**Oracle® Enterprise Single Sign-on
Universal Authentication Manager**

How-To: Using the ESSO-UAM Deployment Tools

Release 11.1.1.5.0

22507-01

March 2011

ORACLE®

Oracle Enterprise Single Sign-on Universal Authentication Manager How-To: Using the ESSO-UAM Deployment Tools

Release 11.1.1.5.0

22507-01

ORACLE

Table of Contents

ORACLE

Introduction

About This Guide

This document describes how to use the optional ESSO-UAM configuration tools:

- **ESSO-UAM command-line configuration tool (`DeployTool.exe`)** – a command-line tool used to automatically configure the service account required by ESSO-UAM to run, as well as encrypt the ESSO-UAM Service Account password if desired. This tool can also force the synchronization of ESSO-UAM user data with the ESSO-UAM repository for a specific user.
- **ESSO-UAM graphical configuration editor tool (`ConfigEditor.exe`)** – a GUI-based tool used to configure ESSO-UAM registry settings and save ESSO-UAM configurations for mass-deployment to end-user machines.

> **Warning:** While Oracle supplies these tools for your convenience, Oracle provides no support for their use. Oracle highly recommends keeping up-to-date backups of your environment's configuration before modifying it.

Prerequisites

Readers of this document should have a thorough understanding of ESSO-LM and ESSO-UAM administration and related concepts.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Abbreviation	Description
ESSO-LM	Enterprise Single Sign-on Logon Manager
ESSO-UAM	Enterprise Single Sign-on Universal Authentication Manager
Agent	ESSO-LM client-side software
Console	ESSO-LM Administrative Console

Accessing ESSO-LM Documentation

We continually strive to keep ESSO-LM documentation accurate and up to date. For the latest version of this and other ESSO-LM documents, visit http://download.oracle.com/docs/cd/E21040_01/index.htm.

Using the ESSO-UAM Command-Line Configuration Tool

Overview of the ESSO-UAM Command-Line Configuration Tool

If you are deploying the ESSO-UAM client in Enterprise mode, you must do the following in order to grant ESSO-UAM's authentication service the permissions necessary to read and write data to its repository:

- Add the ESSO-UAM Service Account to the local machine's "Administrators" group,
- Grant the ESSO-UAM Service Account the "Log on As a Service" permission,
- Configure the ESSO-UAM authentication service to run under the selected ESSO-UAM Service Account.

The included ESSO-UAM command-line configuration tool, `DeployTool.exe`, allows you to perform the above configuration steps automatically; you can configure a workstation locally or remotely by specifying its domain and machine name. The tool also allows you to encrypt a service account password to a text file, as well as force the synchronization of ESSO-UAM data for a specific user.

Oracle recommends using this tool to automate ESSO-UAM deployment enterprise-wide by including it in an automated deployment script.

> **Note:** You can also perform this configuration manually on a per-workstation basis using the graphical ESSO-UAM Configuration Editor if necessary, as described in Configuring the ESSO-UAM Service Account.

Prerequisites for Using the Command-Line Configuration Tool

Before using the tool, ensure that your environment satisfies the following prerequisites:

- You have installed the ESSO-LM Administrative Console and the ESSO-UAM client as described in the *ESSO-UAM Installation Guide* for your version of ESSO-UAM,
- You have initialized the ESSO-UAM repository schema,
- You have configured the ESSO-UAM client on the target workstation(s) to run in Enterprise mode,
- You have administrator privileges on the target workstation and the domain (`DeployTool.exe` will fail if you run it without those privileges),
- If you are configuring a remote workstation, that workstation's Windows Firewall has been configured to pass inbound and outbound file and print sharing traffic,
- You have created the ESSO-UAM Service Account, either on the local machine, or your domain, as appropriate to your environment.

ORACLE®

Using the ESSO-UAM Command-Line Configuration Tool

To use the ESSO-UAM command-line configuration tool, complete the steps below:

1. Expand the ESSO-UAM archive to a temporary directory on the local workstation.
2. Open a command prompt and change to the temporary directory you've created in step 1.
3. Change to the `Utility` directory within the temporary directory.
4. Run `DeployTool.exe` using the following syntax:

   ```
   DeployTool.exe <MODE> –<operation> –<modifier1> <value1> –
   <modifier2> <value2> … <modifierN> <valueN>
   ```

   See the [ESSO-UAM Command-Line Configuration Tool Parameter Reference](#) for more information on the available parameters.

   For example:

   ```
   DeployTool.exe SVCACCT –s –u uam_service –p Password1
   ```

5. Restart the machine to apply your changes.

Using a Password Stored in a Text File

For automation purposes, you can instruct `DeployTool.exe` to parse either a plain-text or an encrypted password for the ESSO-UAM Service Account from a text file.

