# Using PasswordCourier and PasswordCourier Support Staff Classic

**Release 9.1**

**Core Security SDI Corporation**

**1000 Holcomb Woods Parkway**
**Suite 401**
**Roswell, GA 30076**
**Phone: (678) 304-4500**
**Fax: (770) 573-3743**

## Trademarks

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1: Overview

This manual describes how to use Core Security's PasswordCourier® and PasswordCourier Support Stafff password provisioning solutions on the classic platform.

This chapter includes the following sections:



## Components and Requirements

Please see *Installing the Access Assurance Suite.*

## Java Runtime Environment

To use the Customization Manager for PasswordCourier Classic and PasswordCourier Support Staff Classic, you need to install a current version of the Java Runtime Environment on the administrators' client machines that run these applications. You can download it from the following location:

www.java.com

# About PasswordCourier

PasswordCourier empowers end users to reset their own passwords to networks, systems, and applications within a corporate network without contacting the Help Desk.

PasswordCourier automates the following Help Desk and support tasks:

- End user validation and authentication
- Creation of a Trouble ticket
- Generation of an e-mail message sent to serve as an audit trail of password reset requests
- End user password reset if a Password Management Module (PMM) is available for the password target
- Security incident reports in the Help Desk system and/or an e-mail message

PasswordCourier Support Staff allows support staff to authenticate end users, securely reset passwords on behalf of end users without requiring supervisory or administrative privileges on the target system, as well as creating a ticket in the Help Desk.

PasswordCourier Support Staff is similar in operation to PasswordCourier with the following exceptions:

- It can be configured to require identifying information about the support staff member using the product, and optionally validate this information against a database entry.
- It can be configured to require end user information and optionally validate this information against a database entry.
- Support staff can reset specific end user accounts after selecting a Password Target Group and Password Target.

Rather than providing a proprietary Help Desk/problem management system, PasswordCourier and PasswordCourier Support Staff integrate with leading Help Desk management systems.

Through an end user interface you can tailor with the Customization Manager interface, PasswordCourier and PasswordCourier Support Staff prompt the user to take the actions shown in Table 1.

**Table 1: PasswordCourier and PasswordCourier Support Staff Prompts**

| PasswordCourier | PasswordCourier Support Staff |
|---|---|
| | Enter support staff identification. |
| Enter validation information that is checked against the end user's identifying information in a database (the user’s profile). | Enter validation information that is checked against the end user's identifying information in a database (optional). |
| Enter authentication information that will be checked against confidential information in the end user's profile in the a database (optional). | Enter authentication information that is checked against confidential information in the end user's profile in the a database (optional). |

**Table 1: PasswordCourier and PasswordCourier Support Staff Prompts**

| PasswordCourier | PasswordCourier Support Staff |
|---|---|
| Choose a Password Target Group and a Password Target for password reset. | Choose a Password Target Group and a Password Target for password reset. |
| Enter a new password. | Enter a new password. |
| Enter any comments to be used in the configured password reset request tracking mechanisms such as Help Desk ticketing or e-mail (optional). | Enter any comments to be used in the configured password reset request tracking mechanisms such as Help Desk ticketing or e-mail (optional). |

PasswordCourier and PasswordCourier Support Staff offer an easy-to-use graphical interface for the end user with the ability to access help information at any time by clicking the open book icon next to any field in the Java or Web Access methods to display customized help or by pressing F1 function key to display Internet Explorer help.

End users can also access PasswordCourier via the Windows desktop on their PCs or via the telephone.

## Using the Customization Manager

You can customize PasswordCourier to meet company-specific requirements for security and support policies and procedures. The PasswordCourier and PasswordCourier Support Staff Customization Managers allow customization of:

- PasswordCourier end user interface
- Validation and authentication questions for both end users and support staff
- Courion Server password resets via PMMs
- Password constraints on new passwords
- Ticket information
- Trouble ticket information updated by PasswordCourier when an end user password reset succeeds and/or fails
- Security incident ticket information created by PasswordCourier when an end user is not successfully authenticated
- Notification
- E-mail trouble message sent by PasswordCourier when an end user requests a password reset
- E-mail security message sent by PasswordCourier when an end user is not successfully authenticated

Separate Customization Managers are available for PasswordCourier and PasswordCourier Support Staff. You can use one or both products within a company.

Unless specifically mentioned, the PasswordCourier Support Staff Customization Manager functions the same as the PasswordCourier Customization Manager.

## Using Transparent Synchronization on the Classic Platform

The PasswordCourier Transparent Synchronization feature allows PasswordCourier to capture password changes from native operating system tools, such as the Microsoft® Windows® 2000 Professional password change dialog box, and propagate them to the Courion Server for synchronization with a range of targets.

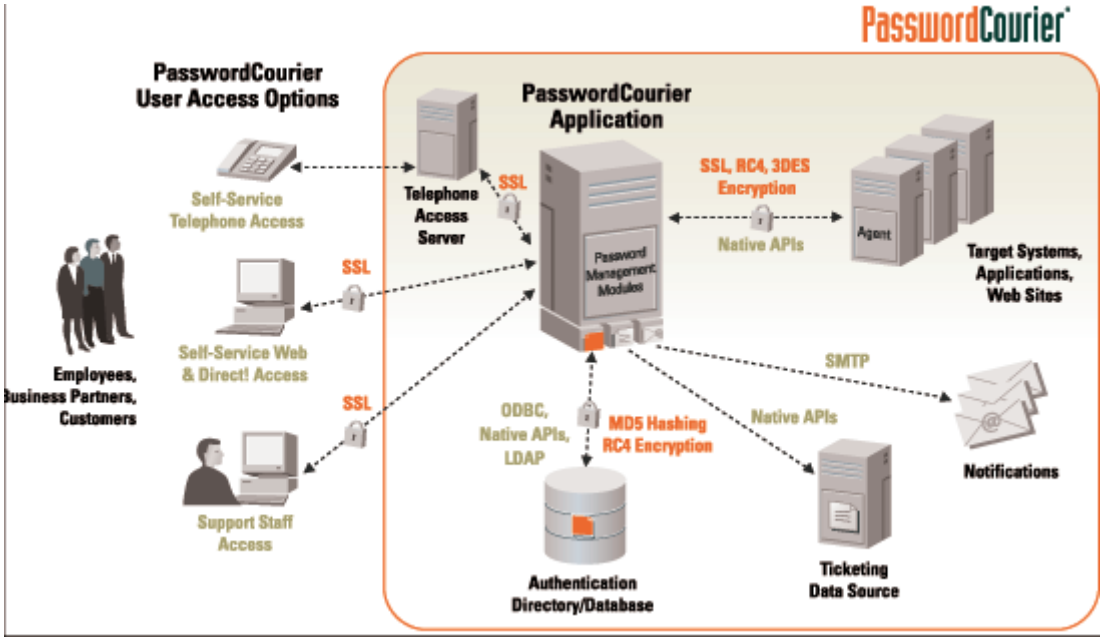
If you have an access key for Transparent Synchronization, PasswordCourier Support Staff is not available. This is because you use the Customization Manager for PasswordCourier Support Staff to configure Transparent Synchronization, and it is therefore not available for support staff functionality.

See *"Configuring PasswordCourier for Transparent Synchronization" on page 105* for details about this feature.

# PasswordCourier Functionality

PasswordCourier uses SSL and other protocols in communication with users and the web, as shown in *Figure 1*.

**Figure 1: PasswordCourier Architecture Overview**




The system administrator uses the PasswordCourier Customization Manager to configure the end user interface. This configuration process includes the following steps:

1. Set up validation (to identify the end user)
2. Set up authentication (to confirm the end user's identity)
3. Specify one or more target systems
4. Define password rules

## Validation

Based on its configuration, PasswordCourier requires the end user to enter between one and four pieces of information that is then checked against the end user's profile. Data type constraints are enforced by the data type in the corresponding field in a database. For example, if the field is a numeric field the end user is not allowed to enter alphabetical characters.

Based on its configuration, PasswordCourier Support Staff requires between zero and two pieces of information in order to validate the support staff representative. PasswordCourier Support Staff checks the entered information against the support staff user's profile.

PasswordCourier Support Staff may then require the support staff user to enter between zero and four pieces of end user information. PasswordCourier validates this information against the end user's profile.

## Authentication

PasswordCourier and PasswordCourier Support Staff can be configured to challenge an end user to enter a piece of confidential authentication information. If the end user enters incorrect information during validation or authentication, PasswordCourier or PasswordCourier Support Staff can create a security incident ticket and/or send an e-mail. If incorrect information is entered, the end user may not continue.

The end user must enter and verify the information that will be checked against his or her profile. PasswordCourier compares the two values on the end user's system before checking against a database. This verification process reduces the number of security incident tickets resulting from end users incorrectly entering their authentication information.

## Target Systems

After the end user is authenticated, PasswordCourier or PasswordCourier Support Staff presents the end user with a list of configured Password Target Groups and the Password Targets within those groups, as determined by the configured PMMs. When a Password Target Group is selected, the list of Password Targets presented changes to reflect the Password Targets within that group. This allows you to place targets in logical groups.

For example, you can create a Password Target Group on the bases of user groups, so that “Sales” includes all targets used by the Sales department. Alternatively, you can group targets by system, so that “UNIX” contained targets such as an HP-UX® system, a Sun Solaris system, and an IBM® AIX® system.

## Passwords

After the end user chooses the password(s) to reset, PasswordCourier prompts the end user to enter a new password. Or PasswordCourier can enter a password previously escrowed in a datasource.

### *Password Strength*

You configure password strength via the PasswordCourier Customization Manager. PasswordCourier enforces password strength. Configurable variables include:

- Password composition (minimum/maximum length, and type/format of characters,
- Password history (including comparing password to history stored on the target)
- Whether passwords are checked against a dictionary.
- Whether to forbid characters from the username in the password with a length equal to or greater than *n* (`0` prohibits entire username).
- Whether to forbid repeating patterns of characters with a length equal to or greater than *n*.
- Whether to forbid a succession of alphabetic or numeric characters with a length equal to or greater than *n*.

PasswordCourier checks the strength criteria of the password the end user entered before attempting a reset across the network.

## Resource Claiming

Resource Claiming is an Access Assurance Suite feature that populates the IdentityMap (the User-Based Targets table in PasswordCourier Classic) by prompting end users to claim resources such as accounts for which they already have access. By defining queries against a specified list of target systems, you can specify a set of rules that determine which accounts should be presented to each user for claiming. Resources that meet the criteria specified by these rules are presented to end users as a list of "suggestions" or account names that they may possibly own. The users then choose the resources for which they possess access credentials and authenticate themselves against these resources.

Resource Claiming is available through the Access Assurance Suite Administration Manager, and PasswordCourier users who do not have an AccountCourier or ComplianceCourier access key can configure this feature in an Administration Manager workflow with View action. The View action is available to all Access Assurance Suite applications without a separate access key.

By creating a workflow with the View action that includes Resource Claiming, an administrator can claim accounts for a group of users or create a self-service workflow that allows users to claim their own accounts. See the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for information about how to create workflows, the View action, and Resource Claiming.

# Configuring Password Management Modules (PMMs)

Password Management Modules provide access to the target systems where passwords are reset. For information about how to configure Password Management Modules, see the manual *"Configuring Password Management Modules (PMMs), Connectors, and Agents.*

## The PMM for Synchronization

The Password Management Module (PMM) for Synchronization enables PasswordCourier and PasswordCourier Support Staff to reset multiple passwords at once on the classic platform. This manual explains how to configure this PMM in the section *"Synchronization" on page 101*.

# Chapter 2: Configuring PasswordCourier and PasswordCourier Support Staff

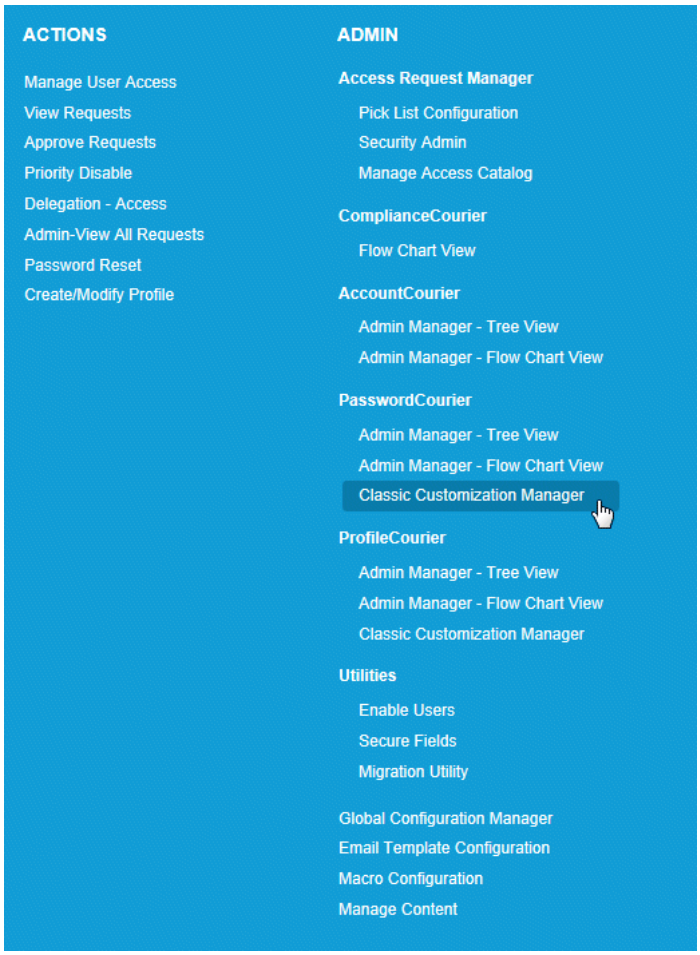
This chapter includes these sections:

# Configuring PasswordCourier and PasswordCourier Support Staff

You configure PasswordCourier Classic and PasswordCourier Support Staff Classic using an interface called the Customization Manager. To access the Customization Manager through the Access Assurance Portal, you can do the following:

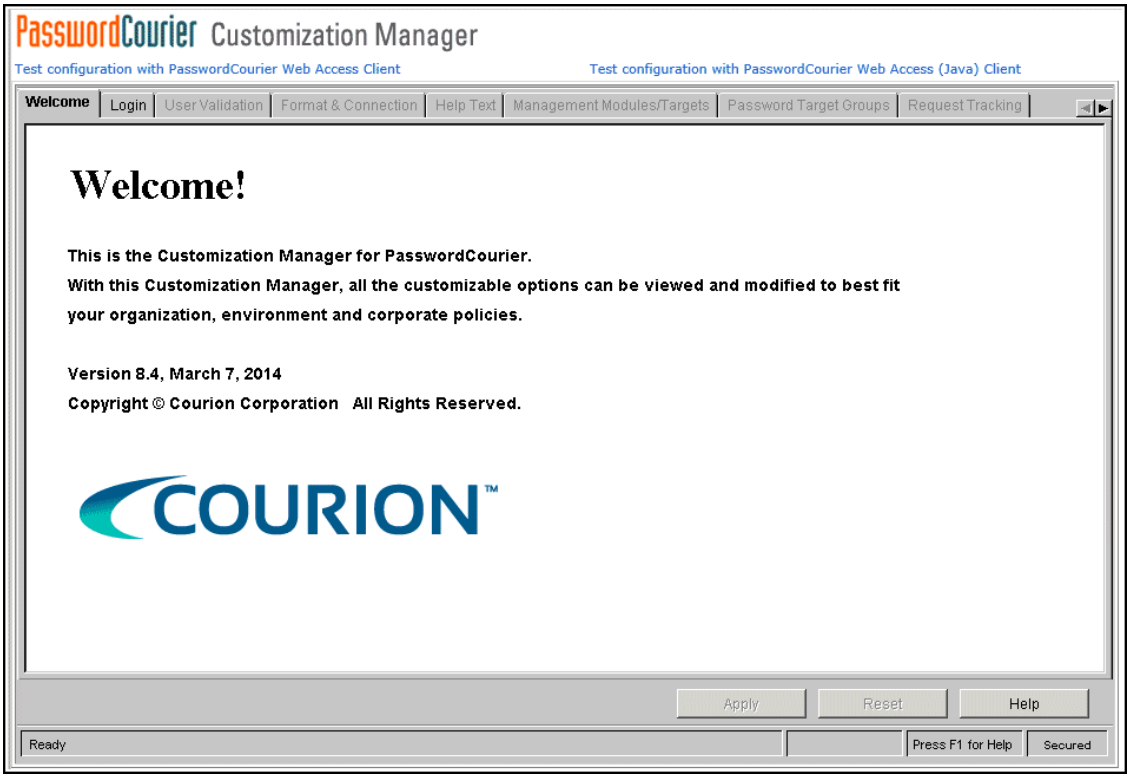
1. When you use Java-based components such as PasswordCourier Customization Manager on the Classic Platform and PasswordCourier Support Staff Customization Manager on the Classic Platform, you must open these components in a new Internet Explorer process.
2. Log in to the Access Assurance Portal Page.
3. Click **CLASSIC CUSTOMIZATION MANAGER** below **PASSWORD COURIER** from the Mega Menu, as shown in *Figure 2*.

**Figure 2: Using the Mega Menu**



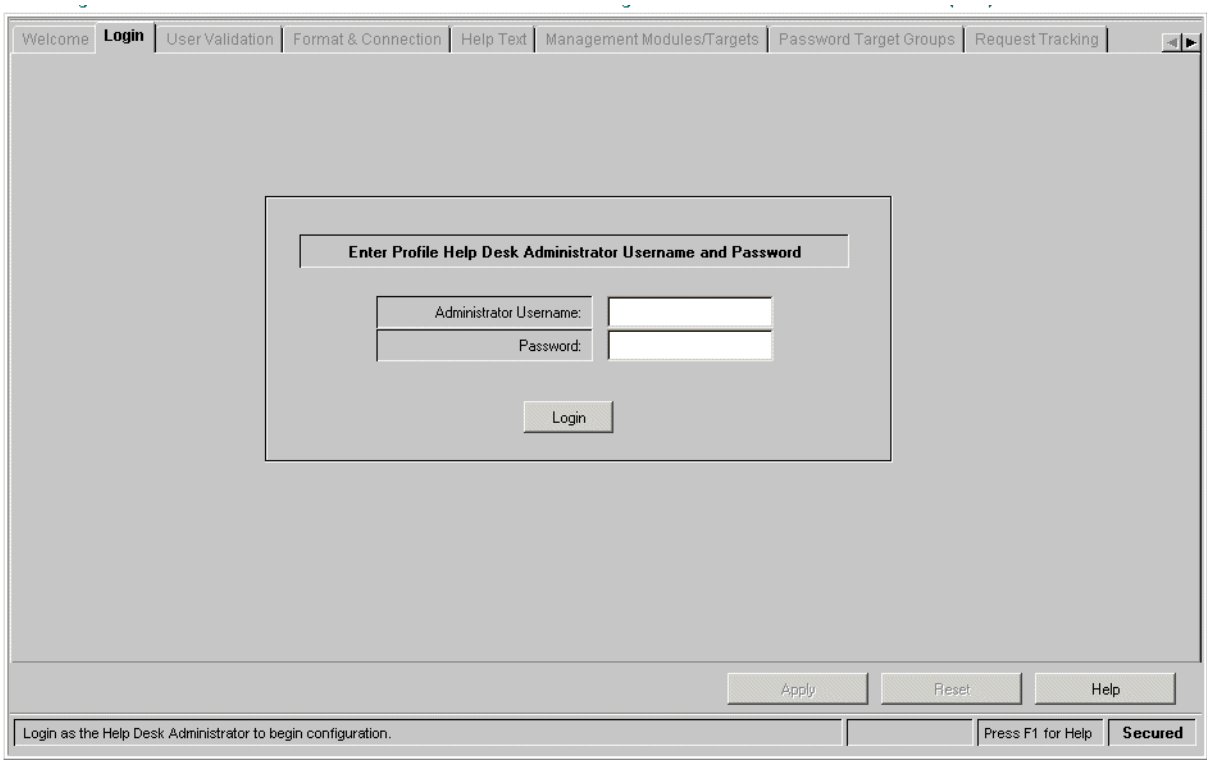

The Customization Manager Welcome page appears as shown in *Figure 3*.The Welcome tab provides version number and other information about PasswordCourier. No configuration is performed on this tab.

**Figure 3: Customization Manager Welcome page**




4. Select the Login tab as shown in *Figure 4*. The PasswordCourier Customization Manager requires the administrator to log on to ensure that only qualified individuals make changes to PasswordCourier's configuration. The administrator is authenticated against the administrator information in the profile data source.

**Figure 4: PasswordCourier Customization Manager Login Tab**

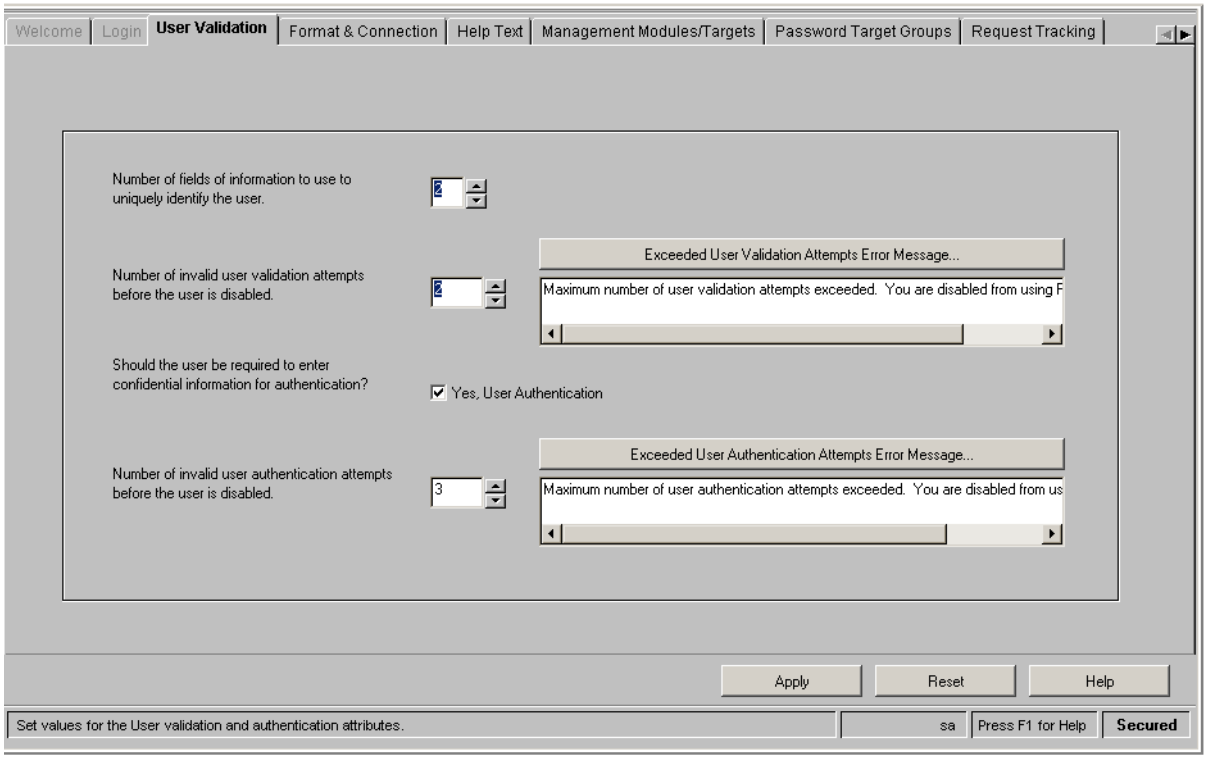



## User Validation Tab

### *End User Validation in PasswordCourier*

The User Validation tab (*Figure 5*) allows you to specify the information used to validate end users when they attempt to change their passwords with PasswordCourier. User validation is divided into two sections: validation (identification) of an end user against public information stored in the his or her profile and authentication of the end user against confidential information also stored in the profile.

**Figure 5: User Validation Tab for PasswordCourier**




## Validation

This step in the configuration allows you to customize the validation prompt(s) presented to each user. In response to these prompts, each user enters information which is compared against their profile in a data source.

1. In the first spin control, specify the number of fields of validation information the end user must enter at the first prompt in the User Validation tab. PasswordCourier can be customized to require the end user to enter between 1 and 4 pieces of personal information for identification purposes.

   Either highlight the number and enter the number of fields or position the mouse pointer on the up or down arrow and click the left mouse button until the appropriate number of fields is shown.

2. In the second spin control, specify the number of times an end user can enter incorrect validation information before PasswordCourier disables that end user from attempting password resets and creates a security incident trouble ticket. (This is one of several security features that enables the Help Desk and support group to track possible security breach attempts.)

3. In the **EXCEEDED USER VALIDATION ATTEMPTS ERROR MESSAGE...** text box, you can provide disabled end users with directions on the procedure for becoming reenabled. The messages may incorporate PasswordCourier macros and, along with the text, it may select information out of the database.

### Authentication Against Confidential Information

This step allows you to configure PasswordCourier to present a custom question to each user. In response to these prompts, each user enters unique information which is compared against unique information previously stored in their profile in a datasource.

You can configure PasswordCourier to require end users to enter one piece of confidential information: their social security number, mother's maiden name, employee number or personal identification number (PIN), for example, that forces them to authenticate themselves before executing a password reset. The end user must verify the information by entering it twice.

1. The checkbox on the User Validation tab allows you to specify whether the end user is challenged with a piece of unique information.
2. The spin control on the User Validation tab allows you to specify the number of times an end user can enter incorrect authentication information before PasswordCourier disables the end user from attempting password resets and creates a security incident ticket.

Use the Enable Users Utility (see *Using the Access Assurance Suite Administration Manager Utilities*) to enable disabled end users so they can access PasswordCourier to reset a password.

As with user validation, PasswordCourier displays a customizable message to end users who have exceeded the configured number of authentication attempts. You can provide these end users with directions on the procedure for becoming reenabled. The message may incorporate PasswordCourier macros and select information out of the database along with the text.

**Note:** You must save the configuration by pressing **APPLY**. The **RESET** button sets all fields back to their previous value.

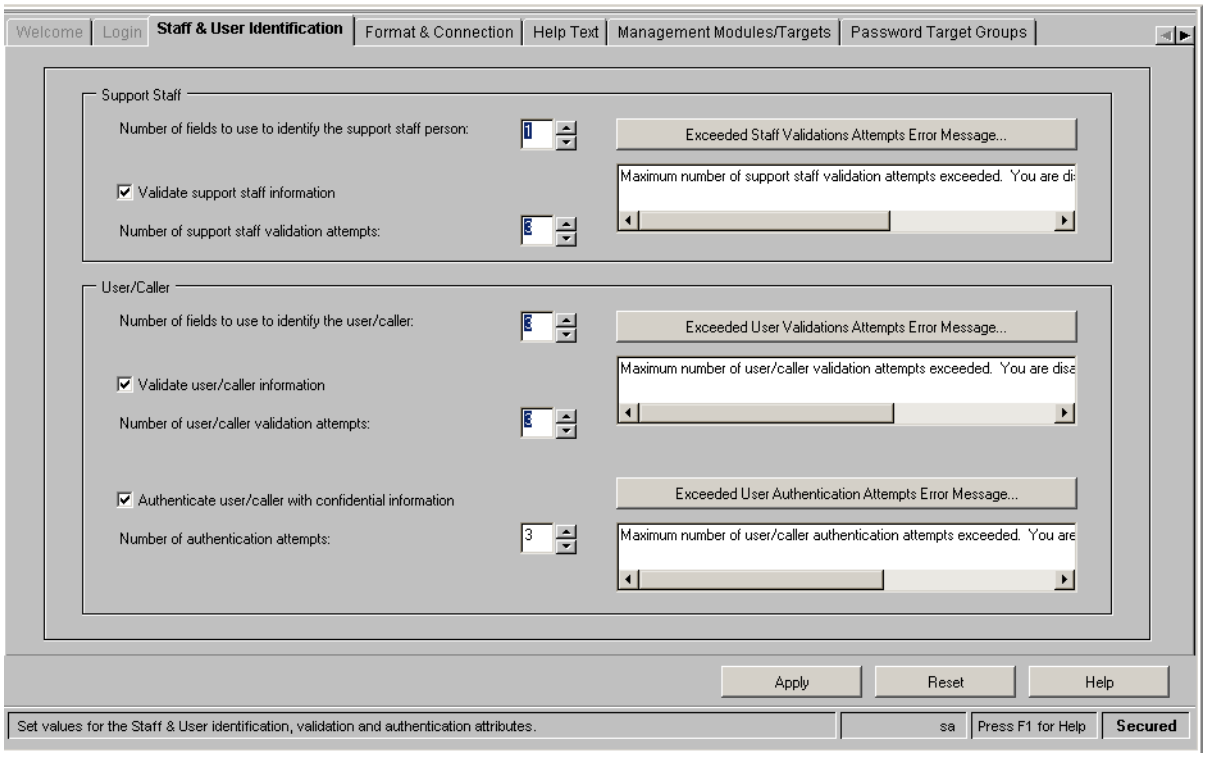
## *Staff and User Identification Tab in PasswordCourier Support Staff*

The Staff and User Identification tab (*Figure 6*) allows you to customize the information used to validate support staff and end users when they attempt to change their passwords with PasswordCourier.

### Support Staff Validation

Support staff validation is optional and can be configured to require from zero to two pieces of information. Additionally, the fields may be configured to either capture information only (to be used later in macros) or to validate against a profile.

**Figure 6: User Validation Tab for PasswordCourier Support Staff**




## End User Validation and Authentication

End user validation in PasswordCourier Support Staff is similar to validation in PasswordCourier. However, in PasswordCourier Support Staff, end user validation is optional. The fields may be configured to simply record information without validating against a profile.

**Caution:** Core Security strongly recommends that either support staff validation or end user validation or both be configured on this tab. If no validation is configured, anyone who downloads PasswordCourier Support Staff can submit a password reset request for any username against any configured Password Target without being challenged for any information.

# Format & Connection Tab

## *Format & Connection Tab in PasswordCourier*

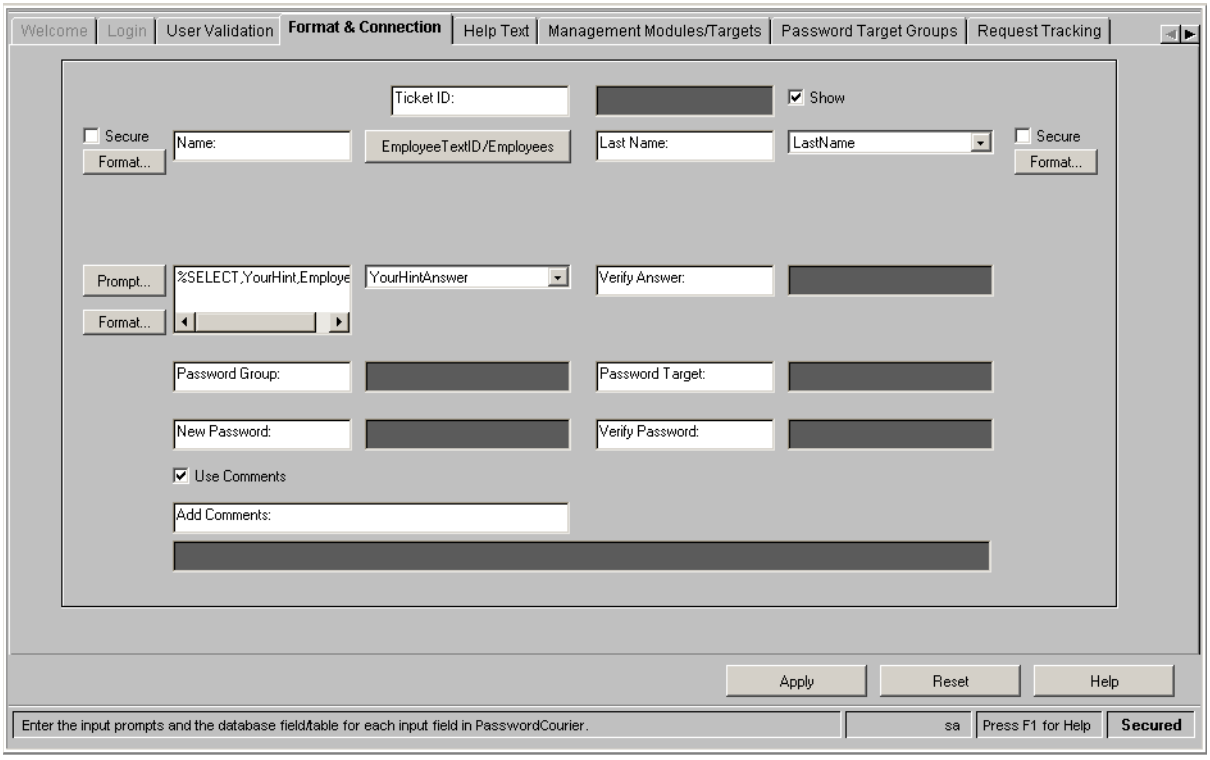
The Format & Connection tab (*Figure 7*) provides three areas of configuration:

- Customization of labels and prompts presented to the end user in PasswordCourier
- Identification of the database fields against which end user information is validated.
- In fields with an associated **FORMAT** button, formatting such as leading characters or suffixes may be applied to data entered by the end user.

The dark gray boxes on this tab mirror this screen to the PasswordCourier screen viewed by end users. The number of fields displayed on this tab is determined by the configuration information entered on the User Validation tab.

**Note:** This applies only to web access (java) for PasswordCourier and PasswordCourier Support Staff.

**Figure 7: Format & Connection Tab for PasswordCourier**




### Ticket Information

The first field, located at the top of the window, contains ticket information that can be referenced by end users when they contact a Help Desk representative. If you select the **SHOW** check box, to the right of the ticket information field and ticketing has been configured in PasswordCourier, the ticket ID (the ticket number or its equivalent) is displayed at the top of the window in the end user interface.

Although it is not necessary to display the ticket ID to the end user in PasswordCourier, Core Security recommends displaying this information so that user actions in PasswordCourier may be tracked. If the checkbox is selected, this field is automatically populated. It is not a part of the Validation and Authentication configuration.

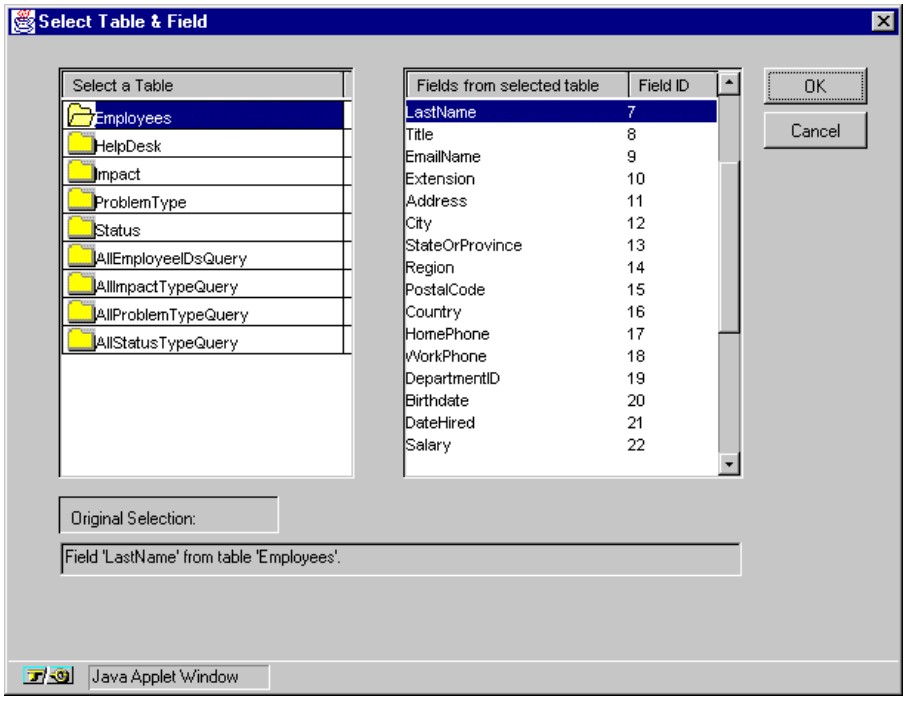
### Configuring End User Validation

To validate and authenticate the end user, you identify a table that contains the profile of each end user and a field in that table to uniquely identify each user. To identify the table and field within the table, click the button under the Ticket ID field. If PasswordCourier has never been configured, the button label will be **SELECT FIELD/TABLE**. If PasswordCourier has been previously configured, the label on the button reflects the table and field previously selected. Because the field selected uniquely identifies each end user, this field also becomes the unique identifier field if User-Based Targets is enabled. For additional information, see *"User-Based Targets" on page 62*.

1. To configure the first user validation entry, in the next line of fields, click the **SELECT FIELD/TABLE** button (labeled **EMPLOYEETEXTID/EMPLOYEES** in *Figure 7*) to select the table and field for the first field of the end user validation. This button provides a mechanism to select the table/field against which user information will be verified.

   A dialog box pops up to allow you to choose the system table that contains the end user profile information (*Figure 8*).

**Figure 8: Connecting a Field to the Table**




2. When a table is selected in the left column, the right column is updated to reflect the fields in that table. Select the desired field. PasswordCourier can now connect to the database to verify the validation information the end user enters to perform a password reset request. Click **OK** to close the window.

   **Note:** The first field selected must contain unique information for each user (e.g., a badge number) if User Based Targets will be used. See *"User-Based Targets" on page 62*.

3. In the Format & Connection tab, in the same line of fields, manually type the name of the field selected or an alias into the first text box. This entry will be shown to the user to prompt the user to enter the appropriate information.
4. To configure the remaining user validation entries (if more than one was indicated on the User Validation tab, for each validation entry, select an end user validation field from the corresponding drop-down menu. This menu duplicates the list of fields from the pop up window. Manually enter the name of the selected field or an alias into the text field to the left of the drop down menu. This entry will be displayed to prompt the end user to enter the appropriate information.
5. To display asterisks rather than text in the validation fields, check the box labeled **SECURE** next to one or both entries.

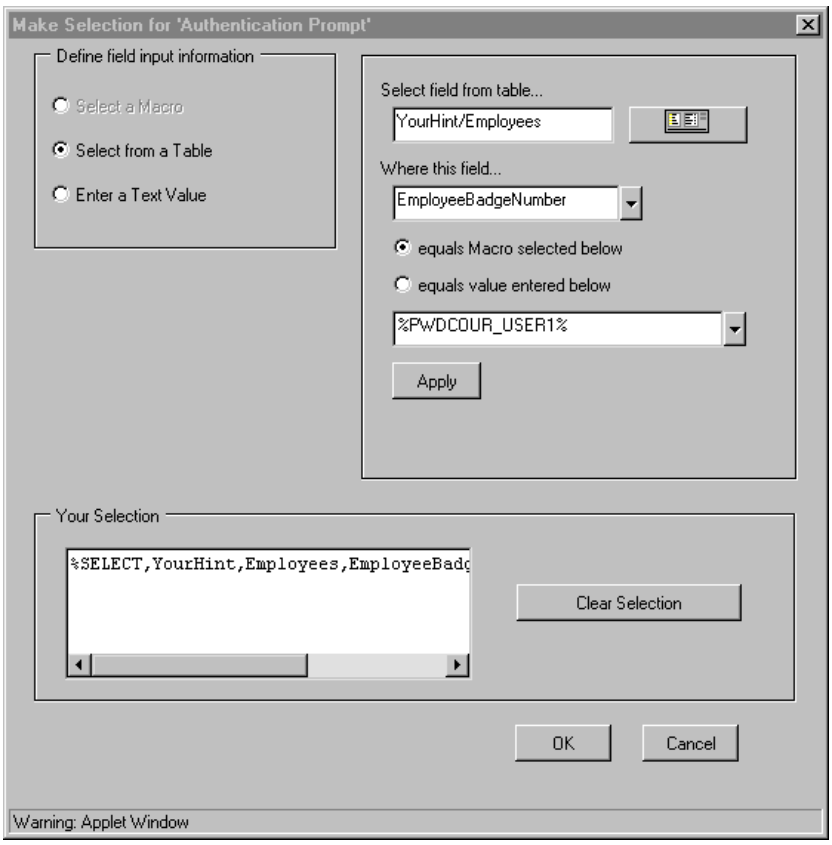
### Configuring End User Authentication

The next line of fields allows the configuration of end user authentication (*"Format & Connection Tab for PasswordCourier"*). You can configure the prompt for the authentication field either as fixed text for every end user or the information can be loaded from the profile database (*Figure 9*).

