CORE SECURITY

Using the Core Access Assurance Suite™ Administration Manager Utilities

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

Copyright © 2018 by Core Security SDI Corporation. All Rights Reserved. The following are trademarks of Core Security Corporation "Core Impact", "Core Vulnerability Insight", "Core Password", "Core Access", "Core Provisioning", "Core Compliance", "Core Access Insight", "Core Mobile Reset", and "Think Like an Attacker". The following are registered trademarks of Core Security Corporation "WebVerify", "CloudInspect", "Core Insight", and "Core Security". The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The names of additional products may be trademarks or registered trademarks of their respective owners.

Table of Contents

Chapter 1: About Core Access Assurance Suite Utilities

The Core Access Assurance Suite Administration Manager includes the following utilities which ensure the security of the workflows and allow you to export workflows and import workflows from other Core Servers:

- *“Enable Users Utility” on page 7*
- *“Data Security Utility” on page 19*
- *“SSL Configuration Utility” on page 31*
- *“Configuration Migration Utility” on page 45*
- *“Using the ConfigMover: Targets Utility” on page 59*
- *“Exporting and Importing Workflows using the ConfigMover: Workflows Utility” on page 65*

These utilities are available through the Core Access Assurance Suite portal page by selecting the **TOOLBOX** option.

Chapter 2: Enable Users Utility

This chapter describes how to use the Access Assurance Suite Enable Users Utility to re-enable end user access to Access Assurance Suite applications and includes the following sections:

This version of the Enable Users Utility is an ASP.NET web application. By default, all network communications between the client web browser and the web server hosting the web application use the standard HTTPS (Hypertext Transfer Protocol Secure) port or the standard HTTP (Hypertext Transfer Protocol) port.

Overview

Core Security products are designed to automatically disable end users who exceed the maximum number of invalid attempts for end user validation or authentication (as defined by the product's configuration). This security feature helps companies avoid security attacks from unauthorized personnel trying to break in and access sensitive information. The Enable Users Utility provides the only way for a disabled end user to be re-enabled.

Note: Only one web browser should be connected to the Enable Users Utility at any given time.

Operation in PasswordCourier Classic, PasswordCourier Support Staff Classic, and ProfileCourier Classic

Disabled end users and support staff are identified by the first field of validation information. Therefore, the first User Validation field (or Staff Validation field in PasswordCourier Support Staff) should be configured with a unique, descriptive field such as "Employee ID." This is configured from the Format & Connection tab of the Customization Manager.

Note: You can configure ProfileCourier to automatically disable the end user after a successful profile creation or after a successful profile update. Configure this on the Feedback Messages tab of the ProfileCourier Customization Manager. For more information, see the manual *Using ProfileCourier Classic*.

Operation on the Provisioning Platform

You can customize a set of forms that an end user completes to access and execute Access Assurance Suite functions. These forms include three end-user authentication forms. While configuring the first authentication step, specify the field used to identify a disabled end user. This option is labeled **FIELD TO USE WHEN DISABLING A USER**. For more information about how to do this, see the manual *Configuring Workflows with the Access Assurance Suite Administration Manager*, and refer to the chapter on Setting Up Workflow Authentication.

Note: If the Courion Server and the Publisher web service are installed on different servers in a distributed installation, you need to edit the server name in the `web.config` file to the name of the server on which the Courion Server is installed. See *"Customizing the Enable Users Utility" on page 13*.

Prerequisites

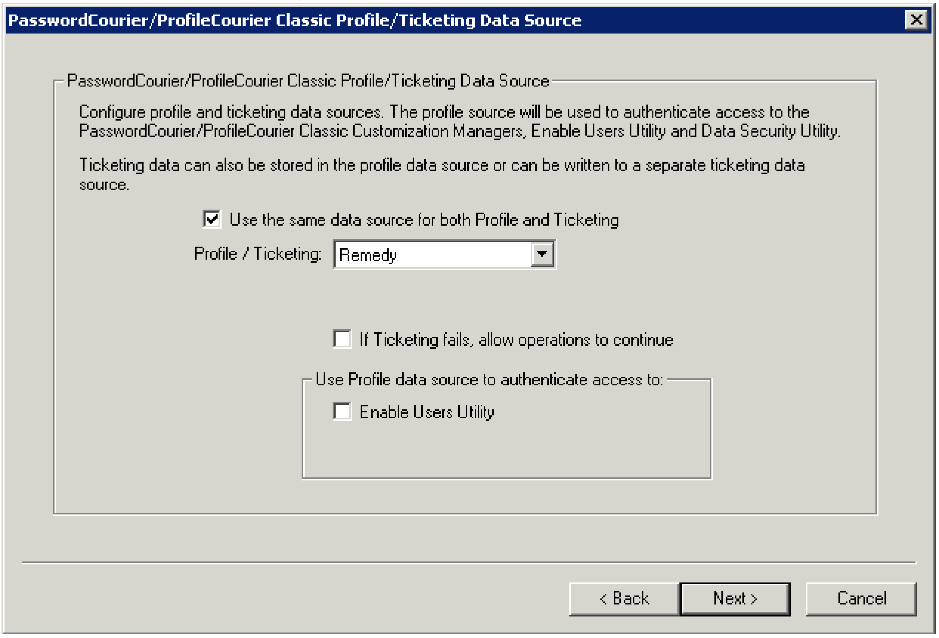
The Enable Users Utility requires that the following be installed:

- Microsoft .Net Framework v1.1 or later
- IIS with a web server certificate if you use HTTPS

Making the Enable Users Utility Available

During Courion Server configuration, the Data Source Selection dialog box appears (*Figure 1*) if an access key is present for PasswordCourier Classic, PasswordCourier Support Staff Classic, or ProfileCourier Classic. These products require you to log into a profile data source to access the Customization Manager. The Provisioning Platform does not use a profile data source for administrator authentication. If you only have access keys for the Provisioning Platform applications, or if you only configure Provisioning Platform applications, the dialog box does not appear.

Figure 1: Data Source Selection



PasswordCourier/ProfileCourier Classic Profile/Ticketing Data Source

PasswordCourier/ProfileCourier Classic Profile/Ticketing Data Source

Configure profile and ticketing data sources. The profile source will be used to authenticate access to the PasswordCourier/ProfileCourier Classic Customization Managers, Enable Users Utility and Data Security Utility.

Ticketing data can also be stored in the profile data source or can be written to a separate ticketing data source.

☑ Use the same data source for both Profile and Ticketing

Profile / Ticketing: Remedy

☐ If Ticketing fails, allow operations to continue

Use Profile data source to authenticate access to:

☐ Enable Users Utility

This dialog box determines the options you have to access the Enable Users Utility.

- If you select the **ENABLE USERS UTILITY** check box, you must authenticate against the profile data source. This option requires you to access the Enable Users Utility through the login dialog box shown in *Figure 2*.
- If you do not select the **ENABLE USERS UTILITY** check box, no authentication against the profile data source is required. Anyone with web access to the EnableUsers virtual directory can access the Enable Users Utility.

  Note: If you turn off authentication in this manner or if the only access key present is for Core Provisioning, RoleCourier, or Core Compliance, (or if you only configure Provisioning Platform applications), Core Security strongly recommends restricting access to the Enable Users Utility by requiring authentication through the web server.

Running the Utility

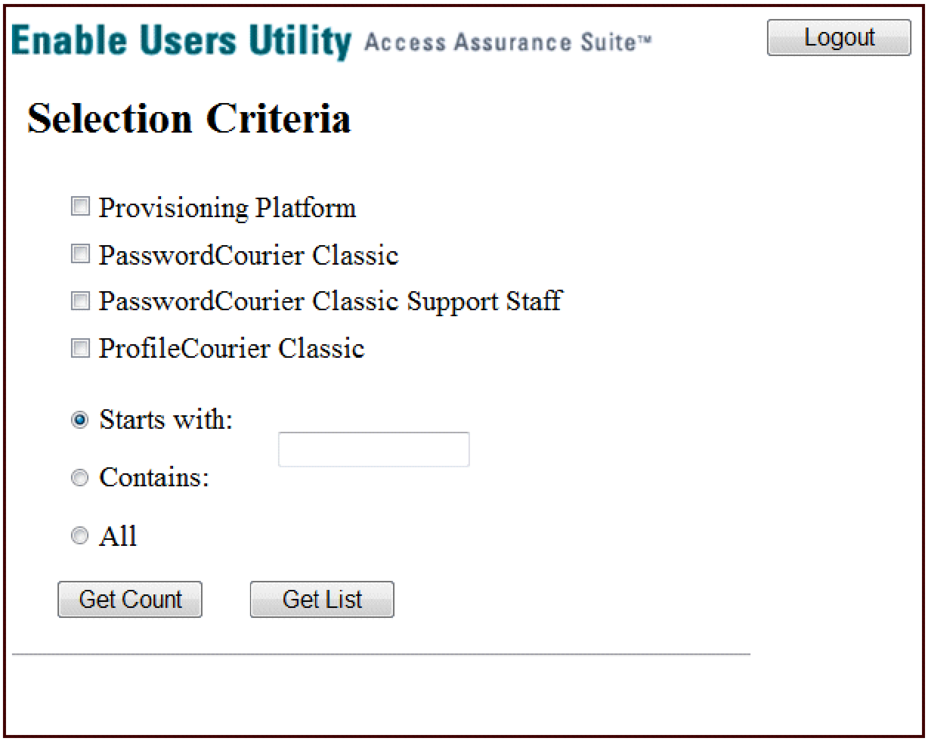
To run the Enable Users Utility:

1. Enter the url of the virtual directory you created when you installed the utility into your browser. For example,

   ```
   http://localhost/EnableUsers
   ```

2. If authentication has been enabled, the login dialog box in appears. If authentication is not required or the required login information has been entered, the Enable Users Utility displays the dialog box shown in *Figure 2*. Enter the appropriate username and password information and click **LOGIN**. The Selection Criteria Dialogue Box shown in *Figure 2* appears.

Figure 2: Selection Criteria Dialogue Box



Enable Users Utility Access Assurance Suite™

Selection Criteria

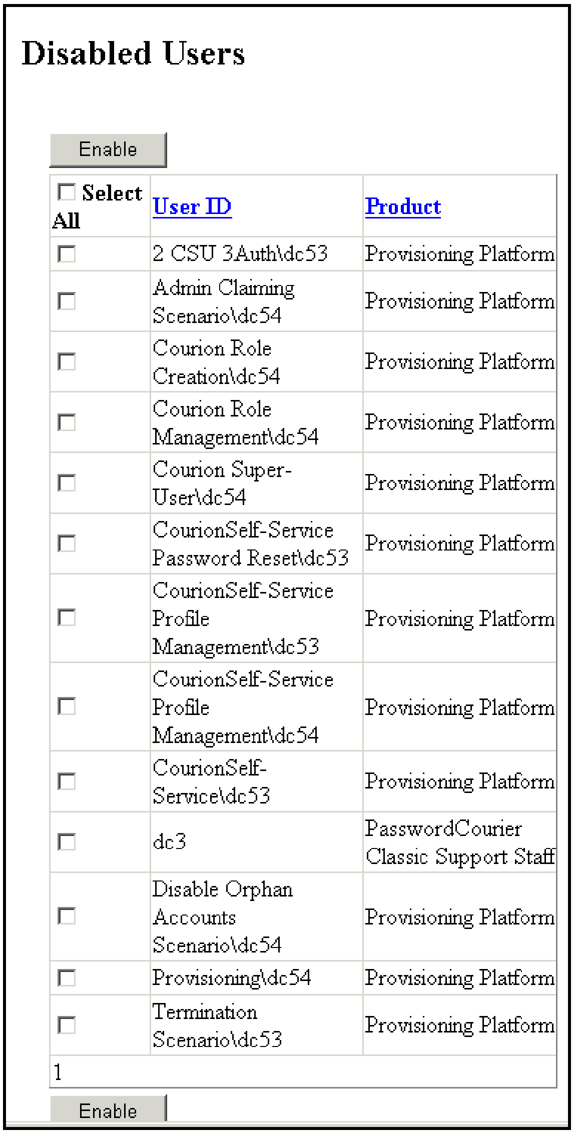
□ Provisioning Platform
□ PasswordCourier Classic
□ PasswordCourier Classic Support Staff
□ ProfileCourier Classic

● Starts with:
○ Contains:
○ All

Listing Disabled Users

See *"Parameter Settings that Disable Options in the Selection Criteria Dialog Box" on page 15* for information on how to use Web.Config or URL settings to restrict the search to disabled users on a domain you specify and to set search criteria to mask-off the options in the Selection Criteria dialogue box so that end users cannot change them.

Figure 3: Enable Users Utility — Disabled Users Displayed



Disabled Users

□ Select All	User ID	Product
□	2 CSU 3Auth\dc53	Provisioning Platform
□	Admin Claiming Scenario\dc54	Provisioning Platform
□	Courion Role Creation\dc54	Provisioning Platform
□	Courion Role Management\dc54	Provisioning Platform
□	Courion Super-User\dc54	Provisioning Platform
□	CourionSelf-Service Password Reset\dc53	Provisioning Platform
□	CourionSelf-Service Profile Management\dc53	Provisioning Platform
□	CourionSelf-Service Profile Management\dc54	Provisioning Platform
□	CourionSelf-Service\dc53	Provisioning Platform
□	dc3	PasswordCourier Classic Support Staff
□	Disable Orphan Accounts Scenario\dc54	Provisioning Platform
□	Provisioning\dc54	Provisioning Platform
□	Termination Scenario\dc53	Provisioning Platform
1		

Enabling End Users

When have a list of disabled users, as in *Figure 3*, you can select one or more users to enable. You can enable users individually or collectively, as follows.

- Individually: Select the check box next to one or more User IDs in the Disabled Users table. Click the **ENABLE** button to enable these users.
- Collectively: Select the **SELECT ALL** check box. This selects all items currently visible in the table. If there are additional pages of disabled users, you need to display each page to select all of the users. Click the **SELECT ALL** button to enable these users.

1. Select a name from the list and click **ENABLE** to enable the selected user or click **ENABLE ALL** to select and enable all end users on the list.

   A green check mark replaces the red X.

2. Click **APPLY**. The end users with green check marks are enabled and removed from the list.

Logging out of the Enable Users Utility

Click the **LOGOUT** button to log out of the Enable Users Utility.

Customizing the Enable Users Utility

This section lists the Enable Users web configuration parameters that allow you to customize the utility:

- *“Port and Server Values”*
- *“Connecting to a Different Version of the Courion Server”*
- *“Configuration for HTTP or HTTPS”*
- *“Parameter Settings that Disable Options in the Selection Criteria Dialog Box”*

Editing the web.config File

To customize the web configuration parameters, edit the web.config file in the following location where [CoreSecurityInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

[CoreSecurityInstallPath]`\www\Utils\EnableUsers`

and specify the correct values.

Near the beginning of this file is a block of statements contained within the <appSettings> and </appSettings> tags. Most of these statements are commented out, as shown:

```
<appSettings>
  <add key="RequireSSL" value="FALSE"/>
<!--
  <add key="Port" value="8189"/>
  <add key="Server" value="localhost"/>
  <add key="MajorVer" value="major version number"/>
  <add key="MinorVer" value="minor version number"/>
  .
  .
  .
  <add key="EnableSearchText" value="FALSE"/>
-->
</appSettings>
```

To use a specific configuration value, move the statement so that it precedes the comment (represented by “<!—“), and change the value as needed. In the following example, the port and server statements have been moved:

```
<appSettings>
  <add key="RequireSSL" value="FALSE"/>
  <add key="Port" value="port number"/>
  <add key="Server" value="server name"/>
<!--
  <add key="MajorVer" value="major version number"/>
  <add key="MinorVer" value="minor version number"/>
  .
  .
  .
 -->
</appSettings>
```

Port and Server Values

The Enable Users Utility has two default values that you must change if:

- The Courion Server and the Publisher web service are installed on different servers in a distributed installation. (The Enable Users Utility runs on the server in which the Publisher is installed.)
- The TCP/IP port value of the machine running the Courion Server is other than the default, 8189.

If either or both of these conditions are true, uncomment the corresponding Port and Server statements, and enter the correct values. For the server value, enter the name of the server on which the Courion Server is installed.

Enabling IP Address Checking

The Enable Users Utility can be configured to check the IP address of the logged-in user and if the session ID has changed, the utility logs the user out and sends the user to the AAS Portal login page.

