Oracle© Enterprise Single Sign-on Logon Manager

Global Agent Settings Reference Guide

Release 11.1.1.5.0

E21028-02

July 2011

Oracle Enterprise Single Sign-on Logon Manager Global Agent Settings Reference Guide, Release 11.1.1.5.0

E21028-02

Table of Contents

Abbreviations and Terminology

Following is a list of commonly used abbreviations and terminology.

Abbreviation or Term	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Agent or Logon Manager
ESSO-Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
ESSO-UAM	Oracle Enterprise Single Sign-on Universal Authentication Manager
FTU	First Time Use Wizard
LDAP	Lightweight Directory Access Protocol
Microsoft AD	Microsoft Active Directory
Microsoft ADAM	Microsoft Active Directory Application Mode

About this Guide

This guide is intended to be a comprehensive reference and companion to the ESSO-LM Administrative Console Global Agent Settings help topics. While some information is duplicated, this guide includes additional and complete information about each setting. It makes the information available to administrators planning an ESSO-LM configuration, without requiring the ESSO-LM Administrative Console to be running in order to refer to the settings.

The tables herein list each registry location, followed (where applicable) by:

- The Display Path (the node in the Console's left pane navigator) and Display Name (the setting in the right pane property sheet).
- The actual registry path and value name, and a description of the setting, defaults, and options (the actual value and its definition).
- Whether the setting is overridable (that is, can be included in an administrative override object or file).
- The Registry Type (DWORD, String, or Binary) and Data Type.

This guide includes an index for fast and easy reference to locate the settings that you want to configure. Several settings have been permanently configured according to the Best Practice documents and are no longer available for user configuration; others have been moved, renamed, or had their default values changed. The appendices at the end of the guide list nodes that have been modified, and settings that have been removed or whose default values have changed.

Settings are organized in this guide in the same order in which they appear in the ESSO-LM Administrative Console tree.

Audience

This guide is intended for experienced administrators responsible for the planning, implementation and deployment of ESSO-LM. Administrators are expected to understand single sign-on concepts, such as password policies, logon methods, credential sharing groups, and application configuration, as well as have familiarity configuring directory servers, databases and repositories. The person completing the installation and configuration procedure should also be familiar with the company's system standards. Readers should be able to perform routine security administration tasks.

User Experience Settings

Screen/Display Path:
User Experience/System tray icon

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Display icon in system tray `Shell:ShowTrayIcon`	Specifies whether to show the ESSO-LM icon in the system tray.	Yes	0-No 1-Yes (Default)	dword/Ø
Use server icon `Shell:TrayIconUseRemote`	Specifies whether to use the alternative server icon, as opposed to the standard system tray icon.	Yes	0-No (Default) 1-Yes	dword/Ø
Tooltip text `Shell:TrayIconName`	Specifies the text to display when the mouse hovers over the system tray icon. (Recommended use: Label each Citrix Server/Terminal Services/Remote server)	Yes	63 characters maximum (Default-Oracle Enterprise Single Sign-on Logon Manager)	string/Ø
Show system name `Shell:TrayIconDisplaySysName`	Specifies whether to append the computer name to the tooltip text, separated by a space-dash-space.	Yes	0-No (Default) 1-Yes	dword/Ø
Allow shutdown `Shell:AllowShutdown`	Specifies whether the “Shut Down” option is enabled on the system tray icon menu for the end user.	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path:
User Experience/Title bar button

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Show title bar button `Shell:ShowAccessBtn`	Specifies whether to show the ESSO-LM button on all window title bars. This button can be configured for single-click application recognition and response, or it can provide a menu similar to the system tray menu, by changing the “Provide Dropdown Menu” setting.	Yes	0-No (Default) 1-Yes	dword/Ø
Always show for `Shell:ShowTitleIconAlwaysForModuleN`	Identifies a list of applications (by executable filename, such as "notepad.exe") for which the title bar button should always be displayed.	Yes		string/Ø
Provide dropdown menu `Shell:ShowAccessBtnMenu`	Specifies whether to show the menu from the title bar button. If turned off, the title bar button acts as a single-click button for application recognition and response.	Yes	0-No (Default) 1-Yes	dword/Ø
Tooltip text `Shell:TitleIconName`	Specifies the text to display when the mouse hovers over the title bar button.	Yes		string/Ø

Screen/Display Path:
User Experience/Application Response

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Log on to waiting applications upon Agent startup `Shell:LogonOnStartup`	Enables the Agent, at startup, to submit credentials to a Windows or Java application that has already presented its logon form before the Agent was initialized and ready. **Note:** Web and host/mainframe application logons are not affected by this setting.	Yes	0-No (Default) 1-Yes	dword/Ø

SendKeys event interval
`Extensions\AccessManager:`
`SendkeysEventInterval`
	The minimum time to be elapsed between SendKeys key events. This is especially useful for eastern languages where keystrokes are sometimes lost.	Yes	0-Best speed (Default)
			60-Typical for eastern languages
			80-Use for slow system
			120-Use for very slow system
				dword/Ø

Respond to hidden and minimized windows `Shell:StrictWindowDetect`	Specifies whether the Agent will respond to hidden and minimized windows.	Yes	0-Yes (Default) 1-No	dword/Ø
Applications that hooks should ignore `Shell:HookIgnorePathsContain`	Specifies applications that are incompatible with hooks, and which ESSO-LM should ignore.	Yes		string/ string

Screen/Display Path:
User Experience/Application Response/Initial Credential Capture/User interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Credential capture mode `Shell:CaptureType`	Configure silent credential capture behavior by selecting a mode.	Yes	0-Do not capture silently 1-Capture, but do not inform user 2-Capture, and inform user with balloon tip (Default) 3-Capture, and present New Logon dialog box	dword/Ø
Enable Auto-Prompt `Shell:UseAutoSense`	Specifies whether to automatically prompt the user to add a logon when a new application is detected.	Yes	0-No 1-Yes (Default)	dword/Ø

Enable Auto-Enter
`Extensions\AccessManager:`
`LogonAfterConfig`
	Whether to log on to an application after configuring it (adding its credentials).	Yes	0-No
			1-Yes (Default)
				dword/Ø

Enable Auto-Recognize `Shell:UseActiveLogin`	Whether to automatically provide credentials to applications.	Yes	0-No 1-Yes (Default)	dword/Ø

Allow creating multiple accounts during credential capture
`Extensions\AccessManager:`
`ShowAddAdditionalLogon`
	Specifies whether to enable the checkbox in the New Logon dialog box that allows the user to add another set of credentials.	Yes	0-No (Default)
			1-Yes
				dword/Ø

Prohibit canceling the addition of new accounts
`Extensions\AccessManager:`
`EnableCancelButton`
	Specifies whether the user has the option to click the Cancel button or close the New Logon dialog box to defer entering credentials. This permits current access to an application and re-prompts the user to enter credentials at the next appropriate instance.	Yes	0-Yes
			1-No (Default)
				dword/Ø

Prohibit disabling the addition of new accounts
`Extensions\AccessManager\`
`EnableNeverButton`
	Specifies whether the Disable button is available in the New Logon dialog box, allowing the user to reject adding credentials for applications permanently. Disabling an application adds it to the Exclusions list in Agent settings.	Yes	0-Yes
			1-No (Default)
				dword/Ø

Prohibit excluding accounts from credential sharing groups
`Extensions\AccessManager:`
`DisableAllowExcludePWSG`
	Specifies whether to disable the checkbox in the New Logon dialog box that allows an account to be excluded from credential sharing groups. This checkbox will be available for the account properties dialog box.	Yes	0-No (Default)
			1-Yes
				dword/Ø

Screen/Display Path:
User Experience/Application Response/Initial Credential Capture/Limit response to predefined applications for…

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

All application types
`Extensions\AccessManager:`
`AllowUnknown`
	Sets the following options:
	1. Whether the Agent should auto respond to an application;
	2. Whether the user should be allowed to create logons for applications that the Administrator has not predefined.
	The 'Predefined applications only' setting prevents options 1 and 2. The 'Unlimited' setting allows options 1 and 2.
		Yes	0-Predefined applications only
			1-Unlimited (Default)
				dword/Ø

Windows applications
`Extensions\AccessManager:`
`AllowUnknownApp`
	This setting determines whether users are allowed to add credentials for Windows applications that are not predefined by the administrator.	Yes	0-Predefined applications only
			1-Unlimited (Default)
				dword/Ø

Web applications
`Extensions\AccessManager:`
`AllowUnknownWeb`
	Sets the following options:
	1. Whether the Agent should auto respond to a Web application;
	2. Whether the user should be allowed to create logons for applications that the Administrator has not predefined.
	The 'Predefined applications only' setting prevents options 1 and 2. The 'Unlimited' setting allows options 1 and 2. The 'Manually add undefined' setting prevents option 1 and allows option 2.
		Yes	0-Predefined applications only
			1-Unlimited (Default)
			2-Manually add undefined<
				dword/Ø

Allowed Web pages
`Extensions\AccessManager\`
`BHOAllowedWebPages:`
`WebPageN`
	Use this setting to list the Web pages allowed by the Agent. Click the "**…**" button to enter the regular expressions that match the URLs.
	Note: This feature is only used when the "All application types" or "Web applications" setting above is set to "Predefined applications only."
		Yes		string/Ø

Screen/Display Path:
User Experience/Application Response/Web Applications/Credential field identification

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Show border
`Extensions\AccessManager\`
`BHO:ShowBorder`
	Enable/disable the border around fields.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Border appearance
`Extensions\AccessManager\`
`BHO:FeedbackColor`
	Default border color/size/style for highlighting detected web page fields.	Yes	(Default-red 6px solid)	string/ string

Screen/Display Path:
User Experience/Application Response/Web Applications/Behavior

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
URL matching precision `Extensions\AccessManager: DNLevelsToMatch`	Number of levels of host portion of the URL used for application detection and response. For the URL http://mail.company.co.uk: ● 2=match to *.co.uk (Default) ● 3=match to *.company.co.uk ● 4=match to *.mail.company.co.uk **Note:** Values below 2 are treated as 2.	Yes	Minimum-2 (Default) Maximum-5	dword/int
Scroll into view `Extensions\AccessManager\ BHO:ScrollIntoView`	Enables/disables scrolling the browser window to bring the logon fields into view. This setting disables scrolling when the user has not yet stored credentials for a Web application. The Agent always scrolls when injecting credentials into the logon fields for an account that already exists.	Yes	0-No (Default) 1-Yes	dword/Ø
Activate tab `Extensions\AccessManager\ BHO:ActivateTab`	Enable/disable activating the tab that identifies the logon fields.	Yes	0-No 1-Yes (Default)	dword/Ø
Respond to IE modal dialogs `Extensions\AccessManager\ BHO:RespondToIEModalDialogs`	Enable this setting to have the Agent respond to a Web page that displays as a modal dialog or HTML application.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path:
User Experience/Application Response/Web Applications/Response control

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Applications to ignore
`Extensions\AccessManager:`
`BHOIgnoredApps`
	Comma-delimited list of applications (without path or extension) that the Browser Helper Object (BHO) should not attach to when searching for logons. Used when the BHO causes conflicts with certain applications.
	Example: ws_ftp, customapp1
		Yes		string/Ø

Web pages to ignore
`Extensions\AccessManager\`
`BHOIgnoredWebPages:`
`WebPageN`
	Use this setting to list the Web pages that the Agent should ignore. Used when the BHO causes conflicts with specific web applications or sites. Click the ellipsis (“**…**”) button to enter the regular expressions that match the URLs to be ignored (one per line).
	Examples:
	● .*http://login\.company\.com/.*
	● .*http://.*\.company\.com/.*
		Yes		string/Ø