1. To configure the authentication question, click the **PROMPT** button. A pop-up window appears (*"Format & Connection Tab for PasswordCourier"*).

   **Note:** If **CLEAR SELECTION** is not clicked at this time, newly configured information will be appended to the existing configuration show in the **YOUR SELECTION** text box rather than replacing it.

**Figure 9: Authentication Prompt Dialog Box**



2. If private authentication question and answer fields are included in the profile database, you can select these in this configuration. Click “OK” to save the configuration and close the window.

For example, in the illustration above, **YOURHINT/EMPLOYEES** (“YourHint” indicating the field and “Employees” indicating the table) is selected from the profile table so that the end user receives the private authentication question originally entered into the profile. The answer would be selected from a drop down menu.

The remaining fields in the Format and Connection tab duplicate the fields seen by the end user.

### Use Comments

The **USE COMMENTS** check box on the Format & Connection tab allows you to specify whether a field for end user-specified comments is displayed in PasswordCourier. To include the comments field, select this box and provide a prompt text string in the text box. Unchecking the box hides the prompt field. When **USE COMMENTS** is checked, the `%PWDCOUR_COMMENTS%` macro is available for use in Update Ticket. When **USE COMMENTS** is not checked, the `%PWDCOUR_COMMENTS%` macro is not available for selection (see *“Macro Dependencies” on page 100*).

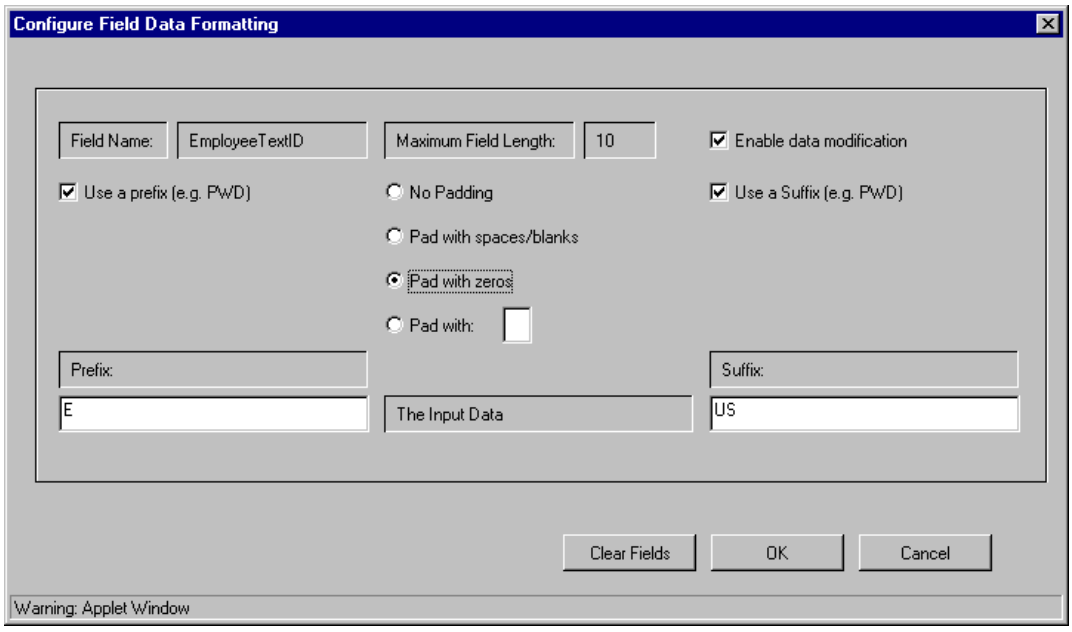
**Note:** If, at an earlier time, a ticket that was configured to use the `%PWDCOUR_COMMENTS%` macro and **USE COMMENTS** is subsequently disabled, other locations that use this macro must be updated because it will no longer have a value associated with it. For more information on Core Server macros for PasswordCourier, see *“Courion Server Macros” on page 93*.

After specifying all desired prompts and field references, click the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous values.

### Field Data Format Configuration

It is possible to format data entered by the end user by configuring the Field Data Formatting Dialog Box (*Figure 10*). To do this, click the **FORMAT** button associated with the field. A dialog box appears with the name of the selected field and the field length.

**Figure 10: Configure Field Data Dialog Box**




Field data formatting can only be performed on text fields; clicking on nontext fields produces an error message. Check the **ENABLE DATA MODIFICATION** check box to configure this field. Once the box is checked, you can select other fields.

There are three ways to configure and modify the data:

- Add a prefix to the data the end user enters in the specified field. The **USE A PREFIX** check box enables the **PREFIX** text entry.
- Add a suffix to the end of the data the end user enters in the specified field. The **USE A SUFFIX** check box enables the **SUFFIX** text entry.
- Add padding when the end user's data, along with the applicable prefix and/or suffix, does not fill the entire field.

For example, the end user enters "5000" into the employee id field and the field is 10 characters long. A prefix of "E" (for employee versus contractors) is specified along with a suffix of "US" (versus overseas). Padding may then be applied:

- No Padding — do not perform any padding. The data is unchanged and is left as E5000US.
- Pad with spaces/blanks — pad the rest of the field with spaces/blanks. The data becomes E 5000US.
- Pad with zeros — pad the rest of the field with zeros. The data becomes E0005000US.
- Pad with specified character — pad the rest of the field with the entered character. If the character specified is "X" then the data becomes EXXX5000US.

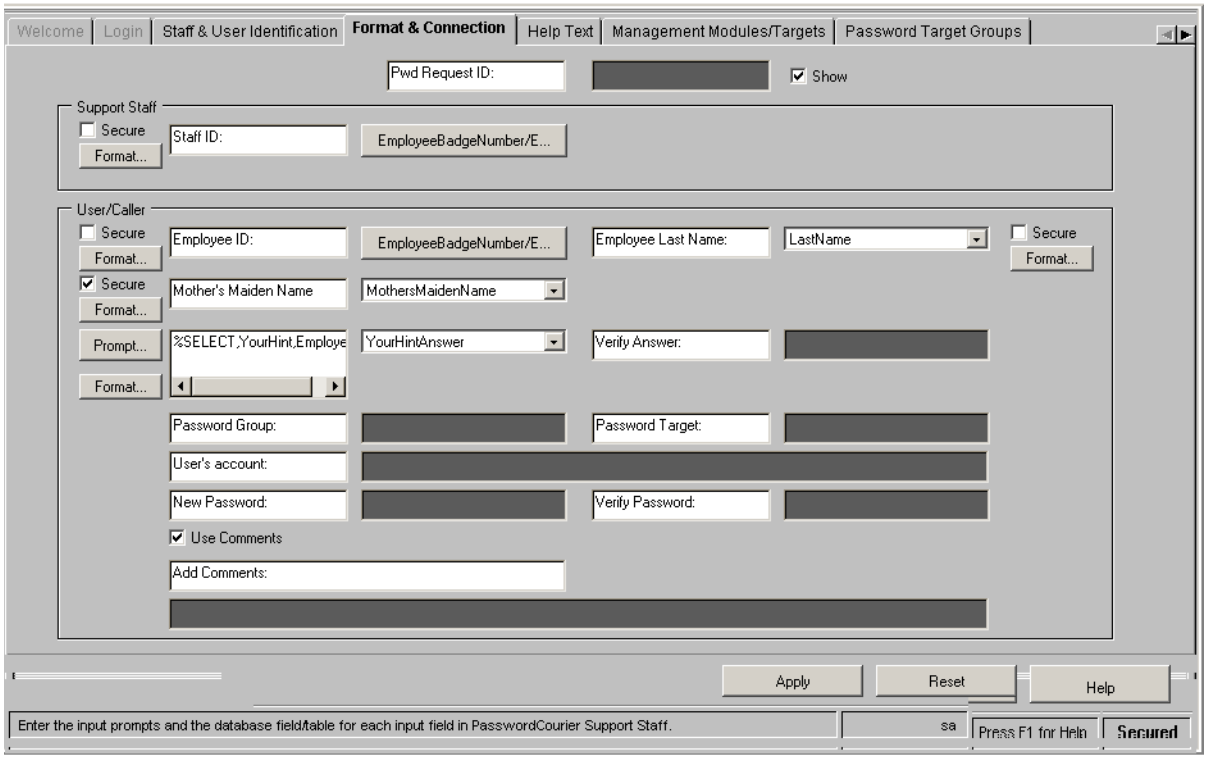
This feature is useful when the end user enters data that is to be stored with additional information. The employee would supply the badge number simply as 5000, but before the look up is done to validate/authenticate the end user using this field, the data is formatted. In the example in the dialog box, the look up is actually done with the badge number = E0005000US.

### *Format & Connection Tab in PasswordCourier Support Staff*

The Format & Connection tab in PasswordCourier Support Staff is exactly like its counterpart in PasswordCourier except that it has an additional section to configure support staff verification (*Figure 11*). The support staff section contains a **USER'S ACCOUNT** feature, which allows customers that do not have a UBT table, or those that keep user's account names in the user's profile, to have an input field so that the Support Staff user can enter the user's account name for the reset.

Configuring the Field Data Formatting tab in PasswordCourier Support Staff is the same as it is in PasswordCourier.

**Figure 11: Format & Connection Tab for PasswordCourier Support Staff**

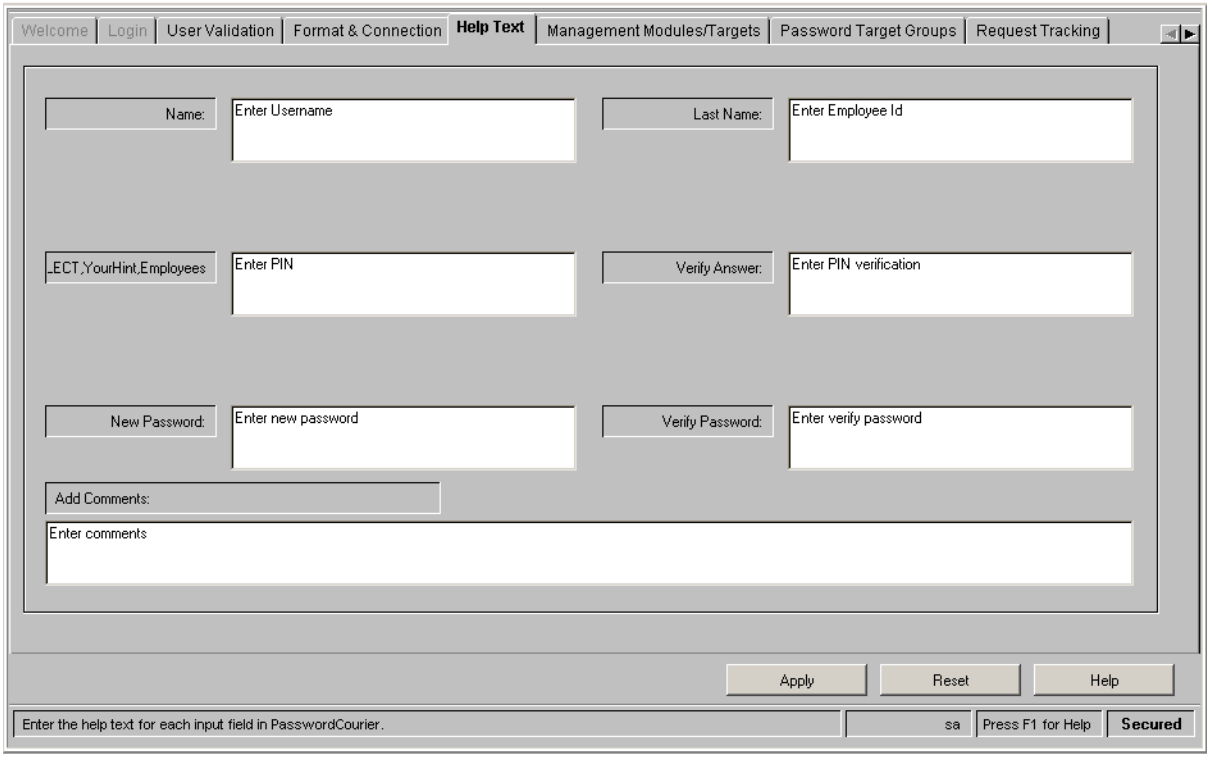



## Help Text Tab

### *Help Text in PasswordCourier*

When the cursor is placed at an entry field and an end user presses the **HELP** button (open book icon) next to a specific field in either Web Access (Java) or Web Access (ASP), PasswordCourier provides help text defined in the PasswordCourier Customization Manager for that field. The Help Text tab allows you to enter the custom help text (*Figure 12*).

**Figure 12: Help Text Tab for PasswordCourier**




Next to each end user prompt, there is a text box where you can enter the appropriate help text. By default, the Help Text tab displays text boxes only for the User Validation fields defined on the User Validation tab. Text boxes for end user authentication and verification are displayed if the **YES, USER AUTHENTICATION** check box is checked.

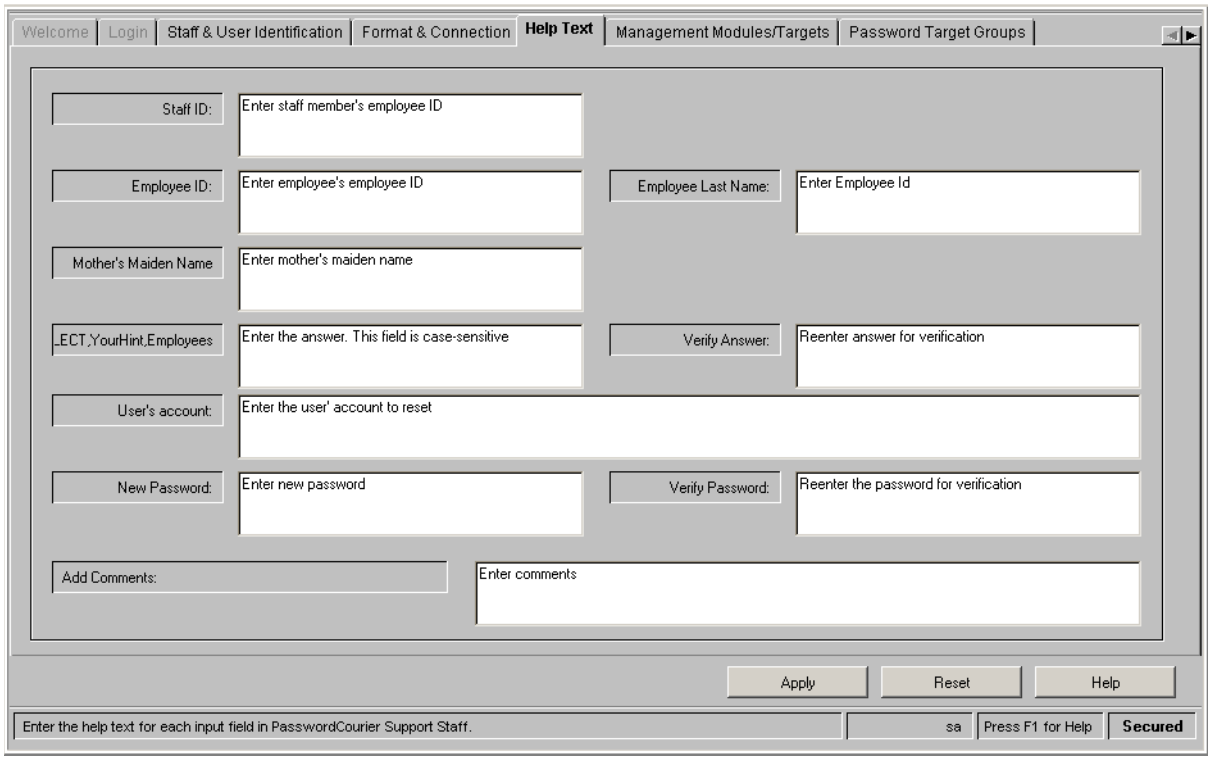
**Note:** Entered text does not automatically wrap. Press **ENTER** to end a line of text and start the next text line. The help text should not exceed seven (7) lines of 40 characters each. To force text to show on a new line, use **CTRL/ENTER** to insert a new line.

Click the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous values.

## *Help Text in PasswordCourier Support Staff*

When the support staff user places the cursor in an entry field and presses either the F1 function key or the **HELP** button, PasswordCourier Support Staff presents help text defined in the PasswordCourier Support Staff Customization Manager for that field (*Figure 13*). The behavior of this tab mirrors that described above for the Help Text tab in PasswordCourier.

**Figure 13: Help Text Tab for PasswordCourier Support Staff**



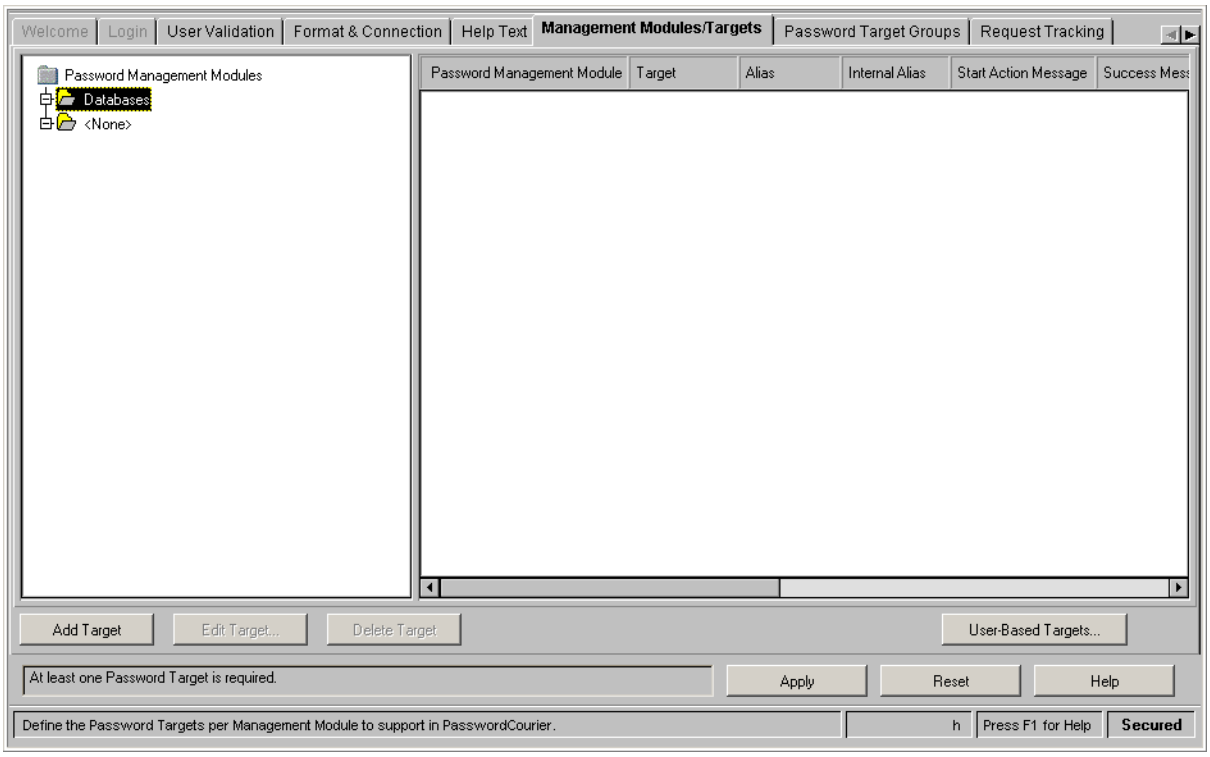

## Management Modules/Targets Tab

You need to define Password Targets before performing password resets in PasswordCourier and PasswordCourier Support Staff. A Password Target is defined to represent a real destination, such as a Windows NT ® Domain or Novell NDS® tree or other supported types of password resets. The Management Modules/Targets tab enables you to define Password Targets under the appropriate PMM(s) (*Figure 14*). The tab is structured with two major display areas. The left hand side of the tab contains a tree structure of configured PMMs with defined Password Targets listed as children. The right hand side of the tab contains a list of Password Target attributes for the selected Target(s).

**Note:** When a PMM is configured here, it must match the target name that was configured in the Customization Manager for that PMM.

**Note:** The Customization Manager will not allow a target to be created with a name that includes the name of the Password Management Module. For example, target names such as “NetscapeDS” or “CorpNetscapeDS” cannot be created for the PMM for NetscapeDS.

**Figure 14: Management Modules/Target Tab**

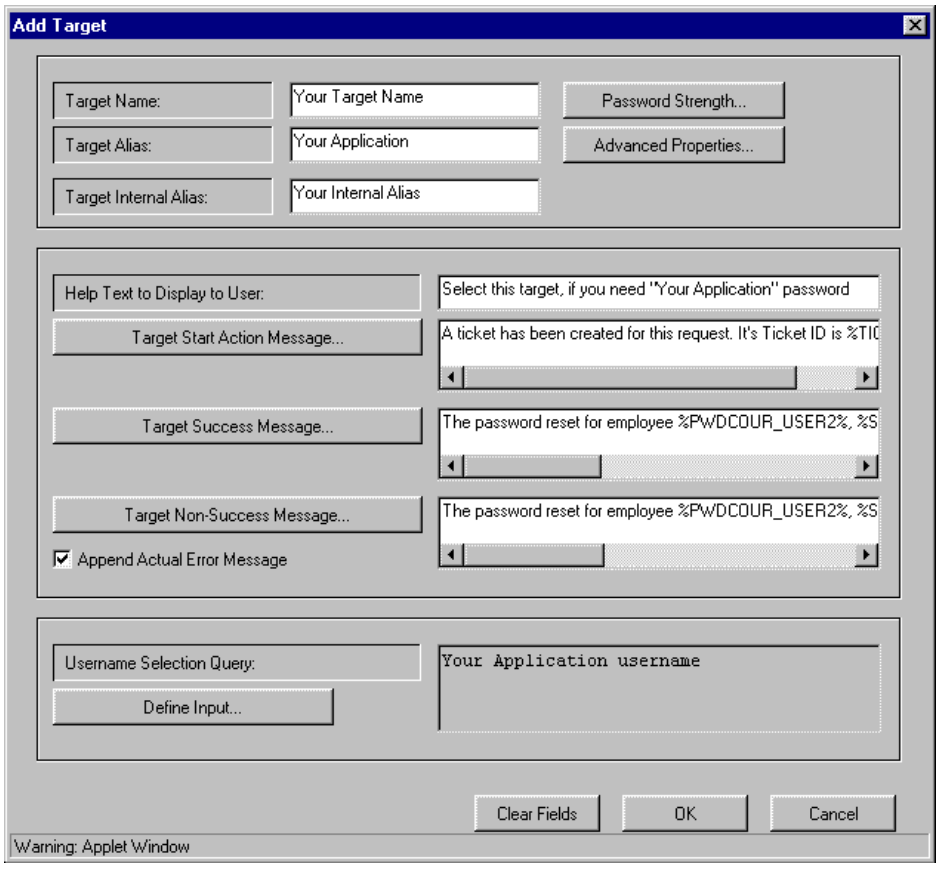



Double-click the **PASSWORD MANAGEMENT MODULES** node to display the list of configured PMMs. The PMM **NONE** is always listed along with any other configured PMM(s). Double-click a PMM to display the defined Password Targets for that module. The right hand tab displays the PMM's targets and target attributes. If a specific target is selected, then only that target's attributes are displayed. To display all defined targets, click the **PASSWORD MANAGEMENT MODULES** node and all defined targets are displayed on the right hand tab.

The following sections describe how to add, edit, and delete targets. The Management Modules/ Targets tab is updated with any changes that result from any addition, modification, or deletion of the target(s). click the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous values.

1. To add a target, click the **PASSWORD MANAGEMENT MODULES** node once. The **ADD TARGET** button at the bottom of the tab will become active. Click the **ADD TARGET** button and an Add Target dialog box will appear (*Figure 15*).

**Figure 15: Add Target Dialog Box**




The fields in this dialog box must be configured according to specific rules.

### *Password Target Definition Rules*

The following rules apply for target definition:

- The target name must match exactly the target name entered in the applicable PMM Configuration Manager
- A target/alias pair must be unique.
- When used with a different target name, an alias can be duplicated.
- A target name/alias pair can belong to multiple groups.

### *Password Target Attributes*

The Add Target dialog box allows you to configure the attributes for each password target. Every password target has the following attributes, which you configure in the top two sections of the Target Attributes dialog box:

**Table 2: Password Target Attributes**

| Attribute Name | Description | Target Attribute Dialog Field |
|---|---|---|
| Target Name | The actual name of the system as defined in the CMM Configuration Manager. | This text field is required. The characters \| , % ^ = + are not allowed. |
| Target Alias | A display name for the actual target. If you define a target alias, PasswordCourier displays this alias to the end user. If you do not define a target alias PasswordCourier displays the actual Target name to the end user. | This is a text field. The characters \| , % ^ = + are not allowed. |
| Target Internal Alias | This is an internal-use-only alias for the actual target. This alias is not displayed to the end user when the user is challenged to select the Password Target. The macro %PWDCOUR_TARGET_INTALIAS% contains this configured internal alias and can be used in the "Request Tracking" auditing actions. PasswordCourier Support Staff's representation of this macro is %PWDSS_TARGET_INTALIAS%. | This is a text field. It is not required. |
| Help Message | PasswordCourier displays this help text when an end user presses the F1 key with the cursor on this target. | This is a scrolling text field. |
| Start Action Message | PasswordCourier displays this text when the end user presses the “Next” button (after the user selects the Password Group and Password Target). Now, the Start Action occurs. Start Actions are configured on the **REQUEST TRACKING** tab. If a ticket is configured to be created on the Start Action, include the %TICKET_ID% in this message. Many, but not all, macros are valid at the Start Action. Macro availability is discussed in *“Courion Server Macros” on page 93*. | This is a scrolling text field. |
| Success Message | This text is displayed to the end user upon successful completion of a password reset for this Password Target. Static text, macros, and information selected from the database can be included in this message. | This is a scrolling text field. |

**Table 2: Password Target Attributes**

| Attribute Name | Description | Target Attribute Dialog Field |
|---|---|---|
| Nonsuccess Message | This text is displayed to the end user if the password reset is not successfully completed for this Password Target. Static text, macros, and information selected from the database can be included in this message. The *User Selection Query section* explains how to provide text, macros, and select from a table in the database. | This is a scrolling text field. |
| Append Actual Error flag | This flag indicates whether the actual error that occurred during reset of this Password Target is appended to the Nonsuccess Message that is configured for this target. | This check box toggles the option on and off. |
| User Name Selection Query | This specifies how to find end user names to reset passwords for this target. | This field is populated by clicking on the "Define Input..." button and filling out the information in the displayed dialog box. |
| Unique Target Identifier | This field replaces the User Name Selection Query field when User-Based Targets is made active. This field reflects the value in the Target ID field on the *"User-Based Targets" on page 62* configuration screen. | This field is populated via the User-Based Targets configuration screen. |

### Username Selection Query

To reset a password, PasswordCourier relies on three pieces of information (known as a triplet):

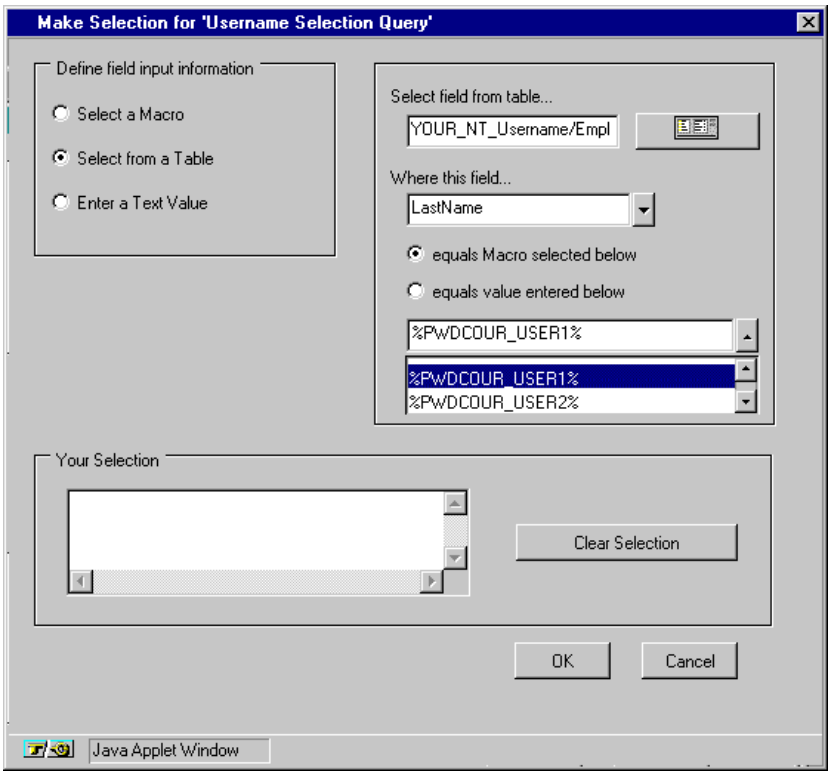
- The PMM, which identifies the system on which the password reset will be performed
- The target name, which identifies the server on which the password reset will be performed
- The user account on which the password reset will be performed

The third piece of information is provided either through the **USERNAME SELECTION QUERY** or through *"User-Based Targets" on page 62*. The bottom section of the Target Attributes dialog box is dedicated to configuring the **USER NAME SELECTION QUERY** (*Figure 15*). For this function, you must configure PasswordCourier to either create or find the end user's user name for every defined target with a macro, a table, or hard coded text.

**Note:** This feature is disabled whenever User-Based Targets is activated.

Click the **DEFINE INPUT** button in the target attributes dialog box and a dialog pops up to configure the **USERNAME SELECTION QUERY** (*Figure 16*).

**Figure 16: Defining User Name via a Macro**



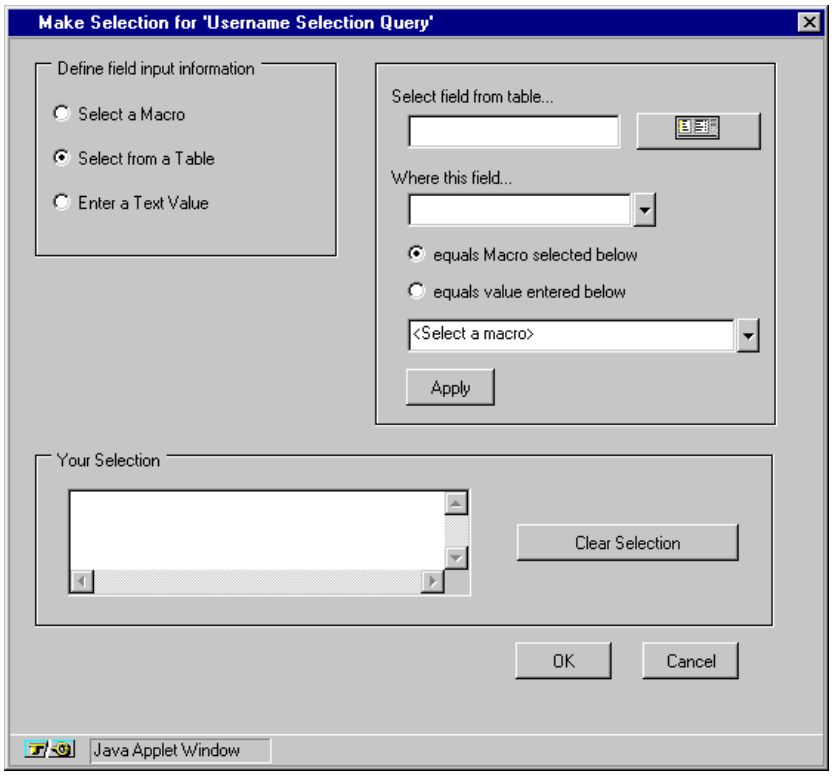

## Macros

A macro will identify the end user's username for the system on which the password reset will be performed if the end user entered this username as a part of the validation information when first logging in to PasswordCourier. To use a macro, click the **SELECT A MACRO** button (*Figure 16*) and select the appropriate macro from the list box. For example, if PasswordCourier is configured to prompt the end user for their user name in the second validation field, then select the `%PWDCOUR_USER2%` macro. See *"Courion Server Macros" on page 93* for a description of the information held by PasswordCourier that is made available via macros.

## Tables

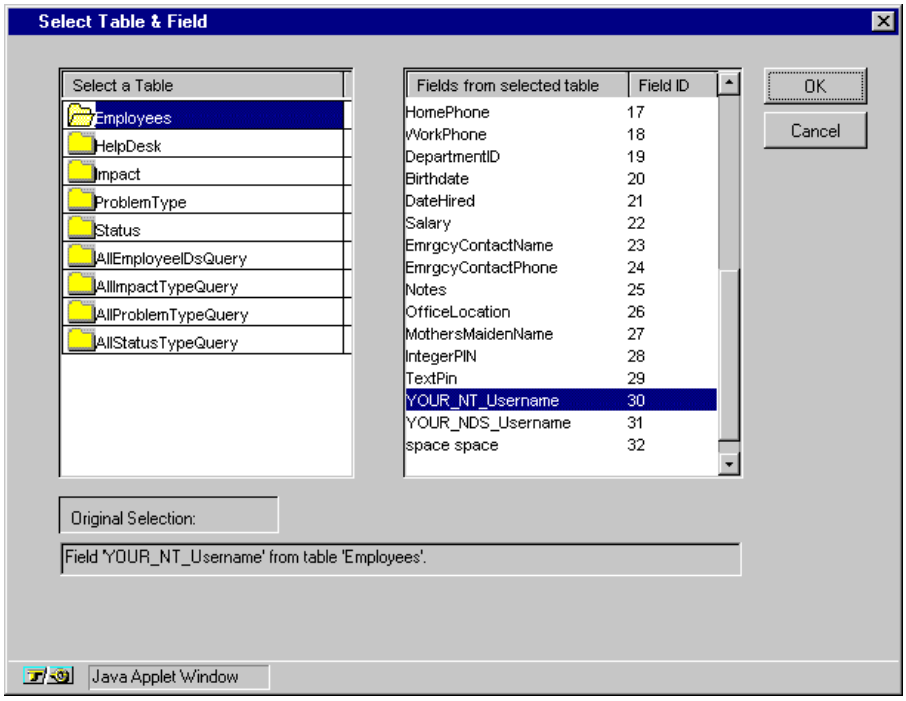
The user name may also be populated from the field in the end user's profile that contains the end user's system user name. Click the **SELECT FROM A TABLE** button (*Figure 17*) and the right side of the dialog box will update with the appropriate fields.

**Figure 17: Defining User Name via Database Information**




On the right side of the dialog box, click the **SELECT FIELD FROM TABLE** button. A table/field selection dialog, similar to the dialog in the Format & Connection tab, pops up (*Figure 18*).

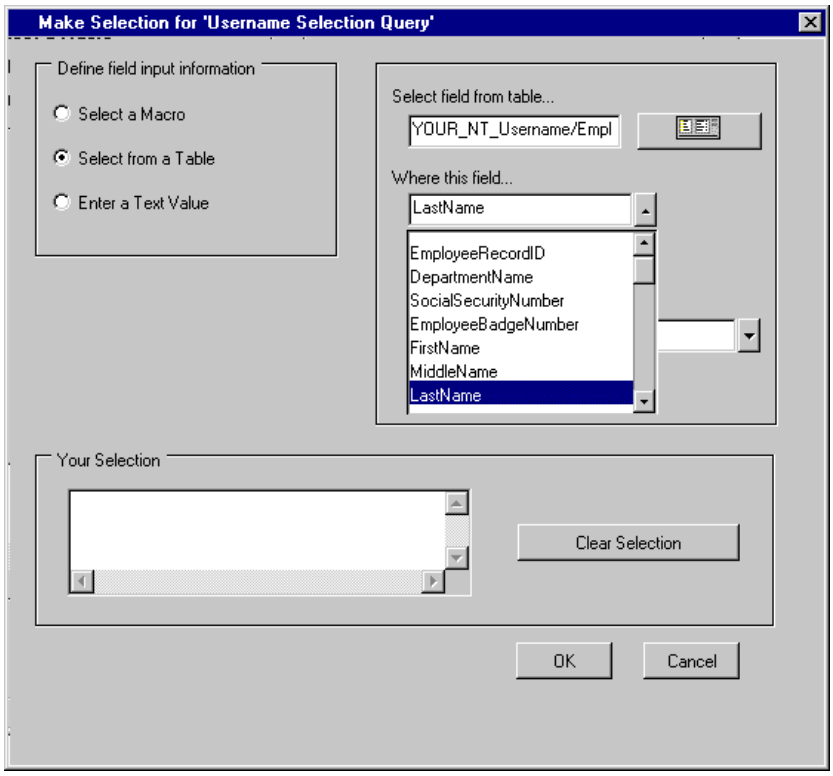
**Figure 18: Selecting the Table & Field Containing the End User's User Name**




1. Click the table containing the end user's username and the available fields are displayed in the right hand column.

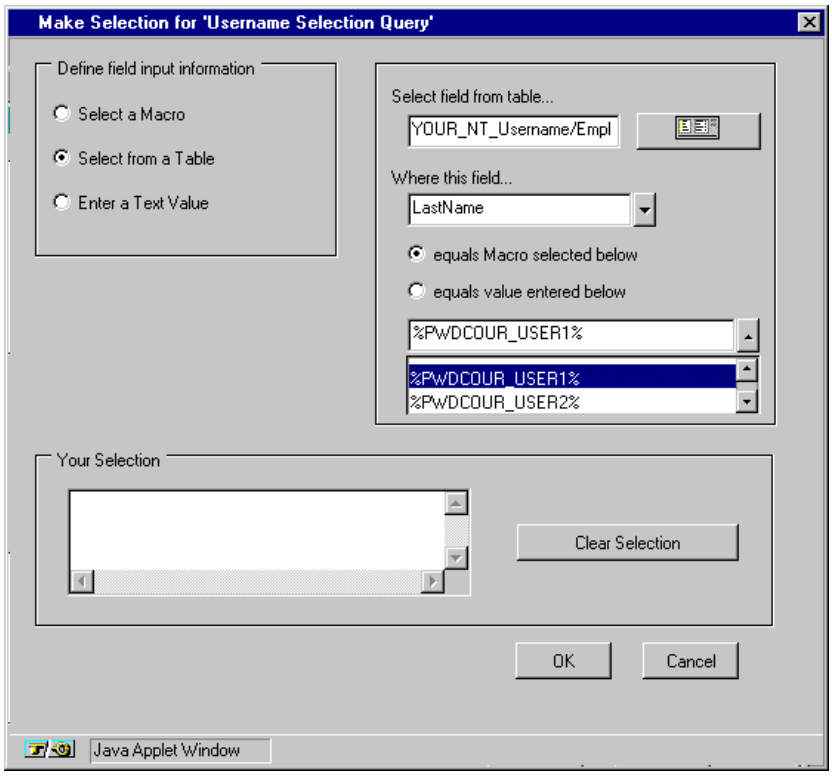
2. Click the field containing the end user's username. Click the **OK** button to close the dialog box and return to defining the selection statement. The field selected is displayed along with the table name in the field labeled **SELECT FIELD FROM TABLE...**.
3. In the drop down menu labeled **WHERE THIS FIELD...**, select the field in the database table that contains the key for the selection from the database (for example, enter the Windows NT user name, based on the key of LastName equal to the end user's entry of the Last Name) (*Figure 19*).

**Figure 19: Choose a Selection Key for Username Selection Query**




4. Below the drop down menu, select whether the value in the key field is to be compared to a macro ("equals Macro selected below") or a value entered here ("equals value entered below") (*Figure 20*).
5. After choosing the key field, enter the desired value. In *Figure 20*, a macro is selected that contains the end user's entry for the first end user validation field; LastName.

