Oracle® Enterprise Single Sign-on Kiosk Manager

Administrator Guide

Release 10.1.4.1.0

E12626-01

April 2009

Oracle Enterprise Single Sign-on Kiosk Manager, Administrator Guide, Release 10.1.4.1.0

E12626-01

Table of Contents

Abbreviations and Terminology 2
About ESSO-KM 3
Events and Actions 4
Create an Action List 6
  Terminate List 7
  Run List 9
  Special Actions List 11
Create a Session State 14
  Kiosk Manager > Session States > Events tab 15
  Kiosk Manager > Session States > Authenticators tab 18
  Kiosk Manager > Session States > Actions tab 19
  Kiosk Manager > Session States > Security Tab 21
About Desktop Manager 23
  Terminate Sessions 25
Customizing the Desktop Manager 26
  Customizing the Text Message 26
  Customizing the Background Image 28
Desktop Status Window 32
Transparent Lock 33
Bypassing the ESSO-KM Agent 35
Closing the ESSO-KM Agent 35
Set up a Trust 36
Event and Audit Logs 37
  Event Log Messages 38
Authenticating to ESSO-KM using ESSO-AM 40
Configuring Smart Card Removal 41
Linking to ESSO-PR 42
Command Line Options 43
.NET API 44
  Externally Callable Interfaces and Methods 44
  .Net API Sample Code 46
Best Practices 48
  Deploying ESSO-KM Settings 48
  Sendkeys 48
  Disable Task Manager and Run 48

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Logon Manager Agent
FTU	First Time Use Wizard
ESSO-AM	Oracle Enterprise Single Sign-on Authentication Manager
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Oracle Enterprise Single Sign-on Kiosk Manager
ESSO-LM	Oracle Enterprise Single Sign-on
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

About ESSO-KM

Oracle Enterprise Single Sign-on Kiosk Manager (ESSO-KM) delivers a secure, easy to use and easy to administer solution that addresses the needs of traditional Single Sign-On in a kiosk environment. ESSO-KM has a client-side agent that suspends or closes inactive sessions and seamlessly shuts down all applications. This solution provides user identification to the kiosk by prompting users to log on with a Windows password or any supported primary authenticator.

Note: Many sections in this document reference settings in the ESSO-LM Administrative Console. For more information on using the Administrative Console, refer to the *ESSO-LM Administrative Console Help*.

The following topics are covered in this guide:

- Events and Actions
- About the Desktop Manager
- Customizing the Desktop Manager
- Desktop Status Window
- Transparent Screen Lock
- Bypassing the Agent
- Closing the Agent
- Events and Audit Logs
- Set up a Trust
- Authenticating to ESSO-KM with ESSO-AM
- Configuring Smart Card Removal
- Linking to ESSO-PR
- Command Line Options
- .NET API
- Best Practices

Events and Actions

The following overview describes ESSO-KM session functionality.

Types of Events

ESSO-KM can be configured such that actions can be performed by any combination of the events below for all types of authenticators supported by ESSO-LM:

- After Session Unlocked
- AM Device In
- AM Device Out
- AM Grace Period
- Authenticator Logon
- Authenticator Timeout
- Before Session Unlocked
- Cached Credential Session Start
- Session End
- Session Locked
- Session Start
- Timer Expired
- Transparent Screen Displayed
- Transparent Screen Hidden
- User Change

Events and Action Lists

Based upon the above events, ESSO-KM can run a specified terminate list, launch a custom task (.NET application or script) through a run list, or specify a special action:

- **Terminate list**. A list of applications to be closed by ESSO-KM on a specified event. (Previously known as black lists or applications to close on session end.)
- **Run list**. Either a .NET API to call or a script of command lines to be executed by ESSO-KM on a specified event.
- **Special actions list**. Special action lists specify how to handle application windows, such as the positioning of the application and the order that this application has actions performed on it.

Configuring Events and Action Lists

These features are configured through the ESSO-LM Administrative Console under **Kiosk Manager** > **Actions** and **Session States**:

- An **Action** tells ESSO-KM to do something, such as call a .NET method or terminate a specific application.
- **Session States** are a list of events, authenticators, and security settings to associate with actions. For example, a defined session state can instruct ESSO-KM that when a session ends, perform this list of actions.

See the following sections for instructions on how to:

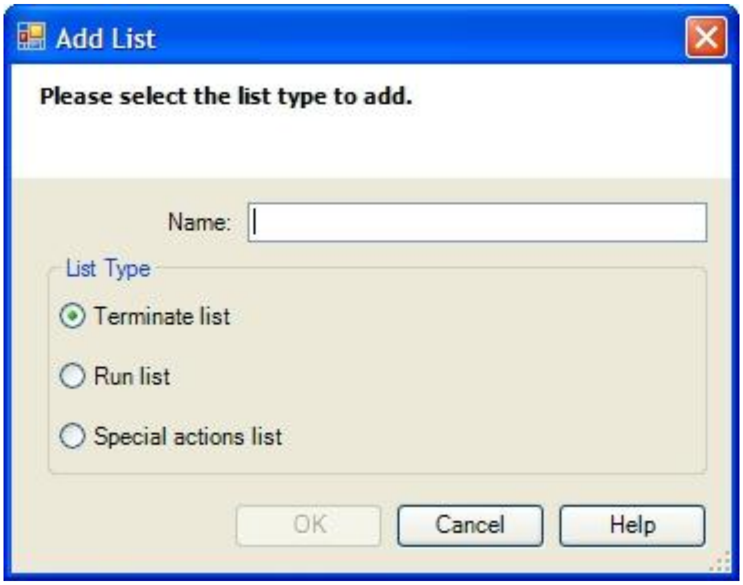
- Create an Action List
- Create a Session State

Create an Action List

An action tells ESSO-KM to do something, such as call a .NET method or terminate a specific application.

To create an action list:

1. Open the ESSO-LM Administrative Console.
2. In the left pane, click **Kiosk Manager**.
3. Click **Actions**.
4. Click **Create**.



Please select the list type to add.

Name:

List Type

● Terminate list

○ Run list

○ Special actions list

5. Select the **List Type** and enter a **Name**. Click **OK** when complete. The three types of actions lists are:
   - Terminate lists
     Terminate lists are a list of applications to be closed by ESSO-KM on session end.
   - Run lists
     Run lists are either a .Net API to call or a script of command lines to be executed by ESSO-KM.
   - Special Actions lists
     Special Action lists specify how to handle application windows, such as the positioning of the application and the order that this application has actions performed on it.

Note: For more information, refer to the specific list section for complete instructions on creating all lists.

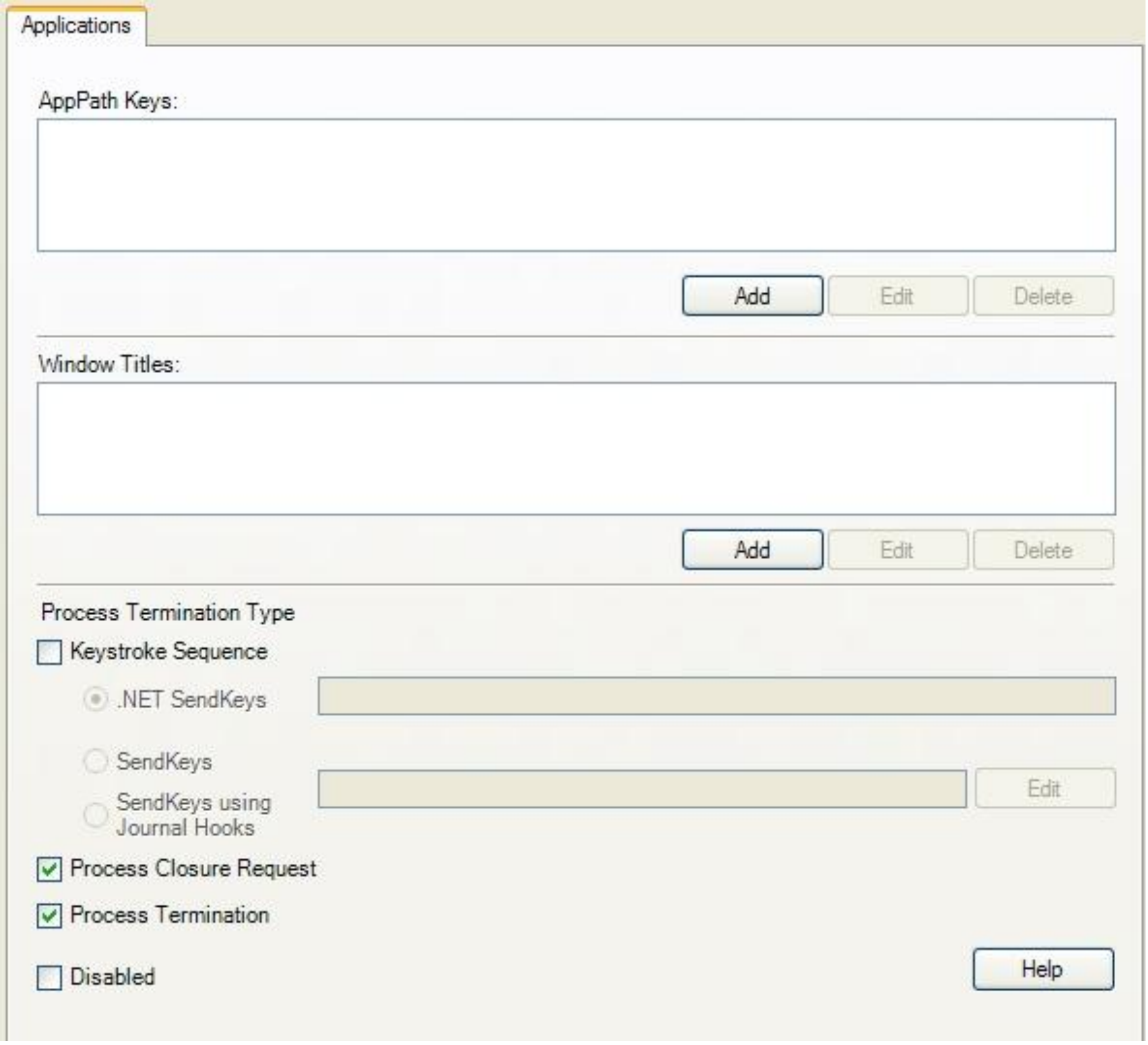
You can also create an action list by:

1. In the left pane, click **Kiosk Manager**.
2. Click **Session States**.
3. Select a Session State and click the **Actions** tab.
4. Click **Create**.

Terminate List

Terminate lists are used to specify applications to be closed by ESSO-KM on session end.

1. In the left pane, click **Kiosk Manager** > **Actions**.
2. Click on any Terminate List.



☐ Keystroke Sequence

● .NET SendKeys

○ SendKeys

○ SendKeys using Journal Hooks

☑ Process Closure Request

☑ Process Termination

☐ Disabled

Controls

AppPath Keys	The Windows registry key identifying an application associated with this logon to match against running processes. (Usually the application executable's name, such as Notepad.exe)
Window Titles	Text matched against logon window titles to identify logon requests.
Process Termination Type	Select the methods of termination for applications to be closed on session end: • **Keystroke Sequence** • **.Net SendKeys** • **SendKeys:** Configure fields by transmitting a keystroke series to the form. Click **Edit** to enter or change the series. • **SendKeys using Journal Hooks:** Configure fields by transmitting a keystroke series to the form using Journal Hooks. Click **Edit** to enter or change the series. **Note:** Sendkeys is not a reliable method and therefore not guaranteed to work as expected. It is recommended that you do not use sendkeys. • Process Closure Requests • Process Termination **Note:** When using keystroke sequences to terminate an application, a visual flicker occurs on the end users screen. This flicker is a function of using sendkeys to terminate an application.
Disabled	Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list. This way you can still refer to the settings and use them with other lists.