Allowed dynamic Web pages
`Extensions\AccessManager\`
`BHOAllowedDynamicWebPages:`
`DynamicWebPageN`
	Use this setting to list the dynamic (DHTML) Web pages allowed by the Agent. By default, the BHO will not detect changes made to a dynamic page after the initial presentation of the page.
	Click the ellipsis (“**…**”) button to enter the regular expressions that match the URLs.
	Examples:
	● .*http://logon\.company\.com/.*
	● .*http://.*\.company\.com/.*
		Yes		string/Ø

Screen/Display Path:
User Experience/Application Response/Windows Applications

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Allow fallback from control IDs to SendKeys
`Extensions\AccessManager:`
`AllowSendKeysFallback`
	Allows fallback to SendKeys when direct injection of credentials using control IDs fails.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Screen/Display Path:
User Experience/Application Response/Java Applications/Exclusions

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Excluded Java versions `Extensions\AccessManager\JHO:JhoExcludeJavaVersionN`	Specify Java versions to exclude, listed as regular expressions. Enter one expression per line.	No		string/Ø
Excluded Java vendors `Extensions\AccessManager\JHO:JhoExcludeJavaVendorN`	Specify Java vendors to exclude, listed as regular expressions. Enter one expression per line.	No		string/Ø

Screen/Display Path:
User Experience/Application Response/Java Applications/Response delays

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Time allowed for Java applets to load `Extensions\AccessManager:MaxAppletLoadTime`	Maximum time (in seconds) that the Agent waits for a Java applet to be fully loaded in the browser.	Yes	(Default-6)	dword/int
Delay after Java runtime startup `Extensions\AccessManager:JHOAttachDelay`	Amount of time (in milliseconds) the JHO should wait before listening to window events at Java startup. Adding a delay can resolve timing conflicts during Java runtime initialization.	Yes	(Default-0)	dword/int
Delay between retries `Extensions\AccessManager:JhoRetryTimeout`	Amount of time (in milliseconds) the JHO should wait between retries of credential injection into a form control.	Yes	(Default-500)	dword/int

Screen/Display Path:
User Experience/Application Response/Java Applications/Retry behavior

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Maximum times to retry credential injection `Extensions\AccessManager:JhoRetryMaxAttempts`	Number of times to retry credential injection.	Yes	(Default-0)	dword/int

Screen/Display Path:
User Experience/Application Response/Java Applications/Java events to respond to

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Hierarchy events
`Extensions\AccessManager:`
`JhoHierarchyEventProcessing`
	Determines which Java hierarchy events are recognized. Set the flag using the following syntax:
	HIERARCHY_EVENT_CHANGED = 0x1
	This instructs the JHO to recognize all hierarchy events.
		Yes	(Default-0)	dword/int

Window events
`Extensions\AccessManager:`
`JhoWindowEventProcessing`
	Determines which Java window events are recognized.	Yes	A combination of the following values:
			WINDOW_EVENT_OPENED = 0x1
			WINDOW_EVENT_CLOSED = 0x2
			WINDOW_EVENT_ACTIVATED = 0x4
			WINDOW_EVENT_DEACTIVATED = 0x8
			WINDOW_EVENT_CLOSING = 0x10
			WINDOW_EVENT_ICONIFIED = 0x20
			WINDOW_EVENT_DEICONIFIED = 0x40
			(Default-255-All window events are recognized.)
			The recommended setting for new installations of ESSO-LM is 3.
				dword/int

Component events
`Extensions\AccessManager:`
`JhoComponentEventProcessing`
	Determines which Java component events are recognized.	Yes	A combination of the following values:
			COMPONENT_EVENT_SHOWN = 0x1
			COMPONENT_EVENT_HIDDEN = 0x2
			COMPONENT_EVENT_ADDED = 0x4
			COMPONENT_EVENT_REMOVED = 0x8
			(Default-15-All component events are recognized.)
			The recommended setting for new installations of ESSO-LM is 0xB (11).
				dword/int

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Injection type
`Extensions\AccessManager:`
`JhoInjectType`
	Determines the injection type used by the JHO to submit data to the controls.	Yes	One of the following values:
			INJECT_TYPE_DEFAULT = 0 (Default)
			The default causes the JHO to attempt injection using each of the following methods in the order shown until injection is successful:
			INJECT_TYPE_METHOD = 1
			(if an appropriate set method has been found for the control)
			INJECT_TYPE_ACCESSIBLE = 2
			(if the control supports accessibility)
			INJECT_TYPE_NONACCESSIBLE = 3
			INJECT_TYPE_ROBOT = 4
			Note: For combo and list boxes, the JHO always uses INJECT_ TYPE_METHOD.
				dword/int

Screen/Display Path:
User Experience/Application Response/Host/Mainframe Applications

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

16-bit screen capture attempts
`Extensions\AccessManager\`
`MHO\ConXP:`
`16BitTimeouts_ToFallback`
	Number of times to attempt the 16-bit screen capture. If an attempt is unsuccessful after the allotted number of tries, the Agent reverts to the 32-bit method.	Yes	(Default-5)	dword/int

Credential request delay interval
`Extensions\AccessManager\`
`MHO:NotNowDelay`
	Interval (in milliseconds) between prompts to create a logon for a mainframe session. When a user logs onto a mainframe session that matches a configured application for which there is no stored password,the Agent prompts the user: "Would you like ESSO-LM to remember your logon information for this application?" If the user selects "Not Now," the next time the user presses any key on the mainframe screen, the Agent prompts the user again. This delay setting is the amount of time the Agent should wait before displaying the question again.	Yes	(Default-60000)	dword/int

Polling interval
`Extensions\AccessManager\`
`MHO:CycleInterval`
	Interval (in milliseconds) between instances when the Agent checks the host emulator for changes. Lower values can use more CPU time, higher values can increase the time between when a screen appears and when the Agent provides credentials.	Yes	(Default-700)	dword/int

Screen/Display Path:
User Experience/Password Change/Password change behavior

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Default password policy `Extensions\AccessManager:DefaultPolicy`	Name of Password Generation Policy that application templates will use when no policy is defined in the application template. To define this setting, ensure that you currently have a defined/named policy loaded in the console, so the dropdown allows you to select the policy. **Note:** If no policy is defined here or in the template, a default policy of exactly eight alpha-only characters applies. For this reason, it is important to define a more appropriate policy.	Yes		string/Ø
Allow user to exclude accounts from credential sharing groups `Extensions\AccessManager:AllowExcludePWSG`	Allows end user to exclude application logons from an assigned credential sharing group.	Yes	0-No (Default) 1-Yes	dword/Ø
Change passwords automatically `Extensions\AccessManager:QuietGenerator`	Specifies the level of control given to the user in the password change process.	Yes	0-Yes, with user confirmation 1-Yes, without user confirmation 2-No (Default)	dword/Ø
Manual password change behavior `Extensions\AccessManager:CPWFlag`	Determines the behavior of the Password Change Wizard when a user encounters a password-change request.	Yes	1-Prompt (Default) 2-Manual, offer auto 4-Auto, offer manual 10-Manual only	dword/Ø
Pop-up dialog text after submission `Extensions\AccessManager:CPVerifyMessage`	To change the default text, select the checkbox and highlight the current text, then type in new text. To restore default text, unselect the checkbox.	Yes	(Default-After closing this message, verify that the application accepted the password. Select OK if it was accepted. If it was rejected, please try again.)	string/Ø

Screen/Display Path:
User Experience/Password Change/Allowed character sets

<table>
<tr><th>Display Name/
Registry Path</th><th>Description</th><th>Overridable</th><th>Options/
Default</th><th>RegType/
DataType</th></tr>
<tr><td><b>Lowercase characters</b>
Extensions\AccessManager:
LowerAlphaChars</td><td>List of characters allowed as "Lowercase Alphabet" characters in password policies.</td><td>Yes</td><td>Any lowercase characters
(Default-All lowercase characters)</td><td>string/Ø</td></tr>
<tr><td><b>Uppercase characters</b>
Extensions\AccessManager:
UpperAlphaChars</td><td>List of characters allowed as "Uppercase Alphabet" characters in password policies.</td><td>Yes</td><td>Any uppercase characters
(Default-All uppercase characters)</td><td>string/Ø</td></tr>
<tr><td><b>Numeric characters</b>
Extensions\AccessManager:
NumericChars</td><td>List characters allowed as "Numeric" characters in password policies.</td><td>Yes</td><td>Any numeric characters
(Default-All numeric characters)</td><td>string/Ø</td></tr>
<tr><td><b>Special characters</b>
Extensions\AccessManager:
SpecialChars</td><td>List of characters allowed as "Special" characters in password policies.</td><td>Yes</td><td>!@#$^&*()_-+=[]\|,?
(Default-!@#$^&*()_-+=[]\|,?)</td><td>string/Ø</td></tr>
</table>

Screen/Display Path:
User Experience/User Interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Language `[Root]:Language`	Language to be used. **Note:** Other values may be acceptable based on localized versions. The display font should support the desired characters in the specified language.	Yes	English (ENG) (Default) Brazilian Portuguese (PTB) Czech (CSY) Dutch (NLD) Finnish (FIN) French (FRA) German (DEU) Italian (ITA) Japanese (JPN) Korean (KOR) Polish (PLK) Simplified Chinese (CHS) Spanish (ESP)	string/Ø
Allow refresh in My Accounts `Extensions\AccessManager:AllowRefresh`	Enables/disables the SSO Manager Refresh button.	Yes	0-No 1-Yes (Default)	dword/Ø
Columns in "Details" view of My Accounts `Extensions\AccessManager\LogonManager:Columns`	Columns to display and order to use in Logon Manager in the "Details" view.	Yes	1-Application Name 2-URL/Module 3-Username/ID 4-Password 5-Modified 6-Last Used 7-Description 8-Reference 9-Group 10-Third Field 11-Fourth Field (Default-1,2,3,4,5,6,7,8,9)	string/Ø

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Columns in Logon Chooser `Extensions\AccessManager\LogonChooser:Columns`	Order of columns displayed in Logon Chooser.	Yes	1-Username/ID 2-Application Name 3-Description (Default-1,2,3)	string/Ø
Logon animation's duration Shell:AutoLogonAnimationTime	Time (in milliseconds) the animated spinner appears (pausing response). **Note:** A value of 0 disables the spinner.	Yes	(Default-0)	dword/int

Screen/Display Path:
User Experience/Setup Wizard

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Show first-time-use (FTU) wizard `Extensions\SetUpManager:HideWizard`	Controls whether the Setup Wizard displays when first-time-use is invoked. **Note:** If more than one authenticator (primary logon method) is installed, then the first authenticator in the list is automatically selected as the end user's primary logon method.	Yes	0-Yes (Default) 1-No	dword/Ø
Selected authenticator `AUI:FTUShowOnly`	Enables the selected logon method as the primary logon method and hides all other installed logon methods. **Note:** To hide the primary logon method selection menu, use the "Show First-Time-Use (FTU) Wizard" setting. If the primary logon method selection page is hidden, and this setting is blank, then the first installed logon method in the list is automatically selected.	Yes	None (Default-End-users select their own primary logon method) MSauth-Windows v2 WinAuth-Windows LDAPauth-LDAP v2 LDAP-LDAP SCauth-Smart Card ROSCAuth-Read-Only Smart Card ProxcardAuth-Proximity Card SecureIDAuth-RSA SecurID Entrust-Entrust MultiAuth-Authentication Manager UAMAuth-UAM	string/Ø
Skip selection page if only one authenticator is installed `AUI:HideSingleSelection`	Skip the step of selecting an authenticator in the Setup Wizard if only one authenticator is installed.	Yes	0-No (Default) 1-Yes	dword/Ø

Authentication Settings

Screen/Display Path:
Authentication\Authentication Manager

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Allowed number of authenticators `AUI\MultiAuth:MaxPreferred`	Allows you to set the maximum number of logon methods to present to a user. Once this number of logon methods have been presented (and skipped by) the user, a "Choose Logon" dialog is displayed. .	Yes	(Default-1)	dword/int

Screen/Display Path: Authentication\Authentication Manager\Enrollment

Use these settings for Multi-Authenticators only.

