

**Oracle® Enterprise Single Sign-on  
Logon Manager**

Global Agent Settings Reference Guide

Release 11.1.1.5.0

**E21028-01**

March 2011

Copyright ©2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

## Table of Contents

Abbreviations and Terminology.....	4
About this Guide.....	5
Audience.....	5
User Experience Settings.....	6
Authentication Settings.....	19
Synchronization Settings.....	38
Security Settings.....	54
Custom Actions Settings.....	56
Audit Logging Settings.....	57
Kiosk Manager Settings.....	66
Appendix 1. Node Modifications and Removed Settings.....	73
Appendix 2. Modified Default Values.....	76
Index.....	77

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

## 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
<b>Display icon in system tray</b> Shell:ShowTrayIcon	Specifies whether to show the ESSO-LM icon in the system tray.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Use server icon</b> 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
<b>Tooltip text</b> 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
<b>Show system name</b> 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
<b>Allow shutdown</b> 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
<b>Show title bar button</b> 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
<b>Always show for</b> Shell:ShowTitleIconAlways ForModuleN	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
<b>Provide dropdown menu</b> 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
<b>Tooltip text</b> 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
<b>Log on to waiting applications upon Agent startup</b> 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.  <b>Note:</b> Web and host/mainframe application logons are not affected by this setting.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>SendKeys event interval</b> 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
<b>Respond to hidden and minimized windows</b> Shell:StrictWindowDetect	Specifies whether the Agent will respond to hidden and minimized windows.	Yes	0-Yes (Default) 1-No	dword/Ø
<b>Applications that hooks should ignore</b> 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
<b>Credential capture mode</b> 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
<b>Enable Auto-Prompt</b> 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
<b>Enable Auto-Enter</b> Extensions\AccessManager: LogonAfterConfig	Whether to log on to an application after configuring it (adding its credentials).	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Enable Auto-Recognize</b> Shell:UseActiveLogin	Whether to automatically provide credentials to applications.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Allow creating multiple accounts during credential capture</b> 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
<b>Prohibit canceling the addition of new accounts</b> 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
<b>Prohibit disabling the addition of new accounts</b> 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
<b>Prohibit excluding accounts from credential sharing groups</b> 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
<b>All application types</b> 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
<b>Windows applications</b> 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
<b>Web applications</b> 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
<b>Allowed Web pages</b> 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.  <b>Note:</b> 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
<b>Show border</b> Extensions\AccessManager\ BHO:ShowBorder	Enable/disable the border around fields.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Border appearance</b> 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
<b>URL matching precision</b> 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: <ul style="list-style-type: none"> <li>• 2=match to *.co.uk (Default)</li> <li>• 3=match to *.company.co.uk</li> <li>• 4=match to *.mail.company.co.uk</li> </ul> <b>Note:</b> Values below 2 are treated as 2.	Yes	Minimum-2 (Default) Maximum-5	dword/int
<b>Scroll into view</b> Extensions\AccessManager\ BHO:ScrollIntoView	Enable/disable scrolling the browser window to bring the logon fields into view.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>Activate tab</b> Extensions\AccessManager\ BHO:ActivateTab	Enable/disable activating the tab that identifies the logon fields.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Respond to IE modal dialogs</b> 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
<b>Applications to ignore</b> 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.  <b>Example:</b> ws_ftp, customapp1	Yes		string/Ø
<b>Web pages to ignore</b> 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).  <b>Examples:</b> <ul style="list-style-type: none"> <li>• .*http://login\company\.com/.*</li> <li>• .*http://.*\company\.com/.*</li> </ul>	Yes		string/Ø
<b>Allowed dynamic Web pages</b> 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.  <b>Examples:</b> <ul style="list-style-type: none"> <li>• .*http://logon\company\.com/.*</li> <li>• .*http://.*\company\.com/.*</li> </ul>	Yes		string/Ø

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

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Allow fallback from control IDs to SendKeys</b> 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
<b>Excluded Java versions</b> Extensions\AccessManager\ JHO:JhoExcludeJavaVersionN	Specify Java versions to exclude, listed as regular expressions. Enter one expression per line.	No		string/Ø
<b>Excluded Java vendors</b> 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	Reg Type/ DataType
<b>Time allowed for Java applets to load</b> 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
<b>Delay after Java runtime startup</b> 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
<b>Delay between retries</b> 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
<b>Maximum times to retry credential injection</b> 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	Reg Type/ Data Type
<b>Hierarchy events</b> 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
<b>Window events</b> 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
<b>Component events</b> 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	Reg Type/ DataType
<b>Injection type</b> 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 <b>Note:</b> 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	Reg Type/ DataType
<b>16-bit screen capture attempts</b> 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
<b>Credential request delay interval</b> 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
<b>Polling interval</b> 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
<b>Default password policy</b> 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.  <b>Note:</b> 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
<b>Allow user to exclude accounts from credential sharing groups</b> Extensions\AccessManager: AllowExcludePWSG	Allows end user to exclude application logons from an assigned credential sharing group.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>Change passwords automatically</b> 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
<b>Manual password change behavior</b> 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
<b>Pop-up dialog text after submission</b> 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**

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



**Screen/Display Path:  
User Experience/User Interface**

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Language</b> [Root]:Language	Language to be used.  <b>Note:</b> 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
<b>Allow refresh in My Accounts</b> Extensions\AccessManager: AllowRefresh	Enables/disables the SSO Manager Refresh button.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Columns in "Details" view of My Accounts</b> 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
<b>Columns in Logon Chooser</b> 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/∅
<b>Logon animation's duration</b> Shell:AutoLogonAnimationTime	Time (in milliseconds) the animated spinner appears (pausing response). <b>Note:</b> 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
<b>Show first-time-use (FTU) wizard</b> Extensions\ SetUpManager\ HideWizard	Controls whether the Setup Wizard displays when first-time-use is invoked. <b>Note:</b> 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/∅
<b>Selected authenticator</b> AUI:FTUShowOnly	Enables the selected logon method as the primary logon method and hides all other installed logon methods. <b>Note:</b> 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/∅
<b>Skip selection page if only one authenticator is installed</b> 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/∅

## Authentication Settings

Screen/Display Path:

Authentication\Authentication Manager

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Allowed number of authenticators</b> 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
<b>Windows v2</b> 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
<b>Windows</b> 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
<b>LDAP v2</b> 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
<b>LDAP</b> 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
<b>Smart card</b> 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
<b>Read-only smart card</b> 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
<b>Proximity card</b> 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
<b>RSA SecurID</b> 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
<b>Entrust</b> 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
<b>Windows v2</b> AUI\MSAuth:AuthGrade	This setting assigns an authentication grade to Windows v2. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>Windows</b> AUI\WinAuth:AuthGrade	This setting assigns an authentication grade to Windows. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>LDAP v2</b> AUI\LDAPAuth:AuthGrade	This setting assigns an authentication grade to LDAP v2. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>LDAP</b> AUI\LDAP:AuthGrade	This setting assigns an authentication grade to LDAP. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>Smart card</b> AUI\SCAuth:AuthGrade	This setting assigns an authentication grade to Smart card. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>Read-only smart card</b> AUI\ROSCAuth:AuthGrade	This setting assigns an authentication grade to Read-only smart card. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>Proximity card</b> AUI\ProxCardAuth:AuthGrade	This setting assigns an authentication grade to Proximity card. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>RSA SecurID</b> AUI\SecureIDAuth:AuthGrade	This setting assigns an authentication grade to RSA SecurID. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0
<b>Entrust</b> AUI\Entrust:AuthGrade	This setting assigns an authentication grade to Entrust. Set a number grade value ( $\geq 1$ ). The higher the grade level specified, the stronger the authentication level that is being requested.	Yes		dword/0