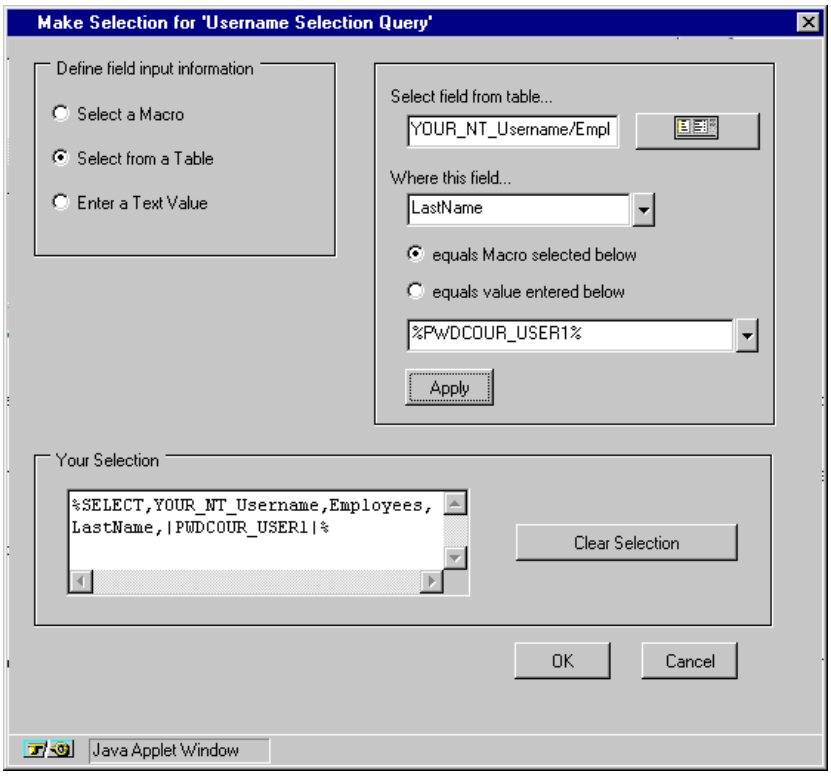
**Figure 20: Choose a Macro for the Selection Key for Username Selection Query**




6. Click the **CLEAR SELECTION** button to remove old configuration information. If this button is not clicked, the new configuration information will be appended to the old configuration rather than replacing it.
7. Click the **APPLY** button to copy the selection to the bottom text field labeled **YOUR SELECTION**. If satisfied with the default query, click the **OK** button.

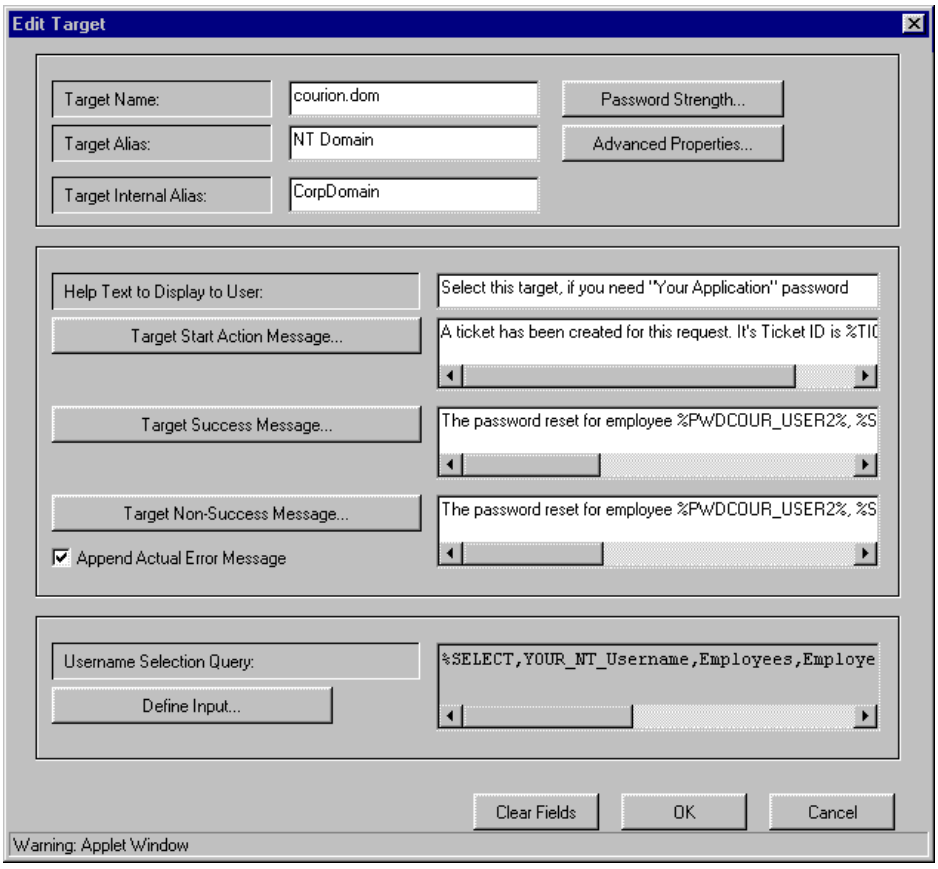
**Note:** whatever is configured in the top half of the dialog box (for tables, macros, or text) is added to the information displayed in the bottom text field labeled **YOUR SELECTION** once the **APPLY** button is clicked (*Figure 21*). Click the **CLEAR SELECTION** button to clear the bottom text field.

**Figure 21: Value for Selection of End User's Password Target User Name**




PasswordCourier copies the information from the Username Selection Query dialog box and fills in the area to the right of the **USERNAME SELECTION QUERY** label on the Edit Target Attributes dialog (*Figure 22*).

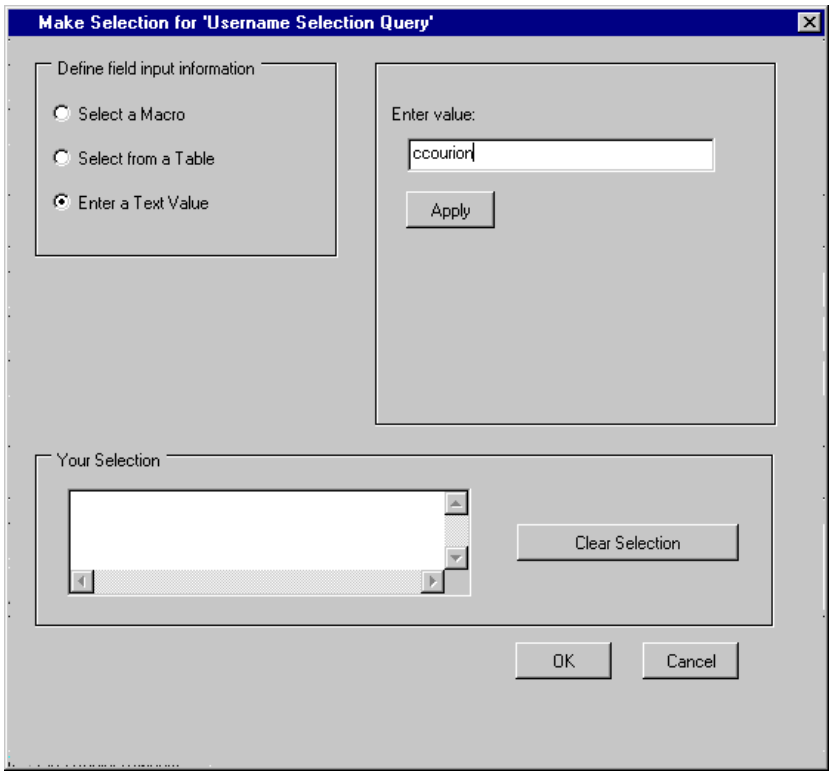
**Figure 22: Completed Username Selection Query**




## Text Values

PasswordCourier provides the functionality to enter custom text in this field (*Figure 23*). This option, however, causes the end user name to remain the same regardless of who resets this Password Target. This can be useful for testing.

**Figure 23: Defining User Name via a Text Value**




## Synchronization Target Configuration

**Note:** Before targets can be added for the PMM for Synchronization, all PMMs with targets that will be included in the synchronized password reset must be configured.

Synchronized targets are targets that may all be set to the same password in a single password reset request. To configure the Synchronization Target when the Username Selection Query is in use, “triplets” of information must be built in the Add Target or Edit Target dialog box. A triplet provides three essential pieces of information:

- the PMM (which identifies the type of system)
- the Target (which identifies the server)\
- the Username (which identifies the account).

To build a list of triplets for all targets to be included in the Synchronization target:

1. In the Management Modules/Targets tab (*Figure 14*), highlight the folder labeled **SYNCHRONIZATION** and click the **ADD TARGET** button to launch the **ADD TARGET** dialog box (*Figure 15*).
2. In the field labeled **TARGET NAME**, enter a descriptive generic target name (for example, “Synch”).

   **Note:** This name cannot be the same name as the installed PMM.
3. In the field labeled **TARGET ALIAS**, enter a descriptive target name that will be viewed by end users. If nothing is entered into this field, it will default to the name entered in the **TARGET NAME** field.
4. If a third alias is desired, enter it in the **TARGET INTERNAL ALIAS** field.

5. In the **HELP TEXT TO DISPLAY TO USERS**, **TARGET START ACTION MESSAGE**, **TARGET SUCCESS ACTION MESSAGE**, and **TARGET NON-SUCCESS MESSAGE** fields, enter help text for the end user. (For more detailed instructions see *"Password Target Attributes" on page 36*.)
6. Under **USERNAME SELECTION QUERY**, click the **DEFINE INPUT** button to launch the Username Selection Query dialog box (*Figure 16*).
7. In the text box under **YOUR SELECTION** at the bottom of the dialog box, type the name of a PMM to be included in the sychronized reset **exactly as it appears in the Management Modules/Targets tab**, followed by a semicolon.
8. Immediately following the semicolon (do not leave a space), type the name of target, followed by a semicolon.
9. Leave the cursor immediately in front of the second semicolon (do not leave a space).
10. In the top half of the dialogue box, indicate the Username Selection Query via a macro or table as described in *"Username Selection Query" on page 37*.
11. Click the **APPLY** button and the information will be inserted after the semicolon in the text box at the bottom of the dialog box, completing the triplet required to reset the password on the target specified.

    *Figure 24* shows an NT and Novell NDS account, both using a selection statement for the username. Notice the triplets separated by semicolon and the elements of the select statement separated by commas.

**Figure 24: Triplets**

```
Windows NT;target1;%SELECT,YOUR_NT_Username,Employees, employeeBadgeNumber|PWDCOUR_USER1|%;
Netware;target2;%SELECT,YOUR_NDS_Username,Employees, EmployeeBadgeNumber|PWDCOUR_USER1|%
```

    **Note:** triplets must always be built in the same order: module, target, username.

12. To add additional targets for a synchronized reset, type a semicolon after the username selection query in the text box at the bottom of the dialog box and repeat steps seven through eleven. Make sure not to include any spaces within or between the triplets.
13. When you have added all desired targets, click the **OK** button on the Make Selection for Username Selection Query dialog box. Click the **OK** button on the Add Target dialog box.

**Note:** The steps to configure the Synchronization target are different when User-Based Targets is enabled. Please see *"Synchronization Target Configuration when User-Based Targets is Enabled" on page 69*.

## *PMM (Password Management Module) Properties*

### Advanced Properties

While target attributes are common to all PMMs, target properties are attributes that are frequently configured so they are supported only by specific PMMs. There are two PMM properties: "Reset to Escrow Password" and the "User Must Change Password at Next Logon."

### “Reset to Escrow Password” Property

1. On the Target Attributes Dialog, click the **ADVANCED PROPERTIES...** button to bring up the Properties dialog (*Figure 25*). The "Reset to Escrow Password" property is available for selection.
2. If this option is selected, click the **DEFINE INPUT...** button to define from where the escrow password should be extracted.

You can configure all PMMs to support the "Reset to Escrow Password" property. When set, this property resets the end user’s password to the defined escrow password. You can define an escrow password to be a field in the database where the information is selected based on key information for the end user. For example, a field in the database containing the escrow password may be obtained using the employee’s badge number. This ensures that each person has a unique escrow password. If an escrow password is being used, the end user is not prompted for a password in PasswordCourier or PasswordCourier Support Staff.

**Note:** When a password target is set to use the "Reset to Escrow Password" property, the password strength constraints are not enforced. Password strength constraints are enforced when the end user provides a password for a specific target linked with specific PMMs.

### “User Must Change Password at Next Log On” Property

Not all PMMs support the "User Must Change Password at Next Logon" property. This property forces end users to change their passwords as soon as they log in, thereby ensuring that the end user is the only one with access to the password information. This is especially useful in the case where PasswordCourier Support Staff is used and a support staff member may have knowledge of the password that was set for the end user or when escrow passwords are being used.

1. On the Target Attributes Dialog, click the **ADVANCED PROPERTIES...** button to bring up the Properties dialog (*Figure 25*).

   When a target is defined for a PMM that supports the "User Must Change Password at Next Log On" property, the box to enable this function is available on the properties dialog box for selection. When a target is defined for a PMM that does not support this property, it does not appear on the properties dialog box at all. This provides the flexibility for properties to be supported only by appropriate PMMs while allowing these properties to be configured on a per target basis.

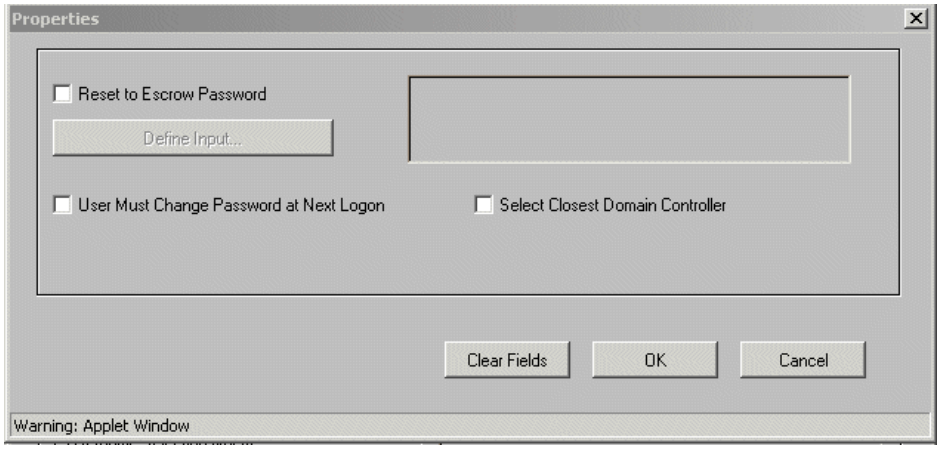
**Note:** In the interest of system security, Core Security strongly recommends the use of the "User Must Change Password at Next Log On" property in conjunction with the use of escrow passwords so that the end user must change passwords after the initial log on.

**Note:** Check the end user account in the Windows NT ® User Manager. If the end user has **PASSWORD NEVER EXPIRES** checked, this overrides the "User Must Change Password at Next Logon" property.

### Select Closest Domain Controller

If the **SELECT CLOSEST DOMAIN CONTROLLER** checkbox is checked, PasswordCourier unlocks and resets accounts on the Domain Controller located nearest to the end user’s machine, rather than performing the reset on the Primary Domain Controller, potentially requiring the end user to wait until the reset is replicated to the rest of the network.

**Figure 25: Advanced Properties**




## Password Strength

To apply password strength capabilities to all new passwords on a target, click the **PASSWORD STRENGTH** button. This opens up a dialog box that describes the current attributes the passwords are to be checked against before attempting the password reset request (*Figure 26*). If any of the characteristics of the new password fail to pass the password strength rules, the password is immediately rejected and the end user is presented a reminder about the rules passwords must follow. When a warning message is displayed and acknowledged, the end user is given another chance to enter a valid password.

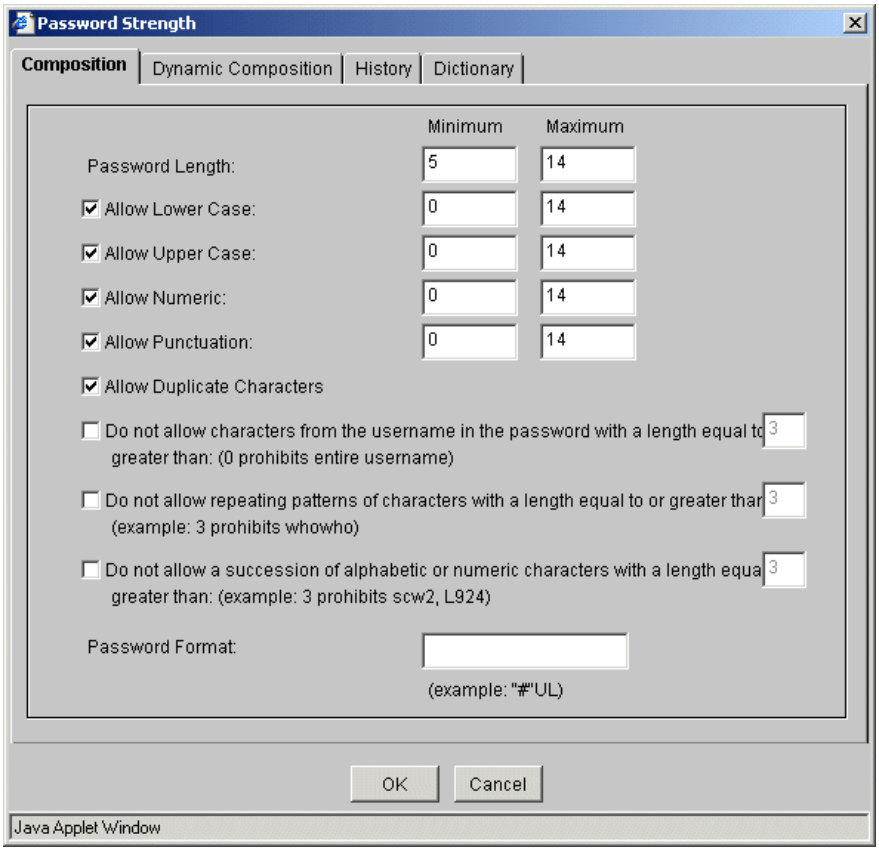
**Note:** Each defined target can be configured to have its own Password Strength and Advanced Property settings. This provides the flexibility to set different criteria on the various configured targets.

**Note:** If a Synchronization target is specified during the end user's password reset process, the composition, history, and dictionary settings of the Synchronization target override those of the individual targets.

### Password Composition

End User password composition includes all criteria associated with the character format of the password.

**Figure 26: Password Composition Tab**




With password composition, you can enforce Minimum/Maximum values on different character sets along with the overall size of the password and its format. Table 3 explains the password composition attributes.

**Table 3: End User Password Composition Attributes**

| Attribute Name | Description | Target Attribute Dialog Field Information |
|---|---|---|
| Password Length Minimum | The minimum length of an acceptable password | Passwords that fall below this value in length are rejected. |
| Password Length Maximum | The maximum length of an acceptable password | Passwords that exceed this value in length are rejected. |
| Lowercase Character Minimum | The minimum number of characters that must be lowercase | This value ranges from 0 to the Password Length Maximum less the total of all minimum required characters from other character sets. |

**Table 3: End User Password Composition Attributes**

| Attribute Name | Description | Target Attribute Dialog Field Information |
|---|---|---|
| Lowercase Character Maximum | The maximum number of characters that can be lowercase | The range of this value depends on the total of all maximum values declared for each of the character sets. This number must meet or exceed the Password Length Minimum. |
| Uppercase Character Minimum | The minimum number of characters that must be uppercase | This value ranges from 0 to the Password Length Maximum less the total of all minimum required characters from other character sets. |
| Uppercase Character Maximum | The maximum number of characters that can be uppercase | The range of this value depends on the total of maximum values declared for each of the character sets. This number must meet or exceed the Password Length Minimum. |
| Numeric Character Minimum | The minimum number of characters that must be numeric | This value ranges from 0 to the Password Length Maximum less the total of all minimum required characters from other character sets. |
| Numeric Character Maximum | The maximum number of characters that can be numeric | The range of this value depends on the total of all maximum values declared for each of the character sets. This total must either meet or exceed the Password Length Minimum. |
| Punctuation Character Minimum | The minimum number of characters that must be punctuation | This value ranges from 0 to the Password Length Maximum less the total of all minimum required characters from other character sets. |
| Punctuation Character Maximum | The maximum number of characters that can be punctuation | The range of this value depends on the total of all maximum values declared for each of the character sets. This total must either meet or exceed the Password Length Minimum. |
| Password Format Field | This field supplies a coded format that is masked against the password value to check conformity to a specific character ordering sequence | The syntax for this field is described in section *“Applying a Password Format” on page 51*. |
| Allow Lowercase | This toggle determines whether the Minimum/Maximum values for lowercase apply as strength checks | |
| Allow Uppercase | This toggle determines whether the Minimum/Maximum values for uppercase apply as strength checks | |
| Allow Numeric | This toggle determines whether the Minimum/Maximum values for numeric characters apply as strength checks | |
| Allow Punctuation | This toggle determines whether the Minimum/Maximum values for punctuation characters are applied as strength checks. | |

**Table 3: End User Password Composition Attributes**

| Attribute Name | Description | Target Attribute Dialog Field Information |
|---|---|---|
| Allow Duplicate Characters | This toggle determines whether the password may contain duplicate characters. If this is unchecked and duplicates are found, the end user is notified of the problem. | |

Note: Be sure that the value you configure for one setting does not conflict with the value you configure for another setting. For example, do not set the maximum password length to 5 and the minimum password length to 10. Or do not set the maximum uppercase to 10 and the minimum password length to 8.

### Selecting Do Not Allow Check Boxes

The Do Not Allow check boxes allow you to strengthen the parameters on a password with features such as: characters allowed from the username in the password, repeating patterns of characters allowed in the password, and the succession of alphabetic or numeric characters allowed in the password with length restrictions enforced on each feature.

By default, each of these features is disabled and the initial length for each feature is set to 3.

- Do not allow characters from the username in the password with a length equal to or greater than N - verifies that the password does not contain more than N sequential characters from the username. For example, if a username contained “janedoe” and the length specified was 4, then a password with characters “jane123” would be invalid. However, a password with characters “jnde123” would be valid. (Entering 0 for the length prohibits the entire username).

  For the strength check only, the check for characters in the comparison of password and username is case-insensitive. For example, if the username is "janedoe" and the number of sequential characters to look for is 4, then a password of "jane1234" or "JANE1234" or "Jane1234" would not pass the password strength check because PasswordCourier would see the first four characters as the same regardless of case.
- Do not allow repeating patterns of characters with a length equal to or greater than N - verifies that the pattern does not repeat in the password for the length (N) specified. For example, if the length specified was 4, then a password with characters “janejane” would be invalid, as the pattern “jane” repeats in the password.
- Do not allow a succession of alphabetic or numeric characters with a length equal to or greater than N - verifies that the alphabetic or numeric characters do not appear in succession for the length (N) specified. For example, if the length specified was 4, then a password with alphabets in succession “abcd7xz” would be invalid. Similarly, a password with numbers in succession “1234yz3” would be invalid.

### Applying a Password Format

The Password Format feature allows you to enforce the rules governing the sequential layout of all password characters. By doing this, you can increase the strength of a password simply by requiring certain types of characters to reside at specified places within the password.

A password format contains a listing of characters that represent different combinations of each of the character sets (uppercase, lowercase, numeric, and punctuation). Table provides the syntax definition of a password format.

**Table 4: Password Format Syntax**

| Symbol | Representation |
|---|---|
| A | This symbol represents all uppercase and lowercase characters. |
| X | This symbol represents all alphanumeric characters (A–Z), (a–z), (0–9). |
| U | This symbol represents all uppercase characters. |
| L | This symbol represents all lowercase characters. |
| N | This symbol represents all numeric characters. |
| P | This symbol represents all punctuation characters (all printable characters that are not alphanumeric; that is, not A–Z, a–z, 0–9). |
| * | This symbol represents any character. |
| ... | The ellipsis symbol represents the division between the prefix and suffix portions of the format statement. |
| Single/Double Quotes | Quotes are used to force literal characters to be qualified as part of the format for example, "a1"). |

The password format uses the ellipsis symbol to represent both a prefix or suffix or both. This provides greater flexibility in defining rules associated with restricting character placement. Table 5 offers a few examples of how password formats can be specified to enforce different criteria.

**Table 5: Password Format Examples**

| Format | What it Means |
|---|---|
| U*N | The password must start with an uppercase character and is followed by any character that is then followed by a numeric character. |
| ...AP | The password must end with an alpha character and is followed by a punctuation character. |
| U...L | The password must start with an uppercase character and end with a lowercase character. |
| "#B8"...X | The password must start with the literal string #B8 and end with an alphanumeric character. |
| U"O'My"...L'ooo"AA' | The password must start with an uppercase character followed by the literal string O'My and must end with a lowercase character followed by the literal string ooo"AA. |

| Format | What it Means |
|---|---|
| "..."P...P | The password must start with the literal string ... followed by a punctuation character. The password must end with a punctuation character. |

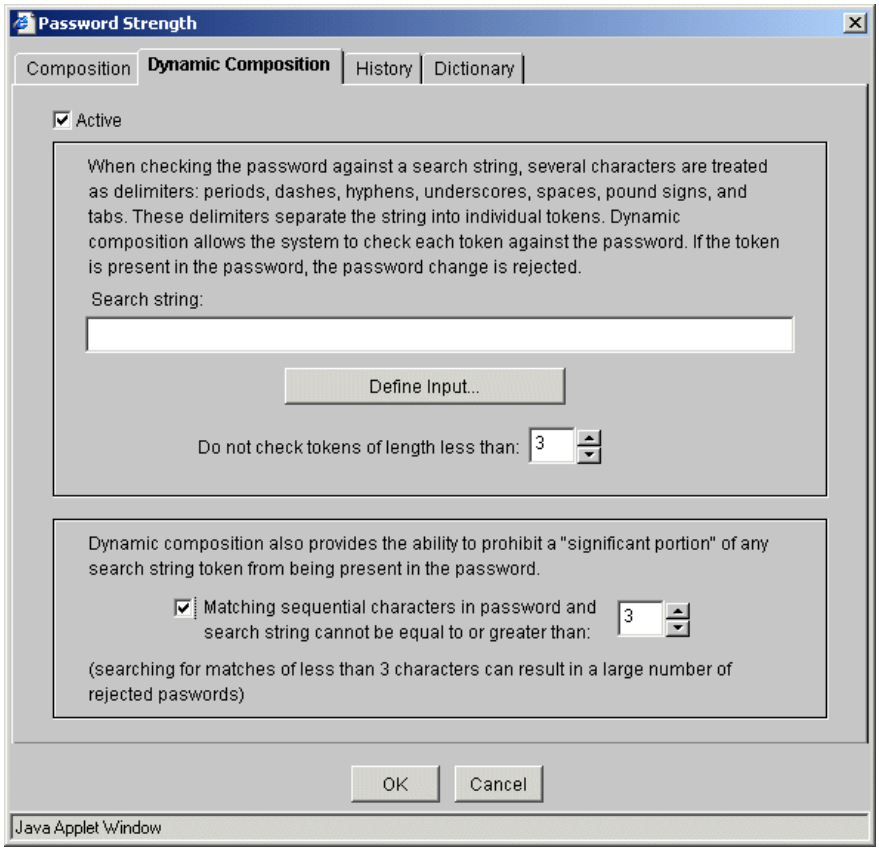
The last two examples in Table 5 demonstrate how password format syntax characters can be used as literal characters. The second to the last example shows how single and double quotes can become literal characters. The last example shows how the ellipsis character can be reinterpreted as three literal periods. With this feature, the entire printable character set can be supported by PasswordCourier.

**Note:** Enclosing characters and/or spaces in quotation marks (“ “) forces the user to include that specific string of characters.

### Dynamic Composition

Dynamic Composition allows you to set a password rule based on information taken form an external source. You can create macros to get information from the external source about the user and not allow that data to be used in the password. For example, you can pull the user's full name from the profile data source and restrict part or all of the user's full name from being in the password.

**Figure 27: Dynamic Composition Tab**




To configure Dynamic Composition:

1. Check the **ACTIVE** checkbox to make the Dynamic Composition feature active. It is not checked by default.

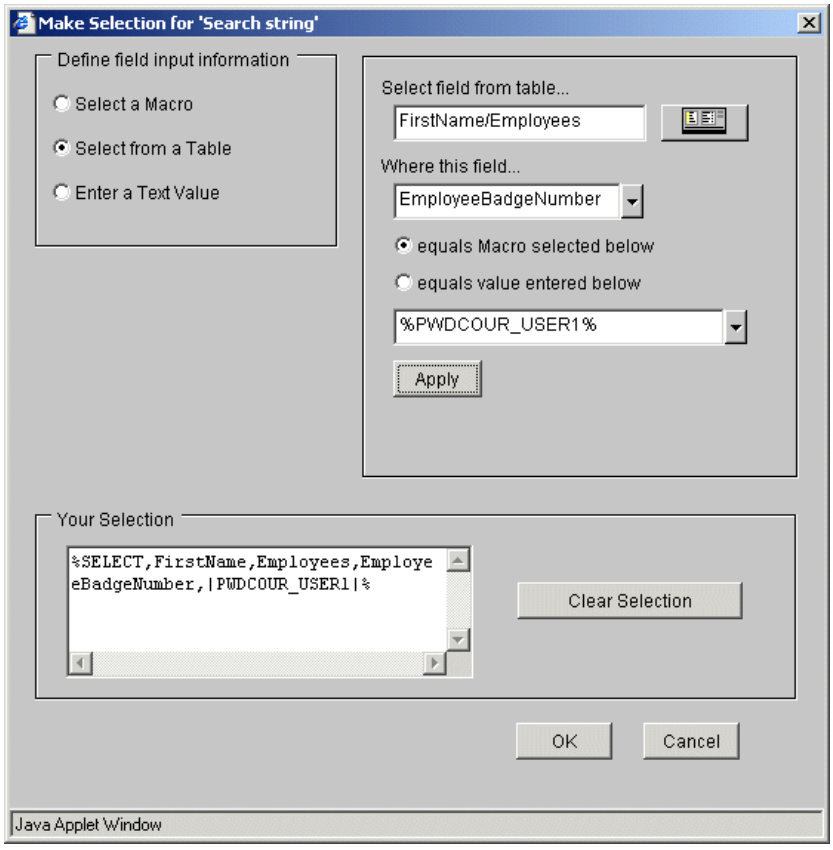
2. **DO NOT CHECK TOKENS OF LENGTH LESS THAN:** The setting in this scroll box determines the minimum length a token must be for it to be used in the requirement search. For example, if this were set to 3 and a macro was used to pull the user's full name, the name "John M. Smith" would be split into three tokens: "John", "M", and "Smith". Because the second token is only one character long, it would be ignored. Therefore, this user could not have a password that included either "John" or "Smith" as a substring anywhere in the password. All of these checks are case-insensitive. This setting will default to 3. That way, it will mimic how Active Directory does a "Full Name" search. The minimum value allowed will be 2 and the maximum will be 99.

3. **MATCHING SEQUENTIAL CHARACTERS IN PASSWORD AND SEARCH STRING CANNOT BE EQUAL TO OR GREATER THAN:** When you select this option, it will pull sequential characters from each token of a length you specify by the number in the scroll box, and search the password. If the substring is found it will reject the password. For example, if this option were enabled and set to 3 and the tokens for a particular entry were "john" and "smith", the password would be searched for the following strings: "joh", "ohn", "smi", "mit", and "ith". This option is disabled by default. If enabled the default setting is 3. The minimum value allowed will be 2 and the maximum is 99.

   Using this option has the potential of significantly slowing down the password strength check process, especially if set to a low number.

4. Click **DEFAULT INPUT** to select a search string. The Make Selection for Search String dialog box appears, as shown in *Figure 28*.

**Figure 28: Make Selection for Search String**



5. Specify the type of input information from the list of options in the **DEFINE FIELD INPUT INFORMATION BOX:** Select a Macro, Select from a Table, or Enter a Text Value. This example shows the Select from a Table option checked.
6. **SELECT FIELD FROM A TABLE** — Specify the table that includes the search string that you will specify.
7. **WHERE THIS FIELD** — Select a field from the table you specified from the drop-down list such as EmployeeBadgeNumber.

   Specify that the field **equals Macro selected below**

   Or

   Specify that the field **equals value entered below**
8. Select a macro or enter text in the drop-down list, then click **APPLY** to copy the selection to the bottom text field labeled Your Selection.

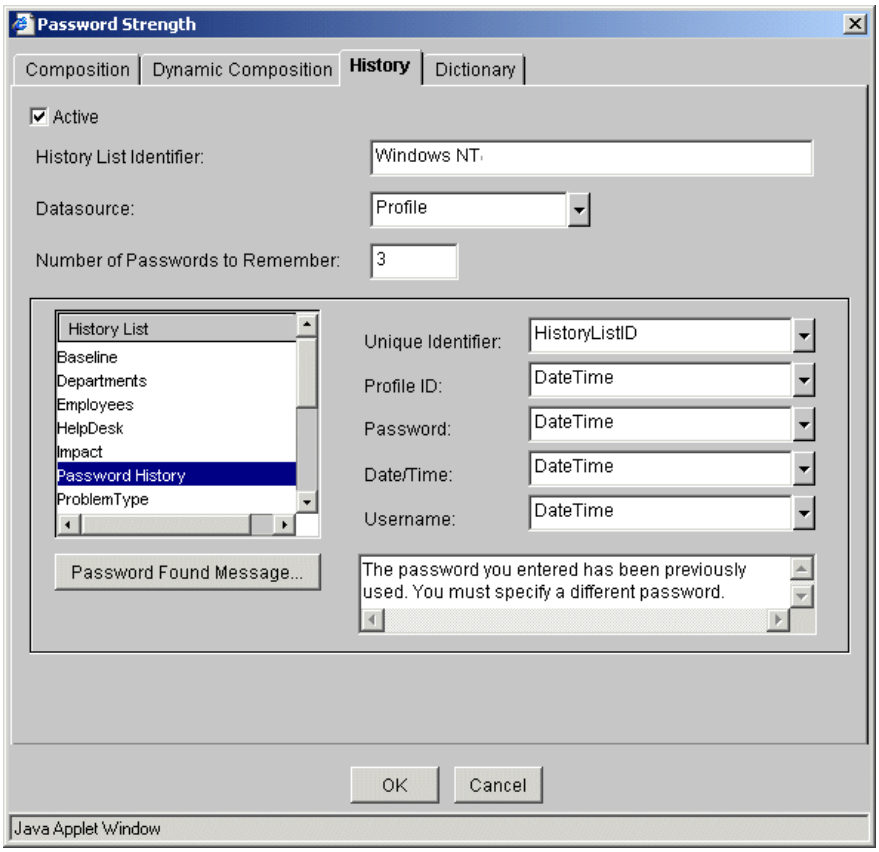
   Your Selection shows the search string you specified. To clear this and enter different information, click Clear Selection.
9. Click OK to accept your selection. You are returned to the Dynamic Composition tab with your selection entered into the **SEARCH STRING** field.

### Password History

To prevent the immediate reuse of passwords, Password History stores passwords that were successfully reset against target systems. Password strength settings, including password history, are validated after the end user enters the new password. If the specified password is found in the history list, a message (customizable by the administrator) is returned to the end user and they must specify a different password. If Password History has been configured for a specific target, a successful password reset against that target results in the new password being saved in the specified history table or file (*Figure 29*).

**Note:** Password History stores the hashed value of passwords, not the passwords themselves.

**Figure 29: Specifying Profile as Password History Data Source**




You can configure Password History so the hashes of passwords used reside in a table in the profile or ticketing data source, or a local file. *Figure 29* shows the Password History tab configured to use the profile data source.

Table 6 describes configurable fields in the Password History configuration tab as shown in Figure 27.

**Note:** For each field on the history definition page, select a column from the drop-down box that is defined as a text type for the data source you selected.

**Table 6: Password History Field Definitions**

| Field | Description |
|---|---|
| Active | This field activates the Password History feature. |
| History List Identifier | This field contains the identifier representing the History List. This identifier is nonexclusive so that multiple targets can share the same History List. |
| Datasource | This field determines where the history for passwords resides (i.e., Profile, Ticketing). If this field is set to “Local File,” the History List Schema is replaced by a text box for the “File that will contain history list.” |
| Number of Passwords to Remember | This field represents the maximum number of passwords to remember for each end user in the target. If the maximum number of passwords is exceeded, the oldest password in the list will be replaced with the new password. If the reserved word "All" is specified, all passwords will be stored. |
| Password Found Message | This field represents the customizable message that is displayed to the end user when a password is found in the History List. This text is populated by means of a macro, a table, or fixed text (see *“Username Selection Query” on page 37*) by clicking on the “Password Found Message...” button. |

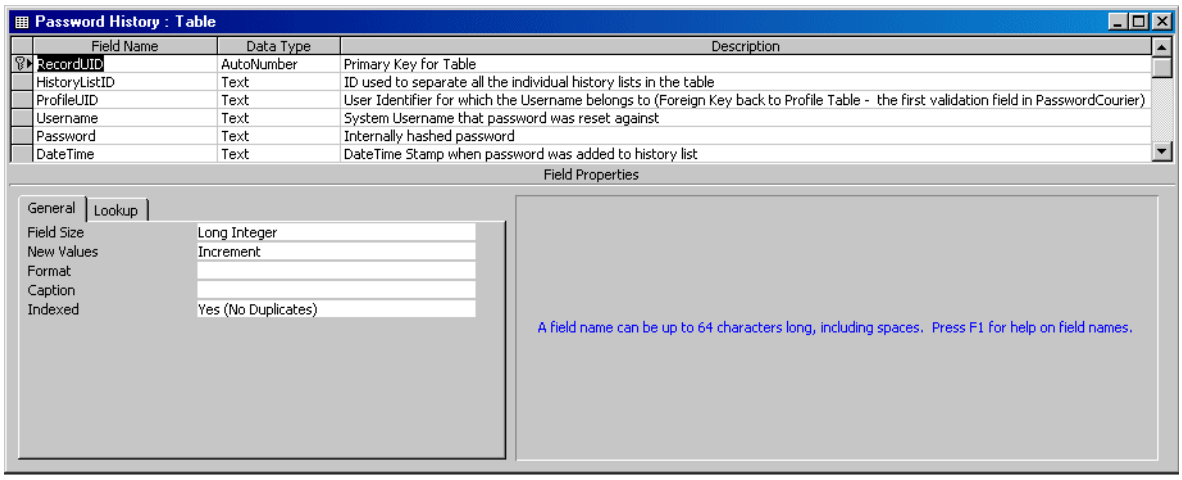
When applying Password History against either the Profile or Ticketing data source, a schema that can be used to house each of the History List items must exist in the Help Desk infrastructure. This schema must include the following fields shown in Table 7:

**Table 7: Password History Schema Definition**

| Field | Comments |
|---|---|
| Record Unique ID | This field represents an auto-incrementing value that uniquely identifies each record in the table. |
| Unique Identifier | This field represents the ID of each entry in the History List. This value may or may not be unique. |
| Profile | This field represents the unique profile identifier of the end user whose password is being reset. |
| Password | This field represents the MD5 hash of the new password that was used to reset an end user account. This field length must be at least 32 characters long. |
| Date/Time | This field represents the date and time the password was entered into the History List. The field is used to expunge old password entries if the maximum size of the History List is reached and a new entry needs to be added. |
| User Name | This field represents the user name that the password is reset against. |

An example of a History List schema is provided in *Figure 30*:

**Figure 30: Sample History List Schema**




**Note:** Password history is not supported for Peregrine® ServiceCenter®, Clarify® eFrontOffice, and LDAP.

**Note:** Password history may be compared against the password history stored on a specific target.

**Note:** All fields in the history schema definition must be text fields. The password field must be able to contain at least 32 characters.

## Password Dictionary Comparison

This feature provides the ability to compare various forms of the password against a standard dictionary and a custom dictionary comprised of words entered by administrators and support staff (*Figure 31*). By applying these types of comparisons, you can protect systems from passwords that are easily guessed through the use of cracker programs, which utilize dictionaries to decipher passwords. If the password fails any of the enforced dictionary comparisons, the end user is informed with a message that explains which checks it failed to pass.

**Note:** The Dictionary and customized dictionary are not target specific. However the actual performance of a dictionary comparison is target-specific based on the configuration. Bulk dictionary customizations can be configured. Please contact customer support at support@coresecurity.com.