> **Warning:** Deploy tool uses a random key to encrypt the stored password; however, this mechanism is intended as a limited snooping prevention measure only and is not guaranteed to be secure in all circumstances. Oracle strongly advises to treat encrypted passwords with the same precaution as plain-text passwords.

- To encrypt the password to a text file for use during deployment, use the following command:

  ```
  DeployTool.exe ENCRPWD –e –o <password_file> -d <days_to_expire>
  ```

  where `<password_file>` is the full path and file name of your password file.

- To have `DeployTool.exe` parse the ESSO-UAM Service Account password from a text file during deployment, use the following syntax:

  ```
  DeployTool.exe SVCACCT –s –u <domain>\<username> < <passwordfile>
  ```

  where `<password_file>` is the full path and file name of your password file.

See the [ESSO-UAM Command-Line Configuration Tool Parameter Reference](#) for more information on the available parameters.

ORACLE®

ESSO-UAM Command-Line Configuration Tool Parameter Reference

The `DeployTool.exe` tool accepts the following categories of command-line parameters:

- **Mode parameters** – determine the operation mode of the tool. Each mode requires at least one operation parameter. You can also specify one or more of the optional modifiers.
- **Operation parameters** – instruct the tool to perform a specific operation in the selected mode.
- **Modifier parameters** – provide the tool with additional, optional information for each mode and operation type.

Operation Modes

Use one of the following mode parameters to select the `DeployTool.exe` tool's operation mode:

Mode	Description
`SVCACCT`	**Service account configuration**. Configures the ESSO-UAM Service Account.
`SYNC`	**Synchronization**. Synchronizes ESSO-UAM user data with the repository.
`ENCRPWD`	**Encrypt password**. Stores an encrypted ESSO-UAM Service Account password to a text file.

Parameters for the `SVCACCT` Mode

Use the following operation parameters to instruct `DeployTool.exe` what to do while in `SVCACCT` mode:

Operation	Description
`-s`	**Service account configuration**. Performs the configuration steps described in [Overview of the ESSO-UAM Command-Line Configuration Tool](#).
`-i`	**Information**. Displays current configuration without making changes.
`-h`	**Help**. Displays help text and exits.

Optionally, you can use the following modifiers along with the `-s` or `-i` operations described earlier:

Modifier	Description
-u	**User name**. Specifies the name of the ESSO-UAM Service Account. Requires `-s` or `-i`. Syntax: `-u <domain>\<user_name>` If omitted, the local SYSTEM account is used.
-p	**Password**. Specifies the desired password for the ESSO-UAM Service Account. Requires `-s` or `-i`. Syntax: `-p <password>` Not required if `-u` is omitted and the local SYSTEM account is used. If omitted, you will be prompted to specify a password interactively. (Your entry will be masked to prevent snooping.) You can also specify a password stored in a plain or encrypted text file as described in Using a Password Stored in a Text File.
-c	**Computer**. Specifies the domain and machine name of the target workstation. Requires `-s` or `-i`. Syntax: `-p <domain>\<computer>` If omitted, the local workstation is configured.
-na	**No-Administrator**. Prevents the ESSO-UAM Service Account from being added to the local "Administrators" group on the target workstation. Requires `-s`.
-ns	**No-Service**. Prevents the "Log On As a Service" permission from being granted to the ESSO-UAM Service Account. Requires `-s`.
-nr	**No-Restart**. Prevents the restarting of the ESSO-UAM authentication service. Requires `-s`.

ORACLE®

Parameters for the `SYNC` Mode

Use the following operation parameters to instruct `DeployTool.exe` what to do while in `SYNC` mode:

Operation	Description
-s	**Synchronize**. Synchronizes ESSO-UAM user data with the repository.
-h	**Help mode**. Displays help text and exits.

Optionally, you can use the following modifiers along with the `-s` operation described earlier:

Modifier	Description
-u	**User name**. Specifies the name of the user account whose data is to be synchronized with the repository. Requires `-s`. Syntax: `-u <domain>\<user_name>` If omitted, the currently logged-in user's data is synchronized.
-t	**Target**. Specifies the type of data to synchronize with the repository. Requires `-s`. The available data types are: • `ALL` – synchronizes all user data. • `DATA` – only synchronizes roaming user data, such as credentials. • `POLICY` – only synchronizes roaming ESSO-UAM policy settings for the user. Syntax: `-t ALL|DATA|POLICY` If omitted, all data is synchronized.

ORACLE®

Parameters for the `ENCRPWD` Mode

Use the following operation parameters to instruct `DeployTool.exe` what to do while in `ENCRPWD` mode:

Operation	Description
-e	**Encrypt password to file mode.** Prompts you for a password and encrypts it.
-h	**Help mode**. Displays help text and exits.