**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
<b>Windows v2</b> 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
<b>Windows</b> 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
<b>LDAP v2</b> 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
<b>LDAP</b> 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
<b>Smart card</b> 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
<b>Read-only smart card</b> 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
<b>Proximity card</b> 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
<b>RSA SecurID</b> 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
<b>Entrust</b> 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
<b>Recovery method</b> AUI\MSauth\ResetMethods: ResetMethodGUID	Specifies the reset method to use when the user's password changes.  <b>Note:</b> 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 <a href="#">ESSO-LM online documentation center</a> .	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/∅
<b>Use Windows Data Protection (DPAPI)</b> 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.  <b>Note:</b> 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/∅

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

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Window title</b> AUI\MSauth:WindowTitle	Use this setting to customize the window title for this authenticator.  <b>Note:</b> This entry is not required.	Yes		string/string
<b>Window subtitle</b> AUI\MSauth:WindowSubTitle	Use this setting to customize the window subtitle for this authenticator.  <b>Note:</b> This entry is not required.	Yes		string/string
<b>Custom image for authentication prompt</b> AUI\MSauth:ImagePath	Fully-qualified path and filename of the image file.	No		string/filename
<b>Reauthentication dialog</b> AUI\MSauth:AuthOptions	Select which method to use when ESSO-LM requires the end-user to re-authenticate.  <b>Note:</b> 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/∅



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

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Include in Domain credential sharing group</b> 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
<b>Share credentials with other authenticators</b> AUI\MSauth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." <b>Note:</b> For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
<b>Share credentials with synchronizers</b> AUI\MSauth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT, LDAPEXT." <b>Note:</b> 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
<b>Message</b> 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. <b>Note:</b> 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
<b>Message dialog title</b> AUI\MSauth\Reset: PassphraseDialogTitle	Use this setting to customize the user agreement style dialog title.	Yes		string/string
<b>Checkbox label</b> AUI\MSauth\Reset: PassphraseChkboxMsg	Use this setting to customize the user agreement style dialog checkbox. <b>Note:</b> 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
<b>Minimum length</b> 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
<b>User can change passphrase</b> 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
<b>Reset with old password</b> AUI\MSauth:ResetWOP	Allows the previous password to be used in the passphrase process.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>Force password re-enrollment when using old password to reset</b> 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.  <b>Warning:</b> 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
<b>Window title</b> AUI\WinAuth: WindowTitle	Use this setting to customize the Window title for this authenticator.  <b>Note:</b> This entry is not required.	Yes		string/string
<b>Window subtitle</b> AUI\WinAuth: WindowSubTitle	Use this setting to customize the Window subtitle for this authenticator.  <b>Note:</b> This entry is not required.	Yes		string/string
<b>Custom image for authentication prompt</b> AUI\WinAuth:ImagePath	Fully-qualified path and filename of the image file.	No		string/filename
<b>Require old password when Windows password changes</b> 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
<b>Share credentials with other authenticators</b> AUI\WinAuth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." <b>Note:</b> For other authenticator names, refer to the list located under HKLM\ Software\ Oracle\ AUI.	Yes		string/string
<b>Share credentials with synchronizers</b> AUI\WinAuth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT, LDAPEXT." <b>Note:</b> 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
<b>Servers</b> 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. <b>Examples:</b> <ul style="list-style-type: none"> <li>• 127.0.0.1</li> <li>• 127.0.0.1:456</li> <li>• somewhereelse.com:8080</li> <li>• anotherplace.com</li> </ul> <b>Note:</b> You must specify at least one server for this extension to work.	No		string/Ø
<b>User paths</b> 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. <b>Note:</b> 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
<b>Use SSL</b> 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
<b>Share credentials with other authenticators</b> AUI\LDAPauth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." <b>Note:</b> For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
<b>Share credentials with synchronizers</b> AUI\LDAPauth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." <b>Note:</b> For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string
<b>Include in LDAP credential sharing group</b> 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
<b>Share credentials with other authenticators</b> AUI\LDAPauth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." <b>Note:</b> For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
<b>Share credentials with synchronizers</b> AUI\LDAPauth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." <b>Note:</b> For other synchronizer names, refer to the list located under HKLM\Software\ Oracle\ Extensions\ SyncManager.	Yes		string/string
<b>Include in LDAP credential sharing group</b> 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
<b>Naming attribute string</b> AUI\LDAPauth: UserPrepend	String to prepend to UserPaths when the DN for a user is in the form of: <ul style="list-style-type: none"> <li>cn=%UserName%,ou=people,dc=computer</li> <li>instead of the form:</li> <li>namingattribute= %UserName%, ou=people, dc=computer</li> </ul> (where namingattribute can be any string). <b>Note:</b> 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
<b>BIND timeout</b> AUI\LDAPauth:Timeout	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
<b>Alternate user ID location</b> AUI\LDAPauth: UserLocation	Use to indicate where to locate a user object when the user validates against an attribute other than the username. <b>Example:</b> If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in: <ul style="list-style-type: none"> <li>ou=people,dc=computer</li> <li>then set UserLocation to:</li> <li>empid=%user,ou=people,dc=computer</li> </ul> instead of to: <ul style="list-style-type: none"> <li>uid=user,ou=people,dc=computer.</li> </ul> <b>Note:</b> For Novell eDirectory, UserLocation should be: <ul style="list-style-type: none"> <li>uid=%user,path to the object.</li> </ul> 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
<b>Naming attribute string</b> AUI\LDAPauth: UserPrepend	String to prepend to UserPaths when the DN for a user is in the form of: <ul style="list-style-type: none"> <li>cn=%UserName%,ou=people,dc=computer</li> </ul> instead of the form: <ul style="list-style-type: none"> <li>namingattribute= %UserName%, ou=people, dc=computer</li> </ul> (where namingattribute can be any string). <p><b>Note:</b> Usually, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.</p>	Yes		string/string
<b>BIND timeout</b> AUI\LDAPauth: Timeout	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
<b>Alternate user ID location</b> AUI\LDAPauth: UserLocation	Use to indicate where to locate a user object when the user validates against an attribute other than the username. <p><b>Example:</b> If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in:</p> <ul style="list-style-type: none"> <li>ou=people,dc=computer</li> <li>then set UserLocation to:</li> <li>empid=%user,ou=people,dc=computer</li> </ul> instead of to: <ul style="list-style-type: none"> <li>uid=user,ou=people,dc=computer.</li> </ul> <p><b>Note:</b> For Novell eDirectory, UserLocation should be:</p> <ul style="list-style-type: none"> <li>uid=%user,path to the object.</li> </ul> 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
<b>Enable Domain name support</b> 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
<b>Default Domain name</b> 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
<b>Window title</b> AUI\LDAP:WindowTitle	Use this setting to customize the Window title name for this authenticator. <b>Note:</b> This entry is not required.	Yes		string/string
<b>Password change window title</b> AUI\LDAPauth: CAP_WindowTitle	Use this setting to customize the Active Directory Change Password Window title name for this synchronizer. <b>Note:</b> This entry is not required.	Yes		string/string
<b>Password change window subtitle</b> AUI\LDAPauth: CAP_WindowSubTitle	Use this setting to customize the Active Directory Change Password Window subtitle name for this synchronizer. <b>Note:</b> This entry is not required.	Yes		string/string
<b>Custom image for authentication prompt</b> AUI\LDAP:ImagePath	Fully-qualified path and filename of the image file.	No		string/filename
<b>Show user path</b> 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
<b>Share credentials with other authenticators</b> AUI\LDAP: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." <b>Note:</b> For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.	Yes		string/string
<b>Share credentials with synchronizers</b> AUI\LDAP: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." <b>Note:</b> 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
<b>Naming attribute string</b> AUI\LDAP:UserPrepend	String to prepend to UserPaths when the DN for a user is in the form of: <ul style="list-style-type: none"> <li>• cn=%UserName%,ou=people,dc=computer</li> <li>• instead of the form:</li> <li>• namingattribute=%UserName%, ou=people,dc=computer</li> </ul> (where namingattribute can be any string). <b>Note:</b> 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
<b>BIND timeout</b> AUI\LDAP:Timeout	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
<b>Alternate user ID location</b> AUI\LDAP:UserLocation	Use to indicate where to locate a user object when the user validates against an attribute other than the username. <b>Example:</b> If users authenticate with an employee ID# for logon (validation against the empid attribute) and the user object is in: <ul style="list-style-type: none"> <li>• ou=people,dc=computer</li> <li>• then set UserLocation to:</li> <li>• empid=%user,ou=people,dc=computer</li> </ul> instead of to: <ul style="list-style-type: none"> <li>• uid=user,ou=people,dc=computer.</li> </ul> <b>Note:</b> For Novell eDirectory, UserLocation should be: <ul style="list-style-type: none"> <li>• uid=%user,path to the object.</li> </ul> If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string
<b>Enable directory search for users</b> 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
<b>Smart card library</b> 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. <b>Note:</b> Set this to PKCS # 11 only if using SafeSign/ RaakSign middleware.	Yes	0-CSP (Default) 1-PKCS#11	dword/Ø
<b>Use default certificate for authentication</b> 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
<b>Store synchronization credentials</b> 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
<b>Store the PIN</b> 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
<b>PKCS#11 Library Path</b> AUI\SCAuth:PKCS11Path	Use this setting to configure the path to the smart card middleware file, which implements the PKCS#11 standard. <b>Note:</b> 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

