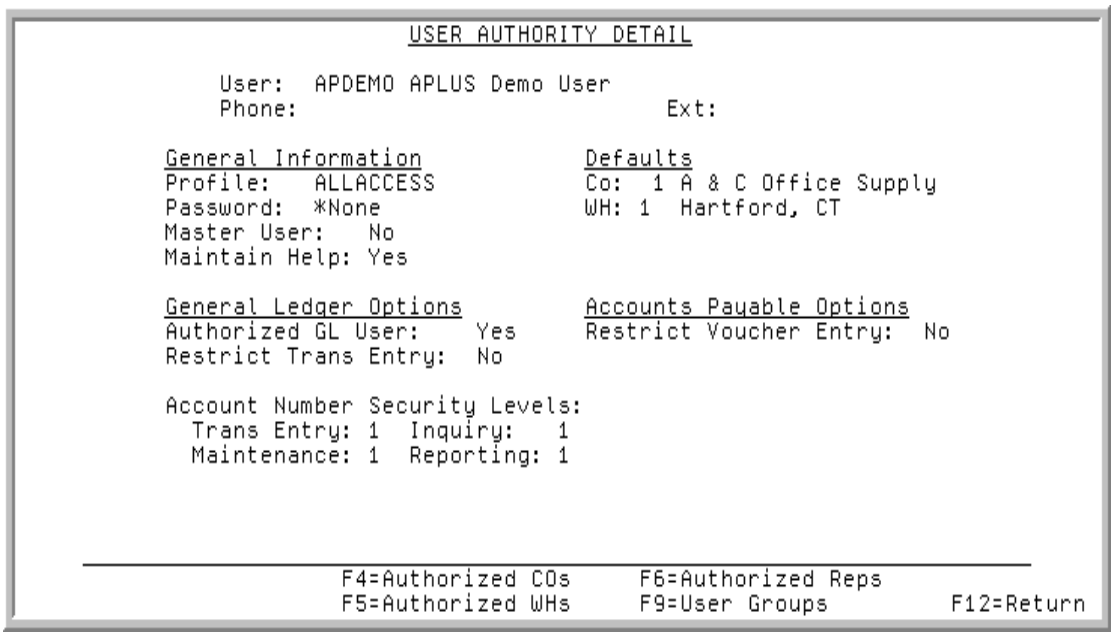
System (Authorization)	This field indicates if the user is authorized to access a specific company, warehouse, or salesrep. One of the following values may be displayed:
	• **Authorized** if any of the following are true:
	  • the security has not been activated through System Options Maintenance (MENU XAFILE)
	  • the user is a Master User
	  • the user's profile is set up to work with the company, warehouse, or salesrep via function keys in Authority Profile Maintenance (MENU XASCTY)
	• **Not Authorized** if none of the above are true.
	Display

Field/Function Key	Description

Function (Authorization)	This field displays the authorization for the specific company, warehouse, or salesrep based on the effective level of security for the user and function.
	One of the following values may be displayed:
	• **Authorized** if any of the following are true:
	  • the security has not been activated through System Options Maintenance (MENU XAFILE)
	  • the user is a Master User
	  • the user's profile is set up to work with the company, warehouse, or salesrep via function keys in Authority Profile Maintenance (MENU XASCTY)
	  • the effective security for this function and user is Bypass
	• **Not Applicable** if the effective security for the function is n/a.
	• **Not Authorized** if none of the above are true; the user is not authorized to this company, warehouse, or salesrep.
	Display

F12=Return	Press **F12=RETURN** to return to the previous screen.
Enter	After entering a Co, WH, and/or Rep, press **ENTER** to confirm your entries. The **System** and **Function** fields will be updated accordingly.

User Authority Detail Screen



This screen displays after entering a user and pressing **ENTER** on the Audit Access By User or User Group Screen. Use this screen to review the authority profile information for a specific user.

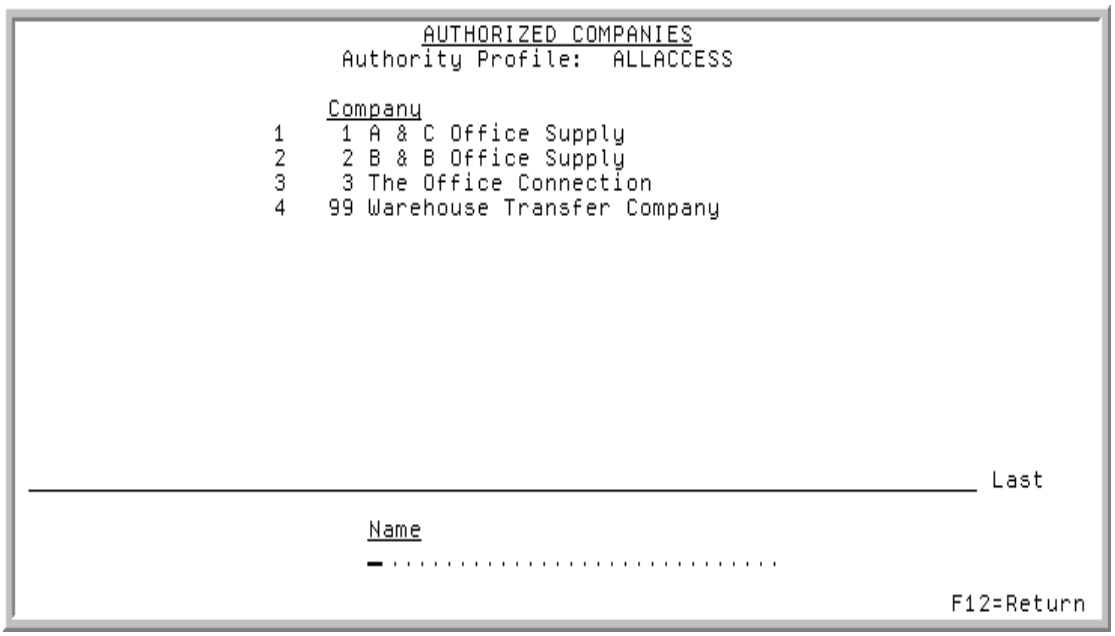
User Authority Detail Screen Fields and Function Keys

Field/Function Key	Description
User ID	The User ID and the first 34 characters of the user profile's name. Display
Phone and Ext	The country code, phone number, and extension, retrieved from the User Master File (USRMST). Display
Profile	This field displays ***Personal** if the user ID is the same as the authority profile for the user; otherwise, the public authority profile for this user ID will display. Display
Password	This field displays the password specified for this user (from the authority profile), if one is specified; otherwise, ***None** will display. Display
Master User	This field indicates by displaying **Yes** or **No** if this user is a Master User, based on the authority profile's Master User flag. Display

Field/Function Key	Description
Maintain Help	This field indicates by displaying **Yes** or **No** if this user is allowed to maintain help text, based on the authority profile's Allow Help Text Maintenance flag. Display
Defaults Co and WH	The following default information is displayed: **Co**: This field displays the default company and description, based on the user's authority profile. **WH**: This field displays the default warehouse and description, based on the user's authority profile. Display
General Ledger Options: Authorized GL User	This field indicates by displaying **Yes** or **No** if this user is an authorized General Ledger user, based on the authority profile's General Ledger **User Authority** flag. Display
General Ledger Options: Restrict Trans Entry	This field indicates by displaying **Yes** or **No** if this user is restricted to perform transaction entry functions, based on the authority profile's **Restrict Transaction Entry** user flag. Display
Accounts Payable Options: Restrict Voucher Entry	This field indicates by displaying **Yes** or **No** if this user is restricted to perform voucher entry functions, based on the authority profile's **Restrict Voucher Entry** user flag. Display
Account Number Security Levels	These fields display the General Ledger account number security levels for this user (based on the user's authority profile definition defined through Authority Profile Maintenance, MENU XASCTY) for Transaction Entry, Inquiry, File Maintenance, and Reporting functions. Account access security levels are assigned to provide or deny access to one or many G/L accounts. When setting up the chart of accounts through G/L Accounts Maintenance (MENU GLFILE), each account is assigned an account access security level from 1 (most secure) to 9 (least secure) for each of the four types of functions. A security level of 1 allows the user in the authority profile to have maximum access while a 9 allows minimum access to GL accounts. Note that if the user is a Master User, all security fields will be 1. Display
F4=Authorized COs	Press **F4=AUTHORIZED COS** to display the Authorized Companies Screen.

Field/Function Key	Description
F5=Authorized WHs	Press **F5=AUTHORIZED WHS** to display the Authorized Warehouses Screen.
F6=Authorized Reps	Press **F6=AUTHORIZED REPS** to display the Authorized SalesReps Screen.
F9=User Groups	Press **F9=USER GROUPS** to display the User Group Associations Screen.
F12=Return	Press **F12=RETURN** to return to the Audit Access By User or User Group Screen.

Authorized Companies Screen



This screen displays after pressing **F4=AUTHORIZED COS** on the User Authority Detail Screen. Use this screen to review the companies that the indicated authority profile is authorized to.

The user is automatically authorized to all companies if any of the following are true:

- company security has not been activated through System Options Maintenance (MENU XAFILE)

  If this is true, “Security Bypassed (System) - Authorized to All Companies” displays under the Authority Profile.

- the authority profile is set up as a Master User

  If this is true, “Master User - Authorized to All Companies” displays under the Authority Profile.

- the authority profile is set up to bypass company security

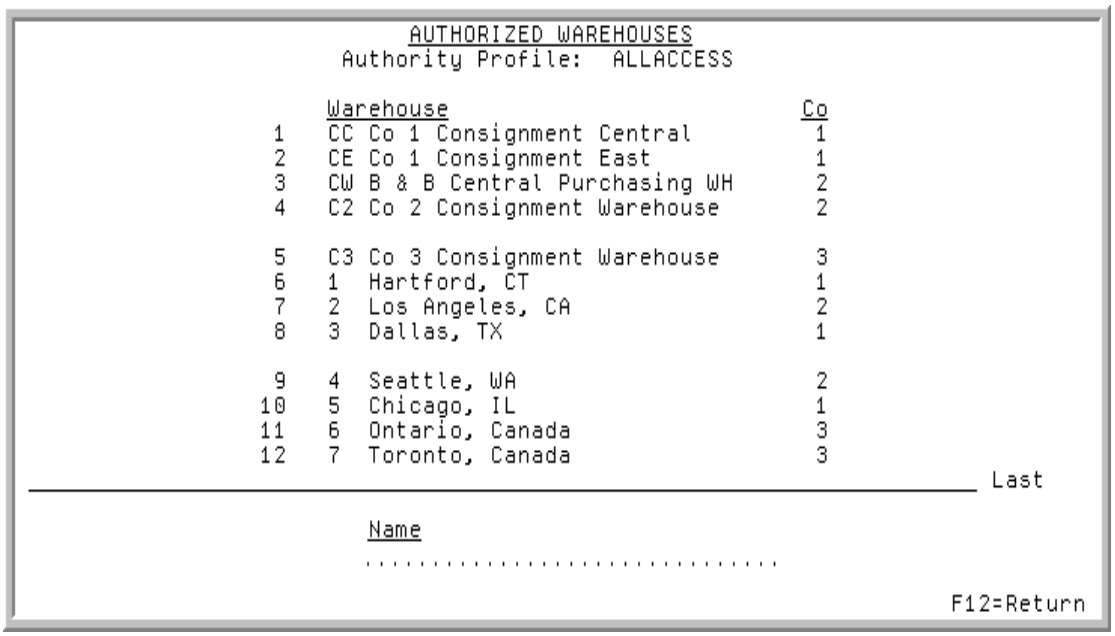
  If this is true, “Security Bypassed (User) - Authorized to All Companies” displays under the Authority Profile.

The lower portion of this screen provides a filter that allows you to limit the criteria on the screen based on the name of the company.

Authorized Companies Screen Fields and Function Keys

Field/Function Key	Description
(Reference Number)	The reference number of the company displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
Company	The number and name of the companies the user/user group is authorized to. Display
Name	Use this field to limit the screen to only those companies that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display companies, if any, matching your criteria. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the User Authority Detail Screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display companies, if any, matching your criteria.

Authorized Warehouses Screen



This screen displays after pressing **F5=AUTHORIZED WHS** on the User Authority Detail Screen. Use this screen to review the warehouses that the indicated authority profile is authorized to.

The user is automatically authorized to all warehouses if any of the following are true:

- warehouse security has not been activated through System Options Maintenance (MENU XAFILE)

  If this is true, “Security Bypassed (System) - Authorized to All Warehouses” displays under the Authority Profile.

- the authority profile is set up as a Master User

  If this is true, “Master User - Authorized to All Warehouses” displays under the Authority Profile.

- the authority profile is set up to bypass warehouse security

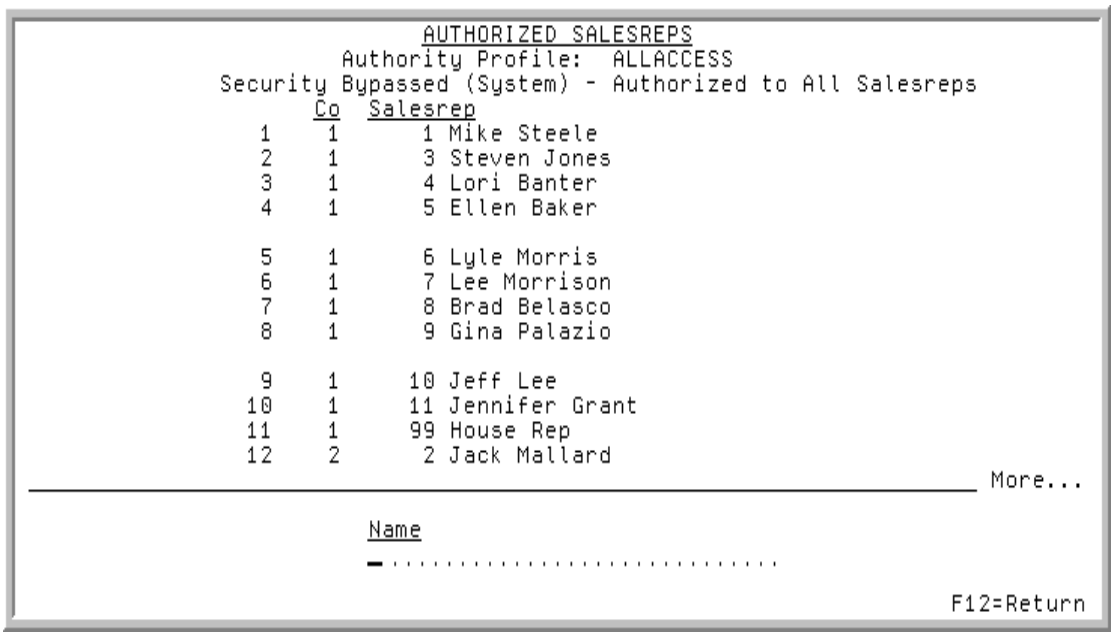
  If this is true, “Security Bypassed (User) - Authorized to All Warehouses” displays under the Authority Profile.