Optionally, you can use the following modifiers along with the `-e` operation described earlier:

Modifier	Description
-o	**Output file.** Specifies the full path and file name for the text file that will store the encrypted ESSO-UAM Service Account password. Requires `-e`. Syntax: `-o <file_name>` If omitted, the encrypted password string is displayed on-screen.
-d	**Days.** Specifies the number of days after which the encrypted password expires. Requires `-e`. Syntax: `-d <number_of_days>` If omitted, encrypted passwords expire after 30 days.

ORACLE®

Using the Graphical ESSO-UAM Configuration Editor Tool

Overview of the ESSO-UAM Configuration Editor Tool

The graphical ESSO-UAM Configuration Editor tool (`ConfigEditor.exe`) allows you to view and modify ESSO-UAM registry settings. You can:

- Create a new or modify an existing ESSO-UAM configuration which you can then save and mass-deploy to end-user machines.
- Audit ESSO-UAM policies on a per-user basis.

Prerequisites for using the ESSO-UAM Configuration Editor

Before you can use the ESSO-UAM Configuration Editor, you must place it in the ESSO-UAM installation directory as follows:

1. Expand the ESSO-UAM archive to a temporary directory on the local workstation.
2. Inside the temporary directory, locate the `Utility\ConfigEditor` directory.
3. Copy `ConfigEditor.vrs` to `%PROGRAMFILES%\Passlogix\v-GO UAM\Lang\Res`.
4. Copy `ConfigEditor.exe` to `%PROGRAMFILES%\Passlogix\v-GO UAM`.
5. Merge `ConfigEditor.reg` into the local machine's registry. Double-click the file and answer **Yes** when prompted.
6. For your convenience, create a desktop shortcut pointing to `%PROGRAMFILES%\Passlogix\v-GO UAM\ConfigEditor.exe`.

Creating or Modifying a Configuration

To create a new configuration, do the following:

1. Launch the ESSO-UAM Configuration Editor.
2. Do one of the following:
    - If you want to use the local machine's ESSO-UAM configuration, proceed to step 3.
    - If you want to create a new configuration with default values for all settings, select **New Configuration** from the **File** menu.
    - If you want to open an existing configuration that you have previously saved to a .REG file, select **Open Configuration → From Live Registry** from the **File** menu, then navigate to and select the target .REG file and click **Open**.

3. To modify a setting, do the following:
   a. In the list of settings, navigate to the target setting and double-click it.

> **Tip:** To sort the settings list per type, target, or category, select the desired sorting method from the **View → Sort By** menu.
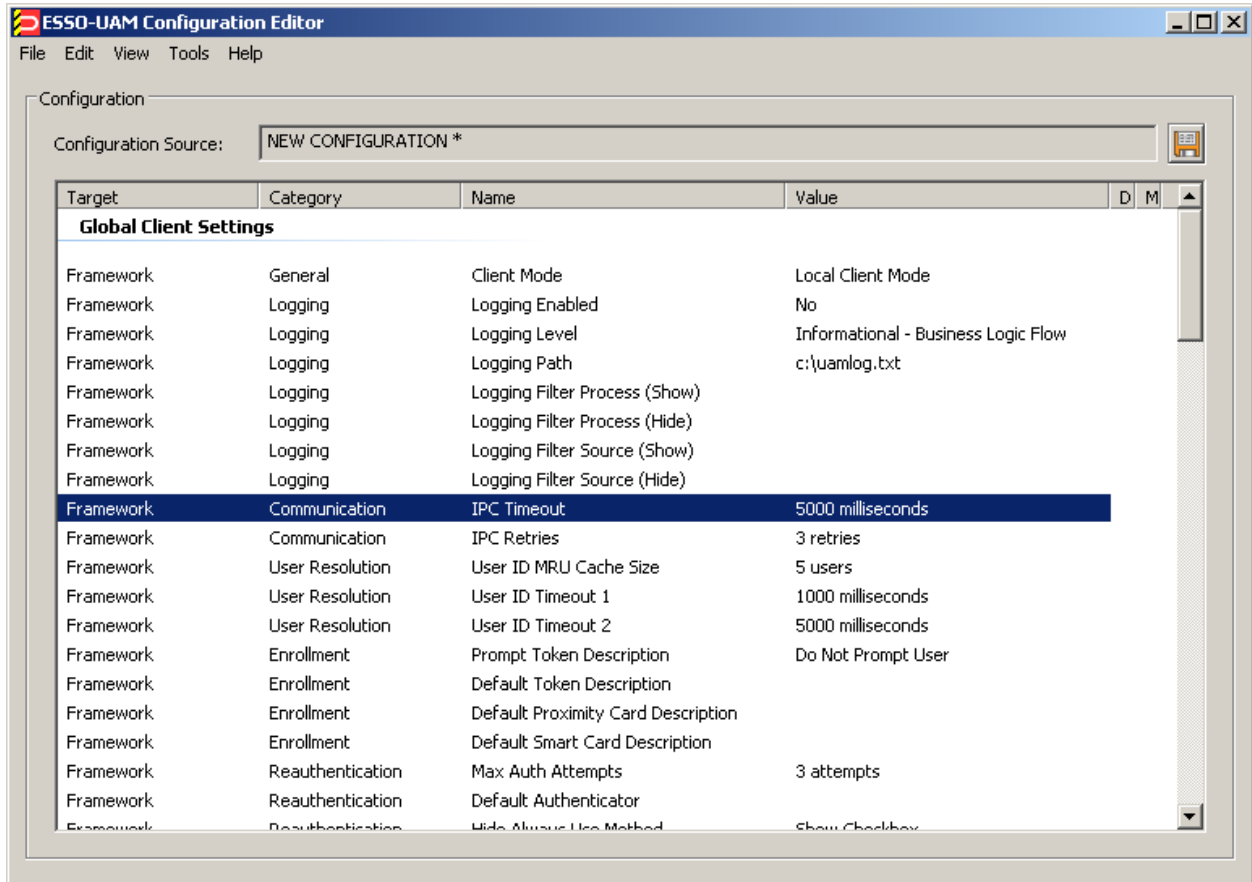
   b. In the properties dialog that appears, do the following:
      i. Select the check box.
      ii. Enter the desired value.
      iii. Click **OK**.