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

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Window title</b> AUI\SCauth:WindowTitle	Use this setting to customize the Window title name for this authenticator.	Yes		string/string
<b>Window subtitle</b> 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
<b>Recovery method</b> AUI\SCAuth: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
<b>Recovery certificate object identifier</b> 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.  <b>Note:</b> You must set the "Recovery method" option to "Encryption certificate." This entry is not required.	Yes		string/string

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

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Store synchronization credentials</b> AUI\ROSCAuth: StoreSyncCreds	Configures whether to store the user's synchronization repository credentials using Secure Data Storage.  <b>Note:</b> You must enable and configure Secure Data Storage.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>PKCS#11 Library Path</b> AUI\ROSCAuth: PKCS11Path	Use this setting to configure the path to the smart card middleware file, which implements the PKCS#11 standard.  <b>Note:</b> 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

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

Display Name/ Registry Path	Description Text	Overridable	Options/ Default	RegType/ DataType
<b>Recovery method</b> 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
<b>Recovery certificate object identifier</b> 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.  <b>Note:</b> 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
<b>Card family</b> AUI\ProxCardAuth: ProximityCardFamily	Configures the proximity card family type.	Yes	0-HID ISO / DUO PROX (Default) 1-iClass 2-Indala / EM	dword/Ø
<b>Reader type</b> 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
<b>Second factor authentication</b> 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
<b>Minimum length</b> AUI\ProxCardAuth: MinPINLength	Configures the minimum length of the user-defined PIN.	Yes		dword/int
<b>Maximum length</b> AUI\ProxCardAuth: MaxPINLength	Configures the maximum length of the user-defined PIN.	Yes		dword/int
<b>Maximum retries</b> AUI\ProxCardAuth: RetryPINCount	Configures the number of PIN attempts before the authentication fails.	Yes		dword/int
<b>Alphanumeric constraints</b> 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
<b>Enable data storage</b> DataStorage:Passlogix SecureDataStorage	Configures whether to store users' synchronization credentials securely within the repository.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>Data storage location</b> 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
<b>Synchronizer order</b> 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.  <b>Examples:</b> LDAPExt,ADExt FileSync Remote,AD,FileSync Local,SmartCard MySmartCard,ADExt,ADExtRemote	Yes		string/ synchronizers
<b>Use configuration objects</b> 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
<b>Allow disconnected operation</b> 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
<b>Delete local cache</b> 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
<b>Deleted credential cleanup</b> 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
<b>Location of entlist.ini file</b> 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
<b>Wait for synchronization at startup</b> 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.  <b>Note:</b> 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
<b>Interval for automatic resynchronization</b> 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
<b>Optimize synchronization</b> 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
<b>Use aggressive synchronization</b> 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).  <b>Note:</b> This feature can have a significant performance impact on both client and server computers.	Yes	0-No (Default) 1-Yes	dword/Ø
<b>Resynchronize when network or connection status changes</b> 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
<b>ADAM Sync DLL location</b> 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
<b>Base location(s) for configuration objects</b> 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: <ul style="list-style-type: none"> <li>OU=SSOConfig,DC=Domain,DC=com</li> </ul> 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
<b>Prepend Domain when naming objects</b> Extensions\SyncManager\ Syncs\%ADAM%: AppendDomain	Enables prepending of the user's Domain to the username in naming the user's container. <p><b>Example:</b> For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled.</p>	Yes	0-No (Default) 1-Yes	dword/Ø
<b>User Domain name to use</b> 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. <p><b>Example:</b> 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.</p>	Yes		string/string



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

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Credentials to use</b> 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
<b>Prompt when disconnected</b> 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
<b>Servers</b> 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.  <b>Examples:</b> <ul style="list-style-type: none"> <li>• Adam1.company.com</li> <li>• Adam2.company.com</li> <li>• Adam3.company.com:50389</li> </ul>	No		string/string
<b>Use SSL</b> 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
<b>Descriptive name</b> Extensions\SyncManager\ Syncs\%ADAM%:DisplayName	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name.	Yes		string/string
<b>Password change window title</b> Extensions\SyncManager\ Syncs\%ADAM%: CAP_WindowTitle	Use this setting to customize the ADAM Change Password Window title name for this synchronizer.	Yes		string/string
<b>Password change window subtitle</b> 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
<b>Share credentials with authenticators</b> Extensions\SyncManager\ Syncs\%ADAM%: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth."  <b>Note:</b> 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
<b>AD Sync DLL location</b> 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	Reg Type/ DataType
<b>Base location(s) for configuration objects</b> 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: <ul style="list-style-type: none"> <li>• OU=SSOConfig,DC=Domain,DC=com</li> </ul> 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/∅
<b>Location for storing user credentials</b> 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/∅
<b>Prepend Domain when naming objects</b> Extensions\SyncManager\ Syncs\%AD%:AppendDomain	Enables prepending of the user's Domain to the username in naming the user's container. <p><b>Example:</b> For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled.</p> <p><b>Note:</b> 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.</p>	Yes	0-No (Default) 1-Yes	dword/∅