**Figure 31: Password Dictionary Configuration Dialog Box**

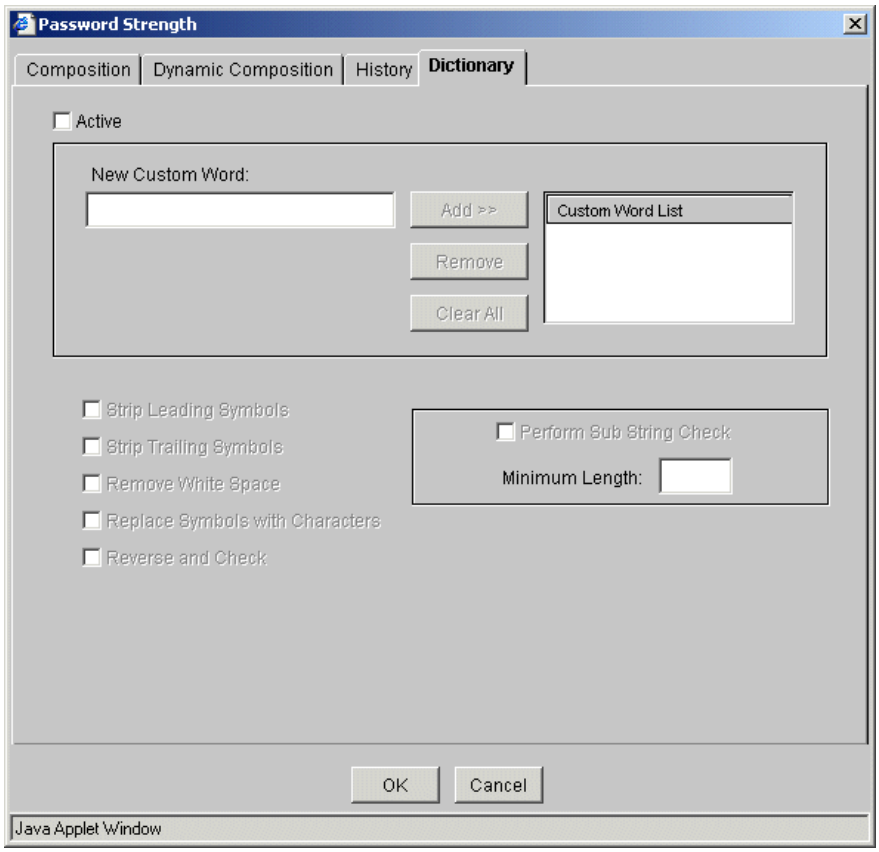



Table 8 describes the fields in the Password Dictionary configuration dialog box. Passwords will be compared against both the standard and the custom dictionaries before being accepted or rejected.

**Table 8: Password Dictionary Configuration**

| Field | Description |
|---|---|
| Active | Activate/deactivate dictionary checks. |
| New Custom Word | A text field to enter the new word into the custom dictionary. |
| Add Button | Adds the entry in the “New Custom Word” field to the custom dictionary. |
| Remove Button | Removes the highlighted entries from the custom dictionary. |
| Clear All Button | Removes all entries from the custom dictionary. |
| Custom Word List | List of words added to the dictionary by administrators and support staff (the custom dictionary). |
| Strip Leading Symbols | Performs a dictionary check after the leading non-alpha characters are removed. |
| Strip Trailing Symbols | Performs a dictionary check after the trailing non-alpha characters are removed. |
| Remove White Space | Performs a dictionary check after all embedded white spaces are removed. |
| Replace Symbols with Characters | Performs a dictionary check after certain symbols are replaced with their character counterpart. The following symbol-character pairs are used during replacement: '$'='s' ; '4'='h' ; '2'='a' ; '3'='e' ; '0'='o' ; '1'='i'. |

**Table 8: Password Dictionary Configuration**

| Field | Description |
|---|---|
| Reverse And Check | Performs a dictionary check after the password is reversed. |
| Perform Substring Check | Performs a dictionary check against each substring of a password until the minimum length allowed is reached. |
| Minimum Length | This field represents the minimum length that a string must be to become eligible for a substring dictionary check. |

PasswordCourier performs configured password checks in the following order:

1. Forward
2. Reverse
3. Forward after stripping leading non-alphanumeric characters
4. Reverse after stripping leading non-alphanumeric characters
5. Forward after stripping trailing non-alphanumeric characters
6. Reverse after stripping trailing non-alphanumeric characters
7. Forward after stripping leading and trailing non-alphanumeric characters
8. Reverse after stripping leading and trailing non-alphanumeric characters
9. Forward after all white space is removed
10. Reverse after all white space is removed
11. Forward after replacing symbols with their character counterparts
12. Reverse after replacing symbols with their character counterparts
13. Forward after stripping leading non-alphanumeric characters and white space is removed
14. Reverse after stripping leading non-alphanumeric characters and white space is removed
15. Forward after stripping trailing non-alphanumeric characters and white space is removed
16. Reverse after stripping trailing non-alphanumeric characters and white space is removed
17. Forward after stripping leading and trailing non-alphanumeric characters and white space is removed
18. Reverse after stripping leading and trailing non-alphanumeric characters and white space is removed
19. Forward after stripping white space and replacing symbols with their character counterparts
20. Reverse after stripping white space and replacing symbols with their character counterparts
21. Forward after stripping leading non-alphanumeric characters and white space and replacing symbols with their character counterparts
22. Reverse after stripping leading non-alphanumeric characters and white space and replacing symbols with their character counterparts

23. Forward after stripping trailing non-alphanumeric characters and whitespace and replacing symbols with their character counterparts
24. Reverse after stripping trailing non-alphanumeric characters and whitespace and replacing symbols with their character counterparts
25. Forward after stripping leading and trailing non-alphanumeric characters and whitespace and replacing symbols with their character counterparts
26. Reverse after stripping leading and trailing non-alphanumeric characters and whitespace and replacing symbols with their character counterparts
27. Forward substring check
28. Reverse substring check

These comparisons all work in collaboration with each other. The total number of comparisons is determined by the total number of different possible combinations of checks. (Mathematically, there are $2^{x-1}$ number of dictionary checks performed per password, where x equals the number of individual checks activated.) The substring check is the only check that doesn't follow this rule. The substring check operates on the password as it was originally specified by the end user.

### *Editing Existing Password Targets*

To edit an existing Password Target, do one of the following:

1. Click the target on the tree structure in the left-hand display area. Note that the **EDIT TARGET** and the **DELETE TARGET** buttons are enabled and the **ADD TARGET** button is disabled. Click the **EDIT TARGET** button and the **EDIT TARGET** dialog is displayed.
2. Click the target in the right-hand Targets Attributes area. Note that the **EDIT TARGET** and the **DELETE TARGET** buttons are enabled and the **ADD TARGET** button is disabled. Click the **EDIT TARGET** button and the **EDIT TARGET** dialog is displayed.
3. Double-click the target in the left-hand display area.

No matter what method you use, the target attributes dialog is displayed with the selected target's attribute settings. Click the **OK** button in the Edit Target dialog to update the target. The right-hand tab is updated to display the updated attribute information for this target. Please refer to *Figure 15* and the *"Password Target Attributes" on page 36* for details regarding that dialog.

### *Deleting Existing Password Targets*

Delete an existing Password Target by one of the following actions:

1. Click the target in the tree structure in the left-hand display area. The **EDIT TARGET** and the **DELETE TARGET** buttons are enabled and the **ADD TARGET** button is disabled. Click the **DELETE TARGET** button.
2. To select the target, click it in the right-hand Targets Attributes area. The **EDIT TARGET** and the **DELETE TARGET** buttons are enabled and the **ADD TARGET** button is disabled. Click the **DELETE TARGET** button. Confirm this deletion by clicking the **YES** button in the confirmation dialog box.

3. When the **DELETE TARGET** button is clicked, a check is done to see if the target belongs to a Password Target Group (see *"Password Target Groups Tab" on page 65* for details). It is necessary to confirm the deletion of the selected target if it belongs to a Password Target Group by clicking the **YES** button in the dialog box that appears.

If the deletion is confirmed, then the target is deleted from this tab as well as from any group where it was a member. Once the deletion is confirmed, the target is removed from the list under the PMM folder as well as from the right-hand target attributes tab.

### *Copying Existing Password Targets*

To copy an existing Password Target:

1. Select the target to copy.
2. Click the **EDIT TARGET** button that displays the Edit Target dialog.
3. Click the **CANCEL** button in the Edit Target dialog.
4. Select the PMM for which the target is to be added.
5. Click the **ADD TARGET** button.

When the **ADD TARGET** dialog appears, the attribute information for the target to be copied should be visible. Fill in the target name/alias name information, make any changes desired, and click the **OK** button to save this new target.

### *Password Targets Used by Support Staff*

If there are no end user accounts in the database, PasswordCourier Support Staff Password Targets can include the `%PWDSS_USERACCT%` macro in the Username Selection Query attribute. This macro contains the end user account information that is entered in PasswordCourier Support Staff after the Password Target is selected.

When the `%PWDSS_USERACCT%` macro is present in the Username Selection Query, the support staff user is prompted for the name of the account for which to reset the password. This value can then be used to compose the complete username. When the `%PWDSS_USERACCT%` macro is not present, the complete username must be composed of data selected from the profile table, macro values, and text that you can enter.

If the end users' accounts in the database are available, configure PasswordCourier Support Staff Password Targets to select the end user account information from the database.

If a PasswordCourier Support Staff Password Target is created with the Username Selection Query attribute containing the `%PWDSS_USERACCT%` macro, PasswordCourier Support Staff displays the field for the support staff to use. The field for the end user's account is not displayed in PasswordCourier Support Staff. The absence of this macro in the Username Selection Query attribute of the target indicates that no input from PasswordCourier Support Staff is needed to determine which end user account to attempt a password reset on.

## *User-Based Targets*

User-Based Targets displays only those groups and targets for which the end user has valid accounts. User-Based Targets utilize a separate table to represent end user accounts for each target. This feature overrides the *"Username Selection Query" on page 37*. Instead of looking into the end user's profile to find the user name for a specific target, a separate schema/table is accessed to obtain the information. This provides more flexibility, since multiple accounts per target (rather than just a single account) can be reset. It also provides a mechanism for selecting and displaying the targets and groups the end user has actual accounts on rather than displaying all targets and groups established in the system.

To configure User-Based Targets, create a schema/table to hold the appropriate information. This table must include a field for the record unique identifier, the target, the username, and the profile datasource.

### Schema Setup in Data Source

A new schema/table needs to be introduced into the data source that houses the User-Based Targets. This schema must meet minimum format and size specifications. You specify the name of the individual schema and fields and may add additional fields to the table.

**Note:** User-Based Targets do not support LDAP data sources, Peregrine® ServiceCenter®, Peregrine Archway, and Clarify®. Use the flat file implementation to support history under such conditions.

### User-Based Target Schema

The schema contains information that links end users to their specific account names for each target in the system. Data is organized in hierarchical form to represent the end users in the system:

There are five individual pieces of information that are needed in the User-Based Targets Schema (Table 9), next.

**Table 9: Schema Field Descriptions**

| Field Name | Data Type | Range | Definition |
|---|---|---|---|
| Rec UID | Numeric | Any | The primary key for the User-Based Target schema |
| Target ID | String | Maximum of 256 Characters | The unique identifier that is associated with each individual target in the Core Server. The data type for this field should allow for string character representation. Target IDs are assigned to actual targets within the Administrator applets on the target attributes dialog.<br>**Note:** Do not use commas or the equal sign in this field or the Target ID will not display properly. |

**Table 9: Schema Field Descriptions**

| Field Name | Data Type | Range | Definition |
|---|---|---|---|
| User Name | String | This string requires a maximum of 256 characters. It also depends on the maximum number of characters allowed for a user name by the target in the system. | The user name established for a particular end user on the specified target. The data type for this field should allow for string character representation. |
| Profile UID | String | Maximum of 256 characters | The end user's unique identifier in the profile schema. The unique identifier is usually a badge number or something similar. This information must be the same as the first piece of information provided during the authentication phase of a password reset. The data type for this field should allow for string character representation. The field acts as a foreign key to the individual end user's profile record. |
| Profile Data Source | String | Profile | Further define the ProfileUID field. In systems where multiple authentication models are followed the ProfileUID is not always unique. This field provides a way of determining which data source corresponds to the contents of the ProfileUID field. When setting the data type in this field, allow for string character representation. **Note:** The User-Based Targets do not utilize this field because the Core Server does not, at this time, support multiple authentication models. |

Because they may adversely affect the operation of User-Based Targets, the following characters should be avoided:

- ; (semicolon)
- & (ampersand)
- , (comma)
- _-_ (space dash space)

This information is used to create a User-Based Targets table (*Figure 32*).

**Figure 32: User-Based Targets Table**

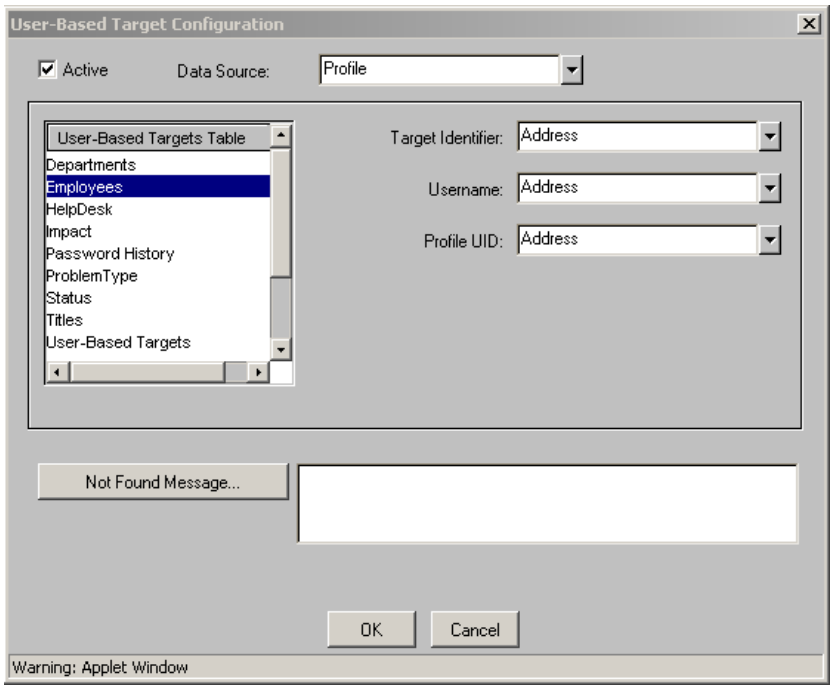
User-Based Targets : Table

| Record UID | TargetID | User name | Profile UID | Profile Data Source | UBT notes |
|---|---|---|---|---|---|
| 1 | Your.dom | ccourion | 5000 | future | one of two NT user names for uid 5000 o |
| 2 | Your.dom | ccourion1 | 5000 | future | two of two NT user names for uid 5000 o |
| 3 | Your.dom | ccourier | 6000 | future | one of two NT user names for uid 6000 o |
| 4 | Your.dom | ccourier2 | 6000 | future | two of two NT user names for uid 6000 o |
| 5 | Your Unix Machine | ccourion_unix1 | 5000 | future | one of two UNIX user names for uid 5000 |
| 6 | Your Unix Machine | ccourion_unix2 | 5000 | future | two of two UNIX user names for uid 5000 |
| 7 | Your Unix Machine | ccourier_unix1 | 6000 | future | one of two UNIX user names for uid 5000 |
| 8 | Your Unix Machine | ccourier_unix2 | 6000 | future | two of two UNIX user names for uid 5000 |
| 9 | Your OS390 | ccourion_os390 | 5000 | future | one OS/390 user name for uid 5000 on ta |

Record: 11 of 11

Click the **USER-BASED TARGETS** button to access the User-Based Target Configuration dialog box (*Figure 33*). The button is located on the bottom right corner of the Password Management Module Targets tab.

**Figure 33: User-Based Targets Configuration Dialog Box**




The word **ACTIVE** appears in red next to the button on the Management Modules/Targets tab when the Active check box is checked. When this active flag appears, the **USER-BASED TARGETS** button replaces the **USERNAME SELECTION QUERY** button found at the bottom of the Target Attributes dialog box (which appears when adding or editing a target from the Management Module Targets tab).

The User-Based Targets Configuration dialog is broken down into three sections: The General Parameters, the Actual Target Schema/Table Parameters, and the Message Definition Parameters (Table 10 and Table 11).

### General Configuration Parameters

**Table 10: General Configuration Parameters**

| | |
|---|---|
| Active Flag | When the Active Flag is checked, the User-Based Targets feature is activated and overrides the *"Username Selection Query" on page 37* found on the target attributes dialog. |
| Data Source | This identifies the data source to query for User-Based Targets. Generally it is the Profile Data Source that stores the end user's profile record. |

### Actual Target Schema/Table Parameters

**Table 11: Target Schema/Table Parameters**

| | |
|---|---|
| Data Source | Determines whether this information will be stored in the profile or ticketing datasource configured during the installation of this product. |
| Target Schema/Table | Shows a list of all tables available in the selected data source (as determined during the configuration of the Core Server). Selection from list identifies which table contains the mapping of targets to end user names (User-Based Targets table). |
| Target Identifier | Allows the selection of the field in the User-Based Targets table that contains the identifier for the target system. The contents of this field indicate the target ID assigned to each of the targets in the PasswordCourier and PasswordCourier Support Staff Customization Managers. |
| User Name | Allows the selection of the field in the target table that represents the user name for a specific target. The contents of this field correspond to an actual user name on the target that this record represents. |
| Profile UID | Allows the selection of the field in the target table that represents the information that uniquely identifies the end user. The contents of this field refer to a foreign key in the end user's profile record. **Note:** This information must be the same as the first piece of validation information that the end user is prompted to enter during a password reset. |

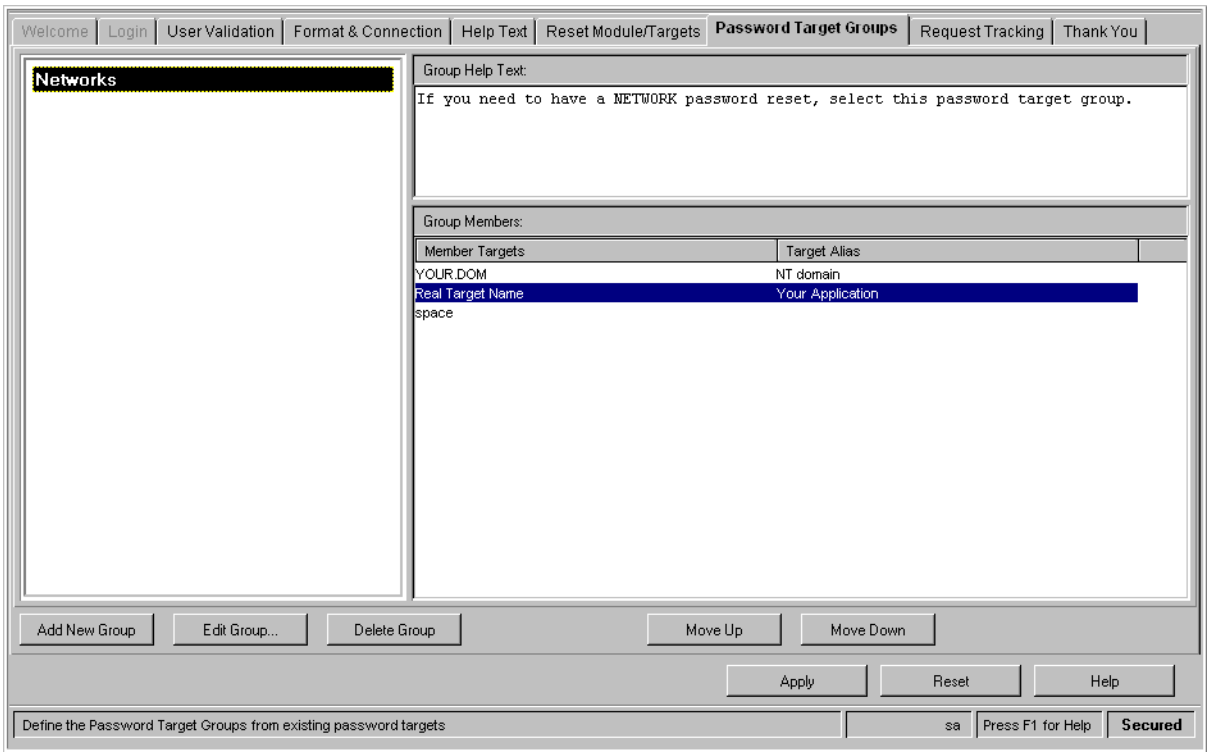
### Message Definition Parameters

This section allows you to define the message that is displayed when the user attempts to reset a password on a target for which they have no valid account.

## Password Target Groups Tab

Password Target Groups tab enable easy and logical groupings or associations of the possible destinations for all of the end users' password resets (*Figure 34*). Simply create target groups and then assign defined targets to the appropriate group(s).

**Figure 34: Password Target Group Tab**




The layout of this tab is separated into three major sections:

- The left-hand side of the tab contains a list of defined groups.
- The top right-hand side of the tab contains the help text for the selected group. This help text is displayed in PasswordCourier when the end user presses the F1 key while the cursor is in the Target Group field.
- The bottom right-hand side of the tab contains a list of the selected group's member targets. This list of members is displayed in PasswordCourier in the Targets box and reflects the data on the selected group. If an alias is defined, it is displayed. If an alias is not defined, the target name is displayed. Targets not assigned to any group are never displayed in PasswordCourier.

The Password Target Groups tab updates to reflect any changes resulting from adding, modifying, or deleting target group(s). Click the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous value.

The **MOVE UP** button moves the highlighted entry further up the list. The **MOVE DOWN** button moves the highlighted entry further down the list. These buttons dictate the way targets and groups are ordered and displayed to the end user. The ordering is only enforced when User-Based Targets is not active. When User-Based Targets is active, the ordering is in ascending order and overrides any ordering placed on the groups and targets through the use of these buttons.

### *Password Target Group Definition Rules*

The following are rules for target group definition:

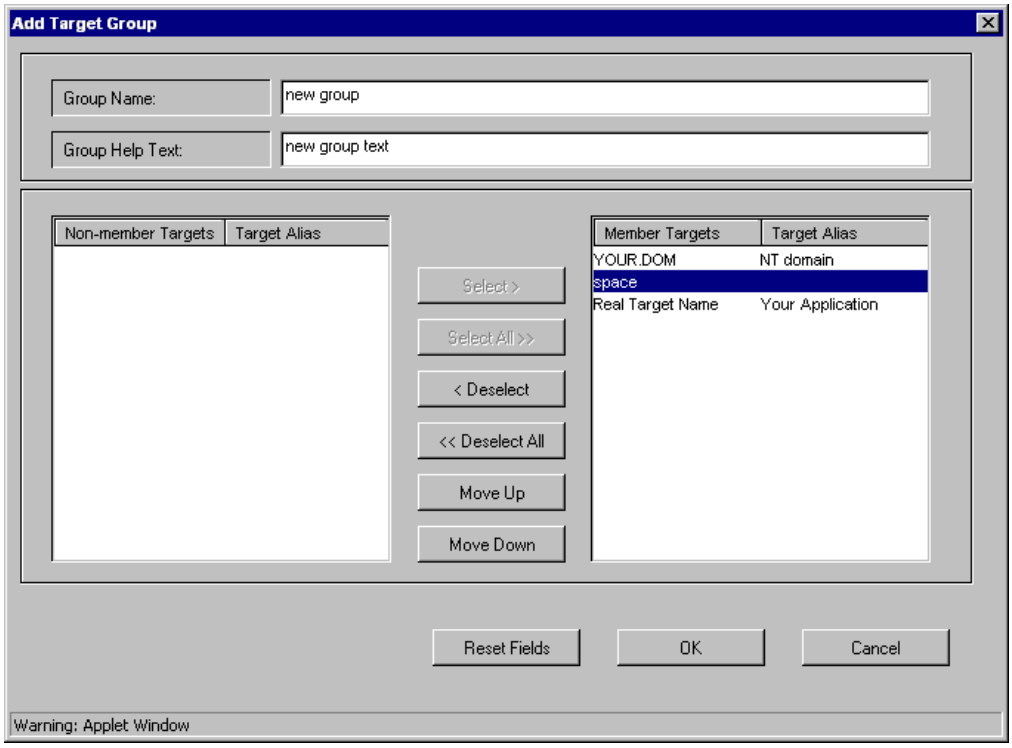
- At least one group must be defined with at least one target as a member.

- A group cannot contain two targets with the same alias since only the alias name is displayed in PasswordCourier.

### *Adding a Password Target Group*

To add a new Password Target Group, click the **ADD NEW GROUP** button. The Add Target Group dialog box appears (*Figure 35*).

**Figure 35: Adding a New Password Target Group**




When the dialog is completed, click the **OK** button in the Add Target Group dialog to create the target group; the Password Target Group tab updates to display the new group. The right hand top and bottom areas of the tab display the information for this new target group.

### Target Group Dialog

Table 12 describes the fields in the Target Group dialog box used to add a new group or edit and existing one.

**Table 12: Target Group Dialog Fields**

| Field Name | Description |
|---|---|
| Group Name | This is the name of the target group. It is displayed in the PasswordCourier Groups list. The characters \| , % ^ = + are not allowed. |
| Group Help Text | This is the help text for the group. It is displayed in PasswordCourier when the end user presses the F1 key while in the group list for the selected group. |
| Non-member Target List Box | This is a list of all defined targets, and their aliases, that are not members of the group. |
| Member List Box | This is a list of all defined targets, and their aliases, that are members of the group. |
| Select Button | This button is only enabled when a target in the Nonmember Target list box is selected. Clicking on this button removes the selected target from the Nonmember list box and moves it to the Member list box. |
| Select All Button | This button is always enabled. Clicking on this button removes all of the targets from the Nonmember list box and moves them to the Member list box. |
| Deselect Button | This button is only enabled when a target in the Member Target list box is selected. Clicking on this button removes the selected target from the Member list box and moves it to the Nonmember list box. |
| Deselect All Button | This button is always enabled. Clicking on this button removes all of the targets from the Member list box and moves them to the Nonmember list box. |
| Move Up Button | This button moves a target higher on the list displayed to the end user. |
| Move Down Button | This button moves a target lower on the list displayed to the end user. |
| Reset Fields Button | This button sets all of the fields back to their original values. |
| OK Button | This button saves changes for a new target group or modified target group and exit from the Target Group dialog. The changes are also reflected in the right-hand side of the Password Target Groups tab. |
| Cancel Button | This button exits the Target Group dialog without saving any additions/ changes. |

### *Editing and Deleting a Password Target Group*

Edit an existing Password Target Group by selecting the group (click it in the left hand area of the Password Target Groups tab). Click the **EDIT GROUP** button and the Target Group dialog is displayed with the current information. Click **OK** to save the changes. The changes are updated in the tab.

Delete an existing Password Target Group by selecting the group (click it in the left hand area of the tab). Click the **DELETE GROUP** button. A confirmation message box is displayed. If the deletion is confirmed, the group is removed from the list of defined groups from the tab.

**Note:** Deleting a Password Target Group deletes the group but not the targets contained in that group.

### *Copying a Password Target Group*

To copy an existing Password Target Group:

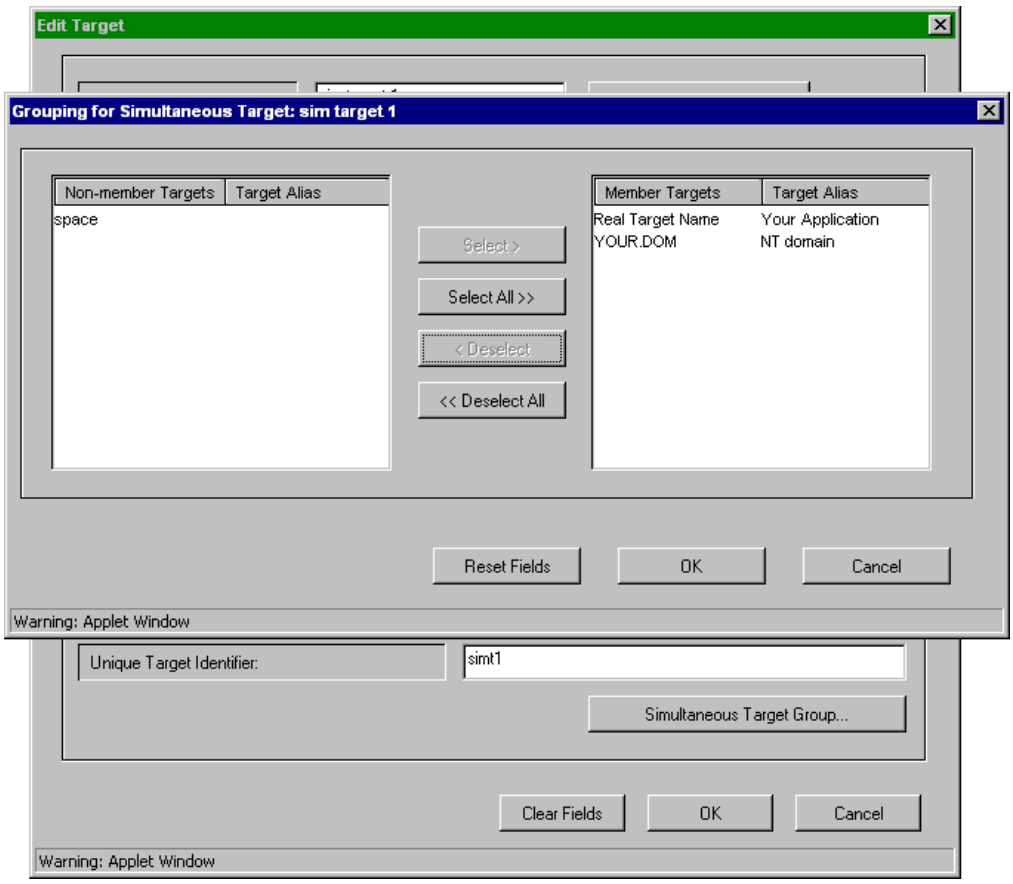
1. Select the target group to be copied.
2. Click the **EDIT GROUP** button, which displays the Edit Target Group dialog.
3. Click the **CANCEL** button in the Edit Target Group dialog.
4. Click the **ADD NEW GROUP** button.

The information for the target group to be copied becomes visible when the Add Target Group dialog is displayed. Fill in the group name, make any changes, and click **OK** to save this new target group.

### *Synchronization Target Configuration when User-Based Targets is Enabled*

Synchronized targets are targets that may all be set to the same password in a single password reset request. To reach this screen, you must configure the PMM for Synchronization. Click the Synchronization Resets folder and click the **ADD TARGET** button to display the **ADD TARGET** dialog box (Figure 15 - *"Add Target Dialog Box" on page 35*) and complete the configuration as described in *"Password Target Attributes" on page 36*. Configure in the same manner as described previously (see *"Synchronization Target Configuration" on page 44*), except the **USERNAME SELECTION...** button is replaced with the **SYNCHRONIZATION TARGET MEMBERS...** button. Click this button to bring up the Members of Synchronization Target screen (*Figure 36*). In this screen, you can configure each Synchronization Target to represent a group of actual targets.

**Figure 36: Members of Synchronization Target Screen**




This representation is used in determining which targets and user names are eligible to be reset. The Synchronization Target is eligible for password reset under the following conditions:

1. The end user has a valid user name on each of the targets represented by the Synchronization Target.
2. The end user has at least one user name on at least one target in the Synchronization Target Group and the **ALLOW NULL ACCOUNTS** flag is activated through the PMM for Synchronization Configuration Manager.

### Add the Records to the Schema

This is where end user names are added to the User-Based Target schema. Refer to the *"User-Based Targets" on page 62* section for information about the values to enter into this schema. Any front-end tool that normally interfaces with the data source can be used to enter this information.

### Migration

For systems that have user names established inside of each profile record, the user name will need to be pulled from the profile record and used to populate the User-Based Target schema. You can delete the user name field from the profile record after the migration is complete.

**Note:** deleting the user name field from the profile record will cause this mechanism for retrieving user names from the profile to fail if you turn off the User-Based Target feature.

Originally, the data for Synchronization reset targets was in a triplet format, delineated by semicolons. It is up to you to parse through the triplet and pull out each component for placement into the new schema. For example, each piece of the triplet can be broken out into the following:

piece 1 ; piece 2 ; piece 3 ; piece 1 ; piece 2 ; ...

1. The first piece is the PMM type.
2. The second piece is the Target Name.
3. The third piece is the user name. This will be associated with the Target ID in the User-Based Target schema.

**Note:** Synchronization Targets only appear to the end user during a password reset on the following conditions:

- All of the actual targets grouped by the Synchronization Target have valid accounts for the specific end user.
- At least one of the actual targets within the Synchronization Target has a valid account for the specific end user and the **ALLOW NULL ACCOUNTS** flag is set in the configuration of the PMM for Synchronization.

## Request Tracking Tab

You can configure PasswordCourier and PasswordCourier Support Staff to track Password Reset Requests and other activities from the Request Tracking tab (*Figure 37*). The actions that can have auditing actions configured to occur are:

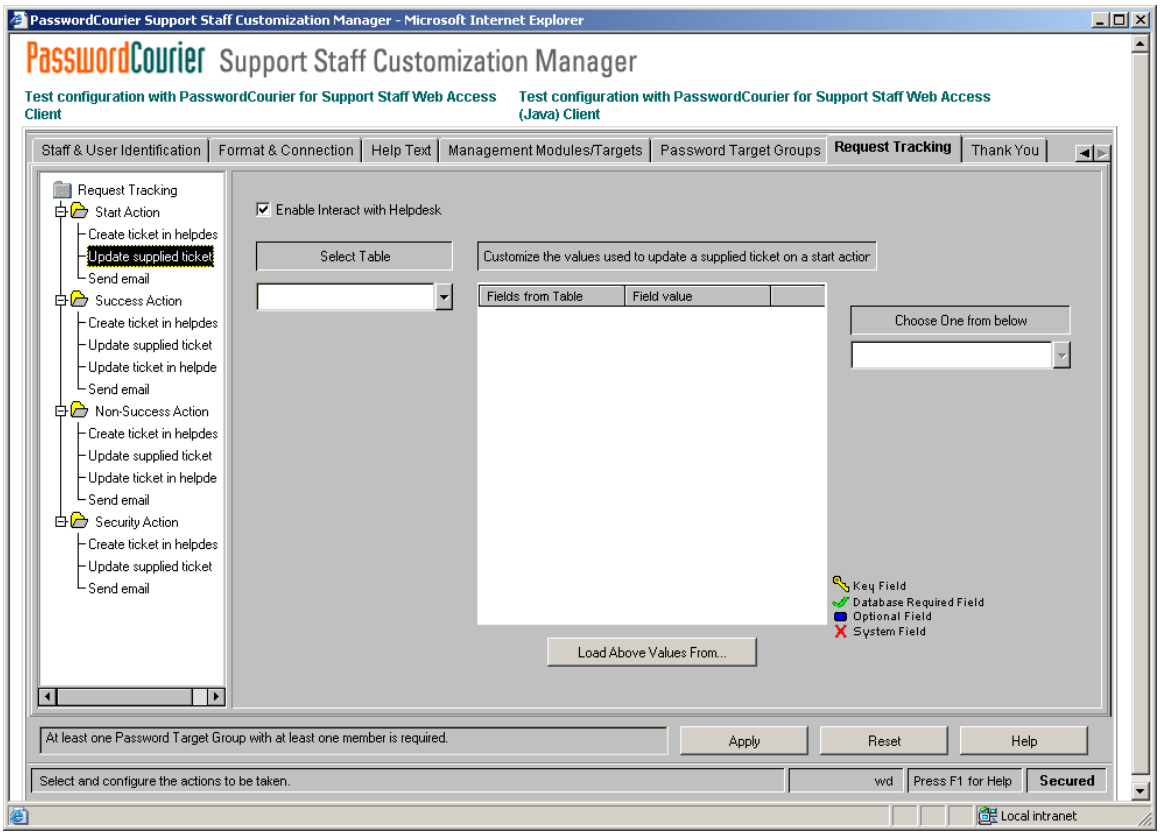
- **Start Action** — a validated and authenticated end user initiates a password reset request and selects the group and target.
- **Success Action** — a successful password reset request is performed.
- **Nonsuccess Action** — a non successful password reset request occurs or the session times out.
- **Security Action** — an end user exceeds the configured number of tries to validate or authenticate himself or herself.

The auditing actions that can be configured to occur are:

- Create a ticket
- Update a ticket
- Send an e-mail

Create Ticket, Update Ticket on Success, Update Ticket on Nonsuccess, and Create Security Ticket frames are organized to support e-mail generation for tracking the password reset requests.

**Figure 37: Request Tracking Tab**




You can also configure PasswordCourier and PasswordCourier Support Staff to create tickets on a nonsuccess password reset request. However, for each password reset request, only one ticket is created during any one use of PasswordCourier or PasswordCourier Support Staff.

You can configure PasswordCourier and PasswordCourier Support Staff to create tickets in the Help Desk system in the following situations:

- Exceeding the configured number of end user/staff validation attempts or end user authentication attempts
- Initiation of Password Reset Request after end user validation, end user authentication, and selection of Password Group and Password Target
- Successful Password Reset Request
- Non successful Password Reset Request

If you configure PasswordCourier or PasswordCourier Support Staff to create tickets upon initiation of a password reset request, then they can also be configured to update the ticket upon a successful password reset request and/or upon a non successful password reset request.

**Note:** When using PasswordCourier Support Staff with Peregrine ServiceCenter, PasswordCourier Support Staff users can also update tickets originating in ServiceCenter by specifying the ticket ID in a query string in their browser's Address field. For more information on this feature, see the chapter on web access in *Installing the Access Assurance Suite.*

If the Help Desk system supports ticket generation via an e-mail message, PasswordCourier and PasswordCourier Support Staff can be configured to send an e-mail to create the ticket in the Help Desk system.

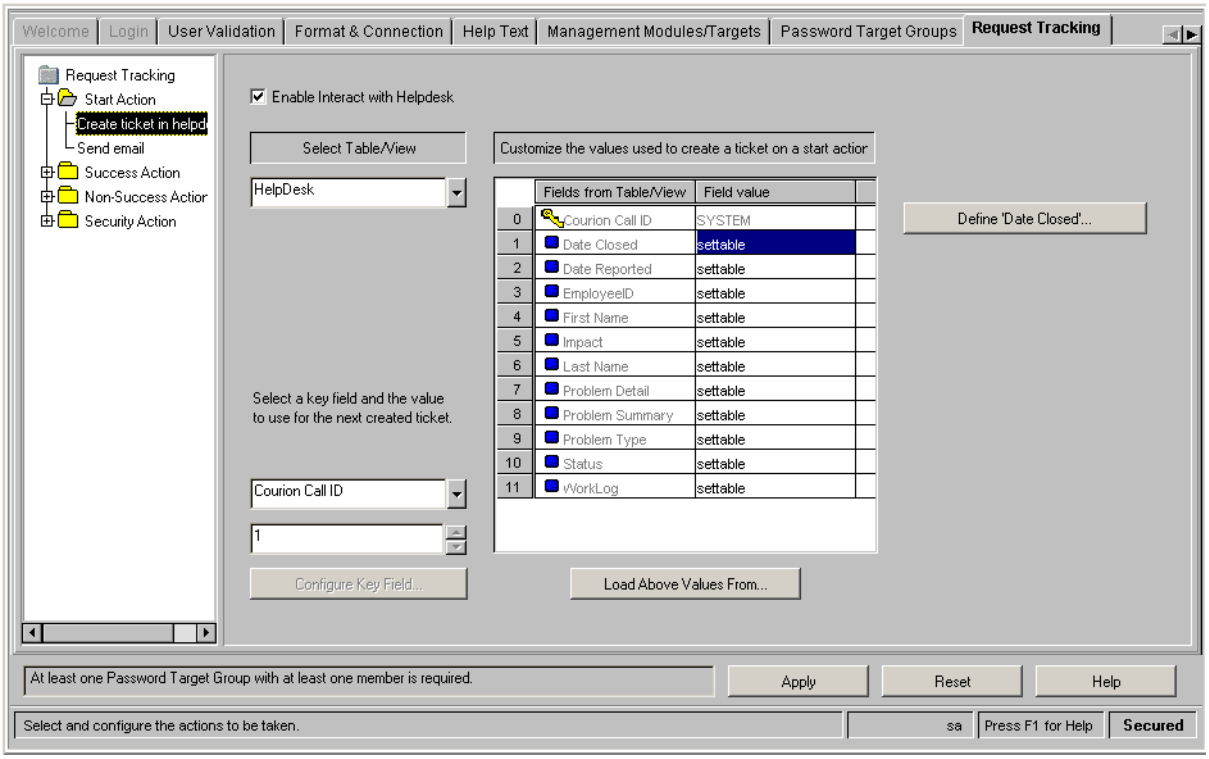
## *Start Action*

The definition of a Start Action varies depending upon the configuration of PasswordCourier or PasswordCourier Support Staff. Generally, the Start Action occurs when the end user selects a password target. In the Start Action screen, configure PasswordCourier and PasswordCourier Support Staff to create a ticket in the Help Desk system.