   When you set the value, a check mark and a floppy disk appear next to the setting to indicate the following:

   - **Floppy disk.** Indicates that the setting's value has been modified from its original state from when the configuration was first created or loaded. To revert a setting to its previous value, select the setting from the list, then select **Revert "<Setting Name>" Setting** from the **Edit** menu.

   > **Tip:** To revert all changes made during the current editing session, select **Revert All Changes** from the **Edit** menu.

ORACLE

12

- **Check mark.** Indicates that the setting has been *defined* – in other words, its value has been explicitly set and the corresponding registry key will be created upon saving the configuration. (Optional) To undefine a setting (i.e., to remove its registry key from the configuration and let ESSO-UAM fall back to the default value), select the setting in the list, then select **Undefine "<Setting Name>" Setting** from the **Edit** menu.

> **Tip:** To undefine all settings in the existing configuration, select **Undefine All Settings** from the **Edit** menu. To define all settings in the existing configuration, select **Define All Settings** from the **Edit** menu.

4. Repeat step 3 for each additional setting you want to configure.
5. Save your configuration. From the **File** menu, select **Save**, then specify the path and file name of the target .REG file and click **Save**.

> **Note:** If you do not wish to include registry keys for undefined settings (i.e., settings that remain at their default values because you have not explicitly defined values for them), deselect the Registry **File Generation → Include undefined settings** option under the **Options** menu before saving your configuration.
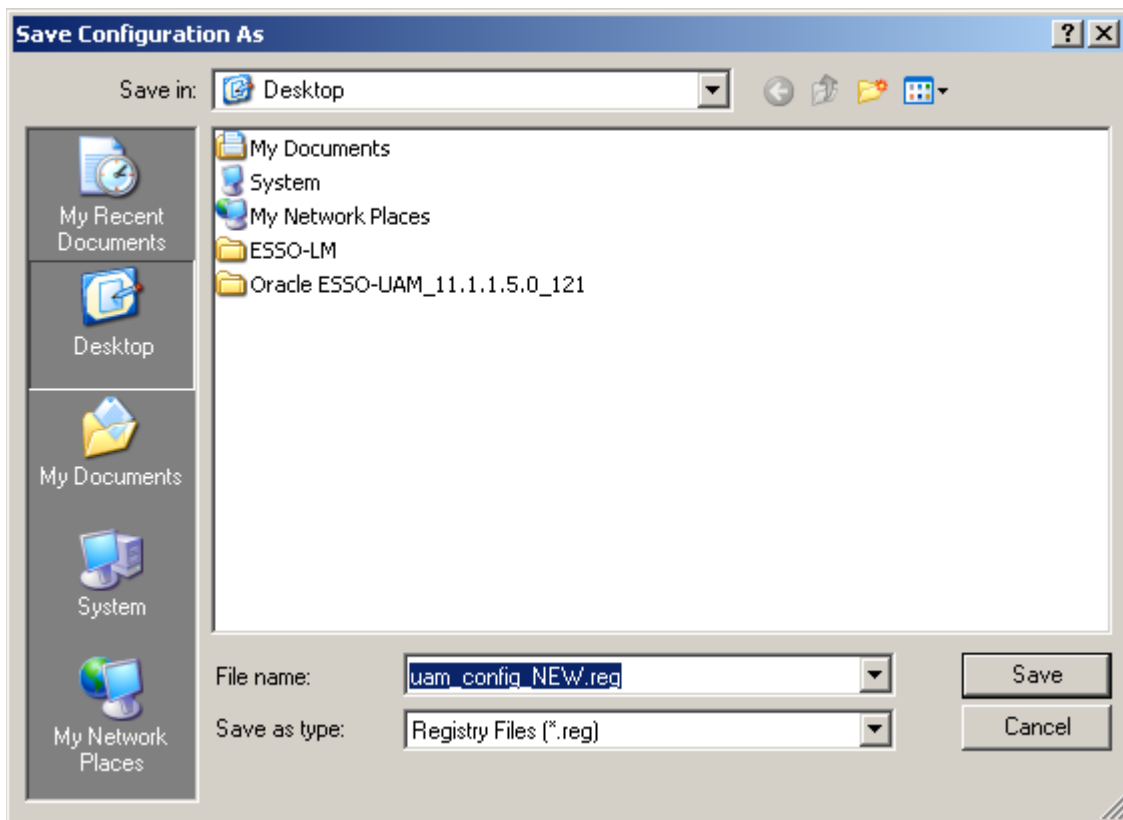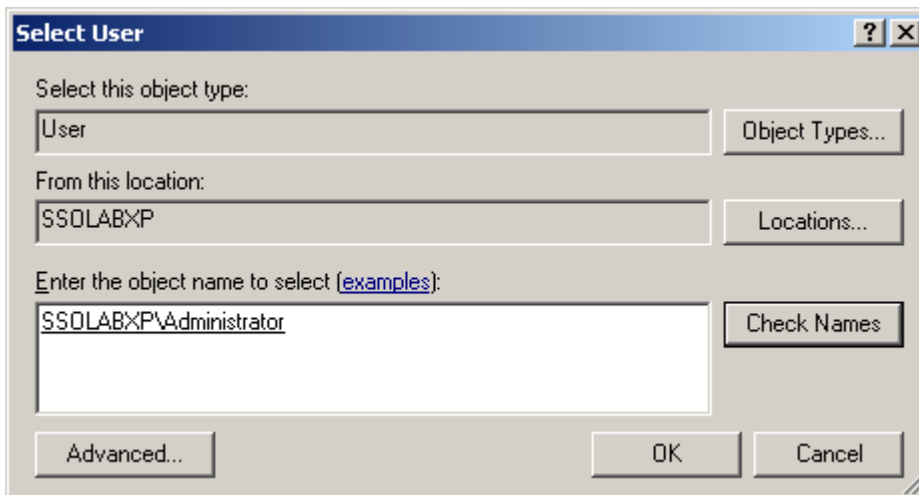
Configuring ESSO-UAM Settings on a Per-User Basis

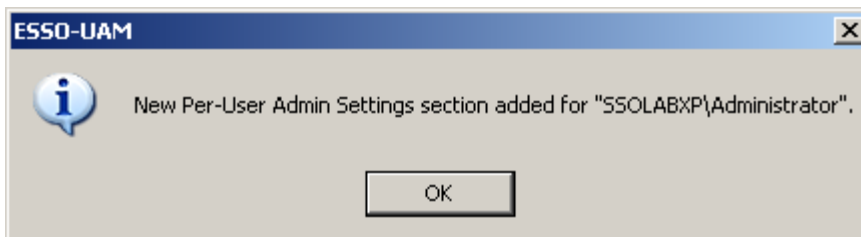If you want to configure ESSO-UAM settings a per-user basis, do the following:

1. From the **Edit** menu, select **Add Per-User Admin Settings**.
2. Read the prompt that appears and click **OK**.
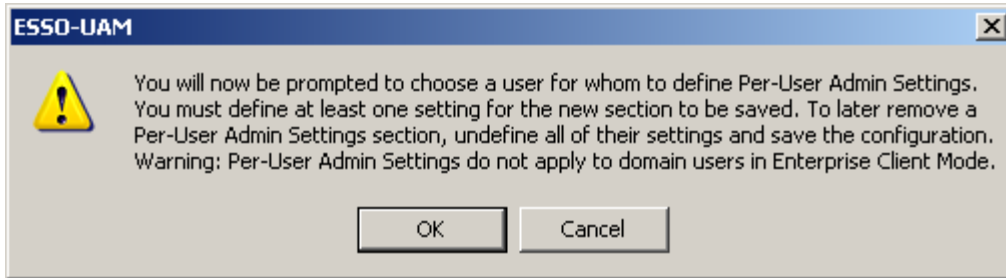
3. In the "Select User" dialog, select the desired user and click **OK**.