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

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Credentials to use</b> 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
<b>Prompt when disconnected</b> 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
<b>Servers</b> 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.  <b>Example:</b> <ul style="list-style-type: none"> <li>• DC1.company.com</li> <li>• DC2.company.com</li> <li>• company.com:8080</li> <li>• companylab.com</li> </ul> <b>Note:</b> 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
<b>User Paths</b> 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.  <b>Note:</b> This entry is not required for this extension.	Yes		string/Ø
<b>Use SSL</b> 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
<b>Logon attempts</b> 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
<b>Descriptive name</b> Extensions\SyncManager\ Syncs\%AD%:DisplayName	Logon dialog title, to help differentiate between multiple synchronizer extensions having the same name.	Yes		string/string
<b>Password change window title</b> 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
<b>Password change window subtitle</b> 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
<b>Share credentials with authenticators</b> Extensions\SyncManager\ Syncs\%AD%: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth."  <b>Note:</b> 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
<b>Limit search to server root</b> 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
<b>DB Sync DLL location</b> Extensions\SyncManager\ Syncs\%DB%:Path	Path\filename of the Database synchronizer extension.	No	(Default-%INSTALLDIR% Plugin\ SyncMgr\ DBEXT\ DBExt.dll)	string/string
<b>Servers</b> Extensions\SyncManager\ Syncs\%DB%\Servers: Server	List of servers to try, entered one per line using full connection strings. <b>Note:</b> You must specify at least one server for this extension to work.	No		string/string
<b>Append Domain when naming objects</b> Extensions\SyncManager\ Syncs\%DB%:AppendDomain	Enables appending of the user's Domain to the username in naming the user's container. <b>Example:</b> 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
<b>File Sync DLL location</b> 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
<b>Prepend Domain when naming user folders</b> Extensions\SyncManager\ Syncs\%File%: AppendDomain	Enables prepending of the user's Domain to the username in naming the user's container. <b>Example:</b> 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
<b>Prompt when disconnected</b> 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
<b>Server</b> Extensions\ SyncManager\ Syncs\%File%\Servers: Server1	UNC path to try. <b>Examples:</b> <ul style="list-style-type: none"> <li>• \\FS1\Users</li> <li>• \\FS2\Extras</li> <li>• D:\Backup</li> </ul> <b>Note:</b> 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
<b>Logon attempts</b> 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
<b>Descriptive name</b> Extensions\SyncManager\ Syncs\%File%: DisplayName	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name. <b>Note:</b> This entry is not required.	Yes		string/string

**Screen/Display Path:**  
**Synchronization\%LDAP%**

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

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

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Base location(s) for configuration objects</b> 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: <ul style="list-style-type: none"> <li>• OU=SSOConfig,DC=Domain,DC=com</li> </ul> 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
<b>Prompt when disconnected</b> 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
<b>Directory type</b> 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
<b>Servers</b> 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.  <b>Examples:</b> <ul style="list-style-type: none"> <li>• LDAP1.company.com</li> <li>• LDAP2.company.com</li> <li>• LDAP3.company.com:50389</li> </ul>	No		string/Ø
<b>User paths</b> 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.  <b>Example:</b> <ul style="list-style-type: none"> <li>• OU=Users,DC=Domain,DC=com</li> </ul> <b>Note:</b> You must specify at least one value for UserPath for this extension to work.	Yes		string/Ø
<b>Use SSL</b> 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
<b>Administrative group DN</b> Extensions\SyncManager\ Syncs\%\LDAP%\AdminGroup	DN for the Administrative group. It is placed this value in the ACI.  <b>Examples:</b> <ul style="list-style-type: none"> <li>• cn=configuration administrators, ou=groups,</li> <li>• ou=topologymanagement, o=netscaperoot</li> </ul>	Yes		string/string
<b>Security version</b> 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
<b>Descriptive name</b> Extensions\SyncManager\ Syncs\%\LDAP%\DisplayName	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name.  <b>Note:</b> This entry is not required.	Yes		string/string
<b>Show user path</b> 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
<b>Logon attempts</b> 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	Reg Type/ DataType
<p><b>Share credentials with authenticators</b></p> <p>Extensions\SyncManager\ Syncs\%LDAP%: ShareCredsToAuths</p>	<p>Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth."</p> <p><b>Note:</b> For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.</p>	<p>Yes</p>		<p>string/Ø</p>

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

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Naming attribute string</b>  Extensions\ SyncManager\ Syncs\%LDAP%: UserPrepend	String to prepend to UserPaths when the DN for a user is in the form of: <ul style="list-style-type: none"> <li>cn=%UserName%,ou=people,dc=computer</li> </ul> instead of the form: <ul style="list-style-type: none"> <li>namingattribute=%UserName%,ou=people,dc=computer</li> </ul> (where namingattribute can be any string).  <b>Note:</b> 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
<b>BIND timeout</b>  Extensions\ SyncManager\ Syncs\%LDAP%:Timeout	Timeout (in milliseconds) of LDAP BIND call.	Yes	(Default depends on the operating system)	dword/int
<b>BIND user DN</b>  Extensions\ SyncManager\ Syncs\%LDAP%: BindUserName	Specifies LDAP "browse only" account user DN. This must be in the format: <ul style="list-style-type: none"> <li>"uid=%username%, ou=people, dc=%CompanyName%"</li> </ul> (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
<b>BIND user password</b>  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
<b>Alternate user ID location</b> Extensions\ SyncManager\ Syncs\%LDAP%: UserLocation	Specifies where to locate a user object when the user validates against an attribute other than the username. <b>Example:</b> If users authenticate with an employee ID # for logon (validation against the empid attribute) and the user object is in: <ul style="list-style-type: none"> <li>ou=people,dc=computer,</li> <li>set UserLocation to:</li> <li>empid=%user,ou=people,dc=computer</li> </ul> instead of to <ul style="list-style-type: none"> <li>uid=user,ou=people,dc=computer.</li> </ul> <b>Note:</b> For Novell eDirectory, UserLocation should be: <ul style="list-style-type: none"> <li>uid=%user,path to the object.</li> </ul> If using UserLocation, do not use UserPrepend or UserPaths.	Yes		string/string
<b>Enable directory search for users</b> 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
<b>Roaming Sync DLL location</b> 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
<b>Store user data on disk in encrypted file</b> 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
<b>Default encryption algorithm</b> CSP:PreferredCSP	Select the default encryption algorithm from the dropdown menu.  <b>Note:</b> 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
<b>Reauthentication timer</b> 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.  <b>Note:</b> 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
<b>Require reauthentication before updating account credentials</b> 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
<b>Obfuscate length</b> 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
<b>Allow revealing</b> Extensions\AccessManager: AllowReveal	Specifies whether the user is permitted to reveal masked fields.	Yes	0-No 1-Yes (Default)	dword/Ø
<b>Require reauthentication to reveal</b> 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
<b>After Agent starts</b> Shell\Tasks:StartupTaskN	Command(s) that will run every time the background task starts (the Tray Icon appears).	Yes		string/Ø
<b>Before Agent starts</b> 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.  <b>Note:</b> 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
<b>When logons are deleted</b> Shell\Tasks:DeletionTaskN	Command(s) that will run every time a user deletes an application configuration.	Yes		string/Ø
<b>When logons change (add, delete, copy, modify)</b> 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
<b>Cache limit</b> Extensions\EventManager\CacheLimit	Maximum number of event log entries to be cached before old events are discarded.	Yes	(Default-200)	dword/int
<b>Retry interval</b> Extensions\EventManager\Retry	Interval (in minutes) between retries for all Event Logging extensions. <b>Note:</b> 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
<b>Connection string</b> 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
<b>Stored procedure</b> 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
<b>Batch size</b> Reporting:BatchSize	Number of events to send to Reporting extensions in one batch.	Yes	(Default-100)	dword/int
<b>Cache limit</b> Reporting:CacheLimit	Maximum number of reporting events to cache before discarding old events.	Yes	(Default-4294967295, or 0xFFFFFFFF)	dword/int
<b>Retry interval</b> 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	Reg Type/ DataType
<b>Windows event logging server</b> 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
<b>Retry interval</b> Extensions\EventManager\ WindowsEvent:Retry	Interval (in minutes) between retries for the Windows Event Logging extension.	Yes	(Default-30)	dword/int
<b>Events to log</b> 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
<b>Destination host</b> 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
<b>Destination port</b> Extensions\EventManager\ Syslog:RemotePort	Sets the destination port for syslog messages using a number.	Yes	(Default-1468)	dword/int
<b>Protocol for sending messages</b> Extensions\EventManager\ Syslog:UseTCP	Specifies whether to send messages via TCP or UDP protocol.  <b>Note:</b> 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
<b>Retry interval</b> 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
<p><b>Events to log</b></p> <p>Extensions\EventManager\ Syslog:Filter</p>	<p>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.</p>	<p>Yes</p>	<p>(Default-0)</p> <p>4-Credential Edit</p> <p>8-Credential Delete</p> <p>10-Credential Copy</p> <p>20-Credential Add</p> <p>100-Provisioning</p> <p>200-Startup/Shutdown</p> <p>400-Help</p> <p>800-Settings Change</p> <p>1000-Reauthentication</p> <p>10000-Sync User Information</p> <p>20000-Logon Field: System Username</p> <p>40000-Logon Field: System Domain</p> <p>80000-Logon Field: Third Field</p> <p>100000-Logon Field: Username</p> <p>200000-Logon Field: Fourth Field</p> <p>800000-Application Password Change</p> <p>1000000-Primary Logon Method Change</p> <p>4000000-Backup/Restore</p> <p>40000000-Event Types: Info</p>	<p>dword/Ø</p>