Configuring an Application

1. Under the AppPath Keys box, click **Add**. The Process Path Key dialog box displays.
2. Enter a valid application key (usually the application executable's name, such as Notepad.exe). Click **OK**.
3. The application has been added to the list of applications to close on session end. ESSO-KM will terminate these applications when a session ends.
4. Use the **Edit** and **Delete** buttons to modify or remove applications from this list.
5. In the Window Titles box, click **Add**. The Windows Title dialog box appears.
6. Enter a valid windows title. Click **OK**.

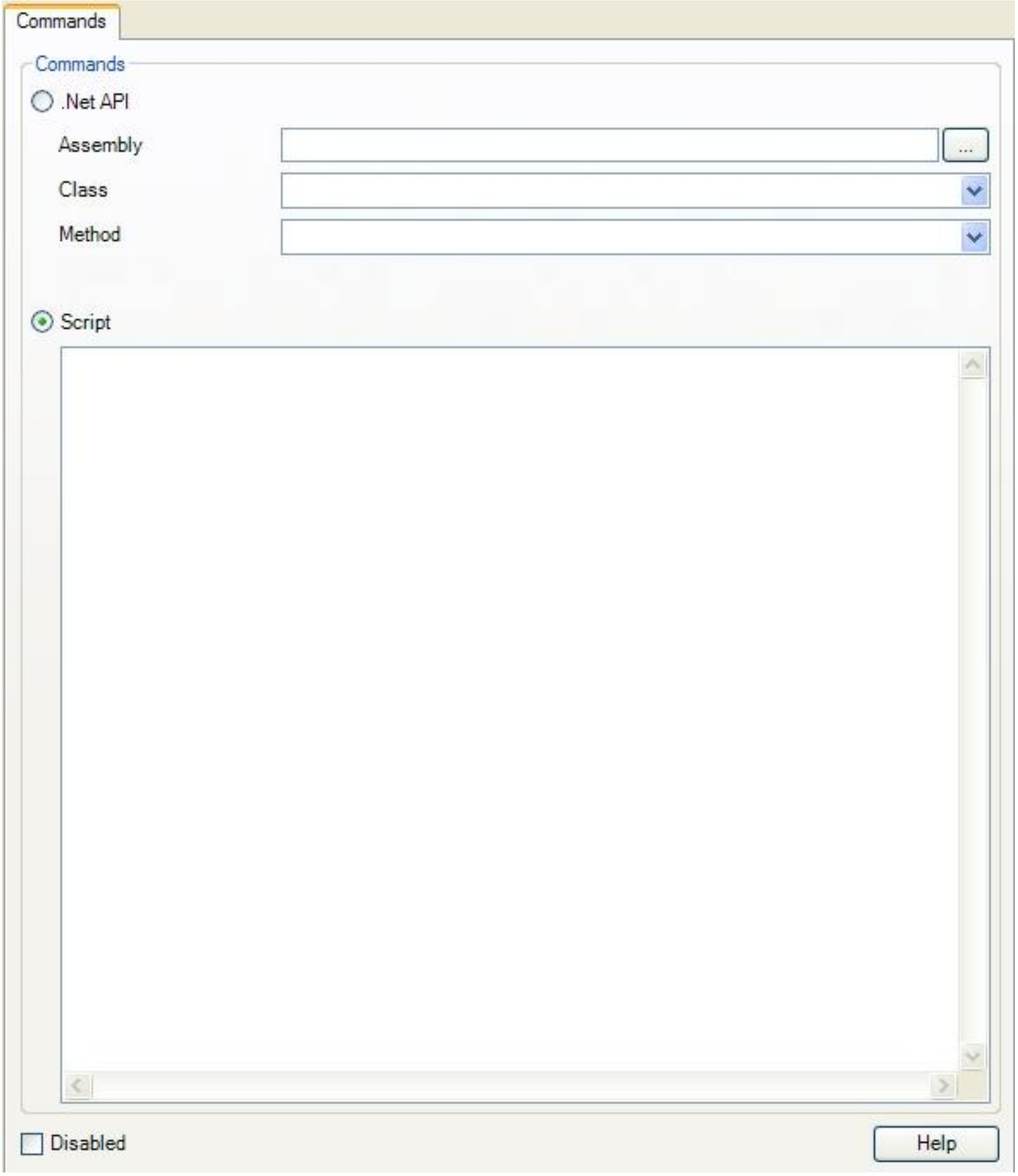
Specifying a Window Title for Matching

1. Enter (or edit) the exact Window Title.
2. Click **OK**.

Run List

Run lists are used to define either a .Net API to call or a script of command lines to be executed by ESSO-KM.

1. In the left pane, click **Kiosk Manager** > **Actions**.
2. Select a Run list .



Commands

Select a **.Net API** or **Script** command to run:

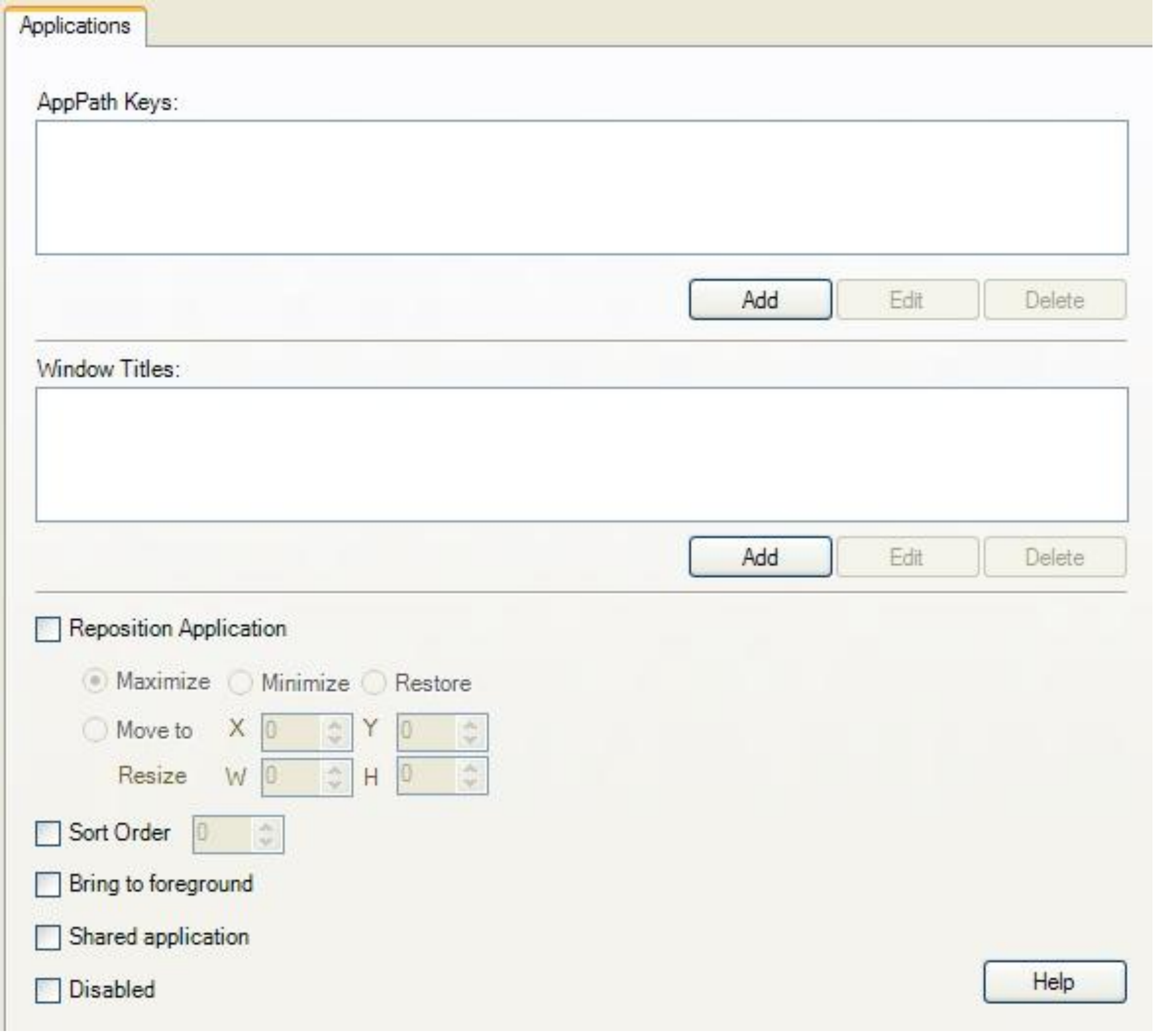
.Net API	Assembly	Click the **"..."** to locate the .Net assembly to use. The assembly loads.
	Class	Select a .Net class using the drop-down box. The .Net classes listed will be those that are available in the selected assembly.
	Method	Select a method to call using the drop-down box. The .Net methods listed will be those that are available in the selected class. The method will be limited to the following signature and will not take any parameters or return any values: `void MethodName();` Unlike the script, processing will not continue until the method returns.
	Click here to see a sample .Net API. **Note:** .Net API calls are synchronous (ESSO-KM will wait for the call to complete).	
Script	Enter a command line script for ESSO-KM to execute. If this list contains multiple commands, each line starts without waiting for the previous task to terminate or checking the previous task's return code. **Note:** Command line calls are asynchronous (run in parallel to other tasks including ESSO-KM).	
Disabled	Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list. This way you can still refer to the settings, and copy them to other lists, etc.	

Special Actions List

Special action lists are used to specify how to handle application windows, such as the positioning of the application and the order that this application has these actions performed on it.

If an application window does not appear in a special actions list, it will be hidden.

1. In the left pane, click **Kiosk Manager** > **Actions**.
2. Click on any Special Actions List.



Controls

AppPath Keys	The Windows registry key identifying an application associated with this logon to match against running processes. (Usually the application executable's name, such as Notepad.exe)
Window Titles	Text matched against logon window titles to identify logon requests.
Reposition Application	This setting and those below it allow you to specify the position of the application. The state of this checkbox determines if the actions listed below it will be applied to the application window. **Options:** • Maximize • Minimize • Restore • Move to. Enter the coordinates for the applications position. • Resize. Enter the width and height for the applications position.
Sort Order	This setting determines the order in which special actions are executed. This ensures that windows which are brought to the foreground can be in a specific order with a preferred window displayed on top when multiple windows are repositioned.
Bring to foreground	This setting ensures that the application window is always first in the application windows order.
Shared application	Check this box to enable an application to be shared among user sessions. For example, if “Notepad.exe” is designated as a shared application, if user1 opens a document in notepad and then locks the session, notepad will be running when user2 starts a session. If user2 then closes notepad and locks their session, notepad will no longer be running when user1 logs back on.
Disabled	Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list. This way you can still refer to the settings and use them with other lists.

