Oracle® Enterprise Single Sign-on Logon Manager

How-To: Using the Trace Controller Utility

Release 11.1.1.5.0

21015-01

March 2011

ORACLE

Oracle Enterprise Single Sign-on Logon Manager How-To: Using the Trace Controller Utility

Release 11.1.1.5.0

21015-01

Table of Contents

Introduction

About This Guide

This document describes how to use the Trace Controller utility to enable and manage trace logging in Oracle ESSO applications. Trace Controller currently supports the following applications:

- ESSO-LM 11.1.1.1.0 and above
- ESSO-AM 11.1.1.2.0 and above (for SmartCard authenticators)

Prerequisites

Readers of this guide should have a thorough understanding of the Windows Event Log and related topics.

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
Agent	ESSO-LM client-side software
Console	ESSO-LM Administrative Console
ESSO-AM	Enterprise Single Sign-On Authentication Manager

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 Trace Controller Utility

The Trace Controller utility allows you to monitor and log events occurring within an Oracle ESSO application. You have the choice to monitor events as they occur in real-time, or log them to a file for later review.

The basic components of trace logging are:

- **Provider** – An Oracle ESSO application that supports trace logging. Each Oracle ESSO application represents a separate provider and establishes a separate logging session when trace logging is enabled.
- **Consumer** – An application that parses, interprets, and displays the logged events, such as the Trace Controller utility (`tracecontroller.exe`) or Windows Event Viewer

The Trace Controller utility serves the following purposes:

- Control and configure the logging of ESSO-LM events. This involves creating a session and enabling logging in the desired provider(s)
- Display the logged events in the desired format, including filtering by a number of criteria

Once you enable logging for a provider, it remains enabled even when Trace Controller, the provider application, or Windows itself is shut down. When Windows starts back up and/or the provider application is relaunched, event capture continues until you explicitly disable it.

Oracle ESSO applications support the following log verbosity levels:

Level	Level Name	Description
1	**Critical**	Abnormal exit or termination
2	**Error**	Server errors that need logging
3	**Warning**	Warnings such as allocation failure
4	**Information**	Includes non-error cases (e.g., Entry-Exit)
5	**Debug**	Detailed traces from intermediate steps

When capture is complete, the Trace Controller utility allows you to display one or more event logs in a single viewer that organizes the events in chronological order. For example, you can view ESSO-LM and ESSO-AM events in a single list, which can then be filtered by a number of custom criteria.

Using the Trace Controller Utility in Graphical Mode

This part explains how to use the Trace Controller utility in its graphical (interactive) mode. Using the utility via command line is explained in xx.

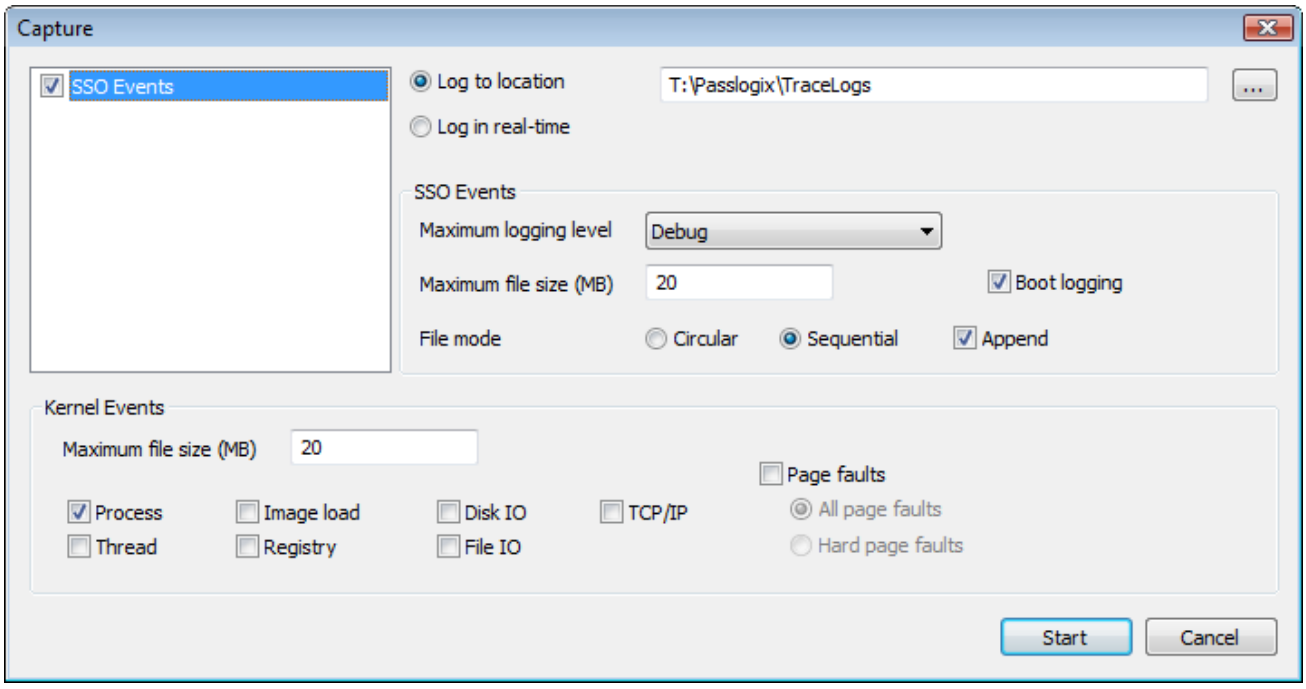
Enabling Trace Logging for an Application