**Screen/Display Path:  
Audit Logging\XML File**

Display Name/ Registry Path	Description	Overridable	Options/ Default	RegType/ DataType
<b>Retry interval</b> Extensions\EventManager\ LocalStorage:Retry	Interval (in minutes) between retries for the Local (XML) File Logging extension.	Yes	(Default-30)	dword/int
<b>Events to log</b> 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
<b>Servers</b> 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
<b>Default server</b> 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
<b>Default table</b> Extensions\EventManager\ Database:Default Table	If no other table is specified, the table to which the database log will be written.	Yes		string/string
<b>Retry interval</b> 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
<p><b>Events to log</b></p> <p>Extensions\EventManager\ Database:Filter</p>	<p>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.</p>	<p>Yes</p>	<p>(Default-0)</p> <p>4-Credential Edit</p> <p>8-Credential Delete</p> <p>10-Credential Copy</p> <p>20-Credential Add</p> <p>100-Provisioning</p> <p>200-Startup/Shutdown</p> <p>400-Help</p> <p>800-Settings Change</p> <p>1000-Reauthentication</p> <p>10000-Sync User Information</p> <p>20000-Logon Field: System Username</p> <p>40000-Logon Field: System Domain</p> <p>80000-Logon Field: Third Field</p> <p>100000-Logon Field: Username</p> <p>200000-Logon Field: Fourth Field</p> <p>800000-Application Password Change</p> <p>1000000-Primary Logon Method Change</p> <p>4000000-Backup/Restore</p> <p>40000000-Event Types: Info</p>	<p>dword/Ø</p>

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

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



Display Name/ Registry Path	Description	Overridable	Options / Default	RegType/ DataType
<b>Field7</b> Extensions\EventManager\ Database\EventFields:Field7	ComputerName	Yes	(Default-Computer name)	string/string
<b>Field8</b> Extensions\EventManager\ Database\EventFields:Field8	SSOSyncUser	Yes	(Default-SSO synchronization user)	string/string
<b>Field9</b> Extensions\EventManager\ Database\EventFields:Field9	Customizable for your needs.	Yes	Open	string/string
<b>Field10</b> 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
<b>Allow administrator to close Kiosk Manager</b> 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
<b>Number of times to process termination</b> 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
<b>Timeout for locked session</b> 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
<b>Maximum number of sessions</b> 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
<b>Track memory consumption</b> 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
<b>Use cached credentials</b> 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
<b>Storage path</b> 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
<b>Expiration date</b> 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
<b>Lock session on smart card removal</b> 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
<b>Lock session on read-only smart card removal</b> 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
<b>Pre-populate on startup</b> SM\Agent:Prepopulate	Specifies when to 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
<b>Event log name</b> SM\Agent:EventLogName	Enter the name of the Windows event log for Kiosk Manager events.	Yes	(Default-Application)	string
<b>Event log machine name</b> 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
<b>Allow computer restart</b> SM\Agent:AllowRestart	Specifies whether to enable the restart computer option in the Desktop Manager. <b>Note:</b> 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
<b>Allow computer shutdown</b> SM\Agent:AllowShutdown	Specifies whether to enable the shutdown computer option in the Desktop Manager. <b>Note:</b> 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
<b>Show confirmation message when restarting kiosk</b> 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
<b>Show confirmation message when shutting down kiosk</b> 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
<b>Lock session when screen saver times out</b> 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
<b>Timeout for authentication prompt</b> 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
<b>Show desktop status window</b> SM\Agent:DisplayDesktopStatus	Specifies whether to show the optional window that displays the current session owner.	Yes	0-No (Default) 1-Yes	dword
<b>X coordinate</b> SM\Agent:DesktopStatusX	Enter the X coordinate (horizontal location) for the status window.	Yes	(Default-0)	dword/int
<b>Y coordinate</b> 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
<b>Use transparent lock</b> 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
<b>Delay period</b> SM\Agent:TransparentLockTime	Specifies the number of seconds to wait for mouse and keyboard inactivity before showing the desktop.	Yes	(Default-5)	dword/int
<b>Ignore delay period if authentication is canceled</b> 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
<b>Only recognize Ctrl-Alt-Del</b> 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
<b>Location of image file</b>  SM\Agent\Desktop: LogoPath	Fully-qualified path and filename of the image file.	Yes		string/filename
<b>X coordinate</b>  SM\Agent\Desktop: LogoX	Enter the X coordinate (horizontal location) for the image.  <b>Note:</b> Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
<b>Y coordinate</b>  SM\Agent\Desktop: LogoY	Enter the Y coordinate (vertical location) for the image.  <b>Note:</b> Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
<b>Width</b>  SM\Agent\Desktop: LogoWidth	Enter the width of the image (in pixels).	Yes	(Default-300)	dword/int
<b>Height</b>  SM\Agent\Desktop: LogoHeight	Enter the height of the image (in pixels).	Yes	(Default-300)	dword/int
<b>Placement behavior</b>  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 clip 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
<b>Message text</b> 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
<b>Name</b> SM\Agent\Desktop: MOTDFontName	Specifies the Text Message font.	Yes		string/font
<b>Size</b> SM\Agent\Desktop: MOTDFontSize	Specifies the Text Message font size.	Yes	(Default-0)	dword/int
<b>Style</b> 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
<b>Background</b> SM\Agent\Desktop: MOTDBackColor	Specifies the Text Message background color.	Yes		string/color
<b>Foreground</b> 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
<b>X coordinate</b> 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. <b>Note:</b> Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
<b>Y coordinate</b> 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. <b>Note:</b> Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Yes	(Default-0)	dword/int
<b>Width</b> SM\Agent\Desktop: MOTDWidth	Specifies the width of the Text Message (in pixels).	Yes	(Default-300)	dword/int
<b>Height</b> SM\Agent\Desktop: MOTDHeight	Specifies the height of the Text Message (in pixels).	Yes	(Default-300)	dword/int
<b>Size automatically</b> 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	<ul style="list-style-type: none"> <li>• Default Backup path</li> </ul>
Password Change\Required	<ul style="list-style-type: none"> <li>• Credential Sharing Groups</li> </ul>
Password Change\Advanced	<ul style="list-style-type: none"> <li>• Notify Primary Logon Method</li> </ul>
Response\Error Loop	<ul style="list-style-type: none"> <li>• Maximum retries before prompting</li> <li>• Maximum time for retries before prompting</li> <li>• Require password confirmation when modifying password</li> </ul>
Response\ Host/Mainframe Apps	<ul style="list-style-type: none"> <li>• Host/Mainframe support</li> </ul>
Response\Host/Mainframe Apps\Error Loop	<ul style="list-style-type: none"> <li>• Maximum retries before prompting</li> <li>• Maximum time for retries before prompting</li> <li>• Require password confirmation when modifying password</li> </ul>
Response\Web Apps\Error Loop	<ul style="list-style-type: none"> <li>• Maximum retries before prompting</li> <li>• Maximum time for retries before prompting</li> <li>• Require password confirmation when modifying password</li> </ul>
Response\Windows Apps	<ul style="list-style-type: none"> <li>• Ignored Window Classes for Applications</li> <li>• Retry for a Window Title Match</li> <li>• Supported Window Classes for Applications</li> <li>• Supported Window Classes for Services</li> </ul>
Response\Windows Apps\Error Loop	<ul style="list-style-type: none"> <li>• Maximum retries before prompting</li> <li>• Maximum time for retries before prompting</li> <li>• Require password confirmation when modifying password</li> </ul>
Advanced\Performance	<ul style="list-style-type: none"> <li>• Increase user data storage priority</li> <li>• Maximum time before forced SSO process shut down</li> <li>• Set delay for first update (after startup) to stored user data</li> <li>• Set delay for storing user data</li> </ul>