Configuring an Application

1. Under the AppPath Keys box, click **Add**. The Process Path Key dialog box displays.
2. Enter a valid application key (usually the application executable's name, such as Notepad.exe). Click **OK**.
3. Use the **Edit** and **Delete** buttons to modify or remove applications from this list.
4. In the Window Titles box, click **Add**. The Windows Title dialog box appears.
5. Enter a valid windows title. Click **OK**.

Specifying a Window Title for Matching

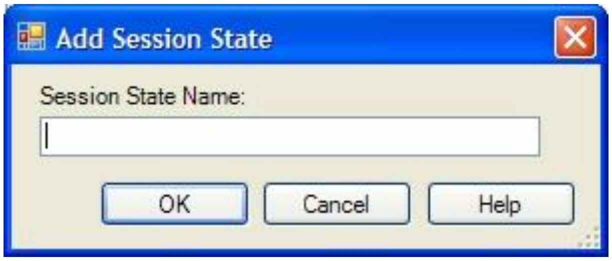
1. Enter (or edit) the exact Window Title.
2. Click **OK**.

Create a Session State

A Session State is a list of events, authenticators, and security settings to associate with actions. For example, a defined Session State can instruct ESSO-KM to perform this list of actions upon session end.

To create a session state:

1. Open the ESSO-LM Administrative Console.
2. In the left pane, click **Kiosk Manager**.
3. Click **Session States**.
4. Click **Create**.



Add Session State

Session State Name:

5. Type a **Session State Name** and click **OK**.
6. The new Session State is created. Each Session State has four tabs associated with it:
   - Events tab
   - Authenticators tab
   - Actions tab
   - Security tab

Kiosk Manager > Session States > Events tab

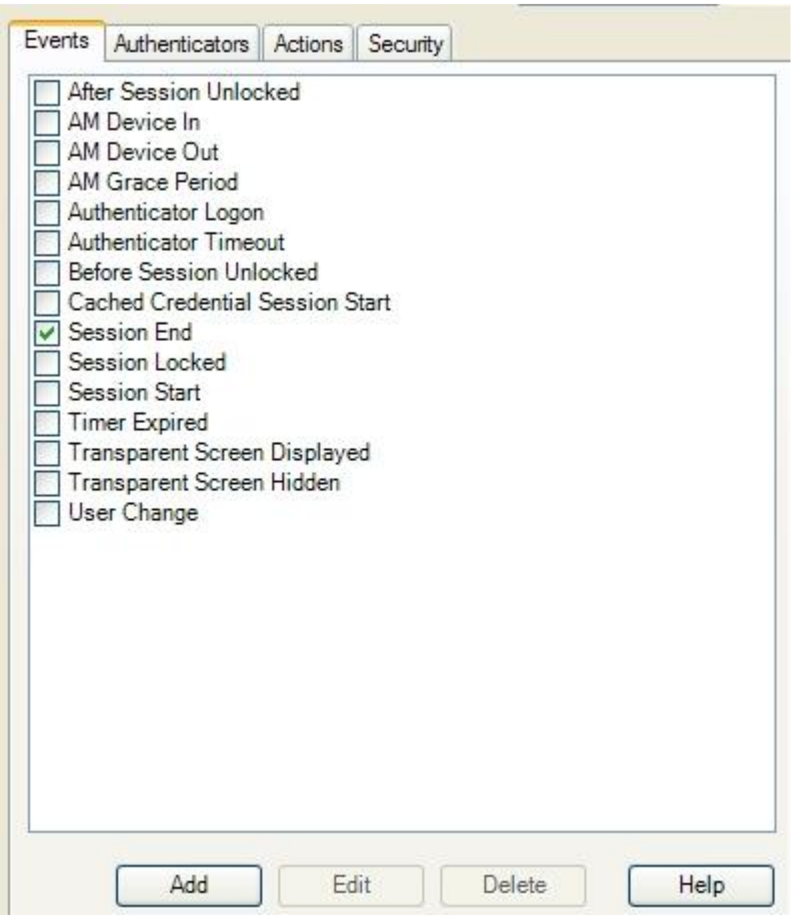
The Events tab contains a list of all the possible events that ESSO-KM can respond to and the option to add custom events. Each listed event has a checkbox next to it that when checked indicates that the associated action lists should be executed when this event occurs. When a new session state is created, **Session End** is checked by default.

There are two ways to create events:

1. Select the pre-defined events for this session state

2. Create your own custom events by clicking the Add button. Use the Edit button to edit the custom event name and the **Delete** button to delete a custom event.

   Pre-defined events are:



☐ After Session Unlocked
☐ AM Device In
☐ AM Device Out
☐ AM Grace Period
☐ Authenticator Logon
☐ Authenticator Timeout
☐ Before Session Unlocked
☐ Cached Credential Session Start
☑ Session End
☐ Session Locked
☐ Session Start
☐ Timer Expired
☐ Transparent Screen Displayed
☐ Transparent Screen Hidden
☐ User Change

Select Predefined Event

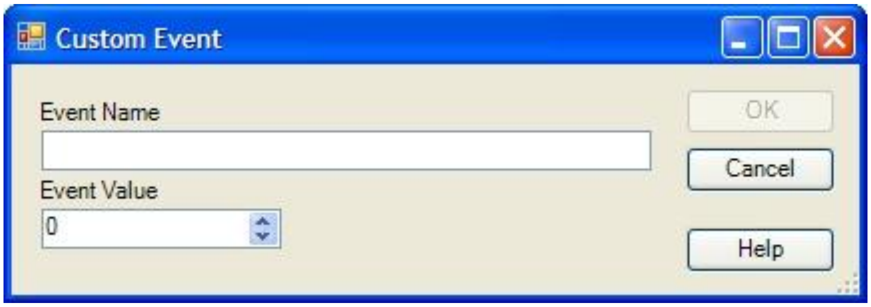
- **After Session Unlocked**
  This event runs when the user unlocks their session after authentication has taken place. If an authentication is canceled, this event will not be triggered.
- **AM Device In**
  This event is triggered when the ESSO-LM device monitor is enabled and a monitored authenticator is detected (for example, a smart card is inserted or a biometrics device is in range).
- **AM Device Out**
  This event is triggered when the ESSO-LM device monitor is enabled and a monitored authenticator is detected (e.g., a smart card is removed or a biometric goes out of range).
  This event will only be triggered when:
  oA session is open or locked
  oA "Device-In" event started the session
- **AM Grace Period**
  This event is triggered if an authenticator which uses a grace period function (for example, Xyloc proximity badges) is being used and a user returns to an open session within the grace period.
- **Authenticator Logon**
  This event is triggered when an authenticator has accepted a logon. For example, the correct password for WinAuth or the correct PIN for smart card is entered.
- **Authenticator Timeout**
  This event is triggered when the ESSO-LM internal timer has expired.
- **Before Session Unlocked**
  This event is triggered when a user unlocks their session but before authentication takes place.
- **Cached Credential Session Start**
  This event is triggered when a session is started and the user has cached credentials stored on the local computer.
- **Session End**
  This event is triggered when the session ends and the timer expires, or when another user starts a session.
- **Session Locked**
  This event is triggered when a session is locked.
- **Session Start**
  This event is triggered when a user starts a new session.
- **Timer Expired**
  This event is triggered when the locked session timer has reached 00:00:00.
- **Transparent Screen Displayed**
  This event is triggered when the transparent lock initiates and the screen is visible to the user in locked mode.
- **Transparent Screen Hidden**
  This event is triggered when the transparent lock is hidden.

- **User Change**
  This event is triggered when a user logs into ESSO-KM. This event sets two properties on the .Net object if they exist (If the properties do not exist, nothing happens):
  - **UserName.** The sync user name.
  - **DomainName**. The sync domain name.

Note: ESSO-AM events run when the authenticator sends a message to ESSO-KM indicating the event type.

Add Custom Event

To add a custom event, click the **Add** button on the **Events** tab. The Custom Event dialog box opens:



1. Type an **Event Name**. This is the event name that displays.
2. Enter an **Event Value**. An external application generates the custom event, sending a message to the ESSO-KM hidden window. The value is the custom value that the other application sends.
3. Click **OK**. The custom event is created.

Kiosk Manager > Session States > Authenticators tab

The **Authenticators** tab contains a list of all the authenticators that ESSO-LM supports as well as the option to add a custom authenticator.

Each authenticator has a checkbox next to it that when checked indicates if the associated action lists should be executed when the selected events occur and the selected authenticator was used to authenticate the user.

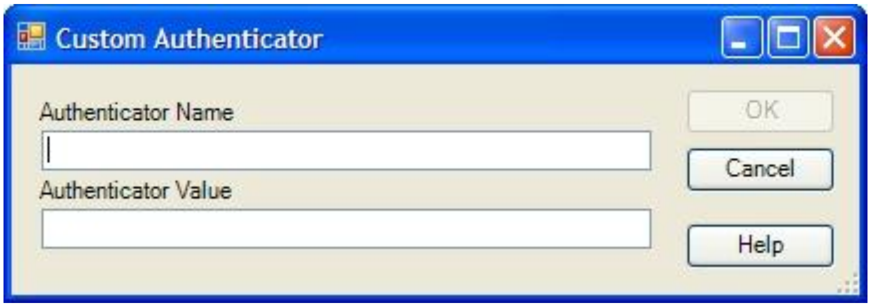
When a new session state is created, all authenticators are checked by default.

There are two ways to select authenticators:

1. Create your own custom authenticator by clicking the **Add** button. Use the **Edit** button to edit the custom event authenticator and the **Delete** button to delete a custom authenticator.
2. Select the pre-defined authenticator for this session state. Available authenticator are:
    - Authentication Manager
    - Entrust
    - LDAP
    - LDAP v2
    - Proximity Card
    - Read-Only Smart Card
    - SAFLINK SAFauthenticator
    - SecurID
    - Smart Card
    - Sphinx
    - Windows Logon
    - Windows Logon v2
    - XylocAuth

Add Custom Authenticator

Custom authenticators allow you to filter events based on that authenticator. To add a custom authenticator, click the **Add** button on the **Authenticators** tab. This opens the Custom Authenticator dialog box:

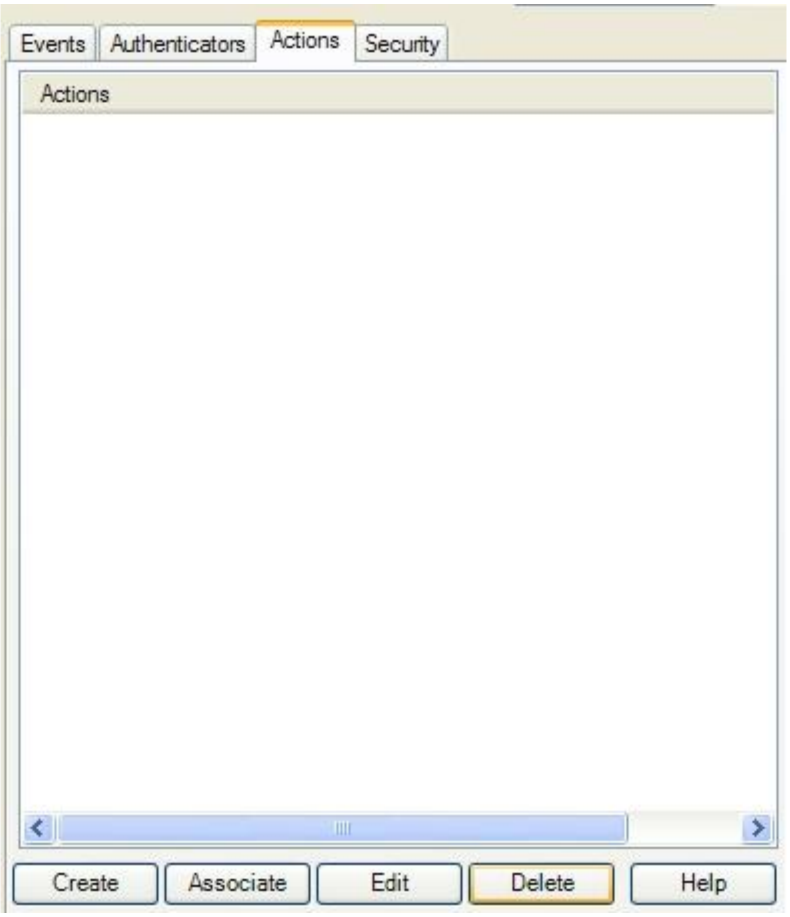


1. Type an **Authenticator Name**. This is the authenticator name that displays.
2. Enter an **Authenticator Value**. The authenticator value is the name that the authenticator is known by within the code. This name comes from the authenticator itself. For example, the value for Windows Authenticator v1 is WinAuth, for Windows Authenticator v2 is MSAuth, and for Smart Card is SCAuth.
3. Click **OK**.