The lower portion of this screen provides a filter that allows you to limit the criteria on the screen based on the name of the warehouse.

Authorized Warehouses Screen Fields and Function Keys

Field/Function Key	Description
(Reference Number)	The reference number of the company displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
Warehouse	The number and name of the warehouse the user/user group is authorized to. Display
Co	The number of the company that owns the specified warehouse. Display
Name	Use this field to limit the screen to only those warehouses that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display warehouses, if any, matching your criteria. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the User Authority Detail Screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display warehouses, if any, matching your criteria.

Authorized SalesReps Screen



This screen displays after pressing **F6=AUTHORIZED REPS** on the User Authority Detail Screen. Use this screen to review the salesreps that the indicated authority profile is authorized to.

The user is automatically authorized to all salesreps if any of the following are true:

- salesrep security has not been activated through System Options Maintenance (MENU XAFILE)

  If this is true, “Security Bypassed (System) - Authorized to All Salesreps” displays under the Authority Profile.

- the authority profile is set up as a Master User

  If this is true, “Master User - Authorized to All Salesreps” displays under the Authority Profile.

- the authority profile is set up to bypass salesrep security

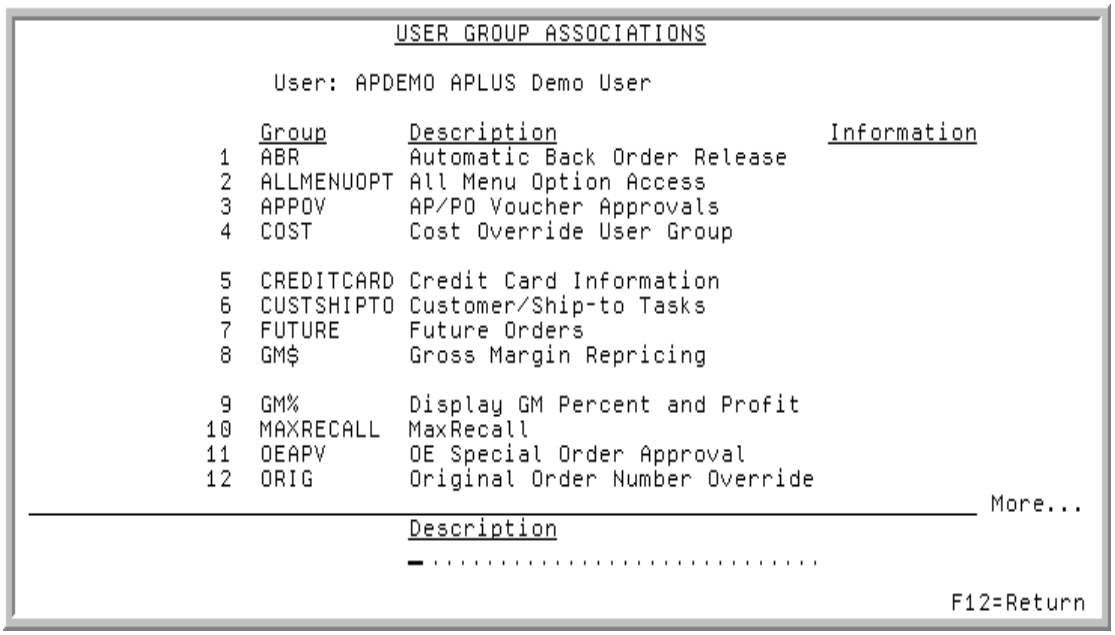
  If this is true, “Security Bypassed (User) - Authorized to All Salesreps” displays under the Authority Profile.

The lower portion of this screen provides a filter that allows you to limit the criteria on the screen based on the name of the salesrep.

Authorized SalesReps Screen Fields and Function Key

Field/Function Key	Description
(Reference Number)	The reference number of the company displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
Co	The number of the company that the sales rep is assigned to. Display
SalesRep	The number and name of the sales rep the user/user group is authorized to. Display
Name	Use this field to limit the screen to only those salesreps that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display salesreps, if any, matching your criteria. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the User Authority Detail Screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display salesreps, if any, matching your criteria.

User Group Associations Screen



This screen displays after pressing **F9=USER GROUPS** on the User Authority Detail Screen. Use this screen to review the user groups to which the indicated user belongs.

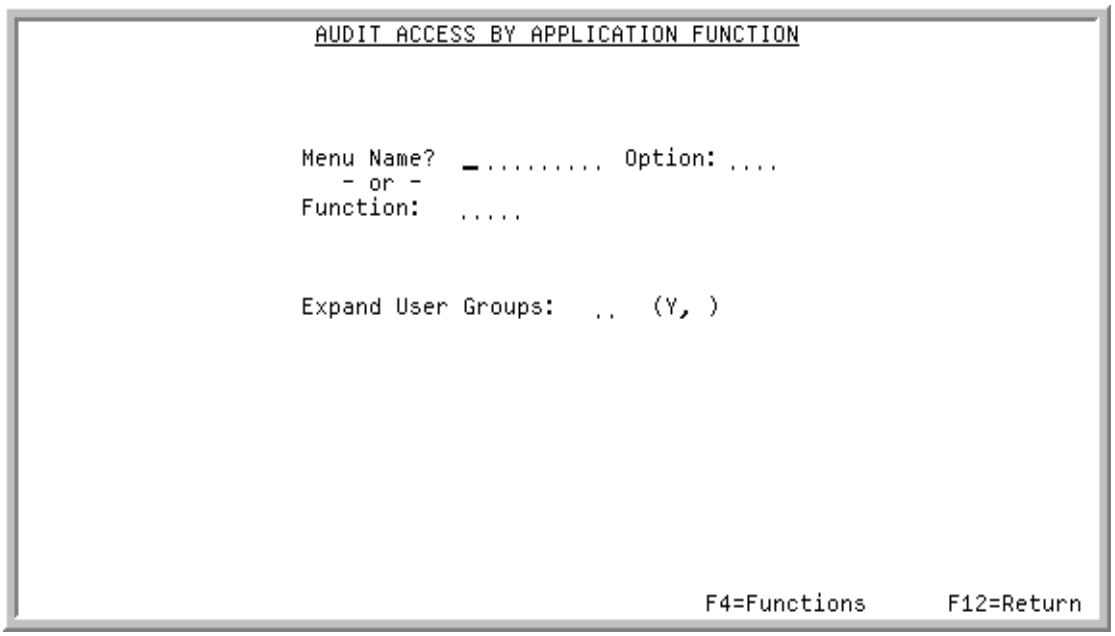
The lower portion of this screen provides a filter that allows you to limit the criteria on the screen based on the description of the group.

User Group Associations Screen Fields and Function Keys

Field/Function Key	Description
User	The User ID and name of the selected user. Display
(Reference Number)	The reference number of the user groups displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
Group	The user group name that the selected user is assigned to. Display
Description	The description of the user group assigned when the group was created/ maintained. Display

Field/Function Key	Description
Information	Indicates when the user group is no longer active by displaying Suspended in this column. Display
Description	Use this field to limit the screen to only those groups that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display groups, if any, matching your criteria. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the User Authority Detail Screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display groups, if any, matching your criteria.

Audit Access By Application Function Screen



This screen displays after keying **2** for Application Function in the **Audit Access By** field on the Security Audit Inquiry Selection Screen. Use this screen to inquire into access authorities for a specific application function, allowing you to review the users and user groups that are allowed access to a specific menu option.

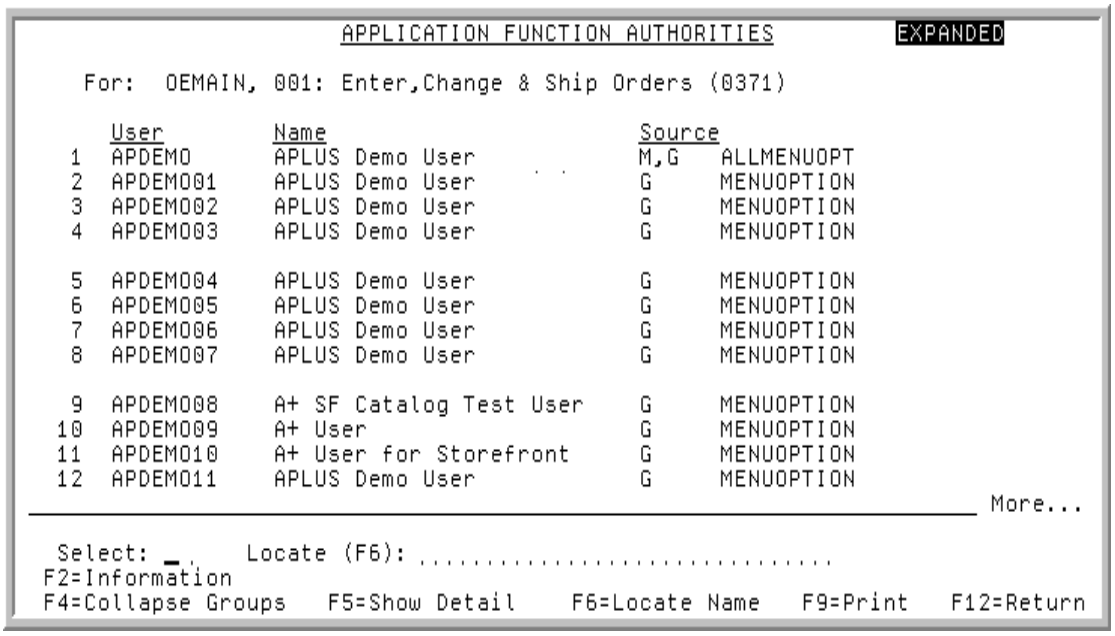
You can select to inquire into information based on a Menu Name and Option or a particular Function. You also have the option to expand user groups and display a list of menu options available on the selected menu (if one was keyed).

Audit Access By Application Function Screen Fields and Function Keys

Field/Function Key	Description
Menu Name / Option	Use this field to inquire into access authorities for a particular menu and option number (an option number must be keyed if you select to inquire into information based on the menu name). Key the menu name and number of the option on the menu you want to review access authorities for. **Valid Values:** A valid menu in the Menu Master File (MNUMST) that contains the option to have its authority rights displayed; a valid option number must also be keyed. (A 10 / N3,0) Optional/Required

Field/Function Key	Description
Function	Use this field to inquire into access authorities for a particular function. Key the function ID you want to review access authorities for. A function ID is a unique 4 character ID associated with each application function. A function is the actual application process that is behind a menu option. While a function is unique, the same function could be accessed by more than one menu option. If you enter a function ID, leave the **Menu Name** and **Option** fields blank. In order to key a Menu Name and Option number (if you enter a function ID), the function ID must belong to the menu and option you entered. **Note:** Once you enter a function and proceed to the next screen, the description of the menu option will be displayed following the function ID. **Valid Values:** A valid function ID in the Function Master File (FNCMST). (N 4,0) Optional/Required
Expand User Groups	This field determines what screen mode you want to access on the Application Function Authorities Screen. Key **Y** in this field if you want the Application Function Authorities Screen to default to the 'expanded' mode. If the screen defaults to the expanded mode, all the users that are part of the user groups will be displayed in place of the user group, if the user group authorizations are present for the selected menu option. Leave this field blank if you want the Application Function Authorities Screen to default to the 'collapsed' mode. If the screen defaults to the collapsed mode, all user groups and users that are authorized to this function will display. (A1) Optional
F4=Functions	Press **F4=FUNCTIONS** to display the Application Functions Screen, where you can review a list of menu options available for the selected menu, if one was keyed.
F12=Return	Press **F12=RETURN** to return to the Security Audit Inquiry Selection Screen without saving entries on this screen.
Enter	Press **ENTER** to confirm your entries and proceed to the Application Function Authorities Screen, which will display either in the expanded mode or collapsed mode, depending on your entry in the **Expand User Groups** field on this screen.

Application Function Authorities Screen



This screen displays after pressing **ENTER** on the Audit Access By Application Function Screen. If you left the **Expand User Groups** field blank on the Audit Access By Application Function Screen, this screen will default to the 'collapsed' mode (the mode of the screen above). If you keyed **Y** in the **Expand User Groups** field on the Audit Access By Application Function Screen, this screen will default to the 'expanded' mode. In the expanded mode, all of the users that are part of the user groups are displayed in place of the user group, if the user group authorizations are present for the selected menu option. The appearance of this screen changes based on the type of mode selected; those differences will be noted in this section.

Use this screen to review the users and user groups that have access authority to the selected menu option/function (collapsed mode) or the users only that have access to the menu option/function (expanded mode).

Note: In the collapsed mode, any users within an authorized group will only display if the user is authorized to the function or is a Master User. In the expanded mode, all users within the function's authorized groups will display for review.