To enable IP address checking for the utility, do the following where [CourionInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

1. Copy the [CourionInstallPath]\CourionService\InputValidation\SessionRestriction.xml file to the [CourionInstallPath]\www\Utils\EnableUsers directory and rename it as CustomSessionRestriction.xml.
2. In an editor, open the CustomSessionRestriction.xml file and uncomment the <IPAddressCheck> node and make sure that the <IPAddressCheck> node is set to True.
3. Save your change.
4. In a text editor, edit the [CourionInstallPath]\www\Utils\EnableUsers\web.config file by adding the SessionRestrictionPolicyFolder appSetting as follows:

```
<appSettings>
  <add key="SessionRestrictionPolicyFolder"
value="[CourionInstallPath]\www\Utils\EnableUsers"/>
  .
  .
</appSettings>
```

5. Save your change.

Connecting to a Different Version of the Courion Server

Use these parameters when you need to connect to a Courion Server of a different version than the Enable Users Utility:

```
<add key="MajorVer" value="XX"/>
<add key="MinorVer" value="XX"/>
```

To determine the major and minor version to use, select Version Information from the Courion Access Assurance Suite folder in the Start menu, or run the `Verdump` utility, on system where the Courion Server is running.

For example, if the Courion Server you are trying to connect to is version 7.70 and you are using an Enable Users utility of version 7.80, uncomment the MajorVer and MinorVer statements, and enter the correct values:

```
<add key="MajorVer" value="7"/>
<add key="MinorVer" value="70"/>
```

Configuration for HTTP or HTTPS

By default, Core Access Assurance Suite does not enforce SSL connectivity. Modify this statement when you want to enable the requirement to enforce SSL connectivity with the Enable Users utility:

```
<add key="RequireSSL" value="TRUE"/>
```

Parameter Settings that Disable Options in the Selection Criteria Dialog Box

These parameter settings allow you to enforce search rules in the Selection Criteria dialog box by:

- Restricting the search to a domain you specify.
- Allowing you to set search criteria and mask-off the options in the Selection Criteria dialogue box so that end users cannot change them.

These settings are useful in configurations where administrators of different domains need to manage their own set of disabled users. They also enforce security policies by limiting end users to searching for disabled users that meet the criteria you set up in the view filters.

See *“Listing Disabled Users” on page 10* for complete information about the selection criteria for searches on disabled users including text strings and search types. Web.Config supports the parameter settings that disable selection criteria in the Enable Users Utility listed in Table 1:

Table 1: Settings that Disable Selection Criteria for the Enable Users Utility (Sheet 1 of 2)

appsetting	Purpose	Value
DisablePrefix	Sets the domain search prefix. With this value in effect, all searches are first tested against this value, then the user name. This search prefix does not apply to searches for disabled users on the Classic platform.	Text string that indicates the domain name
cbProvisioningPlaform cbPasswordCourierClassic cbPasswordCourierClassicSupport Staff cbProfileCourierClassic	Selects one or more specific application check boxes (cb) when the value is set to TRUE.	TRUE or FALSE (must be upper-case)

Table 1: Settings that Disable Selection Criteria for the Enable Users Utility (Sheet 2 of 2)

appsetting	Purpose	Value
rbSearchType	Sets the search type radio buttons (rb) to the value you specify.	0 = Starts with 1 = Contains 2 = All
textSearchString	Sets the search string.	Text string that sets the user specified search string. If you do not specify a search string, no text is accepted in this box.
EnableSearchText EnablePlatformSelection EnableSearchTypeSelection	Disables the search criteria controls (SearchText, Platform Selection, Search Type) when they are set to FALSE.	TRUE or FALSE (must be upper-case)

Example

The following is an example of these parameter settings with appropriate values in a script:

```
<add key="DisablePrefix" value ="CompanyA/"/>

<add key="cbProvisioningPlaform" value="TRUE"/>
<add key="cbPasswordCourierClassic" value="FALSE"/>
<add key="cbPasswordCourierClassicSupportStaff"
value="FALSE"/>
<add key="cbProfileCourierClassic" value="FALSE"/>
<add key="EnablePlatformSelection" value="FALSE"/>

<add key="rbSearchType" value="2"/>
<add key="EnableSearchTypeSelection" value="FALSE"/>

<add key="textSearchString" value =""/>
<add key="EnableSearchText" value="FALSE"/>
```

Specifying Parameter Settings in a URL

Instead of editing the `web.config` file, you can specify the selection criteria parameter settings using a URL query string. This method applies only to the selection criteria parameter settings. This method is not available for the port, server, version number, or SSL connectivity parameters.

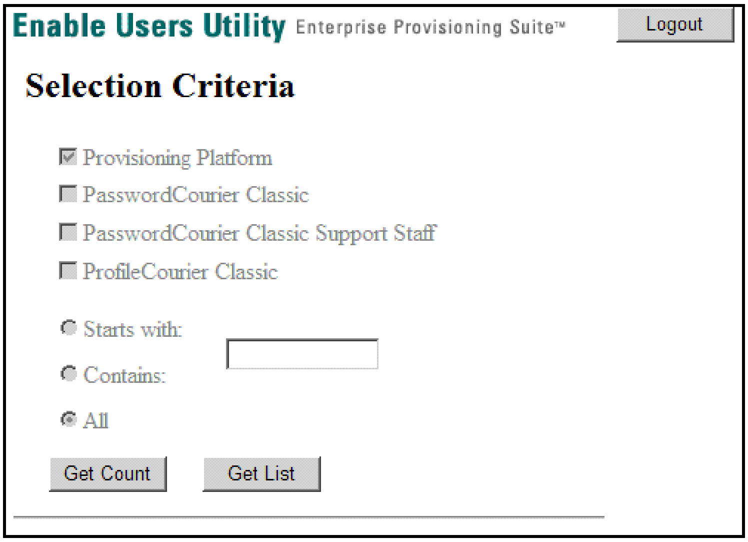
Parameters supplied in the web.config file take precedence over parameters supplied in a URL query string, so these settings must be commented out in the `web.config` file if you want to use a URL query string to specify the values. You do not have to include all the selection criteria parameters in your URL. You can include only the parameters whose values you want to change from the default.

The example below shows a URL with the same settings as the previous script example:

```
http://localhost/EnableUsers/
EnableUsersLoginForm.aspx?DisablePrefix=CompanyA/
&cbProvisioningPlaform=TRUE&cbPasswordCourierClassic=FALSE&cbPasswordCourie
rClassicSupportStaff=FALSE&cbProfileCourierClassic=FALSE&EnablePlatformSele
ction=FALSE&rbSearchType=2&EnableSearchTypeSelection=FALSE&EnableSearchText
=FALSE
```

Figure 4 shows the Selection Criteria dialog box as it would look if you implemented the parameter settings in the example.

Figure 4: Enable Users Utility with Selection Criteria Disabled



Selection Criteria

☑ Provisioning Platform
□ PasswordCourier Classic
□ PasswordCourier Classic Support Staff
□ ProfileCourier Classic

○ Starts with:
○ Contains:
● All

The Selection Criteria dialogue box in *Figure 4* allows an end user to select only the Get Count or Get List buttons to retrieve the disabled users in the domain CompanyA on the Provisioning Platform.

In the script example, this is specified in `<add key="DisablePrefix" value ="CompanyA/"/>`

In the URL query string example, this is specified in `DisablePrefix=CompanyA/`

Notes and Warnings

If there is no local ASPNET user on the system, or an ASP.NET entry does not exist under Web Service Extensions for IIS, then go to the Microsoft.NET folder (C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322), and run the command:

```
aspnet_regiis -l
```

This creates the ASP.NET entry under IIS Web Service Extensions.

Change the settings under Web Service Extensions for IIS so that ASP.NET is Allowed.

Chapter 3: Data Security Utility

This chapter describes the Data Security Utility. The expected reading path is as follows:

Overview

The Access Assurance Suite supports two methods to secure data in the profile management and authentication data source: hashing and encryption. The Data Security Utility is an Access Assurance Suite administrative tool that allows selection of the fields within a data source whose data is to be hashed or encrypted. Core Security products can use secured data fields for end user validation, authentication, profile management, and query operations. Field values cannot be viewed in a meaningful form other than through the approved methods provided by Core Security products.

Implications for the Access Assurance Suite

PasswordCourier Classic, PasswordCourier Support Staff Classic, and ProfileCourier Classic each allow up to two data sources to be configured, one for profile management and authentication and one for ticketing. These data sources are shared across these three products. Applications on the Provisioning Platform support multiple data sources.

The provisioning platform applications do not use the profile management and authentication data source as configured for other Access Assurance Suite products. Because of this, the provisioning platform applications require special consideration. Unlike other Access Assurance Suite products, these applications access the data source through a connector. You use the Connector Configuration Manager to identify and configure targets for authentication and other functions.

If a provisioning platform application and a classic platform application use the same data source table for profile management and authentication, a field marked as hashed or encrypted for one product *must* be marked as hashed or encrypted for the other product. This means that the field must be marked as hashed or encrypted in two places within the Data Security Utility. See *“Using the Data Security Utility” on page 27*.

Refer to the manual *Configuring Password Management Modules (PMMs), Connectors and Agents* for information on connectors and Core Provisioning and Core Compliance functions.

Planning

It is essential that the administrator setting up secure fields understand how the Data Security Utility works and the implications of those settings.

Marking a field hashed or encrypted in the Data Security Utility does *not* hash or encrypt data stored in the selected data source. Marking a field only tells the Core Access Assurance Suite to treat the value in that field as hashed or encrypted. The field values for all existing records remain in their current format—only values entered after a field is marked are stored as hashed or encrypted. Once a field is marked as secure, the Core Access Assurance Suite hashes or encrypts end user input for that field and compares it to stored data. Any records with existing cleartext data or records secured with a different algorithm do not match the secure value generated by the Core Access Assurance Suite and the authentication or query fails.

Note: This means that all end users *must* update their profiles by entering a value for the marked field even if this field already exists and has a stored value. Furthermore, end users must enter a *new* value.

The following example illustrates this functionality:

- The administrator decides to hash the field TextPIN. This field is currently used in cleartext format in end user profiles, and is required for authentication to Core Provisioning, Core Compliance, and PasswordCourier Classic.
- The administrator uses the Data Security Utility to mark TextPIN as hashed in both the profile data source (for PasswordCourier and ProfileCourier) and connector target data source (for AccountCourier and Core Compliance, and PasswordCourier Classic).
- The administrator notifies all end users that they must use ProfileCourier Classic to update their profiles by entering a new value for the field TextPIN.

  If an end user wants to use the original field value (for example, for a field like MothersMaidenName), the end user can enter the original value when updating the profile.
- The end user enters the new authentication data to access Core Provisioning, Core Compliance, or PasswordCourier Classic.

Follow these general steps to use hashed or encrypted fields:

1. Identify the data source and the table whose fields are treated as secure.
2. Identify the fields for which data is stored as hashed or encrypted. The fields must be of type **TEXT**.
3. Make sure the data source fields must be capable of storing the hashed or encrypted value as 90 character strings.
4. Run the Data Security Utility.

Note: If any of the fields marked hashed or encrypted already contain data (that is, a marked field is already included in users' profiles), you should devise a plan for updating that data to hashed or encrypted values.

Note: If the data source is configured to use case-insensitive compares, lowercase letters are converted to uppercase before being hashed and stored. This is done so that regardless of what the end user enters, comparisons can be made against the hashed version of the same string. Do not change the case sensitivity of the data source if data exists in a hashed field or if validations against that existing data fail. Encrypted fields are always encrypted and stored preserving the case, regardless of case insensitivity settings in the data source. Encryption should be used in fields where the data is stored securely in the data source and the original cleartext is extracted with the case preserved.

Note: After unmarking a field, you should re-enter all existing database records in order to store the data as cleartext.

Note: The Data Security Utility does not distinguish between more than one target with the same name. If you use more than one target with the same name, you cannot set up hashing or encryption on the second target.

Hashing

When data should not be viewable in cleartext form, it can be processed through a hashing algorithm and the resulting value stored in the data source. For example, when an end user is authenticated, the cleartext data entered by the end user is hashed and the resulting value is compared against the hashed value stored in the data source. If the values match, the authentication succeeds.

Hashing algorithms are one-way functions that take plain text and produce a fixed length data string. The plain text is a “preimage.” The fixed length output is a “message digest.” Message digest fields are not supported for ticketing actions. Hashing algorithms include the following properties:

- The preimage may be of any length.
- The message digest is always the same fixed length.
- The algorithm is one-way. Computing the preimage from the message digest is extremely difficult.
- The algorithm generates very few collisions. It is extremely difficult to find two different preimages that result in the same message digest.

The Access Assurance Suite supports the SHA2 algorithm for computing message digests. The SHA2 algorithm computes a 512-bit binary message digest from an arbitrary length preimage. To create a hash value from the clear text value, AAS requires three inputs: a cleartext value, a customer salt value of at least 90 characters in length, and a random salt value. An administrator establishes the customer salt value and random salt value during installation of AAS as described in the manual, *Installing the Access Assurance Suite*.

Table 2: SHA2 Attributes

Attribute	Description
Preimage length	The cleartext data may be of any size.
Message digest length	SHA2 results in a 512-bit result.
Data source field types supported	Only text fields may be marked as a hashed/message digest.
Data source field size	The data source field must be at least 90 characters in size to store the ASCII representation of the message digest.

For example, the preimage text for TextPIN field is "norway."

- The 512-bit message digest is V4tuo7B4mMmgqffsgc2EYUISlgAEQLcR8JdMaBi5wKVuyL4u61BJghrOYpbsQU1U3F1Hs2SZgSVrJmL/iPp2Nw==.
- Eighty nine (89) characters are required to store the base 64 encoded string "V4tuo7B4mMmgqffsgc2EYUISlgAEQLcR8JdMaBi5wKVuyL4u61BJghrOYpbsQU1U3F1Hs2SZgSVrJmL/iPp2Nw=="

Encryption

Data that requires recovery back to a cleartext form can be processed by an encryption algorithm and the resulting encrypted value stored in the data source. When the encrypted data needs to be retrieved as cleartext, it is processed by a decryption algorithm.

Encryption algorithms use an encryption key to convert cleartext of a specific length into an incomprehensible cipher text. A decryption key is used to convert a cipher text string back to the original cleartext. Different algorithms use different methods to encrypt streams of data larger than their block size and are, therefore, not limited to encrypting and decrypting a specific size string. Good encryption algorithms include the following properties:

- The cleartext can be of any length.
- The cipher text length is relative to the entered length.
- The algorithm is reversible with the proper decryption key. Symmetric ciphers use the same key for encryption and decryption.
- The algorithm is not susceptible to cleartext attacks (an attacker cannot guess the encryption/decryption keys by encrypting any number of specific strings and analyzing their yield).

The Access Assurance Suite supports the AES (Advanced Encryption Standard) algorithm for encryption and decryption of fields selected to be encrypted. The following table describes some of its features.

Table 3: AES Attributes

Attribute	Description
Input length	The cleartext data may be of any size.
Block size	AES utilizes a block size of sixteen (16) bytes.
Output length	The encrypted text is at most the entered text length plus the block size. An entry of one byte creates an output of sixteen bytes.
Data source field types supported	Only text fields may be marked as encrypted.
Data source field size	The data source field must be twice as large as the sum of the cleartext length and the block size to store the ASCII representation of the encrypted text (see below).

For example, the cleartext in the “Mother’s Maiden Name” field is “Bates.”

- The cipher text value is 9a9e3c9b36908bd9b8aacb39c3941152 (base 16).
- Thirty-two (32) bytes are required to store the string "9a9e3c9b36908bd9b8aacb39c3941152"

Note: Ensure that the table field is large enough to store the data. The general rule of thumb is to round up the length of the data to the nearest multiple of 16 (AES's block size) and multiply by two (so binary data can be written as hexadecimal digits). In the example, the five-character string “Bates” encrypts to 32 binary bytes (round up five to the nearest multiple of 16, which is 16). Multiply 16 by two. Thus a five-character string requires 32 bytes for storage in hexadecimal format. If the data length is already a multiple of 16 such as 32 bytes, add an additional 16 bytes and then multiply by two to get the required field length. ((32+16)*2=96).

Table fields that hold less than 90 characters are not displayed for marking as encrypted fields even though the minimum width needed for encrypted data is 32 characters.