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Windows v2 AUI\MSauth:AuthState	This setting determines whether a user will be required to set up Windows v2 as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
Windows AUI\WinAuth:AuthState	This setting determines whether a user will be required to set up Windows as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
LDAP v2 AUI\LDAPauth:AuthState	This setting determines whether a user will be required to set up LDAP v2 as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
LDAP AUI\LDAP:AuthState	This setting determines whether a user will be required to set up LDAP as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
Smart card AUI\SCauth:AuthState	This setting determines whether a user will be required to set up Smart card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
Read-only smart card AUI\ROSCauth:AuthState	This setting determines whether a user will be required to set up Read-only smart card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Proximity card `AUI\ProxCardAuth:AuthState`	This setting determines whether a user will be required to set up Proximity card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
RSA SecurID `AUI\SecureIDAuth:AuthState`	This setting determines whether a user will be required to set up RSA SecurID as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø
Entrust `AUI\Entrust:AuthState`	This setting determines whether a user will be required to set up Entrust as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	Yes	0-Disabled 1-Optional (Default) 2-Required 3-Incremental	dword/Ø

Screen/Display Path:
Authentication\Authentication Manager\Grade

Use these settings for Multi-Authenticators only.

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Windows v2 `AUI\MSauth:AuthGrade`	This setting assigns an authentication grade to Windows v2. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
Windows `AUI\WinAuth:AuthGrade`	This setting assigns an authentication grade to Windows. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
LDAP v2 `AUI\LDAPauth:AuthGrade`	This setting assigns an authentication grade to LDAP v2. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
LDAP `AUI\LDAP:AuthGrade`	This setting assigns an authentication grade to LDAP. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
Smart card `AUI\SCauth:AuthGrade`	This setting assigns an authentication grade to Smart card. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
Read-only smart card `AUI\ROSCauth:AuthGrade`	This setting assigns an authentication grade to Read-only smart card. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
Proximity card `AUI\ProxCardAuth:AuthGrade`	This setting assigns an authentication grade to Proximity card. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
RSA SecurID `AUI\SecureIDAuth:AuthGrade`	This setting assigns an authentication grade to RSA SecurID. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø
Entrust `AUI\Entrust:AuthGrade`	This setting assigns an authentication grade to Entrust. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/Ø

Screen/Display Path: Authentication\Authentication Manager\Order

Use these settings for Multi-Authenticators only.

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Windows v2 `AUI\MSauth:AuthOrder`	This setting sets the ordered position for Windows v2. This will be the order that Windows v2 will be presented to the end user during reauthentication scenarios.	Yes	(Default-2)	dword/int
Windows `AUI\WinAuth:AuthOrder`	This setting sets the ordered position for Windows. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-2)	dword/int
LDAP v2 `AUI\LDAPauth:AuthOrder`	This setting sets the ordered position for LDAP v2. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-3)	dword/int
LDAP `AUI\LDAP:AuthOrder`	This setting sets the ordered position for LDAP. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-3)	dword/int
Smart card `AUI\SCauth:AuthOrder`	This setting sets the ordered position for Smart card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-1)	dword/int
Read-only smart card `AUI\ROSCauth:AuthOrder`	This setting sets the ordered position for Read-only smart card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-1)	dword/int
Proximity card `AUI\ProxCardAuth:AuthOrder`	This setting sets the ordered position for Proximity card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-6)	dword/int
RSA SecurID `AUI\SecureIDAuth:AuthOrder`	This setting sets the ordered position for RSA SecurID. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-6)	dword/int
Entrust `AUI\Entrust:AuthOrder`	This setting sets the ordered position for Entrust. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	Yes	(Default-4)	dword/int

Screen/Display Path: Authentication\Windows v2\Recovery

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Recovery method `AUI\MSauth\ResetMethods:ResetMethodGUID`	Specifies the reset method to use when the user's password changes. **Note:** Windows Authenticator version 2 is the preferred authenticator for ESSO-LM and is installed by default. For more information about this authenticator, refer to the Best Practice guide in the *ESSO-LM online documentation center*.	Yes	4ED42DB8-B8F1-4AE6-B13A-272F74B48FE7-User passphrase (Default) B623C4E7-A383-4194-A719-7B17D074A70F-Passphrase suppression using user's SID 7B4235FF-5098-435c-9A05-052426D96AA8-Passphrase suppression using secure key	string/Ø
Use Windows Data Protection (DPAPI) `AUI\MSauth:UseDPAPI`	Set to Yes to use a DPAPI key to protect the Kiosk Manager encryption key, instead of the normal two-key system of User Password and Recovery Key. **Note:** Consult Microsoft and Oracle DPAPI best practices to ensure your Active Directory and desktop infrastructure is capable and configured to use DPAPI.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Authentication\Windows v2\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Window title `AUI\MSauth:WindowTitle`	Use this setting to customize the window title for this authenticator. **Note:** This entry is not required.	Yes		string/string
Window subtitle `AUI\MSauth:WindowSubTitle`	Use this setting to customize the window subtitle for this authenticator. **Note:** This entry is not required.	Yes		string/string
Custom image for authentication prompt `AUI\MSauth:ImagePath`	Fully-qualified path and filename of the image file.	No		string/filename
Reauthentication dialog `AUI\MSauth:AuthOptions`	Select which method to use when ESSO-LM requires the end-user to re-authenticate. **Note:** While the setting is called "Use GINA," it also applies to the Credential Provider mechanism in operating systems newer than Windows XP and Windows 2000.	Yes	0-Use SSO dialog (Default) 1-Use GINA	dword/Ø

Screen/Display Path: Authentication\Windows v2\Credential sharing

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Include in Domain credential sharing group AUI\MSauth:PWSEnable	Enables credential sharing from the authenticator to credentials in a special credential sharing group called “Domain.” Whenever a new password is detected by the authenticator, the new password is automatically shared to the Domain credential sharing group.	Yes	0-No 1-Yes (Default)	dword/Ø
Share credentials with other authenticators AUI\MSauth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example “WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
Share credentials with synchronizers AUI\MSauth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string

Screen/Display Path: Authentication\Windows v2\Passphrase\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Message AUI\MSauth\Reset: PassphraseMessage	Use this setting to display a user agreement-style dialog where the user must check a checkbox to continue. This is typically used to suggest the importance of the passphrase that users enter. **Note:** This message may contain multiple lines to a maximum of 180 characters. The character sequence "\n" will be replaced with carriage return and newline characters. If this setting is not set, the dialog is skipped.	Yes		string/string
Message dialog title AUI\MSauth\Reset: PassphraseDialogTitle	Use this setting to customize the user agreement style dialog title.	Yes		string/string
Checkbox label AUI\MSauth\Reset: PassphraseChkboxMsg	Use this setting to customize the user agreement style dialog checkbox. **Note:** Users must check this box before the dialog can be dismissed. The OK button is disabled until they check this box.	Yes		string/string

Screen/Display Path: Authentication\Windows v2\Passphrase\Options

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Minimum length `AUI\MSauth\Reset: MinPassphraseLength`	Default required length of a passphrase. You can override this setting by specifying the required length for a specific question.	Yes		dword/int
User can change passphrase `AUI\MSauth: ShowChangeAnswerOption`	Toggles availability of the user's option to change the answer to the verification question.	Yes	0-No 1-Yes (Default)	dword/Ø
Reset with old password `AUI\MSauth:ResetWOP`	Allows the previous password to be used in the passphrase process.	Yes	0-No (Default) 1-Yes	dword/Ø
Force password re-enrollment when using old password to reset `AUI\MSauth:RWOPSkipReset`	Specifies whether the user can skip the ESSO-LM passphrase prompt. Enabling this feature ensures that after a user enters his previous Windows password, ESSO-LM will prompt him to enter a new passphrase. **Warning:** Disabling this feature runs the risk of a complete lockout of ESSO-LM. This can happen if a user no longer remembers his passphrase, and subsequently forgets his Windows password.	Yes	0-Yes (Default) 1-No	dword/Ø

Screen/Display Path: Authentication\Windows\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Window title `AUI\WinAuth: WindowTitle`	Use this setting to customize the Window title for this authenticator. **Note:** This entry is not required.	Yes		string/string
Window subtitle `AUI\WinAuth: WindowSubTitle`	Use this setting to customize the Window subtitle for this authenticator. **Note:** This entry is not required.	Yes		string/string
Custom image for authentication prompt `AUI\WinAuth:ImagePath`	Fully-qualified path and filename of the image file.	No		string/filename
Require old password when Windows password changes `AUI\WinAuth:PWEnable`	Provide enhanced security by requiring entry of the old password when a new one is in use.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Authentication\Windows\Credential sharing

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Share credentials with other authenticators `AUI\WinAuth: ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\ Software\ Oracle\ AUI.	Yes		string/string
Share credentials with synchronizers `AUI\WinAuth: ShareCredsToSyncs`	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string

Screen/Display Path: Authentication\LDAP v2\Connection information

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Servers `AUI\LDAPauth\ Servers:ServerN`	Servers to try, in the format "computer[:port]" (one server per line), where computer is the server name or IP, and port is assumed to be default (636 for SSL, 389 for no SSL) if not specified. **Examples:** ● 127.0.0.1 ● 127.0.0.1:456 ● somewhereelse.com:8080 ● anotherplace.com **Note:** You musty specify at least one server for this extension to work.	No		string/Ø
User paths `AUI\LDAPauth: UserPathN`	Fully-qualified path to where the user account is located. There can be unlimited paths to search. The extension searches these in order, looking for the user account. If not found, the extension will search the directory tree. **Note:** You must specify a value for either UserPrepend or at least one value for UserPath for this extension to work. If using UserPaths, do not use UserLocation.	Yes		string/Ø
Use SSL `AUI\LDAPauth:UseSSL`	Specify whether to connect via SSL.	Yes	0-No (insecure) (default to port #389) (Default) 1-Yes (default to port #636)	dword/Ø

Screen/Display Path: Authentication\LDAP v2\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Share credentials with other authenticators `AUI\LDAPauth: ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
Share credentials with synchronizers `AUI\LDAPauth: ShareCredsToSyncs`	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string
Include in LDAP credential sharing group `AUI\LDAPauth:PWSEnable`	Enables credential sharing from the authenticator to credentials in the Group Domain. (Also requires AccessManager:PWSEnable to be enabled.)	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path: Authentication\LDAP v2\Credential sharing

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Share credentials with other authenticators `AUI\LDAPauth: ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
Share credentials with synchronizers `AUI\LDAPauth: ShareCredsToSyncs`	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string
Include in LDAP credential sharing group `AUI\LDAPauth:PWSEnable`	Enables credential sharing from the authenticator to credentials in the Group Domain. (Also requires AccessManager:PWSEnable to be enabled.)	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path:
Authentication\LDAP v2\Special Purpose

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Naming attribute string `AUI\LDAPauth: UserPrepend`	String to prepend to UserPaths when the DN for a user is in the form of: ● cn=%UserName%,ou=people,dc=computer ● instead of the form: ● namingattribute= %UserName%, ou=people, dc=computer (where namingattribute can be any string). **Note:** Usually, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.	Yes		string/string
BIND timeout `AUI\LDAPauth:Timeout`	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
Alternate user ID location `AUI\LDAPauth: UserLocation`	Use to indicate where to locate a user object when the user validates against an attribute other than the username. **Example:** If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in: ● ou=people,dc=computer ● then set UserLocation to: ● empid=%user,ou=people,dc=computer instead of to: ● uid=user,ou=people,dc=computer. **Note:** For Novell eDirectory, UserLocation should be: ● uid=%user,path to the object. If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string