### Create Ticket in Help Desk on Start Action

In the PasswordCourier Customization Manager, you can configure PasswordCourier or PasswordCourier Support Staff to create a Help Desk ticket when a Start Action takes place (*Figure 38*).

**Figure 38: Create Ticket in Help Desk Screen**




You can set the contents of the ticket fields by entering any combination of macros containing information gathered by PasswordCourier, with information held in a database, or with text. PasswordCourier enters the defined information after the end user has been successfully validated and has chosen the target to reset.

1. From the **SELECT TABLE/VIEW** drop-down list on the left side of the Create Ticket frame, choose the Help Desk database table where PasswordCourier is to enter information.

   This list of tables is created dynamically, and updates in the database structure are reflected whenever the PasswordCourier Customization Manager is started.

**Note:** To view all the items in the drop-down list, click and drag the mouse to the end of the list. To select an item from the list that appears at the bottom, type the name in the ticket field.

### Ticket Table Key Field

If you configure PasswordCourier to use ODBC as the ticketing data source, then you need to select a ticket id key field after choosing the table. Select the ticket id key field from the drop-down menu located below the **SELECT TABLE/VIEW** drop-down menu in the lower left corner of the Create Ticket screen. In the case of LDAP, this field and its value are used as the relative distinguished name (rdn) of the new directory entry.

**Note:** If AccountCourier is also being used, PasswordCourier and AccountCourier must ticket to separate fields.

**Note:** Please see the appropriate Help Desk integration section in *Installing the Access Assurance Suite* for additional information on Ticket Table Key Field configuration.

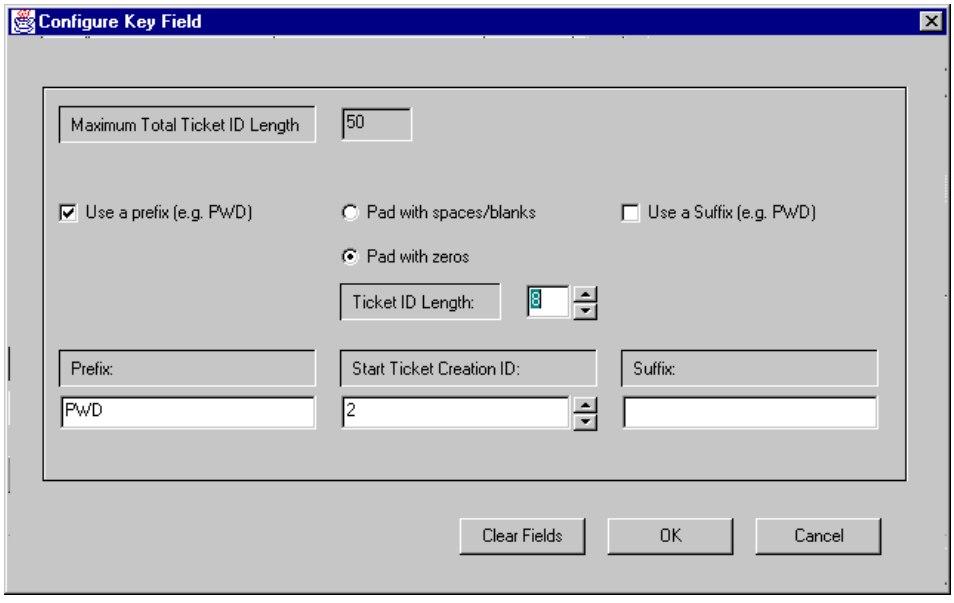
For ODBC installations, the starting ticket number must be specified in the field below the **TICKET ID KEY FIELD** field. If the selected key field is numeric, then a number selection field is presented below the field selection control. The field is initialized with the next sequential record identifier in the table. To modify the starting number to create ticket records, change the integer value by either typing directly in the field or by clicking on the up and down buttons on the right to increment/decrement the number.

If the ticketing source is unreachable, PasswordCourier logs the failed ticket to a comma separated variable file called failed_ticket.csv and performs the password reset or profile action. (**Note:** This functionality is not available for ODBC data sources).

**Note:** The **CONFIGURE KEY FIELD** button is disabled since, with the exception of the starting number, numeric fields are not configurable for these Help Desk applications.

If the selected key field is text, this field may be customized to conform to the requirements for a company's ODBC Help Desk. Click the now enabled **CONFIGURE THE KEY FIELD** button and the Configure Key Field dialog box appears (*Figure 39*).

**Figure 39: Configure Key Field Screen Dialog Box**



This dialog allows the customization of the ticket ID so that it conforms to any requirements the ODBC Help Desk may have. For example, some Help Desks have a ticket ID that is 10 characters long and right justified (e.g. 0000000001 rather than 1). Even if a Help Desk has no special requirements, you can customize this to easily identify PasswordCourier created tickets. This can prevent collision with other sources that may create tickets outside of PasswordCourier.

For example, if the PasswordCourier configuration is limited to specifying that “Start Ticket” begins creation at ID number 2, another support staff user may use the Help Desk directly and create the next ticket as 3. Since PasswordCourier has no knowledge of tickets created by other sources, it attempts to create the next ticket as 3 and fails. To avoid this, use a prefix and/or a suffix that makes PasswordCourier ticket IDs unique.

For example, in *Figure 39* - Configure Key Field dialog box, a prefix of PWD is used with zeros as padding. This means that the first ticket PasswordCourier creates is PWD00000002. This is because the prefix specified is PWD, the length of the ID is 8, and the padding is zeros. The end result is a ticket ID starting with PWD plus 7 zeros for padding and then the start of the ticket id that was configured to be 2. Subsequent tickets also begin with PWD and increment from 2. A suffix may also be used so that all PasswordCourier created ticket IDs end with the same text. Spaces may be also used as padding. The length of the ticket ID along with the prefix and suffix cannot exceed the Maximum Total Ticket ID length displayed at the top left hand corner. Click the **CLEAR FIELDS** button to clear all fields.

### Customizing Ticket Table Fields

The table located in the center of the Create Ticket in Start Action frame displays the fields located in the selected ticket table. The middle row of icons and field definitions that indicate which fields are optional (“settable”), which are required (“required - must be set”), or predetermined. PasswordCourier uses these field definitions to enter information into the Help Desk database during ticket creation(Table 13).

**Table 13: Ticket Table Fields**

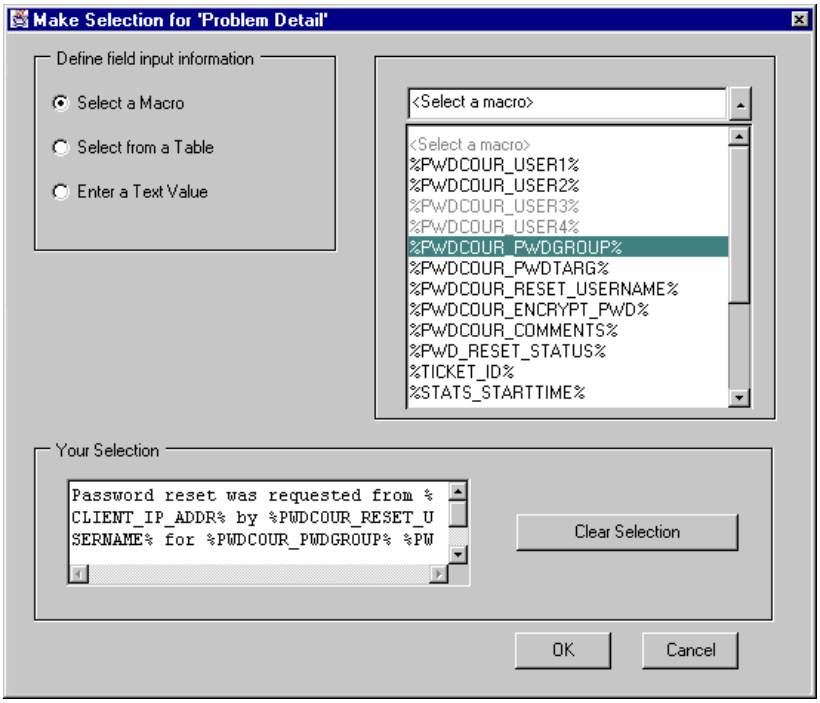
| | | |
|---|---|---|
| | System field | The Help Desk system enters information into these fields. They are not configurable through PasswordCourier |
| | Required fields | These fields must be configured in PasswordCourier in order to enter information into these fields. |
| | Optional fields | These fields may be configured in PasswordCourier in order to enter information into these fields. |
| | Optional field that is is not changeable for this action. | This field is displayed only. |
| | Key | These fields are used as the key for the database table. |

To configure PasswordCourier to enter information into a field, click the row number with the mouse to highlight the field in the entry box in the **CUSTOMIZE THE VALUES FOR SPECIFIC FIELDS USED TO CREATE A TICKET** field (*Figure 38*). The PasswordCourier Customization Manager applies the field constraints to the selected entry to ensure that PasswordCourier is not configured to enter invalid information into the

Help Desk system (for example, entering alphabetic character data into a numeric field). If the selected field has a specific set of entries from which to choose from a drop down box of valid entries is provided from which to select.

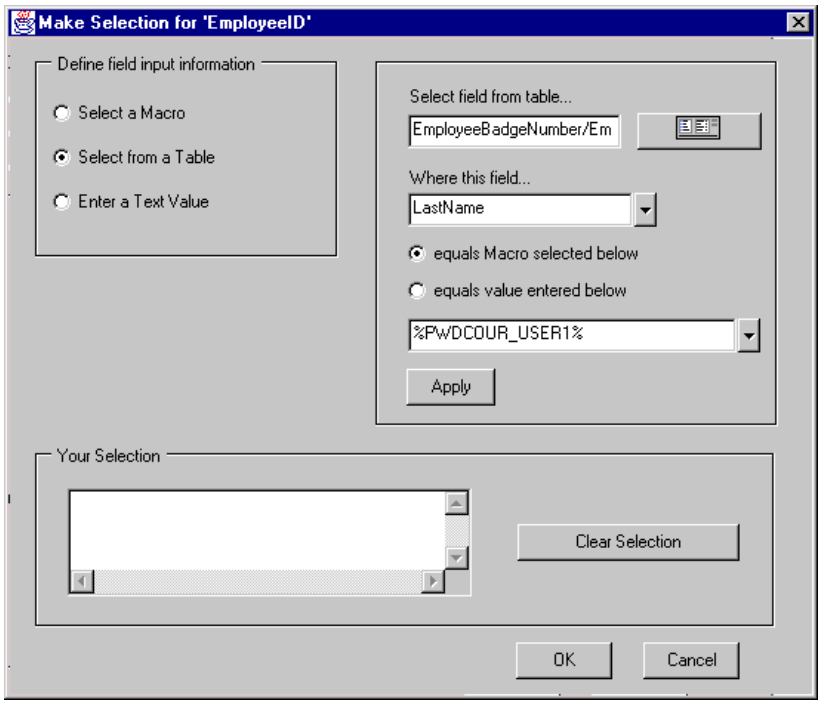
In fields without specific value constraints, it is possible to select macro information gathered by PasswordCourier, specify information from another field in the Help Desk database, enter text, or any combination of these sets of data. If the selected field has already been defined and is again selected to be modified, the current value is displayed in the field under the **DEFINE INPUT** button. Click the **DEFINE INPUT** button. If the current value is present, it is displayed in the bottom text field of the Make Selection for WorkLog dialog box that pops up (*Figure 40*). This dialog box resembles the one in *"Format & Connection Tab" on page 26*.

**Figure 40: Entering Macro Information into a Trouble Ticket Field**



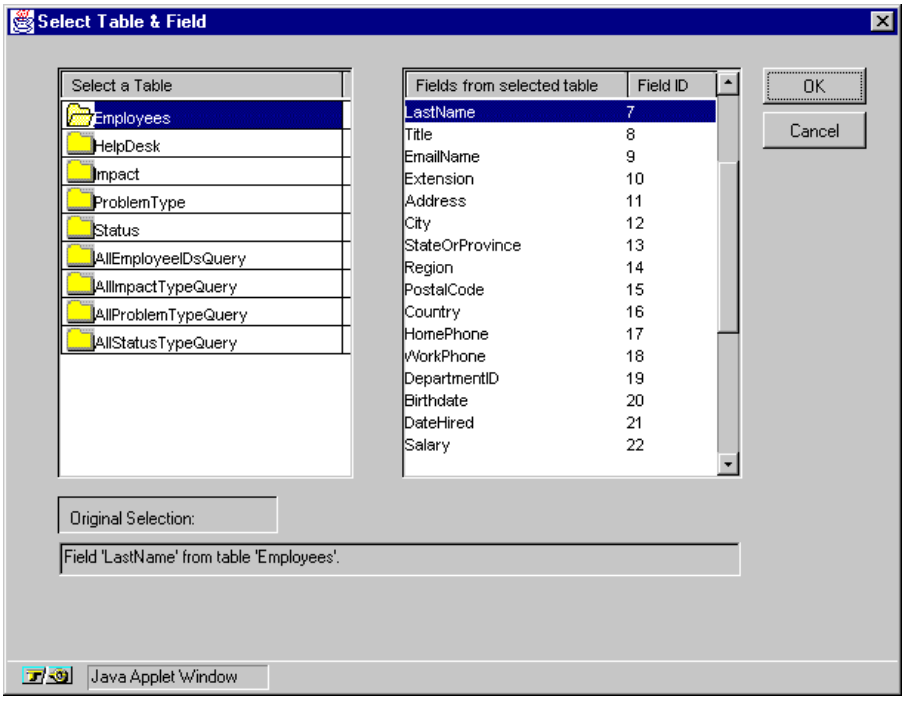

1. Select a macro, information from another field in the Help Desk database or enter text. This selection is added to the bottom text field when the **APPLY** button is clicked. To clear the bottom text field, click **CLEAR SELECTION**. The bottom text field may be edited.
2. Click the **SELECT A MACRO** radio button to enter a macro and choose one of the macros of PasswordCourier information from the pull down menu. As they reflect the number of end user validation fields and the use of comments field defined in the PasswordCourier Customization Manager, some of the `%PWDCOUR_USERn%` and `%PWDCOUR_COMMENTS%` macros may be disabled.
3. Click the **SELECT FROM A TABLE** radio button to select information from another field in the Help Desk system database (*Figure 41*).

**Figure 41: Selecting Data from Another Help Desk Field to Enter in Ticket Field**



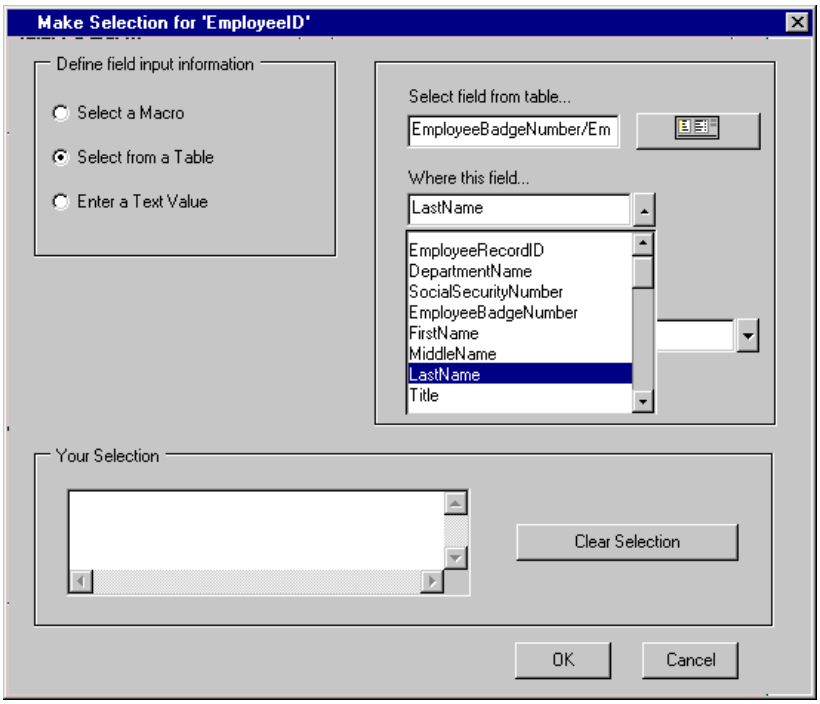

4. Choose the field from the Help Desk database table to be imported into the trouble ticket and click the **SELECT FIELD/TABLE** button. A Select Table & Field for WorkLog dialog box appears (*Figure 42*).

**Figure 42: Ticket Input, Table & Field Selection**



5. Click the table and then on one or more fields to import them into the trouble ticket. From the drop down list, choose the field in the Help Desk database table that contains the key for the selection from the database; for example, import an End User's EmployeeBadgeNumber based on the key of LastName equal to the end user's entry in the LastName field (*Figure 43*).

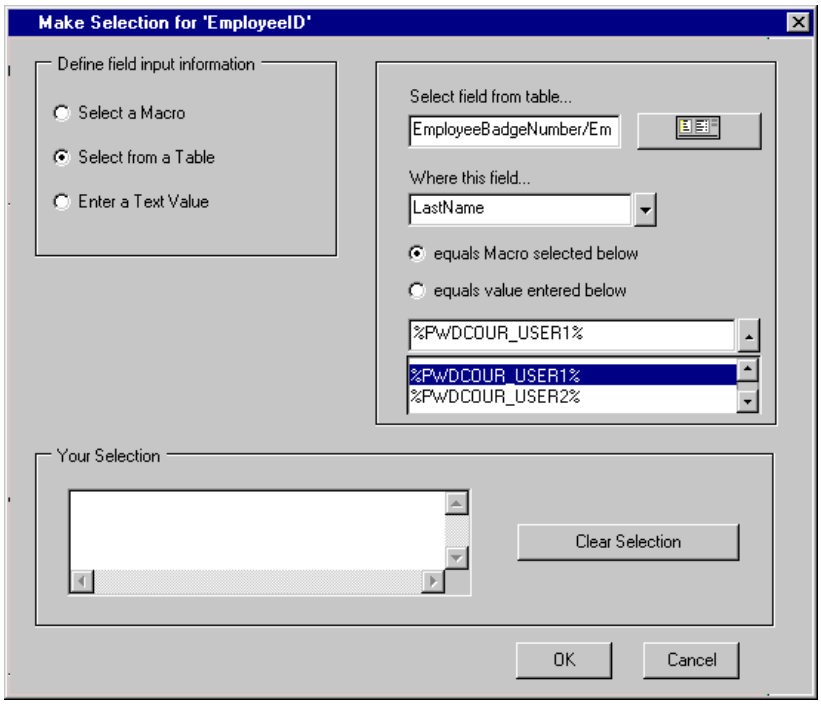
**Figure 43: Choosing a Key for Selecting Data for a Ticket Entry**




6. After you choose the key field, enter the desired value. Enter the information held by PasswordCourier or the customized text.

   *Figure 44* illustrates the use of a macro that contains the end user's information for the first end user validation field, “User's Last Name.”

**Figure 44: Finishing Data Selection for Ticket Entry**




PasswordCourier displays the selection in the text field at the bottom of the dialog box after you check the **APPLY** button.

The defined information is appended to what is already presented on the bottom text field. To replace existing information, click **CLEAR SELECTION** to clear the bottom text field. Click **OK** and the Create Ticket tab is returned. The new selection is applied to the ticket.

If entering text, enter it at the prompt and click **APPLY** to move it to the bottom text field or type directly into the bottom text field. The **RESET** button sets all fields back to their previous value.

For example, to enter text such as "PasswordCourier" in a field that contains the "Help Desk representative," click the **APPLY** button for the new selection to be applied and saved to the selected field in the list box for the configuration.

PasswordCourier supports dual datasource functionality for ticketing. To write authentication information to the ticket, modify the %SELECT...% statements in the ticket to include the word “Authentication” (without quotation marks), to specify that the information will come from the authentication datasource. "Authentication" allows you to configure PasswordCourier to use %SELECT to pull information from the profile datasource and use it in the ticketing datasource. For example, to read the first name field from the authentication table and put this information in the first name field of the ticket, where the first piece of validation information is a badge number, use a statement similar to the following:

```
%SELECT,Authentication,FirstName,Employees,EmployeeBadgeNumber,|PWDCOUR_USER1
  |%
```

**Note:** You can also use "Ticketing" with %SELECT. This keyword allows you to configure PasswordCourier to use %SELECT to pull information from the ticketing datasource and use it in the profile datasource.

The PasswordCourier Customization Manager allows you to move from the Request Tracking tab without entering valid data for all required fields. However, if there are required fields that have not been configured, end users receive error messages during their use of PasswordCourier when a ticket creation is attempted. PasswordCourier allows movement to another tab without completion of configuration because you may need to refer to configurations in other tabs.

**Note:** If all the required fields in this tab are not completely configured, a status is displayed on the bottom of the screen next to the **APPLY** button (*Figure 45*).

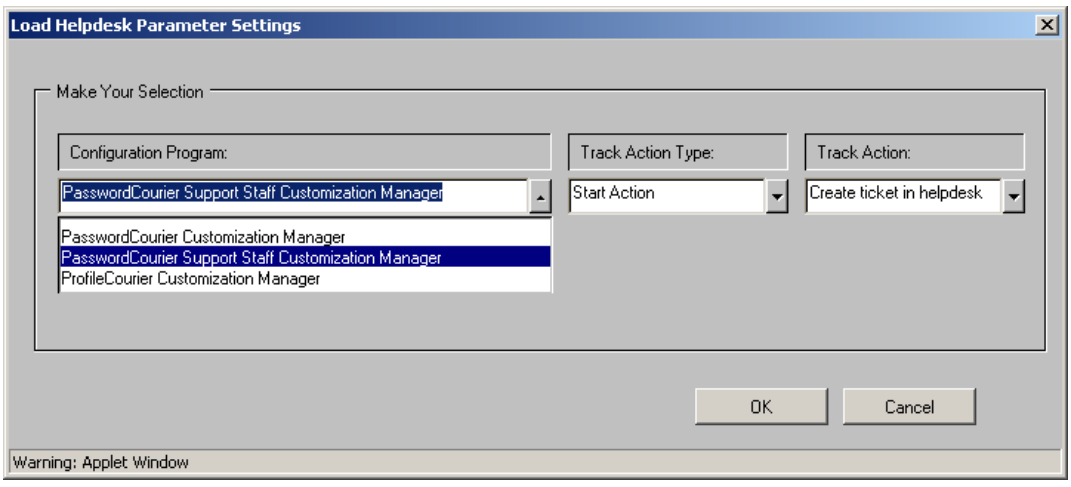
**Figure 45: Not All Required Fields Defined Status**


### Load Values from Another Configuration Program

The values in the table (center grid) can be loaded from another when working from any of the Request Tracking tabs. For example, the values in a PasswordCourier Customization Manager Request Tracking tab's center grid can be loaded from the PasswordCourier Support Staff Customization Manager's Request Tracking tab, or from the ProfileCourier Customization Manager's Request Tracking tab. To use this functionality, go to the tab into which those values will be loaded. This feature works when the table names for the source "load from" and to the selected destination page have the same table name. If the names do not match, this functionality will not work.

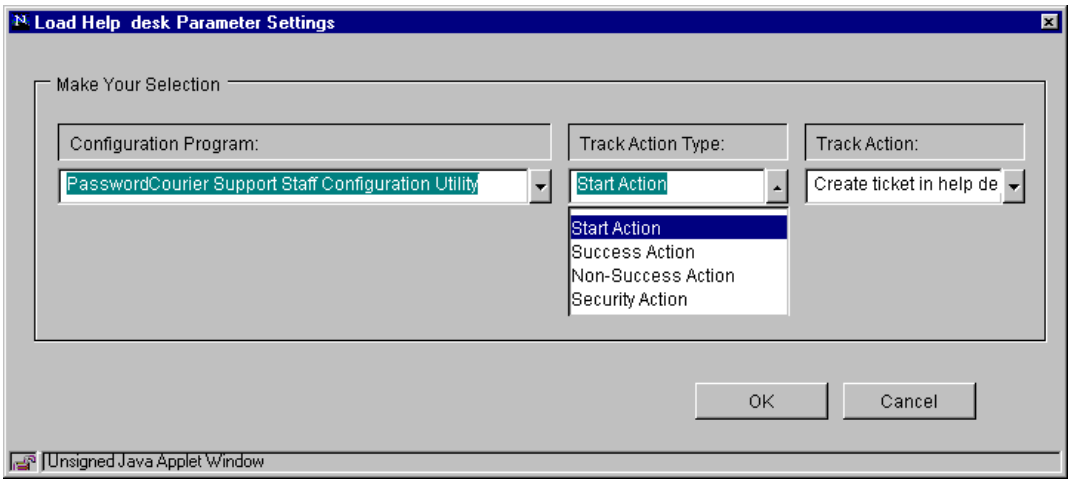
To use this functionality, click the button labeled **LOAD ABOVE VALUES FROM....** below the center grid. The following dialog box appears (*Figure 46*):

**Figure 46: Load Helpdesk Parameter Settings**




Select the Customization Manager to load from. Next, select the Track Action Type; Start Action, Success Action, Nonsuccess Action, or Security Action (*Figure 47*).

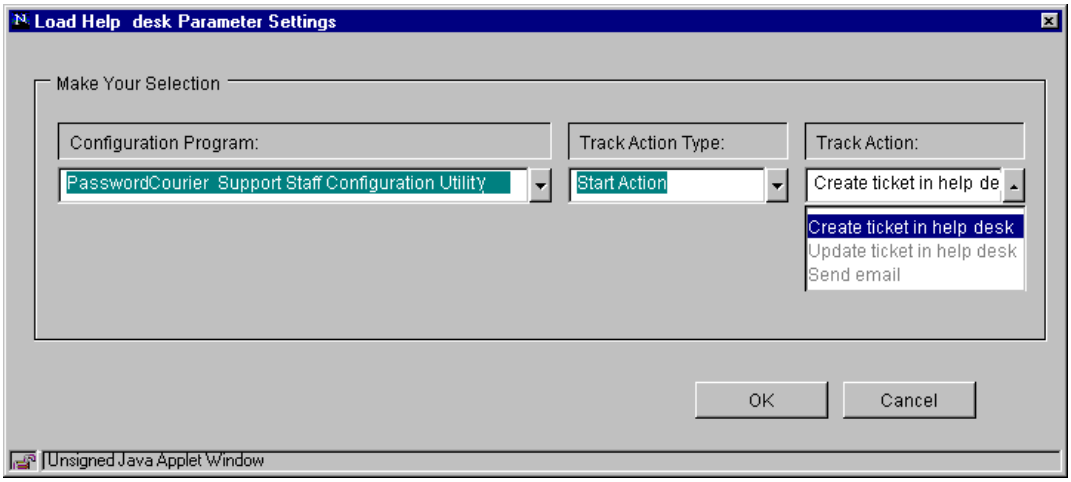
**Figure 47: Select Track Action Type**




Select the Track Action, which will vary depending on the Track Action Type selected (*Figure 48*). For example, it is not possible to select the Send e-Mail action from the Interact with Help Desk. Similarly, it is not possible to select an **INTERACT WITH HELP DESK** action from the Send e-Mail. Nor is it possible to select Update ticket in Help Desk from the Start Action or Security Action.

**Note:** A Start message is only displayed if the **INTERACT WITH HELP DESK** option is selected.

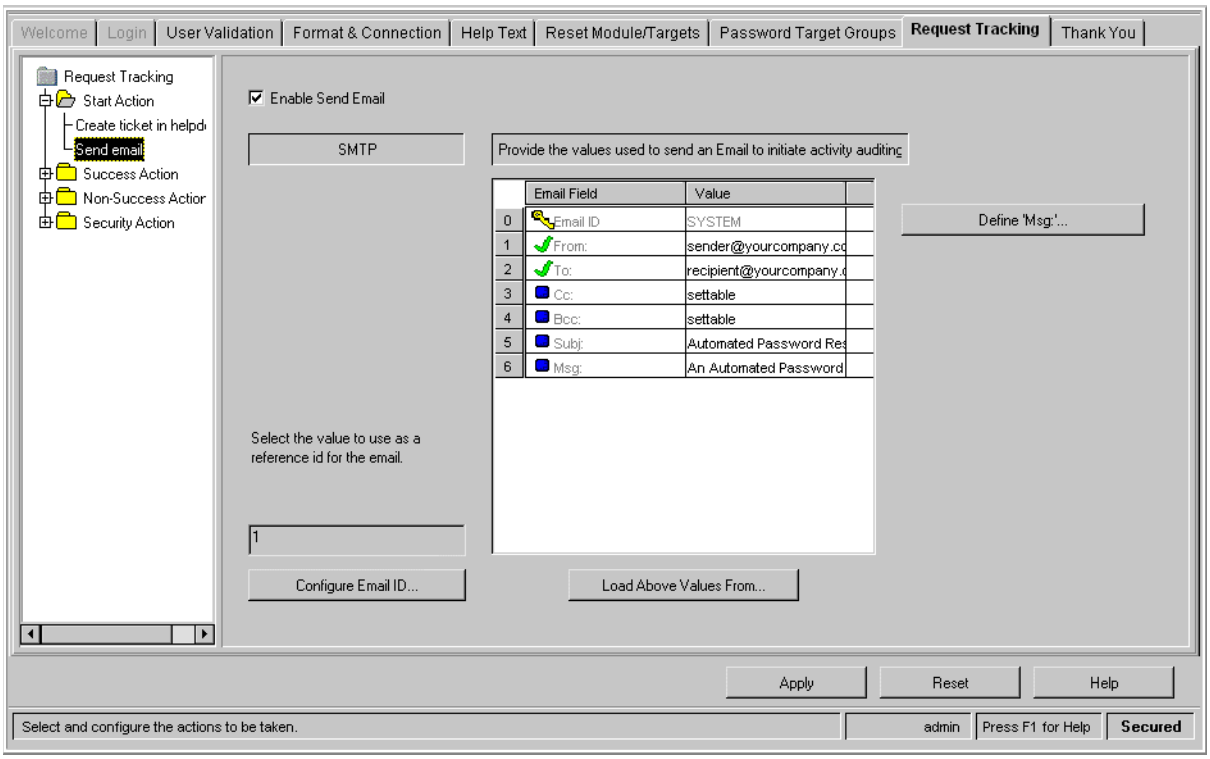
**Figure 48: Track Action Type Selected**




### Send e-Mail on Start Action

The PasswordCourier and PasswordCourier Support Staff Customization Manager enables the Core Server to send e-mail messages on a Start Action through the Request Tracking tab (*Figure 49*).

**Figure 49: Send e-Mail on Start Action**




The following e-mail values can be preconfigured:

- From
- To
- Cc
- Bcc
- Subject
- Msg

E-mail configuration can only be enabled if the SMTP server configuration is completed as part of the Core Server Configuration. To configure these fields, click the **ENABLE SEND EMAIL** checkbox. The e-mail fields are configured in the same manner as the **CREATE TICKET IN HELP DESK** fields.

**Note:** If e-mail notification and ticketing are configured, and email notification fails for an On Start event, PasswordCourier with Web Access (Java) displays an error message to the end user stating that a ticket could not be created. The message is incorrect; the event does successfully create a ticket.

**Note:** If ticketing and e-mail notification are configured on the Start Action in PasswordCourier with Web Access and the ticket is created and the e-mail action fails, the ticket id number only is generated but an error message is not.

**Note**: In the **DEFINE "MSG"** applet window, you can add message text in the Msg field. Including a backslash followed by a lowercase n (`\n`) in the message text creates a carriage return and a line feed (new line) at that location in the body of the e-mail.

## *Success Action*

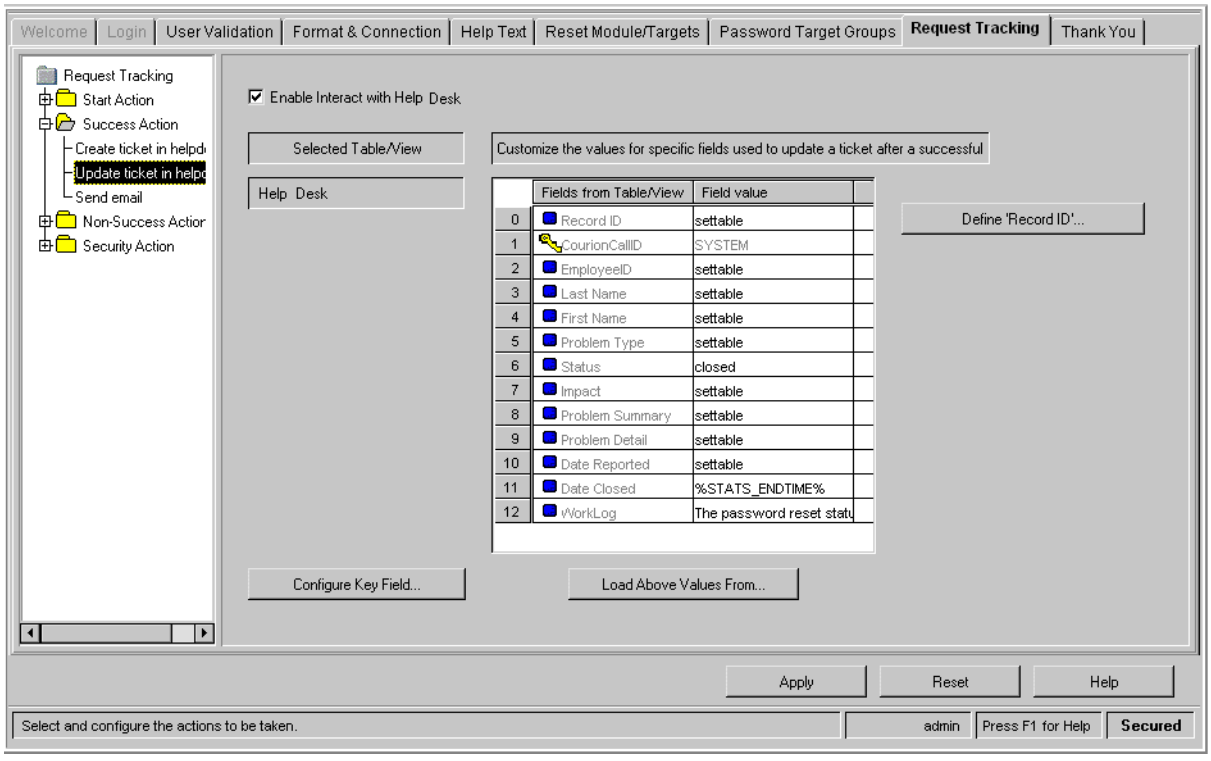
### Create Ticket in Help Desk on Success Action

A Success Action is the successful reset of a password in a target system. PasswordCourier and PasswordCourier Support Staff can be configured to create a ticket in the Help Desk system (if one wasn't created in the Start Action) upon a Success Action. See *"Create Ticket in Help Desk on Start Action" on page 73* for configuration instructions.

### Update Ticket in Help Desk on Success Action

After the end user has completed the password reset request and the password reset attempt was successful, PasswordCourier updates the ticket with the additional information configured in this tab. You can update the ticket with information such as the status of the password reset attempt, the duration of the password reset attempt, and the encrypted form of the password. Press the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous value.

**Figure 50: Update Ticket in Help Desk on Success Action Tab**




### Send e-Mail on Success Action

See *"Send e-Mail on Start Action" on page 81* for configuration instructions.

## *Nonsuccess Action*

A nonsuccess action takes place when a password is not reset.

The three nonsuccess conditions that could occur are:

- The password reset using a PMM failed.
- The password reset request was successful, but no PMM exists in the system. The password reset request is still considered incomplete or a nonsuccess because a password reset request was not attempted.
- The end user cancels out of the password request after the start action has occurred.

### Create Ticket in Help Desk on Nonsuccess Action

You can configure PasswordCourier and PasswordCourier Support Staff to update the ticket created in the Start Action or create a ticket in the Help Desk system (if one wasn't created in the Start Action) on a nonsuccess action. See *"Create Ticket in Help Desk on Start Action" on page 73* for configuration instructions.

### Update Ticket in Help Desk on Nonsuccess Action

After the end user has submitted the password reset request and, if one of the nonsuccess results occurs, PasswordCourier updates the ticket information with the additional information that you configure in this tab.

The ticket may be updated with information such as the status of the password reset attempt, the duration of the password reset attempt, and the encrypted form of the password. Press the **APPLY** button to save the configuration. The **RESET** button sets all fields back to their previous value. See *"Update Ticket in Help Desk on Success Action" on page 83* for configuration instructions.

### Send e-Mail on Nonsuccess Action

See *"Send e-Mail on Start Action" on page 81* for configuration instructions.

## *Security Action*

### Create Security Ticket in Help Desk on Security Action

If an end user reaches the maximum number of end user validation or end user authentication attempts PasswordCourier disables the end user from using PasswordCourier and creates a Security Incident trouble ticket. You can configure PasswordCourier and PasswordCourier Support Staff to create a ticket in the Help Desk system on a security action. See *"Create Ticket in Help Desk on Start Action" on page 73* for configuration instructions.

### Send e-Mail on Security Action

See *"Send e-Mail on Start Action" on page 81* for configuration instructions.

## Final Configuration Recommendations

After you configure PasswordCourier, you can perform a test run to ensure satisfaction with the end user validation and authentication process, the accuracy of the Password Targets attributes, and creation/updating of tickets in the Help Desk system. In the test run exceed the defined end user validation or authentication attempts to create a Security Ticket. In addition, be sure to try a reset on each of the defined group/target pairs.

# Notes, Warnings, and Limitations

## Encryption and Security

Core Security strongly recommends that access to this program be protected and restricted.

Various forms of data encryption are used throughout PasswordCourier to provide security for the sensitive data being communicated and stored within the application. All encryption in PasswordCourier uses a public key encryption algorithm. Encryption is used to provide security to the following elements of PasswordCourier:

- Communication between clients and the Core Server (clients include the six applets in the product, PasswordCourier, PasswordCourier Customization Manager, PasswordCourier Support Staff, PasswordCourier Support Staff Customization Manager, Enable Users Utility and the Data Security Utility.)
- Passwords that are passed as arguments to a PMM
- Passwords that are stored in the configuration repository such as:
- Help Desk administrator password
- NDS® passwords for the PMM for Novell® NDS®
- ODBC Data Source Name connection string

## Secure Sockets Layer

Security for the communications between the Core Server and its clients is accomplished using the Secure Sockets Layer (SSL) protocol. This industry standard communications protocol provides a secure connection between the service and its clients by encrypting all transmitted data.

## Help Desk Security

A detailed explanation of the security between the Core Server server and the Help Desk is out of the scope of this document. Security is left to the Help Desk API. However, each administrator applet (PasswordCourier Customization Manager, and Enable Users Utility) requires that the user be a valid Help Desk administrator to run it.

## Windows NT Security

Encryption and security in Windows NT are out of the scope of this document. During the PMM for Windows NT configuration, you are prompted to enter a Windows NT user name and password pair for the service to use for Windows NT password resets. This password is stored in encrypted format.

## Password Reset Request without a Module

If a user requests a password reset for a target that had the PMM "<None>" defined in the PasswordCourier Customization Manager, then the nonsuccess actions are executed and no password reset occurs.

**Note**: A "Success" message is returned if the request is successfully submitted; however, a non-success action is taken as the request for password reset was not fully completed. For example, if a phone queue to the helpdesk was long and a PMM did not exist, the PMM “<None>” would allow a request to be captured and logged to a ticket in a non-disclosed state. A helpdesk person could later follow up with the submitter and complete the request.

## Minimal Configuration

The following is the required minimal configuration that must be done in the PasswordCourier Customization Manager in order for PasswordCourier to run:

- In the Format Connection tab, if no table has been selected, the button in the first field has a label: **SELECT FIELD/TABLE**. Click this button and select the appropriate table to be used for end user validation/authentication. Also, make sure that all subsequent fields are selected to use the appropriate field information. If PasswordCourier Support Staff is being used and support staff validation is checked, then it is necessary to also specify the table/field for the support staff validation. For details on this topic, please refer to *“Format & Connection Tab” on page 26*.
- At least one target must be defined in the Password Management Module/Targets tab. See *“Management Modules/Targets Tab” on page 33*.
- In the Password Target Groups tab, at least one target group must be defined with at least one target as a member. See *“Password Target Groups Tab” on page 65*.
- If ticketing is active, in the Create Ticket screen, all required fields must be configured. If there are no required fields, then at least one field must be configured. If ODBC is being used, the unique key field must be configured with a starting record id. See *“Create Ticket in Help Desk on Start Action” on page 73*.
- If ticketing is active, in the Security Ticket screen, all required fields must be configured. If there are no required fields then at least one field must be configured. See *“Create Security Ticket in Help Desk on Security Action” on page 84*.