Kiosk Manager > Session States > Actions tab

The **Actions** tab contains a list of all the actions associated with a specific session state. This list will be empty for newly created session states. After actions are associated with the session state, they will be listed in this tab.

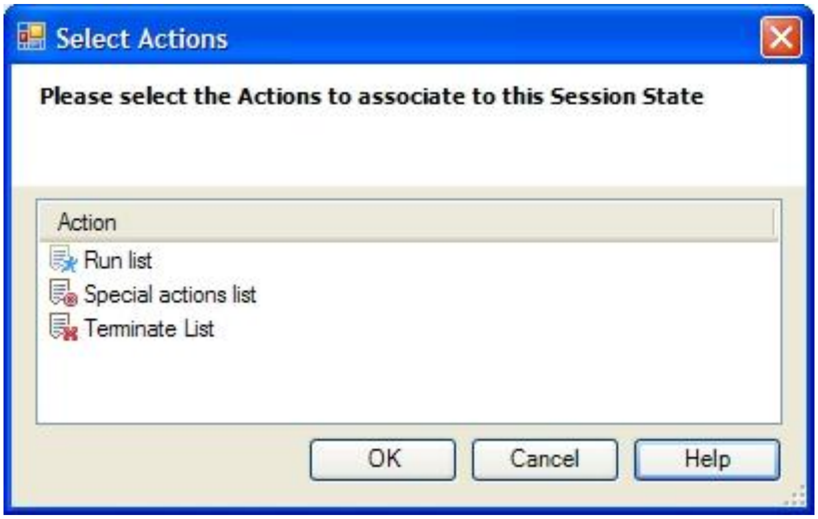
Use this tab to create, associate, edit and delete actions.



- To define a new action list, click Create. If a new action is created from this tab, it is automatically added to this session state.
- To associate a defined action with this session state, click Associate and select an action from the list.
- To make changes to an action, highlight it and click **Edit**.
- To delete an action from a session state, click **Delete**. This deletes the action only from the current session state, not the actions list.

Associate Actions

Use the Select Actions dialog box to select one or more actions to associate to this session state.



Select the actions to add to this session state (use **Ctrl+click**, or **Shift+click** to select multiple entries). Click **OK**.

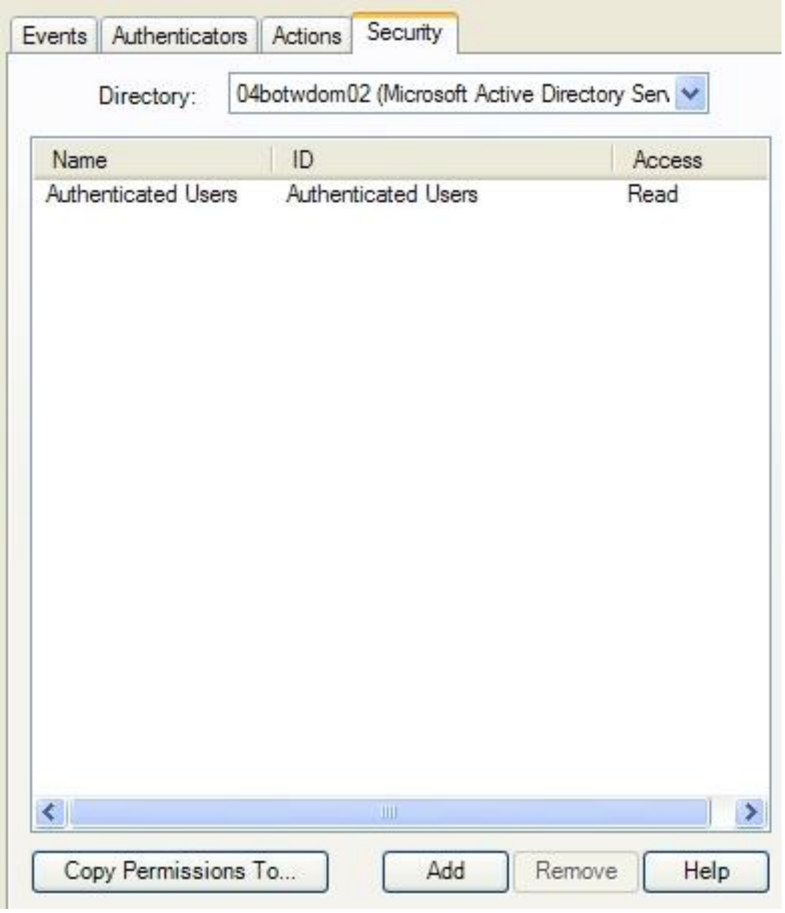
Note: If actions are associated with this session state, and you are adding new actions, ALL actions need to be re-selected, otherwise the list of actions will be replaced with the newly selected actions.

Kiosk Manager > Session States > Security Tab

Use the **Security** tab to set the access rights for this session state. You can assign access rights to these items:

- Application logons (including associated credential sharing groups)
- Password generation policies
- Global agent settings
- Passphrase question sets

Note: The security tab will only show up if Role/Group security is enabled.



Directory: 04botwdom02 (Microsoft Active Directory Ser

Name	ID	Access
Authenticated Users	Authenticated Users	Read

Controls

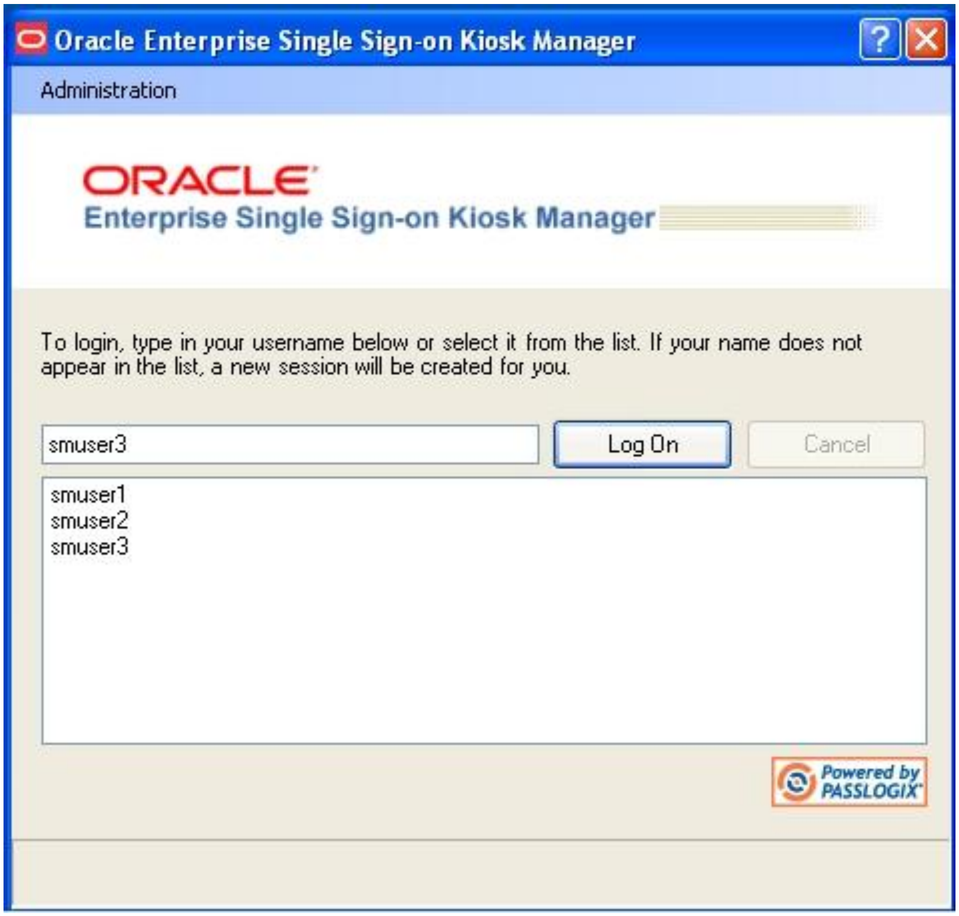
Directory	Select the target directory server.
Access information	
Name	Lists the groups or users who currently have access to this session state.

ID	The user account name.
Access	Indicates whether the user or group has read/write or read-only access rights to the currently selected session state. To change a user or group's access rights, right-click the user or group and select **Read** or **Read/Write** from the shortcut menu.
Actions	
Copy Permissions to	Use this button to easily apply the security rights for the current application to multiple applications. Clicking this button displays a dialog listing all the applications. Select the applications that you want these security rights to be copied to. Use **Ctrl+click** to select multiple entries. Click **OK**.
Add	Displays the Add User or Group dialog box (for LDAP or Active Directory) to select the users or groups who should have access to the currently selected session state.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+click** or **Shift+click** to select multiple entries.

About Desktop Manager

The Desktop Manager is the logon dialog that manages the ESSO-KM sessions on the kiosk. End users can start and unlock sessions from this dialog. Administrators can terminate sessions, shut down the computer, restart the computer and exit ESSO-KM.

Note: The Desktop Manager is configured through the ESSO-LM Administrative Console on the Global Agent Settings > Kiosk Manager panel. Refer to the ESSO-KM *Installation and Setup Guide* or the ESSO-LM Administrative Console help for more information.


Oracle Enterprise Single Sign-on Kiosk Manager
Administration
ORACLE
Enterprise Single Sign-on Kiosk Manager

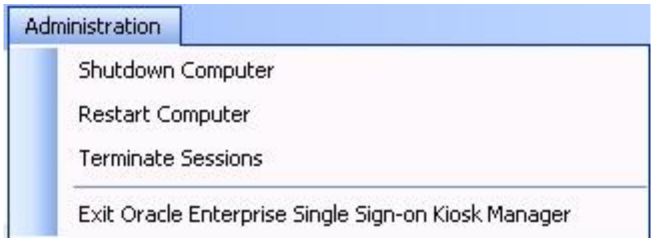
To login, type in your username below or select it from the list. If your name does not appear in the list, a new session will be created for you.

smuser3

smuser1
smuser2
smuser3

Administration Menu

The **Administration** menu is located on the top of the Desktop Manager.