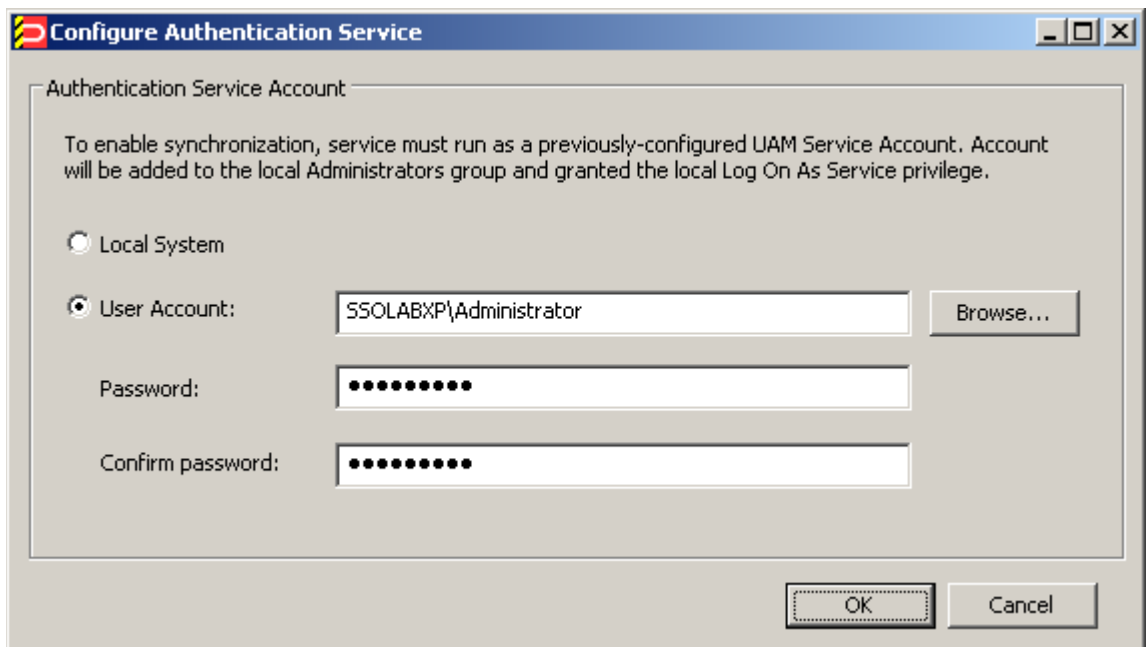4. In the confirmation prompt that appears, click **OK**.

5. In the settings list, navigate to the newly created per-user settings group and complete their configuration by following steps 3-7 in Creating or Modifying a Configuration.

Configuring the ESSO-UAM Service Account

The ESSO-UAM Configuration Editor allows you to specify or modify the service account used by ESSO-UAM's authentication service to write and read data to and from its repository, as described in Overview of the ESSO-UAM Command-Line Configuration Tool.

> **Note:** Before starting this procedure, ensure that you have satisfied the prerequisites described in Prerequisites for Using the Command-Line Configuration Tool.

1. From the **Tools** menu, select **Deployment → Configure Authentication Service**.
2. In the "Configure Authentication Service" dialog, select or specify the desired ESSO-UAM Service Account, provide its password, and click **OK**.
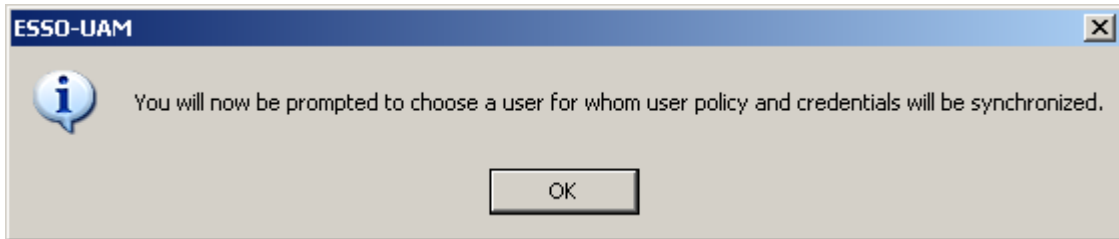