Application Function Authorities Screen Fields and Function Keys

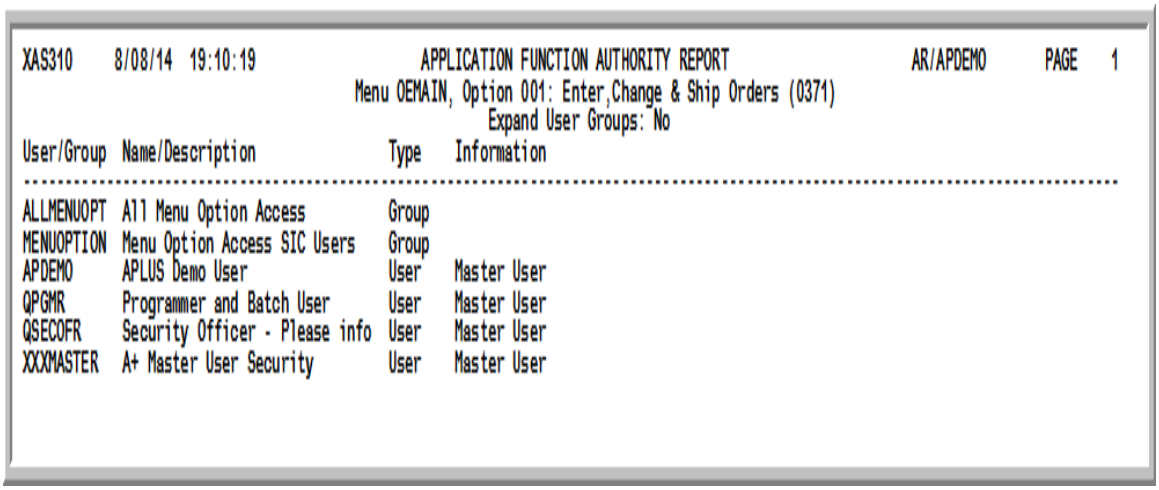
Field/Function Key	Description
For	The menu name, option number, menu option description, and assigned function code based on the selection criteria from the previous screen. Display

Field/Function Key	Description
(Reference Number)	The reference number of the users and user groups displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
User User/Group	In expanded mode, the ID of the user that has access authority to the selected menu option/function. In collapsed mode, the User ID of the user or the Group ID of the user group that has access authority to the selected menu option/function. Display
Name Name/Description	In expanded mode, the name of the user. In collapsed mode, the name of the user and the description of the user group Display
Source	This column displays for collapsed mode and is available in expanded mode with the **F2=INFORMATION / F2=SOURCE** function key. Source is the type of authorization: • **U** displays if the User level authorization is present; that is, a record exists in the Function Authority File for this user. • **M** displays if Master User authorization is present; that is, this user is set up as a Master User. • **G** displays if Group level authorizations are present; that is, the user belongs to groups that are set up with function authority. If this is the case, the groups will appear to the right of the G. If not all group information can be provide due to space limitations, a '+' sign will display in the last position of the **Source** field. Display
Information	This column displays for collapsed mode and is available in expanded mode with the **F2=INFORMATION / F2=SOURCE** function key. Information indicates if the user is a Master User or if the user is Suspended. Display

Field/Function Key	Description
Type	This column only displays for collapsed mode. Type indicates **User** for a user or **Group** for a user group. Display
Select	Use this field to inquire into further access details for the selected user or user group. Key the corresponding selection number of the user or user group you want to choose, and press **ENTER** to proceed to the User/User Group Access Full Details Screen. (N 2,0) Optional
Locate (F6)	Use this field in conjunction with the **F6=LOCATE NAME** key to locate a user's name or group's description you want displayed on the first line of this screen. Key search criteria and press **F6=LOCATE NAME**. The screen will refresh and display the user or user group, if any, matching your criteria. (A 30) Optional
F2=Information / F2=Source	The **F2=INFORMATION / F2=SOURCE** function key displays only in the expanded mode (accessed by keying Y in the Expand User Groups field on the Audit Access By Application Function Screen, or if you toggle the **F4=COLLAPSE GROUPS** function key on this screen to display collapse groups). Press **F2=INFORMATION / F2=SOURCE** to toggle between displaying information for users (indicating if the user is a **Master User** or if user is **Suspended**) or the type of source (indicating if **U**ser, **M**aster, or **G**roup level authorizations are present for the user).
F4=Expand Groups / Collapse Groups	Press **F4=EXPAND GROUPS / F4=COLLAPSE GROUPS** to change the mode of the screen to either the expanded mode or the collapsed mode. The default mode of the screen is the collapsed mode, unless **Y** was keyed in the **Expand User Groups** field on the Audit Access By Application Function Screen.
F5=Show Detail	After selecting a user, press **F5=SHOW DETAIL** to display the User Authority Detail Screen. After selecting a user group, press **F5=SHOW DETAIL** to display the User Group Details Screen.

Field/Function Key	Description
F6=Locate Name	Use the **F6=LOCATE NAME** key in conjunction with the **Locate** field to locate a user's name or group's description you want displayed on the first line of this screen. After keying search criteria in the **Locate** field, press **F6=LOCATE NAME** to display the user or user group, if any, matching your criteria.
F9=Print	Press **F9=PRINT** to print the Application Function Authority Report. Prior to the report printing, the Report Option Screen displays. On the Report Option Screen, select to print the report interactively (the report cannot be submitted to batch). Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
Enter	After selecting a user or user group, press **ENTER** to proceed to the User/User Group Access Full Details Screen.

Application Function Authority Report



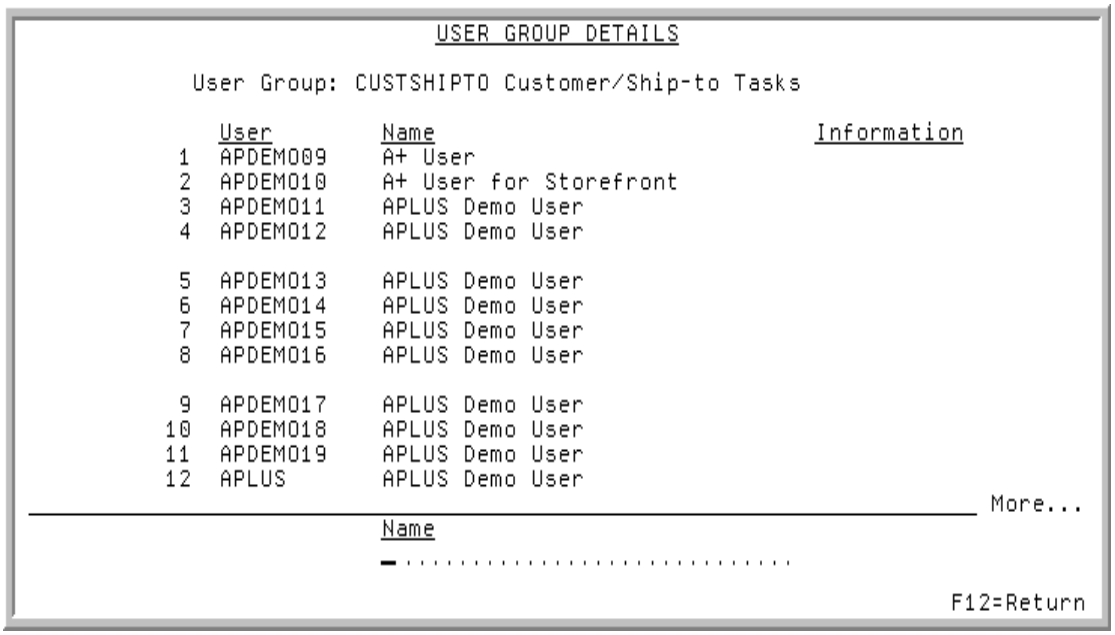
```
XAS310    8/08/14  19:10:19              APPLICATION FUNCTION AUTHORITY REPORT                AR/APDEMO      PAGE    1
                                  Menu OEMAIN, Option 001: Enter,Change & Ship Orders (0371)
                                                  Expand User Groups: No
User/Group  Name/Description             Type    Information
-------------------------------------------------------------------------------------------------------------------
ALLMENUOPT  All Menu Option Access       Group
MENUOPTION  Menu Option Access SIC Users Group
APDEMO      APLUS Demo User              User    Master User
QPGMR       Programmer and Batch User    User    Master User
QSECOFR     Security Officer - Please info User  Master User
XXXMASTER   A+ Master User Security      User    Master User
```

This report prints after pressing **ENTER** on the Report Option Screen, which displayed after pressing **F9=PRINT** on the Application Function Authorities Screen. On the Report Option Screen, select to print the report interactively (the report cannot be submitted to batch). Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen.

Use this report to review the users and user groups that have access authority to the selected menu option/function. Information from the Application Function Authorities Screen is printed.

Note: The fields that print on this report change depending on if the Application Function Authorities Screen was in the expanded or collapsed mode when you pressed **F9**. For a description of the fields on this report, refer to the Application Function Authorities Screen.

User Group Details Screen



This screen displays after selecting a user group and pressing **F5=SHOW DETAIL** on the Application Function Authorities Screen or Application Action Authorities Screen. It also displays after entering a user group and pressing **ENTER** on the Audit Access By User or User Group Screen.

Use this screen to review the users that are included in the selected user group.

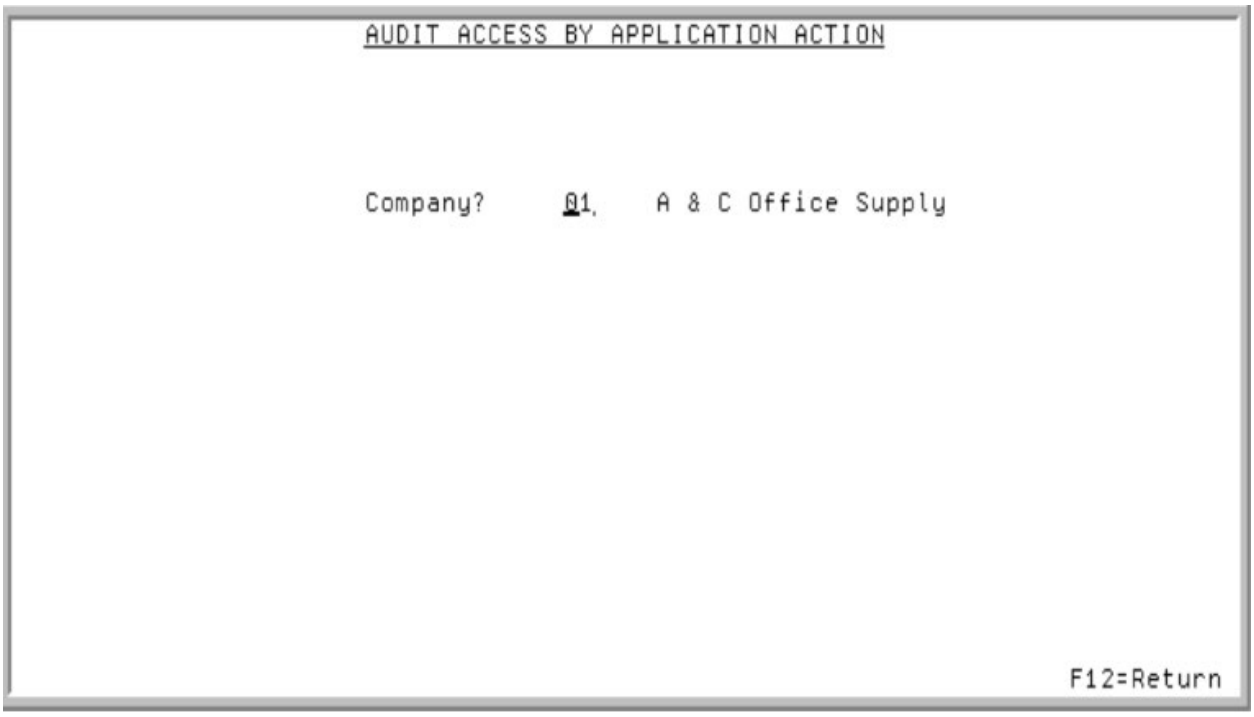
The lower portion of this screen provides a filter that allows you to limit the criteria on the screen based on the name of the user.

User Group Details Screen Fields and Function Keys

Field/Function Key	Description
User Group	The User Group ID and description Display
(Reference Number)	The reference number of the users displayed on this screen. This number is **1** through **12** for the twelve lines that may display. When rolling forward or backward, the reference numbers do not change. Display
User	The user ID assigned to the selected user group. Display
Name	The user name from the IBM i user profile. Display

Field/Function Key	Description
Information	The information about the users indicating if the user is a **Master User** or a **Suspended User** through User Maintenance (MENU XASCTY). Display
Name	Use this field to limit the screen to only those users that match the criteria you key in this field. Key the criteria and press **ENTER**. The screen will refresh and display users, if any, matching your criteria. (A 30) Optional
F12=Return	Press **F12=RETURN** to return to the previous screen.
Enter	After entering filter criteria on this screen, press **ENTER** to confirm your entry. The screen will refresh and display users, if any, matching your criteria.

Audit Access By Application Action Screen



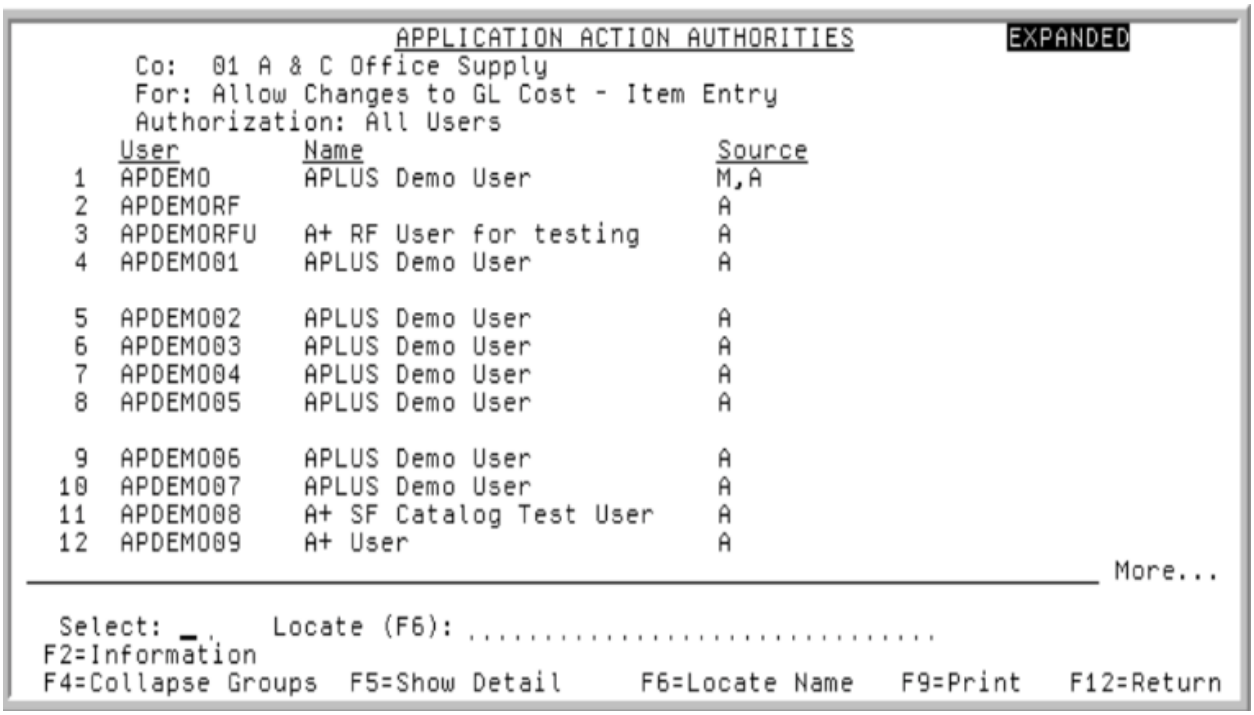
This screen displays after keying **3** for Application Action in the **Audit Access By** field on the Security Audit Inquiry Selection Screen. Use this screen to key the company number for which you want to inquire into access authorities for a specific application action (for example, changes to blanket orders, changes to item cost, etc.).

Audit Access By Application Action Screen Fields and Function Keys

Field/Function Key	Description
Company	This field is protected if **Multi-Company** is **N** in System Options Maintenance (MENU XAFILE). Key the company number for which you want to inquire into access authorities for a specific application action. **Default Value:** The default company defined on the Authority Profile Definition Screen accessed through User or Authority Profile Maintenance on the Distribution A+ Security Menu (MENU XASCTY) if one has been defined; otherwise, this is the default company defined through System Options Maintenance (MENU XAFILE). **Valid Values:** Any valid company number that has been created through Company Name Maintenance (MENU XAFILE). (N 2,0) Required

Field/Function Key	Description
F12=Return	Press **F12=RETURN** to return to the previous screen.
Enter	After entering a company number, press **ENTER** to confirm your entry and proceed to the Application Action Inquiry Screen which will display all available actions associated with the company.