The settings that are used to configure this menu are:

- **Restart Computer**. Options are **Disable**, **Enable**, or **Administrator must supply password**. Default is disable.
- **Shutdown Computer**. Options are **Disable**, **Enable**, or **Administrator must supply password**. Default is disable.
- **Allow administrator to close ESSO-KM.** Options are **Yes** or **No**. Default is yes. This setting controls the Exit Oracle Enterprise Single Sign-on Kiosk Manager option and the **X** in the title bar.

Note: If the Kiosk account does not have sufficient privileges, the **Restart Computer** and **Shutdown Computer** options may not work even if they are disabled.

Open Sessions (Multi-Sessions)

The Desktop Manager includes a list that displays all open sessions. Multiple sessions can be running at one time. There is no maximum amount of sessions. To configure the number of open sessions allowed:

1. Open the ESSO-LM Administrative Console, expand **Global Agent Settings** > **Kiosk Manager**.
2. Locate the **Maximum number of sessions** setting.
3. Set this value to the number of sessions allowed. There is no maximum. The default is 1.

A large number of open sessions at one time can cause memory to run low. Track memory consumption provides a way to set a threshold to close locked sessions when memory conditions are low.

To configure this feature:

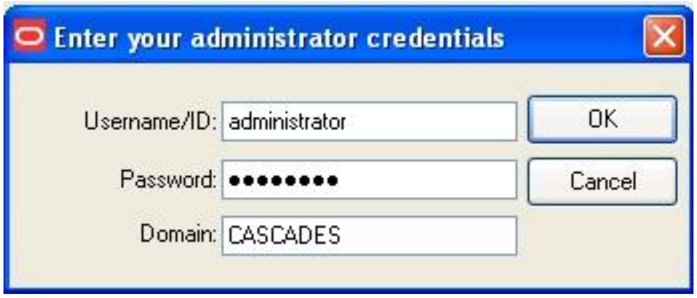
1. Open the ESSO-LM Administrative Console, expand **Global Agent Settings** > **Kiosk Manager**.
2. Locate the **Track Memory Consumption** setting.
3. Set this value as necessary. Default is 90%. Minimum = 0 (disabled) and maximum = 100.

When system memory use has reached the percentage as set by this value, ESSO-KM will automatically close oldest user sessions.

Terminate Sessions

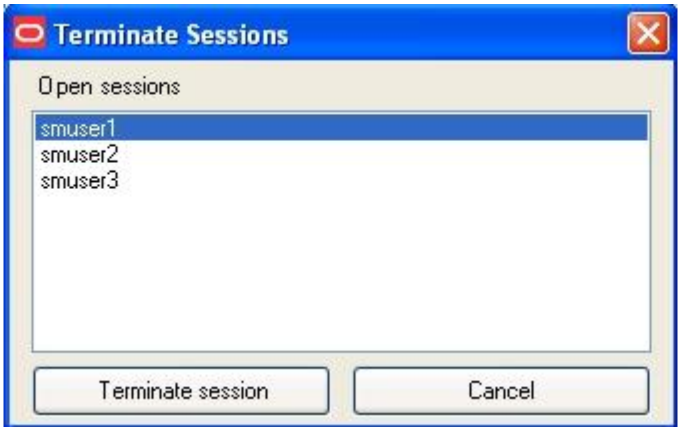
Administrators can terminate ESSO-KM user sessions from the Desktop Manager by clicking **Terminate Sessions** from the **Administration** menu. This menu option is not configurable.

When clicked, the Authenticate as Administrator dialog appears prompting the administrator to enter administrative credentials before performing this action.



Username/ID: administrator
Password: •••••••••
Domain: CASCADES

Once credentials are entered, the Terminate Sessions dialog appears.



smuser1
smuser2
smuser3

Only one session can be selected at a time. **Cancel** and the **X** close this dialog.

Customizing the Desktop Manager

The Desktop Manager can be customized in the following ways:

- Add a custom text message around the logon dialog
- Upload a background image around the logon dialog
- Replace the Oracle and ESSO-KM logo banner on the logon dialog

You may choose to display a company logo as the background image, or an important custom text message to inform your users of any important information.

This section provides instructions and examples to help you control the positioning and appearance of the background image and text message, as well as an example. It also provides instructions on how to replace the logon dialog logo banner.

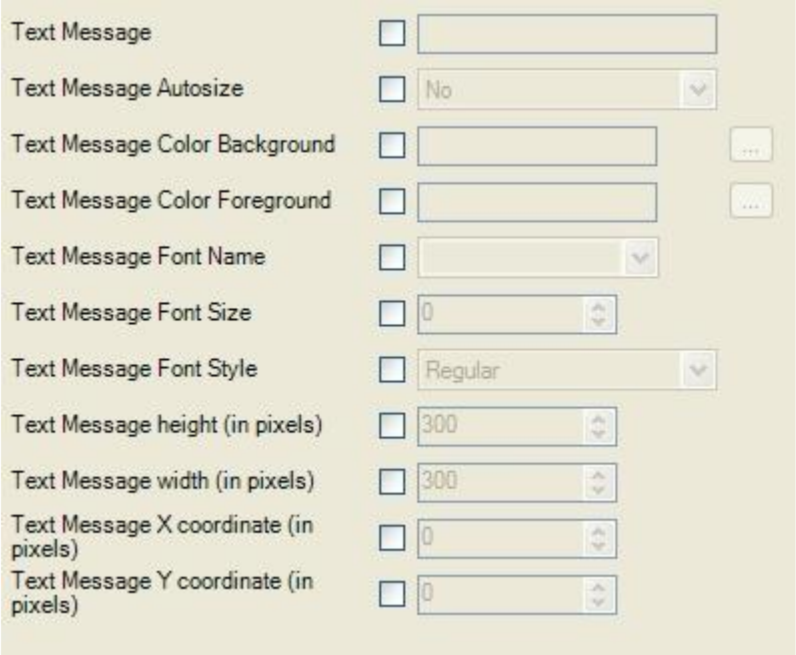
Note: The Desktop Manager customization is configured through the ESSO-LM Administrative Console on the **Global Agent Settings > Kiosk Manager > Desktop > Background Image** and **Text Message** panels.

Customizing the Text Message

ESSO-KM provides the ability to insert a custom text message on the Desktop Manager. This feature can be used to inform your users of any important information.

To configure the Administrative Settings for Desktop Manager text message:

1. Open the ESSO-LM Administrative Console.
2. Navigate to **Global Agent Settings > Live > Kiosk Manager > Desktop > Text Message**.



Text Message	□	
Text Message Autosize	□	No
Text Message Color Background	□	
Text Message Color Foreground	□	
Text Message Font Name	□	
Text Message Font Size	□	0
Text Message Font Style	□	Regular
Text Message height (in pixels)	□	300
Text Message width (in pixels)	□	300
Text Message X coordinate (in pixels)	□	0
Text Message Y coordinate (in pixels)	□	0

Text Message	Message text to provide on the ESSO-KM Desktop Manager. This message will be displayed when the Desktop Manager is active.
Text Message Autosize	**This setting is new as of version 10.1.4.1.0.* Select whether the text message should be auto-sized. This setting automatically sets the size of the control based on the size of the message. **Options:** • Yes • No
Text Message Color Background	Click the ellipses **...** button to select the background color for the text message.
Text Message Color Foreground	Click the ellipses **...** button to select the foreground color for the text message.
Text Message Font Name	The font that the text message will display in. Select a font from the drop-down list.
Text Message Font Size	The font size the text message will display in.
Text Message Font Style	The font style the text message will display in. **Options:** • Regular • Bold • Italic
Text Message height (in pixels)	The height of the message of the day (in pixels). Default is 300.
Text Message width (in pixels)	The width of the message of the day (in pixels). Default is 300.
Text Message X coordinate (in pixels)	The X coordinate for the text message. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
Text Message Y coordinate (in pixels)	The Y coordinate for the text message. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.

Customizing the Background Image

ESSO-KM provides the ability to insert a custom background image on the Desktop Manager. This feature can be used to upload a company logo.

To configure the administrative settings for the Desktop Manager text message:

1. Open the ESSO-LM Administrative Console.
2. Navigate to **Global Agent Settings > Live > Kiosk Manager > Desktop > Background Image**.

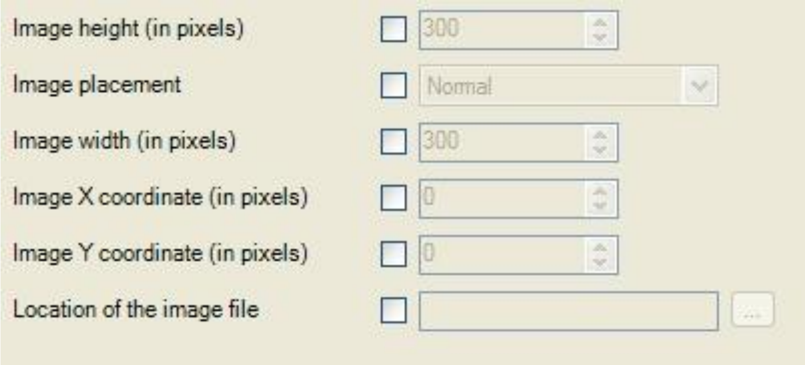


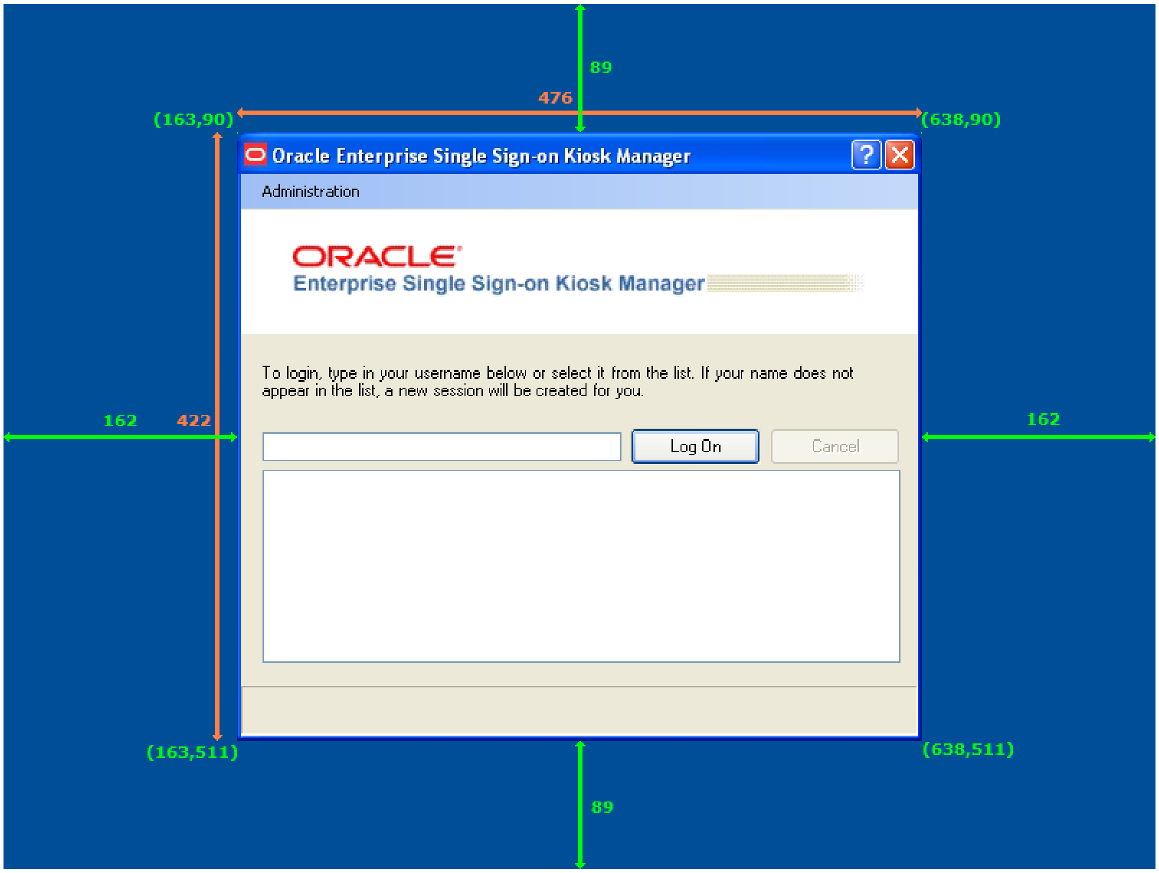
Image height (in pixels)	□	300
Image placement	□	Normal
Image width (in pixels)	□	300
Image X coordinate (in pixels)	□	0
Image Y coordinate (in pixels)	□	0
Location of the image file	□	