Data Source Actions

If a field is marked as a secure field in the Data Security Utility, then the hashed or encrypted text is computed from the preimage for these actions against the data source:

Table 4: Database Actions on Secure Fields

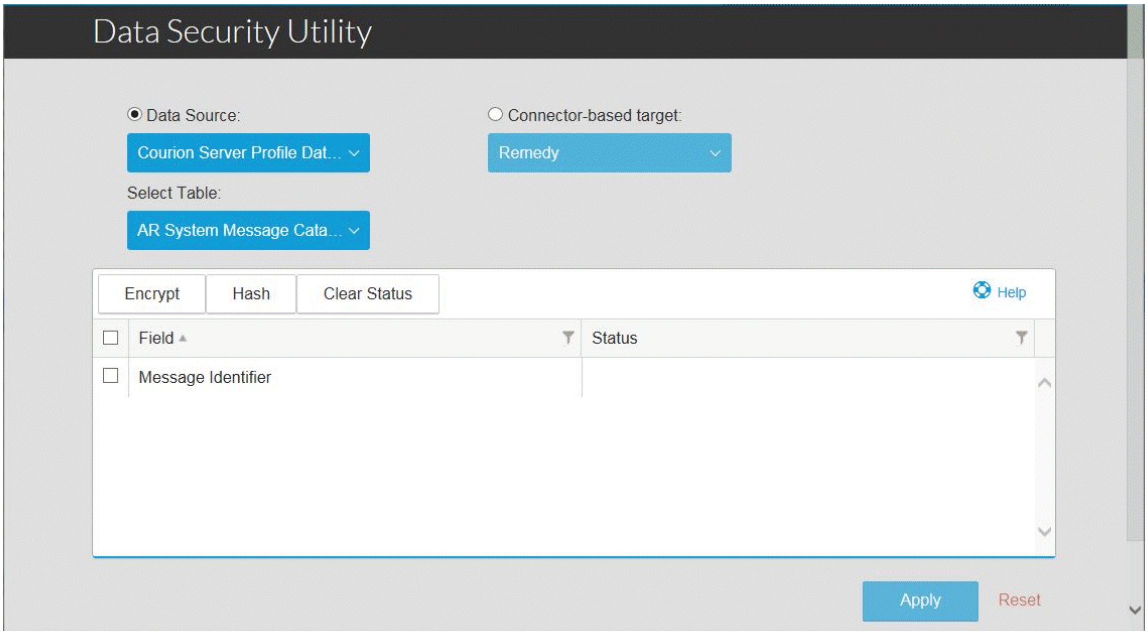
Database Action	Description
Create Record	1. The hashed or encrypted text is computed from the preimage. 2. The output is stored in the field.
Update Record	If the preimage value is changed or the field is an encrypted field: 1. The hashed or encrypted text is computed from the preimage. 2. The output is stored in the field.
Select Query (for user validation and authentication)	1. If a secure field is in the “Where” clause, compute the hashed/message digest or cipher text, generate a new “Where” clause. 2. Hashed or encrypted text may be returned in the resulting record set. 3. If a returned field is an encrypted field, the data is decrypted.

Using the Data Security Utility

After you have completed the planning of securing fields and configured the Data Security Utility, you can begin to use the utility. To run the Data Security Utility, do the following:

1. Log into the Access Assurance Portal as a member of the “Admin” (ARM Admins) community.
2. From the **Main Menu**, select **Configuration**. then **SECURE FIELDS**. The Data Security Utility displays the dialog box shown in *Figure 5*.

Figure 5: Data Security Utility Dialog Box



3. Select *one* of the following options:

- **DATA SOURCE** — Choose this option to mark field values for hashing or encryption for the PasswordCourier, PasswordCourier Support Staff, ProfileCourier, or profile data source. The drop-down list contains a single entry, **COURION SERVER PROFILE DATA SOURCE**. If your Access Assurance Suite configuration includes only AccountCourier or ComplianceCourier access keys, this option is disabled and unavailable.
- **CONNECTOR-BASED TARGET** — Choose this option to mark field values for hashing or encryption for AccountCourier or ComplianceCourier data sources. The drop-down list includes all target data sources added to connectors that support authentication, profile creation, and query. If your Access Assurance Suite configuration does not include AccountCourier or ComplianceCourier access keys, this option is disabled and unavailable.

  Note: If a provisioning platform application and a classic platform application use the same actual physical table in a data source, it is critical that a field marked as hashed or encrypted for one product be marked as hashed or encrypted for the other product. This means you must mark the field as hashed or encrypted in two places within the Data Security Utility: once for the **COURION SERVER PROFILE DATA SOURCE** and again for the corresponding Provisioning Platform connector target. Furthermore, the administrator must know which data source in the

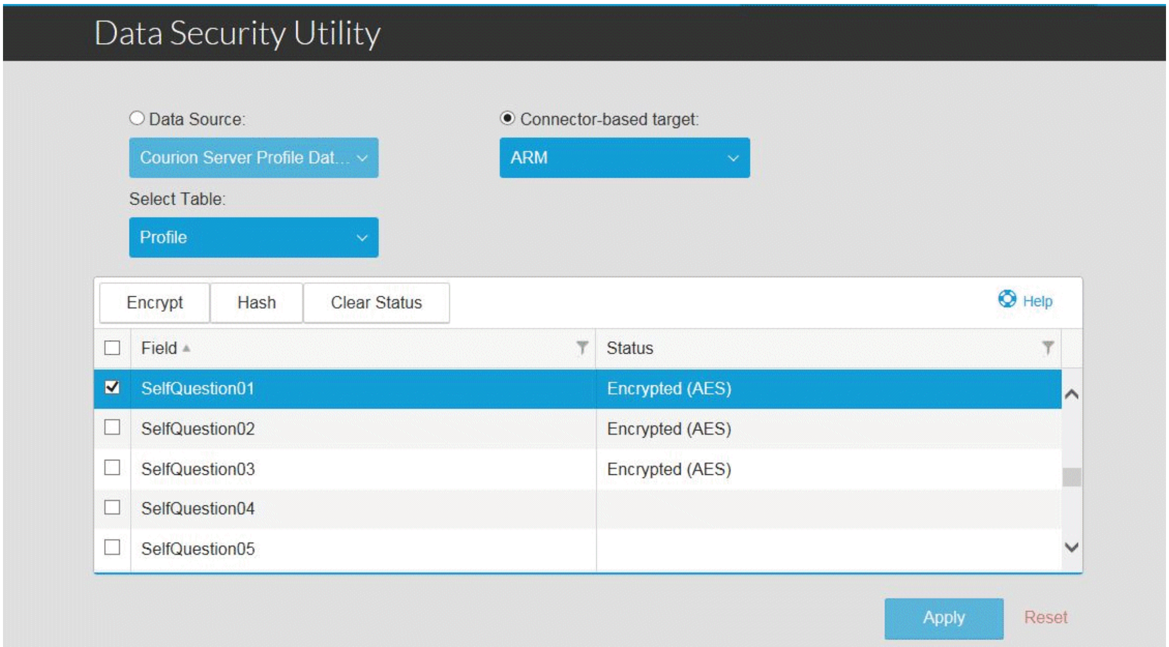
Connector-based Target drop-down list corresponds to the **Courion Server Profile Data Source**.

Note: Hashed or encrypted fields may not be used in the Transaction Repository. If you are using the Microsoft ADO connector with an operation for the Transaction Repository and also want to use that connector for other operations in which hashed or encrypted fields are involved, you must configure two separate targets for that connector.

Assign one target to the Transaction Repository operation and the other target to any supported operations except the Transaction Repository. Any target that is configured for the Transaction Repository does not appear in the **Connector-based Target** drop-down list.

4. In the **Select Table** drop-down list, select the table that contains the field or fields you want to mark as hashed or encrypted.

Figure 6: Data Security Utility Dialog Box—Marking a Field



Data Security Utility

○ Data Source: Courion Server Profile Dat...

● Connector-based target: ARM

Select Table: Profile

☐	Field	Status
☑	SelfQuestion01	Encrypted (AES)
☐	SelfQuestion02	Encrypted (AES)
☐	SelfQuestion03	Encrypted (AES)
☐	SelfQuestion04	
☐	SelfQuestion05	

5. The **Field** list only contains fields that meet the minimum length. Select a field name and click **Hash** or **Encrypt**.

   The **Status** column for the selected field indicates either **Hashed(SHA2)** or **Encrypted(AES)**.

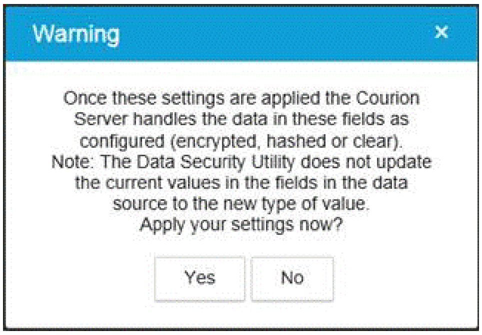
6. Do one of the following:

   To remove a field selection, click **Clear**.

   To return all settings to their last applied status, click **Reset**.

   To save all the settings for the selected table, click **Apply**. The Data Security Utility displays the warning message shown in *Figure 7*.

Figure 7: Data Security Utility Warning Message


Warning

Once these settings are applied the Courion Server handles the data in these fields as configured (encrypted, hashed or clear).
Note: The Data Security Utility does not update the current values in the fields in the data source to the new type of value.
Apply your settings now?

7. To apply the security settings, click **YES**.

If you have used the Data Security Utility to mark fields for hashing and encryption, the following apply:

- Future updates to marked fields from using a classic or provisioning platform workflow write hashed or encrypted data into the drop-down fields.
- For end user authentications for all Access Assurance Suite products, the Courion Server hashes or encrypts data for marked fields and compares it to the stored field values.

Note: If data already existed as a result of running profile workflows and you have used the Data Security Utility to mark fields for hashing and encryption, an existing value in a marked field remains in cleartext. End users *must* enter a new value for all marked fields so that data is stored in a secure form.

Resetting a Secured Field

A field previously marked as hashed or encrypted can be unmarked. To remove the security setting from a field, select the field and click **CLEAR**, then click **APPLY**.

- All values currently stored in an unmarked field remain in the current hashed or encrypted form and cannot be successfully used for user validation, authentication, or queries.
- Future updates and comparisons will use cleartext values.
- End users *must* update their profiles by entering a value for all unmarked fields so that data is stored in cleartext. This update replaces the hashed or encrypted value with a cleartext value.

Note: Unlike the profile update required when changing from a cleartext to hashed or encrypted value, an end user can re-enter the same value to return to cleartext.

Chapter 4: SSL Configuration Utility

This chapter includes the following information about the SSL Configuration Utility:

Overview

The SSL Configuration Utility is used to configure a certificate for the Core Server when it uses a Secure Sockets Layer v3.0 (SSL) communication channel to communicate with the following components on the same system:

- CourATLAdminService
- CourATLService
- PasswordCourier / ProfileCourier Classic Admin managers
- Enable Users Utility
- Secure Fields Utility

The SSL Configuration Utility enables the use of certificates with the Core Server. It is ready for use and requires no additional configuration. Diffie-Hellman parameters are used by default, but you can configure the utility to use server certificates for the authentication of the clients over SSL connections.

Configuration

A wizard guides you through the installation of the SSL Configuration Utility.

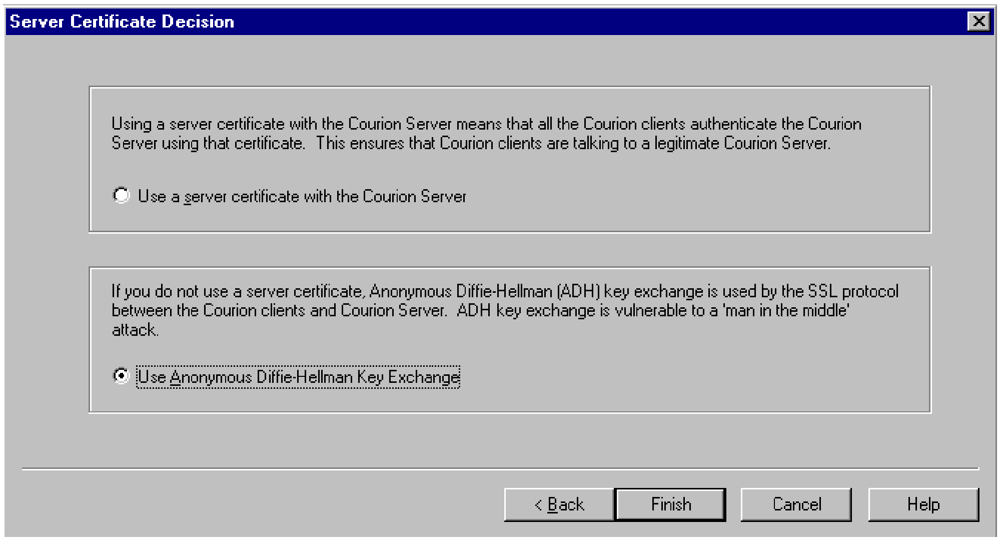
Note: If the **NEXT** or **FINISH** button is not enabled, required data is missing from that page.

Server Certificate Decision

The Server Certificate Decision dialog box (*Figure 8*) gives you the option of configuring the SSL Utility to use a server certificate. If you use a server certificate, all the clients authenticate to the Core Server using that certificate. This ensures that clients are talking to a legitimate Core Server.

Click on the appropriate radio button to indicate whether or not to use a server certificate.

Figure 8: Server Certificate Decision



Server Certificate Decision

Using a server certificate with the Courion Server means that all the Courion clients authenticate the Courion Server using that certificate. This ensures that Courion clients are talking to a legitimate Courion Server.

○ Use a server certificate with the Courion Server

If you do not use a server certificate, Anonymous Diffie-Hellman (ADH) key exchange is used by the SSL protocol between the Courion clients and Courion Server. ADH key exchange is vulnerable to a 'man in the middle' attack.

● Use Anonymous Diffie-Hellman Key Exchange

If you do not use a server certificate, Anonymous Diffie-Hellman (ADH) key exchange is used by the SSL protocol.

Because an ADH key exchange is vulnerable to a man in the middle attack, Core Security recommends the use of a server certificate. It is the administrator's responsibility to obtain a server certificate. The SSL Utility assists in the generation of a certificate signing request and in the installation of a signed certificate.

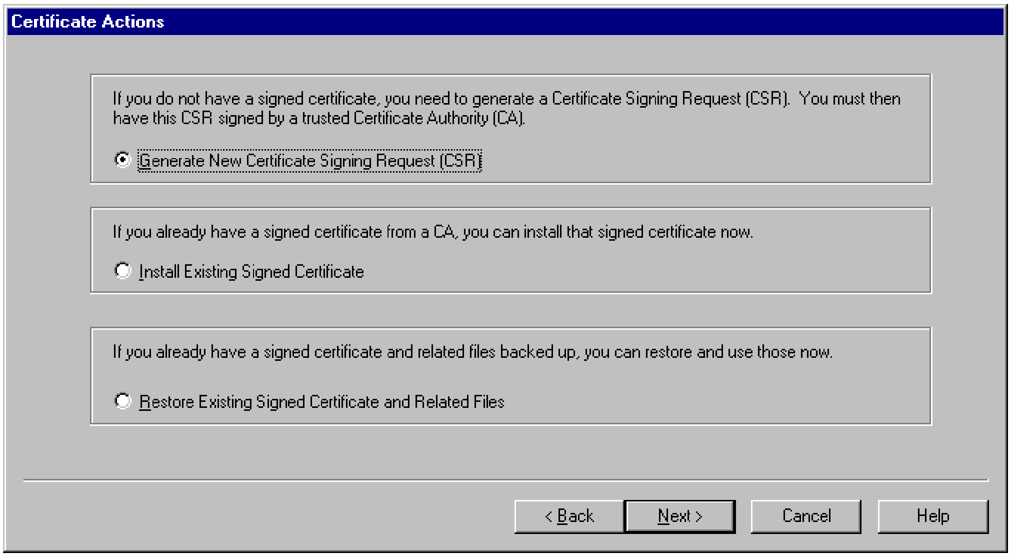
If you use Anonymous Diffie-Hellman, the **NEXT** button becomes a **FINISH** button because there is no additional configuration to perform.