Screen/Display Path: Authentication\LDAP\Connection information

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Naming attribute string `AUI\LDAPauth: UserPrepend`	String to prepend to UserPaths when the DN for a user is in the form of: ● cn=%UserName%,ou=people,dc=computer instead of the form: ● namingattribute= %UserName%, ou=people, dc=computer (where namingattribute can be any string). **Note:** Usually, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.	Yes		string/string
BIND timeout `AUI\LDAPauth: Timeout`	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
Alternate user ID location `AUI\LDAPauth: UserLocation`	Use to indicate where to locate a user object when the user validates against an attribute other than the username. **Example:** If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in: ● ou=people,dc=computer ● then set UserLocation to: ● empid=%user,ou=people,dc=computer instead of to: ● uid=user,ou=people,dc=computer. **Note:** For Novell eDirectory, UserLocation should be: ● uid=%user,path to the object. If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string

Screen/Display Path: Authentication\LDAP\Active directory

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Enable Domain name support `AUI\LDAPauth:UsingAD`	Enables Active Directory Domain name support. End users can specify the Domain name (for example, domainname\ username) at primary logon. Alternatively, the administrator can specify a default Domain name (see the "Active Directory: Set Domain name" setting) to let end users log on by username alone. If you don't specify a Domain, ESSO-LM uses the local workstation's Domain.	Yes	0-No (Default) 1-Yes	dword/Ø
Default Domain name `AUI\LDAP:ADDomain`	The Active Directory Domain name to use for primary logon if you don't specify a Domain for the username/ID credential (for example, domainname\username). Use this setting only if you set the "Active Directory: Domain name support enabled" setting to "Use AD Domain names." If you enable Domain name support and this setting is blank (and the end user does not specify a Domain), then ESSO-LM uses the local workstation's Domain.	Yes		string/string

Screen/Display Path: Authentication\LDAP\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Window title `AUI\LDAP:WindowTitle`	Use this setting to customize the Window title name for this authenticator. **Note:** This entry is not required.	Yes		string/string

Password change window title
`AUI\LDAPauth:`
`CAP_WindowTitle`
	Use this setting to customize the Active Directory Change Password Window title name for this synchronizer.
	Note: This entry is not required.
		Yes		sting/string

Password change window subtitle
`AUI\LDAPauth:`
`CAP_WindowSubTitle`
	Use this setting to customize the Active Directory Change Password Window subtitle name for this synchronizer.
	Note: This entry is not required.
		Yes		string/string

Custom image for authentication prompt `AUI\LDAP:ImagePath`	Fully-qualified path and filename of the image file.	No		string/filename
Show user path `AUI\LDAP:ShowUserPath`	Use this setting to show/hide User Path combo box control in the LDAP authentication dialog.	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path: Authentication\LDAP\Credential sharing

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Share credentials with other authenticators `AUI\LDAP: ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example “WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
Share credentials with synchronizers `AUI\LDAP: ShareCredsToSyncs`	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\ Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string

Screen/Display Path:
Authentication\LDAP\Special Purpose

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Naming attribute string `AUI\LDAP:UserPrepend`	String to prepend to UserPaths when the DN for a user is in the form of: ● cn=%UserName%,ou=people,dc=computer ● instead of the form: ● namingattribute=%UserName%, ou=people,dc=computer (where namingattribute can be any string). **Note:** Usually, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.	Yes		string/string
BIND timeout `AUI\LDAP:Timeout`	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
Alternate user ID location `AUI\LDAP:UserLocation`	Use to indicate where to locate a user object when the user validates against an attribute other than the username. **Example:** If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in: ● ou=people,dc=computer ● then set UserLocation to: ● empid=%user,ou=people,dc=computer instead of to: ● uid=user,ou=people,dc=computer. **Note:** For Novell eDirectory, UserLocation should be: ● uid=%user,path to the object. If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string
Enable directory search for users `AUI\LDAP:LDAPBindSearch`	Enables or disables directory search for the user account. When the user account is not found in the given path, the authenticator will search for it from that location down the directory tree. The search is performed whether using "User Paths" or the "Alternate User ID location."	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Authentication\Smart Card\Options

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Smart card library `AUI\SCauth: SmartCardAPI`	Configures whether to use the Cryptographic Service Provider (CSP) or the PKCS #11 library to perform cryptographic operations on the smart card. **Note:** Set this to PKCS # 11 only if using SafeSign/ RaakSign middleware.	Yes	0-CSP (Default) 1-PKCS#11	dword/Ø
Use default certificate for authentication `AUI\SCauth: UseCertOnCard`	Configures whether to use the default logon certificate (provided by the administrator) on the card for authentication. If not enabled (the default), the public/private keys in the SSO container on the card will be used (and created if necessary).	Yes	0-No (Default) 1-Yes	dword/Ø
Store synchronization credentials `AUI\SCauth: StoreSyncCreds`	This setting configures whether to store the user's synchronization repository credentials on the smart card.	Yes	0-No (Default) 1-Yes	dword/Ø
Store the PIN `AUI\SCauth: AuthOptions`	Whether to store the Smart Card PIN (and thus the Agent may prompt for the PIN), or to let the Smart Card drivers deal with requesting the PIN.	Yes	0-No (Default) 1-Yes	dword/Ø
PKCS#11 Library Path `AUI\SCAuth:PKCS11Path`	Use this setting to configure the path to the smart card middleware file, which implements the PKCS#11 standard. **Note:** This entry is not required unless "Smart card library" is set to PKCS #11, "Store synchronization credentials" is set to Yes, or smart cards are being used with Kiosk Manager.	Yes		string/string
Custom certificate check extension path `AUI\SCAuth:CCCEPath`	Use this setting to specify the path to the custom certificate check extension. There is no default for this setting. **Note:** This entry is not required.	Yes		string/string
Allow secure PIN entry `AUI\SCAuth:AllowSPE`	Use this setting to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry.	Yes	0-Only allow non-SPE login (Default) 1-Only allow SPE login	dword/Ø

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Lock desktop on smart card removal `AUI\SCauth:LockDesktopOnRemoval`	Specifies whether to lock the desktop when the smart card owner removes the smart card from the reader. By default, this value is set to **No**. If the value is set to **Yes**, the user's workstation locks when the smart card is removed. If the user locks the desktop using Ctrl+Alt-Delete, the authentication status remains unchanged.	Yes	0-No (Default) 1-Yes	dword/Ø

Allow forced verification
`AUI\SCauth:`
`AllowForcedVerification`
	Specifies whether ESSO-LM should automatically authenticate users after they authenticate to Windows with a smart card.
	Setting this to **No** (the default) requires a user to enter a PIN for both Windows logon and to authenticate to ESSO-LM. Setting this to **Yes** eliminates the double PIN prompt and the user needs to enter a PIN only to authenticate to Windows, while ESSO-LM automatically authenticates the user.
	Note: To use this feature, Network Provider MUST be installed with ESSO-LM. This is available during the installation on the Advanced Setup panel under Authenticators. Refer to the *ESSO-LM Installation and Setup Guide* for more information.
		Yes	0-No (Default)
			1-Yes
				dword/Ø

Screen/Display Path: Authentication\Smart Card\User interface

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Window title `AUI\SCauth:WindowTitle`	Use this setting to customize the Window title name for this authenticator.	Yes		string/string

Window subtitle
`AUI\SCauth:`
`WindowSubTitle`
	Use this setting to customize the Window subtitle name for this authenticator.	Yes		string/string

Screen/Display Path: Authentication\Smart Card\Recovery

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Recovery method `AUI\SCauth:ResetEnable`	Specifies the supplier of the reset passphrase to be used: the user (entering the passphrase in a dialog box), the newest non-default encryption certificate on the card itself, or the smart card PIN.	Yes	1-Passphrase (Default) 2-Encryption certificate 3-Smart card PIN	dword/Ø
Recovery certificate object identifier `AUI\SCAuth:ResetCertOID`	Configures the object identifier used to identify the certificate to use for the certificate-based passphrase feature. The authenticator searches the "Enhanced Key Attributes" of each certificate on the smart card for this Object Identifier. **Note:** You must set the "Recovery method" option to "Encryption certificate." This entry is not required.	Yes		string/string

PIN recovery group
`AUI\SCauth:`
`PINRecoveryDomainGroupName`
	Enter the domain security group name (in format domain\group) for the PIN Recovery Group. Members of this group will be allowed to authenticate to ESSO-LM without a smart card, and using only a PIN.
	This setting is useful in a scenario where users lose their cards and are waiting for new ones. While the cards are being replaced, users can be added to this PIN recovery group so that they can authenticate to ESSO-LM without their cards. To use this feature, the Recovery method setting above MUST be set to Smart card PIN.
	Note: You cannot use a PIN recovery group in conjunction with secure PIN entry.
		Yes		string/string

Screen/Display Path: Authentication\Read-Only Smart Card\Options

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Store synchronization credentials AUI\ROSCauth: StoreSyncCreds	Configures whether to store the user's synchronization repository credentials using Secure Data Storage. **Note:** You must enable and configure Secure Data Storage.	Yes	0-No (Default) 1-Yes	dword/Ø
PKCS#11 Library Path AUI\ROSCAuth: PKCS11Path	Use this setting to configure the path to the smart card middleware file, which implements the PKCS#11 standard. **Note:** This entry is not required unless "Store synchronization credentials" is set to Yes or read-only smart cards are being used with Kiosk Manager.	Yes		string/string
Custom certificate check extension path AUI\ROSCauth:CCCEPath	Use this setting to specify the path to the custom certificate check extension. There is no default for this setting. **Note:** This entry is not required.	Yes		string/string
Allow secure PIN entry AUI\ROSCauth:AllowSPE	Use this setting to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry.	Yes	0-Only allow non-SPE login (Default) 1-Only allow SPE login	dword/Ø

Screen/Display Path: Authentication\Read-Only Smart Card\Recovery

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Recovery method AUI\ROSCauth: ResetEnable	Enables the use of the reset passphrase. The passphrase can be supplied either by the user (entering the passphrase in a dialog box) or by the newest non-default encryption certificate on the card itself.	Yes	1-Passphrase (Default) 2-Encryption certificate	dword/Ø
Recovery certificate object identifier AUI\ROSCAuth: ResetCertOID	Configures the object identifier used to identify the certificate to use for the certificate-based passphrase feature. The authenticator searches the "Enhanced Key Attributes" of each certificate on the smart card for this Object Identifier. **Note:** You must set the "Recovery method" option to "Encryption certificate." This entry is not required.	Yes		string/string

Screen/Display Path: Authentication\Proximity Card\Options

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Card family `AUI\ProxCardAuth: ProximityCardFamily`	Configures the proximity card family type.	Yes	0-HID ISO / DUO PROX (Default) 1-iClass 2-Indala / EM	dword/Ø
Reader type `AUI\ProxCardAuth: ReaderName`	Configures the name of the proximity card reader to use.	Yes	OMNIKEY CardMan 5x25-CL 0-Omnikey CardMan 5125 OMNIKEY CardMan 5x21-CL 0-Omnikey CardMan 5121 OMNIKEY CardMan 5x21-CL 0-Omnikey CardMan 5321 No entry-RFIdeas (all readers) (Default)	string/Ø
Second factor authentication `AUI\ProxCardAuth: AuthenticationMethod`	Configures whether to use the Active Directory password or a user-defined PIN for the second factor in authentication.	Yes	0-AD password (Default) 1-User-defined PIN	dword/Ø

Screen/Display Path: Authentication\Proximity Card\PIN settings

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Minimum length `AUI\ProxCardAuth: MinPINLength`	Configures the minimum length of the user-defined PIN.	Yes		dword/int
Maximum length `AUI\ProxCardAuth: MaxPINLength`	Configures the maximum length of the user-defined PIN.	Yes		dword/int
Maximum retries `AUI\ProxCardAuth: RetryPINCount`	Configures the number of PIN attempts before the authentication fails.	Yes		dword/int
Alphanumeric constraints `AUI\ProxCardAuth: AlphabeticRequirements`	Configures the alphanumeric requirements of the user defined PIN.	Yes	1-Numbers only 2-Letters only 3-Numbers and letters (Default)	dword/Ø