If PasswordCourier is not minimally configured, the courion.log file stops at the first field that is not minimally configured. Test the configuration by running PasswordCourier. If no error messages occur, then the configuration is a success.

If the "Not minimally configured" message box is displayed, check the `courion.log` file on the system running the Windows NT Core Server. This log file identifies the required parameter found not to be configured.

## Float Fields

If a float field is set in a call ticket, leading zeros should be added. For example, if a float field is configured for the range 1.00 to 1000.00 and a value of 9.00 is to be entered, it must be typed as 0009.00. Decimal and Numeric fields may have the same behavior if the scale of these data types is greater than zero.

## Enable Users Utility

It is highly recommended that access to the Enable User Utility be protected and restricted. See *Installing the Access Assurance Suite* for more information about this.

The list of disabled users has a maximum capacity of 1400.

## Core Server

1. Protect access to all server .dll and .exe files as well as to the cfgfile.txt file.
2. PasswordCourier includes a macro called `%CLIENT_NT_SESSIONS%` that allows the inclusion of Windows NT User Session information in request tracking options. For this macro to work, the Core Server must be logged into the Windows NT domain as Domain Administrator and have local administrator access to the machine that the Service resides upon. For more information see *Installing the Access Assurance Suite*
3. If the Core Server is changed to run as a Windows NT account, other than LOCALSYSTEM, make sure that account has full control of the Core Server folder and its files and the registry keys under CourionPasswordCourier in the LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services.

The Audit Log file keeps a record of all changes made with PasswordCourier Customization Manager. For the best view of the Audit.log file import to Microsoft Excel® using Delimited/Tab.

If the Help Desk administrator password is changed, the Core Server must be updated.

Restrict web access to the PasswordCourier Customization Manager, PasswordCourier Support Staff Customization Manager, and Enable User Utility on the web server. Only Help Desk administrators should be allowed to access these applets.

Restrict Windows NT end user access to the PwdApi.DLL file and the entire Core Server folder.

Protect the Windows NT administrator password.

Protect the Help Desk administrator password.

Protect cfgfile.txt and all log files (*.log).

By default all log files except `courion.log` and `ntmodule.log` are accessible by local administrators and the reset account assigned to PasswordCourier during installation. The files `courion.log` and `ntmodule.log` are accessible only by the PasswordCourier reset account.

If the migration plan does not include populating fields in the profile record with user names and if the User-Based Target feature is deactivated, the mechanism for retrieving user names from the profile record will fail.

### *Log File Permissions*

All log files generated by PasswordCourier are generated by default with the following permissions:

- Local System account
- Local administrators group

The only exception to this rule is the ntmodule.log, which, in addition to the above accounts, also gives permission to the account specified during PMM for Windows NT and Windows 2000 configuration for performing Windows NT password resets. For more information, see the chapter “Microsoft Windows 2000 and Windows NT — PMM and Connector” in the manual *Configuring Password Management Modules (PMMs), Connectors, and Agents*.

## Help Text Display

If the Web Access (Java) client is used, to ensure clear presentation of Success, Non-Success, and Help text to the end user, do not exceed 50 characters per line.

# Integrating with Support Web Pages

With the integration of PasswordCourier and an end user support web site, end users can click on a link to download PasswordCourier and easily start the password reset process. The web (HTML) portion of PasswordCourier is customizable to display logos, Help Desk phone numbers, or any other company specific information the end user might need.

The PasswordCourier Customization Manager and Enable Users Utility may also be embedded in web pages for use by the Help Desk or support staff.

During the installation process the file PwdCourUser.html was installed. This HTML file may be modified to become a company specific portal for password resets.

For Web Access (Java) clients, PasswordCourier can be embedded in a previously designed and designated web page by placing the following code in the web page:

```
<applet ARCHIVE="pwdcour.jar" CODEBASE="http://
www.myserver.com/myfolder/www/javacode"
CODE="PwdCour.class" WIDTH=550 HEIGHT=405 alt="Password
Reset Applet">
<PARAM NAME="Title" VALUE="PasswordCourier">
<PARAM NAME="Port" VALUE="8189">
</APPLET>
```

The web browser must be Java™ technology-enabled to use PasswordCourier.

Please note that the width and height figures for PasswordCourier must be as specified above.

Add the following parameters to the above specification to redirect end users to a specific URL:

```
<PARAMNAME=SuccessRedirectToVALUE="http://www.company.com/
pwdcour/pwdresetsucc.html">
<PARAMNAME=SuccessRedirectTargetVALUE="_self">
<PARAMNAME=NonSuccessRedirectToVALUE="http://
www.company.com/pwdcour/pwdresetnonsucc.html">
<PARAMNAME=NonSuccessRedirectTargetVALUE="_self">
```

If these parameters are present, the end users are redirected to the specified URL upon pressing the **FINISH** button. This button is presented after a password reset request is completed for PasswordCourier and for PasswordCourier Support Staff.

If these parameters are not present end users are able to run the particular applet again upon pressing the **FINISH** button.

**Note:** All www files for PasswordCourier are located in the folder "www " that was specified during installation. To modify these files, copy this folder to the appropriate location on the HTTP server and modify the copies. Edit the applet urls in the HTML files to point to the correct location. HTML files are located in the Utils Folder for utilities, the CustMgrs folder for Customization Managers that use Java™ technology (PasswordCourier, PasswordCourier Support Staff, and ProfileCourier).

# Alternate Sources for Parameter Configurations

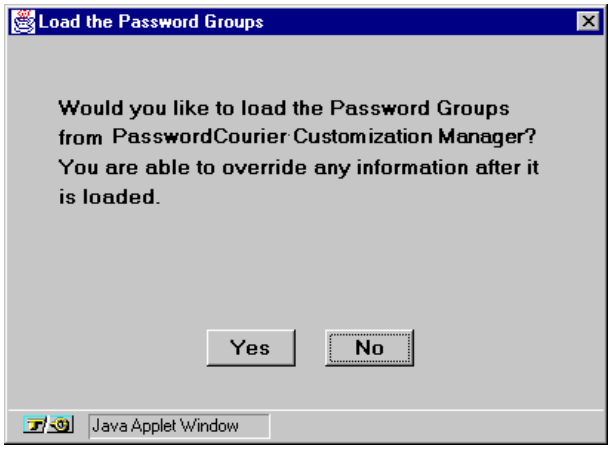
For tabs that look and function the same in PasswordCourier and PasswordCourier Support Staff parameters may be loaded from one to the other on the corresponding Request Tracking tabs located inside the Customization Manager.

Parameters may also be loaded from a related Request Tracking tab in the current configuration. For example, if the table in the Create Ticket in Help Desk tab is to be the same as the table in the Create Security Ticket in same tab, the parameters from the former can be loaded into the latter using the **LOAD ABOVE PARAMETERS FROM...** button.

For the Management Module/Targets and Password Target Groups tabs, the Customization Manager provides the option of loading the appropriate parameters from PasswordCourier to PasswordCourier Support Staff (or vice versa) if one is configured and the other is not.

*Figure 51* offers an example of the presented message box:

**Figure 51: Load Parameters from PasswordCourier Message**




Note that this feature:

- Prompts only if a tab has never been configured
- Prompts only if the tab in the Customization Manager in the other product is configured (i.e., prompts in PasswordCourier if the corresponding tab in PasswordCourier Support Staff is configured and vice versa)

Targets and groups loaded by this feature may have additional targets and groups added, and they may be modified or deleted.

To save changes, click the **APPLY** button. **RESET** will return the settings to their original configuration.

PasswordCourier and PasswordCourier Support Staff will also provide a prompt if a tab that was not fully configured is opened. If a tab is configured and any aspect is saved by clicking on “Apply,” no prompts will be displayed on subsequent entries to the tab. **APPLY** or **RESET** must be clicked before moving to a different tab if any changes have been made.

There are instances where loading parameters from PasswordCourier to PasswordCourier Support Staff (or vice versa) may not make sense. For example, macros are not interchangeable between PasswordCourier and PasswordCourier Support Staff. The purpose of this load feature is to save time by reusing common configuration parameters and then modifying them appropriately.

For a list of macros and where they are used, please refer to *"Courion Server Macros" on page 93*.

# Core Server Specific Errors

If an attempt to start the service fails due to a problem specific to the Core Server, the returns service specific errors.

The defined Core Server specific errors are:

- Server specific error 1 deals with SSL Socket related errors. This server specific error is logged when a problem related to SSL occurs that prevents the server from starting. Check the event log and the courion.log file for additional information.
- Server specific error 2 concerns Windows NT registry access errors. This server specific error is logged when a problem related to Windows NT registry occurs that prevents the server from starting. Check the registry access for the Access Assurance Suite.
- Server specific error 3 deals with Help Desk related errors. This server specific error is logged when a problem related to the Help Desk occurs that prevents the server from starting. This could, for example, be related to problems connecting to the specified Help Desk for the installation or similar problems. Check the Help Desk connection and check courion.log for details.
- Server specific error 4 involves account log in related errors. This server specific error is logged when a problem related to the local account occurs that prevents the server from starting. The error could be caused because the account used to install/run the account does not have the appropriate privileges. Check courion.log for details.
- Server specific error 5 deals with configuration file related errors. This server specific error is logged when a problem related to the cfgfile.txt configuration file occurs that prevents the server from starting. The problem could be related to access restrictions such as the end user having incorrect privileges or the configuration being read-only. Check the event log as well as courion.log for more details.

# Core Server Macros

Macros are available for substituting information gathered by the Core Server into Access Assurance Suite products. The Core Server not only gathers information entered by the end user, but it also collects statistics on the use of the product. This may be useful for tracking service level performance.

**Note:** some macros are not assigned values until after requests have been attempted. If a macro of this kind is used for substitution before it has a meaningful value, the value <<macro has no value>> is substituted for the macro.

## *PasswordCourier Macros*

Table 14 list supported macros useful when they have valid values:

**Table 14: PasswordCourier Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWDCOUR_USER1% | Input entered into user validation field 1 in PasswordCourier. | Yes | Yes | Yes | Yes | Yes |
| %PWDCOUR_USER2% | Input entered into user validation field 2 in PasswordCourier (if 2 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDCOUR_USER3% | Input entered into user validation field 3 in PasswordCourier (if 3 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDCOUR_USER4% | Input entered into user validation field 4 in PasswordCourier (if 4 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDCOUR_PWDGROUP% | Password group selected in PasswordCourier. | Yes | Yes | Yes | Yes | No |

**Table 14: PasswordCourier Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWDCOUR_PWDTARG% | Password target selected in PasswordCourier. If an alias is defined for the selected Password Target, this macro represents the real target and its alias. | Yes | Yes | No | Yes | No |
| %PWDCOUR_TARGET_NAME% | The target name of the selected Password Target (%PWDCOUR_PWDTARG%) in PasswordCourier. | Yes | Yes | No | Yes | No |
| %PWDCOUR_TARGET_ALIAS% | The alias of the selected Password Target (%PWDCOUR_PWDTARG%) in PasswordCourier. | No | Yes | No | Yes | No |
| %PWDCOUR_TARGET_INTALIAS% | The internal alias of the selected Password Target (%PWDCOUR_PWDTARG%) in PasswordCourier. | No | Yes | No | Yes | No |
| %PWDCOUR_COMMENTS% | Comments entered by the user in the comments field of PasswordCourier (if configured).* | No | Yes | No | No | No |
| %PWDCOUR_RESET_USERNAME% | The username against which the password reset is attempted. | No | Yes+ | No | No | No |

**Table 14: PasswordCourier Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWD_ RESET_ STATUS% | The status of the password reset request. Values may be SUCCESS, FAILURE, CANCELLED, or NONE RESET MODULE.<br>The status is CANCELLED when the browser is shut down after the ticket is created, but before the reset request has been made.<br>The status is NONE PASSWORD MANAGEMENT MODULE when the selected target is configured to use the "<None>" Password Management Module. This macro's value usually ends with a period. There is no need to include a period after specifying this macro. | No | Yes | No | No | No |
| %PWD_ RESET_ MODULE% | The password management module used for the requested password reset request. | Yes | Yes | No | Yes | No |

*See “Macro Dependencies” on page 100.
+Applies to Success and Non Success only. Does not apply to Start.

### *PasswordCourier Support Staff Macros*

Table 15 lists supported PasswordCourier Support Staff macros.

**Table 15:** PasswordCourier Support Staff **Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWDSS_ STAFF1% | Input entered into Support Staff Validation field 1 in PasswordCourier Support Staff (if 1 or more staff fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ STAFF2% | Input entered into Support Staff Validation field 2 in PasswordCourier Support Staff (if 2 staff fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ USER1% | Input entered into user validation field 1 in PasswordCourier Support Staff (if 1 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ USER2% | Input entered into user validation field 2 in PasswordCourier Support Staff (if 2 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ USER3% | Input entered into user validation field 3 in PasswordCourier Support Staff (if 3 or more user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ USER4% | Input entered into user validation field 4 in PasswordCourier Support Staff (if 4 user fields are configured).* | Yes | Yes | Yes | Yes | Yes |
| %PWDSS_ PWDGROUP % | Password group selected in PasswordCourier Support Staff. | No | Yes | No | Yes | No |

**Table 15:** PasswordCourier Support Staff **Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWDSS_ PWDTARG% | Password target selected in PasswordCourier Support Staff. If an alias is defined for the selected Password Target, this macro represents the real target and its alias. | No | Yes | No | Yes | No |
| %PWDSS_ TARGET_ NAME% | The target name of the selected Password Target (%PWDSS_PWDTARG%) in PasswordCourier Support Staff. | No | Yes | No | Yes | No |
| %PWDSS_ TARGET_ ALIAS% | The target's alias for the selected Password Target (%PWDSS_PWDTARG%) in PasswordCourier Support Staff. | No | Yes | No | Yes | No |
| %PWDSS_ TARGET_ INTALIAS% | The target's internal alias of the selected Password Target (%PWDSS_PWDTARG%) in PasswordCourier Support Staff. | No | Yes | No | Yes | No |
| %PWDSS_ COMMENTS% | Comments entered by support staff in the comments field in PasswordCourier Support Staff (if configured).* | No | Yes | No | No | No |
| %PWDSS_ USERACCT% | The user account name for which the password reset was attempted. It is entered by support staff in the user account field in the PasswordCourier Support Staff.* | No | Yes | No | No | No |
| %PWDSS_ RESET_ USERNAME% | The full text that results from the expanded Username Selection Query for the target. | No | Yes | No | No | No |

**Table 15:** PasswordCourier Support Staff **Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %PWD_ RESET_ STATUS% | The status of the password reset request. Values may be SUCCESS, FAILURE, CANCELLED, or NONE RESET MODULE.<br>The status is CANCELLED when the browser is shut down after the ticket is created, but before the reset request has been made.<br>The status is NONE PASSWORD MANAGEMENT MODULE when the selected target is configured to use the "<None>" Password Management Module. This macro's value usually ends with a period. There is no need to include a period after specifying this macro. | No | Yes | No | No | No |
| %PWD_ RESET_ MODULE% | The reset module used for the requested password reset request. | Yes | Yes | No | Yes | No |

*See “Macro Dependencies” on page 100.

## *Core Server Common Macros*

Table 16 lists supported Core Server macros.

**Table 16: Core Server Common Macros**

| Macro Name | Description | Request Tracking Actions | | | Password Target Messages | User Validation Messages |
|---|---|---|---|---|---|---|
| | | Validation Messages | Start Success/ Non Success | Security | | |
| %TICKET_ID% | The Ticket ID of the ticket created by the Help Desk for the request. If an e-mail is sent instead of creating a ticket at the Start Action, the e-Mail Reference ID is returned.* | No | Yes | No | Yes | No |
| %EMAIL_ID% | The e-Mail ID of the e-mail sent during the start action.* | No | Yes | No | Yes | No |
| %CLIENT_IP_ ADDR% | The IP address of the client running the applet. | Yes | Yes | Yes | Yes | Yes |
| %CLIENT_HOST _NAME% | The Host Name of the client system running the applet. | Yes | Yes | Yes | Yes | Yes |
| %CLIENT_APP_ NAME% | The name of the applet currently running. | Yes | Yes | Yes | Yes | Yes |
| %STATS_ STARTTIME% | Time starts when the start action or the security action is initiated. | Yes | Yes | Yes | Yes | Yes |
| %STATS_ ENDTIME% | Time is stopped after the password reset attempt. | No | Yes | No | No | No |
| %STATS_ DURATION% | Duration in seconds from user validation to after reset attempt. | No | Yes | No | Yes | No |
| %Behavior.Langu age% | References the language value specified in an end user's initial ASP page or calling URL by the variable "lang=". See the Multilanguage chapter in the *Access Assurance Suite Implementation Guide*. | Yes | Yes | Yes | Yes | Yes |

*See "Macro Dependencies" on page 100.

### *Macro Dependencies*

Table 17 shows macros with dependencies that affect availability.

**Table 17: Macro Dependencies**

| Macro Name | Dependency |
|---|---|
| %PWDSS_STAFF1%<br>%PWDSS_STAFF2% | The availability of the Macros depends on the setting for the number of fields of information to be used to uniquely identify the support staff. This setting can be found on the User Validation tab of the PasswordCourier Support Staff Customization Manager. For example, if you choose to use one field, %PWDSS_STAFF1% is available. |
| %PWDSS_USER1%<br>%PWDSS_USER2%<br>%PWDSS_USER3%<br>%PWDSS_USER4% | Macro availability depends on the setting for the number of fields of information to use to uniquely identify the user. This setting can be found on the User Validation tab of the PasswordCourier Support Staff Customization Manager. For example, if you choose to use two fields, both %PWDSS_USER1% and %PWDSS_USER2% are available. |
| %PWDCOUR_USER1%<br>%PWDCOUR_USER2%<br>%PWDCOUR_USER3%<br>%PWDCOUR_USER4% | Macro availability depends on the setting for the number of fields of information to be used to uniquely identify the user. This setting can be found on the User Validation tab of the PasswordCourier Customization Manager. Example: If you choose to use two fields, both %PWDCOUR_USER1% and %PWDCOUR_USER2% are available. |
| %PWDCOUR_TARGET_ALIAS%<br>%PWDSS_TARGET_ALIAS% | The availability of the macro depends on whether the selected password target was configured to have an alias which is used to present a more user friendly password target name to the applet user. If an alias is not defined for a specific target, the %PWDCOUR_PWDTARG% macro contents are the same as the %PWDCOUR_TARGET_NAME% macro. The same is true for the %PWDSS_PWDTARG% macro and the %PWDSS_TARGET_NAME% in the PasswordCourier Support Staff. |
| %PWDCOUR_COMMENT%<br>%PWDSS_COMMENTS% | Macro availability depends on whether the "Use Comments" check box is selected on the Format & Connection tab of the PasswordCourier Customization Manager or the PasswordCourier Support Staff Customization Manager. If the box is selected, the macro is available. |
| %TICKET_ID% | Macro availability depends on the Request Tracking Start Action. If no Help desk ticket is created, this macro does not have a value. If the Request Tracking Start Action is configured to create a Help Desk ticket, this macro contains the ID of the ticket created in the Help Desk |
| %EMAIL_ID% | Macro availability depends on the Request Tracking configuration. This macro is not available if e-mail is not configured. |
| %PWDSS_USERACCT% | Macro is only useful if a value is entered by the support staff user. |

# Chapter 3: Synchronization

This chapter explains how to configure the PMM for Synchronization.

The Password Management Module (PMM) for Synchronization enables PasswordCourier and PasswordCourier Support Staff to reset multiple passwords at once. The PMM for Synchronization is installed with the Courion Enterprise Provisioning Suite. For more information on the installation and requirements, please refer to *Installing the Enterprise Provisioning Suite*.

The correct access keys are necessary to run this PMM.

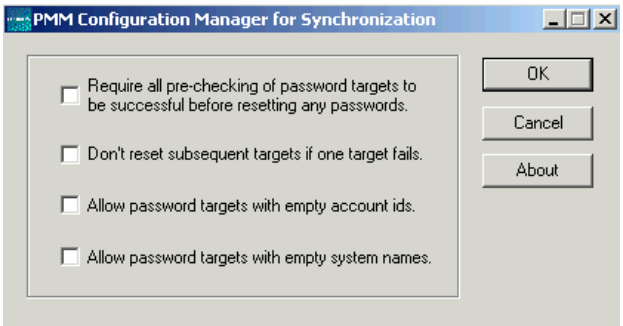
## PMM Configuration

To begin the PMM configuration, select

Start > Programs > Courion Enterprise Provisioning Suite> Password Management Modules > Synchronization.

The PMM Customization Manager for Synchronization is displayed (*Figure 52*).

**Figure 52: PMM Customization Manager for Synchronization**




This PMM consecutively resets the passwords for a list of user accounts specified in the target definition. Each user account is described by three values:

- The PMM name
- The PMM target name
- The user account name

Please see the “Synchronization Target Configuration” section in *“Configuring PasswordCourier and PasswordCourier Support Staff” on page 20* for details on configuring this list. The configuration allows administrators to specify how the PMM behaves when only some of the specified user accounts and system names are valid.

## Require Pre-Checking

Select the **REQUIRE ALL PRECHECKING OF PASSWORD TARGETS TO BE SUCCESSFUL BEFORE RESETTING ANY PASSWORDS** check box to require that the PMM validate all system names and user accounts before attempting to reset any of the passwords.

**Note:** This behavior is independent of User-Based Targets set as active or inactive.

## Target Failure

The configuration also allows the configuration manager to decide whether the failure of one password reset should affect the other password resets.

Select the **DON'T RESET SUBSEQUENT TARGETS IF ONE TARGET FAILS** check box to cancel further password resets in the event of a reset failure.

**Note:** passwords that were reset prior to the failure will retain the new password. If the check box is not selected, all specified password resets are attempted regardless of any reset failure.

**Note:** This behavior is independent of User-Based Targets set as active or inactive.

## Empty Account IDs

Select the **ALLOW PASSWORD TARGETS WITH EMPTY ACCOUNT IDS** checkbox to allow the PMM to ignore empty account IDs in the list of reset targets. Click this box to have the PMM for Synchronization skip all targets with a valid PMM type and system name and an empty account ID. No error is generated. When the box is not checked, an empty account ID is passed to the PMM for Synchronization and processed normally, producing the target specific error for an invalid account ID.

**Note:** If the check box is marked, a user only needs to be listed for some targets in the Synchronization Target Screen in PasswordCourier. If the check box is not selected, a user must be on the list for all targets listed in the target screen to have synchronized reset function. A user is listed for a specific target when the User-based Targets table has a record that includes a target ID. The target ID must match the value that is assigned in the PasswordCourier application for that specific target.

## Empty System Names

Select the **ALLOW PASSWORD TARGETS WITH EMPTY SYSTEM NAMES** check box to allow the PMM to ignore empty system names in the list of reset targets. When this box is checked, targets with a specified PMM type and account ID, but with an empty system name, are skipped and no error generated. When it is not checked, an empty system name is passed to the PMM and processed normally, producing the target specific error for an invalid system name.

**Note:** This switch does not apply if User-Based targets are set as active.

## Notes and Warnings

For more information on Synchronization Target configuration, please review the Synchronization Target Configuration and Synchronization Target Configuration when User-Based Targets is Enabled sections in *"Configuring PasswordCourier and PasswordCourier Support Staff" on page 20*. It is necessary to configure PasswordCourier and PasswordCourier Support Staff correctly in order for the PMM for Synchronization to work correctly.

# Chapter 4: Configuring PasswordCourier for Transparent Synchronization

In this chapter:

# Overview

The PasswordCourier Transparent Synchronization feature allows PasswordCourier to capture password changes from native operating system tools, such as the Microsoft Windows 2000 Professional password change dialog box, and propagate them to the Courion Server for synchronization with a range of targets.

The Transparent Synchronization feature:

- Provides end-users with access to PasswordCourier password resets through their native operating system change password interface.
- Ensures that passwords are synchronized on all targets.
- Provides a high level of security for password resets.
- Counts native password resets against the PasswordCourier history list

The Transparent Synchronization feature has two main components: The Transparent Synchronization service and the Transparent Synchronization Listener.

## The Transparent Synchronization Service

The Transparent Synchronization service runs on a Courion Server. The Transparent Synchronization service:

- Maintains a lists of Transparent Synchronization Listeners in the network.
- Maintains a Global Arrestor Table (GAT) service. The Transparent Synchronization service uses the information in this table to prevent circular password resets when it receives reset requests from a Transparent Synchronization Listener. The GAT service can reside on the Courion Server where you install the Transparent Synchronization service or on another Courion Server.

## The Transparent Synchronization Listener

A copy of the Transparent Synchronization Listener runs on each domain controller in any domain where you want to detect password changes and use Transparent Synchronization to synchronize your targets. The Listener:

- Detects native operating system password changes and notifies the Transparent Synchronization service.
- Performs both native operating system strength checking and Core Security password strength checking on the new password before it allows the native reset to occur.

For more information about how to install and configure the Transparent Synchronization Listeners currently supported, please see *"Installing and Configuring the Transparent Synchronization Listener" on page 126*.

# Requirements

For Courion software requirements, please refer to the Product Requirements chapter in *Installing the Access Assurance Suite*.

The Courion Server where you run the Transparent Synchronization service software and the GAT service software has these requirements:

- The Password Management Module (PMM) for Synchronization. You must install and configure this PMM before you use the Transparent Synchronization feature. See *"Synchronization" on page 101* for information about how to install and configure this PMM.

  **Note:** The Transparent Synchronization feature is subject to any settings you select when you configure the PMM for Synchronization. For example, if you select the option **DON'T RESET SUBSEQUENT TARGETS IF ONE TARGET FAILS**, the Transparent Synchronization service may not synchronize the password reset on all the targets.
- Access to the profile or ticketing database that contains User-based Target information if you are using User-based Targets.
- Usernames in the IdentityMap are case-sensitive in Transparent Synchronization configurations. The case of the username in the IdentityMap table's username column must match the case of the username as it is reported by the Transparent Synchronization listener.

## Transparent Synchronization Access Key

The Transparent Synchronization feature requires an access key. If you have questions about how to obtain an access key for Transparent Synchronization, contact Core Security Customer Support.

## The Transparent Synchronization Service and PasswordCourier Support Staff

The Transparent Synchronization service requires exclusive use of the PasswordCourier Support Staff workflow on the Courion Server where the Transparent Synchronization service is installed. On that Courion Server, the PasswordCourier Support Staff clients are disabled when you install the Transparent Synchronization access key. If you want to use PasswordCourier Support Staff and the Transparent Synchronization feature in the same environment, install the Access Assurance Suite with PasswordCourier Support Staff on a separate Courion Server.

# Sample Transparent Synchronization Configurations

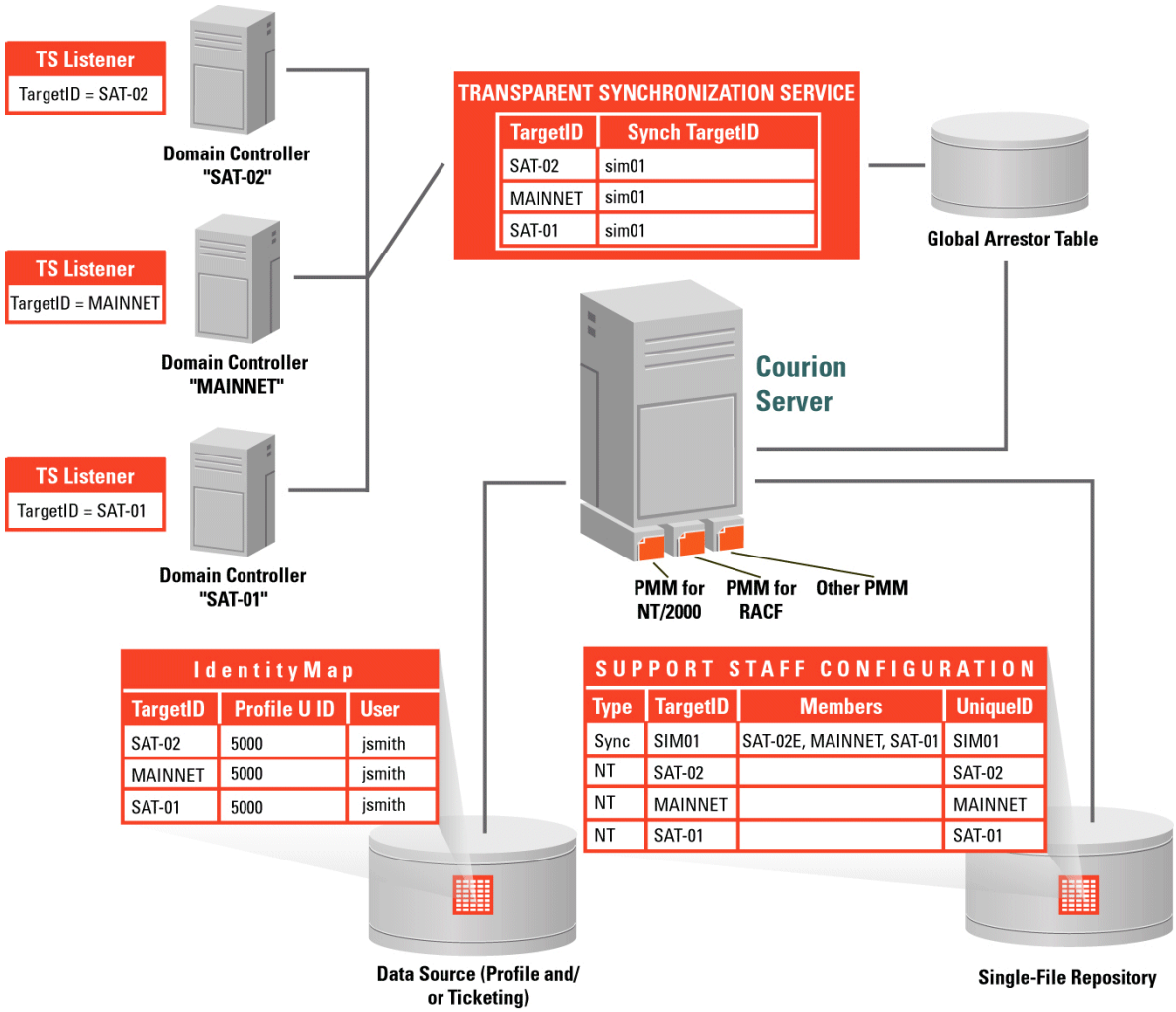
You can use transparent synchronization with or without the User-based Target option.

**Note:** Core Security recommends that you use a User-Based Target with the Transparent Synchronization feature. See *"User-Based Targets" on page 62*.

## Transparent Synchronization with User-based Targets

*Figure 53* represents transparent synchronization configuration with User-based Targets

**Figure 53: Transparent Synchronization with User-based Targets**




In this configuration, the Transparent Synchronization service and the GAT service reside on the same Courion Server. The synchronous reset target is SIM01. Three Transparent Synchronization listeners, (SAT-02, MAINNET, and SAT-01) are configured as target IDs in PasswordCourier Support Staff and as members of the synchronous reset target. As a result, a password reset being triggered on any one of these listeners causes password synchronization to the members of the synchronous reset target. The target IDs are configured in the UBT database for user jsmith.

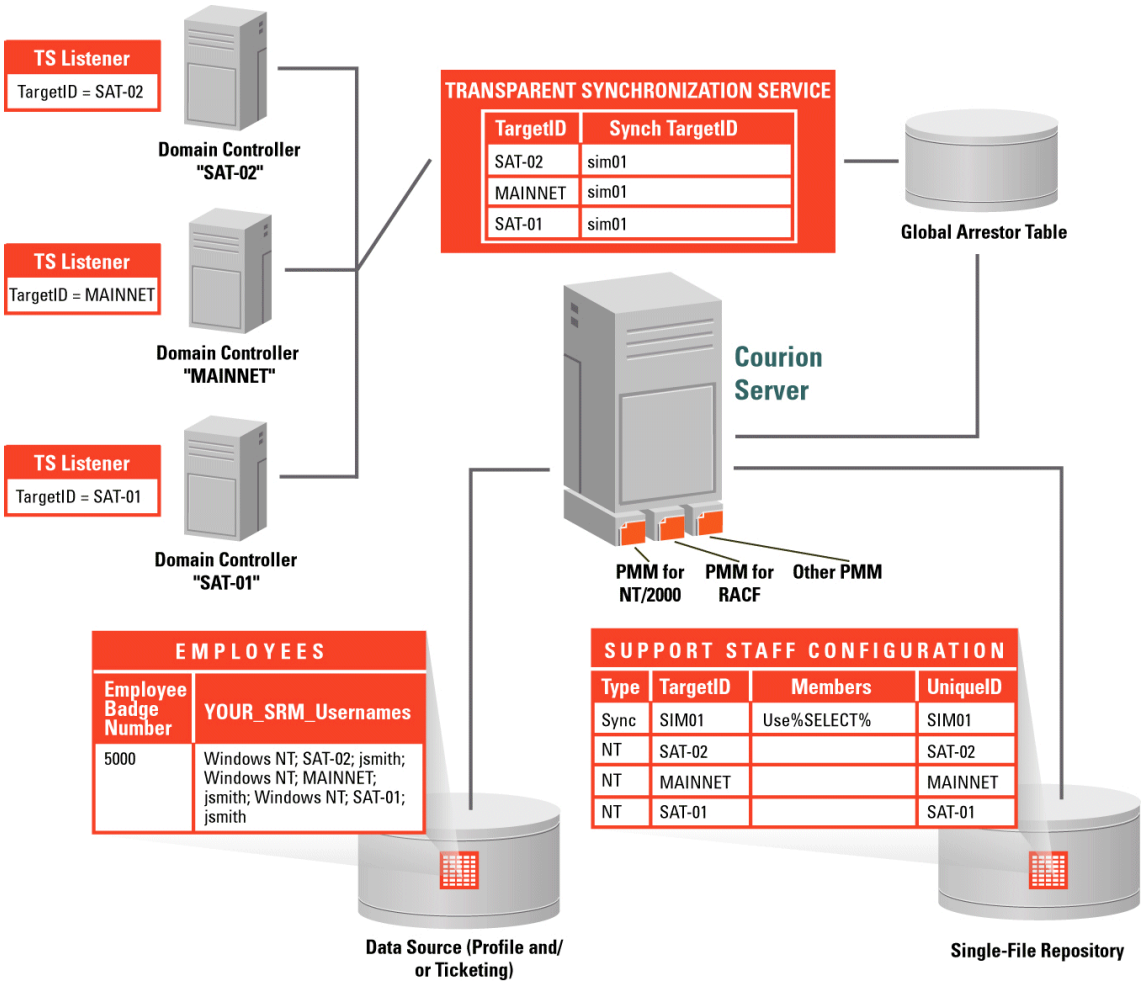
**Note:** It is not necessary for the listener to be a member of the synchronous reset target. It is necessary to have an entry in the User-based Target that corresponds to the user performing the native password reset on the listener target.

**Note:** The synchronous reset target can contain members that are not Transparent Synchronization listeners.

## Transparent Synchronization without User-based Targets

*Figure 54* represents a transparent synchronization configuration without **User-based targets**.

**Figure 54: Transparent Synchronization Without User-based Targets**




In this configuration, the Transparent Synchronization service and the GAT service reside on the same Courion Server. The synchronous reset target is SIM01. Three Transparent Synchronization listeners, (SAT-02, MAINNET, and SAT-01) are configured as target IDs in PasswordCourier Support Staff and are members of the set of targets generated by the synchronous reset target's user selection query.

# Configuring PasswordCourier Support Staff for Use by the Transparent Synchronization Service

This section describes how to configure PasswordCourier Support Staff for use by the Transparent Synchronization service. It explains how to configure:

- One or more targets based on the PMM for Synchronization. In the example described in this section, the name of the target is **SIM01**.
- A synchronous reset target that includes all the Target IDs of the targets based on the PMM for Synchronization. In the example described in this section, the name of the group is **TRANSPARENTSYNC**.

Before you begin these procedures, complete these steps:

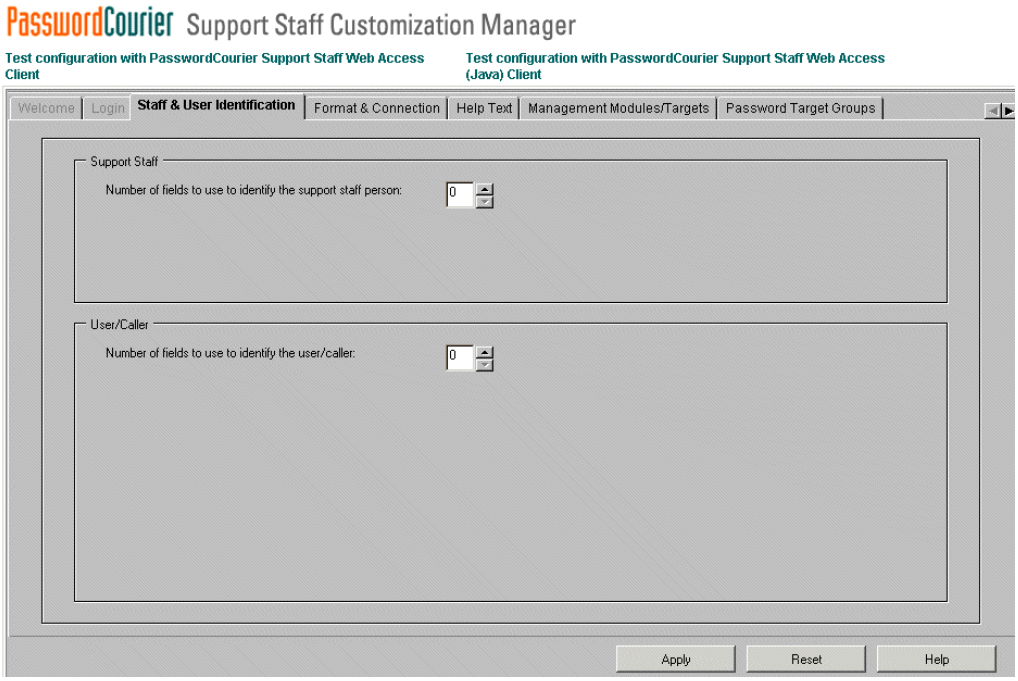
- Install and configure the PMM for each target type that you will use to synchronize password resets, such as the PMM for Windows NT and Windows 2000, the PMM for HP-UX, or the PMM for Novell NDS.
- Install and configure the PMM for Synchronization (see *"Synchronization" on page 101*.)
- Configure one target to correspond to each Transparent Synchronization Listener. These examples show these previously configured targets: MAINNET, and SAT-O1.

**Note:** In the examples that follow, the names of the Target IDs, the synchronous reset target, and the Transparent Synchronization Listeners correspond to the names of these elements in the sample configurations shown in *Figure 53*, *"Transparent Synchronization with User-based Targets"* and *Figure 54*, *"Transparent Synchronization Without User-based Targets"* .

To access the PasswordCourier Support Staff Customization Manager from a web browser, enter the URL of the Courion Server. From the Access Assurance Suite main page:

1. Click PasswordCourier.
2. From the PasswordCourier main page, click Support Staff Customization Manager.
3. Launch Support Staff Customization Manager.
4. Login using a valid user name and password.
5. Select the **STAFF & USER IDENTIFICATION** tab. The window in *Figure 55* appears. You need to disable Support Staff and User authentication. The Transparent Synchronization service uses the native password change for user authentication and validation.