Certificate Actions

If you use a server certificate, you can generate a Certificate Signing Request (CSR), install an existing signed certificate, or restore an existing signed certificate and related files. Install a signed certificate if one is available. If a signed certificate is not available, generate a Certificate Signing Request (CSR) from the Certificate Actions dialog box (*Figure 9*).

Note: The first time this utility is used, select the **GENERATE NEW CERTIFICATE SIGNING REQUEST (CSR)** radio button. This ensures that a certificate designated for the Access Assurance Suite is used.

Figure 9: Certificate Actions



Certificate Actions

If you do not have a signed certificate, you need to generate a Certificate Signing Request (CSR). You must then have this CSR signed by a trusted Certificate Authority (CA).

● Generate New Certificate Signing Request (CSR)

If you already have a signed certificate from a CA, you can install that signed certificate now.

○ Install Existing Signed Certificate

If you already have a signed certificate and related files backed up, you can restore and use those now.

○ Restore Existing Signed Certificate and Related Files

Generate a New Certificate Signing Request (CSR)

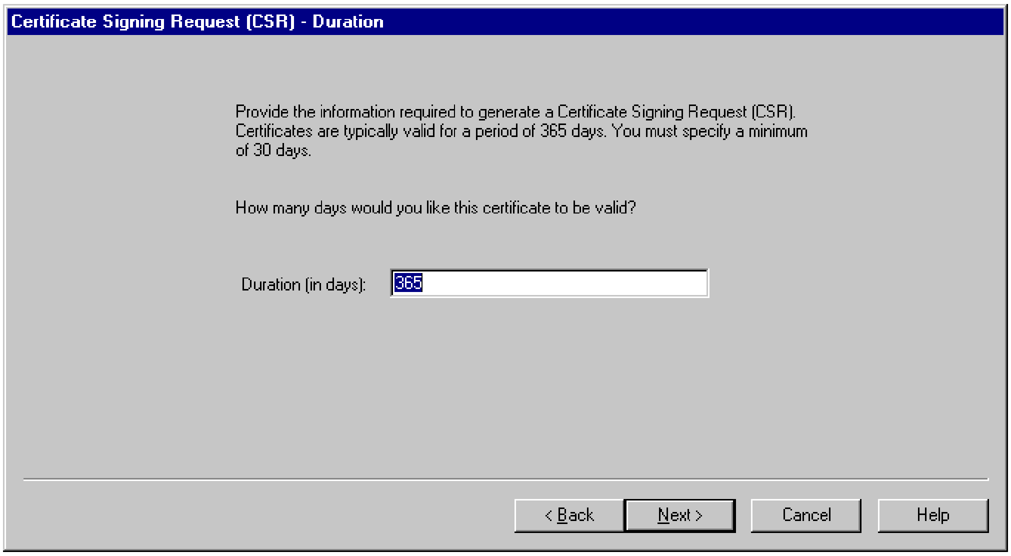
Select the **GENERATE NEW CERTIFICATE SIGNING REQUEST (CSR)** radio button. A CSR is created through a wizard.

CSR Certificate Signing Request Duration

The Certificate Signing Request (CSR) - Duration dialog box (*Figure 10*) allows you to configure the number of days for which the certificate is valid. The CA may replace this number with one of their own choosing.

1. Enter the number of days for which the certificate is valid.
2. Click the **NEXT** button.

Figure 10: Duration



Certificate Signing Request (CSR) - Duration

Provide the information required to generate a Certificate Signing Request (CSR). Certificates are typically valid for a period of 365 days. You must specify a minimum of 30 days.

How many days would you like this certificate to be valid?

Duration (in days): 365

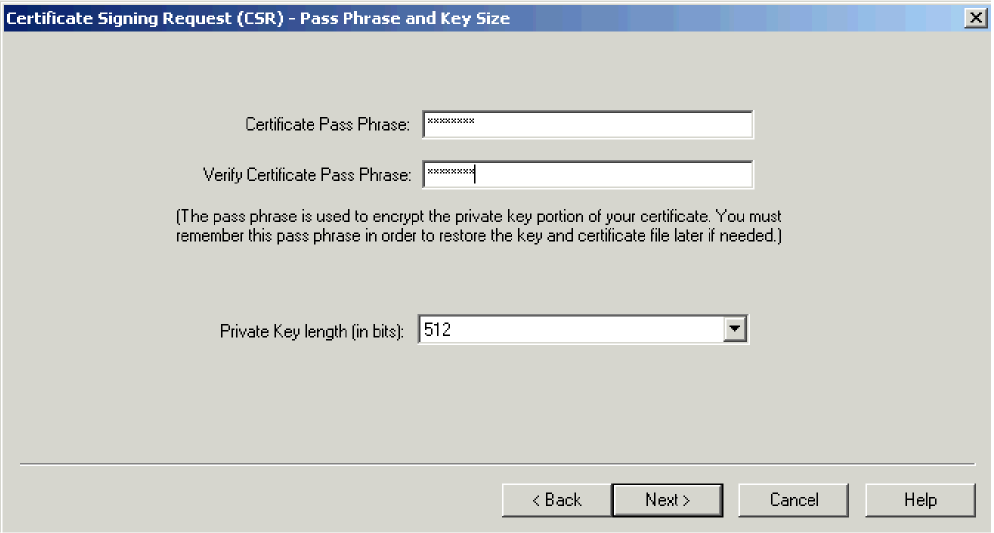
CSR Pass Phrase and Key Size

Because the Access Assurance Suite supports certificates based on public key cryptography, the CSR must include a public/private key pair. The public key is included in the CSR and the certificate on the Pass Phrase and Key Size dialog box (*Figure 11*).

1. Enter a pass phrase to protect the private key and verify the pass phrase.
2. Enter the length of the key, either drop-down12 or 1024. The longer the key, the more secure it is.
3. Click the **NEXT** button.

The pass phrase keeps unauthorized end users or applications from reading the private key file. It is important to remember this pass phrase; it is necessary if for the restoration of a private key and certificate from backup.

Figure 11: Pass Phrase and Key Size



Certificate Signing Request (CSR) - Pass Phrase and Key Size

Certificate Pass Phrase: *********

Verify Certificate Pass Phrase: *********

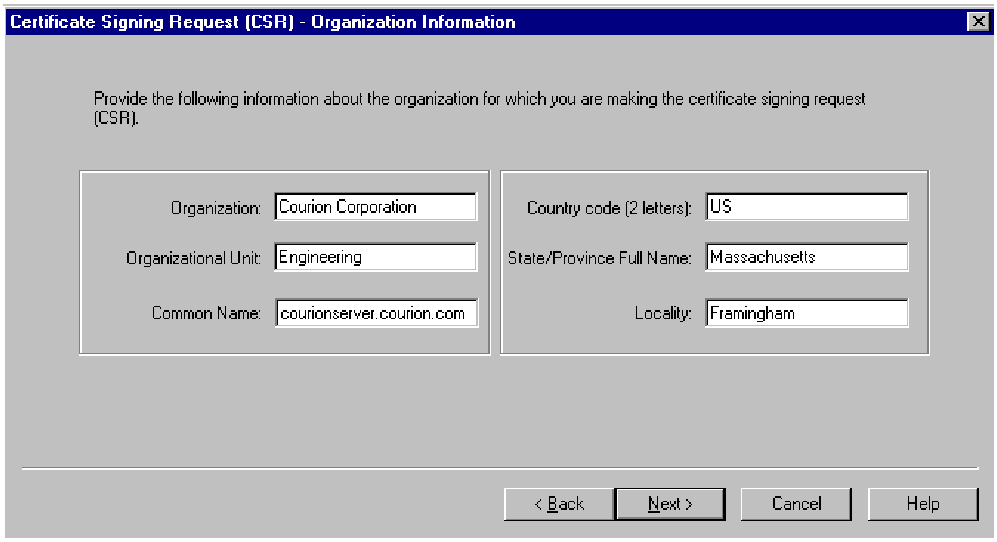
(The pass phrase is used to encrypt the private key portion of your certificate. You must remember this pass phrase in order to restore the key and certificate file later if needed.)

Private Key length (in bits): 512

CSR Organization Information

The Organization Information dialog box (*Figure 12*) creates a distinguished name, which provides an identity for the Certificate Signing Request in a specific context.

Figure 12: Organization Information



Certificate Signing Request (CSR) - Organization Information

Provide the following information about the organization for which you are making the certificate signing request (CSR).

Organization: Courion Corporation

Organizational Unit: Engineering

Common Name: courionserver.courion.com

Country code (2 letters): US

State/Province Full Name: Massachusetts

Locality: Framingham

1. In the **ORGANIZATION** field, enter the company name.
2. In the **ORGANIZATIONAL UNIT** field, enter the department name.
3. In the **COMMON NAME** field, enter the host name of the machine running the Core Server. The Common Name is included in the certificate so that the client can verify the name.
4. In the **COUNTRY CODE** field, enter the two-letter country code.
5. In the **STATE/PROVINCE FULL NAME** field enter the name of the state or province.

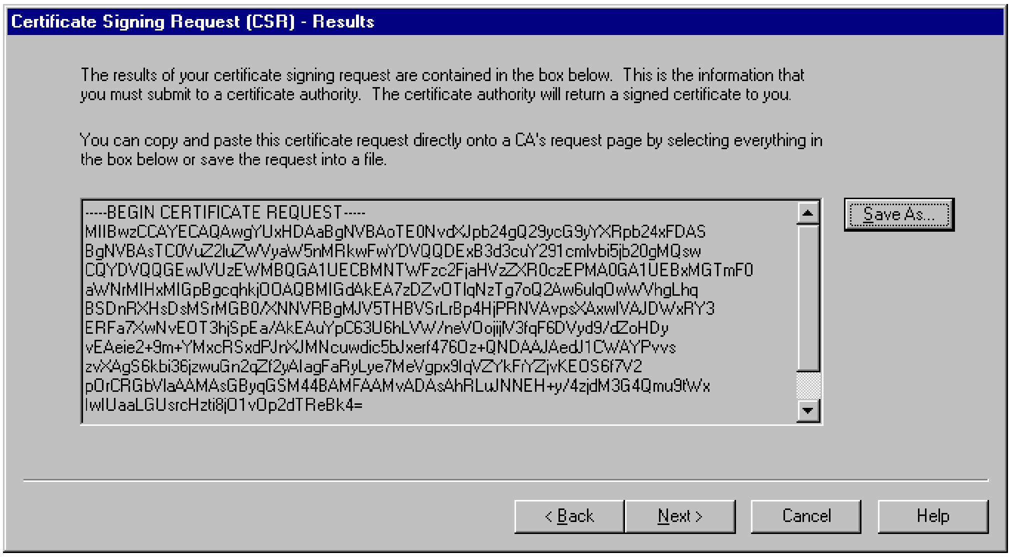
   Note: Do not use abbreviations; they render the CSR invalid.

6. In the **LOCALITY** field, enter the city or town name.
7. Click the **NEXT** button.

CSR Results

The Results dialog box (*Figure 13*) displays the generated CSR. Copy the CSR directly from the text box and pasted into a CA's certificate request page. Alternatively, save the CSR to a file via the **SAVE AS** button.

Figure 13: Results



The results of your certificate signing request are contained in the box below. This is the information that you must submit to a certificate authority. The certificate authority will return a signed certificate to you.