Application Action Authorities Screen



This screen displays after selecting an application action and pressing **F6=ACTION AUTHORITY** on the Application Action Inquiry Screen. The default mode of this screen is the collapsed mode, unless the action is set up with an authorization of **A** for All Users, then the expanded mode will display. In the expanded mode, all of the users that are part of the user groups are displayed in place of the user group, if the user group authorizations are present for the selected application action. The appearance of this screen changes based on the type of mode displayed; those differences will be noted in this section.

Use this screen to review the users and user groups that have access authority to the selected application action (collapsed mode) or the users only that have access to the application action (expanded mode).

Note: In the collapsed mode, any users within an authorized group will only display if the user is authorized to the action or is a Master User. In the expanded mode, all users within the action's authorized groups will display for review.

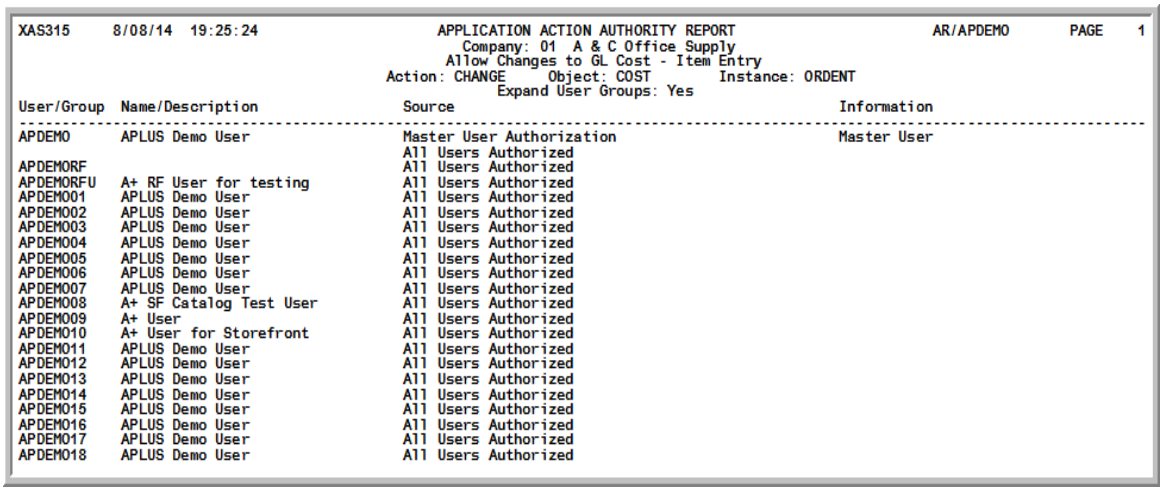
Application Action Authorities Screen Fields and Function Keys

Field/Function Key	Description
Co	The company for the selected action authority upon which the displayed information is based.

Field/Function Key	Description
User	The ID of the user that has access authority to the selected application action. Display
Group	The ID of the user group that has access authority to the selected application action. Display
Name	The name of the user. Display
Description	The description of the user group. Display
Type	Type indicates **User** for a user or **Group** for a group. Display
Source	Source is the type of authorization: • **U** displays if the User level authorization is present; that is, a record exists in the Action Authority File for this user. • **M** displays if Master User authorization is present; that is, this user is set up as a Master User. • **A** displays if this user is authorized since all users are authorized to this action. • **G** displays if Group level authorizations are present; that is, the user belongs to groups that are set up with action authority. If this is the case, the groups will appear to the right of the **G**. If not, all group information can be provide due to space limitations, a '+' sign will display in the last position of the **Source** field. Display
Information	Information indicates if the user is a **Master User** or if the user or user group is a **Suspended User**. Display
Select	This field is not available for user groups. Use this field to inquire into general action authority details for a particular user. Key the corresponding selection number of the user you want to choose, and press **ENTER** to proceed to the Action Authority Detail Screen. (N 2,0) Optional

Field/Function Key	Description
Locate (F6)	Use this field in conjunction with the **F6=LOCATE NAME** key to locate a user's name or group's description you want displayed on the first line of this screen. Key search criteria and press **F6=LOCATE NAME**. The screen will refresh and display the user or user group, if any, matching your criteria. (A 30) Optional
F2=Information / F2=Source	This function key displays only in the expanded mode or if you toggle the **F4=EXPAND GROUPS / F4=COLLAPSE GROUPS** function key on this screen to display collapse groups. Press **F2=INFORMATION / F2=SOURCE** to toggle between displaying information for users (indicating if the user is a **Master User** or **Suspended User**) or the type of source (indicating if **U**ser, **M**aster, or **G**roup level authorizations are present for the user).
F4=Expand Groups / F4=Collapse Groups	Press **F4=EXPAND GROUPS / F4=COLLAPSE GROUPS** to change the mode of the screen to either the expanded mode or the collapsed mode.
F5=Show Detail	After selecting a user, press **F5=SHOW DETAIL** to display the User Authority Detail Screen. After selecting a user group, press **F5=SHOW DETAIL** to display the User Group Details Screen.
F6=Locate Name	Use this function key in conjunction with the **Locate** field to locate a user's name or group's description you want displayed on the first line of this screen. After keying search criteria in the **Locate** field, press **F6=LOCATE NAME** to display the user or user group, if any, matching your criteria.
F9=Print	Press **F9=PRINT** to print the Application Action Authority Report. Prior to the report printing, the Report Option Screen displays. On the Report Option Screen, select to print the report interactively (the report cannot be submitted to batch). Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen.
F12=Return	Press **F12=RETURN** to return to the previous screen without saving entries on this screen.
Enter	After selecting a user, press **ENTER** to proceed to the Action Authority Detail Screen.

Application Action Authority Report



```
XAS315     8/08/14  19:25:24          APPLICATION ACTION AUTHORITY REPORT                AR/APDEMO     PAGE    1
                                        Company: 01  A & C Office Supply
                                      Allow Changes to GL Cost - Item Entry
                                 Action: CHANGE     Object: COST       Instance: ORDENT
                                            Expand User Groups: Yes
User/Group  Name/Description              Source                                  Information
-------------------------------------------------------------------------------------------------------------------
APDEMO      APLUS Demo User               Master User Authorization               Master User
                                          All Users Authorized
APDEMORF                                  All Users Authorized
APDEMORFU   A+ RF User for testing        All Users Authorized
APDEMO01    APLUS Demo User               All Users Authorized
APDEMO02    APLUS Demo User               All Users Authorized
APDEMO03    APLUS Demo User               All Users Authorized
APDEMO04    APLUS Demo User               All Users Authorized
APDEMO05    APLUS Demo User               All Users Authorized
APDEMO06    APLUS Demo User               All Users Authorized
APDEMO07    APLUS Demo User               All Users Authorized
APDEMO08    A+ SF Catalog Test User       All Users Authorized
APDEMO09    A+ User                       All Users Authorized
APDEMO10    A+ User for Storefront        All Users Authorized
APDEMO11    APLUS Demo User               All Users Authorized
APDEMO12    APLUS Demo User               All Users Authorized
APDEMO13    APLUS Demo User               All Users Authorized
APDEMO14    APLUS Demo User               All Users Authorized
APDEMO15    APLUS Demo User               All Users Authorized
APDEMO16    APLUS Demo User               All Users Authorized
APDEMO17    APLUS Demo User               All Users Authorized
APDEMO18    APLUS Demo User               All Users Authorized
```

This report prints after pressing **ENTER** on the Report Option Screen, which displayed after pressing **F9=PRINT** on the Application Action Authorities Screen. On the Report Option Screen, select to print the report interactively (the report cannot be submitted to batch). Refer to the Appendix section of the Infor Distribution A+ Cross Applications User Guide for details about the Report Option Screen.

Use this report to review the users and user groups that have access authority to the selected application action. Information from the Application Action Authorities Screen is printed.

Note: The fields that print on this report change depending on if the Application Action Authorities Screen was in the expanded or collapsed mode when you pressed **F9**. For a description of the fields on this report, refer to the Application Action Authorities Screen.

Appendix A User Security Technical Notes

This section describes technical functions that you should be aware of due to the Distribution A+ User Security Feature. We recommend that you review this section before you begin the installation of Distribution A+ Version 6.0 Cumulative 5 or later.

Security Functions Service Program XA950S

A service program has been created to contain the defined functions that will perform all security checking logic. This service program will be bound by reference to all application programs that require the use of a security routine. The functions that are contained in this service program are listed in this section. Tables in this section contain definitions of each function, its inputs (arguments) and its outputs (return value) and an example of its usage.

Binding directories (a map for the RPG compiler) has been created for each program that will have this service program bound. This will simplify the process to compile these programs assuring that the security functions are available to the application program.

Each application program requiring these security functions will contain an additional H spec to define the binding directory and a /copy statement to include the prototype statements used to create this program correctly. By using this method, these ILE programs can be compiled the same way as programs that are not bound to the service program. They can be compiled using the CRTBNDRPG command. This means that the command N4 can be used to create these programs without any special options or additional binding steps. An example of an H spec entry is: H BNDDIR('OE101A'). This needs to be placed at the top of any program that requires a security function immediately following the line /COPY QCPYSRC,H_SPEC and the prototype statements required for each program using security functions as follows: /COPY QCPYSRC,P_XA950S.

Security Function Directory

ChkActAut - Check if a user is authorized to a GL Account	
Export: ***YES**	Usage: Authorized=ChkActAut (@user : @acno : @type : @cono); If ChkActAut (@user : @acno : @type : @cono);
Received: User Id (A10)Authorized = ChkActAut(@user : @acno : @type : @cono); GL Acct No (N7,0) Usage Type (A1) Company No (N2,0)If ChkActAut(@user : @acno : @type : @cono)	
Returned: Authorized (logical)	
1 If GL Security is not active, user is authorized. **2 If the user is a "Master" user, then the user is authorized.** **3 If GL account groups are active and the user is in the account group and if account level security is active and the account level of the account is greater than or equal to the users account level, then the user is authorized.**	

ChkMstUsr - Check if a user is a master user	
Export: ***YES**	Usage: MasterUser= ChkMstUsr(@user); If ChkMstUsr(@user); - or - MasterUser = ChkMstUsr(@user : @cono); if ChkMstUsr(@user : @cono);
Received: • User Id (A10) • Company No (N2,0)	
Returned: • MasterUser (Logical)	

1 If user security is not active, the user is authorized. **2 If the user is the master user (System options), then the user is authorized.** **3 * If the user is the master user for the company (Company Name) or if the company master user is a group that the user is in, then the user is authorized.** **4 If the user is a master user (Authority Profile), then the user is authorized.** *** Optional (Note passing a company is optional)**

UsrInGrp - Check to see if a user is in a user group	
Export: ***YES**	Usage: InGroup = UsrInGrp(@user : @group); if UsrInGrp(@user : @group);
Received: • User Group (A10) • User Id (A10)	
Returned: • InGroup (Logical)	
1 If the user passed is in the group passed, then the user is authorized.	

GetGLLvl - Get the users GL Account Authority Level	
Export: ***YES**	Usage: SecLvl = GetGLLvl(@user : @type); if GetGLLvl(@user : @type);
Received: • User ID (A10) • Type (A1)	
Returned: • SecLvl (1,0)	

1 This function returns the users GL Account security level as defined by the user profile. ***Note*** Type: M=Maintenance, T=Transaction Entry, I=Inquiry and R=Report. The returned level is a number from 1 to 9

ChkCoAut - Check if a user or group is authorized to a company.	
Export: ***YES**	Usage: Authorized = ChkCoAut(@user : @cono1 {: @cono2}); If ChkCoAut(@user : @cono1 {: @cono2});
Received: • User Id (A10) • Company No (N2,0) • Company No 2 (N2,0)* *Optional {}	
Returned: • Authorized (Logical)	
1 If company authority (System Options) is not activated, then the user is authorized. **2 If the user profile (Authority Master) does not require company authority checking, then the user is authorized.** **3 If the function being accessed (Function Master) does not require company authority checking, then the user is authorized.** **4 If the function being accessed does not require company authorization for the user accessing (Function Authority), then the user is authorized.** **5 If the user has an entry for the company being accessed (Authorized Companies), then the user is authorized.**	

****Notes****

- If a second company is passed, then the check is performed as a range (from/to). The user will receive authorization only if all companies in the range are authorized.
- If only one company is passed and has a value of zero (0), then the user must have all companies to allow authorization.

ChkWhAut - Check if a user or group is authorized to a warehouse	
Export: ***YES**	Usage:
Received: • User Id (A10) • Warehouse No (A2) • Warehouse No 2 (A2)* *Optional {}	Authorized = ChkWhAut(@user : @whid1 {: @whid2});
Returned: • Authorized (Logical)	If ChkWhAut(@user : @whid1 {: whid2});

1. **If warehouse authority (System Options) is not activated, then the user is authorized.**
2. **If the user profile (Authority Master) does not require warehouse authority checking, then the user is authorized.**
3. **If the function being accessed (Function Master) does not require warehouse authority checking, then the user is authorized.**
4. **If the function being accessed does not require warehouse authorization for the user accessing (Function Authority), then the user is authorized.**
5. **If the user has an entry for the warehouse being accessed (Authorized Warehouses), then the user is authorized.**

****Notes****

• If a second warehouse is passed, then the check is performed as a range (from/to). The user will only receive authorization if all warehouses in the range are authorized. • If only one warehouse is passed and has a value of zero (0), then the user must be authorized to all warehouses.	

ChkRepAut: Check if a user or group is authorized to a sales rep	
Export: ***YES**	Usage: Authorized = ChkWhAut(@user : @whid1 {: @whid2}); If ChkWhAut(@user : @whid1 {: whid2});
Received: • User Id (10A) • Warehouse No (2A) • Warehouse No 2 (2A)* *Optional {}	
Returned: • Authorized (Logical)	

1 If sales rep authority (System Options) is not activated then the user is authorized.

2 If the user profile (Authority Master) does not require sales rep authority checking than the user is authorized.

3 If the function being accessed (Function Master) does not require sales rep authority checking than the user is authorized.

4 If the function being accessed does not require sales rep authorization for the user accessing (Function Authority) then the user is authorized.