Screen/Display Path:
Authentication\Secure Data Storage

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
Enable data storage `DataStorage:Passlogix SecureDataStorage`	Configures whether to store users' synchronization credentials securely within the repository.	Yes	0-No (Default) 1-Yes	dword/Ø
Data storage location `SecureDataStorage: LocationDN`	Fully-qualified path to the location in the repository where the data will be stored.	Yes		string/string

Synchronization Settings

Screen/Display Path:
Synchronization/Options

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Synchronizer order
`Extensions\SyncManager:`
`SyncOrder`
	Sets the order of synchronization extensions to use. If no value is specified, all extensions are used (in an unpredictable order). For reads, the first operational synchronizer is authoritative, and no other synchronizer is queried. For writes, all synchronizers are updated, in the order specified in this setting.
	Examples: LDAPExt,ADExt FileSync Remote,AD,FileSync Local,SmartCard MySmartCard,ADExt,ADExtRemote
		Yes		string/ synchronizers

Use configuration objects
`Extensions\SyncManager:`
`RetrieveCO`
	When turned off, all templates and policies are consolidated into one of two objects: CN=vgoentlist and CN=vgoadminoverride.
	When turned on, all template and policies are independent objects for directory-based synchronizers. In this mode, additional features are available, including role/group security and directory hierarchy support.
		Yes	0-No (Default)
			1-Yes
				dword/Ø

Allow disconnected operation
`Extensions\SyncManager:`
`AllowDisconnected`
	Specifies whether the offline cache is usable or whether the First-Time-Use setup wizard executes when the Agent is unable to connect to any synchronizer repository. If set to No, and the repository is not available, the Agent shuts down.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Delete local cache `Shell:CleanupOnShutdown`	Specifies whether to delete the user's data files and registry keys upon shutdown of the Agent.	Yes	0-No (Default) 1-Yes	dword/Ø
Deleted credential cleanup `Shell:nDelDays`	Length of time (in days) for which a credential's "deleted" flag is retained, after a credential is deleted. Used to ensure that the credential is deleted from all of a user’s local caches on multiple systems. (Default is 30 days)	Yes	(Default-30)	dword/int

Location of entlist.ini file
`Extensions\AccessManager:`
`EntList`
	Fully-qualified path and filename to the entlist.ini file. Only applicable in standalone (no synchronizer) mode.
	This setting should be used only to deploy ESSO-LM Administrative Console templates locally to the workstation when synchronization is not installed.
	The setting should NOT be used when synchronization is installed and application templates are deployed via a repository such as Active Directory. Refer to the ESSO-LM Administrative Console online help topic, "Configuring Application Templates," for more information."
		Yes		string/filename

Screen/Display Path: Synchronization/Behavior

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Wait for synchronization at startup `Extensions\SyncManager:WaitForStartupSync`	Specifies whether to wait for synchronization at startup, which ensures that the user's data is current, and new templates and policies are put into effect before ESSO-LM logs on to applications. **Note:** When set, ESSO-LM does not respond until the synchronization is complete; synchronization times vary based on your synchronization infrastructure and the number of templates and policies in the repository.	Yes	0-No 1-Yes (Default)	dword/Ø
Interval for automatic resynchronization `Extensions\SyncManager:CycleInterval`	Interval (in minutes) between automatic resynchronizations. This synchronization interval is not reset if a manual, user-generated sync event (such as an ESSO-LM refresh) takes place. A value of zero (0) disables this setting, which means that synchronization occurs only during normal sync events such as ESSO-LM startup or user credential update. Generally set when ESSO-PG is in use, to ensure that updates are delivered in a timely manner.	Yes	(Default-0)	dword/int
Optimize synchronization `Extensions\SyncManager:OptimizedSync`	When enabled, the synchronization function uses a checksum object called SyncState to determine changed credentials, rather than retrieving all credentials. Changed credentials are then independently synchronized without synchronizing all credentials. Note that templates and policies are always synchronized in full during each sync event.	Yes	0-No 1-Yes (Default)	dword/Ø
Use aggressive synchronization `Extensions\SyncManager:AggressiveSync`	When turned on, each time ESSO-LM detects a logon event, a synchronization occurs before the target application credential is decrypted and passed to the application. This feature ensures that the most current credentials or settings are used at all times. The feature is normally only used in special cases where a user uses multiple systems to simultaneously access the same application (such as through a Citrix farm). **Note:** This feature can have a significant performance impact on both client and server computers.	Yes	0-No (Default) 1-Yes	dword/Ø
Resynchronize when network or connection status changes `Shell:MonitorNetwork`	Enables/disables monitoring for changes in the network connection status. Enabling this setting causes the Agent to perform resynchronization when a status change occurs (for example, reconnecting to the network).	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\%ADAM%

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
ADAM Sync DLL location `Extensions\SyncManager\Syncs\%ADAM%:Path`	Path\filename of the Active Directory synchronizer extension.	No	(Default-%INSTALLDIR%Plugin\ SyncMgr\ ADAMext\ ADAMsyncExt.dll)	string/filename

Screen/Display Path: Synchronization\%ADAM%/Data storage configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Base location(s) for configuration objects `Extensions\SyncManager\Syncs\%ADAM%\COBaseLocations:LocationN`	Where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as: ● OU=SSOConfig,DC=Domain,DC=com The search starts from the specified location(s) and searches all subordinate OUs (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.	No		string/Ø
Prepend Domain when naming objects `Extensions\SyncManager\Syncs\%ADAM%:AppendDomain`	Enables prepending of the user's Domain to the username in naming the user's container. **Example:** For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled.	Yes	0-No (Default) 1-Yes	dword/Ø
User Domain name to use `Extensions\SyncManager\Syncs\%ADAM%:UserDomain`	Domain name to use in the container name (for example, DomainName.UserName) when you enable the Prepend Domain setting. The user can specify another domain the in the logon dialog. **Example:** If User Domain is "MyDomain" (with Prepend Domain enabled) and the user logs on as jamesk, the container name used is MYDOMAIN.jamesk. If the user logs on as HISDOMAIN\jamesk the container name used is HISDOMAIN.jamesk.	Yes		string/string

Screen/Display Path: Synchronization\%ADAM%/Connection information

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Credentials to use `Extensions\SyncManager\Syncs\%ADAM%:AuthType`	Specifies which credentials to use when authenticating to the ADAM server.	Yes	0-Local computer credentials 1-ADAM server account 2-Try local computer credentials before using ADAM server account (Default)	dword/Ø
Prompt when disconnected `Extensions\SyncManager\Syncs\%ADAM%:AllowOffline`	Allows the user to work offline without prompting/notification if a synchronization event fails.	Yes	0-Yes 1-No (Default)	dword/Ø
Servers `Extensions\SyncManager\Syncs\%ADAM%\Servers:ServerN`	Servers to try, in the format "computer[:port]" (one server per line), where “computer” is the server name, and “port” is assumed to be the default (636 for SSL, 389 for no SSL) if not specified. **Examples:** ● Adam1.company.com ● Adam2.company.com ● Adam3.company.com:50389	No		string/string
Use SSL `Extensions\SyncManager\Syncs\%ADAM%:UseSSL`	Specify to connect via SSL.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\%ADAM%/User interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Descriptive name `Extensions\SyncManager\Syncs\%ADAM%:DisplayName`	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name.	Yes		string/string
Password change window title `Extensions\SyncManager\Syncs\%ADAM%:CAP_WindowTitle`	Use this setting to customize the ADAM Change Password Window title name for this synchronizer.	Yes		string/string
Password change window subtitle `Extensions\SyncManager\Syncs\%ADAM%:CAP_WindowSubTitle`	Use this setting to customize the ADAM Change Password Window subtitle name for this synchronizer.	Yes		string/string

Screen/Display Path: Synchronization\%ADAM%/Credential sharing

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Share credentials with authenticators `Extensions\SyncManager\Syncs\%ADAM%:ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example “WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string

Screen/Display Path: Synchronization\%AD%

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
AD Sync DLL location `Extensions\SyncManager\Syncs\%AD%:Path`	Path\filename of the Active Directory synchronizer extension.	No	(Default-%INSTALLDIR%Plugin\ SyncMgr\ ADEXT\ adsync.dll)	string/filename

Screen/Display Path: Synchronization\%AD%/Data storage configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Base location(s) for configuration objects `Extensions\SyncManager\Syncs\%AD%\COBaseLocations:LocationN`	Where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as: ● OU=SSOConfig,DC=Domain,DC=com The search starts from the specified location(s) and searches all subordinate OUs (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.	No		string/Ø
Location for storing user credentials `Extensions\SyncManager\"Syncs\%AD%:LocateInUser`	Credentials can either be stored as objects subordinate to the Active Directory user object, or as specified by an Oracle locator object.	Yes	0-As specified by locator object (Default) 1-Under respective directory user objects	dword/Ø
Prepend Domain when naming objects `Extensions\SyncManager\Syncs\%AD%:AppendDomain`	Enables prepending of the user's Domain to the username in naming the user's container. **Example:** For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled. **Note:** If you enable Prepend Domain, do not enable Enable Storing Credentials under User Object (in the Directory menu). If you enable credential storage in User Objects, you must disable this option (the default setting). If you enable both options, synchronization does not occur.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\%AD%/Connection information

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Credentials to use Extensions\SyncManager\Syncs\%AD%:AuthType	Which credentials to use when authenticating to the Active Directory Server.	Yes	0-Use local computer credentials only 1-Use Active Directory server account only (recommended that UserPathN be set) 2-Try local computer credentials; if it fails, use Active Directory server account (Default)	dword/Ø
Prompt when disconnected Extensions\SyncManager\Syncs\%AD%:AllowOffline	Allows the user to work offline without prompting/notification if a synchronization event fails.	Yes	0-No 1-Yes (Default)	dword/Ø
Servers Extensions\SyncManager\Syncs\%AD%\Servers:ServerN	Servers to try, in the format "computer[:port]" (one server per line), where "computer" is the server name, and "port" is assumed to be the default (636 for SSL, 389 for no SSL) if not specified. **Example:** ● DC1.company.com ● DC2.company.com ● company.com:8080 ● companylab.com **Note:** This setting is not normally used when storing Oracle data in Active Directory. Active Directory requires use of computer names (not IP addresses).	No		string/Ø
User Paths Extensions\SyncManager\Syncs\%AD%:UserPathN	Fully-qualified path to where the user account is located. There can be unlimited paths to search. The extension searches these in order, looking for the user account. If not found, the extension will search the directory tree. **Note:** This entry is not required for this extension.	Yes		string/Ø
Use SSL Extensions\SyncManager\Syncs\%AD%:UseSSL	Connect via SSL.	Yes	0-No (insecure) (default to port #389) (Default) 1-Yes (default to port #636)	dword/Ø
Logon attempts Extensions\SyncManager\Syncs\%AD%:RetryLockCount	Number of times to present the Synchronization dialog to the user. For example, if you set this value to 3, the Synchronization dialog displays a maximum of three times if the user submits incorrect credentials.	Yes	(Default-3)	dword/int

Screen/Display Path: Synchronization\%AD%/User interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Descriptive name `Extensions\SyncManager\Syncs\%AD%:DisplayName`	Logon dialog title, to help differentiate between multiple synchronizer extensions having the same name.	Yes		string/string
Password change window title `Extensions\SyncManager\Syncs\%AD%:CAP_WindowTitle`	Use this setting to customize the Active Directory Change Password Window title name for this synchronizer.	Yes		string/string
Password change window subtitle `Extensions\SyncManager\Syncs\%AD%:CAP_WindowSubTitle`	Use this setting to customize the Active Directory Change Password Window subtitle name for this synchronizer.	Yes		string/string

Screen/Display Path: Synchronization\%AD%/Credential sharing

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Share credentials with authenticators `Extensions\SyncManager\Syncs\%AD%:ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string