To enable trace logging for an Oracle ESSO application, you must use the Trace Controller utility. The utility allows you to select the desired provider, logging method, and the desired event types, as well as configure additional logging options.

> **Note:** You must have administrative privileges to run the Trace Controller utility. If you are not logged in as a user with administrative privileges, the utility will prompt you for administrative credentials when launched.

To enable trace logging:

1. Launch `TraceController.exe`.
2. If prompted, enter the credentials of an account with administrative privileges.
3. Select **Capture Events** from the **File** menu. The "Capture" window appears.



4. In the “Capture” window, do the following:

    a. Select the provider whose events you want to log. By default, **SSO Events**, the main ESSO-LM logging provider, is selected.

    b. Select whether you would like to log events to a file or display them in real-time. If logging to a file, click the **Browse (…)** button and specify the path and file to which you want to log.

    c. Specify the **Maximum logging level** (see table on page 6 for a list of available logging levels) for the **SSO Events** provider.

    d. Specify the **Maximum file** size for the SSO Events provider. The default value is 20MB.

    e. Select the desired log file write mode:

        - **Circular** – once the maximum log file size is reached, the utility begins overwriting old data in chronological order. The log is cleared each time logging is started.
        - **Sequential** – once the maximum log file size is reached, the utility stops logging. The log is cleared each time logging is started, unless you select the **Append** check box.

    f. If you want logging to begin at boot time, select the **Boot logging** check box. When this feature is enabled, events will be logged as soon as Windows completes startup and will not require a user logon.

    g. For the **Kernel Events** provider, select the types of events you would like to log, and the maximum log file size (the default value is 20MB). In most cases, only kernel process events should be logged for ESSO-LM troubleshooting.