5 If the user has an entry for the Sales Rep being accessed (Authorized Salesreps) than the user is authorized.

****Notes****

1	**Authorization will only be checked for the number of sales reps that are passed. If only one rep is passed than the user must be authorized to that rep if more than one rep is passed then the user must be authorized to at least one of the reps that are passed.**

GetAutUsr - Returns the authority profile for the user	
Export: ***YES**	Usage: AuthValue = GetAutUsr(@user);
Received: • User Id (A10)	
Returned: • AuthValue (A10)	
1 Returns the personal or generic profile name that is used to determine a given users general authorities. **2 Personal authority profiles are always the same as the user id and cannot be shared.** **3 Generic profiles are used to define users in groups.**	

ChkFncAut - Is a User or Group is Authorized to a given application function	
Export: ***YES**	Usage: Authorized = ChkFncAut(@user : @fnid); if ChkFncAut(@user : @fnid);
Received: • User Id (A10) • Function Id (A4)	
Returned: • Authorized(logical)	

1. **If program security is not active, then the user is authorized.**
2. **If the user is suspended, then the user is not authorized.**
3. **If the user has a generic profile and that profile is suspended, then the user is not authorized.**
4. **If the user has been given authority to the function (Entry in Function Authority File for the user), then the user is authorized.**
5. **If a user is in an unsuspended group that has authority to the function, then the user is authorized.**

ChkUsrSus - Check if a user has been suspended.	
Export: ***YES**	Usage: Suspended = ChkUsrSus(@user); If Suspended = ChkUsrSus(@user);
Received: • User Id (A10)	
Returned: • Suspended(logical)	

1. **If the suspend flag is set in the User Master File (USRMST), then the function will return a logical yes/true.**

ChkPrfSus - Check if a generic authority profile has been suspended.	
Export: ***YES**	Usage:
Received: • Profile Id (A10)	

Returned: • Suspended(logical)	Suspended = ChkPrfSus(@prfid); If Suspended = ChkPrfSus(@prfid);
1 If the suspend flag is set in the Authority Master File (AUTMST), then the function will return a logical yes/true.	

GetGrpNam - Return the name (description) of a user group.	
Export: ***YES**	Usage: description = GetGrpNam(@group); If GetGrpNam(@group) = '*Not-Found';
Received: • User Group (A10)	
Returned: • Description(A30)	
1 Returns the description or name of the user group. If the group is not found, then the function will return the value "*Not-Found".	

GetUsrPass - Return the users password.	
Export: ***YES**	Usage: password = GetUsrPass(@User); If GetUsrPass(@user) = '*Not';
Received: • User Id (A10)	
Returned: • Password(A4)	
1 Returns the password of the user passed to the function. If the user has a password the function will return the value "*Not".	

ChkGLUsr - Check is a user is a GL user	
Export: ***YES**	Usage: GLUser = ChkGLUsr(@User); If ChkGLUsr(@User);
Received: • User Id (A10)	
Returned: • GLUser(Logical)	
1 If the user is defined as a GL user in the Authority Master File (AUTMST), then the function will return a logical yes/true.	

GLUsrSec - Check if GL user security is active	
Export: ***YES**	Usage: active = GLUsrSec(); If GLUsrSec();
Received: • *none	
Returned: • Active(Logical)	
1 If GL User Security is active (GL System Options), then the function will return a logical yes/true.	

RstVchEnt - Restrict Voucher Entry	
Export: ***YES**	Usage: restrict = RstVchEnt (@user); If RstVchEnt (@user);
Received: • User Id (A10)	
Returned: • Restrict(Logical)	
1 If restricted voucher entry is required for this user (Authority Master), then the function will return a logical yes/true.	

RstGLTrEnt - Restrict GL Transaction Entry	
Export: ***YES**	Usage: restrict = RstGLTrEnt (@user); If RstGLTrEnt (@user);
Received: • User Id (A10)	
Returned: • Restrict (Logical)	
1 If restricted GL transaction entry is required for this user (Authority Master), then the function will return a logical yes/true.	

AlwHlpMnt - Help Text Maintenance allowed	
Export: ***YES**	Usage: allowed = AlwHlpMnt (@user); If AlwHlpMnt (@user);
Received: • User Id (A10)	
Returned: • Allowed (Logical)	
1 If Help Text Maintenance is allowed for this user (Authority Master), then the function will return a logical yes/true.	

SecLvlAct: Check if GL Account Level and/or Group Security are active	
Export: ***NO**	Usage: Values = SecLvlAct(@cono); If subst(SecLvlAct(@cono) : 1 : 1) = 'Y'; If subst(SecLvlAct(@cono) : 2 : 1) = 'Y';
Received: • Company Number	
Returned: • Values (A2)	
1 Checks the GL Company Options record to determine if GL Account Level security and GL Account Group Security is active. **2 This function returns a 2 character value. The first position contains the Account level security Flag and the second position contains the Account Group security flag.**	

GetFncId: Get the current jobs function Id (security id)	
Export: ***YES**	Usage: id = GetFncId(); if GetFncId() = '1234';
Received: • *NONE	
Returned: • Function Id (A4)	
1 This function is used to retrieve the current application function id. This is used when one application function is called from within another application function and the current function needs to be saved in order to be refreshed after the called application function returns control to the calling application function.	

UpdFncId: Update the current jobs function id (security id)	
Export: ***YES**	Usage: UpdFncId(id);
Received: • Function Id (A4)	
Returned: • *NOBE	
1 This function is used to update the current application function id. This is used when one application function is called from within another application function and the current function needs to refresh the jobs stored function id after the called application function returns control to the calling application function.	

ChkFncInst: Check if a function is part of an installed application	
Export: ***YES**	Usage: Installed = ChkFncInst(@@fnid); If ChkFncInst(@@fnid);
Received: • Function Id (A4)	
Returned: • Installed (Logical)	
1 This function checks to see if the function Id that is passed to it is part of an installed application.	

ChkAppInst: Check if an application is installed	
Export: ***YES**	Usage: Installed = ChkAppInst(@@apid); If ChkAppInst(@@apid);
Received: • Application Id (A2)	
Returned: • Installed (Logical)	
1 This function checks to see if the Application Id that is passed is an installed application.	

<table>
<tr><td>ChkActionAut: Check if a user (or clerk) is authorized to an Application Action</td><td></td></tr>
<tr><td>Export:
*YES</td><td rowspan="3">Usage:

Authorized = ChkActionAut(@user : @cono : @whid : @Action : @object {: @instance} {: @extInst} {: @bypass});

If ChkActionAut(@user : @cono : @whid @Action : @object {:@instance} {: @extInst} {: @bypass);</td></tr>
<tr><td>Received:
• User Id (10A)
• Company No (2,0)
• Warehouse No 2 (2A)
• Action (10A)
• Object (10A)
• Instance (10A)*
• Inst Extender (10A)*
• Bypass Auth Code (Logical)*
*Optional {}</td></tr>
<tr><td>Returned:
• Authorized (Logical)</td></tr>
<tr><td colspan="2">1 All of the parameters are passed as values therefore constant values such as 'ENTER' and
2 *BLANKS are valid.
3 The user parameter must contain a user id if the action master defines the action as a user type action and a clerk id if the action is a clerk type action.
4 The Bypass Authorization Code flag is used to suppress the prompt for an authorization code when an action is not authorized to the user or clerk passed and the action allows the use of authorization codes.
5 Company number is required.
6 Warehouse is optional and not used currently for non POS actions at this time.</td></tr>
</table>

ShutDown: Close all open security files (Security Process End)	
Export: ***YES**	Usage: ShutDown();
Received: • *NONE	
Returned: • *NONE	
1 This function will close all of the files opened by the security service program for the current job.	

ChkActionLmt: Check if a user (or clerk) is authorized to an Action (w/limits)	
Export: ***YES**	Usage: Authorized = ChkActionLmt @ctlval : @reqval :@user : @cono : @whid :@Action : @object {: @instance} {: @extInst} {: @bypass}); If ChkActionLmt (@ctlval : @reqval :@user : @cono : @whid@Action : @object {:@instance} {: @extInst} {: @bypass});
Received: • Control Value (11,5) • Requested Value (11,5) • User Id (10A) • Company No (2,0) • Warehouse No 2 (2A) • Action (10A) • Object (10A) • Instance (10A)* • Inst Extender (10A)* • Bypass Auth Code (Logical)* *Optional {}	
Returned: • Authorized (Logical)	
1 All of the parameters are passed as values therefore constant values such as 'ENTER' and *BLANKS are valid.	

2 The user parameter must contain a user id if the action master defines the action as a user type action and a clerk id if the action is a clerk type action. **3 The Bypass Authorization Code flag is used to suppress the prompt for an authorization code when an action is not authorized to the user or clerk passed and the action allows the use of authorization codes.** **4 Company number is required.** **5 Warehouse is optional and not used currently for non POS actions at this time.** **Note:** This action not only checks that the user (or clerk) is authorized to the action, but it also checks any limiting value defined for the action.	

ActAutCode: Action Authorization Code Processing	
Export: ***YES**	Usage: Authorized = ActAutCode (@cono :@whid : @Action : @object :@instance : @extInst :@LmtTyp : LmtUpper :@LmtLower); If ActAutCode (@cono : @whid @Action : @object : @LmtTyp : LmtUpper :@LmtLower);
Received: • Company No (2,0) • Warehouse No 2 (2A) • Action (10A) • Object (10A) • Instance (10A) • Inst Extender (10A) • Limit Type (1A) • Limit Upper Max (11,5) • Limit Lower Max (11,5)	
Returned: • Authorized (Logical)	
1 If an action allows authorization codes then this function will display a window for an authorization can be entered. **2 The Limit parameters are I/O parameters and will return limit values to the calling program.**	

ClkInGrp: Check to see if a clerk is in a clerk group	
Export: ***YES**	Usage: InGroup = ClkInGrp(@group : @clerk); if ClkInGrp(@ group : @clerk);
Received: • Clerk Group (10A) • Clerk Id (10A)	
Returned: • InGroup (Logical)	
1 If the clerk passed is in the clerk group passed than the clerk is authorized.	

Installation Procedure Notes

Security File Conversions

There are major security file conversions that are run when this enhancement is installed. Although the new security enhancements contain many features not available in the previous version, the conversion is intended to duplicate the previous security profile when initially installed. Once the enhancement is installed, customer installations will be able to take advantage of the new security features by defining new security authority profiles and changing user security definitions.

Security Conversion Functions

- Converts all users in the Security File (**SECTY**) to the User Master File (**USRMST**) and Authority Master File (**AUTMST**). All users are given a personal authority profile equal to their user ID.
- Creates Company Authority File (**COAUT**) records for the default company.
- Creates Warehouse Authority File (**WHAUT**) records for the default warehouse.
- Creates Company Authority File (**COAUT**) records for all companies in the authorized company array in the Security File (**SECTY**).

- Converts all function authorizations (application functions that a user has access rights) in the Security File (**SECTY**) to the Application Function Authority File (**FNCAUT**).
- Converts USERG records to the Group Master File (**GRPMST**) and Group/User File (**GRPUSR**).

Conversion Assumptions

- If a user in the Security File (**SECTY**) does not have a matching IBM i user profile, then the following will apply:
  - If the user id in the Security File (**SECTY**) is shorter than 8 characters, its security profile will not be converted.
  - If the user id in the Security File (**SECTY**) is 8 characters long, then the conversion will look for a user profile longer than 8 that matches the first 8 characters in the Security File (**SECTY**) and the conversion will use that user profile id to convert the security profile. If there is no match, then the security profile will not be converted.
- If any user has companies listed in the authorized companies array in the Security File (**SECTY**), it is assumed that the system option Company Authorization should be activated.
- The system option Warehouse Authorization will not be activated.
- The system option Salesrep Authorization will not be activated.
- If a user has companies listed in the authorized companies array in the Security File (**SECTY**), it is assumed that the user will be subject to the new company authorization logic. If a user does not have any companies listed in the authorized companies array in the Security File (**SECTY**), it is assumed that the user will bypass company authorizations.
- If it is determined that company authority should be activated, any users that are assumed to bypass authorization will be flagged to bypass in their user authority profile. This is to assure that the security will function identical to prior to the upgrade.
- If it is determined that company authority should be activated, all application functions that are not defined as an Accounts Payable or General Ledger function will be flagged to bypass company authorization checking. This is to assure that the security will function identical to prior to the upgrade.

Application Action Security Conversion

Due to Application Action Security, a conversion occurs from the Option records to the Action Security Database and various security options are removed and replaced with new application actions on the Distribution A+ Security Menu (MENU XASCTY). The table below lists all the previous security options that were removed and the security options (or application actions) that replaced them. A description of each column in the table follows.

Column 1 - Menu/Option/Menu Name: This column lists the menu/option/menu name the removed security options were located in prior to Version 6 Cumulative 8.

Column 2 - Security Options Removed: This column lists the security options that were removed from the menu/option shown in column 1.

Column 3- New Application Actions: This column lists the new application actions that replaced the previous security options. Application actions are located in Application Action Authority Maintenance (MENU XASCTY), Authorization Codes Maintenance (MENU XASCTY or MENU PSFILE), or Clerk/Clerk Groups Maintenance (MENU PSFILE) for Point of Sale application actions.

Column 4 - Conversion Assumptions: This column lists the values from the previous security options (shown in quotes; or quotes following to indicate a previous option) and the values used for the authorization type for the new application actions (shown in parenthesis).

Note:

- Refer to APPENDIX C: Application Action Authorities for a list of all the company level, system level, and authorization code action authorities.
- For new installs, refer to APPENDIX C: Application Action Authorities to review the default value for each new application action.