Screen/Display Path: Synchronization\%AD%/File mode configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Limit search to server root `Extensions\SyncManager\Syncs\%AD%:StopAtRoot`	Controls how the Agent searches for locator and override objects.	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path: Synchronization\ %DB%

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
DB Sync DLL location `Extensions\SyncManager\Syncs\%DB%:Path`	Path\filename of the Database synchronizer extension.	No	(Default-%INSTALLDIR% Plugin\ SyncMgr\ DBEXT\ DBExt.dll)	string/string
Servers `Extensions\SyncManager\Syncs\%DB%\Servers:Server`	List of servers to try, entered one per line using full connection strings. **Note:** You must specify at least one server for this extension to work.	No		string/string
Append Domain when naming objects `Extensions\SyncManager\Syncs\%DB%:AppendDomain`	Enables appending of the user's Domain to the username in naming the user's container. **Example:** For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "jamesk.company" with this flag enabled.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\ %File%

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
File Sync DLL location `Extensions\SyncManager\Syncs\%File%:Path`	Path\filename of the File System synchronizer extension.	No	(Default-%INSTALLDIR% Plugin\ SyncMgr\ FileSyncExt\ filesync.dll)	string/filename

Screen/Display Path: Synchronization\ %File%/Data storage configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Prepend Domain when naming user folders `Extensions\SyncManager\Syncs\%File%:AppendDomain`	Enables prepending of the user's Domain to the username in naming the user's container. **Example:** For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled.	Yes	0-No 1-Yes (Default)	dword/Ø

Screen/Display Path:
Synchronization\ %File%/Connection information

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Prompt when disconnected `Extensions\SyncManager\Syncs\%File%:AllowOffline`	Allows the user to work offline without prompting/notification if a synchronization event fails.	Yes	0-Yes 1-No (Default)	dword/Ø
Server `Extensions\ SyncManager\Syncs\%File%\Servers:Server1`	UNC path to try. **Examples:** ● \\FS1\Users ● \\FS2\Extras ● D:\Backup **Note:** You must specify Server1 for this extension to work. The File System extension requires use of proper UNC paths. Only one path is supported; failover is not supported.	No		string/string
Logon attempts `Extensions\SyncManager\Syncs\%File%:RetryLockCount`	Number of times to present the retry dialog to the user.	Yes	Minimum value of 1 (Default-3)	dword/int

Screen/Display Path:
Synchronization\ %File%/User interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Descriptive name `Extensions\SyncManager\Syncs\%File%:DisplayName`	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name. **Note:** This entry is not required.	Yes		string/string

Screen/Display Path: Synchronization\%LDAP%

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
LDAP Sync DLL location `Extensions\SyncManager\Syncs\%LDAP%:Path`	Path\filename of the LDAP Directory Server synchronizer extension.	No	(Default-%INSTALLDIR%Plugin\ SyncMgr\ LDAP\ ldapsync.dll)	string/filename

Screen/Display Path: Synchronization\%LDAP%/Data storage configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Base location(s) for configuration objects `Extensions\SyncManager\Syncs\%LDAP%\COBaseLocations:LocationN`	Where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as: ● OU=SSOConfig,DC=Domain,DC=com The search starts from the specified location(s) and searches all subordinate OUs (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.	No		string/Ø

Screen/Display Path:
Synchronization\%LDAP%/Connection information

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Prompt when disconnected `Extensions\SyncManager\Syncs\%LDAP%:AllowOffline`	Allows the user to work offline without prompting/notification if a synchronization event fails.	Yes	0-Yes 1-No (Default)	dword/Ø
Directory type `Extensions\SyncManager\Syncs\%LDAP%:DirectoryType`	The specific type of directory server. If the directory server is not listed, select "Unspecified LDAP Directory" for backwards compatibility in upgrade scenarios; otherwise select "Generic LDAP Directory."	Yes	0-Unspecified LDAP Directory (Default) 3-Novell eDirectory 5-Generic LDAP Directory 8-Oracle Directory Server Enterprise Edition 9-IBM Tivoli Directory Server 10-Oracle Internet Directory 11-Siemens DirX Directory Server	dword/Ø
Servers `Extensions\SyncManager\Syncs\%LDAP%\Servers:ServerN`	Servers to try, in the format "computer[:port]" (one server per line), where "computer" is the server name, and "port" is assumed to be the default (636 for SSL, 389 for no SSL) if not specified. **Examples:** ● LDAP1.company.com ● LDAP2.company.com ● LDAP3.company.com:50389	No		string/Ø
User paths `Extensions\SyncManager\Syncs\%LDAP%:UserPathN`	Fully-qualified (distinguished) path to the location of the user account when LDAP Directory Search is not enabled. There can be unlimited paths to search. The extension searches these in order, looking for the user account. When using LDAP Directory Search, if the user account is not found in the given userpath, the extension searches down the directory tree from that path. **Example:** ● OU=Users,DC=Domain,DC=com **Note:** You must specify at least one value for UserPath for this extension to work.	Yes		string/Ø
Use SSL `Extensions\SyncManager\Syncs\%LDAP%:UseSSL`	Connect via SSL.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\%LDAP%/Administrative security

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Administrative group DN `Extensions\SyncManager\Syncs\%LDAP%:AdminGroup`	DN for the Administrative group. It is placed this value in the ACI. **Examples:** • cn=configuration administrators, ou=groups, • ou=topologymanagement, o=netscaperoot	Yes		string/string
Security version `Extensions\SyncManager\Syncs\%LDAP%:SecurityVersion`	Update the ACI with a new :AdminGroup value when this value is higher than :SecurityUpgrade.	Yes		dword/int

Screen/Display Path: Synchronization\%LDAP%/User interface

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Descriptive name `Extensions\SyncManager\Syncs\%LDAP%:DisplayName`	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name. **Note:** This entry is not required.	Yes		string/string
Show user path `Extensions\SyncManager\Syncs\%LDAP%:ShowUserPath`	Use this setting to show/hide the User Path combo box control in the LDAP synchronizer authentication dialog.	Yes	0-No 1-Yes (Default)	dword/Ø
Logon attempts `Extensions\SyncManager\Syncs\%LDAP%:RetryLockCount`	Number of times to present the retry dialog to the user.	Yes	Minimum value of 1 (Default-3)	dword/int

Screen/Display Path: Synchronization\%LDAP%/Credential sharing

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Share credentials with authenticators `Extensions\SyncManager\Syncs\%LDAP%:ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/Ø

Screen/Display Path: Synchronization\ %LDAP%\ Special Purpose

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Naming attribute string `Extensions\ SyncManager\ Syncs\%LDAP%: UserPrepend`	String to prepend to UserPaths when the DN for a user is in the form of: ● cn=%UserName%,ou=people,dc=computer instead of the form: ● namingattribute=%UserName%,ou=people,dc=computer (where namingattribute can be any string). **Note:** Typically, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.	Yes		string/string
BIND timeout `Extensions\ SyncManager\ Syncs\%LDAP%:Timeout`	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
BIND user DN `Extensions\ SyncManager\ Syncs\%LDAP%: BindUserName`	Specifies LDAP "browse only" account user DN. This must be in the format: ● "uid=%username%, ou=people, dc=%CompanyName%" (for example, uid=jsmith, ou=people, dc=passlogix, dc=com). You must enable anonymous binding on the directory for LDAP Directory Search functionality. If you do not enable anonymous binding, you must use this account to perform the directory search. The search is performed whether using "User Paths" or the "Alternate User ID location."	Yes		string/string
BIND user password `Extensions\ SyncManager\ Syncs\%LDAP%: BindUserPassword`	Specifies LDAP "browse only" account user password. You must enable anonymous binding on the directory for LDAP Directory Search functionality. If you do not enable anonymous binding, you must use this account to perform the directory search. The search is performed whether using "User Paths" or the "Alternate User ID location."	Yes		string.MaskedString

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Alternate user ID location `Extensions\SyncManager\Syncs\%LDAP%:UserLocation`	Specifies where to locate a user object when the user validates against an attribute other than the username. **Example:** If users authenticate with an employee ID # for logon (validation against the empid attribute) and the user object is in: • ou=people,dc=computer, • set UserLocation to: • empid=%user,ou=people,dc=computer instead of to • uid=user,ou=people,dc=computer. **Note:** For Novell eDirectory, UserLocation should be: • uid=%user,path to the object. If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string
Enable directory search for users `Extensions\SyncManager\Syncs\%LDAP%:LDAPBindSearch`	Enables or disables directory search for the user account. When the user account is not found in the given path, the extension will search for it from that location down the directory tree. The search is performed whether using "User Paths" or the "Alternate User ID location."	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path: Synchronization\ %ROAM%\ Required

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Roaming Sync DLL location `Extensions\SyncManager\Syncs\%ROAM%:Path`	Path\filename of the roaming synchronizer extension.	No	(Default-%INSTALLDIR% Plugin\ SyncMgr\ RoamExt\ RoamSyncExt.dll)	string/filename

Security Settings

Screen/Display Path:
Security/Options

Display Name/ Registry Path	Description	Overridable	Options/Default	RegType/ DataType
Store user data on disk in encrypted file `Extensions\StorageManager\InMemShr:LocalStorage`	Store a copy of user data (for example, credentials) locally in an encrypted database file in each user's ApplicationData folder.	Yes	0-No 1-Yes (Default)	dword/Ø
Default encryption algorithm `CSP:PreferredCSP`	Select the default encryption algorithm from the dropdown menu. **Note:** Non-MS CAPI algorithms have been deprecated and are listed for upgrade scenarios only. Do not select these algorithms.	Yes	0-Cobra 128-bit 512-Cobra 128-bit (also) 513-Blowfish 448-bit 1028-Triple-DES 168-bit 1285-AES 256-bit 25700-Triple-DES (MS CAPI) (All OSs) (Default) 25723-Triple-DES (MS CAPI) (XP/2003 only) 25956-RC-4 (MS CAPI) (All OSs) 25979-RC-4 (MS CAPI) (XP/2003 only) 26491-AES (MS CAPI) (XP/2003 only)	dword/Ø
Reauthentication timer `Extensions\AccessManager:AutoLogin`	Time (in milliseconds) between reauthentication requests. If set to 4,294,967,295 (0xFFFFFFFF), the time never expires and the user will never need to reauthenticate, except in forced authentication scenarios. **Note:** Default value for client-side installation is 900,000 (15 minutes). Default in a Terminal Services environment is 4,294,967,295 (disabled).	Yes	(Default-900000)	dword/int
Require reauthentication before updating account credentials `Extensions\AccessManager:RequireAuthCred`	Specifies whether the user must enter ESSO-LM credentials before changing application credentials, even though the authentication timer has not expired.	Yes	0-No (Default) 1-Yes	dword/Ø

Screen/Display Path:
Security/ Masked fields

Display Name/ Registry Path	Description	Overridable	Options/Default	RegType/ DataType

Obfuscate length
`Extensions\AccessManager:`
`HideMaskedFieldLength`
	Specifies whether to display encrypted fields with a string of blank characters different from the length of the obfuscated data.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Allow revealing
`Extensions\AccessManager:`
`AllowReveal`
	Specifies whether the user is permitted to reveal masked fields.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Require reauthentication to reveal
`Extensions\AccessManager:`
`ReauthOnReveal`
	Specifies whether the user must enter ESSO-LM credentials in order to reveal masked fields, assuming that he is permitted to do so.	Yes	0-No
			1-Yes (Default)
				dword/Ø

Custom Actions Settings

Screen/Display Path:
Custom Actions

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
After Agent starts `Shell\Tasks:StartupTaskN`	Command(s) that will run every time the background task starts (the Tray Icon appears).	Yes		string/Ø
Before Agent starts `Shell\Tasks:PreTaskN`	Command(s) that will run before any Agent process starts (any time a new instance of SSOShell is launched). Every background synchronization and every opening of ESSO-LM will execute this command before continuing. **Note:** The Agent will not continue if any of these tasks fails (as indicated by the resultant registry value located at License:PreCheck).	Yes		string/Ø
When logons are deleted `Shell\Tasks:DeletionTaskN`	Command(s) that will run every time a user deletes an application configuration.	Yes		string/Ø
When logons change (add, delete, copy, modify) `Shell\Tasks:RefreshTaskN`	Command(s) that will run every time credentials and user configurations are modified.	Yes		string/Ø