Image height (in pixels)	The height of the image (in pixels). Default is 300.
Image Placement	**This setting is new as of version 10.1.4.1.0.* The placement of the logo image. **Options:** • Normal. Image is placed in upper left corner of coordinates and clipped if larger than specified height and width. • Autosize. Image is placed in upper left corner of coordinates. • Center. Image is centered within coordinates and clipped if larger than specified height and width. • Stretch. Image is stretched or shrunk to fit within specified coordinates. • Maximize. Image is stretched to full screen size.
Image width (in pixels)	The width of the image (in pixels). Default is 300.
Image X coordinate (in pixels)	The X coordinate for the image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.

Image Y coordinate (in pixels)	The Y coordinate for the image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
Location of the image file	Full- qualified path and filename to the image file. Click the **...** button to locate the file.

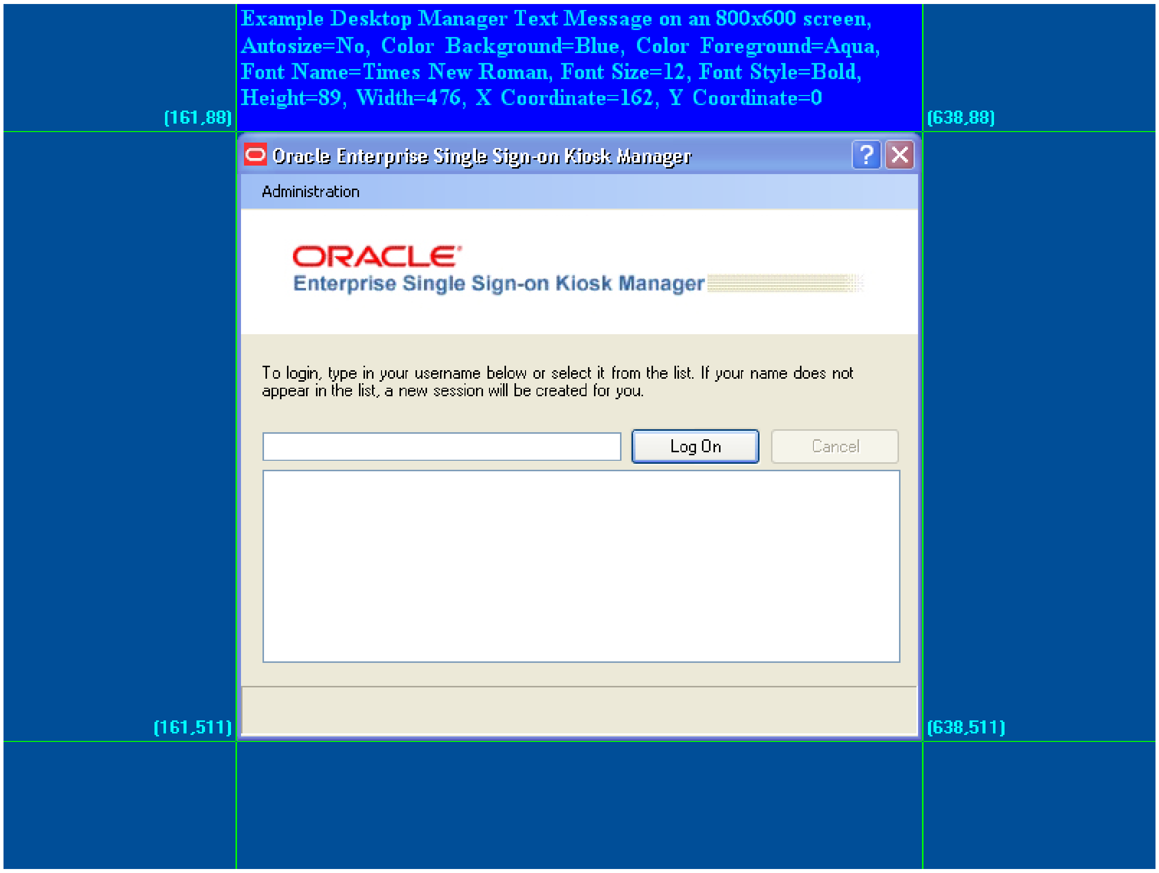
Example on an 800x600 display:

This screen shot illustrates the horizontal and vertical dimension of the Desktop Manager logon dialog and the location of it on the screen.


89
476
(163,90)
(638,90)
Oracle Enterprise Single Sign-on Kiosk Manager
Administration
ORACLE
Enterprise Single Sign-on Kiosk Manager
162
422
162
Log On
Cancel
(163,511)
(638,511)
89

To login, type in your username below or select it from the list. If your name does not appear in the list, a new session will be created for you.

This screen shot illustrates an example of a text message. This text message displays the values used to customize the text message as seen in this screen shot.



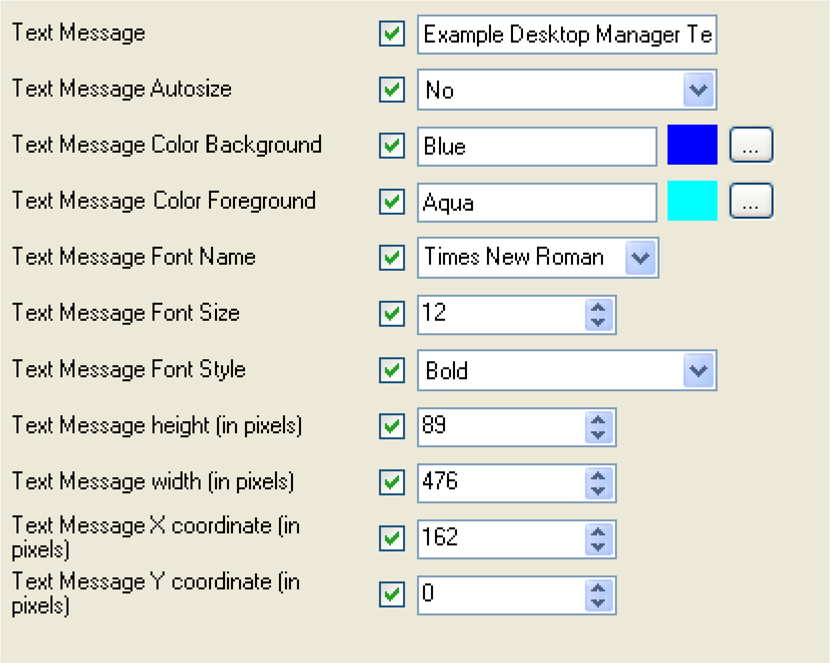
Example Desktop Manager Text Message on an 800x600 screen, Autosize=No, Color Background=Blue, Color Foreground=Aqua, Font Name=Times New Roman, Font Size=12, Font Style=Bold, Height=89, Width=476, X Coordinate=162, Y Coordinate=0

(161,88)
(638,88)
Oracle Enterprise Single Sign-on Kiosk Manager
Administration
ORACLE
Enterprise Single Sign-on Kiosk Manager

To login, type in your username below or select it from the list. If your name does not appear in the list, a new session will be created for you.

Log On
Cancel
(161,511)
(638,511)

This screen shot displays the actual values used to produce the text message as seen above.



Text Message	☑	Example Desktop Manager Te
Text Message Autosize	☑	No
Text Message Color Background	☑	Blue
Text Message Color Foreground	☑	Aqua
Text Message Font Name	☑	Times New Roman
Text Message Font Size	☑	12
Text Message Font Style	☑	Bold
Text Message height (in pixels)	☑	89
Text Message width (in pixels)	☑	476
Text Message X coordinate (in pixels)	☑	162
Text Message Y coordinate (in pixels)	☑	0

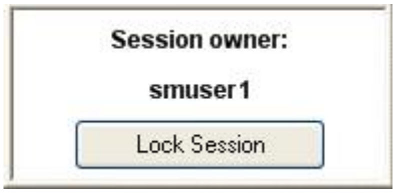
Replacing the Logo Banner

The ability to modify the Oracle ESSO-KM logo banner on the Desktop Manager logon dialog is available through a manual step. To replace that logo you must:

1. Create a "branding" folder in the directory that SMAgent.exe is installed to, for example C:\Program Files\Passlogix\ESSO-KM\branding.
2. Place the customized logo banner in the branding folder with the name "banner.gif".
3. Customized banner will appear next time ESSO-KM is started.

Desktop Status Window

The Desktop Status window is a small window that displays during a ESSO-KM session which allows you to conveniently view the current session owner and lock the session. If enabled, by default it displays in the upper right corner of the desktop during a session.


Session owner:

smuser1

A configuration setting is available in the ESSO-LM Administrative Console to configure this window (under **Global Agent Settings** > **Kiosk Manager**: **Desktop Status Window**).

The desktop status window is hidden by default. Select your preference. The default values are calculated at runtime. The window is placed in the upper-right hand corner of the display with 10 pixels between the edge of the window and the physical edge of the screen. The location of this window can be manually configured from the Kiosk Manager panel:

1. **Status Window X coordinate.** The X coordinate for the status window in pixels. This is the horizontal location of the status window on the desktop.
2. **Status Window Y coordinate**. The Y coordinate for the status window in pixels. This is the vertical location of the status window on the desktop.

Transparent Lock

The transparent lock feature provides the ability to lock desktop inputs (keyboard and mouse) in view mode, so for example, a monitoring application can be viewed without starting a session. It is similar to the screen saver functionality. When ESSO-KM invokes the transparent lock, the desktop and applications on the desktop shall continue to be displayed on the monitor in real time.

Transparent lock is disabled by default.

When there are multiple sessions running, the last active session is displayed when transparent lock engages.