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
MENU XAFILE - Option 2 (Company Name)	Display Cost & Profit	Display GL Cost and Profit (OE, SA, AR, some PO)	If 'Y': All Users (A); If not 'Y': Master Users (M)
MENU XAFILE - Option 12 (Purchasing Options; for company)	1) Authorized Users 2) PO-AP Voucher Hold	Allow the Release of Vouchers on Variance Hold	'*NONE': Master Users (M); '*ALL': All Users (A); If Group 'group name': Selected (S)
MENU XAFILE - Option 13 (Special Order Options)	Buyer/Purchasing Approval Authority User Group (OE)	Authorized to S/O Change Requests - OE	If blank ' ' or no ORCTL record found: No Users (N); If Group 'group name': Selected (S)
	Customer Service Approval Authority User Group (PO)	Authorized to S/O Change Requests - PO	If blank ' ' or no ORCTL record found: No Users (N); If Group 'group name': Selected (S)
MENU XAFILE - Option 4 (Accounts Receivable)	1) Allow Access to AR Quick Pay 2) Authorized Users	Allow Access to AR Quick Pay	If option is not 'Y' or Electronic Payments has not been activated - EPLIVE is 'N': No Users (N); if 'Y' and '*ALL': All Users (A); if Group 'group name': Selected (S)

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
MENU EPFILE - Option 1 (Credit Card Options)	1) Allow Access to Credit Card Inquiry 2) Authorized Users	Allow Access to Credit Card Inquiry	If option is not 'Y' or Electronic Payments has not been activated - EPLIVE is 'N': No Users (N); if 'Y' and '*ALL': All Users (A); if Group 'group name': Selected (S)
MENU XAFILE - Option 5 (Order Entry Options)	1) Allow Price Changes during OE 2) Authorized Users	Allow Changes to Item Price - Item Entry	If 'N': Master Users (M); If 'Y'/ '*ALL': All (A); If 'Y/group name': Selected (S)
	1) Allow Cost Changes during OE 2) Authorized Users	Allow Changes to Item Cost - Item Entry	If 'N': Master Users (M); If 'Y'/ '*ALL': All (A); If 'Y/group name': Selected (S)
	1) Display GM% and Profit Amt during OE 2) Authorized Users	Display GM% and Profit in Order Entry	If option is not 'Y': No Users (N); if 'Y' and '*ALL': All Users (A); if 'Y/group name': Selected (S)
	1) Allow Automatic GM Repricing 2) Authorized Users	Allow Gross Margin Repricing	If option is not 'Y': No Users (N); if 'Y' and '*ALL': All Users (A); if 'Y/group name': Selected (S)
	Override Contract Prices (If GM Reprice is N, this will be set to N, regardless of existing values. Authorized users will be established from GM Repricing during the conversion.)	Allow GM Repricing on Contract Priced Items	If option is not 'Y': No Users (N); if 'Y' and '*ALL': All Users (A); if 'Y/group name': Selected (S)

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
	Override Qty/Family Prices (If GM Reprice is N, this will be set to N, regardless of existing values. Authorized users will be established from GM Repricing during the conversion.)	Allow GM Repricing on Qty/Family Priced Items	If option is not 'Y': No Users (N); if 'Y' and '*ALL': All Users (A); if 'Y/group name': Selected (S)
	Override Manual Override Prices, including vendor rebate prices (If GM Reprice is N, this will be set to N, regardless of existing values. Authorized users will be established from GM Repricing during the conversion.)	Allow GM Repricing - Override/Rebate Priced Items	If option is not 'Y': No Users (N); if 'Y' and '*ALL': All Users (A); if 'Y/group name': Selected (S)
	1) Original Order Info Required on Returns 2) Override User Group	Allow Returns without Original Order Reference	If 'N': All Users (A); If 'Y/ *NONE': No Users (N); If 'Y/group name': Selected (S)
	10 Users Authorized to Run ABR	Allow Automatic Backorder Release	Selected (S); **Note:** First user specified can be a User Group.
MENU XAFILE - Option 5 (Order Entry Options) and MENU OEMAST - Option 1 (Authorized Users)	1) Restrict Activity on Ship Confirmed Orders 2) Authorized Users	1) Allow Quantity Changes - Ship Confirmed Order 2) Allow Ship Date Changes - Ship Confirmed Order 3) Allow Item Deletes - Ship Confirmed Order 4) Allow Deletions of Ship Confirmed Orders	If 'N': All Users (A); If 'Y/ *NONE': No Users (N); If 'Y/group name': Selected (S)

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
	Prevent Deletion of Special-Order Items	Allow Deletion of Special-Order Items	If 'Y': No Users (N); if not 'Y': All Users (A)
MENU XAFILE - Option 5 (Order Entry Options) and MENU OEMAST - Option 1 (Authorized Users) Continued....	1) User ID for Security 2) Authorization Required for Returns 3) Authorized Users	Allow Entry of Return Orders	If User ID for Sec is 'N' or Auth Req for Returns is 'N': All Users (A); otherwise, Selected (S) First user specified can be a User Group
	1) User ID for Security 2)Authorization Required for Reprint/ Clear Pick List 3) Authorized Users	Allow the Reprint of Pick Lists	If User ID for Sec is 'N' or Auth Req for P/L Reprints is 'N': All Users (A); otherwise, Selected (S) First user specified can be a User Group
	1) User ID for Security 2) Authorization Required for Future Order Release 3) Authorized Users	Allow the Release of Future Orders	If User ID for Sec is 'N' or Auth Req for Future Ord Rel is 'N': All Users (A); otherwise, Selected (S) First user specified can be a User Group
	1) User ID for Security 2) Authorization Required for Credit Release 3) Authorized Users	Allow the Release of Held Orders	If User ID for Sec is 'N' or Auth Req for CR is 'N': All Users (A); otherwise, Selected (S) First user specified can be a User Group
	1) User ID for Security 2) Authorization Required for Other Release 3) Authorized Users		If User ID for Sec is 'N' or Auth Req for Other is 'N': All Users (A); otherwise, Selected (S) First user specified can be a User Group
MENU PSFILE - Option 3 (Clerks)	Allow Orders for Multiple Stores	Allow Entry of POS Orders for Alternate Stores	S - Selected
	Allow Returns	Allow Entry of Returns in POS	S - Selected

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
MENU PSFILE - Option 3 (Clerks) / MENU PSFILE - Option 4 (Authorization Codes)	1) Allow Cancel of Orders 2) Authorize Cancel of Orders	Allow Deletion of Point of Sale Orders	S - Selected
	1) Allow Cancel of Lines 2) Authorize Cancel of Lines	Allow Item Deletes - Point of Sale Orders	S - Selected
	1) Allow View Cost 2) Authorize View Cost	Display Cost in Point of Sale Entry	S - Selected
	1) Allow Maintain Cost 2) Authorize Maintain Cost	Allow Changes to Item Cost - POS Item Entry	S - Selected
	1) Allow Access to Price Header Information 2) Authorize Access to Price Header Information	1) Display Header Price Info in POS 2) Allow Changes to Item Price List - POS Entry	S - Selected
	1) Allow No Sale 2) Authorize No Sale	Allow Entry of No Sale Transactions in POS	S - Selected
	1) Allow Override Price 2) Authorize Override Price	Allow Changes to Item Price - POS Entry	S - Selected
MENU PSFILE - Option 4 (Authorization Codes)	Authorize Slow Pay Orders	Allow Entry of Slow Pay Orders in POS	S - Selected
	Authorize Credit Limit Orders	Allow Entry of POS Order Exceeding Credit Limit	S - Selected
	Authorize Store Credit Overrides	Allow Store Credit Overrides in POS	S - Selected

Menu/Option/Menu Name	Security Options Removed	New Application Actions	Conversion Assumptions
	Authorize Entry of Returns in POS without Original Order Info	Allow Returns without Original Order Reference POS	S - Selected
	Authorize CC Authorization Mode Overrides	Allow Changes to CC Authorization Mode in POS	S - Selected

Security Infrastructure

In the original security infrastructure, every menu level CL program called a common security CL program to perform the security checking for application function (or menu option) security authorizations. These programs were XASCTYP, APSCTYP and GLSCTYP. These programs received one parameter (the function number) and returned one parameter (pass/fail flag). This has not changed with the new infrastructure; therefore, if a function was secured in the original infrastructure, it will be secured in the new infrastructure. What has changed is the program that these CL programs call. The new programs XASCT2, APSCT2 and GLSCT2 replace their obsolete counterparts XASCTY, APSCTY and GLSCTY. This service program performs all of the actual security checking logic throughout the entire application. In fact, besides the new security definition maintenance programs that maintain the new security database, the security service program is the only program that will ever access the security definition data.

Company and Warehouse

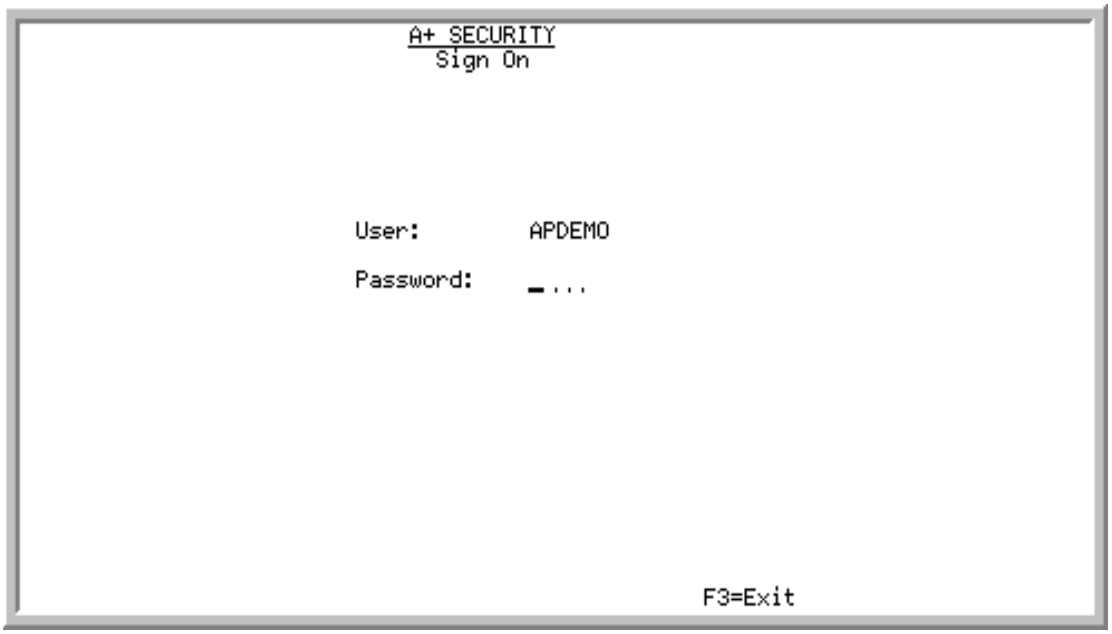
One of the categories of the company and warehouse authorizations is the bypassing of data to display on a report or file listing. Many of these options perform their data extract by use of APFMTDTA. To perform this function, the logic of APFMTDTAP has been modified to perform an additional step when building the format data member that is used by the FMTDTA system utility. This new step identifies instructions that have been placed into the FMT source member. It then replaces these instructions with data omit statements that are built using the companies and warehouses that the user running the report is not authorized to and omitting this data from the Extract File. All sorts run through this new logic even if they were not changed by this enhancement.

Report and listings that bypass data due to user restrictions will display a common message on the first page of each report in the selection criteria section of the report.

Appendix B Security Screen

If password security is chosen for a user on the Authority Profile Definition Screen through User Maintenance (MENU XASCTY) for a private profile, or Authority Profile Maintenance (MENU XASCTY) for a public profile, this screen will appear throughout Distribution A+ for that user.

A+ Security Screen



This screen requires the user (for whom password security has been activated) to enter a password in order to access a menu option.

A+ Security Screen Fields and Function Keys

Field/Function Key	Description
User	Your user ID or the ID of the user signed onto the IBM i displays in this field. Display
Password	Passwords are defined for users through Authority Profile Maintenance (MENU XASCTY). Use this field to select the password that was defined for the user displayed in the **User** field. You will not be allowed access to a menu option unless you know the user's password. Key the appropriate password. (A 4) Required
F3=Exit	Press **F3=EXIT** to exit this screen and return to the menu.
Enter	Press **ENTER** to confirm your selection. You will be able to access the desired menu option.

Appendix C Application Action Authorities

This appendix provides a list of all of the company level, system level, and authorization code action authorities, the application associated with the action, a description of the action, and the action's default setting.

This appendix also provides a list of all extended instances associated with application actions.

Note: As of Version 6 Cumulative 8, application actions replaced various tailoring options in Distribution A+. To review a list of the old tailoring options and what new application actions replaced them, refer to Application Action Security Conversion in APPENDIX A: User Security Technical Notes. New application actions were also added.

System Level Application Actions

The following table lists and describes the system level application actions for which you can create/maintain authorizations on the Define Application Action Authority Screen in Application Action Authorities Maintenance (MENU XASCTY). For these application actions, you determine who will be allowed to perform the application actions: all users (A), master users only (M), selected users (S) or user groups, or no users (N).

AP	Application Action	Description	Default Setting
AP	ACH File Template Maintenance	This application action determines if users are authorized to access ACH (Automatic Clearing House) File Template Maintenance. This function is available in Bank Account Maintenance (MENU APFIL2), via the **F4=ACH TEMPLATE** function key. The **F4=ACH TEMPLATE** function key allows a user to define the ACH template being added or maintained (the user will also be able to delete an existing ACH Template). For each Bank Account that will be using ACH payments, an ACH File Template must be defined.	N

AP	Application Action	Description	Default Setting
AP	Vendor ACH Information	This application action determines if users are authorized to access ACH information in Vendor Master Maintenance (MENU APFILE), via the **F4=ACH INFORMATION** function key. This application action also determines if users are authorized to maintain the **ACH** flag in Vendor Master Maintenance. This flag indicates the default value of a vendor's payment preference. **ACH** (Automatic Clearing House) Payments or paper checks are the available payment preference options.	N
IA	Fields Used in Item Wild Card Search	This application action determines if users are authorized to search on item fields within the Item Master File, Extended Item Comments File, or Extended Search Description File when performing a wild card search to locate an item. A wild card search will only be performed on the fields a user has authority to access. Refer to the Fields Used in Item Wild Card Search Extended Instance Table for a list of extended instances associated with the Item Search. **Note:** The Default Setting is **A** (for all users) for the **Item Description 1** field and Item Description 2 field. For the Item Description 2 field, the value is based on the system option to search on an item description line (as determined in the **Search 2nd Desc** Line field through System Options Maintenance, MENU XAFILE). For the **Extended Item Search Description** and the **Extended Item Comments**, the Default Setting is **N** (No Users).	A or N
IA	Allow Maintenance of Transport/ HazMat Information	This application action determines if the user is authorized to have access to the Item Master Hazmat Code Maintenance Screen in Item Master Maintenance (MENU IAFILE) to maintain item hazardous material OHSA/DOT information. This application action also determines if the user is authorized to make modifications of the content of the DOT Shipping Papers document generated through Carrier Order Inquiry (MENU OEMAIN).	N
OE	Allow Maintenance of Rebate Comments	This application action determines if users are authorized to maintain comments for a rebate in Rebate Master Maintenance (MENU OERFILE).	A

AP	Application Action	Description	Default Setting
OE	Allow Maintenance of Rebate Companies	This application action determines if users are authorized to maintain companies for a rebate in Rebate Master Maintenance (MENU OERFILE).	A
OE	Allow Maintenance of Rebate Customers	This application action determines if users are authorized to maintain customers for a rebate in Rebate Master Maintenance (MENU OERFILE).	A
OE	Allow Maintenance of Rebate Items	This application action determines if users are authorized to maintain items for a rebate in Rebate Master Maintenance (MENU OERFILE).	A
OE	Allow Maintenance of Rebate Ship-Tos	This application action determines if users are authorized to maintain ship to addresses for a rebate in Rebate Master Maintenance (MENU OERFILE).	A
OE	Allow Maintenance of Rebate Vendors	This application action determines if users are authorized to maintain vendors for a rebate in Rebate Master Maintenance (MENU OERFILE).	A
OE	Allow Ship To Display on Credit Card List	This application action determines the ability to view credit card numbers for the customer and all customer ship to addresses on the Credit Card List Screen.	M
PO	Allow Date Changes on Req/ PO Information Screens	This application action determines if users will be allowed to make changes to the Req/PO **Due Date** and **Vendor Ship Date** that appears on information screens accessed from the Req/PO Inquiry (MENU POMAIN). If authorized, an **F13=CHANGE DATE** function key will appear on appropriate Req/PO screens and provide access to a Req/PO Date Entry pop-up screen. From this pop-up screen, authorized users will be able to change the Req/PO **Due Date** and **Vendor Ship Date** (if available) without changing other data on the Req/PO.	N
PO	Allow Reprint History Purchase Order	This application action determines if users will be allowed to reprint Purchase Orders from history that previously printed. If allowed, the reprint functionality will be provided in the Req/PO Inquiry (MENU POMAIN) and when printing Purchase Orders (MENU POMAIN).	N