**Figure 55: Staff and User Identification Window**



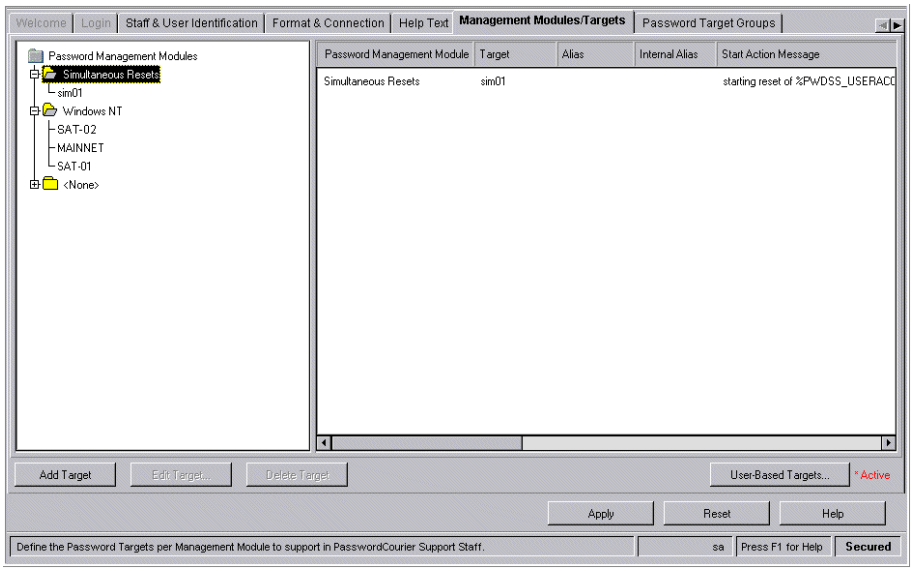

- **SUPPORT STAFF** — In the **NUMBER OF FIELDS TO USE TO IDENTIFY THE SUPPORT STAFF PERSON** field, enter 0. When you enter 0, the other options in this section of the screen disappear.
- **USER/CALLER** — In the **NUMBER OF FIELDS TO USE TO IDENTIFY THE USER/CALLER** field, enter 0. When you enter 0, the other options in this section of the screen disappear.
- Click the **APPLY** button. A warning box appears: *It is recommended to configure at least one field with validation to prevent unchallenged access to password resets*. Click the **OK** button in response to this warning.

6. Select the **MANAGEMENT MODULES/TARGETS** Tab. The steps that follow depend on whether you use User-based Targets or do not use them.

### *User-based Target Configuration*

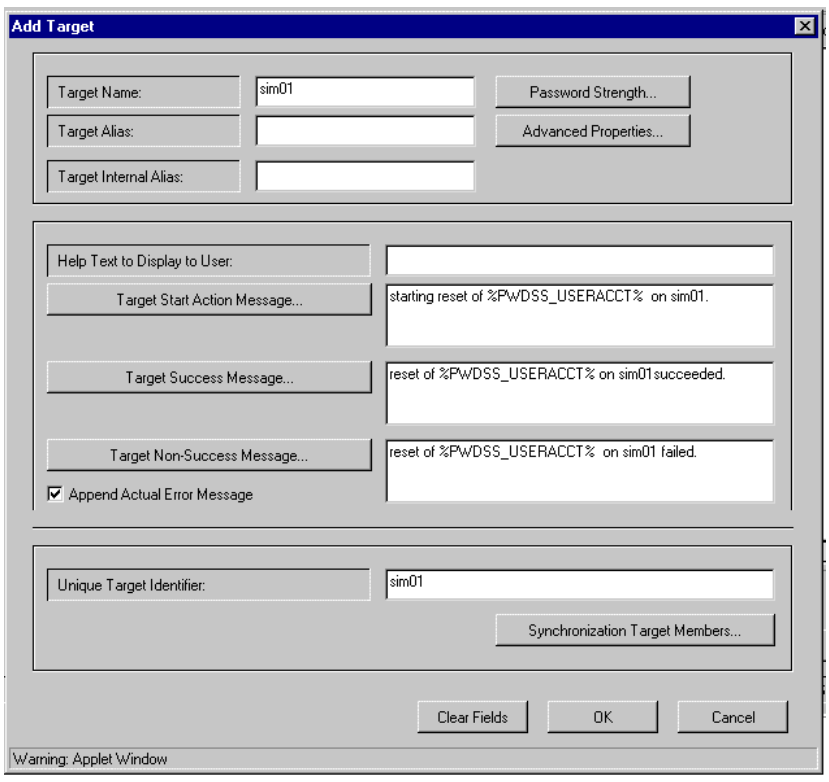
The Management Modules/Targets window in *Figure 56* appears.

**Figure 56: Management Modules/Targets Window (UBT)**



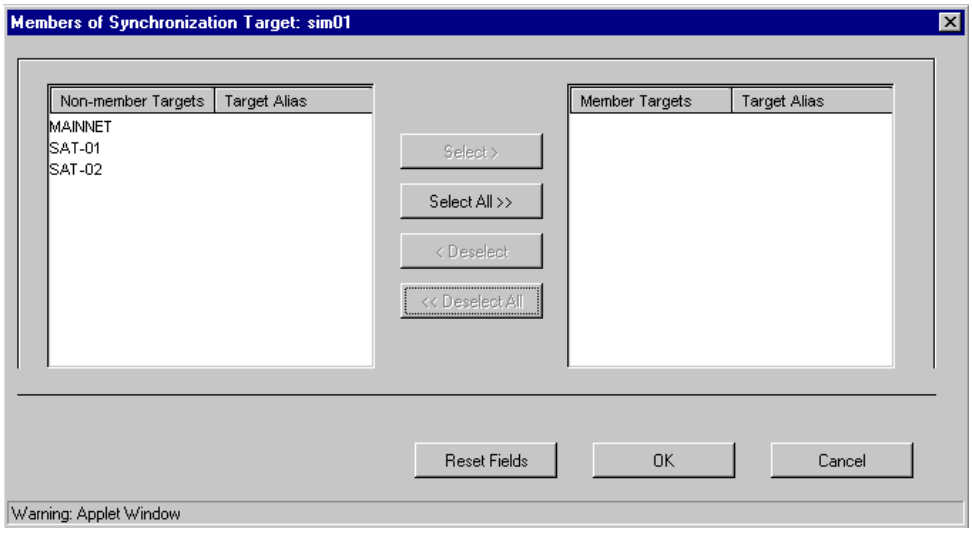

- Click User-based Targets. Follow the instructions in *"User-Based Targets" on page 62* for information about how to configure User-based Targets.
- Click **SIMULTANEOUS RESETS.**
- Click the **ADD TARGET** button. The Add Target dialog box appears as in *Figure 57*.

**Figure 57: Add Target Dialog Box (UBT)**



- **TARGET NAME** — Enter a target name such as **SIM01** to use as the Synchronous Reset Target ID name in the Transparent Synchronization Listener Configuration dialog box (see *Figure 71*). This name must match the Unique Target Identifier. Complete the rest of the Target information. For User-based Targets, ensure that the Unique Target Identifier matches the target name.
- **TARGET ALIAS** — If you specify a target alias in this dialog box, it must match the target alias you specify in the Listener Configuration dialog box (see *Figure 71* on page 123).
- Click the **SYNCHRONIZATION TARGET MEMBERS** button. The Members of Synchronization Target dialog box appears as in *Figure 58*.

**Figure 58: Synchronization Target Members Dialog Box**




- Select the target names in the Non-member Targets area and move them to the Member Targets area. Click the **OK** button.

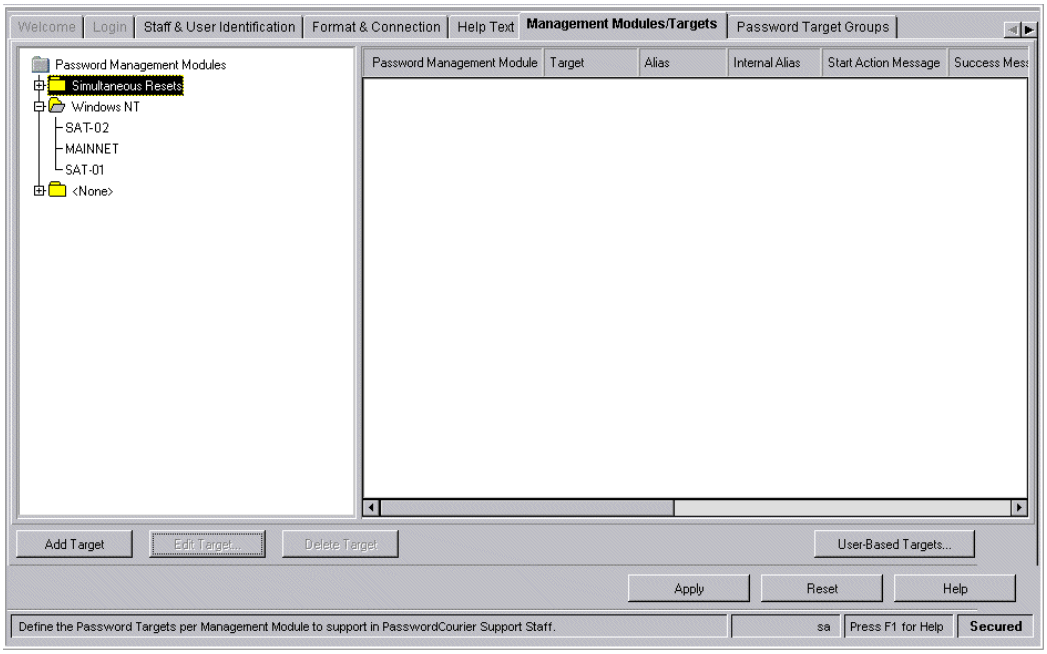
  Click the **OK** button when you have completed the Add Target dialog box**.** The **MANAGEMENT/MODULES TARGETS** window appears.
- Click the **USER-BASED TARGETS** button on the lower-right of the window. Configure a User-based Target data source.

  Click the **APPLY** button when you have configured the data source.
- Go to *"Adding a Password Target Group" on page 115*.

## *Configuration with Non User-based Targets*

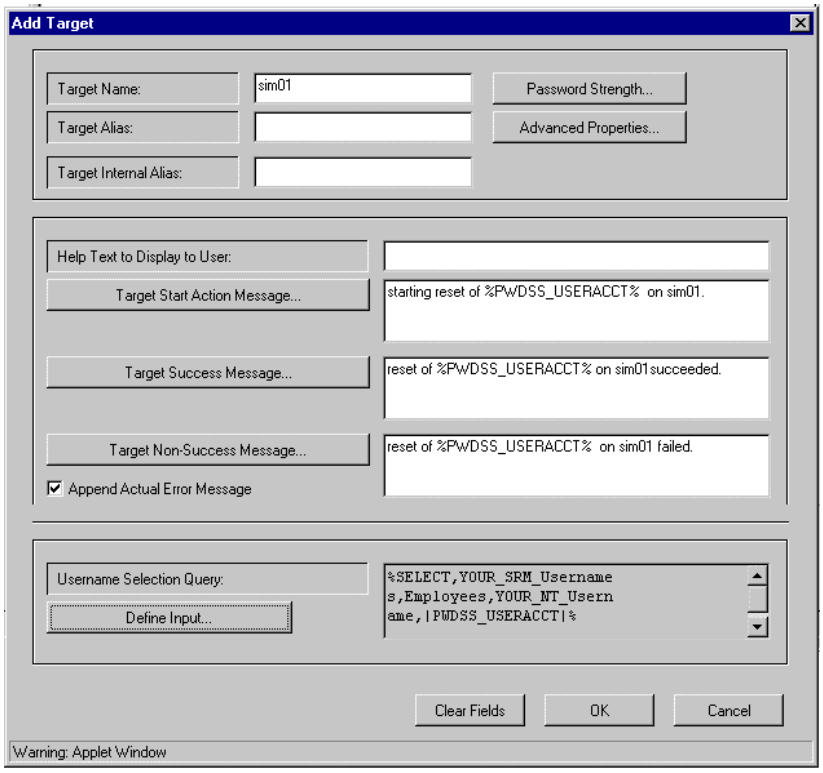
The Management Modules/Targets window in *Figure 59* appears.

**Figure 59: Management Modules/Targets Window (non-UBT)**




- Click Simultaneous Resets.
- Click the **ADD TARGET** button. The Add Target dialog box appears as in *Figure 57*.

**Figure 60: Add Target Dialog Box (non-UBT)**




- **TARGET NAME** — Enter a target name such as **SIM01** to use as the Synchronous Reset Target ID name in the Transparent Synchronization Listener Configuration dialog box (see *Figure 71*). Complete the rest of the Target information.

- **TARGET ALIAS** — If you specify a target alias in this dialog box, it must match the target alias you specify in the Listener Configuration dialog box (see *Figure 71* on page 123).
- Select the **DEFINE INPUT** button to create a query that results in a string of triplets as defined in the Synchronization Reset Module (see *"Synchronization Target Configuration" on page 44*).

  **Note:** In non-UBT mode, the Courion Server keys the Username Selection Query from the UserID passed to it from the native operating system password reset.

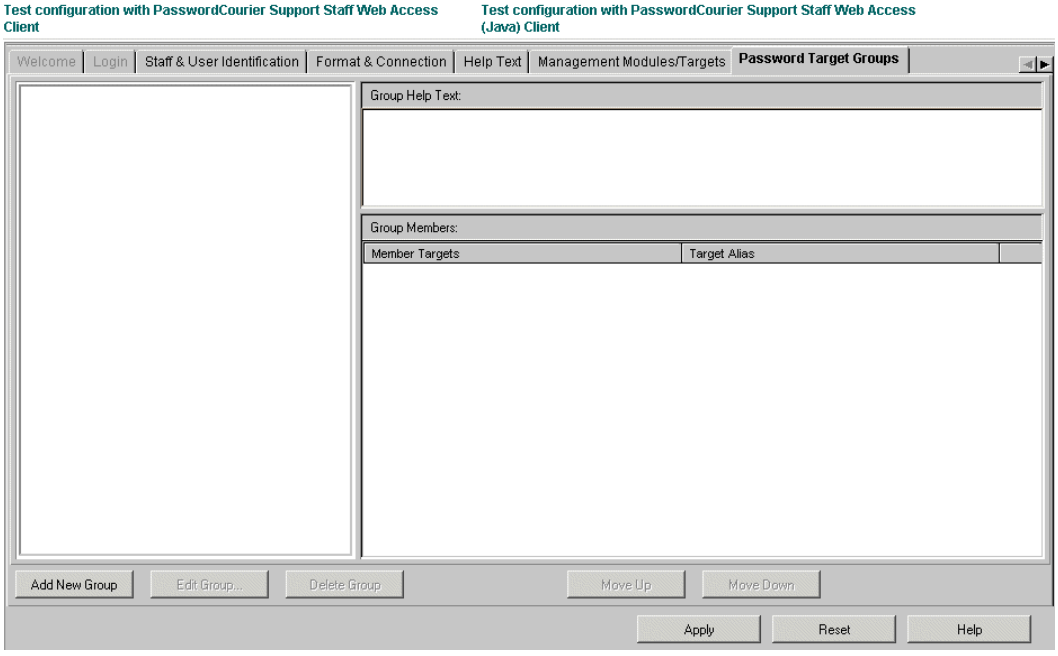
  Click the **OK** button when you have completed the Add Target dialog box**.** The **MANAGEMENT/MODULES TARGETS** window appears.

  Click the **APPLY** button. Continue with the section *"Adding a Password Target Group"*.

## *Adding a Password Target Group*

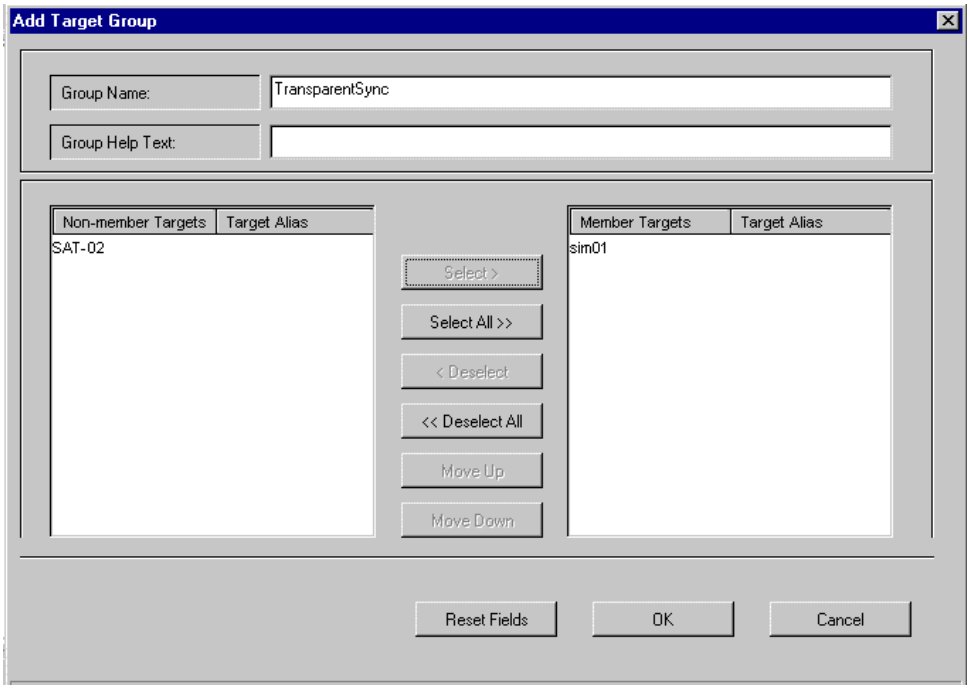
7. Select the **PASSWORD TARGET GROUPS** Tab. The Password Target Groups window appears as in *Figure 61*.

**Figure 61: Password Target Groups**




8. Click the **ADD NEW GROUP** button. Add a new group. This example uses a target group called TransparentSync. Make sure that all synchronization reset module targets for all Listeners are included in the Member Targets for this group. *Figure 62* shows an example of the Add Target Group dialog box.

**Figure 62: Add Target Group**




9. Click the **OK** button when you have completed the Add Target Group Dialog box. Close the PasswordCourier Support Staff Customization Manager window.

You can now add the targets you configured through PasswordCourier Support Staff to the list of configured Listeners on the Transparent Synchronization server through the Transparent Synchronization Configuration Manager.

# Managing the Transparent Synchronization and GAT Services

Installing the Transparent Synchronization feature includes two major steps: Installing the Global Arrester Table (GAT) service and Installing the Transparent Synchronization service. These components can reside on different Courion Servers or the same server. You can install these components in any order. These examples show the GAT service installed first.

**Note:** If the GAT service and the Transparent Synchronization service are on separate Courion Servers, they must share the same security pass phrase. To update the security pass phrase on a Courion Server from the Microsoft Windows Start menu, select:

Programs>Courion Access Assurance Suite>Courion Server>Configuration Manager

Click **NEXT** on the Access Key Selection dialog box. On the Site-specific Information dialog box, enter a pass phrase. Click **NEXT** through the remaining dialog boxes, and follow the instructions to accept changes.

After you install and configure the Transparent Synchronization service and the GAT service, you can manage these components through shortcuts on the Microsoft Windows Start menu. See *"Using the Start Menu to Manage the Transparent Synchronization Service and the GAT Service" on page 124*.

## Installing the GAT Service

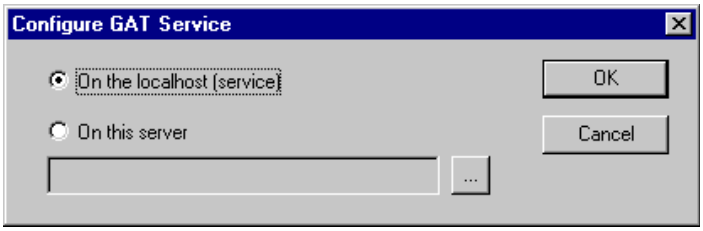
**Note:** In an environment with more than one Courion Server, one GAT service is used by all Courion Servers whether they use Transparent Synchronization or not.

To install the GAT service from the Microsoft Windows Start menu, select:

Programs>Courion Access Assurance Suite > Transparent Synchronization > Configure GAT Service

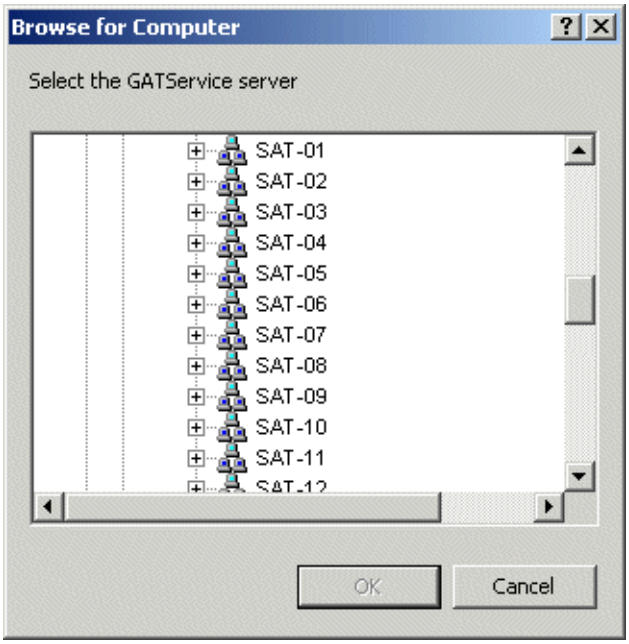
The Configure GAT Service dialog box appears, as in *Figure 63*.

**Figure 63: Configure GAT Service Dialog Box**




- To install the GAT Service on the host where you installed the Transparent Synchronization software, select **ON THE LOCALHOST (SERVICE)** and click **OK**. You can now install the Transparent Synchronization Service (see *"Installing the Transparent Synchronization Service" on page 121*).
- To browse the network for another host, select **ON THIS SERVER**. The browser window in *Figure 64* appears.

**Figure 64: Browse for Computer Window**




- Select a server from the list and click **OK**.

If you selected a Courion Server on the network, you must configure the GAT service on that server. From the Microsoft Windows Start menu on the Courion Server where you will install the GAT service, select:

Programs > Courion Access Assurance Suite > Transparent Synchronization > Configure GAT Service

The Configure GAT Service dialog box appears as in *Figure 63*. Select **ON THE LOCALHOST (SERVICE)** and click **OK**.

If your environment has only one Courion Server, continue with the steps in the section *"Installing the Transparent Synchronization Service" on page 121*.

## *Running the Distributed COM Configuration Utility in Environments with Multiple Courion Servers*

If you have more than one Courion Server in your networking environment, you need to choose one Courion Server to run the GAT Service. Then you need to configure the Distributed COM (DCOM) profile of the GAT service on that Courion Server to set the correct security parameters for that environment.

The dialog box used to change the DCOM profile is called "CourGATService Properties".

### Accessing the CourGatService Properties

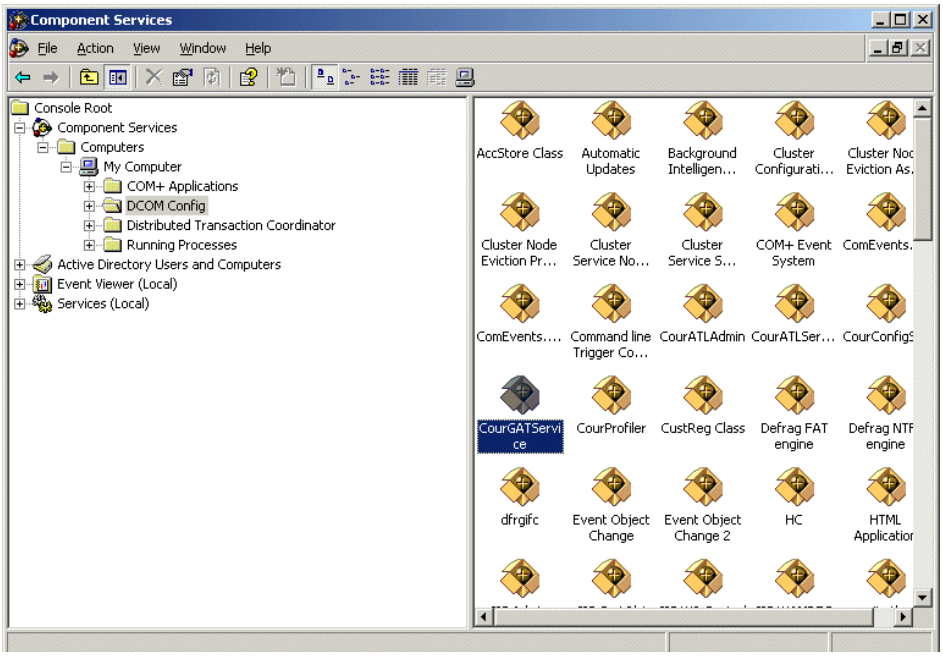
Launch the Component Services MMC snap-in on the server where you installed the GAT service:

1. From the Start Menu, select:

   Settings>Control Panel>Administrative Tools>Component Services

   This launches the MMC snap-in, show in *Figure 65*.

**Figure 65: MMC Snap-In**

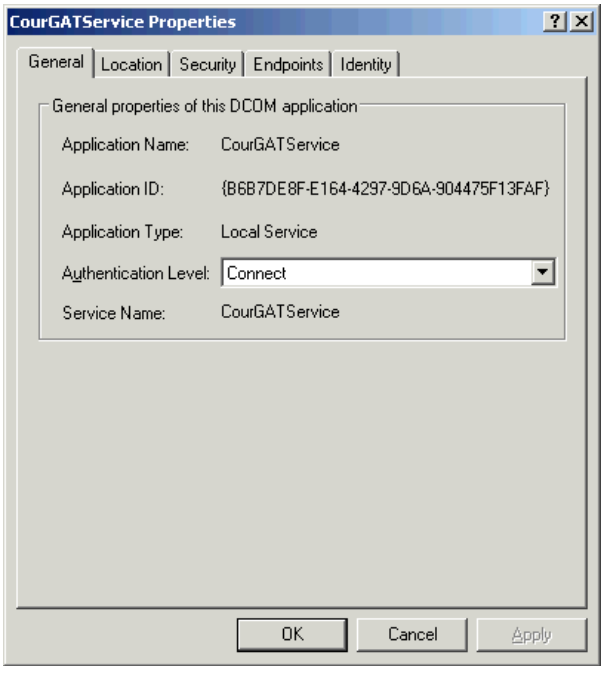



2. From the directory tree on the left side of the screen, select:

   Component Services>Computers>My Computer>DCOM Config

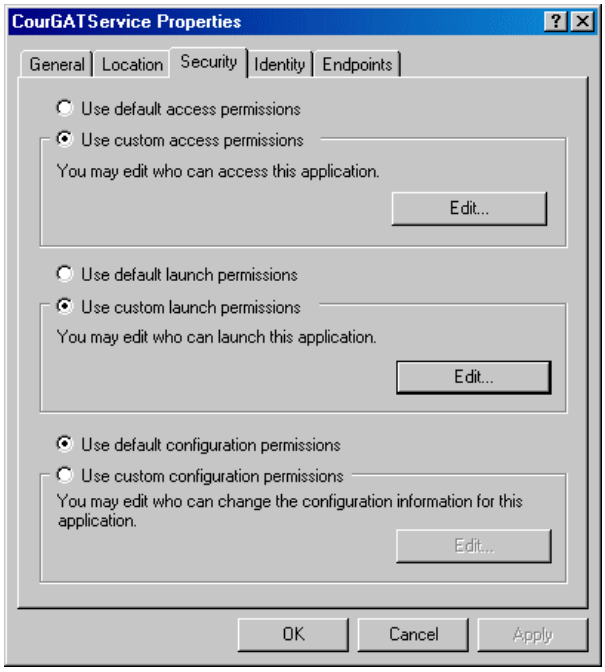
   On the container view in the right side of the screen, select CourGATService, right-click the mouse, and select Properties. The CourGATService Properties dialog box appears as in *Figure 66*.

**Figure 66: CourGATService Properties Dialog Box**



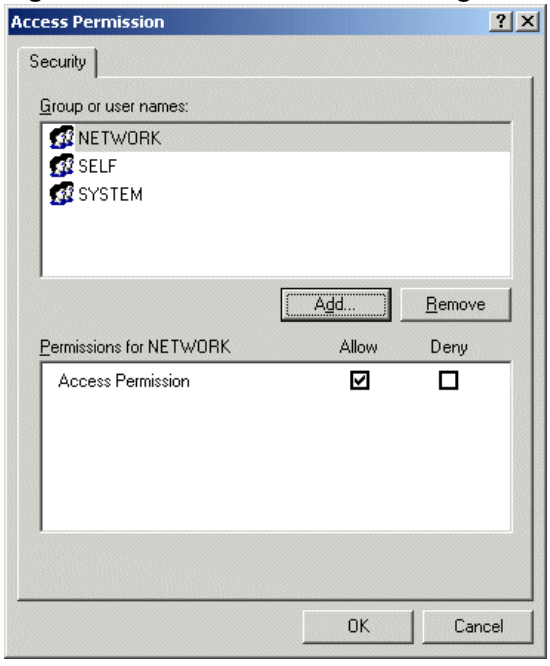

3. Select the **SECURITY** tab. The CourGATService security properties dialog box appears as in *Figure 67*.

**Figure 67: CourGATService Security Properties Dialog Box**



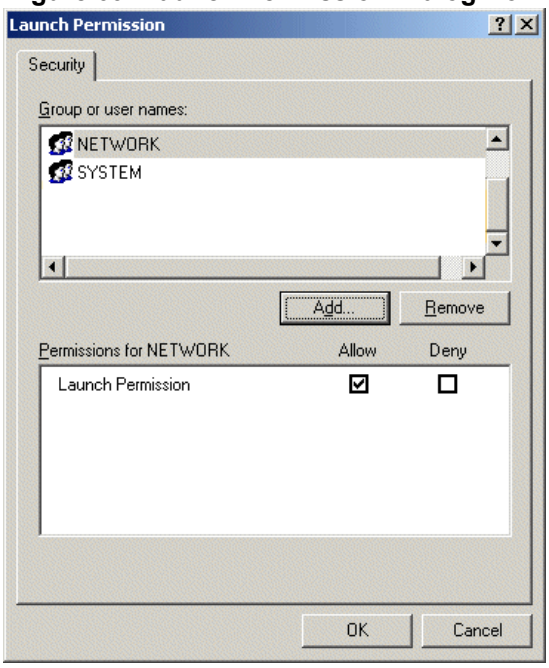

4. Select Use custom access permissions and click **EDIT...** The Access Permission dialog box appears as in *Figure 68*.

**Figure 68: Access Permission Dialog Box**




5. Ensure that the NETWORK user is on the list of **GROUP OR USER NAMES**. If it is not on the list, click **ADD...** and select the NETWORK user from the list of users and click **OK**. From the CourGATService Properties dialog box, select **USE CUSTOM LAUNCH PERMISSIONS** and click **EDIT...** The Registry Value LaunchPermission dialog box appears as in *Figure 69*.

**Figure 69: Launch Permission Dialog Box**




6. Check that the NETWORK user is on the list of names. If it is not on the list, click **ADD...** and select the NETWORK user from the list of users and click **OK**.
7. On the CourGATService Properties dialog box click **OK**.

You can now configure the Transparent Synchronization Service.

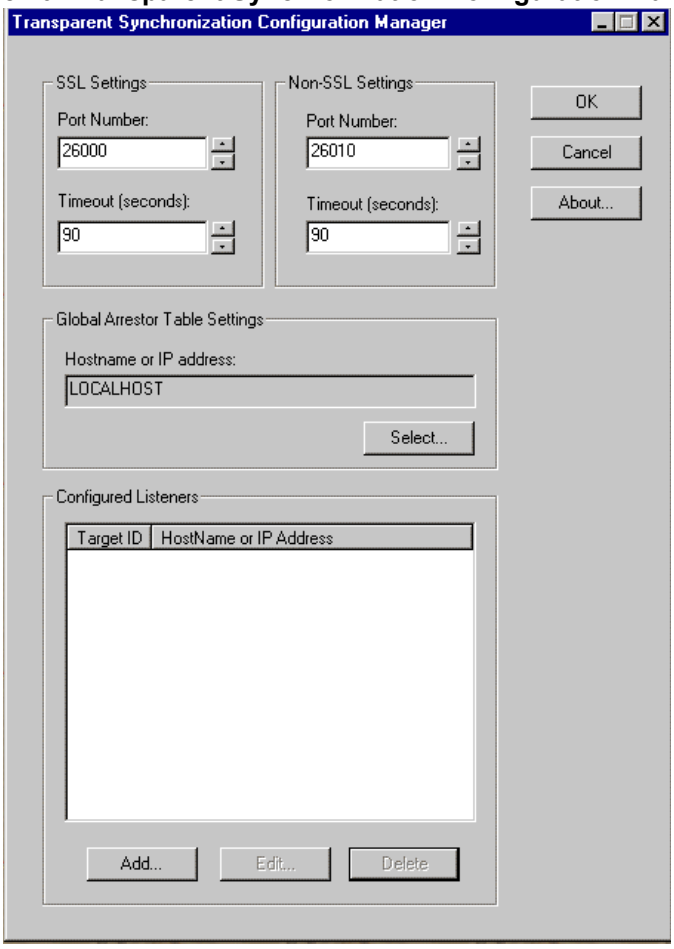
## Installing the Transparent Synchronization Service

From the Microsoft Windows Start menu, select:

Programs>Courion Access Assurance Suite>Transparent Synchronization>Install Transparent Synchronization Service

The Transparent Synchronization Configuration Manager dialog box appears as in *Figure 70*.

**Figure 70: Transparent Synchronization Configuration Manager**




**SSL SETTINGS** — The Secure Socket Layer (SSL) protocol ensures security for the communications between the Transparent Synchronization service and the Listener.

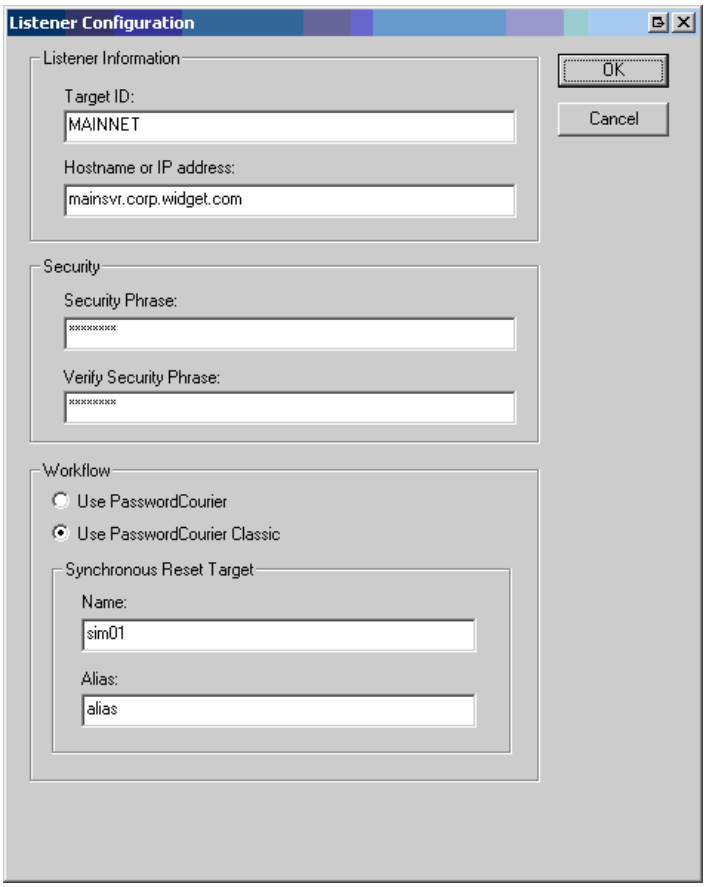
- **PORT NUMBER** — The port number you enter here must be the same as the port number in the Listener Configuration dialog box. (See *"Transparent Synchronization Listener Configuration" on page 128*.)
- **TIMEOUT (SECONDS)** — How long the Transparent Synchronization service waits for communication from the Listener before it assumes the Listener is unavailable and logs an error.

**NON-SSL SETTINGS** — (These settings do not apply to this version of the Access Assurance Suite).

**GLOBAL ARRESTOR TABLE SETTINGS** — This is the host name or IP address of the Courion Server where you installed the GAT service. LOCALHOST appears by default if you have not installed the GAT service or if you have installed the GAT service on this server. If you have not installed the GAT service and choose to do so now, click the **SELECT** button. The dialog box in *Figure 63* appears. Follow the instructions in the section *"Installing the GAT Service" on page 117* to complete this dialog box.

**CONFIGURED LISTENERS** — From the Configured Listeners section of the Transparent Synchronization Configuration Manager dialog box, click the **ADD** button to add a Listener. The Listener Configuration Dialog box appears as in *Figure 71*.

**Figure 71: Listener Configuration**




**LISTENER INFORMATION** — The Listener information you enter here corresponds to the information you enter in the Transparent Synchronization Listener Configuration dialog box when you install the Listener.

- **TARGET ID** — Enter the name of the target you created through PasswordCourier Support Staff Customization Manager. This is the name of the domain or workstation where the Listener software is installed. It must match the name of the Target ID in the Transparent Synchronization Listener Configuration dialog box (see *Figure 74* on page 128).
- **HOSTNAME OR IP ADDRESS** — Enter the hostname or IP address of the Target ID of the Listener on the domain controller (see *Figure 74* on page 128).

**SECURITY** — Enter the security phrase.

- **SECURITY PHRASE** — Enter a text string to use as a security phrase (128 characters maximum). This security phrase must match the security phrase that you enter in the Listener Configuration window in the Transparent Synchronization Listener Configuration dialog box (see page 128).

  Re-enter the security phrase in the **VERIFY SECURITY PHRASE** window.

**WORKFLOW** — Select **USE PASSWORDCOURIER CLASSIC**.

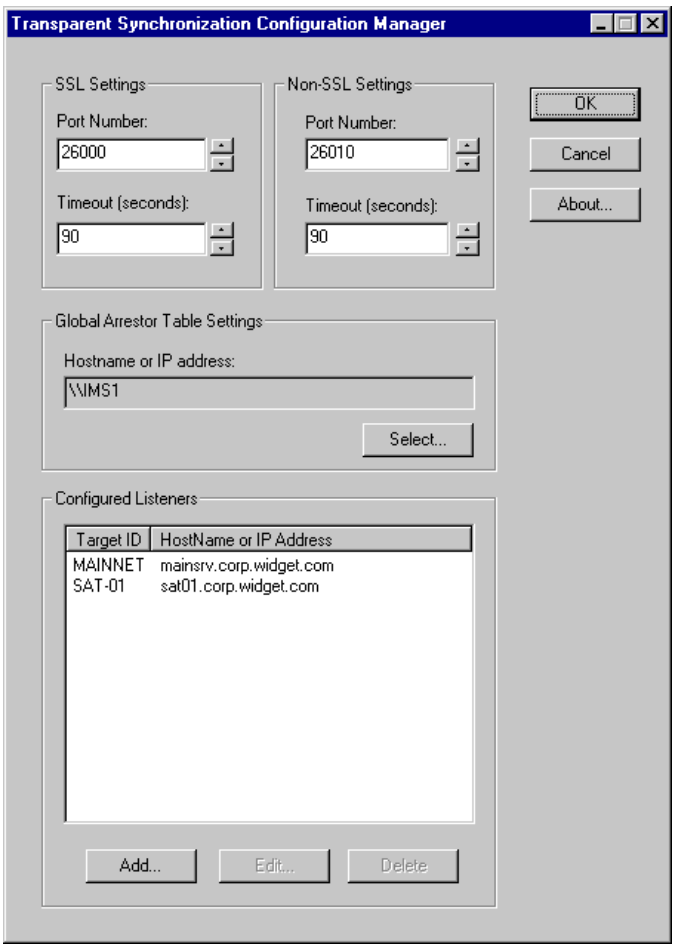
**SYNCHRONOUS RESET TARGET** — The information you enter here corresponds to the entered in the PasswordCourier Support Staff customization manager when you configured the targets (with our without UBT).

- **NAME** — This is the target name of the PMM for Synchronization target that you configured through the PasswordCourier Support Staff Customization Manager.
- **ALIAS** — If you specified a target alias in the Add Target dialog box of PasswordCourier Support Staff, enter the name of the target alias here.

Click **OK**.

Using the GAT server host name and Listener names in this example, the Transparent Synchronization Configuration Manager dialog box appears as in *Figure 72*.

**Figure 72: Transparent Synchronization Configuration Manager with Configured Listeners**




If you are satisfied with the configuration information, click **OK**.

## Using the Start Menu to Manage the Transparent Synchronization Service and the GAT Service

You can update the Transparent Synchronization service and the GAT service settings, or remove these services, through the Microsoft Windows Start menu.

To access these options from the Microsoft Windows Start menu, select:

Programs>Courion Access Assurance Suite>Transparent Synchronization

You can select these options:

**CONFIGURE GAT SERVICE** — Displays the Configure GAT Service Dialog box (*Figure 63*) and allows you to specify a GAT server.