5. Click **Start** to begin logging events. Note the following:

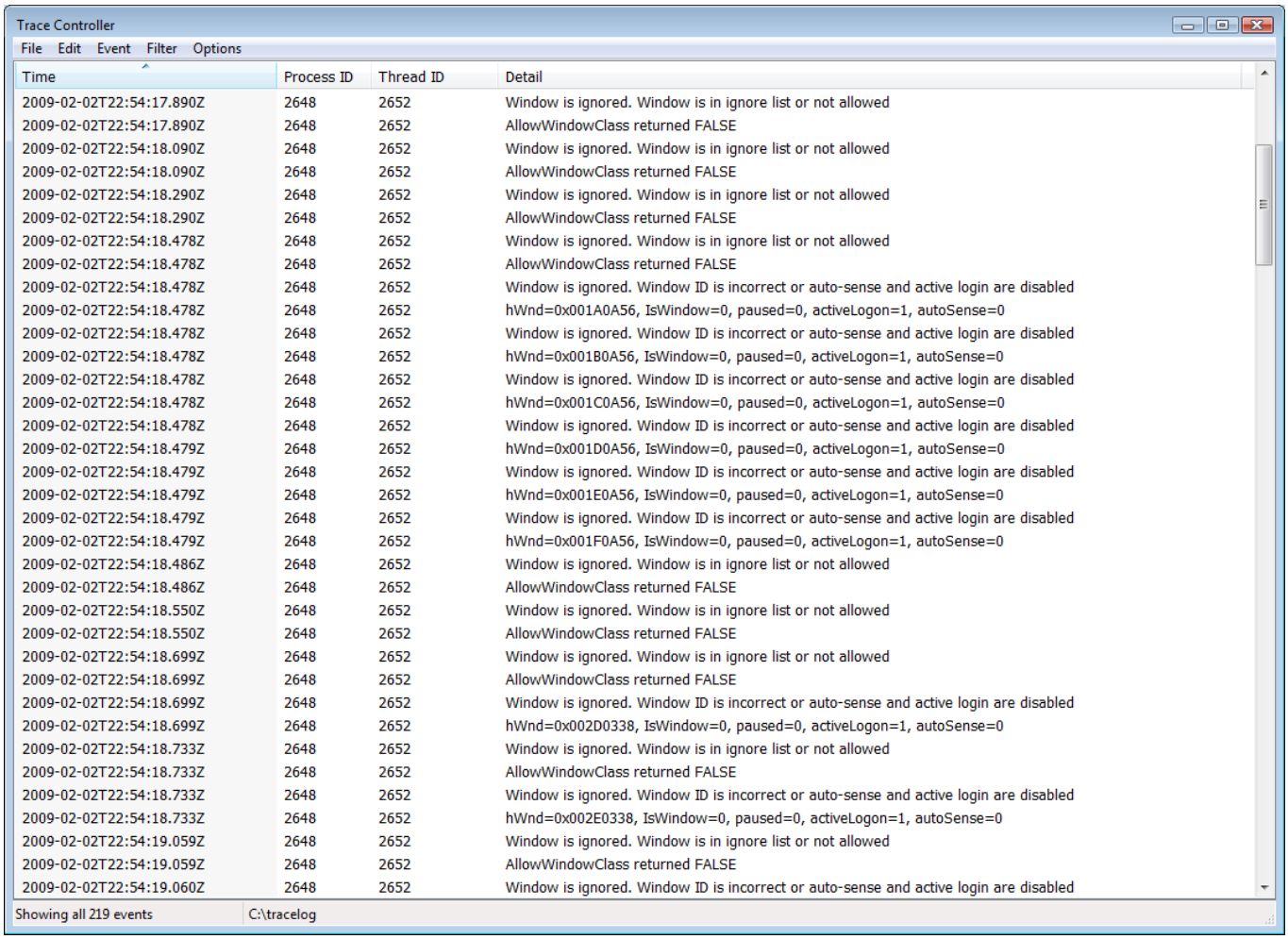
    - Logging will remain enabled until you explicitly disable it.
    - When the Trace Controller utility is running, its system tray icon animates to indicate events are being captured.

Note: Once you have configured your initial capture settings, you can configure the Trace Controller utility to start and stop event capture using hot keys. To set up the hot keys, see Configuring Event Capture Hot Keys.

Viewing Logged Events

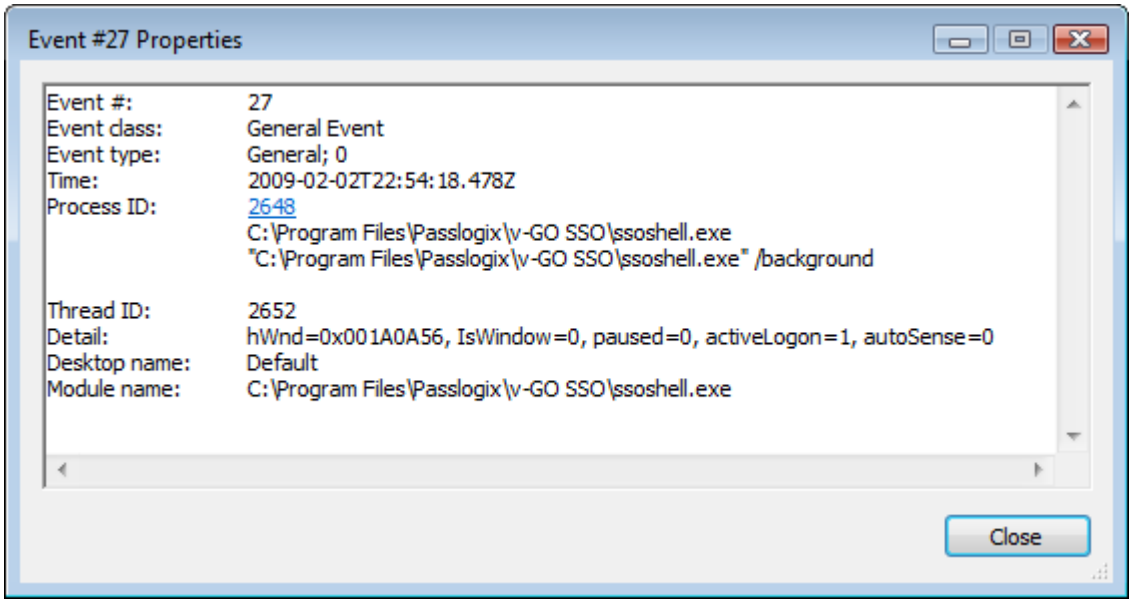
To view events logged to a file, do the following in the Trace Controller utility:

1. Open the desired log file:
   a. From the **File** menu, select **Open Events.**
   b. Browse to the desired provider's log file and click **Open**.
      The events stored in the log file are displayed as a list in chronological order.
   c. If you want to view events from multiple log files simultaneously, repeat steps 1a and 1b for each additional file you want to open. The events from all open log files are displayed in the list in chronological order.



Note: To reverse the sort order, click the **Time** column header. An arrow in the header indicates the currently selected sort direction.

2. To view details for a specific event, navigate to it in the list and double-click it. The details are displayed in a pop-up window.



When you are finished viewing the event details, click **Close** to return to the event list.

Hint: If you are viewing events from multiple log files, you can see which log files are currently open by selecting **Show Open Log Files** from the **File** menu.

Customizing the Event List View

You can customize the following aspect of the event list:

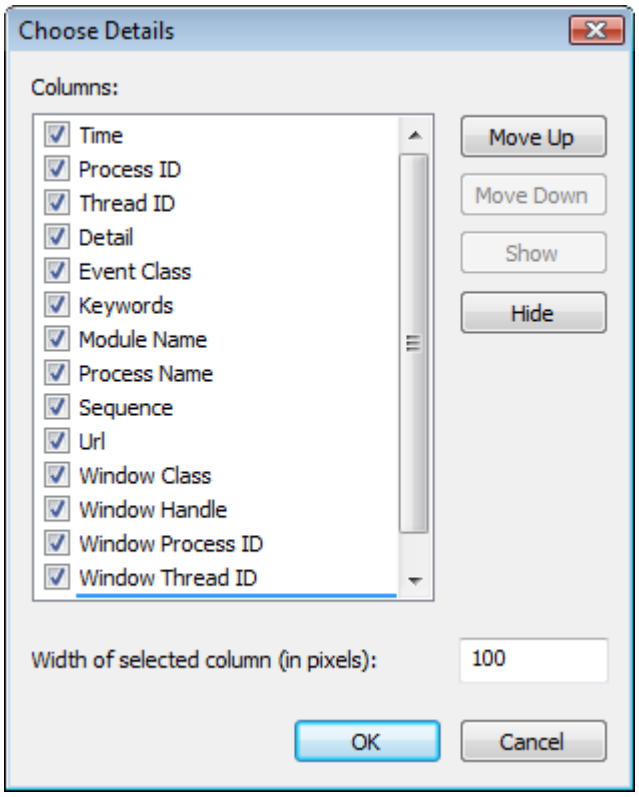
- Event list columns
- Event filter
- Font style and size
- Timestamp format

Customizing Event List Columns

You can select which columns will be displayed in the event list and in what order as follows:

1. Select **Choose Details** from the **Options** menu.

   The "Choose Details" window appears.



2. In the **Columns** list, select the check box next to each column you want to be visible; deselect the check box to hide the column.
3. To move a column left in the event list, select it in the **Columns** list and click **Move Up**; to move a column right, select it and click **Move Down**.
4. To set a column's width, select it in the **Columns** list and enter the desired width (in pixels) into the **Width of selected column** field.
5. When you have finished, click **OK** to save your changes.