Application priorities and positioning are configurable in the Special Actions lists .

Transparent lock events are set up in the Events panel of the Session States section.

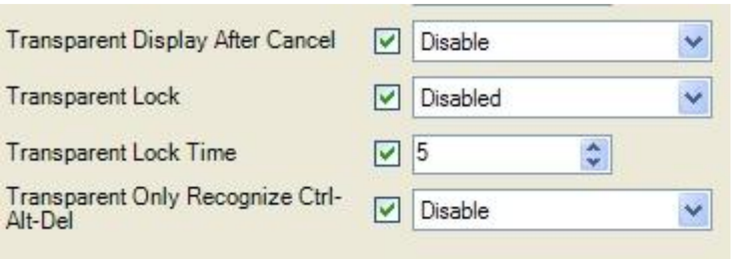
- **Transparent Screen Displayed**
  This event is triggered when the transparent lock initiates and the screen is visible to the user in locked mode.
- **Transparent Screen Hidden**
  This event is triggered when the transparent lock is hidden.

Transparent lock can be invoked in the following ways:

- **Timeout**
- **Canceling** out of an authentication if **Transparent Display After Cancel** is set to **Enable**.

To initiate a session while transparent lock is running, move mouse or click any keyboard button. If **Transparent Only Recognize Ctrl-Alt-Delete** is set to **Enable**, users will have to click Ctrl+Alt+Delete to disengage Transparent Lock.

Note: Transparent screen lock is configured through the ESSO-LM Administrative Console on the **Global Agent Settings** > **Kiosk Manager** panel.



Transparent Display After Cancel ☑ Disable

Transparent Lock ☑ Disabled

Transparent Lock Time ☑ 5

Transparent Only Recognize Ctrl-Alt-Del ☑ Disable

Transparent Display After Cancel	This setting determines whether the display after cancel feature should be enabled. If disabled, ESSO-KM will revert to the inactivity timer to determine when to display the desktop. If enabled, when an authentication or synchronization dialog is canceled, the desktop will be viewable instantly. **Note:** The Transparent Lock setting below must be turned on in order for this feature to work. **Options:** • Disable (default) • Enable
Transparent Lock	This setting determines whether the transparent lock feature should be enabled. Transparent screen lock provides the ability to lock the desktop inputs (keyboard and mouse) in view mode, so for example, a monitoring application can be viewed without starting a session. When there are multiple sessions running, the last active session is displayed when transparent screen lock engages. **Options:** • Disabled (default) • Show desktop with active session. Transparent screen lock will be enabled as long as there is an active session running. • Show desktop. If this option is chosen, the transparent screen lock will be enabled with or without an active session. If the setting is set to **Show desktop with active session**, the transparent screen lock will only be enabled if there is an active session.
Transparent Lock Time	This setting determines the number of seconds to wait for mouse and keyboard inactivity before showing the desktop (default=5). **Note:** The Transparent Lock setting above must be turned on in order for this feature to work.
Transparent Only Recognize Ctrl-Alt-Delete	This setting determines whether clicking Ctrl+Alt+Delete is the only method to turn off the transparent screen lock and display the Desktop Manager. If disabled, any keyboard or mouse activity results in displaying the Desktop Manager. If enabled, all keyboard and mouse activity will be ignored. Only Ctrl-Alt-Del and authenticators that support "device-in" will be recognized to display the Desktop Manager.

	Warning! If this setting is enabled, the machine will appear frozen if there is not any indication that Ctrl-Alt-Del is required. **Options:** • Disable (default) • Enable

Bypassing the ESSO-KM Agent

If needed, the ESSO-KM Agent can be bypassed when a kiosk starts up.

The ESSO-KM Agent will not start if you hold the **Shift** key down when logging into the computer.

Closing the ESSO-KM Agent

If needed, the ESSO-KM Agent can be closed on a kiosk by:

- Pressing **ALT + F4** on the keyboard.
- Clicking **Exit Oracle Enterprise Single Sign-on Kiosk Manager** from the **Administration** menu on the Desktop Manager.
- Clicking the **X** located on the top right of the window title bar.

The administrator is then prompted to enter his or her credentials. Only an administrator's credentials will succeed in closing the agent.

This feature is disabled by default. To enable this feature:

1. Open the ESSO-LM Administrative Console, expand **Global Agent Settings** > **Kiosk Manager**.
2. Check the **Allow administrator to close ESSO-KM** setting.
3. Select **Yes**.

Set up a Trust

ESSO-KM has the capability to allow other applications that trust ESSO-KM authentication to retrieve the logged-in username. ESSO-KM provides a public function in SSOUserInfo.dll with the following function signature:

```
extern "C" BOOL _stdcall GetUserId(BSTR* bstr);
```

Parameters:

```
bstr
```

Object to retrieve the username into.

Return Value:

Returns `TRUE` if the function succeeds and a user is currently logged in.

Returns `FALSE` if the function fails. `Use GetLastError()` for more information.

Note: If the function succeeds, the username will be returned as: "`DomainName\UserName`".

ESSO-KM can be set up to run a command line or call a .NET method after a user successfully starts a session. Utilize this mechanism to trigger the other application to request the logged-on username from ESSO-KM.

Event and Audit Logs

ESSO-KM logs agent events to the local machine's Windows Event Viewer. This functionality is enabled by default. For a list of ESSO-KM events that are logged, please see the table in the following section, Event Log Messages.

ESSO-KM can also log events to a Syslog server application on the local kiosk machine or a remote machine.

To use a Syslog application to view ESSO-KM events on a local or remote machine:

ESSO-LM Agent on the Kiosk

Note: This step must be performed before installing ESSO-KM.

1. Launch **Add-Remove Programs** from the Control Panel.
2. Click on **Oracle Enterprise Single Sign-on** and click **Change**.
3. Select **Modify** on the Program Maintenance panel.
4. On the Custom Setup panel, expand **Extensions**, and then expand **Event Manager**.
5. Select **Syslog** for installation.
6. Follow the prompts to complete installation of Syslog.

ESSO-LM Administrative Console

1. Open the ESSO-LM Administrative Console, expand **Global Agent Settings** > **Event Logging** >**Syslog**.
2. Configure the settings for the target Syslog machine according to your environment. If logging to a remote machine, specify either a hostname or IP address of the remote machine in the **Send messages to which host?** setting.

Event Log Messages

The following is the list of messages that currently are logged in the Event Viewer for applications:

Message	Notes about message, if applicable
User session started: domain/username	When a user session is started.
User session ended: domain/username	When a user session ends.
User session locked: domain/username	When a session is locked.
User session unlocked: domain/username	When a session is unlocked.
Process action: action type, action name	(IE, Terminate list, notepad_close) This corresponds to the session actions in the repository. If the action does not have a corresponding state that triggers, you should not see the action logged in the event viewer.
Process state: state name, event GUID	(IE, Session_locked, {6D5B7645-25A5-42f3-B641-BFE4DC4F774C}) This corresponds to the session states in the repository. A log entry is only generated if a state is triggered, such as a session lock. The GUID corresponds to the GUID for that state, if you viewed the state from the console. For example, if you have a state in the repository for Transparent Lock but you do not have Transparent lock turned on, you should not see an event logged.
Transparent lock screen DISPLAYED	When transparent lock displays.
Transparent lock screen HIDDEN	When transparent lock is hidden.
Method Invocation: file path/file name, method name	Corresponds with Run List .Net API Assembly name and method.
Run list command: command name	Corresponds with Run List Script commands.
The following applications were not terminated:	This will only log applications that are specified in a terminate list and did not terminate.

Message	Notes about message, if applicable
Oracle Enterprise Single Sign-on Kiosk Manager STARTED	When ESSO-KM is started.
Oracle Enterprise Single Sign-on Kiosk Manager SHUTDOWN	When ESSO-KM is shut down.
Successfully closed: Application name	Applicable to all three closure methods in the terminate list - keystroke sequence, closure request and process termination. This event is logged when the application in a terminate list is closed. Logs are not generated for applications that are closed but not specified in a terminate list.

Authenticating to ESSO-KM using ESSO-AM

ESSO-KM supports ESSO-AM for all authentication events. All authentication events take place within the authenticator so that ESSO-KM does not need to be configured for different authenticators. ESSO-KM communicates with every ESSO-AM authenticator in the same way.

When configured with smart card, proximity card, or other presence-sensing authenticator, ESSO-KM automatically initiates a session when an authenticator is detected.

When configured with smart card, proximity card, or other presence-sensing authenticator, ESSO-KM automatically suspends a session when an authenticator is no longer present.

Configuring Smart Card Removal

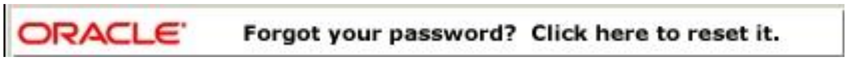
A setting is available in the ESSO-LM Administrative Console (under **Global Agent Settings >Primary Logon Methods** > **Smart Card** > **Advanced**: **Lock ESSO-KM session on removal**) that allows an administrator to configure ESSO-KM to not lock a session when the session owner removes the smart card from the smart card reader.

By default, this value is set to **Lock**. If set to **Not Lock**, the ESSO-KM session will remain open when the smart card is removed.

This setting is useful in a scenario where employees must have their smart cards displayed at all times, and, therefore, cannot leave them in a reader.

Linking to ESSO-PR

A link to ESSO-PR can be installed to the ESSO-KM Desktop Manager. This allows users to reset their own kiosk passwords (for example, AD via LDAP auth) using ESSO-PR.



Forgot your password? Click here to reset it.

Clicking this banner launches the ESSO-PR Web interface. Users can then follow the prompts to reset their password.

A link to the ESSO-PR client can be installed as a DOS command, using the following command syntax:

```
msiexec /i [/q] c:\v-GO_SMAgent.msi programURLs
```

`/q` Quiet mode: suppress all installer user-interface messages. Refer to the description of other Windows Installer command-line options for msiexec at http://msdn.microsoft.com.

programURLs (required):

```
REG_RESETURL=" http://host
    /vgoselfservicereset/resetclient/default.aspx"

REG_STATUSURL="http://host
    /vgoselfservicereset/resetclient/checkstatus.aspx"
```

where: *`host`* is the server name (or domain name or IP address) and path of the folder that holds the ESSO-PR service root folder.

Command Line Options

Command-line options are available to support non-kiosk environments and allow ESSO-KM to run on a desktop machine without presenting a user interface.

```
/EVENT <EventName1> [EventName2…]
```

This option triggers the named event and ESSO-KM performs the tasks associated with the event and terminates. The authenticator filters are ignored.

```
/RUN <ListName1> [ListName2…]
```

This option triggers ESSO-KM to perform the tasks associated with the named list and terminate. The event and authenticator filters are ignored.

`ListName` can be either a Session State or an Action.

For example, "`SMAgent /run StartVisualSourceSafe`".

Note: Any `SessionAction` or `SessionState` names that have spaces in them must be enclosed in double quotes.

Some command-line options prevent others from working. For example, multiple lists can be run with the `/RUN` command. If `/LOCK` appears on the command line, the session is locked and the rest of the command line is ignored, including any options that appeared before `/LOCK`.

`/SHUTDOWN, /LOCK`, and `/TERM` are the command-line options that cause ESSO-KM to ignore the rest of the command line.