### Event Logging Node

Sub-Node Path	Removed Settings
	<ul style="list-style-type: none"> <li>Select events to log</li> </ul>
Reporting	<ul style="list-style-type: none"> <li>Extension location</li> </ul>
Database	<ul style="list-style-type: none"> <li>Extension location</li> </ul>
Syslog	<ul style="list-style-type: none"> <li>Extension location</li> </ul>
Windows Event Viewer\Advanced	<ul style="list-style-type: none"> <li>Extension location</li> </ul>
XML File	<ul style="list-style-type: none"> <li>Extension location</li> </ul>
Advanced	<ul style="list-style-type: none"> <li>Event Server Message Library location</li> <li>Extension location</li> <li>Shutdown Delay</li> <li>Shutdown Immediately</li> </ul>

### Primary Logon Methods Node

Sub-Node Path	Removed Settings
LDAP\Advanced	<ul style="list-style-type: none"> <li>SSL Fallback</li> </ul>
LDAP v2\Advanced	<ul style="list-style-type: none"> <li>Passphrase</li> <li>When SSL fails</li> </ul>
Windows v2\ Advanced	<ul style="list-style-type: none"> <li>Passphrase</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  As of version 11.1.1.5.0, Passphrase options are available under Authentication &gt; Windows v2 &gt; Passphrase.                 </div>

### Reporting Node

Sub-Node Path	Removed Settings
Database	<ul style="list-style-type: none"> <li>Extension location</li> </ul>

**Synchronization Node**

<b>Sub-Node Path</b>	<b>Removed Settings</b>
%AD%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>
%AD%\Advanced	<ul style="list-style-type: none"> <li>• Search for locator and override objects</li> <li>• When SSL fails</li> </ul>
%ADAM%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>
%ADAM%\Advanced	<ul style="list-style-type: none"> <li>• When SSL fails</li> </ul>
%DB%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>
%File%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>
%LDAP%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>
%LDAP%\Advanced	<ul style="list-style-type: none"> <li>• DSAME disabled-account support</li> <li>• When SSL fails</li> </ul>
%ROAM%\Required	<ul style="list-style-type: none"> <li>• Extension location</li> </ul>

## 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 ( <i>User Experience</i> )	Title Bar Button Menu	Do not show
End-User Experience ( <i>User Experience</i> )\Password Change\Required	Credential Sharing Groups	Enabled
End-User Experience ( <i>User Experience</i> )\Response\Error Loop	Maximum retries before prompting	0
End-User Experience ( <i>User Experience</i> )\Response\Host/Mainframe Apps\Error Loop	Maximum retries before prompting	0
End-User Experience ( <i>User Experience</i> )\Response\Web Apps	Scroll Into View	Disabled
End-User Experience ( <i>User Experience</i> )\Response\Web Apps\Error Loop	Maximum retries before prompting	0
End-User Experience ( <i>User Experience</i> )\Response\Windows Apps\Error Loop	Maximum retries before prompting	0
Primary Logon Methods ( <i>Authentication</i> )\LDAP\Required	SSL	Do not use SSL
Primary Logon Methods ( <i>Authentication</i> )\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

## 1

16-bit screen capture attempts, Host/Mainframe Application Response. . . . . 14

## A

Activate tab, Web Applications Behavior. . . . . 10

### Active Directory

LDAP Authentication. . . . .	31
Default Domain name. . . . .	31
Enable Domain name support. . . . .	31
Synchronization. . . . .	42
AD Sync DLL location. . . . .	42
Connection information. . . . .	44
Credentials to use. . . . .	44
Logon attempts. . . . .	44
Prompt when disconnected. . . . .	44
Servers. . . . .	44
Use SSL. . . . .	44
User paths. . . . .	44
Credential sharing. . . . .	45
Share credentials with authenticators. . . . .	45
Data storage configuration. . . . .	43
Base location(s) for configuration objects. . . . .	43
Location for storing user credentials. . . . .	43
Prepend Domain when naming objects. . . . .	43
File mode configuration. . . . .	45
Limit search to server root. . . . .	45
User interface. . . . .	45
Descriptive name. . . . .	45
Password change window subtitle. . . . .	45
Password change window title. . . . .	45
AD Sync DLL location, AD Synchronization settings. . . . .	42

### ADAM

Connection information	
Prompt when disconnected. . . . .	41
Synchronization. . . . .	39
Connection information	
Credentials to use. . . . .	41
Servers. . . . .	41
Synchronization. . . . .	41
Use SSL. . . . .	41
Credential sharing. . . . .	42
Share credentials with authenticators. . . . .	42
Data storage configuration	
Base location(s) for configuration objects. . . . .	40
Prepend Domain when naming objects. . . . .	40
User Domain name to use. . . . .	40
Sync DLL location. . . . .	39
User interface	
Descriptive name. . . . .	42
Password change window subtitle. . . . .	42
Password change window title. . . . .	42
ADAM Synchronization, User interface. . . . .	42
Administrative group DN, LDAP Synchronization Administrative security. . . . .	50
Administrative security, LDAP Synchronization. . . . .	50
After Agent starts, Custom Actions. . . . .	56
All application types, Initial Credential Capture, Limit response to predefined applications for. . . . .	9
Allow administrator to close Kiosk Manager. . . . .	66
Allow computer restart, Kiosk Manager. . . . .	68
Allow computer shutdown, Kiosk Manager. . . . .	68
Allow creating multiple accounts during credential capture, Initial Credential Capture. . . . .	8
Allow disconnected operation, Synchronization Options. . . . .	38
Allow fallback from control IDs to SendKeys, Windows Applications. . . . .	11
Allow refresh in My Accounts, User Interface. . . . .	17
Allow revealing of masked fields. . . . .	55

Allow user to exclude accounts from credential sharing groups, Password change behavior..... 15