Filtering Events

The Trace Controller utility allows you to filter the displayed events by one or more criteria of your choice. To enable filtering, do the following:

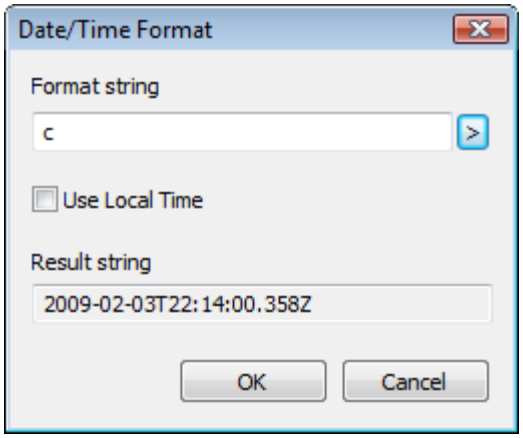
1. From the **Filter** menu, select **Filter**.
2. In the window that appears, configure your first criterion as follows:
   a. Select the parameter to filter against.
   b. Select the operator (is, is not, less than, greater than, and so on)
   c. Enter the value to match the parameter against. Plain text strings as well as regular expressions are supported.
   d. Select whether this criterion should include or exclude matches from the results.
   e. Click **Add**.
3. Repeat step 2 to add more criteria.
4. When you are finished, click **OK**. Your results are updated to reflect the filtering criteria you have configured.

> **Note:** The **Advanced Filter** option is a special feature reserved for developers. Use the standard filter to filter your event list.

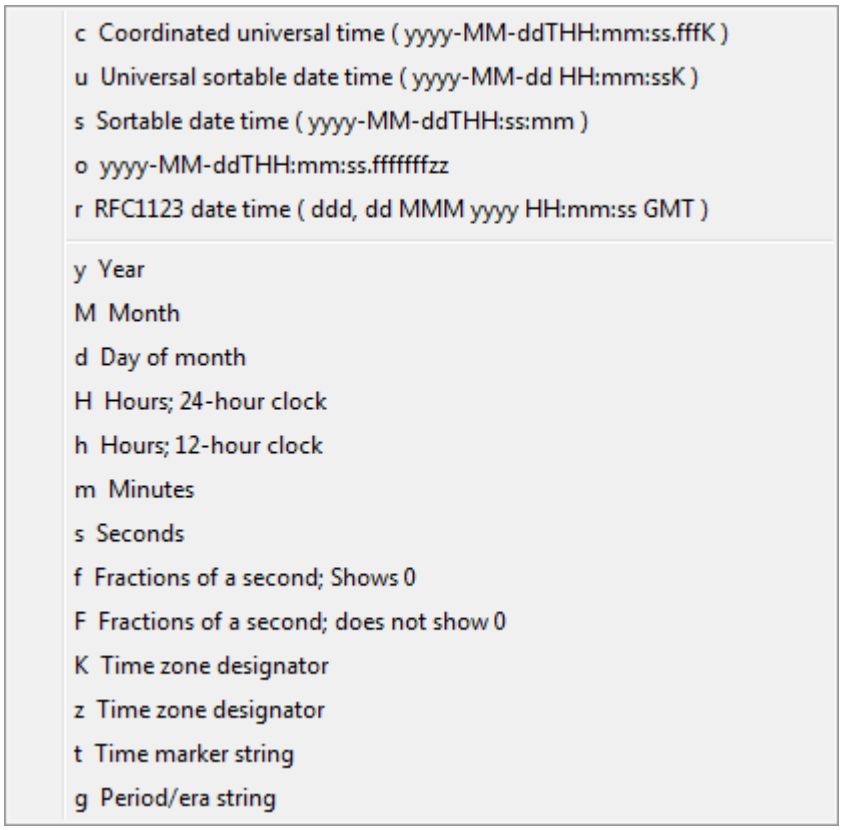
Customizing the Timestamp Format

You can customize the event timestamp format as follows:

1. From the **Options** menu, select **Date/Time Format**.
   The "Date/Time Format" window appears.



2. Select or enter the desired timestamp format string as follows:
   - If you want to choose one of the preset timestamp formats, click the arrow button to the right of the **Format string** field and select it from the upper section of the menu.
   - If you want to enter a custom string, click the arrow button to the right of the **Format string** field and examine the legend in the lower section of the menu, then construct your custom string using the building blocks of your choice.