Audit Logging Settings

Screen/Display Path:
Audit Logging

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Cache limit `Extensions\EventManager:CacheLimit`	Maximum number of event log entries to be cached before old events are discarded.	Yes	(Default-200)	dword/int
Retry interval `Extensions\EventManager:Retry`	Interval (in minutes) between retries for all Event Logging extensions. **Note:** If you are using Reporting, you should set this value to zero (0).	Yes	(Default-30)	dword/int

Screen/Display Path:
Audit Logging\Reporting Server/Database

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Connection string `Reporting\Extensions\Database:ConnectionString`	Database connection string in the OLE DB format: "Provider=SQLOLEDB; Data Source=myServerName; Initial Catalog=myDatabaseName; UserId=myUsername; Password=myPassword".	No		string/string
Stored procedure `Reporting\Extensions\Database:StoredProcedure`	The name of the stored procedure used to populate the database with events.	No	(Default-dbo.sp_WriteEvents)	string/string

Screen/Display Path:
Audit Logging\Reporting Server/Options

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Batch size `Reporting:BatchSize`	Number of events to send to Reporting extensions in one batch.	Yes	(Default-100)	dword/int
Cache limit `Reporting:CacheLimit`	Maximum number of reporting events to cache before discarding old events.	Yes	(Default-4294967295, or 0xFFFFFFFF)	dword/int
Retry interval `Reporting:RetryInterval`	Interval (in minutes) between retries for all Reporting event logging extensions.	Yes	(Default-30)	dword/int

Screen/Display Path:
Audit Logging\Windows Event Viewer

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Windows event logging server `Extensions\EventManager\WindowsEvent:EventServer`	Server name for the Windows Event Logging extension (do not provide leading "\\" characters). If missing, logged to local computer. The server should have a trusted relationship with the user's account and the user's computer, depending on access rights and restrictions.	Yes		string/string
Retry interval `Extensions\EventManager\WindowsEvent:Retry`	Interval (in minutes) between retries for the Windows Event Logging extension.	Yes	(Default-30)	dword/int
Events to log `Extensions\EventManager\WindowsEvent:Filter`	Event logging filter delineating which events (of those logged by the root Filter setting) to log to the Windows Event Logging extension.	Yes	(Default-0) 4-Credential Edit 8-Credential Delete 10-Credential Copy 20-Credential Add 100-Provisioning 200-Startup/Shutdown 400-Help 800-Settings Change 1000-Reauthentication 10000-Sync User Information 20000-Logon Field: System Username 40000-Logon Field: System Domain 80000-Logon Field: Third Field 100000-Logon Field: Username 200000-Logon Field: Fourth Field 800000-Application Password Change 1000000-Primary Logon Method Change 4000000-Backup/Restore 40000000-Event Types: Info	dword/Ø

Screen/Display Path:
Audit Logging\Syslog Server

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Destination host `Extensions\EventManager\Syslog:RemoteAddress`	Enter the hostname that will receive messages, using either a hostname or dotted IP v4-address. Use 0.0.0.0 to disable sending to syslog-daemon, or use 255.255.255.255 to send to any daemon that is set up to receive broadcast messages. The broadcast does not reach beyond a router; the daemon must be on your local network.	No	(Default-localhost)	string/string
Destination port `Extensions\EventManager\Syslog:RemotePort`	Sets the destination port for syslog messages using a number.	Yes	(Default-1468)	dword/int
Protocol for sending messages `Extensions\EventManager\Syslog:UseTCP`	Specifies whether to send messages via TCP or UDP protocol. **Note:** The UDP protocol is connectionless, so it is impossible to tell whether the Syslog Daemon is reachable at the specified hostname and port. If the UseTCP parameter is set to "Use UDP," the Syslog Extension returns S_OK on both success and failure. If it is necessary to make the Syslog Extension return the correct state, enable TCP in the Syslog Daemon and set this parameter to "Use TCP."	Yes	0-Use UDP 1-Use TCP (Default)	dword/Ø
Retry interval `Extensions\EventManager\Syslog:Retry`	Interval (in minutes) between retries for the Syslog extension.	Yes	(Default-30)	dword/int

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Events to log `Extensions\EventManager\Syslog:Filter`	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Syslog extension. Click the ellipsis "**...**" button to see a list of events to log.	Yes	(Default-0) 4-Credential Edit 8-Credential Delete 10-Credential Copy 20-Credential Add 100-Provisioning 200-Startup/Shutdown 400-Help 800-Settings Change 1000-Reauthentication 10000-Sync User Information 20000-Logon Field: System Username 40000-Logon Field: System Domain 80000-Logon Field: Third Field 100000-Logon Field: Username 200000-Logon Field: Fourth Field 800000-Application Password Change 1000000-Primary Logon Method Change 4000000-Backup/Restore 40000000-Event Types: Info	dword/Ø

Screen/Display Path:
Audit Logging\XML File

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Retry interval `Extensions\EventManager\LocalStorage:Retry`	Interval (in minutes) between retries for the Local (XML) File Logging extension.	Yes	(Default-30)	dword/int
Events to log `Extensions\EventManager\LocalStorage:Filter`	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Local (XML) File Logging extension.	Yes	(Default-0) 4-Credential Edit 8-Credential Delete 10-Credential Copy 20-Credential Add 100-Provisioning 200-Startup/Shutdown 400-Help 800-Settings Change 1000-Reauthentication 10000-Sync User Information 20000-Logon Field: System Username 40000-Logon Field: System Domain 80000-Logon Field: Third Field 100000-Logon Field: Username 200000-Logon Field: Fourth Field 800000-Application Password Change 1000000-Primary Logon Method Change 4000000-Backup/Restore 40000000-Event Types: Info	dword/Ø

Screen/Display Path:
Audit Logging\Database

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Servers `Extensions\EventManager\Database\Servers:ServerN`	Click the ellipsis "**...**" button to open a window in which to enter Database servers. Enter one server name per line, using the OLE DB format: "Provider=sqloledb; Data Source=myServerName; Initial Catalog=myDatabaseName; User Id=myUsername; Password=myPassword".	No		string/Ø
Default server `Extensions\EventManager\Database:Default Server`	If no other server is specified, the server to which the database log will be written. (OLE DB connection string)	No	(Default-Server1)	string/string
Default table `Extensions\EventManager\Database:Default Table`	If no other table is specified, the table to which the database log will be written.	Yes		string/string
Retry interval `Extensions\EventManager\Database:Retry`	Interval (in minutes) between retries for the Database extension.	Yes	(Default-30)	dword/int

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Events to log `Extensions\EventManager\Database:Filter`	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Database extension. Click the ellipsis "**...**" button to see a list of events to log.	Yes	(Default-0) 4-Credential Edit 8-Credential Delete 10-Credential Copy 20-Credential Add 100-Provisioning 200-Startup/Shutdown 400-Help 800-Settings Change 1000-Reauthentication 10000-Sync User Information 20000-Logon Field: System Username 40000-Logon Field: System Domain 80000-Logon Field: Third Field 100000-Logon Field: Username 200000-Logon Field: Fourth Field 800000-Application Password Change 1000000-Primary Logon Method Change 4000000-Backup/Restore 40000000-Event Types: Info	dword/Ø

Screen/Display Path:
Audit Logging\Database\Event Fields

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
AppName `Extensions\EventManager\Database\EventFields:AppName`	The name of the application of the event log.	Yes	(Default-AppName)	string/string
Category `Extensions\EventManager\Database\EventFields:Category`	The category of the event.	Yes	(Default-Category)	string/string
Type `Extensions\EventManager\Database\EventFields:Type`	The specific type of event.	Yes	(Default-Type)	string/string
TimeStamp `Extensions\EventManager\Database\EventFields:TimeStamp`	The time of the event.	Yes	(Default-TimeStamp)	string/string
Field1 `Extensions\EventManager\Database\EventFields:Field1`	EventType	Yes	(Default-Event type)	string/string
Field2 `Extensions\EventManager\Database\EventFields:Field2`	UserID	Yes	(Default-User ID)	string/string
Field3 `Extensions\EventManager\Database\EventFields:Field3`	ThirdField	Yes	(Default-Third field)	string/string
Field4 `Extensions\EventManager\Database\EventFields:Field4`	FourthField	Yes	(Default-Fourth field)	string/string
Field5 `Extensions\EventManager\Database\EventFields:Field5`	WindowsUser	Yes	(Default-Windows user)	string/string
Field6 `Extensions\EventManager\Database\EventFields:Field6`	Domain	Yes	(Default-Domain)	string/string

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Field7 `Extensions\EventManager\Database\EventFields:Field7`	ComputerName	Yes	(Default-Computer name)	string/string
Field8 `Extensions\EventManager\Database\EventFields:Field8`	SSOSyncUser	Yes	(Default-SSO synchronization user)	string/string
Field9 `Extensions\EventManager\Database\EventFields:Field9`	Customizable for your needs.	Yes	Open	string/string
Field10 `Extensions\EventManager\Database\EventFields:Field10`	Customizable for your needs.	Yes	Open	string/string

Kiosk Manager Settings

Screen/Display Path:
Kiosk Manager/Session termination

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Allow administrator to close Kiosk Manager `SM\Agent: AdministrativeClose`	Specifies whether an administrator has the ability to close Kiosk Manager. With this setting enabled, only a user with administrator credentials can close the Agent.	Yes	0-No 1-Yes (Default)	dword
Number of times to process termination `SM\Agent: TerminationIteration`	Enter the number of times that Kiosk Manager should process the termination of an application. This setting instructs the termination process to loop a certain number of times or until it is done, which ever comes first. This allows Kiosk Manager to react to an application if it displays multiple screens during the termination process.	Yes	(Default-1)	dword/int
Timeout for locked session `SM\Agent:ExpireTerm`	Enter the amount of time (in seconds) after which a suspended/locked session is closed.	Yes	(Default-600 ([15 minutes])	dword/int

Screen/Display Path:
Kiosk Manager/Multisession configuration

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Maximum number of sessions `SM\Agent: MaxSessions`	Sets the maximum number of sessions allowed at one time. 0 will be interpreted as 1. There is no maximum.	Yes	(Default-1)	dword/int
Track memory consumption `SM\Agent: TrackMemoryConsumption`	When system memory use has reached the percentage as set by this value, Kiosk Manager automatically closes the oldest user sessions.	Yes	Minimum-0 (disabled) Maximum-100 (Default-90)	dword/int

Screen/Display Path:
Kiosk Manager/Cached credentials

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Use cached credentials `SM\Agent: UseCachedCredentials`	Specifies whether to use cached credentials. If enabled, at logon, the Agent displays a list of cached credentials for users to choose from. If disabled, the Agent does not display the list, and users must enter a user name at logon.	Yes	0-No (Default) 1-Yes	dword
Storage path `SM\Agent: CachedCredentialsStoragePath`	The default folder to store cached credentials. If this value is empty (the default), the folder is: C:\Documents and Settings\&lt;Kiosk User&gt;\ Local Settings\ Application Data\Passlogix\ SessionData\&lt;Kiosk Manager User&gt;	Yes	(Default-An empty string.)	string
Expiration date `SM\Agent: CachedCredentialExpiration`	Specifies the number of days to retain cached credentials. Zero indicates that this feature is disabled.	Yes	(Default-30)	dword/int