Allowed character sets, Password change..... 16

Allowed dynamic Web pages, Web Applications Response control..... 11

Allowed number of authenticators, Authentication Manager..... 19

Allowed Web pages, Initial Credential Capture, Limit response to predefined applications for..... 9

Alphanumeric constraints

- Proximity Card Authentication PIN..... 37

Alternate user ID location

- LDAP Authentication Connection information..... 30, 33
- LDAP Synchronization Special Purpose..... 53
- LDAP v2 Authentication Special Purpose..... 29

Always show for, User Experience Title bar button..... 6

Append Domain when naming objects, Database Synchronization..... 46

Application Response, User Experience..... 7

Applications that hooks should ignore, User Experience Application Response..... 7

Applications to ignore, Web Applications Response control..... 11

AppName, Database Event Fields Audit Logging..... 64

Audit Logging..... 57

- Database..... 62
  - Default server..... 62
  - Default table..... 62
- Event Fields..... 64
  - AppName..... 64
  - Category..... 64
  - Field10..... 65
  - Field2..... 64
  - Field3..... 64
  - Field4..... 64
  - Field5..... 64
  - Field6..... 64
  - Field7..... 65
  - Field8..... 65

- Field9..... 65
- Numbered Fields..... 64
- TimeStamp..... 64
- Type..... 64
- Events to log..... 63
- Retry interval..... 62
- Servers..... 62

Reporting Server

- Batch size..... 57
- Cache limit..... 57
- Options..... 57
  - Retry interval..... 57
- Retry interval..... 57

Syslog Server..... 59

- Destination host..... 59
- Destination port..... 59
- Events to log..... 60
- Protocol for sending messages..... 59
- Retry interval..... 59

Windows Event Viewer..... 58

- Events to log..... 58
- Retry interval..... 58
- Windows event logging server..... 58

XML File..... 61

- Events to log..... 61
- Retry interval..... 61

Audit Logging Settings

- Cache limit..... 57
- Kiosk Manager..... 68
- Reporting Server Database Connection string..... 57
- Reporting Server Database Stored procedure..... 57

Authentication..... 19

- Authentication Manager..... 19
  - Allowed number of authenticators..... 19
  - Enrollment
    - Entrust..... 21

LDAP v2.....	20
Proximity card.....	21
Read-only smart card.....	20
RSA SecurID.....	21
Smart card.....	20
Windows.....	20
Windows v2.....	20
Grade.....	22
Entrust.....	22
LDAP.....	22
LDAP v2.....	22
Proximity card.....	22
Read-only smart card.....	22
RSA SecurID.....	22
Smart card.....	22
Windows.....	22
Windows v2.....	22
Order.....	23
Entrust.....	23
LDAP.....	23
LDAP v2.....	23
Proximity card.....	23
RSA SecurID.....	23
Smart card.....	23
Windows v2.....	23
LDAP	
Active Directory.....	31
Default Domain name.....	31
Enable Domain name support.....	31
Connection information.....	30
BIND timeout.....	30
Naming attribute string.....	30
Credential sharing.....	32
Share credentials with other authenticators.....	32
Share credentials with synchronizers.....	32

Special Purpose.....	33
Alternate user ID location.....	33
BIND timeout.....	33
Enable directory search for users.....	33
User interface.....	31
LDAP v2	
Connection information.....	27
Servers.....	27
Credential sharing.....	28
Include in LDAP credential sharing group.....	28
Share credentials with other authenticators.....	28
Share credentials with synchronizers.....	28
Special Purpose.....	29
BIND timeout.....	29
Naming attribute string.....	29
User interface.....	28
Include in LDAP credential sharing group.....	28
Share credentials with other authenticators.....	28
Share credentials with synchronizers.....	28
LDAP v2 Connection information	
Use SSL.....	27
User paths.....	27
Proximity Card	
Options.....	36
Card family.....	36
Reader type.....	36
PIN settings.....	36-37
Alphanumeric constraints.....	37
Maximum length.....	37
Maximum retries.....	37
Minimum length.....	37
Read-Only Smart Card	
Options.....	35
PKCS#11 Library Path.....	35
Store synchronization credentials.....	35

Recovery.....	36
Recovery certificate object identifier.....	36
Recovery method.....	36
Secure Data Storage.....	37
Data storage location.....	37
Enable data storage.....	37
Smart Card	
Options.....	34
PKCS#11 Library Path.....	34
Smart card library.....	34
Store synchronization credentials.....	34
Store the PIN.....	34
Use default certificate for authentication.....	34
Recovery.....	35
Recovery certificate object identifier.....	35
Recovery method.....	35
User interface.....	34
Window subtitle.....	34
Window title.....	34
Windows	
Credential sharing.....	27
Share credentials with other authenticators.....	27
Share credentials with synchronizers.....	27
User interface.....	26
Custom image for authentication prompt.....	26
Window subtitle.....	26
Window title.....	26
Windows Authentication	
User interface	
Require old password when Windows password changes.....	26
Windows v2	
Credential sharing.....	25
Include in Domain credential sharing group.....	25
Share credentials with other authenticators.....	25
Share credentials with synchronizers.....	25

Passphrase	
Options.....	26
Force password re-enrollment when using old password to reset.....	26
Minimum length.....	26
Reset with old password.....	26
User can change passphrase.....	26
User interface.....	25
Checkbox label.....	25
Message.....	25
Message dialog title.....	25
Recovery.....	24
Recovery method.....	24
Use Windows Data Protection (DPAPI).....	24
User interface.....	24
Custom image for authentication prompt.....	24
Reauthentication dialog.....	24
Window title.....	24
Authentication Manager	
Enrollment.....	20
Grade.....	22
Order.....	23

**B**

Background color, Kiosk Manager Text Message.....	71
Background Image, Kiosk Manager User Interface.....	70
Base location(s) for configuration objects	
AD Data storage configuration.....	43
ADAM Data storage configuration.....	40
LDAP Data storage configuration.....	48
Batch size, Audit Logging Reporting Server, Options.....	57
Before Agent starts, Custom Actions.....	56
Behavior	
Synchronization.....	39



BIND timeout	
LDAP Authentication.....	33
LDAP Authentication Connection information.....	30
LDAP Synchronization Special Purpose.....	52
LDAP v2 Authentication Special Purpose.....	29
BIND user DN, LDAP Synchronization Special Purpose.....	52
BIND user password, LDAP Synchronization Special Purpose.....	52
Border appearance, Web Applications Credential field identification.....	9

**C**

Cache limit	
Audit Logging general settings.....	57
Audit Logging Reporting Server, Options.....	57
Cached credentials expiration date, Kiosk Manager.....	67
Cached credentials, Kiosk Manager.....	67
Card family, Proximity Card Authentication Options.....	36
Category, Database Event Fields Audit Logging.....	64
Change passwords automatically, Password change behavior.....	15
Checkbox label, Windows v2 Authentication Passphrase User interface.....	25
Columns in "Details" view of My Accounts, User Interface.....	17
Columns in Logon Chooser, User Interface.....	18
Component events, Java events to respond to.....	13
Connection information	
File Synchronization.....	47
LDAP Authentication.....	30
LDAP Synchronization.....	49
LDAP v2 Authentication.....	27
Connection string	
Audit Logging Reporting Server, Database.....	57
Credential capture mode, Initial Credential Capture.....	8
Credential field identification, Web Applications Response.....	9
Credential request delay interval, Host/Mainframe Application Response.....	14