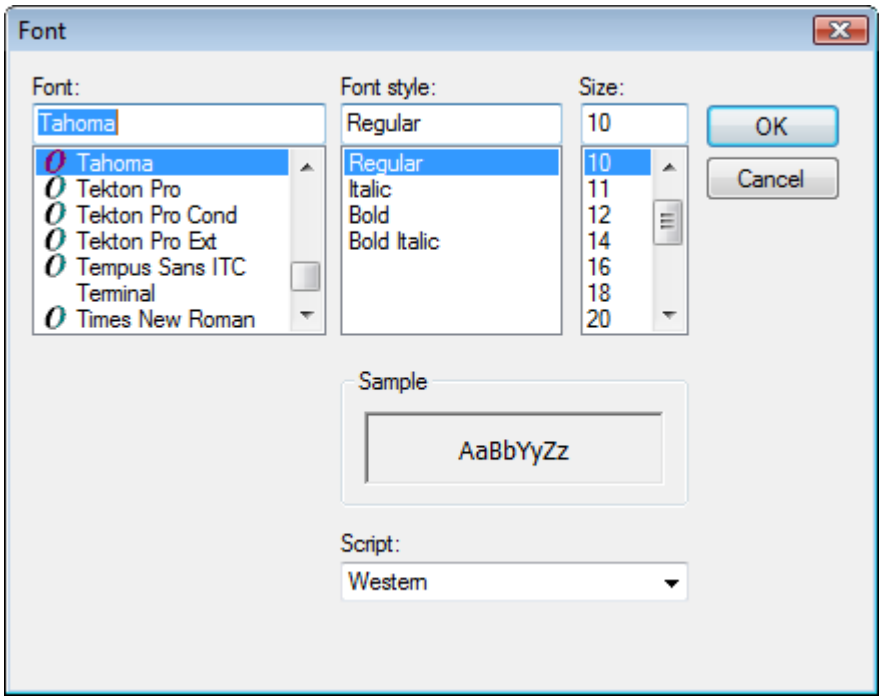


3. When you have finished, click **OK** to save your changes.

Customizing the Event List Font

You can customize the font used to display the events in the list as follows:

1. From the Options menu, select Font.
   The “Font” window appears.

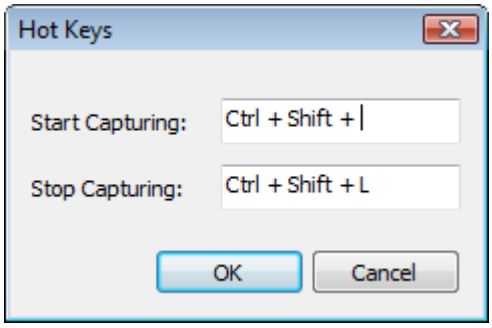


2. In the “Font” window, make your changes, then click **OK**.

Configuring Event Capture Hot Keys

You can configure the Trace Controller utility to start and stop event capture using hot keys as follows:

1. From the **Options** menu, select **Hot Keys**. The "Hot Keys" window appears:



2. Configure the **Start Capturing** hot key:
   a. Click within the **Start Capturing** field.
   b. Press the desired key combination. The combination will appear in the field.
3. Configure the Stop Capturing hot key:
   a. Click within the **Stop Capturing** field.
   b. Press the desired key combination. The combination will appear in the field.
4. Click **OK** to save your changes.

Using the Trace Controller Utility in Command Line Mode

The Trace Controller utility can be launched and configured from the command line without the need to interact with its graphical interface. This part explains the command-line syntax accepted by the utility.

Command Line Switch Reference

The Trace Controller utility accepts the following command-line switches. Required switches are shown in bold; non-bold switches are optional.

Switch	Purpose
`/start`	Start logging.
`/stop`	Stop logging.
`/boot`	Start logging on boot.
`/noui`	Start in silent mode (suppress graphical interface).
`/path`	Specifies the path in which log files will be stored in the following format: /path "<path_to_log_files>. If not specified, log files will be written to `%SYSTEMROOT%\System32\LogFiles\Vgo`. (This default folder is only accessible to users with administrative privileges.)
`/event`	Specifies the event type(s) to log in the following format: `/event "EventType1" [verbosity level] [write mode] [log file size]` If omitted, events of all currently supported types (except kernel) will be logged.
`/level`	Specifies the maximum logging verbosity level in the following format: `/level x` where `x` is an integer from `1` - `5`. The available verbosity levels are: `1` – Critical, `2` – Error, `3` – Warning, `4` – Information, `5` – Debug (The default verbosity level is 4.)
`/circular`	Specifies the log file write mode to be circular. In this mode, once the maximum log file size is reached, the utility begins overwriting old data in chronological order. The log is cleared each time logging is started. This is the default mode.
`/sequential`	Specifies the log file write mode to be sequential. In this mode, once the maximum log file size is reached, the utility stops logging. The log is cleared each time logging is started, unless you also specify the `/append` switch.
`/append`	If `/sequential` is used, the utility will continue writing to the log file at the end of the existing data instead of clearing it.
`/fsize`	Specifies the maximum size of the log file in megabytes in the following format: `/fsize x` (The default size is 20MB.)
`filename`	Specifies the log file name to open for viewing in the following format: `TraceController.exe "<path_to_log_file>\<log_file_name>"`

Command-Line Use Examples

The following are examples of operating the Trace Controller utility from the command line.