Screen/Display Path:
Kiosk Manager/Strong authentication options

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Lock session on smart card removal `AUI\SCauth: LockSMOnRemoval`	Specifies whether to lock a session when the session owner removes the smart card from the reader. If set to not lock, the session remains open after smart card removal. This setting is useful in a scenario where employees must display their smart cards at all times.	Yes	0-No 1-Yes (Default)	dword
Lock session on read-only smart card removal `AUI\ROSCauth: LockSMOnRemoval`	Specifies whether to lock a session when the session owner removes the read-only smart card from the reader. If set to not lock, the session remains open after read-only smart card removal. This setting is useful in a scenario where employees must display their read-only smart cards at all times.	Yes	0-No 1-Yes (Default)	dword
Pre-populate on startup `SM\Agent:Prepopulate`	Specifies whento pre-populate on session startup.	Yes	0-On device-in event (Default) 1-Always 2-Never	dword

Screen/Display Path:
Kiosk Manager/Audit Logging

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Event log name `SM\Agent:EventLogName`	Enter the name of the Windows event log for Kiosk Manager events.	Yes	(Default-Application)	string
Event log machine name `SM\Agent:EventLogMachine`	Enter the name of the local machine to log Kiosk Manager events.	No		string

Screen/Display Path:
Kiosk Manager/User Interface/Options

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Allow computer restart `SM\Agent:AllowRestart`	Specifies whether to enable the restart computer option in the Desktop Manager. **Note:** If the Kiosk account does not have sufficient privileges, restarting might still be disabled.	Yes	0-No (Default) 1-Yes 2-Administrator must supply password	dword
Allow computer shutdown `SM\Agent:AllowShutdown`	Specifies whether to enable the shutdown computer option in the Desktop Manager. **Note:** If the Kiosk account does not have sufficient privileges, shutting down might still be disabled.	Yes	0-No (Default) 1-Yes 2-Administrator must supply password	dword
Show confirmation message when restarting kiosk `SM\Agent:ConfirmRestart`	Specifies whether to prompt the user with a confirmation message after choosing to restart the kiosk.	Yes	0-No (Default) 1-Yes	dword
Show confirmation message when shutting down kiosk `SM\Agent:ConfirmShutdown`	Specifies whether to prompt the user with a confirmation message after choosing to shut down the kiosk.	Yes	0-No (Default) 1-Yes	dword
Lock session when screen saver times out `SM\Agent:LockOnScreenSaver`	Specifies whether to lock a session after the screen saver timeout occurs. A blank value has the same effect as setting the value to "No."	Yes	0-No (Default) 1-Yes	dword
Timeout for authentication prompt `SM\Agent:AuthTerm`	Enter the amount of time (in seconds) after which the synchronization/authentication dialog closes (due to inactivity).	Yes	(Default-600 [15 minutes])	dword/int

Screen/Display Path:
Kiosk Manager/User Interface/Status window

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Show desktop status window `SM\Agent:DisplayDesktopStatus`	Specifies whether to show the optional window that displays the current session owner.	Yes	0-No (Default) 1-Yes	dword
X coordinate `SM\Agent:DesktopStatusX`	Enter the X coordinate (horizontal location) for the status window.	Yes	(Default-0)	dword/int
Y coordinate `SM\Agent:DesktopStatusY`	Enter the Y coordinate (vertical location) for the status window.	Yes	(Default-0)	dword/int

Screen/Display Path:
Kiosk Manager/User Interface/Transparent screen lock

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Use transparent lock `SM\Agent:TransparentLock`	Specifies whether to enable the transparent screen lock.	Yes	0-No (Default) 1-Yes, but only for active session 2-Yes	dword
Delay period `SM\Agent:TransparentLockTime`	Specifies the number of seconds to wait for mouse and keyboard inactivity before showing the desktop.	Yes	(Default-5)	dword/int
Ignore delay period if authentication is canceled `SM\Agent: TransparentDisplayAfterCancel`	Specifies whether transparency should take effect immediately after canceling an authenticator or synchronizer dialog.	Yes	0-No (The desktop displays when the inactivity timer expires.) (Default) 1-Yes (The desktop displays instantly.)	dword
Only recognize Ctrl-Alt-Del `SM\Agent: TransparentOnlyRecognizeCAD`	Specifies whether the Agent should recognize only Ctrl-Alt-Del and authenticators that support "device-in" to display the Desktop Manager.	Yes	0-No (The Agent recognizes any keyboard or mouse activity) (Default) 1-Yes (The Agent ignores all keyboard or mouse activities)	dword

Screen/Display Path:
Kiosk Manager/User Interface/Background Image

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType

Location of image file
`SM\Agent\Desktop:`
`LogoPath`
	Fully-qualified path and filename of the image file.	Yes		string/filename

X coordinate
`SM\Agent\Desktop:`
`LogoX`
	Enter the X coordinate (horizontal location) for the image.
	Note: Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
		Yes	(Default-0)	dword/int

Y coordinate
`SM\Agent\Desktop:`
`LogoY`
	Enter the Y coordinate (vertical location) for the image.
	Note: Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
		Yes	(Default-0)	dword/int

Width
`SM\Agent\Desktop:`
`LogoWidth`
	Enter the width of the image (in pixels).	Yes	(Default-300)	dword/int

Height
`SM\Agent\Desktop:`
`LogoHeight`
	Enter the height of the image (in pixels).	Yes	(Default-300)	dword/int

Placement behavior
`SM\Agent\Desktop:`
`LogoMode`
	Specifies how to handle the image with respect to its coordinates and dimensions.	Yes	0-Normal (Place image in upper left corner of coordinates and clipp if larger than specified height and width) (Default)
			1-Auto (Place image in upper left corner of coordinates)
			2-Center (Center image within coordinates and clip if larger than specified height and width)
			3-Stretch (Stretch or shrink image to fit within specified coordinates)
			4-Maximize (Stretch image to full screen size)
				dword

Screen/Display Path: Kiosk Manager/User Interface/Text Message/Message

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Message text `SM\Agent\Desktop: MOTDText`	Enter a message to display on Desktop Manager. This message appears when the user unlocks a new session.	Yes		string/string

Screen/Display Path: Kiosk Manager/User Interface/Text Message/Font

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Name `SM\Agent\Desktop: MOTDFontName`	Specifies the Text Message font.	Yes		string/font
Size `SM\Agent\Desktop: MOTDFontSize`	Specifies the Text Message font size.	Yes	(Default-0)	dword/int
Style `SM\Agent\Desktop: MOTDFontStyle`	Specifies the Text Message font style.	Yes	0-Regular (Default) 1-Bold 2-Italic	dword

Screen/Display Path: Kiosk Manager/User Interface/Text Message/Color

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
Background `SM\Agent\Desktop: MOTDBackColor`	Specifies the Text Message background color.	Yes		string/color
Foreground `SM\Agent\Desktop: MOTDForeColor`	Specifies the Text Message foreground color.	Yes		string/color

Screen/Display Path:
Kiosk Manager/User Interface/Text Message/Placement

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
X coordinate `SM\Agent\Desktop:MOTDX`	Enter the X coordinate for the Text Message, positioned relative to the Status image on the Kiosk Manager Desktop screen. A negative value places the message to the left of the Status image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
Y coordinate `SM\Agent\Desktop:MOTDY`	Enter the Y coordinate for the Text Message, positioned relative to the Status image on the Kiosk Manager Desktop screen. A negative value places the message above the Status image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
Width `SM\Agent\Desktop:MOTDWidth`	Specifies the width of the Text Message (in pixels).	Yes	(Default-300)	dword/int
Height `SM\Agent\Desktop:MOTDHeight`	Specifies the height of the Text Message (in pixels).	Yes	(Default-300)	dword/int
Size automatically `SM\Agent\Desktop:MOTDAutoSize`	Specifies whether to auto-size the Text Message to fit the available area.	Yes	0-No (Default) 1-Yes	dword

Appendix 1. Node Modifications and Removed Settings

The following nodes have changed in version 11.1.1.5.0 of the ESSO-LM Administrative Console:

- "End User Experience" has been renamed "User Experience."
- "Event Logging" has been renamed "Audit Logging."
- "Primary Logon Methods" has been renamed "Authentication."
- Reporting settings are now a sub-node of the Audit Logging node.

The following settings have been removed from the ESSO-LM Administrative Console:

End-User Experience Node

Sub-Node Path	Removed Settings
Environment	• Default Backup path
Password Change\Required	• Credential Sharing Groups
Password Change\Advanced	• Notify Primary Logon Method
Response\Error Loop	• Maximum retries before prompting • Maximum time for retries before prompting • Require password confirmation when modifying password
Response\ Host/Mainframe Apps	• Host/Mainframe support
Response\Host/Mainframe Apps\Error Loop	• Maximum retries before prompting • Maximum time for retries before prompting • Require password confirmation when modifying password
Response\Web Apps\Error Loop	• Maximum retries before prompting • Maximum time for retries before prompting • Require password confirmation when modifying password
Response\Windows Apps	• Ignored Window Classes for Applications • Retry for a Window Title Match • Supported Window Classes for Applications • Supported Window Classes for Services
Response\Windows Apps\Error Loop	• Maximum retries before prompting • Maximum time for retries before prompting • Require password confirmation when modifying password
Advanced\Performance	• Increase user data storage priority • Maximum time before forced SSO process shut down • Set delay for first update (after startup) to stored user data • Set delay for storing user data

Event Logging Node

Sub-Node Path	Removed Settings
	• Select events to log
Reporting	• Extension location
Database	• Extension location
Syslog	• Extension location
Windows Event Viewer\Advanced	• Extension location
XML File	• Extension location
Advanced	• Event Server Message Library location • Extension location • Shutdown Delay • Shutdown Immediately

Primary Logon Methods Node

Sub-Node Path	Removed Settings
LDAP\Advanced	• SSL Fallback
LDAP v2\Advanced	• Passphrase • When SSL fails
Windows v2\ Advanced	• Passphrase As of version 11.1.1.5.0, Passphrase options are available under Authentication> Windows v2> Passphrase.

Reporting Node

Sub-Node Path	Removed Settings
Database	• Extension location

Synchronization Node

Sub-Node Path	Removed Settings
%AD%\Required	• Extension location
%AD%\Advanced	• Search for locator and override objects • When SSL fails
%ADAM%\Required	• Extension location
%ADAM%\Advanced	• When SSL fails
%DB%\Required	• Extension location
%File%\Required	• Extension location
%LDAP%\Required	• Extension location
%LDAP%\Advanced	• DSAME disabled-account support • When SSL fails
%ROAM%\Required	• Extension location

Appendix 2. Modified Default Values

The following settings' default values have changed. Where node names have changed, the new node name follows the previous name *(in parentheses)*.

Node/Path	Setting	New Default Value
End-User Experience *(User Experience)*	Title Bar Button Menu	Do not show
End-User Experience *(User Experience)*\Password Change\Required	Credential Sharing Groups	Enabled
End-User Experience *(User Experience)*\Response\Error Loop	Maximum retries before prompting	0
End-User Experience *(User Experience)*\Response\Host/Mainframe Apps\Error Loop	Maximum retries before prompting	0
End-User Experience *(User Experience)*\Response\Web Apps	Scroll Into View	Disabled
End-User Experience *(User Experience)*\Response\Web Apps\Error Loop	Maximum retries before prompting	0
End-User Experience *(User Experience)*\Response\Windows Apps\Error Loop	Maximum retries before prompting	0
Primary Logon Methods *(Authentication)*\LDAP\Required	SSL	Do not use SSL
Primary Logon Methods *(Authentication)*\LDAP v2\Required	SSL	Do not use SSL
Synchronization\%AD%\Required	SSL	Do not use SSL
Synchronization\%AD%\Advanced	Prompt when disconnected	Do not prompt
Synchronization\%ADAM%\Required	SSL	Do not use SSL
Synchronization\%ADAM%\Advanced	Prompt when disconnected	Do not prompt
Synchronization\%File%\Advanced	Prompt when disconnected	Do not prompt
Synchronization\%LDAP%\Required	SSL	Do not use SSL
Synchronization\%LDAP%\Advanced	Prompt when disconnected	Do not prompt

Index