AP	Application Action	Description	Default Setting
PO	Allow Access to Federal Tax ID	This application action determines if users will be allowed to view an un-encrypted Federal Tax ID where it has been encrypted in Purchasing and Accounts Payable.	M
WM	Allow Changes to the Lot Aging Date	This application action determines who will be able to change the Lot Aging Date of a lot item in Warehouse Management (MENU WMMAIN), where applicable. For those users that are authorized, the **Lot Aging Date** field will be input-cable for lot items and can be overridden, if needed. For those users that are not authorized, the **Lot Aging Date** field will still appear but will be protected.	N
XA	Allow Deletion of Pending Day- End Jobs	This application action determines if users are authorized to delete a pending day-end job from the Application Plus Day-End Processing Submitted Day- End Jobs/Transaction Processor Inquiry Screen in Day-End Processing (MENU XAMAST).	M
XA	Allow Email Generic Reports	This application action determines the ability to see and use the 'Email Report' option presented on the Report Options screen in various places throughout the A+ application if A+ Mail Server being used. Reports may be emailed in addition to or instead of being exported and/or printed.	A
XA	Allow Export of Generic Reports	This application action determines the ability to see and use the 'Export Report' option presented on the Report Options screen in various places throughout the A+ application if A+ Mail Server being used. Reports may be exported in a CSV/TSV format to a spreadsheet program in addition to or instead of being emailed and/or printed.	A
XA	Maintain Linked Reports	This application action determines if the user will be able to maintain the linked reports provided on the Linked Report List Screen of the Linked Document Inquiry. Users with this authority will be allowed to create (**F5=Add**) / maintain (F10=Maintain) reports and also access Application Action Authority Maintenance (MENU XASCTY) to secure those reports. Refer to the Maintained Linked Reports Extended Instance Table for a list of extended instances associated with maintain linked reports.	A

AP	Application Action	Description	Default Setting
XA	Run Linked Reports	This application action determines if the user will be able to run the linked reports provided on the Linked Report List Screen of the Linked Document Inquiry. Only reports that the user is authorized to run are displayed on the Linked Report List Screen. Refer to the Run Linked Report Extended Instance Table for a list of extended instances associated with run linked reports.	A
XA	Maintain MaxRecall Queries	This application action determines if users are authorized to maintain queries in MaxRecall Query Definition Maintenance (XAMFILE). **`F10=MAINTAIN QUERY`** will display as a function key in this menu option only for users who are authorized to perform the function.	S
XA	Run MaxRecall Query	This application action determines if users are authorized to view predefined queries in MaxRecall Query Definition Maintenance (XAMFILE). Only the predefined queries users are authorized to view will display in this menu option. Predefined queries are provided for the following documents: • Acknowledgement • Invoice • Pack List • Pick List • Purchase Order • Vendor Invoice Refer to the Run MaxRecall Query Extended Instance Table for a list of extended instances associated with the run MaxRecall query.	S

Company Level Application Actions

The following table lists and describes the company level application actions for which you can create/ maintain authorizations on the Define Application Action Authority Screen in Application Action Authorities Maintenance (MENU XASCTY). For these application actions, you determine who will be allowed to perform the application actions: all users (A), master users only (M), selected users (S) or user groups, or no users (N). This table is sequenced by application (AP) and then by Application Action.

Company Level Application Actions

AP	Application Action	Description	Default Setting
AR	Allow Access to AR Quick Pay	This application action determines if the Quick Pay feature will be available during the Customer A/R Inquiry (MENU ARMAIN).	N
AR	Allow Changes to Customer Invoice Age Date	This application action determines who will be able to change the invoice aging date on the Invoice Detail Screen of the Customer A/R Inquiry (MENU ARMAIN).	N
AR	Allow Copy Ship To Information	This application action determines if ship to information can be automatically copied from one customer to another and/or if one customer's ship to information can be pulled into another customer's order during Enter, Change, & Ship Orders (MENU OEMAIN).	N
AR	Allow Deletion of Customer or Ship-to	This application action determines if deleting existing customer or ship-to records will be allowed during Customer/Ship to Master Maintenance (MENU ARFILE).	A
AR	Allow Suspend or Reinstate of Customer	This application action determines if suspending or reinstating a customer record will be allowed during Customer/Ship to Master Maintenance (MENU ARFILE).	A
AR	Allow Suspend or Reinstate of Customer Ship-To	This application action determines if suspending or reinstating a customer ship-to record will be allowed during Customer/Ship to Master Maintenance (MENU ARFILE) or Offline Ship-to Maintenance.	A
AR	Maintain Customer Credit Information	This application action determines if access to customer and ship to credit information fields will be allowed during Customer/Ship to Master Maintenance (MENU ARFILE). **Note:** Maintaining Customer Credit Information applies to both Customer Master Maintenance and Ship-to Master Maintenance.	A
AR	Maintain Customer Sales and Marketing Information	This application action determines if access to sales and marketing information fields will be allowed during Customer/Ship to Master Maintenance (MENU ARFILE) for a customer master record. **Note:** Maintaining Sales and Marketing Information applies to Customer Master Maintenance only. When maintaining a ship-to record, access to sales and marketing fields will always be granted as long as the user has the authority to maintain ship-to's.	A

AP	Application Action	Description	Default Setting
AR	Maintain Customer Ship to Numbers	This application action determines if ship-to numbers will be allowed to be added or maintained for a customer during Customer/Ship to Master Maintenance (MENU ARFILE).	A
AR	Allow Addition of A/R Comments	This application action determines if users are authorized to add new A/R comments accessed from the Customer A/R Inquiry (MENU ARMAIN), Customer Collections Inquiry (MENU ARMAIN), or Enter, Change, & Ship Orders (MENU OEMAIN).	A
AR	Allow Maintenance of A/R Comments	This application action determines if users are authorized to maintain A/R comments accessed from the Customer A/R Inquiry (MENU ARMAIN) or Customer Collections Inquiry (MENU ARMAIN).	A
AR	Allow Delete of A/R Comments	This application action determines if users are authorized to delete A/R comments accessed from the Customer A/R Inquiry (MENU ARMAIN) or Customer Collections Inquiry (MENU ARMAIN).	A
EP	Allow Access to Bank Accounts in Maintenance	This application action determines if the full bank account number will display when maintaining a customer's bank account number.	N
EP	Allow Access to Credit Card Inquiry	This application action determines if the Credit Card Transaction Inquiry will be available from the Order Display Screen accessed from the Open Orders Inquiry (MENU OEMAIN) and Customer A/R Inquiry (MENU ARMAIN), or the Invoice Inquiry Detail 1 Screen accessed from the Customer A/R Inquiry (MENU ARMAIN). **Note:** The Credit Card Transaction Inquiry displays the full credit card number. For security reasons, it is recommended that you give careful consideration to which users have access to this inquiry	N

AP	Application Action	Description	Default Setting
EP	Allow Access to Credit Card Numbers in EP Inquiry	This application action determines if the full creditN card number will display when inquiring on a customer/ship to credit card number. Due to Electronic Payments Security Logging (required via PA-DSS v2.0 Requirement 4.1b), when a user is successfully allowed access to this application action, it will be logged in the Electronic Payments Security Logging File (**EPSLOG**). This file can be purged and exported through the Purge/Export EP Security Log option on the Electronic Payments File Maintenance Menu (MENU EPFILE).	N
EP	Allow Access to Credit Card Numbers in Maintenance	This application action determines if the full creditN card number will display when maintaining a customer/ship to credit card number. Due to Electronic Payments Security Logging (required via PA-DSS v2.0 Requirement 4.1b), when a user is successfully allowed access to this application action, it will be logged in the Electronic Payments Security Logging File (**EPSLOG**). This file can be purged and exported through the Purge/Export EP Security Log option on the Electronic Payments File Maintenance Menu (MENU EPFILE).	N
EP	Allow Access to Maintain EP Status	This application action determines if access to change the status of an EP transaction will be allowed. System Administrators should check with the third-party payment provider and/or their Authorization Networks before the status of an order is updated. If changing the status of an order is allowed, the system will be updating the status of Distribution A+ and will not be communicating with the third-party payment provider. It is suggested that you validate the status with your provider. Due to Electronic Payments Security Logging (required via PA-DSS v2.0 Requirement 4.1b), when a user is successfully allowed access to this application action, it will be logged in the Electronic Payments Security Logging File (**EPSLOG**). This file can be purged and exported through the Purge/Export EP Security Log option on the Electronic Payments File Maintenance Menu (MENU EPFILE).	S

AP	Application Action	Description	Default Setting
EP	Allow Display of All Cards on Secure Card List	This application action determines who will be allowed to view all cards for all ship-tos that fall under a particular customer (even if the order was originally entered for a particular customer/ship-to). If allowed, the **F4=SHOW ALL CARDS/F4=SHOW PRV CARDS** toggle function key will display on the Secure Card List Screen in Secure Card Maintenance (MENU EPFILE).	N
OE	Allow Access to the Contract Calculator	This application action determines who will be allowed to access the contract calculator screen from Contract Maintenance (MENU OEPRCE) or Enter, Change, and Ship Orders (MENU OEMAIN).	N
OE	Allow Automatic Backorder Release	This application action determines who will be allowed to perform functions of the Automatic Backorder Release (ABR) process.	S
OE	Allow Change of Rebate ID	This application action determines the ability to change the rebate ID during Enter, Change & Ship Orders (MENU OEMAIN).	A
OE	Allow Change to Bypass Rebate	This application action determines the ability to bypass a rebate during Enter, Change & Ship Orders (MENU OEMAIN).	A
OE	Allow Change to Rush PO - Item Entry	This application action determines the ability to flag a suggested order as a rush in the Inventory Control Center (ICC) module. If this field is defined as **A** (all users), **S** (selected users), or **M** (master users) in Application Action Authority (MENU XASCTY) and you are an authorized user (**S**) or a master user (**M**), during Order Entry (on the Item Review Screen), a Rush PO (**RP**) field will appear allowing you to mark the next suggested order of the particular item as a rush in ICC.	A
OE	Allow Changes to Blanket Orders	This application action determines if changes will beA allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to an existing blanket order, or if changes will be allowed to an existing master order to flag it as a blanket order. **Note:** In order to change a blanket order, the user must also be authorized to change a master order.	A

AP	Application Action	Description	Default Setting
OE	Allow Changes to Consignment Invoices	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing consignment invoices.	A
OE	Allow Changes to Consignment Stock Transfer Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing consignment stock transfer orders.	A
OE	Allow Changes to Customer Invoices	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “I” invoices.	A
OE	Allow Changes to Customer Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “O” orders.	A
OE	Allow Changes to Customer Quotes	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “Q” customer quotes.	A
OE	Allow Changes to Future Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “F” future orders.	A
OE	Allow Changes to GL Cost - Item Entry	This application action determines if overrides to the item’s GL cost will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Entry/ Item Review screens. You must also be authorized to see GL cost.	M
OE	Allow Changes to OE Cost - Item Entry	This application action determines if overrides to the item’s OE cost will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Entry/ Item Review screens. You must also be authorized to see OE cost.	M
OE	Allow Changes to Item Price - Item Entry	This application action determines if item price overrides will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Review Screen.	M
OE	Allow Changes to Master Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “M” master orders.	A
OE	Allow Changes to Qty Ordered - Credit, Rebill, Dupe	This application action determines if the quantity ordered will be allowed to be changed during the credit, rebill, and duplicate order processes performed through Customer Order/Shipment Inquiry (MENU OEMAIN).	A

AP	Application Action	Description	Default Setting
OE	Allow Changes to Return Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing type “R” return orders.	A
OE	Allow Changes to Terms – Order Entry	This application action determines the ability to change the AR Terms Code assigned to an order in the Terms field during Enter, Change & Ship Orders (MENU OEMAIN).	A
OE	Allow Changes to Warehouse Transfer Orders	This application action determines if changes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) to existing warehouse transfer orders (warehouse transfer company).	A
OE	Allow Contract Creation from Contract Calculator	This application action determines which users will see the **F9=CREATE CONTRACT** on the Contract Calculator Screen.	N
OE	Allow Copy Master Order to Multiple Ship-To Addresses	This application action provides authority to users that will be allowed to copy master orders and create duplicate sales orders for a customer’s multiple ship-to addresses.	n
OE	Allow Deletion of Blanket Orders	This application action determines if deleting existing blanket orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Consignment Invoices	This application action determines if deleting existing consignment invoices will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Consignment Transfer Orders	This application action determines if deleting existing consignment transfer orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Customer Invoices	This application action determines if deleting existing type “I” invoices will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Customer Orders	This application action determines if deleting existing type “O” orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Customer Quotes	This application action determines if deleting existing type “Q” quotes will be allowed during Delete Open Orders (MENU OEMAIN).	A

AP	Application Action	Description	Default Setting
OE	Allow Deletion of Future Orders	This application action determines if deleting existing type “F” future orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Master Orders	This application action determines if deleting existing type “M” master orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Return Orders	This application action determines if deleting existing type “R” return orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Ship Confirmed Orders	This application action determines if orders that are ship confirmed can be deleted during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Pick List Printed Orders	This application action determines if orders that are Pick List printed can be deleted during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Special-Order Items	This application action determines if special order items can be deleted from an order in Enter, Change, & Ship Orders (MENU OEMAIN), and/or if an order containing special order items can be deleted through Delete Open Orders (MENU OEMAIN).	A
OE	Allow Deletion of Warehouse Transfer Orders	This application action determines if deleting existing warehouse transfer orders will be allowed during Delete Open Orders (MENU OEMAIN).	A
OE	Allow Display of Rebate Information	This application action determines the ability to access the Rebate Display Screen from various inquiries.	A
OE	Allow Entry of Blanket Orders	This application action determines if the entry of new blanket orders will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Consignment Invoices	This application action determines if the entry of new consignment invoices will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Consignment Transfer Orders	This application action determines if the entry of new consignment transfer orders will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A

AP	Application Action	Description	Default Setting
OE	Allow Entry of Customer Invoices	This application action determines if the entry of new invoices will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Customer Orders	This application action determines if the entry of new orders will be allowed during Enter, Change, & Ship orders (MENU OEMAIN).	A
OE	Allow Entry of Customer Quotes	This application action determines if the entry of new quotes will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Future Orders	This application action determines if the entry of new future orders will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Master Orders	This application action determines if the entry of new master orders will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Entry of Return Orders	This application action determines if the entry of new returns (credit memos) will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	M
OE	Allow Gross Margin Repricing	This application action determines if gross margin repricing will be allowed from the End Order Screen in Enter, Change, & Ship Orders (MENU OEMAIN).	N
OE	Allow GM Repricing on Contract Priced Items	This application action determines that if gross margin repricing is allowed, even contract priced line items will be repriced if the “target” gross margin value entered during Enter, Change, & Ship Orders (MENU OEMAIN) is not met.	N
OE	Allow GM Repricing on Qty/Family Priced Items	This application action determines that if gross margin repricing is allowed, even line items which used quantity discounts to derive their prices will be repriced if the “target” gross margin value entering during Enter, Change, & Ship Orders (MENU OEMAIN) is not met.	N
OE	Allow GM Repricing - Override/Rebate Priced Items	This application action determines that if gross margin repricing is allowed, even line items whose prices were manually entered during Enter, Change, & Ship Orders (MENU OEMAIN) will be repriced if the “target” gross margin value entered during Enter, Change, & Ship Orders (MENU OEMAIN) is not met.	N