Starting Logging

To start logging, use the `/start` switch, plus one of the optional startup switches.

```
TraceController.exe /start [/noui] [/boot] [/path "<log_file_path>"]
```

For most troubleshooting scenarios, you will want to log all supported event types at the `debug` verbosity level and using Oracle-specified defaults for all other configuration options:

```
TraceController.exe /start /level 5
```

Specifying Logging Options for Multiple Event Types

When specifying more than one event type, you have the option to specify custom logging options for each individual type, as shown below. You can also specify them globally after specifying the event types, in which case all event types will be logged with the same configuration options.

Custom configuration options for each event type:

```
TraceController.exe /start /noui /path "T:\Oracle\TraceLogs"
/event "EventType1" /level 2 /circular /fsize:10 /event "EventType2"
/level 3 /sequential /append
```

Global configuration options for all event types:

```
TraceController.exe /start /noui /path "T:\Oracle\TraceLogs"
/level 2 /circular /fsize 10 /event "EventType1" /event "EventType2"
```

Stopping Logging

To stop logging, use the `/stop` switch:

```
TraceController.exe /stop
```

Viewing a Log File

You can open one or more log files for viewing as follows:

```
TraceController.exe "logfile1" "logfile2" … "logfile3"
```

ESSO-AM Error Messages

This appendix lists the messages logged in ESSO-AM during smart card authentication:

Warning Level Messages

Event Message	Description
Failed to retrieve the random password from the registry.	This message can be ignored if the user has just completed the First Time Use (FTU) process, otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the random password was successfully saved and verify that synchronization process has completed successfully.
Failed to retrieve the PIN from the registry.	This message can be ignored if the user has just completed the FTU process, or the first time after configuration was changed to store the PIN. Otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the PIN was successfully saved and verify that synchronization process has completed successfully.
Failed to retrieve the certificate passphrase from the registry.	This message can be ignored if the user has just completed the FTU process, otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the passphrase was successfully saved and verify that synchronization process has completed successfully.

Error Level Messages

Event	Description
Smart card selection failed.	Either the user canceled out of the smart card selection dialog, or the inserted smart card was not recognized by the system. Check to ensure that the proper middleware for the smart card is installed and configured correctly.
Exporting session key failed.	Could not export a session key off of the smart card. Verify that the "SmartcardAPI" console setting is configured properly for the middleware. Some middleware may not support exporting session keys.
Importing session key failed.	Could not import a session key onto the smart card. Verify that the "SmartcardAPI" console setting is configured properly for the middleware and verify that synchronization process has completed successfully.
Failed to set application data on the smart card.	Application data could not be stored on the smart card. This message can be ignored if ESSO-KM is not in use. Verify that the middleware includes support for PKCS #11 and the smart card is not "read only".
Failed to get application data from the smart card.	This error message is usually encountered when application data could not be successfully stored on the smart card.
Failed to get the smart card serial number.	The middleware does not support retrieving the smart card serial number. This message can be ignored if ESSO-KM is not in use.
Failed to enumerate encryption certificate key containers.	The Cryptographic Service Provider (CSP) installed by the middleware does not support enumerating key containers on the smart card.
Failed to locate logon certificate.	A smart card logon certificate could not be located on the card. Verify that the logon certificate is present on the card and is the default certificate.

Failed to locate encryption certificate.	If this error is encountered during FTU, no encryption certificates could be located on the card. The smart card logon certificate cannot be used for this purpose. Verify that a separate, non-logon encryption certificate is present on the card. If this error is encountered after successful FTU, verify that the encryption certificate used during FTU is present on the card and available for use.
Failed to obtain exchange key.	The exchange key could not be obtained for use. If configured for logon certificates, verify that the certificate is available on the card for use. If SSO keys are configured, verify that the SSO container has been created on the card and contains keys.
Failed to create session key.	A session key could not be created on the card. Verify that the “SmartcardAPI” console setting is configured properly for the middleware and the smart card is not “read only”.