**INSTALL TRANSPARENT SYNCHRONIZATION SERVICE** — Installs the Transparent Synchronization service and displays the Transparent Synchronization Configuration Manager dialog box (*Figure 70*). Use this option for first-time installations or after you have removed the Transparent Synchronization Service and want to re-install it.

**REMOVE GAT SERVICE** — Removes the GAT service from the Courion Server where you installed it. Removing the GAT service disables the Transparent Synchronization feature.

**REMOVE TRANSPARENT SYNCHRONIZATION SERVICE** — Removes the Transparent Synchronization service from the Courion Server where you installed it. Removing the Transparent Synchronization service disables this feature.

**TRANSPARENT SYNCHRONIZATION CONFIGURATION MANAGER** — Displays the Transparent Synchronization Configuration Manager dialog box. Use this option to modify information associated with the Transparent Synchronization service.

# Installing and Configuring the Transparent Synchronization Listener

This section explains how to install and configure the Transparent Synchronization Listeners.


- *"Transparent Synchronization Listener for Microsoft Windows" on page 126*
- *"Transparent Synchronization Listener for i5/OS" on page 131*
- *"Errors Returned by the Transparent Sync Listener" on page 147*


For general definition of the Transparent Synchronization Listener and functionality details, see *"The Transparent Synchronization Listener" on page 106*.

## Transparent Synchronization Listener for Microsoft Windows

A copy of the Transparent Synchronization Listener runs on each domain controller in any domain where you want to detect password changes and use Transparent Synchronization to synchronize your targets. Install the Listener on backup domain controllers if they exist.

### *Requirements*

Install the latest version of the Microsoft XML Core Services (MSXML). To download MSXML go to:

```
http://www.microsoft.com/downloads
```

Reboot the computer after the installation is complete.

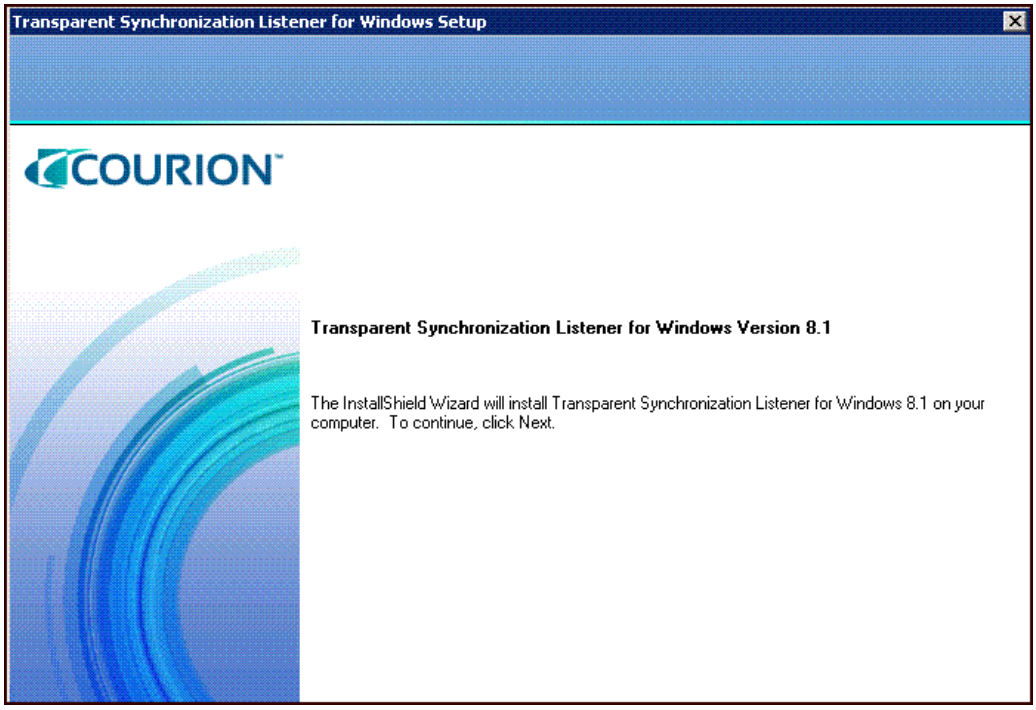
### *Installing the Listener*

To Install the Listener:

1. Locate the folder for the Listener software in the following subdirectory on the Courion Server where you installed the Transparent Synchronization software. This example shows the location of the MIcrosoft Windows listener:

   C:\Program Files\Courion Corporation\Listeners\Windows
2. Copy the folder to the domain controller or workstation where you want to install the Listener or launch the Listener setup.exe file from the network.
3. Launch the setup.exe file. The Transparent Synchronization Listener for Windows Install Shield Wizard appears as in *Figure 73*.

**Figure 73: Transparent Synchronization Listener Install Shield Wizard**




4. Click Next and follow the Installation Wizard instructions.
5. Reboot the computer after the installation is complete.

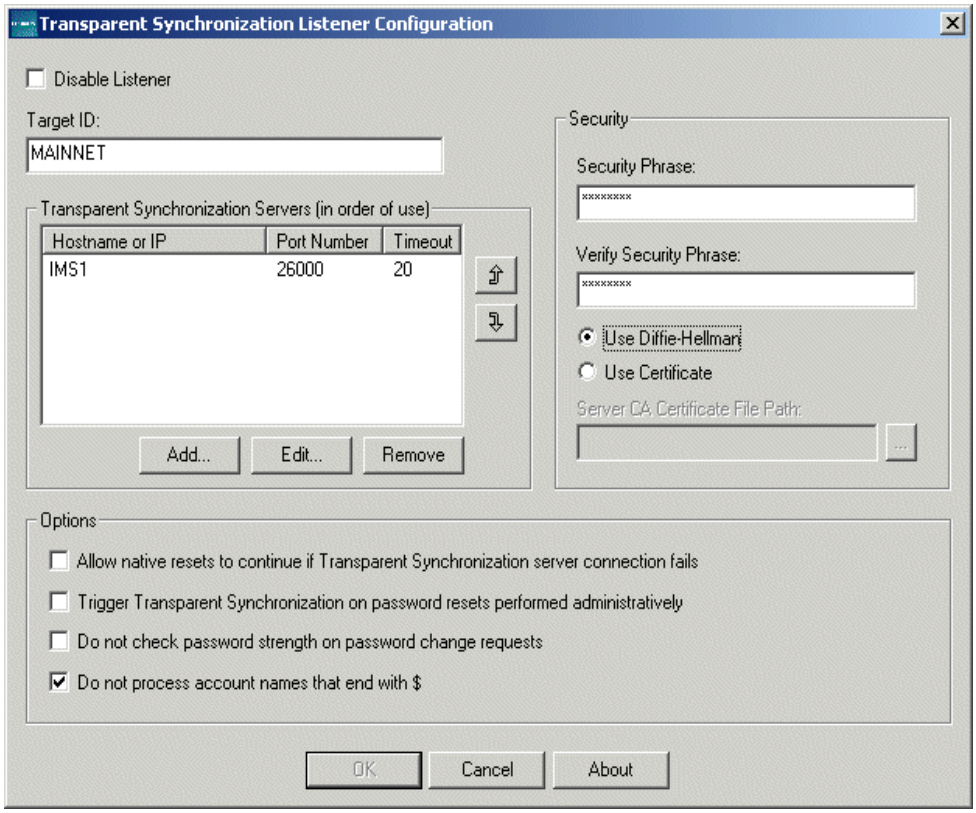
### *Configuring the Listener*

To configure the listener, from the Microsoft Windows Start menu, select:

Programs>Courion Access Assurance Suite>Transparent Synchronization>Transparent Synchronization Listener for Windows

The Transparent Synchronization Listener Configuration dialog box appears as in *Figure 74*.

**Figure 74: Transparent Synchronization Listener Configuration**




**DISABLE LISTENER** — The Disable Listener checkbox appears in the upper right corner of *Figure 74*. By default, it is checked (enabled) the first time you run the Listener configuration. When it is checked, the Listener does not perform password resets. Uncheck this box if you want to activate this Listener.

**TARGET ID** — This is the name of the computer or domain where you are installing this listener. If it is a computer name, use UNC format (\\mymachine). This must match the name in the Target ID field in the Listener Configuration dialog box of the Transparent Synchronization Configuration Manager (see page 123).

**Note:** Each server associated with this listener must have the same Target ID.

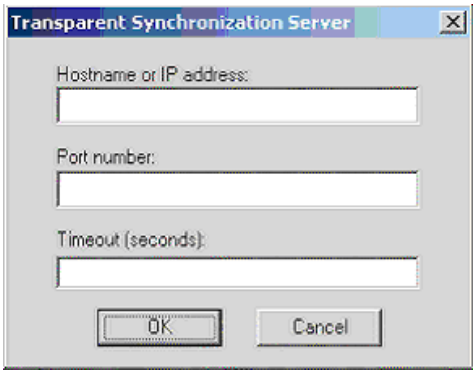
**TRANSPARENT SYNCHRONIZATION SERVERS (IN ORDER OF USE)** — This feature allows you to specify multiple Transparent Synchronization servers and the priority of use for these servers. You can associate more than one Transparent Synchronization server with the same listener to provide redundancy in case the primary server fails.

To add a server:

1. Click the **ADD** button.

   The Server Configuration dialog box appears as in *Figure 75*

**Figure 75: Transparent Synchronization Server Configuration**




- **HOSTNAME OR IP ADDRESS** — Enter the hostname or IP address of the Transparent Synchronization server associated with the Listener.
- **PORT NUMBER** — Enter the port number on the Transparent Synchronization server where the Listener will send notifications of password resets. This port number must match the port number that you specify under SSL Settings on the Transparent Synchronization Configuration Manager dialog box (see page 123).
- **TIMEOUT (SECONDS)** — How long the Listener waits for communication from the Transparent Synchronization service before it assumes the Transparent Synchronization service is unavailable and logs an error.

2. Click OK.

   The new server name appears in the list of Transparent Synchronization servers. Repeat this process to add more servers.

When you add more servers, the servers appear in the list in the order that you added them. The primary server is the first in the list. In the event that the listener cannot communicate with this server, the listener automatically begins using the next server in the list. To change the order of the servers in the list, single click the server name or IP address and click the up or down arrows.

Double clicking on a server in the list causes the Transparent Synchronization Server configuration box to appear.

You can edit server configuration parameters or remove a server from this listener configuration with the **EDIT** and **REMOVE** buttons.

**SECURITY** — Enter security information.

- **SECURITY PHRASE** — Enter a text string to use as a security phrase (128 characters maximum). This security phrase must match the security phrase that you entered in the Listener Configuration window in the Transparent Synchronization service configuration (see page 123).
- Re-enter the security phrase in the Verify Security Phrase window.
- **USE CERTIFICATE OR USE DIFFIE-HELLMAN** — Select which method of authentication and encryption to use for communication between the Listener and the Transparent Synchronization service. Diffie-Hellman is the default. If you have a digital certificate to use for authentication and encryption between the Listener and the Transparent Synchronization service, select Use Certificate. Use the Server CA Certificate File Path dialog box to locate your certificate.

**OPTIONS** — Enable or disable password reset options (these options are disabled by default).

- **ALLOW NATIVE RESETS TO CONTINUE IF TRANSPARENT SYNCHRONIZATION SERVER CONNECTION FAILS** — When you select this option, password resets occur on the native operating system even if the listener cannot communicate with the transparent synchronization server. The native strength rules still apply in this case.
- **TRIGGER TRANSPARENT SYNCHRONIZATION ON PASSWORD RESETS PERFORMED ADMINISTRATIVELY** — When you select this option, password synchronization occurs when a system administrator resets a password (not only when a user performs a Ctrl-Alt-Delete, changes the password, and verifies the change).
- **DO NOT CHECK PASSWORD STRENGTH ON PASSWORD CHANGE REQUESTS** — This option ignores the PasswordCourier password strength settings in the PasswordCourier Customization Manager.
- **DO NOT PROCESS ACCOUNT NAMES THAT END WITH $** — This option allows the filtration of password change notifications for machine accounts in Active Directory and Microsoft Windows domains.

  To complete a Transparent Synchronization operation, entries must exist in the User—based target for the originating listener as well as the targets to be synchronized. Synchronization does not occur if a Transparent Synchronization listener detects a reset but no corresponding entries exist for the targets to be synchronized. Entries of log messages are made in the Courion log files following a Transparent Synchronization operation.

  If your Active Directory domain or Microsoft Windows domain contains a significant number of machines, then the number of entries logged in the Courion log files could be significantly high. Since machine accounts end with “$”, enabling this option would eliminate the log entries for machine accounts and substantially reduce the size of the log files.

  This option is checked (enabled) by default.

Click **OK** when you have completed this dialog box.

# Transparent Synchronization Listener for i5/OS

The Transparent Synchronization Listener installed on i5/OS® systems detects the native i5/OS operating system's password change events, and propagates them to the Courion Server for synchronization with a range of targets.

## *Requirements*

Requirements for the Transparent Synchronization Listener (TSL) for i5/OS:

- Install i5/OS or OS/400 V5R1 or higher
- Install and configure the Password Management Module (PMM) Agent for i5/OS
- FTP capabilities to the i5/OS system

## *Installing the TSL for i5/OS*

To install the Transparent Synchronization Listener (TSL) for i5/OS the user profile used in the install process needs to have *SECADM and *ALLOBJ special authorities. Courion recommends using QSECOFR during the installation process. To install the Transparent Synchronization Listener for i5/OS:

1. Sign on to the i5/OS as QSECOFR or a user profile with *ALLOBJ and *SECADM authority.
2. End PMM Agent for i5/OS
   a. Display the PMM Agent for i5/OS menu by entering: (*Figure 76*)

      `GO COURAGENT/PMMMNU`

**Figure 76: PMM Agent for i5/OS (OS/400) Menu**

```
PMMMNU                    PMM Agent for OS/400 Menu
                                                          System:    OS400A
Select one of the following:

     1. Start PMM Agent for OS/400
     2. End PMM Agent for OS/400
     3. Configure PMM Agent for OS/400
     4. Maintain Excluded Profiles
     5. Purge Message and Output Queues
     6. Print Configuration Files
     7. Print Message Queue
     8. Display Message Queue
     9. Display Output Queue

    90. Sign Off



Selection or command
===> ____________________________________________________________________
F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
COPYRIGHT (C) 2002 COURION CORPORATION.
```

   b. Select **END PMM AGENT FOR OS/400** and press **ENTER** to confirm.

c. Enter the following command to ensure that the PMM Agent for i5/OS is not active. (*Figure 77* displays the PMM Agent for i5/OS with active jobs).

```
WRKUSRJOB USER(COURAGENT) STATUS(*ACTIVE)
```

**Figure 77: PMM Agent for i5/OS Active Jobs**

```
                              Work with User Jobs                        OS400A
                                                          02/27/02  15:07:33
Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect

Opt  Job         User        Type     -----Status-----  Function
__   QJVACMDSRV  COURAGENT   BATCHI   ACTIVE
__   QZRCSRVS    COURAGENT   BATCHI   ACTIVE
__   SSLAG08191  COURAGENT   BATCH    ACTIVE            CMD-STRPMM

                                                                        Bottom
Parameters or command
===> ____________________________________________________________________________
F3=Exit      F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display schedule data
F12=Cancel   F17=Top     F18=Bottom   F21=Select assistance level
Intermediate assistance level used.
```

3. There should not be any active jobs for COURAGENT (*Figure 78*)

**Figure 78: PMM Agent for i5/OS Inactive Jobs**

```
                              Work with User Jobs                        OS400A
                                                          02/27/02  15:53:28
Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect

Opt  Job         User        Type     -----Status-----  Function

  (No jobs to display)

                                                                        Bottom
Parameters or command
===> ____________________________________________________________________________
F3=Exit      F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display schedule data
F12=Cancel   F17=Top     F18=Bottom   F21=Select assistance level
```

4. Press **F3** until you exit the PMM Agent for i5/OS menu.
5. Enter the following command to launch a Command Entry screen:

```
CALL QCMD
```

6. Grant temporary authority

   a. The COURAGENT user profile temporarily needs authority to the RSTLIB and RST commands.

      **Note:** The install process requires access to the COURAGENT user profile.

   b. Temporarily grant authority to the RSTLIB and RST commands to COURAGENT to perform product restore operations.

```
GRTOBJAUT OBJ(RSTLIB) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*USE)
```

```
GRTOBJAUT OBJ(RST) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*USE)
```

c. Sign off as QSECOFR or the user ID used to make the changes.

7. FTP the save-file (.savf) file to the i5/OS

   a. Sign on to the i5/OS as COURAGENT.

   **Note:** it is important that the FTP, RST and RSTLIB commands issued below be done under the COURAGENT user profile. The system will not be set up correctly if the administrator configuring it does not sign on as COURAGENT.

   b. Create a save file in QGPL

   ```
   CRTSAVF QGPL/COURTSL
   ```

   The extracted i5/OS programs are delivered in a *SAVF file and must be uploaded to the i5/OS system.

   c. Copy the COURTSL.savf file from the Access Assurance Suite install directory (OS400 subfolder) to the root directory of C:\ on your Windows NT/ 2000/XP system.

   d. Using FTP, enter the following commands from the PC where the COURTSL.savf file is stored and perform the following steps:

   ```
   FTP myAS400ipAddress
   User: COURAGENT
   Password: (COURAGENT password)
   cd QGPL
   lcd C:\
   binary
   put COURTSL.savf COURTSL
   quit
   ```

8. Restore the TSL for i5/OS product library

   a. On the i5/OS, signed on as COURAGENT, issue this restore command:

   ```
   RSTLIB SAVLIB(COURTSL) DEV(*SAVF) SAVF(QGPL/COURTSL)
   OUTPUT(*PRINT)
   ```

9. Run the TSL for i5/OS installation program

   ```
   CALL COURTSL/INSTALLTSL
   ```

   This step will:

   - restore the pmm400.jar file
   - delete the QGPL/COURTSL save-file
   - grant *PUBLIC *USE authority to the product library COURTSL.

10. Configure the TSL for i5/OS. See *"Configuring the TSL for i5/OS" on page 135*. Save your configuration and press **F3** to return to the PMM agent for i5/OS menu.

11. Start the PMM Agent for i5/OS

    a. Enter the command: (*Figure 76*)

    ```
    GO COURAGENT/PMMMNU
    ```

    b. Select **START PMM AGENT FOR OS/400**

    This command will submit the PMM Agent for i5/OS to the job queue you specified in the configuration.

12. Revoke Temporary Authority

After installing the TSL for i5/OS, you can remove the temporary authority you granted to the RSTLIB and RST commands.

a. Sign off as the user COURAGENT

b. Sign on again as QSECOFR, or a user profile with *ALLOBJ and *SECADM authority.

c. Revoke the authority you gave to COURAGENT to restore objects:

```
RVKOBJAUT OBJ(RSTLIB) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*ALL)
```

```
RVKOBJAUT OBJ(RST) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*ALL)
```

13. Configure the i5/OS system values

The instructions below include details about how to set the QPWDVLDPGM system value to *REGFAC, and how to add the exit point programs using the WRKREGINF command.

a. Signed on as QSECOFR or a user profile with *ALLOBJ and *SECADM authority, display the current system value:

```
DSPSYSVAL SYSVAL(QPWDVLDPGM)
```

b. Save the displayed system value for your records.

c. If the QPWDVLDPGM system value is not already set to *REGFAC, then change it:

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
```

d. Work with registration information for QIBM_QSY_VLD_PASSWRD exit point: (*Figure 79*)

```
WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD)
```

**Figure 79: Work with Registration Information**

```
                        Work with Registration Information

Type options, press Enter.
  5=Display exit point   8=Work with exit programs

                            Exit
    Exit                    Point
Opt Point                   Format    Registered  Text
 8  QIBM_QSY_VLD_PASSWRD    VLDP0100     *YES     Validate Password

                                                                  Bottom
Command
===> ____________________________________________________________________
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

e. Select option 8 = **WORK WITH EXIT PROGRAMS**. (*Figure 80*)

Add the exit point programs TSLPSR and TSLTSR. If other exit point programs exist, then change the keyword PGMNBR() sequence so that the TSLPSR exit point program executes before any other exit point program, and TSLTSR executes after all other exit point programs.

**Figure 80: Work with Exit Programs**

```
                          Work with Exit Programs

Exit point:   QIBM_QSY_VLD_PASSWRD     Format:   VLDP0100

Type options, press Enter.
  1=Add   4=Remove   5=Display   10=Replace

              Exit
            Program     Exit
Opt          Number     Program        Library
__                      __________     __________
__               30     CHGPWDEXIT     QGPL

                                                                    Bottom
Command
===> ____________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel
```

In the example below, the TSLPSR and TSLTSR exit point programs are added, and the keyword PGMNBR() sequence is set to 20 and 40 respectively.

Enter the following two commands at the command line:

```
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD)FORMAT(VLDP0100)
      PGMNBR(20)PGM(COURTSL/TSLPSR)
      TEXT('TSL for OS/400 Password Strength Request')
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD)FORMAT(VLDP0100)
      PGMNBR(40)PGM(COURTSL/TSLTSR)
      TEXT('TSL for OS/400 Transparent Sync Request')
```

**Note:** The TSLPSR is the exit point program to indicate a Password Strength Request (PSR). The TSLTSR is the exit program to indicate a Transparent Sync Request (TSR).

14. Sign off as QSECOFR. The TSL for i5/OS configuration is now complete.

## *Configuring the TSL for i5/OS*

Once the Transparent Synchronization Listener (TSL) for i5/OS has been installed, it is ready for configuration. To configure the listener, you must be signed on as COURAGENT. Enter the command:

```
GO COURTSL/TSLMNU
```

The TSL for i5/OS Menu appears as in *Figure 81*.

## TSL for i5/OS (OS/400) Menu

**Figure 81: TSL for i5/OS (OS/400) Menu**

```
TSLMNU                          TSL for OS/400 Menu
                                                                 System:   XXXXXXX
Select one of the following:

     1. Maintain the TSL configuration
     2. Maintain TSL specific excluded profiles
     3. Purge log file
     4. Print the TSL configuration
     5. Print log file
     6. Display output queue

    90. Sign Off





Selection or command
===> ____________________________________________________________________________
F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
COPYRIGHT (C) 2004 COURION CORPORATION.
```

In *Figure 81*, you can either select the menu option or type the command for each option at the command line. See Table 18 for the menu options and the corresponding commands to execute.

### TSL for i5/OS Menu Commands

**Table 18: TSL for i5/OS Menu Commands**

| Option # | Menu Options | Command to Execute |
|---|---|---|
| 1 | Maintain the TSL Configuration | TSLMNTCFG |
| 2 | Maintain TSL Specific Excluded Profiles | CALL TSLMNTEXPC |
| 3 | Purge Log File | TSLPRGLOG |
| 4 | Print the TSL Configuration | TSLPRTCFG |
| 5 | Print Log File | TSLPRTLOG |
| 6 | Display Output Queue | WRKOUTQ TSLOUTQ |
| 90 | Sign Off | SIGNOFF |

### Maintain the TSL Configuration

When you select **MAINTAIN THE TSL CONFIGURATION** in *Figure 81*, the configuration screen appears as in *Figure 82*. This screen allows you to configure the TSL for i5/OS.

**Figure 82: TSL for i5/OS Configuration (1 of 3)**

```
                    Maintain the TSL Configuration (TSLMNTCFG)

Type choices, press Enter.

Library where installed  . . . . > COURTSL       Name
TSL enabled  . . . . . . . . . .   *YES          *YES, *NO
Trace enabled  . . . . . . . . .   *NO           *YES, *NO
Use PMM excluded profiles  . . .   *NO           *YES, *NO
Process native if connect fail     *YES          *YES, *NO
Enforce password rules in PWC  .   *YES          *YES, *NO
TSL client settings:
  Port . . . . . . . . . . . . .   08902        1024-65536
  Timeout  . . . . . . . . . . .   00010        SECONDS
  Retry attempts . . . . . . . .   01           01-99

                                                                      More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

**LIBRARY WHERE INSTALLED** — Displays the name of the current library where the product TSL for i5/OS is installed. This is a read-only field.

**TSL ENABLED** — This option allows you to decide whether or not to allow the TSL for i5/OS to process password change requests. The default value for this option is ***NO.**

**TRACE ENABLED** — This option allows you to decide whether or not to allow the Transparent Synchronization Listener (TSL) Validate Password Exit Program to produce trace level debugging information. The default value for this option is ***NO.**

**USE PMM EXCLUDED PROFILES** — This option allows you to decide whether or not to allow the TSL Validate Password Exit Program to pass requests to change passwords for the profiles that have been specified for exclusion on the PMM Agent for i5/OS on to the Transparent Synchronization Service. The default value for this option is ***NO**.

If you select ***YES**, the TSL Validate Password Exit Program will check for profiles that have been excluded on the TSL for i5/OS, and will also check for user profiles that have been excluded on the PMM Agent for i5/OS.

If you select ***NO**, only the profiles specified on the TSL for i5/OS will be excluded.

**PROCESS NATIVE IF CONNECT FAILS** — This option controls what happens to a password change in the event of a communications failure. The default value for this option is ***YES**.

If you select ***YES**, then any communications failure between the TSL Validate Password Exit Program and the Listener for i5/OS Communication Module, or the Listener for i5/OS Communication Module and the Transparent Synchronization Service will still process a native password change successfully in i5/OS.

If you select ***NO**, then any communications failure between the TSL Validate Password Exit Program and the Listener for i5/OS Communication Module, or the Listener for i5/OS Communication Module and the Transparent Synchronization Service will not process a native password change in i5/OS.

**ENFORCE PASSWORD RULES IN PWC** — This option controls whether or not to enforce the password strength rules specified in PasswordCourier when changing a password. The default value for this option is ***YES**.

If you select ***YES**, the PasswordCourier password strength rules will be used before changing a password. If you select ***NO**, the PasswordCourier password strength rules will not be applied for a password change. The **NO** option can speed up processing of password changes.

**Note:** The TSL for i5/OS detects the native password change event on the i5/OS system. Upon detecting this password change, the TSL Validate Password Exit Program captures the username and password information and begins the communication exchange to the Transparent Synchronization Service. Before the TSL Validate Password Exit Program communicates the exchange to the Transparent Synchronization Service, the password may be forced to uppercase depending on the password level (QPWDLVL). If your i5/OS QPWDLVL system value is set to 0 or 1, then all i5/OS passwords are captured in uppercase, regardless of how the user has entered the password. If the QPWDLVL system value is set to 2 or 3, then all i5/OS passwords are captured in mixed case (upper and lower) — exactly based on the case the user has entered.

For example, if you select ***YES,** the password is checked against the PasswordCourier password strength rules. If a password strength rule says that one or more characters must be in lowercase, then that rule will not pass if QPWDLVL is set to 0 or 1. You must give special consideration when configuring Password Strength check, since the QPWDLVL system value determines if lowercase is to be allowed in i5/OS passwords. For more information on password strength rules, please refer to *"Password Strength"*. For more information on QPWDLVL, please see the appropriate i5/OS manual.

**TSL CLIENT SETTINGS** — This option is specific to the TSL Validate Password Exit Program and the Listener for i5/OS Communication Module.

- **Port** — The port on which the Listener for i5/OS Communication Module will talk to the TSL Validate Password Exit Program. The default value is 08902.
- **Timeout** — The time out in seconds for the Listener for i5/OS Communication Module when it attempts to communicate with the TSL Validate Password Exit Program. The default value is 00010.
- **Retry attempts** — The number of attempts the TSL Validate Password Exit Program will make to communicate with the Listener for i5/OS Communication Module. The default value is 01.

**Note:** If you make any changes to the TSL client settings, then you must stop and restart the PMM Agent for i5/OS.

Press the **PAGE DOWN** key on your keyboard. The second screen for the menu option **MAINTAIN THE TSL CONFIGURATION** appears as in *Figure 83*.

**Figure 83: TSL for i5/OS Configuration (2 of 3)**

```
                    Maintain the TSL Configuration (TSLMNTCFG)

 Type choices, press Enter.

 TSL server settings:
   Server name  . . . . . . . . .   '192.168.1.5'
_____________________________________________________________
_______
   Port . . . . . . . . . . . . .   26000          1024-65536
   Timeout  . . . . . . . . . . .   00005          SECONDS
                + for more values _
```

**TSL SERVER SETTINGS** — This option allows you to specify values for the Transparent Synchronization Service.

**Note:** You can provide information for up to 10 servers. If you enter details for a particular server, then all the of the options must be filled.

- **SERVER NAME** — This is the host name or the IP address that the Listener for i5/OS Communication Module uses to communicate with this server.
- **PORT** — The port on which the Listener for i5/OS Communication Module will communicate with the Transparent Synchronization Service. You can configure up to 10 ports.
- **TIMEOUT —** The time out in seconds for the Listener for i5/OS Communication Module when it attempts to communicate with the Transparent Synchronization Service. You can configure up to 10 timeouts.

**Note:** If you make any changes to the TSL server settings, then you must stop and restart the PMM Agent for i5/OS.

Press the **PAGE DOWN** key on your keyboard. The third screen for the menu option **MAINTAIN THE TSL CONFIGURATION** appears as in *Figure 83*.

**Figure 84: TSL for i5/OS Configuration (3 of 3)**

```
                    Maintain the TSL Configuration (TSLMNTCFG)

Type choices, press Enter.

Target ID  . . . . . . . . . . .   server5

Security phrase  . . . . . . . .

Verify security phrase  . . . .









F3=Exit   F5=Refresh   F12=Cancel
```

**TARGET ID** — Enter the name of the system where the listener is installed. The system name must match the name entered in the Target ID field in the Listener Configuration dialog box of the Transparent Synchronization Configuration Manager. For more information about the Transparent Synchronization Configuration Manger, please see "*"Installing the Transparent Synchronization Service" on page 121*".

**Note:** Each server name associated with this listener must have the same Target ID.

**Note:** If you make any changes to the target id, then you must stop and restart the PMM Agent for i5/OS.

**SECURITY PHRASE** — Enter a text string to use as a security phrase (128 characters maximum). This security phrase must match the security phrase that you enter in the Listener Configuration window in the Transparent Synchronization Listener Configuration dialog box. For more information about the Transparent Synchronization Configuration Manger, please see "*"Installing the Transparent Synchronization Service" on page 121*".

**Note:** If you change the **SECURITY PHRASE** entry, another field will appear which will allow you to re-enter the security phrase to verify that it has been entered correctly.

**Note:** If you make any changes to the security phrase, then you must stop and restart the PMM Agent.

### Maintain TSL Specific Excluded Profiles

When you select **MAINTAIN TSL SPECIFIC EXCLUDED PROFILES** in *Figure 81*, the following screen is displayed (*Figure 85*).

This option allows you to prevent the TSL Validate Password Exit Program from forwarding password change requests to the Transparent Synchronization Service for specific user profiles.

**Figure 85: TSL for i5/OS Maintain Excluded Profiles**

```
 9/18/04                        TSL for OS/400                        XXXXXXXX
10:58:25            Maintain TSL Specific Excluded Profiles           USERIDXX

Type in additional profiles, blank out to remove.  Press Enter to update.

        Profile      Profile      Profile      Profile      Profile
        COURAGENT    COURAGSEC    Q*           ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________
        ________     ________     ________     ________     ________

                                  Page 1 of 4


F3=Exit   F5=Refresh   F8=Restore Defaults
```

**PROFILE** — The values you enter must be valid user profile names. The first character must be an alphabet or a special character ($, @, #). The remaining characters can be alphanumeric, a period, an underscore or a special character ($, @, #). The default values provided with this option are Q*, COURAGSEC, and COURAGENT.

**Note:** An exception to the “special characters” rule is the wildcard (*). The wildcard may only be used as the last character of a profile name. It allows you to specify a group of profiles, as defined by the characters preceding the wildcard (*) to be excluded. For example, if you specify K* or GR*, all profile names that begin with “K” or “GR” are excluded.

**Note:** You may exclude up to 200 user profiles.

**Note:** If you make any changes to the TSL specific excluded profiles, then you must stop and restart the PMM Agent for i5/OS.

### Purge Log File

When you select **PURGE LOG FILE** in *Figure 81*, the following screen appears (*Figure 86*).

This option allows you to purge some or all of the entries from the TSL for i5/OS Log file (TSLLOG).

**Figure 86: Purge Log File**

```
                         Purge Log File (TSLPRGLOG)

 Type choices, press Enter.

 #Days to retain information  . .   7____          1 - 365, *NONE
 Reorganize file after purge  . .   *NO___         *YES, *NO

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

**DAYS TO RETAIN INFORMATION** — Select ***NONE** to purge all records in the log file. If you enter a number from 1 through 365, the log file will retain log entries for those many days going back from the current date.

**Note:** If you make any changes to the number of days to retain information, then you must stop and restart the PMM Agent for i5/OS.

**REORGANIZE FILE AFTER PURGE** — This option controls whether or not the TSL for i5/OS log file will be reorganized after the records have been purged. Select ***YES** if you want to reorganize the log file.

### Print TSL Configuration

When you select **PRINT THE TSL CONFIGURATION** in *Figure 81*, the following screen appears (*Figure 87*).

This option creates a listing that shows the current TSL for i5/OS configuration parameters and their associated default values.

**Figure 87: Print the TSL Configuration**

```
                    Print the TSL Configuration (TSLPRTCFG)



 F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More
keys

 No parameters to show; press Enter to run, F3 to exit.
```

### Print Log File

When you select **PRINT LOG FILE** in *Figure 81*, the following screen appears (*Figure 88*).

**Figure 88: Print Log File**

```
                         Print Log File (TSLPRTLOG)

 Type choices, press Enter.

 Start Time and Date:
   Begin Time . . . . . . . . . .   *AVAIL        Time, *AVAIL
   Begin Date . . . . . . . . . .   *CURRENT      Date, *CURRENT, *BEGIN
 End Time and Date:
   End Time . . . . . . . . . . .   *AVAIL        Time, *AVAIL
   End Date . . . . . . . . . . .   *CURRENT      Date, *CURRENT, *END

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

**START TIME AND DATE** — This option allows you to include log entries on the print log file list that were created on or after the date and time specified.

- **BEGIN TIME** — Select ***AVAIL** if you want to include all of the logged entries for the specified starting date, or you can enter the starting time for the specified starting date. The time is specified in a 24-hour format.
- **BEGIN DATE** — Select ***CURRENT** to include all of the logged entries for the current date, and those that get logged between the starting and ending times (if specified).

  Select ***BEGIN** to include log entries from the beginning of the log.

  Or, you may specify the starting date in the job date format with or without a separator.

**Note:** If you make any changes to the start time and date, then you must stop and restart the PMM Agent for i5/OS.

**END TIME AND DATE** — This option allows you to include log entries on the print log file list that were created on or before the date and time specified.

- **END TIME** — Select ***AVAIL** if you want to include all of the logged entries for the specified ending date, or you can enter the ending time for the specified ending date. The time is specified in a 24-hour format.
- **END DATE** — Select ***CURRENT** to specify that the current date is the last day for which logged entries are to be included on the list.

  Select ***END** to include entries of the last day on which the entries were logged.

  Or, you may specify the ending date in the job date format with or without a separator.

**Note:** If you make any changes to the end time and date, then you must stop and restart the PMM Agent for i5/OS.

### Display TSL Output Queue

When you select **DISPLAY TSL OUTPUT QUEUE** in *Figure 81*, the following screen appears (*Figure 89*).

**Figure 89: Display TSL Output Queue**

```
                              Work with Output Queue

Queue:    TSLOUTQ        Library:    COURTSL        Status:    RLS

Type options, press Enter.
  1=Send    2=Change    3=Hold    4=Delete    5=Display    6=Release    7=Messages
  8=Attributes         9=Work with printing status

Opt  File        User        User Data   Sts   Pages   Copies  Form Type   Pty
 _   TSLPRTLOGP  COURAGENT   TSLPRTLOGR  RDY       2       1    *STD         5
 _   TSLPRTCFGP  COURAGENT   TSLPRTCFGR  RDY       1       1    *STD         5

                                                                          Bottom
Parameters for options 1, 2, 3 or command
===> ____________________________________________________________________________
F3=Exit   F11=View 2   F12=Cancel   F20=Writers   F22=Printers
F24=More keys
```

This option displays a standard i5/OS screen from where you can print the COURTSL output queue spool file entries (TSLOUTQ).

## *Uninstalling the TSL for i5/OS*

To uninstall the Transparent Synchronization Listener (TSL) for i5/OS product library, you must sign on to the i5/OS as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL authority. You must have access to a 5250 emulation session.

**Note:** The uninstall procedure removes the TSL for i5/OS product library, but will leave the Listener for i5/OS Communication Module intact.

1. Remove TSL for i5/OS commands

   If you have added any TSL for i5/OS commands to the QSTRUP program or to the i5/OS Job Scheduled (WRKJOBSCDE), then you must remove these entries before proceeding with uninstall. Look for any of the following commands and remove them:

   `COURTSL/TSLMNTCFG` (TSL Configuration Maintenance)

   `COURTSL/TSLPRGLOG` (Purge Transparent Sync Log)

   `COURTSL/TSLPRTCFG` (Print TSL Configuration)

   `COURTSL/TSLPRTLOG` (Print Transparent Sync Log)

   **Note:** You must compile the QSTRUP program, if you removed any of the above TSL for i5/OS commands.

2. End PMM Agent for i5/OS

   a. Display the PMM Agent for i5/OS menu by entering: (*Figure 76*)

      `GO COURAGENT/PMMMNU`

   b. Select **END PMM AGENT FOR OS/400** and press **ENTER** to confirm.

c. Enter the following command to ensure that the PMM Agent for i5/OS is not active: See *Figure 77* and *Figure 78*.

```
WRKUSRJOB USER(COURAGENT) STATUS(*ACTIVE)
```

3. Remove the TSL Validate Password Exit Program

**Note:** You must be signed on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL authority,

a. Enter the following command to work with registration information for QIBM_QSY_VLD_PASSWRD exit point: (*Figure 90*)

```
WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD)
```

**Figure 90: Work with Exit Programs**

```
                          Work with Exit Programs

Exit point:   QIBM_QSY_VLD_PASSWRD     Format:   VLDP0100

Type options, press Enter.
  1=Add   4=Remove   5=Display   10=Replace

              Exit
            Program     Exit
Opt          Number     Program        Library
__                      ________       __________
__              20      TSLPSR         COURTSL
__              30      CHGPWDEXIT     QGPL
__              40      TSLTSR         COURTSL

                                                                  Bottom
Command
===> ____________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel
```

b. Select option 4 = **REMOVE** to remove the TSLPSR and TSLTSR exit point programs

**Note:** The TSLPSR is the exit point program to indicate a Password Strength Request (PSR). The TSLTSR is the exit program to indicate a Transparent Sync Request (TSR).

c. Press **ENTER** to confirm the removal

d. Press **F3** to return to the previous menu

4. Delete TSL for i5/OS Product Library

**Note:** You must be signed on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL authority,

a. Enter the following command to clear the TSLOUTQ entries.

```
CLROUTQ COURTSL/TSLOUTQ
```

b. Delete the COURTSL product library

```
DLTLIB COURTSL
```

c. Sign off as QSECOFR

The TSL for i5/OS product library is now uninstalled. At this point you can restart the PMM Agent for i5/OS to resume PasswordCourier processing.

*Notes and Warnings*

- Password changes using the CHGPWD command and the Change User Password (QSYCHGPW) API are supported. Password changes using the CHGUSRPRF command are not supported.
- Passwords will be forced to uppercase when i5/OS QPWDLVL is set to 0 or 1. Passwords will not be forced to uppercase with QPWDLVL set to 2 or 3.

## Errors Returned by the Transparent Sync Listener

Below is a list of error codes that may be returned to the Transparent Sync listener. They are logged in the Event Log on the DC that processes the password reset.

```
#define ERR_LISTENER_SUCCESS 0x00000

#define ERR_LISTENER_DISABLED 0x10001

#define ERR_LISTENER_INVALIDPACKAGE 0x10002

#define ERR_LISTENER_UNKNOWNREQUEST 0x10003

#define ERR_LISTENER_PACKAGECORRUPTED 0x10004

#define ERR_LISTENER_COMMFAILED 0x10005

#define ERR_LISTENER_SENDFAILED 0x10006

#define ERR_LISTENER_EMPTYPASSWORD 0x10007

#define ERR_LISTENER_AGENTNOTSTARTED 0x10008

#define ERR_LISTENER_INVALIDRESPONSE 0x10009

#define ERR_LISTENER_ERRORRECEIVED 0x1000A
```

# INDEX

## P



## Q



## R



## S

## T



## U



## V



## W