AP	Application Action	Description	Default Setting
OE	Allow Item Deletes - Ship Confirmed Orders	This application action determines if items can be deleted from ship confirmed orders during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Review Screen.	A
OE	Allow Item Additions - Pick List Printed Orders	This application action determines if items can be added to an order from Line-Item Entry, Order History, or History List during Enter, Change, & Ship Orders (MENU OEMAIN) on the Customer Order History Screen, if the order has been Pick List printed.	A
OE	Allow Item Deletes - Pick List Printed Orders	This application action determines if items on an order that is Pick List printed can be deleted during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Review Screen.	A
OE	Allow Mass Reprint of Invoices	This application action determines if users are authorized to the mass reprint of History invoices, available through Print Invoices (MENU OEMAIN).	A
OE	Allow Override of Unauthorized Items	This application action determines if item overrides for unauthorized items (those not on a customer's Authorized Item Code) will be allowed during Enter, Change & Ship Orders (MENU OEMAIN). Authorized Item Codes are defined through Authorized Item Codes Maintenance (MENU OEFIL3) and assigned to a customer/customer ship-to through Customer Master Maintenance (MENU ARFILE). Only those items defined on the Authorized Item Code assigned to a customer, if any, can be purchased by the customer unless this field is set to allow users to perform an override of the unauthorized item(s).	N
OE	Allow Quantity Changes - Promotional Get Items	This application action determines if quantity changes can be made during Enter, Change, & Ship Orders (MENU OEMAIN) to items that are promotional 'get' items.	A
OE	Allow Quantity Changes - Ship Confirmed Orders	This application action determines if ship quantity changes for a line item on an order can be made to orders that are ship confirmed during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Review Screen.	A

AP	Application Action	Description	Default Setting
OE	Allow Quantity Changes - Pick List Printed Orders	This application action determines if ship quantity changes for a line item on an order can be made to orders that are Pick List printed during Enter, Change, & Ship Orders (MENU OEMAIN) on the Item Review Screen.	A
OE	Allow Returns without Original Order Reference	This application action determines if original order number information will be required on the Item Review Screen during Enter, Change, & Ship Orders (MENU OEMAIN) when a line item with a negative amount is entered on the Item Entry Screen. Providing the original order number information allows the system to check the quantities being returned against what was shipped to the customer for that line/order. This applies to order types: Order, Invoice, Return and Future. This action also determines if an automatic credit memo may be performed by the user against some or all lines on a history order if that history order has already had at least one return placed against it. Based on this security, over-returns may not be allowed; so, if a user attempts to create an automatic credit memo for an order in history that has already had returns placed against it, and the user does not have the authority to create the return without the original order reference, the credit memo will either not be processed or will be processed without all the line items.	A
OE	Allow Ship Confirmation of an Order	This application action determines if ship confirmation of an order will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN).	A
OE	Allow Ship Date Changes - Ship Confirmed Orders	This application action determines if ship date changes can be made during Enter, Change, & Ship Orders (MENU OEMAIN) to orders that are ship confirmed.	A
OE	Allow the Release of Customer Quotes	This application action determines if the release of quotes will be allowed during Release Held Orders, Quotes, Backorders & Futures (MENU OEMAIN).	A
OE	Allow the Release of Future Orders	This application action determines if the release of future orders will be allowed during Release Held Orders, Quotes, Backorders & Futures (MENU OEMAIN).	M

AP	Application Action	Description	Default Setting
OE	Allow the Release of Held Orders	This application action determines if the release of other types of held orders (that is, orders held with user defined hold codes), and orders on credit hold (slow pay hold and credit limit hold) will be allowed during Enter, Change, & Ship Orders (MENU OEMAIN) or Release Held Orders, Quotes, Backorders & Futures (MENU OEMAIN). The authorization for this application action is defined on the Define Extended Instance Screen at the individual hold code level. Refer to the Allow the Release of Held Orders Extended Instance Table for a list of extended instances associated with the releasing of held orders.	M
OE	Allow the Reprint of Pick Lists	This application action determines if the reprinting or clearing of pick list runs will be restricted.	M
OE	Authorized to S/O Change Requests - OE	This application action determines if users are authorized to the Order Entry features and functions of the change request process.	N
OE	Display GM% and Profit in Order Entry	This application action determines if the gross margin percent and the actual profit amount will display on the Item Review Screen and End Order Screen in Enter, Change, & Ship Orders (MENU OEMAIN).	N
PO	Allow the Release of Vouchers on Variance Hold	This application action determines who will be allowed to release vouchers with the **PO-AP Voucher Hold Code** designated through Purchasing Options Maintenance (MENU XAFILE).	A
PO	Authorized to S/O Change Requests - PO	This application action determines if users are authorized to the Purchasing features and functions of the change request process.	N
WO	Allow Insufficient Qty Override in Work Order Rcpt	This application action determines if users are authorized to override the Insufficient Components Quantities Exist message on the Work Order Receipt End Screen in Receipt Entry (MENU WOMAIN).	M
XA	Allow Access to Cost Load Window	Tis application action determines who will be allowed to access the Cost Load Screen located in Item Inquiry (MENU IAMAIN) and Item Balance Maintenance (MENU IAFILE).	N

AP	Application Action	Description	Default Setting
XA	Allow Changes to allowed threads of a TP Job	This application action determines if changes to the threads allowed for a TP job will be allowed in the Transaction Processor Inquiry (MENU XAMAST). **Note:** This action authority only needs to be set for the system default company; all companies will use the setting for the default company.	M
XA	Allow Changes to the priority of a TP Job	This application action determines if change to the TPM run priority will be allowed for a job in the Transaction Processor Inquiry (MENU XAMAST). **Note:** This action authority only needs to be set for the system default company; all companies will use the setting for the default company.	M
XA	Display GL Cost and Profit (OE, SA, AR, some PO)	This application action determines if the GL cost and profit will display during Order Entry, Sales Analysis, Accounts Receivable, and Inventory Accounting inquiries.	M
XA	Display OE Cost and Profit (OE, SA, AR, some PO)	This application action determines if the OE cost and profit will display during Order Entry, Sales Analysis, Accounts Receivable, and Inventory Accounting inquiries.	M
XA	Display Average Cost	This application action determines if the average cost will display during selected Inventory Accounting and Order Entry processes.	M
XA	Display Standard Cost	This application action determines if the standard cost will display during selected Inventory Accounting and Order Entry processes.	M
XA	Display User Cost	This application action determines if the user cost will display during selected Inventory Accounting and Order Entry processes.	M
XA	Display Last Cost	This application action determines if the last cost will display during selected Inventory Accounting and Order Entry processes.	M
XA	Display Vendor/Item Cost	This application action determines if the vendor/item cost will display during selected Inventory Accounting and AIM/IM&P processes.	M
XA	Display PO Cost	This application action determines if the PO cost will display during selected Purchasing processes.	M

AP	Application Action	Description	Default Setting
XA	Display Commission Cost	This application action determines if the commission cost will display during selected Inventory Accounting and Order Entry processes.	M
XA	Display WM Cost	This application action determines if the WM cost willM display during selected Warehouse Management processes.	M

Authorization Codes Application Actions

The following table lists and describes the application actions for which you can create/maintain authorization codes on the Application Action Authority Screen in Authorization Codes Maintenance (MENU XASCTY). For these application actions, you determine who will be allowed to perform the application actions: all clerks (A), selected clerks (S), or no clerks (N).

Authorization Codes Application Actions

AP	Application Action	Description	Default Setting
PS	Allow Access to OE Order Information	This application action determines if you will be allowed to access order entry order information during Point of Sale Entry (MENU PSMAIN). Depending on your response to this action, the **F13=OE ORDER** function key will or will not be available on the Enter Order/Enter Return Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Changes to CC Authorization Mode in POS	This application action determines if the default credit card authorization mode for credit card orders can be overridden during Point of Sale.	S
PS	Allow Changes to Deposits	This application action determines if the deposit amount for a pickup/delivery order can be changed on the Deposit Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Quantity Changes – POS Promo Get Items	This application action determines if quantity changes can be made during Point of Sale Entry (MENU PSMAIN) to promotional ‘get’ items added to POS orders.	S

AP	Application Action	Description	Default Setting
PS	Allow Changes to Item GL Cost - POS Item Entry	This application action determines if the item's GL cost can be maintained on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Changes to Item OE Cost - POS Item Entry	This application action determines if the item's OE cost can be maintained on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Changes to Item Price - POS Entry	This application action determines if an item's price or discount percentage can be overridden on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Changes to Item Price List - POS Entry	This application action determines if an item's price list can be overridden on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Deletion of POS Orders	This application action determines if Point of Sale orders can be canceled.	S
PS	Allow Entry of Drop Ship Items in POS	This application action determines whether or not the entry of a drop ship item will be allowed during Point of Sale Entry (MENU PSMAIN). **Note:** A drop ship item is automatically made a pickup/delivery item in POS Entry.	S
PS	Allow Entry of Drop/Pull Transaction in POS	This application action determines whether or not the entry of a drop/pull transaction will be allowed during Point of Sale Entry (MENU PSMAIN).	A
PS	Allow Entry of No Sale Transaction in	This application action determines whether or not the entry of a no sale transaction will be allowed during Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Entry of Pickup/Delivery Items in POS	This application action determines whether or not the entry of a pickup/delivery item will be allowed during Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Entry of POS Orders for Alternate Stores	This application action determines if Point of Sale orders can be entered for stores other than the clerk's default store in Clerk Maintenance (MENU PSFILE).	S

AP	Application Action	Description	Default Setting
PS	Allow Entry of POS Orders Exceeding Credit Limit	This application action determines if Point of Sale orders for assigned customers exceeding the credit limit without an authorization code will be allowed. Customer orders are placed on credit hold if the customer's credit limit is less than the total credit used. The values used to calculate the total credit used are based on the value specified in the Include Future Invoices in Credit Limit Check field in Order Entry Options Maintenance (MENU XAFILE).	S
PS	Allow Entry of Returns in POS	This application action determines if returns can be entered in Point of Sale (this is required for the PS: Allow Returns without Original Order Reference POS action).	S
PS	Allow Entry of Slow Pay Orders in POS	This application action determines if POS orders (slow pay) for assigned customers with outstanding invoices will be allowed without an authorization code in Point of Sale.	S
PS	Allow Entry of Special-Order Items in POS	This application action determines whether or not the entry of a special order item will be allowed during Point of Sale Entry (MENU PSMAIN). **Note:** A special order item is automatically made a pickup/delivery item in POS Entry.	S
PS	Allow Entry of Will Call Items in POS	This application action determines whether or not the entry of a will call item will be allowed during Point of Sale Entry (MENU PSMAIN).	S
PS	Allow Item Deletes - POS Orders	This application action determines if line items can be canceled on an order. Lines include items, special charges, and comments.	S
PS	Allow Returns without Original Order Reference	This application action determines if returns without the original order information can be entered in Point of Sale. This also includes orders with negative quantities.	S
PS	Allow Store Credit Overrides in POS	This application action determines if orders that exceed the store credit balance or orders without a valid store credit will be allowed during Point of Sale.	S
PS	Display GL Cost in POS Entry	This application action determines if GL cost information will be displayed on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN). This is required for changes to an item cost.	S

AP	Application Action	Description	Default Setting
PS	Display OE Cost in POS Entry	This application action determines if OE cost information will be displayed on the Enter Order/Enter Return Item Review Screen in Point of Sale Entry (MENU PSMAIN). This is required for changes to an item cost.	S
PS	Display Header Price Info in POS Entry	This application action determines if the POS Header Screen can be accessed in Point of Sale Entry (MENU PSMAIN).	S

Application Action Extended Instances

The following tables list the extended instances associated with application actions.

Allow the Release of Held Orders Extended Instance Table

Ex Instance	Description
Note: all defined hold codes will display in the list so to be available for security authorizations.	
CR	Credit Hold
GM	Minimum Gross Margin Hold
GX	Maximum Gross Margin Hold
NC	New Customer Hold
OM	Order Minimum
SP	Slow Pay Hold
user-defined	Automated Invoice Hold
user-defined	Boxing Hold
user-defined	Consolidated Invoice Hold
user-defined	Declined Credit Card Hold
user-defined	Drop Ship Hold
user-defined	Expired Authorization Hold
user-defined	EDI Order Hold
user-defined	EDI Order Error Hold
user-defined	Pending Authorization Hold

Ex Instance	Description
user-defined	Processing Error Hold
user-defined	RGA (Return Goods Authorization) Hold
user-defined	Replenishment Hold
user-defined	Warehouse Management Hold
user-defined	Web Order Hold Code
user-defined	Web Order Error Hold Code

Fields Used in Item Wild Card Search Extended Instance Table

Ex Instance	File Name	Description
IMITCL	ITMST	Item Class
IMITD1	ITMST	Item Description 1
IMITD2	ITMST	Item Description 2
IMITNO	ITMST	Item Number
IMITSC	ITMST	Item Subclass
IMMC01	ITMST	Miscellaneous Code 1
IMMC02	ITMST	Miscellaneous Code 2
IMMC03	ITMST	Miscellaneous Code 3
IMMFNO	ITMST	Manufacturers Item Number
IMUS5A	ITMST	User Field 1
IMUS5B	ITMST	User Field 2
IMUS5C	ITMST	User Field 3
IMUS5D	ITMST	User Field 4
IMUS5E	ITMST	User Field 5
IMUS5F	ITMST	User Field 6
INCMTX	IAEIC	Extended Item Comments Comment Text
ISEISD	IAESD	Extended Item Search Description

Maintained Linked Reports Extended Instance Table

Ex Instance	Description
MAINT	Linked Query Maintenance
1	IBM Query/400
2	Microsoft Reporting Services
3	Corvu HyperVu
4	Structured Query Language (SQL)

Run Linked Report Extended Instance Table

Ex Instance	Description
00000001	Order History
00000002	Run Order History Report

Run MaxRecall Query Extended Instance Table

Ex Instance	Description
ACKCUSTPO	Acknowledgement by Customer PO
ACKORDER	Acknowledgement by Order
INVCUSTPO	Invoice by Customer PO
INVORDER	Invoice by Order
ORDFLD	Order Folder
PACKCUSTPO	Pack List by Customer PO
PACKORDER	Pack List by Order
PICKCUSTPO	Pick List by Customer PO
PICKORDER	Pick List by Order
POBYPO	Vendor Purchase Order by PO
VNDINV	Vendor Invoice by Invoice