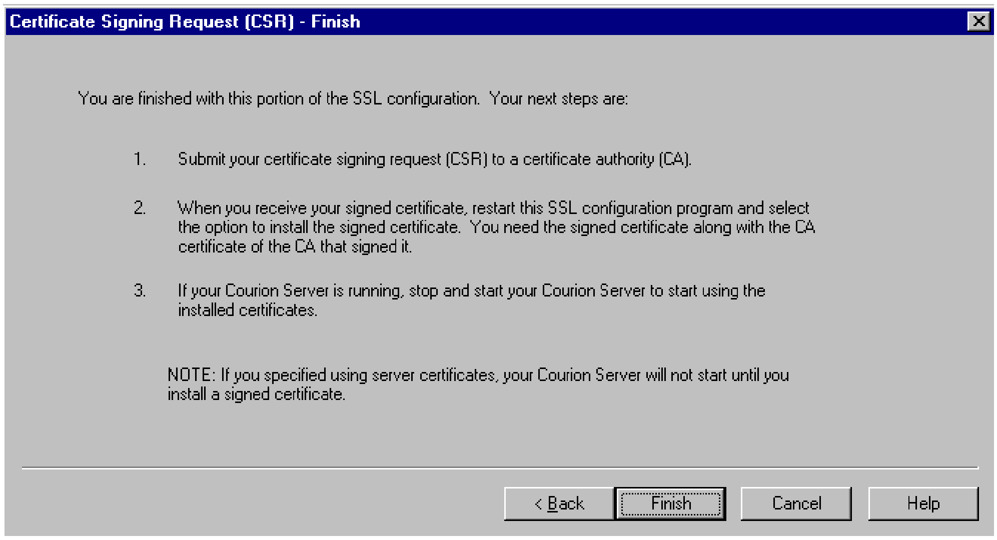
You can copy and paste this certificate request directly onto a CA's request page by selecting everything in the box below or save the request into a file.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBwzCCAYECAQAwgYUxHDAaBgNVBAoTE0NvdXJpb24gQ29ycG9yYXRpb24xFDAS
BgNVBAsTC0VuZ2luZWVyaW5nMRkwFwYDVQQDExB3d3cuY291cmlvbi5jb20gMQsw
CQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czEPMA0GA1UEBxMGTmF0
aWNrMIHxMIGpBgcqhkjOOAQBMIGdAkEA7zDZv0TIqNzTg7oQ2Aw6ulq0wWVhgLhq
BSDnRXHsDsMSrMGB0/XNNVRBgMJV5THBVSrLrBp4HjPRNVAvpsXAxwlVAJDWxRY3
ERFa7XwNvEOT3hjSpEa/AkEAuYpC63U6hLVW/neVOojjlV3fqF6DVyd9/dZoHDy
vEAeie2+9m+YMxcRSxdPJnXJMNcuwdic5bJxerf476Oz+QNDAAJAedJ1CWAYPvvs
zvXAgS6kbi36jzwuGn2qZf2yAIagFaRyLye7MeVgpx9IqVZYkFrYZjvKEOS6f7V2
pOrCRGbVlaAAMAsGByqGSM44BAMFAAMvADAsAhRLwJNNEH+y/4zjdM3G4Qmu9tWx
lwlUaaLGUsrcHzti8jO1vOp2dTReBk4=
```

CSR Finish

The Finish dialog box (*Figure 14*) outlines the steps to take once a CSR is generated. Follow the directions and click the **FINISH** button.

Figure 14: Finish



You are finished with this portion of the SSL configuration. Your next steps are:

1. Submit your certificate signing request (CSR) to a certificate authority (CA).
2. When you receive your signed certificate, restart this SSL configuration program and select the option to install the signed certificate. You need the signed certificate along with the CA certificate of the CA that signed it.
3. If your Courion Server is running, stop and start your Courion Server to start using the installed certificates.

NOTE: If you specified using server certificates, your Courion Server will not start until you install a signed certificate.

Install Existing Signed Certificate

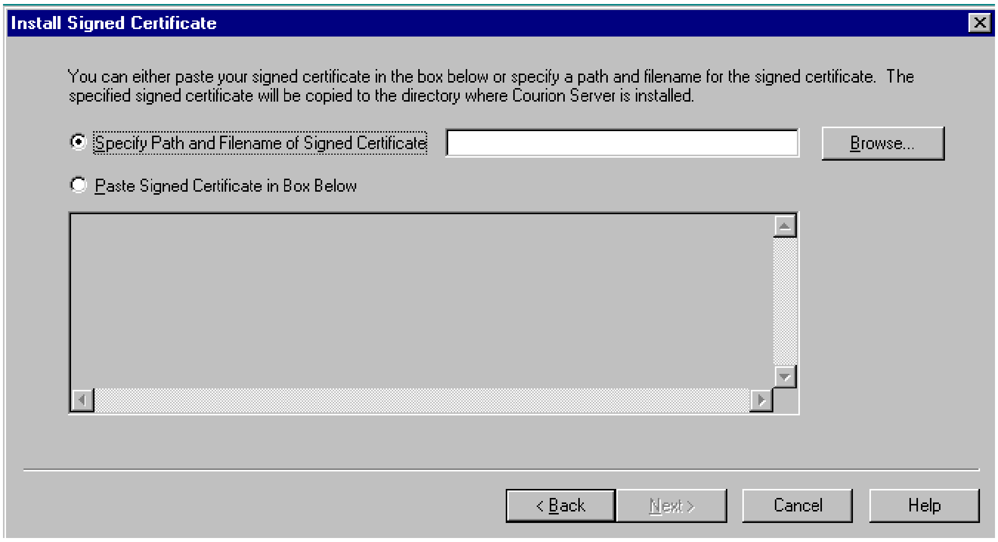
This section describes the pages presented to the administrator when the **INSTALL AN EXISTING SIGNED CERTIFICATE** option is selected.

Install Signed Certificate

The Install Signed Certificate dialog box (*Figure 15*) appears if you selected the **INSTALL EXISTING SIGNED CERTIFICATE** radio button on the Certificate Actions dialog box (*Figure 9*).

To install an existing signed certificate, either specify the file path and name or paste the certificate into the text box. If you use the file path and name method, fill in or select the path with the **BROWSE** button. If you use the paste method, the text box becomes enabled and you need to paste the contents of the signed certificate file into the text box. A CA may send back a file, an e-mail, or an HTML page from which you can copy the signed certificate.

Figure 15: Install Signed Certificate



Install Signed Certificate

You can either paste your signed certificate in the box below or specify a path and filename for the signed certificate. The specified signed certificate will be copied to the directory where Courion Server is installed.

● Specify Path and Filename of Signed Certificate

○ Paste Signed Certificate in Box Below

Regardless of the method you use, you need to specify a signed certificate.

Note: If you paste a signed certificate into the box, include the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines.

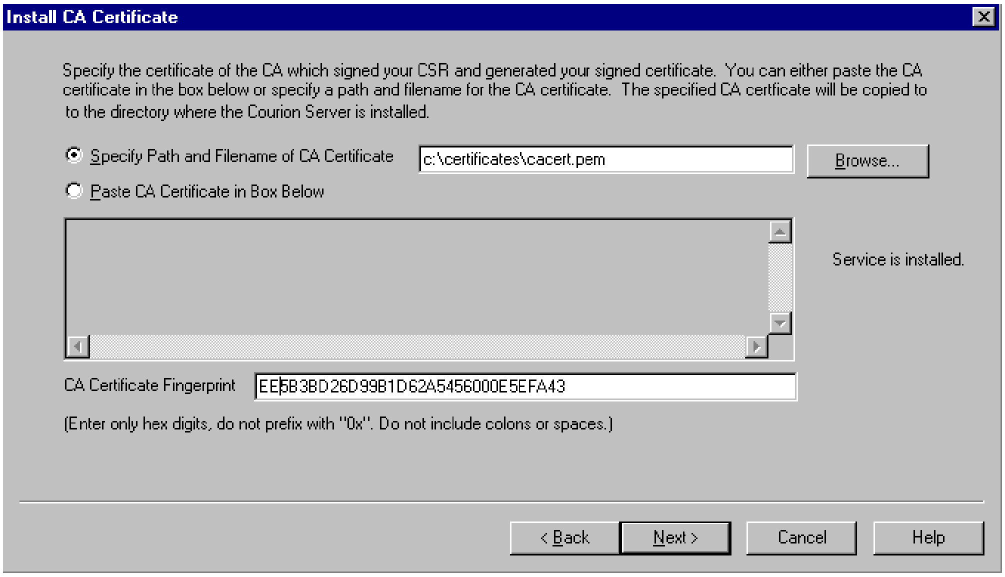
Install CA Certificate

To use a signed certificate, you need to have the corresponding CA certificate also.

To install an existing CA certificate, specify the file path and name or paste the certificate into the text box in the Install CA Certificate dialog box (*Figure 16*). If you use the file path and name method, fill in or select the path with the **BROWSE** button. If you use the paste method, the text box becomes enabled and you need to paste the contents of the signed certificate file into the text box. A CA may send back a file, an e-mail, or an HTML page from which you can copy the signed certificate.

Note: If you paste a CA certificate into the box, include the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines.

Figure 16: Install CA Certificate



Specify the certificate of the CA which signed your CSR and generated your signed certificate. You can either paste the CA certificate in the box below or specify a path and filename for the CA certificate. The specified CA certficate will be copied to to the directory where the Courion Server is installed.

● Specify Path and Filename of CA Certificate: c:\certificates\cacert.pem

○ Paste CA Certificate in Box Below

Service is installed.

CA Certificate Fingerprint: EE5B3BD26D99B1D62A5456000E5EFA43

(Enter only hex digits, do not prefix with "0x". Do not include colons or spaces.)

Enter the CA Certificate Fingerprint in the designated field below the text box. The fingerprint, which may be provided with the CA certificate, is a series of hexadecimal digits (0 to 9 and a to f) that uniquely identify that certificate. Enter only the hexadecimal digits and not the 0x before the digits. Remove all spaces and colons in the fingerprint for it to function properly.

Note: It may be necessary to contact the CA administrator directly for the certificate and fingerprint.

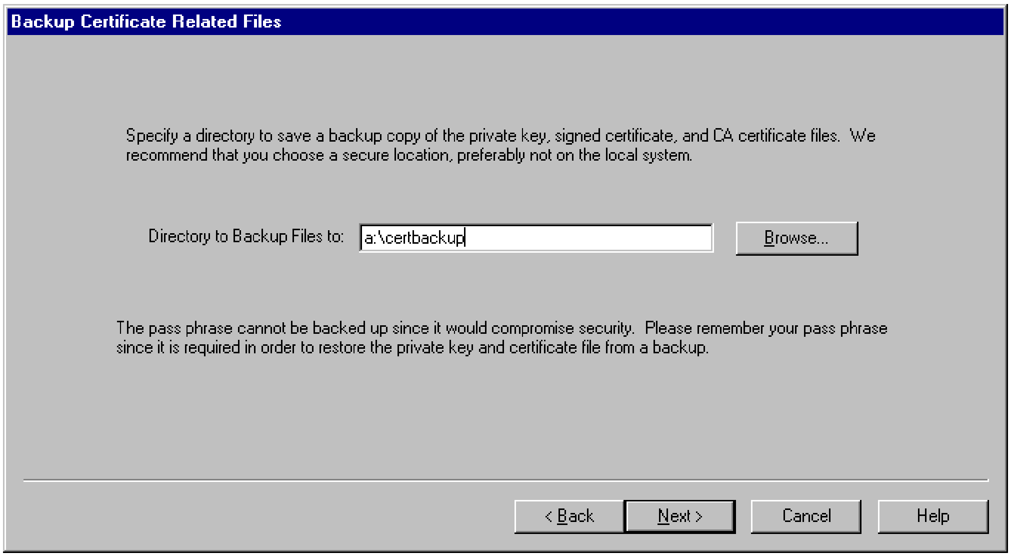
Note: Use the MDdrop-down fingerprint and not the SHA1 fingerprint (or thumbprint).

Backup Certificate Related Files

Once you install the certificate, the utility prompts you to backup certificate-related files with the Backup Certificate Related Files dialog box (*Figure 17*). This procedure backs up the following files:

1. The private key file associated with the public key on the signed certificate
2. The signed certificate
3. The certificate of the CA that signed the server's certificate
4. The fingerprint of the CA certificate

Figure 17: Backup Certificate and Related Files



Backup Certificate Related Files

Specify a directory to save a backup copy of the private key, signed certificate, and CA certificate files. We recommend that you choose a secure location, preferably not on the local system.

Directory to Backup Files to: a:\certbackup

The pass phrase cannot be backed up since it would compromise security. Please remember your pass phrase since it is required in order to restore the private key and certificate file from a backup.

Filled in the full file path or select it with the **Browse** button. If the specified folder does not exist, you are prompted to create the folder path. If the files already exist in the specified folder, you are prompted before the files are overwritten. Keep the folder path in a secure location in the system where it is accessible only by specified users, preferably a path to a different system or external device in case of system failure.

The backup suggestion is an important security measure to protect the key and certificate files in case of system failure, etc. The original files still exist in the original backup folder.

Restore an Existing Signed Certificate and Related Files

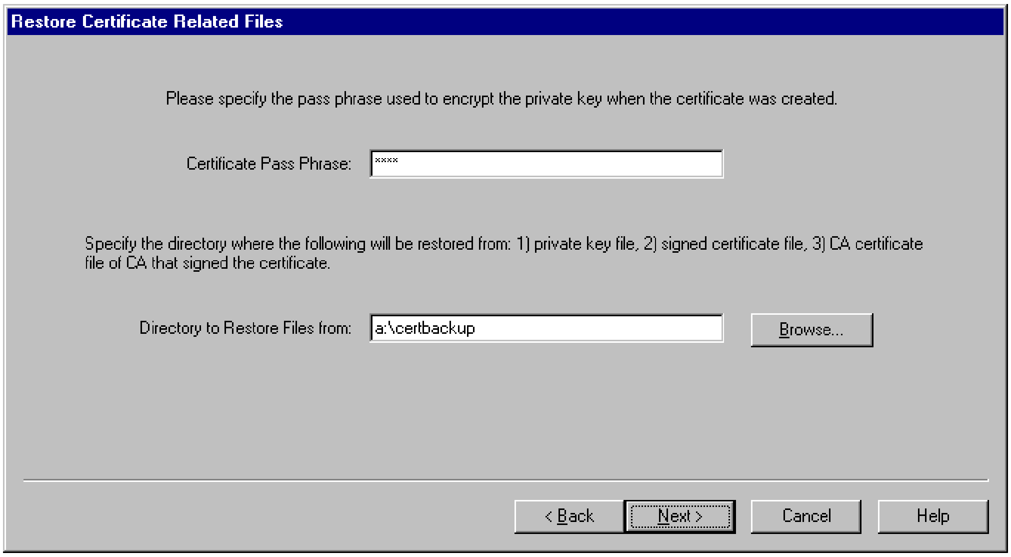
The **Restore Existing Signed Certificate and Related Files** radio button (*Figure 9*) is selected only when a signed certificate from a CA is available and a private key file and CA certificate have been backed up using the SSL Configuration Utility.

Restore Certificate Related Files

If the **Restore Existing Signed Certificate and Related Files** radio button is selected, the Restore Certificate Related Files dialog box appears when you click the **Next** button (*Figure 18*).

Note: You can restore only files that were backed up by SSLConfig.exe (*"Backup Certificate Related Files" on page 40*).

Figure 18: Restore Certificate Related Files



Restore Certificate Related Files

Please specify the pass phrase used to encrypt the private key when the certificate was created.

Certificate Pass Phrase: ****

Specify the directory where the following will be restored from: 1) private key file, 2) signed certificate file, 3) CA certificate file of CA that signed the certificate.

Directory to Restore Files from: a:\certbackup

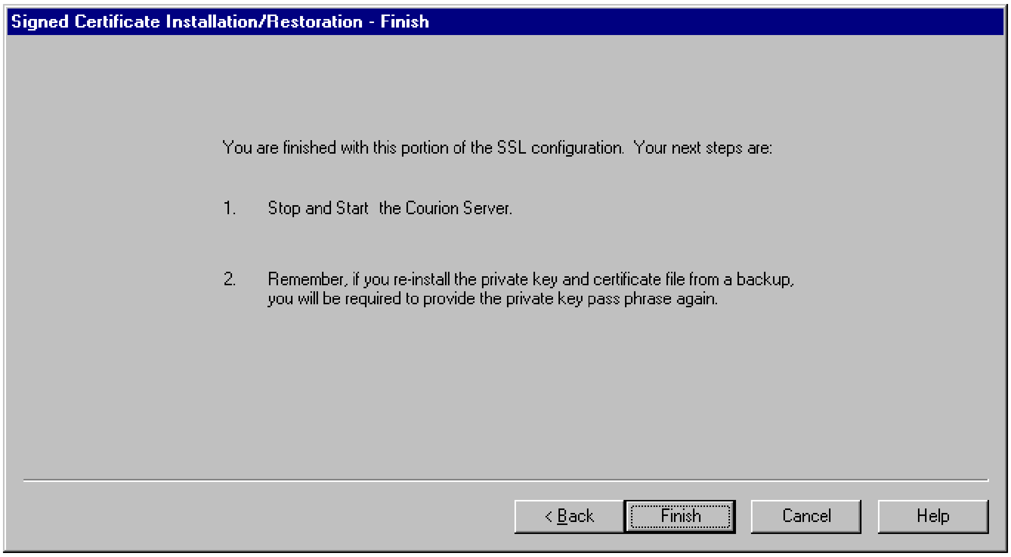
1. Enter the pass phrase used to encrypt the private key.
2. Enter the path to the folder of the certificate and related files to be restored:
   a. The private key file associated with the public key or the CSR for the signed certificate
   b. The signed certificate
   c. The certificate of the CA that signed the server certificate
   d. The fingerprint of the CA certificate
3. Click the **Next** button.

The files are restored from the specified folder. The utility issues a restore success notification or a restore error notification.

Completion of a Certificate Installation/Restoration

The Signed Certificate Installation/Restoration - Finish dialog box confirms that the signed certificate installation is complete and provides further instructions (*Figure 19*).

Figure 19: Install/Restore Signed Certificate Finish



Signed Certificate Installation/Restoration - Finish

You are finished with this portion of the SSL configuration. Your next steps are:

1. Stop and Start the Courion Server.

2. Remember, if you re-install the private key and certificate file from a backup, you will be required to provide the private key pass phrase again.

When you click the **FINISH** button, a check is made to determine whether or not the Core Server is running. If the server is not running, the utility prompts you to start the Core Server. If it is already running, the utility prompts you to stop and restart the Core Server for the changes to take effect.

Notes & Warnings

- The certificate used with the SSL Configuration Utility must be different than the certificate used for the web server.
- During the installation of a signed certificate on a single-server installation, the SSL Configuration Utility writes a file called netca.dat into the [CoreSecurityInstallPath]www\javacode folder. If any of the applet JAR files are moved into other folders, you must move a copy of the netca.dat file with them. If you do not move them, the applets are not able to establish an SSL connection with the Core Server.
- Anonymous Diffie-Hellman presents the possibility of a man in the middle attack and is not recommended.
- Anonymous Diffie-Hellman mode may be used in between the time that the CSR is generated and the signed certificate is received by running this configuration program and selecting the option to use ADH instead of a server certificate.
- When the signed certificate is available, the utility should be run again. Select the option to use a server certificate and the option to install a signed certificate. The information saved from the request to generate the CSR is used at this time.
- If a server certificate for the Core Server is being used, that certificate is checked against its expiration date every time the Core Server starts. If the certificate is due to expire within 30 days, a warning is written to the courion.log file.

Chapter 5: Configuration Migration Utility

The Configuration Migration Utility allows you to move configurations for any Access Assurance Suite application from one application server to another application server, such as a server in a test environment, to other Courion servers, such as those in production environments.

This chapter describes how to use the Configuration Migration Utility to import and export configurations for Core Security applications on the provisioning platform (Core Provisioning, Core Compliance, RoleCourier, and PasswordCourier) as well as PasswordCourier and PasswordCourier Support Staff Classic and ProfileCourier Classic.

This chapter includes the following topics:

Exporting Data in a Distributed Server Installation

In a single server installation, the Configuration Migration Utility exports most configuration data. In a distributed server installation, it exports data that exists on the server where the Courion Server component is installed. If the Connector Framework Manager is installed on a separate server from the Courion Server, you cannot export connector or PMM configuration data using this utility. In this scenario, use the Archive option to save connector and PMM configuration data. For details, see the chapter “Using the Archive Option” in the manual *Configuring Workflows with the Access Assurance Suite Administration Manager*.

Editing the utils.asp File

If the Courion Server and the Publisher web service are installed on different servers, you need to edit the file `utils.asp,` located in the following directory on the server hosting the Publisher where [CourionInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

[CourionInstallPath]\www\Utils\ConfigMigration

Open `utils.asp` in a text editor and search for the term “localhost.” Find the following statement: `server = “localhost”.` Replace localhost with the name of the server on which the Courion Server is installed.

If you changed the port of the Courion Server when you configured the Courion Server, you also need to edit the `port =` statement that follows the `server =` statement to the new port number. The default port number is 8189.

Choosing a Windows 2003 Authentication Method

You need to choose a Windows 2003 authentication method for the Core virtual directory before running the Configuration Migration Utility. You can select one of two authentication methods:

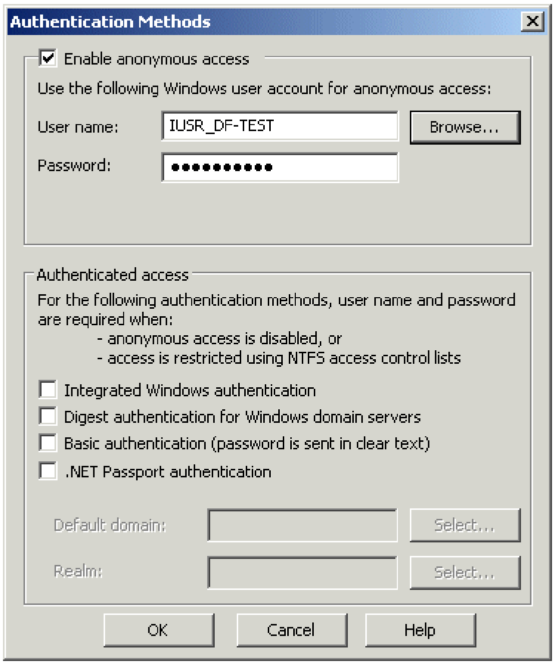
- **Anonymous Access** — The anonymous access option is enabled by default. Use this method if you have configured the Configuration Migration Utility to require authentication. Authentication is enabled if you selected the Configuration Migration Utility checkbox on the Administrator Authentication Configuration dialog during Core Server configuration. If authentication is enabled, you are required to enter a user name and password when accessing the Configuration Migration Utility.
- **Integrated Windows Authentication** — Choose this method if you have configured the Configuration Migration Utility so that it does not require authentication. With this method, the user signed on to the computer must be a member of the domain and group specified on the Administrator Authentication Configuration dialog during Core Server configuration.

To set an authentication method, follow these steps:

1. Launch Internet Information Service (IIS) Manager. Expand your local computer name, then expand Web Sites, and then Default Web Site.
2. Right-click on the Courion virtual directory and select **PROPERTIES**.
3. Select the Directory Security, then click **EDIT**.
4. Enable either **ENABLE ANONYMOUS ACCESS** or **INTEGRATED WINDOWS AUTHENTICATION**. If you select anonymous access, you must also enter a user account and password used for the anonymous access.

Figure 20 shows the Authentication Methods dialog box with Anonymous Access selected.

Figure 20: Authentication Methods Dialog Box



Authentication Methods

☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_DF-TEST

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

Configurations You Can Import and Export

When you use the configuration migration utility to move configurations from one server to another, you export the configurations to a server you specify, then import the configurations from that server to another Courion Server on the network. The configurations you can export and import depend on which applications you have configured and the features you have configured within those applications:

- **The Provisioning Platform** — On the provisioning platform, you can export and import workflows and all the configuration settings associated with those workflows. You can also export and import the targets associated with the connectors (including the PMM Gateway Connector) you configured for the workflows.
- **PasswordCourier and PasswordCourier Support Staff Classic** — For PasswordCourier and PasswordCourier Support Staff Classic, you can export and import PasswordCourier configurations (including Transparent Synchronization) and PMM configurations.
- **ProfileCourier Classic** — For ProfileCourier Classic, you can export an import user validation and profile update configurations.

For both the provisioning and classic platforms, you can export and import user validation, and ticketing and email configurations.

Global Settings You Can Export and Import

Global Settings include certain Courion Server configuration settings as well as application-specific configuration settings. These settings appear on the list of global settings only if you have configured them. Global settings can only be selected individually if you select **CUSTOM** on the Migration Actions dialog. Platform specific global settings are also exported in the **PROVISIONING CLONE** and **CLASSIC CLONE** options but can't be individually selected

Table 5 lists the global settings and where you can find more information about how you configure them.

Table 5: Global Settings you Can Import and Export (Sheet 1 of 3)

Setting	Notes
Data Source Settings	You specify these settings during Courion Server configuration, if you select Classic Platform configuration. See the manual *Installing the Access Assurance Suite* for information about Ticketing Data Source Selection.
Server Connection Port Setting	You specify this port during Courion Server configuration. See the manual *Installing the Access Assurance Suite* for information about this setting.
Data Security Settings	You specify these settings through the Data Security Utility. See the *"Data Security Utility" on page 19* for information about how to configure these settings.