The `/RUN` and `/EVENT` commands trigger ESSO-KM to treat the rest of the command line as event and list names to be run. These will be run when all of the command line options have finished processing. The type of the parameter depends on the previous command. The command-line parameter type resets with the next `/EVENT` or `/RUN` parameter received. For example:

```
SMAgent /Event "SM session start" "SM session end" /RUN termlist1
termlist2 runlistA "My SessionState"
```

This command line will run the lists associated with events "`SM session start`" "`SM session end`" and run the named lists: `termlist1, termlist2, runlistA` and "`My SessionState`".

.NET API

Externally Callable Interfaces and Methods

A class named `KioskAPI` is available within the SMAgent.exe that is loaded by external programs.

The object is instantiated as follows:

```
Passlogix.SM.Manager.KioskAPI kiosk = new

Passlogix.SM.Manager.KioskAPI();
```

The following methods are available:

```
void Lock();

void Term();

void Shutdown();

void Event(string eventName);

void Run(string runtaskName);
```

- **Lock**. Locks the current ESSO-KM session.
- **Term**. Ends the user's session as if the ESSO-KM timer expired for a user.
- **Shutdown**. Terminates the SMAgent.exe.
- **Event**. Simulates the named event to occur causing ESSO-KM to perform tasks associated with the named event without filtering by the authenticator. Event names are the GUID strings from Events.xml.
- **Run**. Starts the named task without filtering by the event or authenticator. Task names are the `SessionAction` and `SessionState` names that are displayed by the ESSO-LM Administrative Console.

Note: Any `SessionAction` or `SessionState` names that have spaces in them must be enclosed in double quotes.

```
kiosk.Run("\"My SessionAction\"");
```

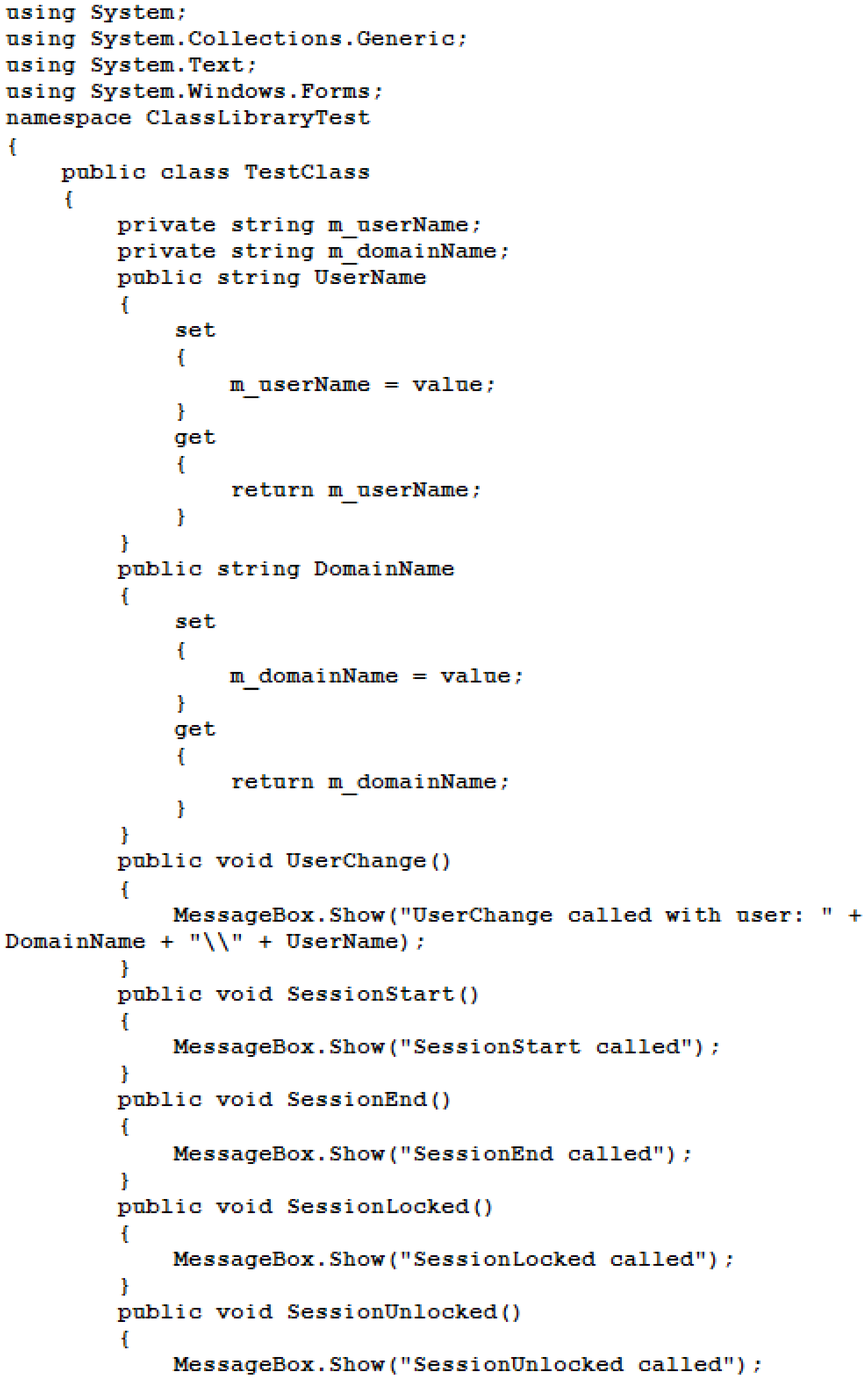
Example to run tasks associated with the "`SM Session End`" event:

```
Passlogix.SM.Manager.KioskAPI kiosk = new

Passlogix.SM.Manager.KioskAPI();
```

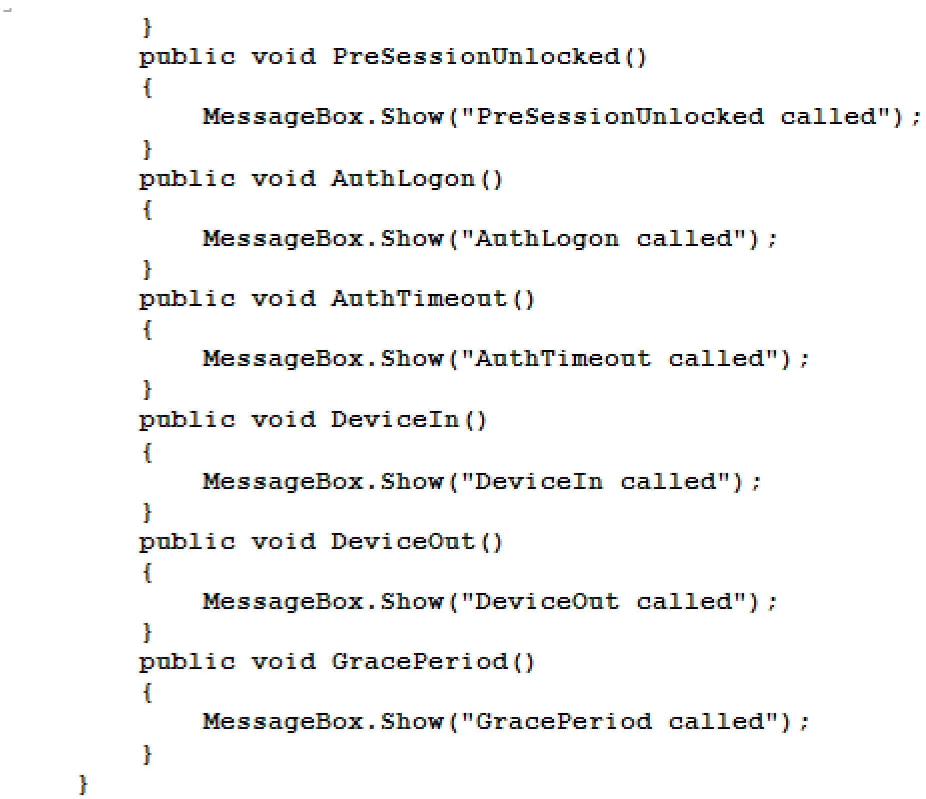
```
if (kiosk != null)

 kiosk.Event("{A644ED55-6A3F-4160-A355-C713C90733DF}");
```

Note: Refer to the .Net API Sample Code.

.Net API Sample Code



```
using System;
using System.Collections.Generic;
using System.Text;
using System.Windows.Forms;
namespace ClassLibraryTest
{
    public class TestClass
    {
        private string m_userName;
        private string m_domainName;
        public string UserName
        {
            set
            {
                m_userName = value;
            }
            get
            {
                return m_userName;
            }
        }
        public string DomainName
        {
            set
            {
                m_domainName = value;
            }
            get
            {
                return m_domainName;
            }
        }
        public void UserChange()
        {
            MessageBox.Show("UserChange called with user: " +
DomainName + "\\" + UserName);
        }
        public void SessionStart()
        {
            MessageBox.Show("SessionStart called");
        }
        public void SessionEnd()
        {
            MessageBox.Show("SessionEnd called");
        }
        public void SessionLocked()
        {
            MessageBox.Show("SessionLocked called");
        }
        public void SessionUnlocked()
        {
            MessageBox.Show("SessionUnlocked called");
```



```
        }
        public void PreSessionUnlocked()
        {
            MessageBox.Show("PreSessionUnlocked called");
        }
        public void AuthLogon()
        {
            MessageBox.Show("AuthLogon called");
        }
        public void AuthTimeout()
        {
            MessageBox.Show("AuthTimeout called");
        }
        public void DeviceIn()
        {
            MessageBox.Show("DeviceIn called");
        }
        public void DeviceOut()
        {
            MessageBox.Show("DeviceOut called");
        }
        public void GracePeriod()
        {
            MessageBox.Show("GracePeriod called");
        }
    }
```

Best Practices

These best practices are recommendations that will help you implement an optimal ESSO-KM configuration.

Deploying ESSO-KM Settings

The most convenient way to mass deploy ESSO-KM settings from the ESSO-LM Administrative Console is to create a customized MSI package and distribute it to end user kiosk machines using a deployment tool of your choice.

Note: Administrative Overrides are not available for use with ESSO-KM settings.

Sendkeys

Sendkeys is not a reliable method and therefore not guaranteed to work as expected. It is recommended that you do not use sendkeys.

Disable Task Manager and Run

The Windows Task Manager and Run menu option are disabled programmatically as a function of the ESSO-KM Registry Service. For added security, we recommend disabling these functions for any user account that is to be used as a ESSO-KM kiosk user account.

To remove the Run menu option from the Start menu:

1. Open Group Policy editor by double clicking on 'gpedit.msc' (C:\WINNT\system32\gpedit.msc)
2. Navigate to **User Configuration** > **Administrative Templates** > **Start Menu** and **Toolbar**.
3. In the right pane double-click **Remove Run from start menu**.
4. Select **Enabled** and click **Apply** and **OK**.

To disable Task Manager:

1. Open Group Policy editor by double clicking on 'gpedit.msc' (C:\WINNT\system32\gpedit.msc)
2. Navigate to **User Configuration** > **Administrative Templates** > **System** >**Ctrl+Alt+Delete Options**.
3. In the right pane double-click **Remove Task Manager**.
4. Select **Enabled** and click **Apply** and **OK**.