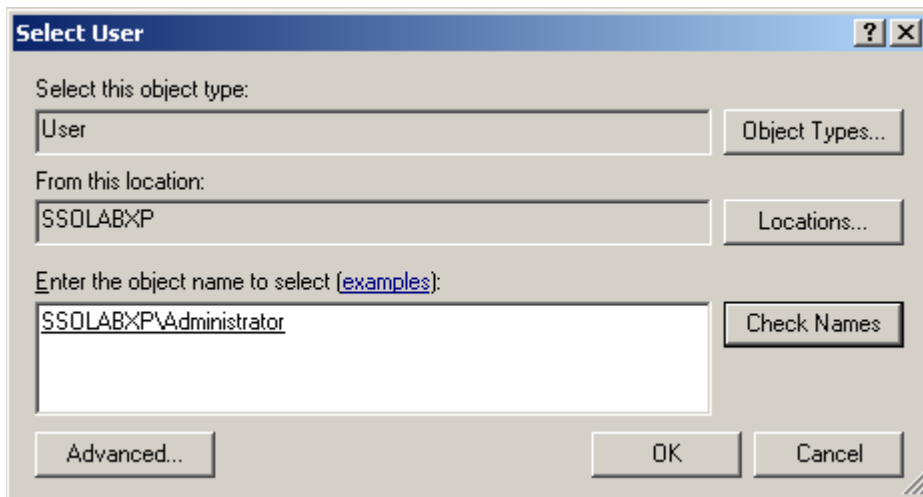3. In the confirmation prompt that appears, click **OK**.
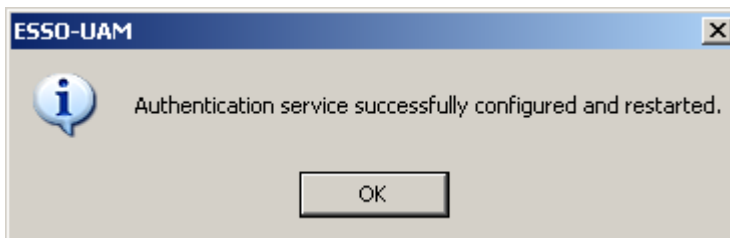
Synchronizing ESSO-UAM Data for a Specific User

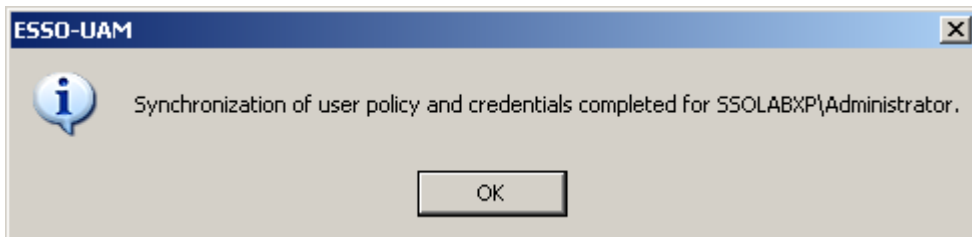To force ESSO-UAM to synchronize user data for a specific user, do the following:

1. From the **Tools** menu, select **Deployment → Synchronize User Data**.
2. Read the prompt that appears and click **OK**.

3. In the "Select User" dialog, select the desired user and click **OK**.

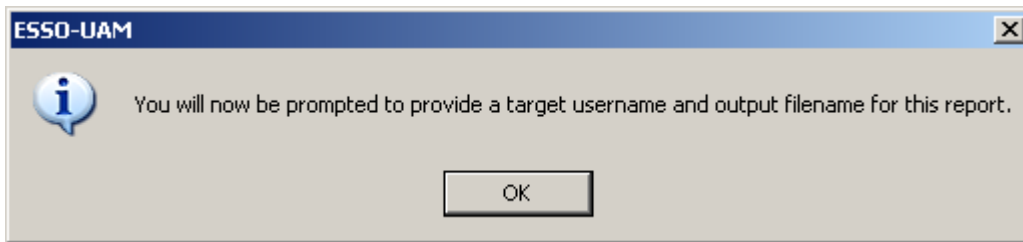4. In the confirmation prompt that appears, click **OK**.

ORACLE

# Auditing ESSO-UAM Settings Policy for a Specific User

To audit the ESSO-UAM settings policy for a specific user, do the following:

Tip: If you want the ESSO-UAM Configuration Editor to display the report immediately upon its generation, select **Display Report After Generation** from the **Tools → Options → Report File Generation** menu.
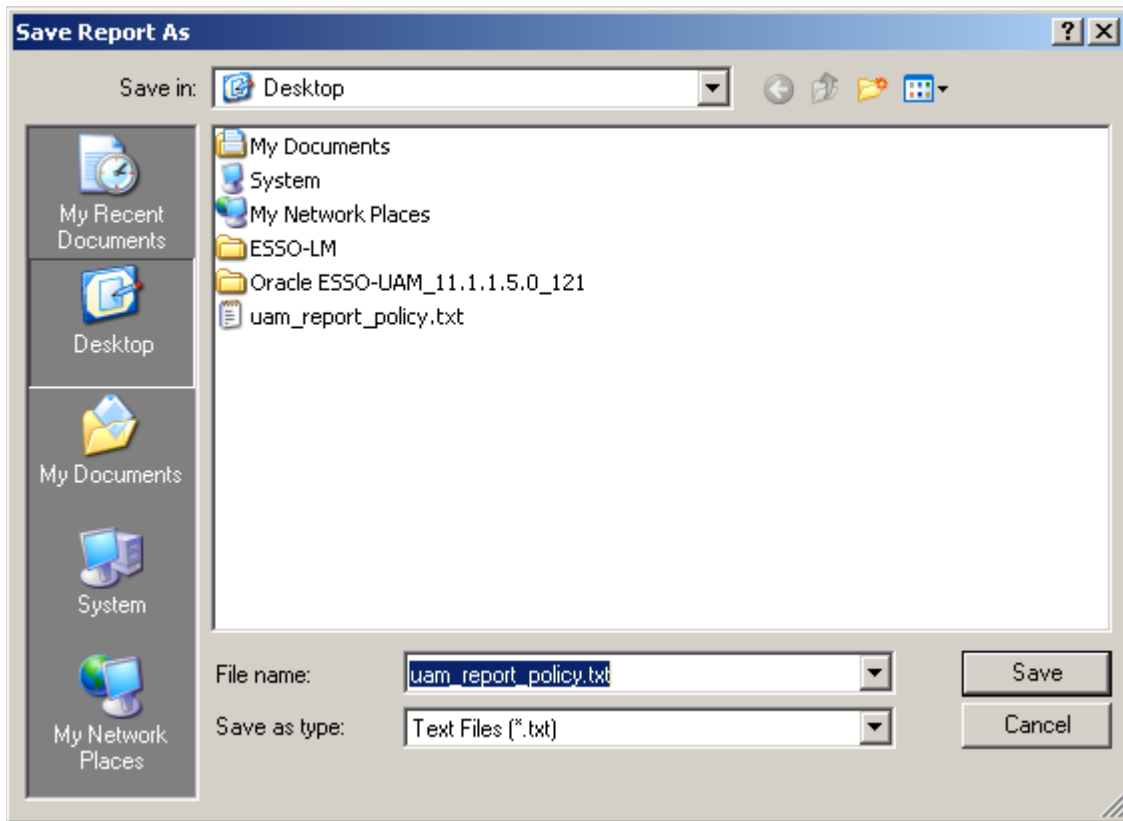
1. From the **Tools** menu, select **Reports → Generate User Policy Report**.
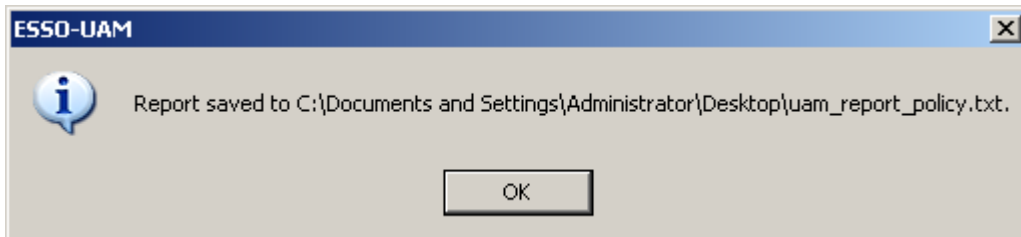2. Read the prompt that appears and click **OK**.

3. In the "Select User" dialog, select the desired user and click **OK**.
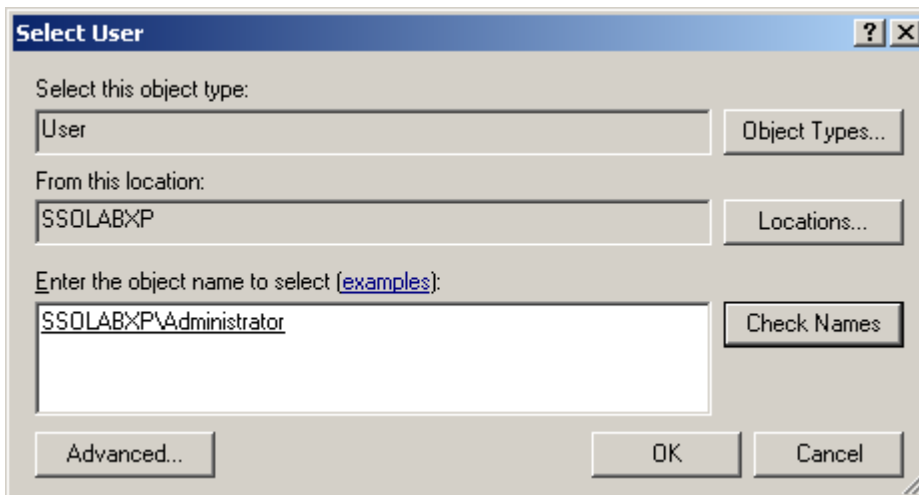
4. In the "Save As" dialog, specify the desired path and file name for the report and click **OK**.

5. In the confirmation prompt that appears, click **OK**.

> **Note:** If you have configured ESSO-UAM Configuration Editor to display the report upon successful generation, the report opens in the machine's default text file editor.