Table 5: Global Settings you Can Import and Export (Sheet 2 of 3)

Setting	Notes
Administrator Authentication Configuration	You specify these settings during Courion Server configuration. See the manual *Installing the Access Assurance Suite* for information about SMTP configuration settings.
Transaction Repository Database Configuration	You specify these settings during Courion Server configuration. See the manual *Installing the Access Assurance Suite* for information about SMTP configuration settings.
Enable Users Utility Settings	See the *“Enable Users Utility” on page 7* for information about how to configure these settings.
Disabled User’s List	See *“Listing Disabled Users” on page 10* for the Enable Users Utility.
PIN Generator	See the manual *Using ProfileCourier Classic* for information about this feature.
Transparent Sync SPML File	These settings are contained in the SPML file accessed by the PasswordCourier Transparent Sync feature (via the XML Access Option). See the *Access Assurance Suite Implementation Guide* for details.
SMTP Configuration	You specify these settings during Courion Server configuration. See the manual *Installing the Access Assurance Suite* for information about SMTP configuration settings.
SSL Config	See *“SSL Configuration Utility” on page 31* for information about the settings for this utility.
Remote PMM Targets	You specify these settings in the Remote Proxy Configuration manager. See the chapter “Configuring a Proxy Server for Remote Password Management” in the manual *Installing the Access Assurance Suite* for information about these settings.
PMM Agent Configuration for Netscape Directory Server	See the manual *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information about how to configure agents.
ProfileCourier Classic Web Access Configuration Manager	See the chapter “Web Access (ASP) Configuration” in the *Access Assurance Suite Implementation Guide* for information about how to configure these settings.
PasswordCourier Support Staff Web Access Configuration Manager	See the chapter “Web Access (ASP) Configuration” in the *Access Assurance Suite Implementation Guide* for information about how to configure these settings.
PasswordCourier Web Access Configuration Manager	See the chapter “Web Access (ASP) Configuration” in the *Access Assurance Suite Implementation Guide* for information about how to configure these settings.
Access Assurance Suite Web Access Configuration	See the chapter “Web Access (ASP) Configuration” in the *Access Assurance Suite Implementation Guide* for information about how to configure these settings.
Access Assurance Suite Administration Manager Configuration	See the chapter “Web Access (ASP) Configuration” in the *Access Assurance Suite Implementation Guide* for information about how to configure these settings.

Table 5: Global Settings you Can Import and Export (Sheet 3 of 3)

Setting	Notes
Access Key Configuration	You specify access keys during Courion Server configuration. See the manual *Installing the Access Assurance Suite* for information about access key configuration.
Performance Settings	These settings relate to application performance.

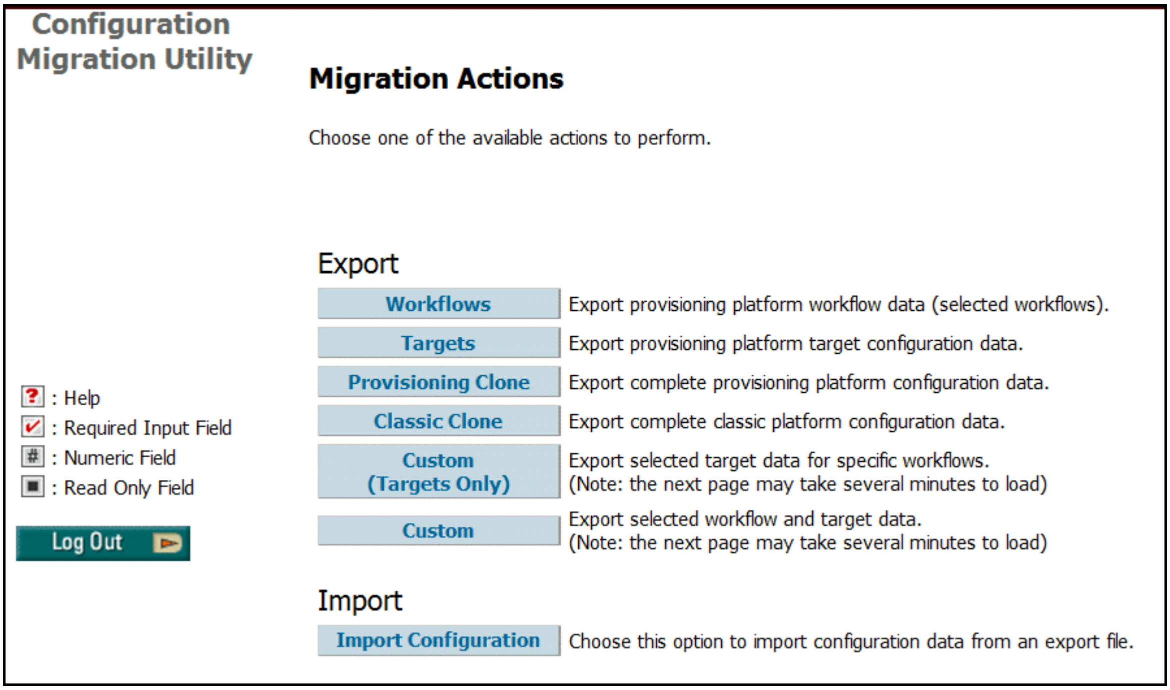
Launching the Configuration Migration Utility

To run the Configuration Migration Utility:

1. From the Access Assurance Suite administration console, click **Toolbox**.
2. Click **Migration**, then click **Start**.
3. If authentication is enabled, enter the appropriate username and password information and click **Submit**. (Authentication is enabled if the Configuration Migration Utility checkbox was enabled on the Administrator Authentication Configuration dialog during Courion Server configuration.)

   If authentication is not required or the required login information has been entered, the Configuration Migration Utility displays the dialog box shown in *Figure 21*.

Figure 21: Migration Actions Screen



Configuration Migration Utility

Migration Actions

Choose one of the available actions to perform.

Export

Workflows	Export provisioning platform workflow data (selected workflows).
Targets	Export provisioning platform target configuration data.
Provisioning Clone	Export complete provisioning platform configuration data.
Classic Clone	Export complete classic platform configuration data.
Custom (Targets Only)	Export selected target data for specific workflows. (Note: the next page may take several minutes to load)
Custom	Export selected workflow and target data. (Note: the next page may take several minutes to load)

Import

Import Configuration	Choose this option to import configuration data from an export file.

? : Help
✓ : Required Input Field
: Numeric Field
■ : Read Only Field

Log Out

From this screen you can export configuration information from the Courion Server (see *"Exporting Configurations" on page 52*) or import previously saved configuration from another Courion Server (see *"Importing Configurations" on page 55*).

There are six different options for exporting configuration information:

- **Workflows** — This option selects all workflow data. You can select individual workflows or all of them. Target data from within the workflows is included, but not the data from the Data Security Utility, the Connector Configuration Manager and individual PMM configuration.
- **Targets** — This option selects target data. You can select individual targets or all of them. Target data from the Connector Configuration Manager and individual PMM configuration is included, but not the target data configured from within workflows.

- **PROVISIONING CLONE** — This option selects all workflow data, and all global and target data that applies to the provisioning platform. It does not include PMMs that have been configured for the classic platform only. With this option, all provisioning platform data is saved—you can not select individual workflows or targets. If you know that you want to export all provisioning data, this option is the best choice; it loads faster than the custom option because a selection tree is not built.
- **CLASSIC CLONE** — This option selects all Customization Manager configuration data and all global target data that applies to the classic platform. It does not include PMMs that have been configured for the provisioning platform only. With this option, all classic platform data is saved—you can not select individual targets.
- **CUSTOM (TARGETS ONLY)** — This option selects all target data from the Target option, plus all target configuration data from within the workflows. You can select individual targets or all of them.
- **CUSTOM** — This option selects all workflow, target, and global data. You can select everything or select individual workflows, targets, and global settings.

Exporting Configurations

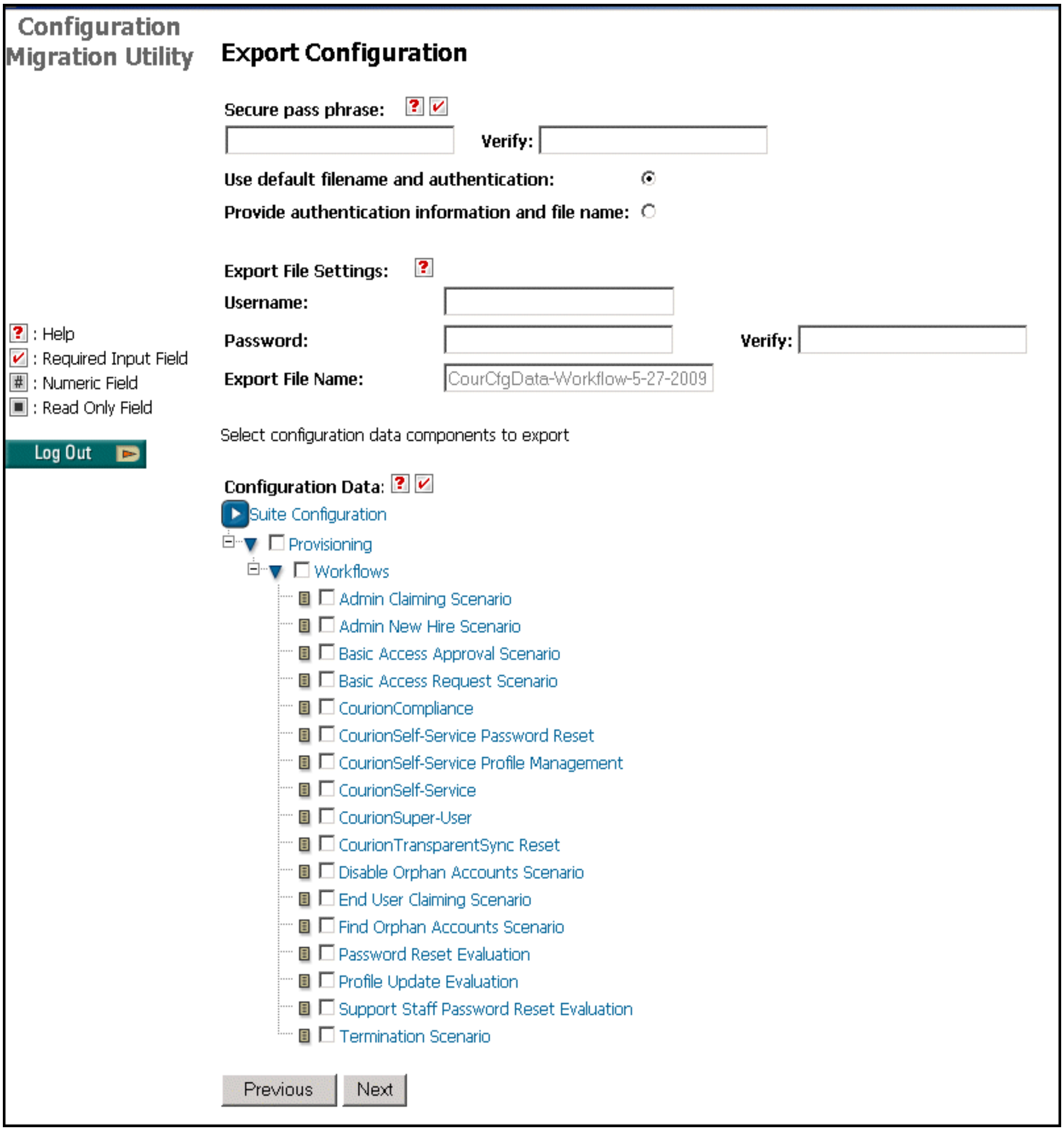
The Export options export configuration information to a secure XML file in a location you specify.

To export configuration information:

1. Select an Export option from the Migration Actions screen (*Figure 21*). There is a pause while the utility generates an export tree. The pause can be quite lengthy, depending on which option was selected and the number of configured workflows and targets.

   An Export Configuration dialog box appears as in *Figure 22*, which shows the dialog box for the Workflows option. The Workflows data folder is expanded in this figure to show the workflows available to export.

Figure 22: Export Configuration Screen



Configuration Migration Utility

Export Configuration

Secure pass phrase: ? ✓

Verify:

Use default filename and authentication: ●

Provide authentication information and file name: ○

Export File Settings: ?

Username:

Password: Verify:

Export File Name: CourCfgData-Workflow-5-27-2009

? : Help
✓ : Required Input Field
: Numeric Field
■ : Read Only Field

Log Out

Select configuration data components to export

Configuration Data: ? ✓

Suite Configuration
- □ Provisioning
  - □ Workflows
    - □ Admin Claiming Scenario
    - □ Admin New Hire Scenario
    - □ Basic Access Approval Scenario
    - □ Basic Access Request Scenario
    - □ CourionCompliance
    - □ CourionSelf-Service Password Reset
    - □ CourionSelf-Service Profile Management
    - □ CourionSelf-Service
    - □ CourionSuper-User
    - □ CourionTransparentSync Reset
    - □ Disable Orphan Accounts Scenario
    - □ End User Claiming Scenario
    - □ Find Orphan Accounts Scenario
    - □ Password Reset Evaluation
    - □ Profile Update Evaluation
    - □ Support Staff Password Reset Evaluation
    - □ Termination Scenario

Previous Next

The Export Configuration dialog box for other configuration options are similar to this one, except that the choices in the Configuration Data section are specific to the option that you chose.

2. In the Export Configuration dialog box, enter the following information into the appropriate fields:

   In the **SECURE PASS PHRASE** box, enter the pass phrase that was provided when the server was configured. Re-enter this pass phrase in the **VERIFY** box.

   Select **USE DEFAULT FILENAME AND AUTHENTICATION** to use the **USERNAME** and **PASSWORD** that you used to authenticate into the Configuration Migration utility. This option also uses the default **EXPORT FILE NAME**. When you select this option, you cannot enter new Export File Settings in the next section of the dialog box.

   The export file is saved to the [CourionInstallPath]\Courion Service directory where [CourionInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation.

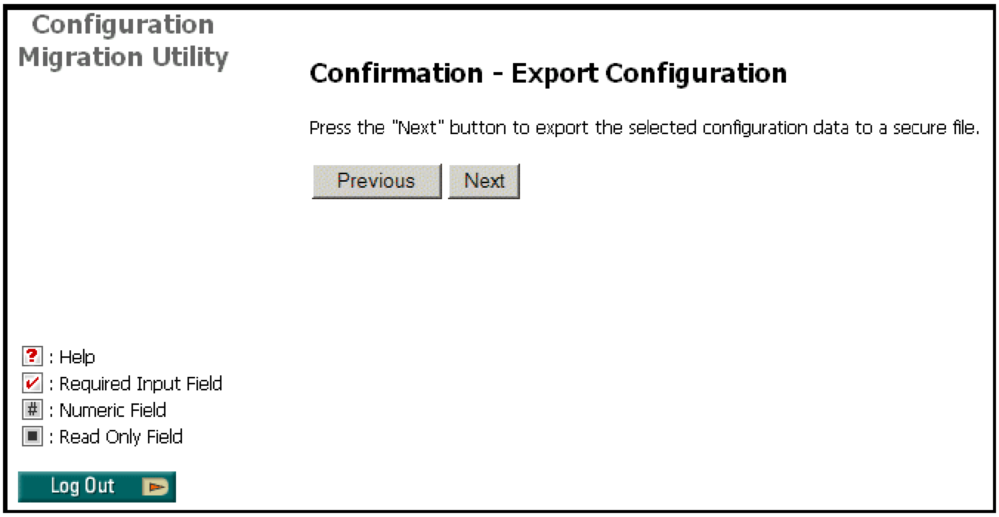
   Select **PROVIDE AUTHENTICATION INFORMATION AND FILE NAME** to enter new Export File Settings. You can save to a directory other than the default directory by specifying the complete path\file name.

   Note: Whether you use the default username or enter a different username, you must make sure that the user has permissions to write to the directory on the server where you specify the export file name.

   Check the boxes next to the **CONFIGURATION DATA** that you want to export. Checking a “parent” box automatically selects all “child” boxes associated with that parent. Expand the parent box to select individual child boxes.

   Click **NEXT** to start the export process. The Export Configuration Confirmation screen appears as in *Figure 23*.

Figure 23: Export Configuration Confirmation

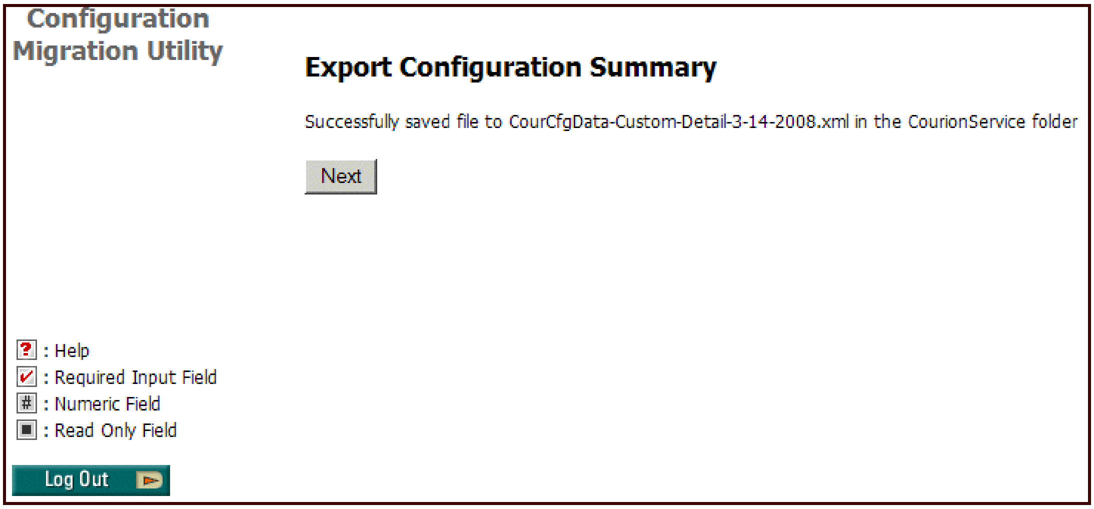


Confirmation - Export Configuration

Press the "Next" button to export the selected configuration data to a secure file.

3. Click **NEXT** to continue with the export configuration operation. The Export Configuration Summary screen appears, as shown in *Figure 24*. A message confirms the name of the saved file and its location.

Figure 24: Export Configuration Summary Screen



Export Configuration Summary

Successfully saved file to CourCfgData-Custom-Detail-3-14-2008.xml in the CourionService folder

4. Click **NEXT** to return to the Migration Actions screen.

   Note: Core Security does not recommend that you edit the configuration data in the XML file.

Importing Configurations

The Import Configuration option allows you to import a previously saved configuration information from a secure XML file.

Note: The version and update level of the Access Assurance Suite running on the system where you created the configuration file that you exported must be the same as the version and update level of the Access Assurance Suite running on the destination system. For example, if the Courion Server where you created the configuration file is running 7.80 update 1, the Courion Server where you are importing the configuration file must be running 7.80 update 1. If the version and software levels do not match, the Migration Utility does not import the file.

Importing Large Files

Timeout Limit

If an XML file you are importing or exporting is very large, more than one MB for example, increase the ASP script timeout to at least 300 seconds. If you do not do this, the ASP page may time out while the file is being transferred and some data may be lost. To increase the ASP script timeout:

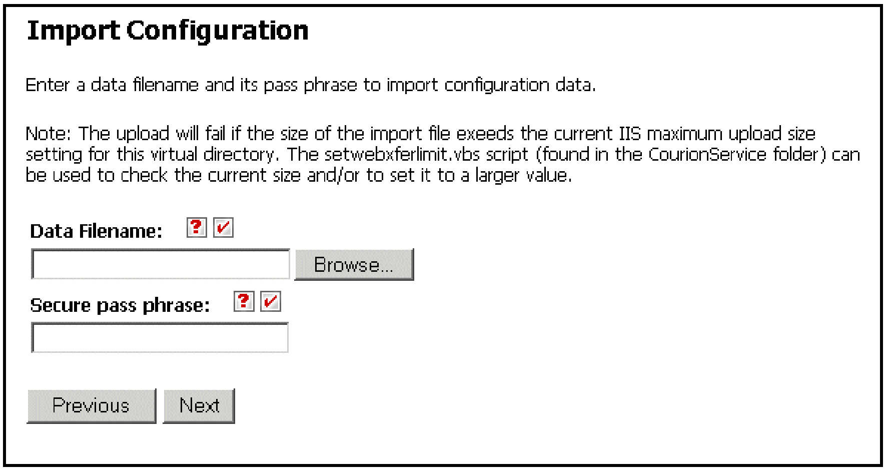
1. Launch Internet Information Service (IIS) Manager. Expand the computer, then expand web Sites, and then Default Web Site.
2. Right-click on the Courion virtual directory and select **PROPERTIES**.
3. On the Virtual Directory tab, click the **CONFIGURATION** button.
4. Click the **OPTIONS** tab.
5. Change the **ASP SCRIPT TIMEOUT**.
6. Click **OK** twice.

Importing Configuration Data

1. Select **IMPORT CONFIGURATION** from the Migration Actions screen (*Figure 21*). The import configuration screen appears as in *Figure 25*.

   A note on the screen indicates that the upload will fail if the size of the import file exceeds the current IIS maximum upload size for the virtual directory. The Courion virtual directory created during the installation process is automatically set to 20MB, so it should not need to be changed if you are using the default virtual directory. If you create your own virtual directories, you must run the `setwebxferlimit.vbs` script in the CourionService folder to increase the size of the web transfer limit. See the chapter “Providing Provisioner Access to Workflows” in the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for details.

Figure 25: Import Configuration Screen



Import Configuration

Enter a data filename and its pass phrase to import configuration data.

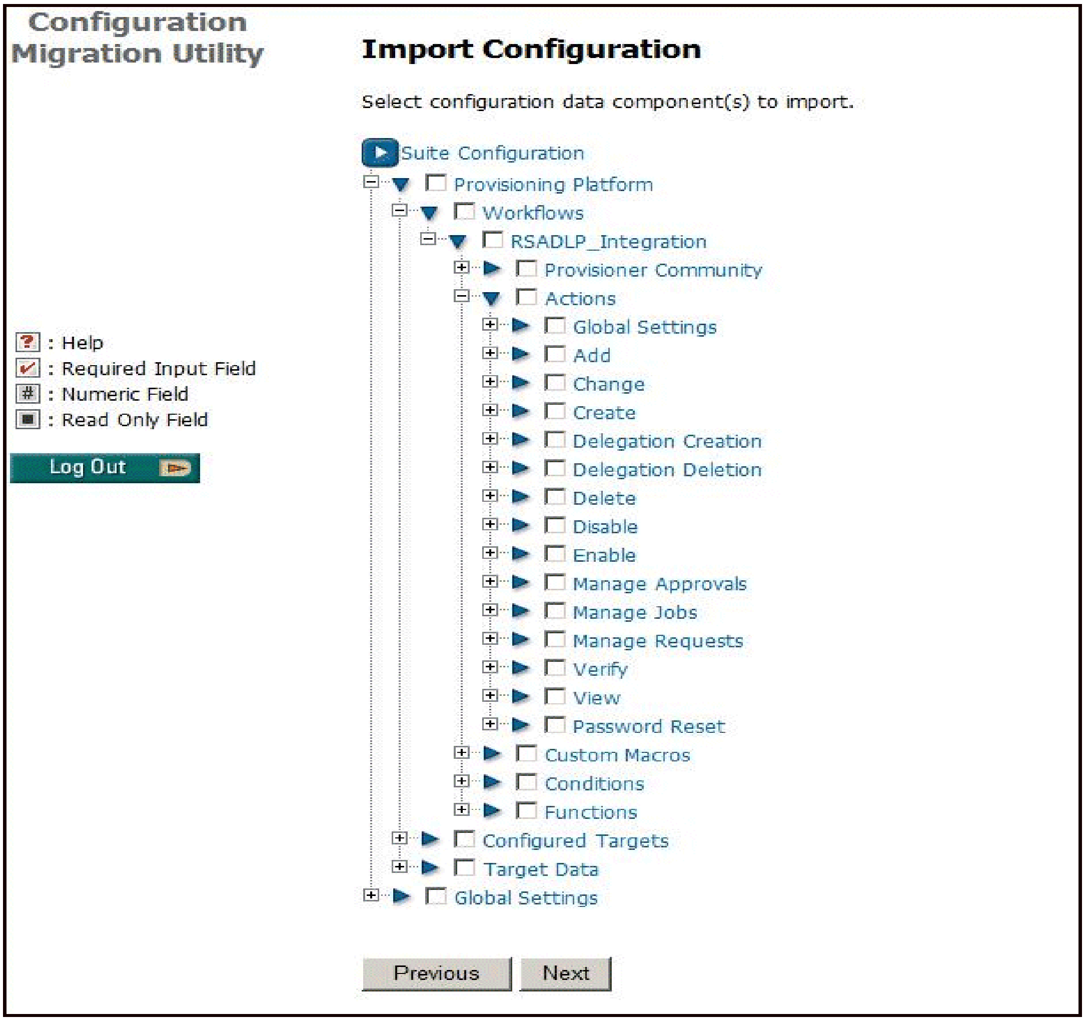
Note: The upload will fail if the size of the import file exeeds the current IIS maximum upload size setting for this virtual directory. The setwebxferlimit.vbs script (found in the CourionService folder) can be used to check the current size and/or to set it to a larger value.

2. In the **Data Filename** box, enter the name of the XML file with the configuration information you want to import, or click the **Browse...** button to select a file from the list. By default, the browser starts in the folder where the last configuration file was saved.

3. Enter the **Secure Pass Phrase** you entered when you exported the configuration file. Click **Next**.

4. The Import Configuration screen appears. *Figure 26* shows an example of an Import Configuration screen with configuration data from the provisioning platform.

Figure 26: Import Configuration Screen



Configuration Migration Utility

Import Configuration

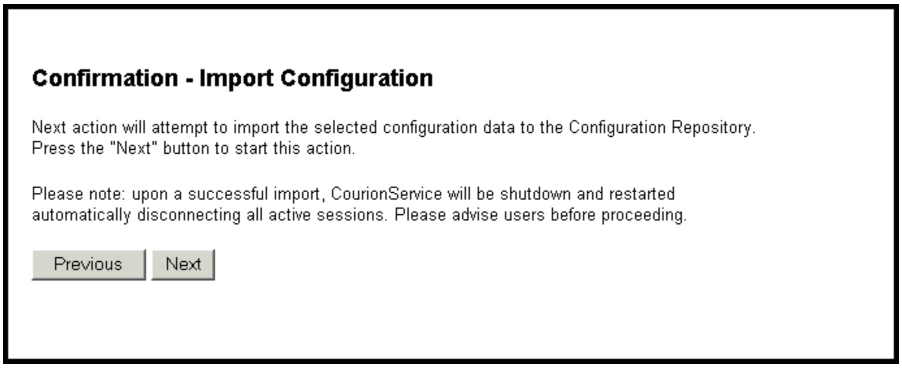
Select configuration data component(s) to import.

- Suite Configuration
  - □ Provisioning Platform
    - □ Workflows
      - □ RSADLP_Integration
        - □ Provisioner Community
        - □ Actions
          - □ Global Settings
          - □ Add
          - □ Change
          - □ Create
          - □ Delegation Creation
          - □ Delegation Deletion
          - □ Delete
          - □ Disable
          - □ Enable
          - □ Manage Approvals
          - □ Manage Jobs
          - □ Manage Requests
          - □ Verify
          - □ View
          - □ Password Reset
        - □ Custom Macros
        - □ Conditions
        - □ Functions
    - □ Configured Targets
    - □ Target Data
  - □ Global Settings

? : Help
✓ : Required Input Field
: Numeric Field
■ : Read Only Field

5. Select the configurations that you want to import from the Import Configuration Screen. Click **NEXT**. The Import Configuration Confirmation Screen appears (*Figure 27*).

Figure 27: Confirmation-Import Configuration Screen



Confirmation - Import Configuration

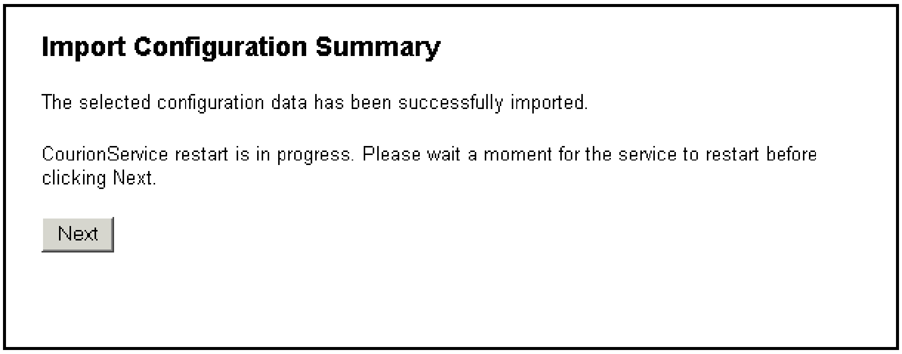
Next action will attempt to import the selected configuration data to the Configuration Repository.
Press the "Next" button to start this action.

Please note: upon a successful import, CourionService will be shutdown and restarted automatically disconnecting all active sessions. Please advise users before proceeding.

6. Click **NEXT** to start importing the configuration to the destination Courion Server. The utility imports the data to the appropriate files. After the configuration file has been imported successfully, the utility automatically shuts down and restarts the

CourionService. Additionally, web services are restarted if the import contains PMM or connector configuration data. While services are being restarted, the Import Configuration Summary screen appears, as in *Figure 28*.

Figure 28: Import Configuration Summary Screen



Import Configuration Summary

The selected configuration data has been successfully imported.

CourionService restart is in progress. Please wait a moment for the service to restart before clicking Next.

After the CourionService restarts, click **NEXT**.

Notes on Importing Specific Configuration Information

For PasswordCourier and PasswordCourier Support Staff you must manually specify some information after you import configurations with the Configuration Migration Utility.

- **Transparent Synchronization** — You need to install and configure Transparent Synchronization services (including the Transparent Synchronization Service and the GAT Service) on the destination server after you migrate this configuration, if it is not already installed and configured on this server.
- **Peregrine Ticketing Configurations** — You must edit the WINDOWS Services file to specify the tcp port and the udp port on the Courion Server for Peregrine ticketing configurations. To do this, navigate to the following directory:

  ```
  WINDOWS\system32\drivers\etc
  ```

  Select the Services file, open it, and add the following Service Name and Port Number information for tcp and udp:

  ```
  <service name>     <port number>
  scauto              12690\tcp
  scauto              12690\udp
  ```

- **Data Source Migration for Database Password Management Modules** — You must manually create the target data source on the destination server after you import configurations for database PMMs, including the PMMs for Microsoft SQL Server™, Oracle®, and Sybase® Adaptive Server®. The Target Data Source Name on the destination server must match the Target Data Source Name on the server with the source configuration for the PMM.
- **ODBC Ticketing** — If the help desk database has a primary key that is the key field for ODBC ticketing and the ticketing is not configured on the destination server, then you need to configure the ticket ID if after you import a configuration.

Chapter 6: Using the ConfigMover: Targets Utility

The ConfigMover: Targets utility reads target configuration data stored in the Microsoft Windows Management Interface (WMI) and exports it into an XML file that you specify. You can then use the utility to import the configuration data back to the WMI. Include a passphrase to encrypt the XML file with the configuration data to make it secure.

The configuration data in the XML file includes the information about the target provided through the Connector Configuration Manager. See the manual *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information about using the Connector Configuration Manager to configure specific targets.

You can use the ConfigMover: Targets utility by issuing commands from the Windows Command Prompt or through the ConfigMover: Targets dialog box. This chapter describes how to access the ConfigMover: Targets utility, use the utility to import and export configuration data, and provides examples of how to do this in the following sections:

- *"Using the ConfigMover: Targets Dialog Box" on page 60*
- *"Using the ConfigMover: Targets Utility from the Windows Command Prompt" on page 62*
- *"Logging" on page 64*

Requirements

You need to be a member of the local Administrator group on the local system where you run the ConfigMover: Targets utility.

You need to launch the ConfigMover: Targets utility with the Run as Administrator option.

Stopping and Starting Courion Services

Before you run this utility from the Windows Command Prompt, stop all Courion Services on the Connector Framework Manager (CFM) and all Connector Frameworks (CFs). When you have completed running the utility, restart Courion Services.

If you access the ConfigMover: Targets dialog box, Courion Services are automatically stopped and restarted. No manual intervention is required.

Using the ConfigMover: Targets Dialog Box

To access the ConfigMover: Targets dialog box, click on the ConfigMoverTargets.exe file in the following location where [CoreSecurityInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

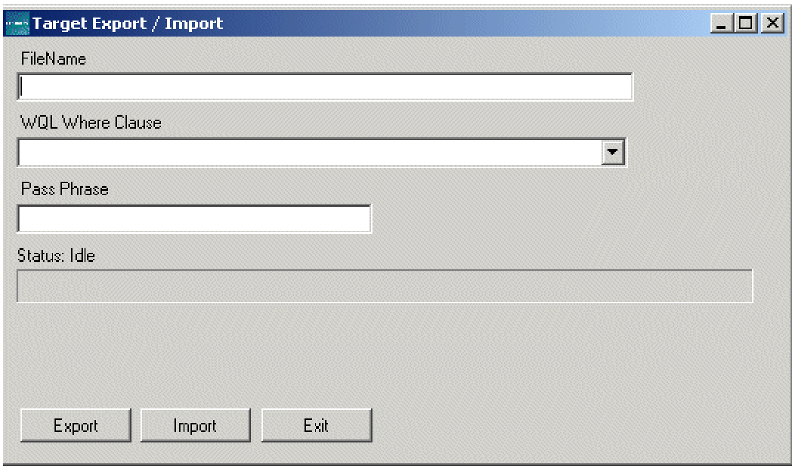
[CourionInstallPath]\CourionService

Or enter the following from the Command Prompt at that location:

```
ConfigMoverTargets.exe
```

Figure 29 shows the ConfigMover: Targets dialog box.

Figure 29: ConfigMover: Targets Dialog Box



Enter the following information:

FILENAME - Enter the name of the file that you want to export or import. It must have a .xml extension. This field is required. If you do not specify a pathname, the utility exports it to the CourionService directory. Example: C:\MyFiles\MyCore\MyExportFiles\AD-Targets.xml

WQL WHERE CLAUSE - This optional field applies to the export action only. You can enter a WQL compliant “where” clause to limit export to specific targets or connectors. You can select either a connector or target name from the drop-down list or enter your own “where” clause:

Where Connector = ‘<*insert Connector*>’

Where Name = ‘<*insert Target Name*>’

Examples:

Where Connector = ‘Microsoft-ADS-drop-down.x’

Where Name = ‘Active Directory’

See the manual *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information about connector names.

For more information about WMI compliant “where” clauses, see:

http://msdn.microsoft.com/en-us/library/aa392902(VS.8drop-down).aspx

PASS PHRASE - Supply an alphanumeric passphrase that encrypts the data that you are exporting. You need to supply this phrase to import the data and decrypt it. Example: 123ActDir

STATUS - This field displays **IDLE** until you press the **EXPORT** or **IMPORT** button, then it displays **PROCESSING**. When the action is complete, it displays **FINISHED** and the elapsed time. You do not enter data into this field.

EXPORT - Click this button to export the file you specified. The utility encrypts the data you are exporting.

IMPORT - Click this button to import the file you specified. Supply the passphrase in the Pass Phrase field.

Using the ConfigMover: Targets Utility from the Windows Command Prompt

To access the ConfigMover: Targets utility, do the following:

1. Log in as a member of the local Administrator group.
2. Launch the command prompt as an administrator. Go to **START** > **ALL PROGRAMS** > **COMMAND PROMPT**.
3. Right-click and select **RUN AS ADMINISTRATOR**.
4. Navigate to the following directory where [CourionInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

   [CourionInstallPath]`\CourionService`
5. Enter the `ConfigMoverTargets.exe` command with arguments to import and export data.

Entering the `ConfigMoverTargets.exe` command without arguments produces the ConfigMover: Targets dialog box, as described in *"Using the ConfigMover: Targets Dialog Box" on page 60*.

Note: The `ConfigMoverTargets.exe` command and command arguments are case-sensitive.

ConfigMoverTargets.exe Arguments

Table 6 describes the ConfigMoverTargets.exe arguments.

Table 6: ConfigMoverTargets.exe Arguments (Sheet 1 of 2)

Argument	Description
`-help` -h -?	Any one of these arguments displays help text for the ConfigMoverTargets.exe command.
`-export -filename=<`*`name`*`>`	Where *`name`* is the name of the file that you want to export. It must have a .xml extension. Example: AD-Targets.xml
`-passphrase=<`*`passphrase`*`>`	Argument with the `-export` argument. Where *`passphrase`* is a passphrase that encrypts the data you are exporting. You must supply the same passphrase when you import the data.

Table 6: ConfigMoverTargets.exe Arguments (Sheet 2 of 2)

Argument	Description

`[-queryString=<WQL Query String>]`	Optional argument with the `-export` argument.
	Where *WQL Query String* is a WQL compliant “where” clause to limit export to specific targets or connectors.
	Examples:
	`“Where Connector = ‘Microsoft-ADS-drop-down.x’”`
	`“Where Name = ‘Active Directory’”`
	See the manual *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information about connector names.
	For more information about WMI compliant “where” clauses, see:
	http://msdn.microsoft.com/en-us/library/aa392902(VS.8drop-down).aspx

`[-overwrite]`	Optional argument with the `-export` argument. Overwrites an existing XML configuration data file with the same name.
`-import -filename=<name>`	Where *name* is the name of the file that you want to import. It must have a .xml extension. Example: AD-Targets.xml. With the `-import` argument, you must include the following argument if the file you are importing was exported with a pass phrase: `[-passphrase=<passphrase>]` Where *passphrase* is a phrase specified when the file you are importing was exported.

Examples

Sample syntax for exporting all targets configured for the Connector for Microsoft Active Directory:

```
ConfigMoverTargets.exe -export -filename=AD-Targets.xml
-passphrase=123ActDir -queryString=”Where Connector = ‘Microsoft-ADS-drop-
down.x’”
```

Sample syntax for importing all targets configured for the Connector for Microsoft Active Directory:

```
ConfigMoverTargets.exe -import -filename=AD-Targets.xml
-passphrase=123ActDir
```

Sample syntax for exporting a single target called Company Domain:

```
ConfigMoverTargets.exe -export -filename=AD-Targets.xml
-passphrase=123ActDir -queryString=”Where Name = ‘Company Domain’”
```

Logging

The ConfigMover: Targets utility log file is ConfigMoverTargets.log.

The utility supports 3 levels of logging: 0, 1 and 2. Each level is more verbose than the last. The logging level is controlled by editing the file ConfigMoverTargets.exe.config. An example of the file is shown below. Make sure the utility is not running when you edit this file.

```
<?xml version="1.0" encoding="utf-8" ?>

<configuration>

  <appSettings>

    <add key="LogLevel" value="1"/>

  </appSettings>

</configuration>
```

Set the value of the LogLevel to 0, 1 or 2. Then save the file.

Chapter 7: Exporting and Importing Workflows using the ConfigMover: Workflows Utility

The ConfigMover: Workflows utility reads workflow configuration data stored in the Cfgfile.db file and exports it into an XML file that you specify. You can then use the utility to import the configuration data back to Cfgfile.db. The ConfigMover: Workflows utility runs within a Windows command line session.

The configuration data in the XML file includes the information about the workflow provided through the Access Assurance Suite Administration Manager. Refer to the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for information about using the Administration Manager to configure specific workflows.

Version Checking

By default, the utility checks that the version and update level of the Access Assurance Suite running on the server from where you exported the file is the same as the version and update level of the Access Assurance Suite running on the server where you are importing the file. For example, if the server where you exported the file is running 8.4 Update 1, the server where you import the file should be running 8.4 Update 1. Otherwise, the utility does not import the file and displays the following warning message:

```
“WARNING: Version mismatch. Import workflow version does
not match this system.  Import version: (version number)
Local system: (version number) - abort import process.”
```

However, if you want to import a configuration file from a server running a different version and/or update level of the Access Assurance Suite, you can override the default behavior with the -noversioncheck argument when you import the file. If you use this argument and the versions do not match, the utility displays the following warning message:

```
"WARNING: Version matching turned off. Import version:
(version number)   Local system: (version number) -
continue to import."
```

Planning

The ConfigMover: Workflow utility supports importing of workflows originating from different AAS releases.

- If the source system is running a release of AAS prior to 8.4, no pass phrase is required to import the workflow.
- If the source system is running AAS release 8.4, the specified pass phrase must match the pass phrase that was entered in the Site Settings window of the Configuration Manager.

Also, if the pass phrase contains a special character (including but not limited to symbols such as @, #, $, %, ^, &, *), when you specify it in the command line, you must escape the special character using a backslash. For example, if the pass phrase is **Hello$Test**, you would specify the following:

–passphrase=Hello\$Test

If the passphrase contains a space such as **Hello Test**, you must enclose the passphrase in quotations marks as follows:

-passphrase="Hello Test"

- If the source system is running AAS release 8.4 update 1 or later, the pass phrase must match the value that was specified using the -passphrase argument during the export of the workflow configuration file. That is, each workflow has its own unique pass phrase.
- White space or blank elements are preserved when importing the workflow configuration data from an exported XML file. For example, a workflow is exported from Server A which contains white space that is either user defined or by default in the text entered for form instructions. When this workflow is imported to Server B, and opened in the Administration Manager, the text for form instructions correctly shows the white spaces that were imported.

Requirements

You need to be a member of the local Administrator group on the local system where you run the ConfigMover: Workflows utility.

You need to launch the ConfigMover: Workflows utility with the Run as Administrator option.

Stopping Courion Services

Before you run this utility, stop all Courion Services on the Connector Framework Manager (CFM) and all Connector Frameworks (CFs).

Using the ConfigMover: Workflows Utility

To access the ConfigMover: Workflows utility, do the following:

1. Log in as a member of the local Administrator group.
2. Launch the command prompt as an administrator. Go to **START** > **ALL PROGRAMS** > **COMMAND PROMPT**.
3. Right-click and select **RUN AS ADMINISTRATOR**.
4. Navigate to the following directory where [CourionInstallPath] represents the default path of C:\Program Files (x86)\Courion Corporation:

   [CourionInstallPath]`\CourionService`
5. Enter the `ConfigMoverWorkflows.exe` command with arguments to import and export data.

Note: The Access Assurance Suite does not support the United States Federal Information Processing Standard (FIPS) algorithm. Before installing AAS, you should disable the FIPS setting in Windows Server. It may have been enabled as a local security setting or as part of a domain Group Policy setting. For more information, refer to the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/811833.

To display the help usage for the command, run the following command:

```
ConfigMoverWorkflows.exe -h
```

To display the list of all available workflows, run the following command:

```
ConfigMoverWorkflows.exe -listworkflows
```

During export or import, the following arguments are required:

-workflow=<workflow name>
The name of the workflow to be imported or exported. The workflow name is case-sensitive. If the workflow name includes spaces or punctuation, enclose the workflow name in quotation marks as shown in the example.

-filename=<file name>
Specifies the location and name of the XML file to be used for import or export. The file extension must be .xml. If you do not specify a path, the utility searches for the file in the CourionService folder. You can specify a full pathname or a relative pathname. If the filename already exists in the location you specify, an export fails unless you specify the -overwrite argument.

-passphrase=<pass phrase value>
Specifies the passphrase value to secure the data during import or export

The following argument is optional:

-overwrite
During import, the existing workflow is overwritten. During export, an existing xml file is overwritten.

Example of Exporting a Workflow Configuration File

```
ConfigMoverWorkflows.exe -export
-workflow="Core-Service Password Reset"
-filename="c:\exported\CoreSelf-Service Password Reset.xml"
-overwrite
-passphrase=jsf787sfljLJ3K
```

Example of Importing a Workflow Configuration File

```
ConfigMoverWorkflows.exe -import
-workflow="CoreSelf-Service Password Reset"
-filename="c:\exported\CoreSelf-Service Password Reset.xml"
-overwrite
-passphrase=jsf787sfljLJ3K
```

Starting Courion Services

When you have completed running the utility, restart Courion Services.

Logging

As each file or workflow is imported or exported, all messages are logged to the courion.log file.

INDEX