Credential sharing	
AD Synchronization.....	45
LDAP Authentication.....	32
LDAP Synchronization.....	51
LDAP v2 Authentication.....	28
Windows Authentication.....	27
Windows v2 Authentication.....	25
Credentials to use	
AD Connection information.....	44
ADAM Connection information.....	41
Custom Actions Settings	
After Agent starts.....	56
Before Agent starts.....	56
When logons are deleted.....	56
When logons change.....	56

**D**

Data storage configuration	
AD Synchronization.....	43
File Synchronization.....	46
LDAP Synchronization.....	48
Data storage location	
Secure Data Storage Authentication.....	37
Database	
Audit Logging.....	62
Event Fields, Audit Logging.....	64
Synchronization.....	46
DB Sync DLL location.....	46
Servers.....	46
Database Event Fields, Numbered	
Database Event Fields Audit Logging.....	64-65
DB Sync DLL location, Database Synchronization.....	46
Default Domain name, Active Directory LDAP Authentication.....	31
Default encryption algorithm, Security.....	54

Default password policy, Password change behavior.....	15
Default table, Database, Audit Logging.....	62
Default Values Modified in version 11.1.1.5.0.....	76
Delay after Java runtime startup, Java Applications Response delays.....	12
Delay between retries, Java Applications Response delays.....	12
Delay period, Kiosk Manager User Interface Transparent screen lock.....	69
Delete local cache, Synchronization Options.....	38
Descriptive name	
AD Synchronization User interface.....	45
ADAM Synchronization User interface.....	42
File Synchronization User interface.....	47
LDAP Synchronization User interface.....	50
Destination host	
Syslog Server, Audit Logging.....	59
Destination port, Syslog Server Audit Logging.....	59
Directory type, LDAP Synchronization Connection information.....	49
Display icon in system tray, User Experience System tray icon.....	6

**E**

Enable Auto-Enter, Initial Credential Capture.....	8
Enable Auto-Prompt, Initial Credential Capture.....	8
Enable Auto-Recognize, Initial Credential Capture.....	8
Enable data storage, Secure Data Storage Authentication.....	37
Enable directory search for users	
LDAP Authentication.....	33
LDAP Synchronization Special Purpose.....	53
Enable Domain name support, Active Directory LDAP Authentication.....	31
Enrollment, Authentication Manager.....	20
Entrust	
Authentication Manager	
Enrollment.....	21
Grade.....	22

Order.....	23
Event Fields, Database, Audit Logging.....	64
Event log machine, Kiosk Manager.....	68
Event log name, Kiosk Manager.....	68
Events to log	
Audit Logging Windows Event Viewer.....	58
Database, Audit Logging.....	63
Syslog Server, Audit Logging.....	60
XML File, Audit Logging.....	61
Excluded Java vendors, Java Applications Exclusions.....	12
Excluded Java versions, Java Applications Exclusions.....	12
Exclusions, Java Applications.....	12

**F**

File mode configuration, AD Synchronization.....	45
File Sync DLL location, File Synchronization.....	46
File Synchronization.....	46
Force password re-enrollment when using old password to reset, Windows v2.....	26
Authentication.....	
Foreground color, Kiosk Manager User Interface Message.....	71

**G**

Grade, Authentication Manager.....	22
------------------------------------	----

**H**

Height	
Kiosk Manager Background Image.....	70
Kiosk Manager Text Message Placement.....	72
Hierarchy events, Java events to respond to	
Hierarchy events.....	13
Host/Mainframe Applications, Application Response.....	14

**I**

Ignore delay period if authentication is canceled, Kiosk Manager User Interface ..... 69

Transparent screen lock ..... 69

Include in Domain credential sharing group, Windows v2 Authentication Credential ..... 25

sharing ..... 25

Include in LDAP credential sharing group, LDAP v2 Authentication ..... 28

Injection type, Java events to respond to ..... 14

Interval for automatic resynchronization, Synchronization Behavior ..... 39

**J**

Java events to respond to, Java Applications ..... 13

**K**

Kiosk Manager Settings ..... 66

    Audit Logging ..... 68

        Event log machine ..... 68

        Event log name ..... 68

    Cached credentials ..... 67

        Expiration date ..... 67

        Storage path ..... 67

        Use cached credentials ..... 67

    Multisession configuration ..... 66

        Maximum number of sessions ..... 66

        Track memory consumption ..... 66

    Session termination ..... 66

        Allow administrator to close Kiosk Manager ..... 66

        Number of times to process termination ..... 66

        Timeout for locked session ..... 66

    Strong authentication options ..... 67

        Lock session on smart card removal ..... 67

        Pre-populate on startup ..... 67

User Interface ..... 68

    Allow computer restart ..... 68

    Allow computer shutdown ..... 68

    Background Image ..... 70

        Height ..... 70

        Location of image file ..... 70

        Placement behavior ..... 70

        Width ..... 70

        X coordinate ..... 70

        Y coordinate ..... 70

    Lock session when screen saver times out ..... 68

    Message Color ..... 71

        Background ..... 71

        Foreground ..... 71

    Message Font ..... 71

        Name ..... 71

    Message Text ..... 71

        Placement ..... 72

            Height ..... 72

            Size automatically ..... 72

            Width ..... 72

            X coordinate ..... 72

            Y coordinate ..... 72

        Size ..... 71

        Style ..... 71

    Show confirmation message when restarting kiosk ..... 68

    Show confirmation message when shutting down kiosk ..... 68

    Status window ..... 69

        Show desktop status window ..... 69

        X coordinate ..... 69

        Y coordinate ..... 69

    Timeout for authentication prompt ..... 68

    Transparent screen lock ..... 69

        Ignore delay period if authentication is canceled ..... 69

        Only recognize Ctrl-Alt-Del ..... 69

Use transparent lock.....69  
 Delay period..... 69

**L**

Language, User Interface.....17

LDAP Authentication

- Authentication Manager Settings
  - Enrollment .....20
  - Grade..... 22
  - Order.....23
- Special Purpose
  - Naming attribute string..... 33
- User interface
  - Custom image for authentication prompt .....31
  - Password change window subtitle..... 31
  - Password change window title.....31
  - Show user path..... 31
  - Window title..... 31

LDAP v2, Authentication Manager Settings

- Enrollment..... 20
- Grade.....22
- Order..... 23

Limit response to predefined applications for..., Initial Credential Capture..... 9

Limit search to server root, AD File mode configuration..... 45

Location for storing user credentials, AD Data storage configuration..... 43

Location of entlist.ini file, Synchronization Options..... 38

Location of image file, Kiosk Manager User Interface Background Image.....70

Lock session
 

- on read-only smart card removal.....67
- on smart card removal, Kiosk Manager..... 67
- when screen saver times out, Kiosk Manager User Interface..... 68

Log on to waiting applications upon Agent startup, Uer Experience Application Response.7

Logon animation's duration, User Interface..... 18

Logon attempts
 

- AD Connection information.....44
- File Synchronization Connection information.....47
- LDAP Synchronization User interface..... 50

Lowercase characters, Password Change Allowed character sets..... 16

**M**

Manual password change behavior..... 15

Masked field security settings..... 55

Maximum length, Proximity Card Authentication PIN settings.....37

Maximum number of sessions, Kiosk Manager..... 66

Maximum retries
 

- credential injection, Java Applications Retry behavior..... 12
- Proximity Card Authentication PIN..... 37

Message
 

- Color, Kiosk Manager User Interface.....71
- dialog title, Windows v2 Authentication Passphrase User interface.....25
- Font, Kiosk Manager User Interface Message.....71
- Placement, Kiosk Manager User Interface.....72
- Text, Kiosk Manager User Interface..... 71
- Windows v2 Authentication Passphrase User interface..... 25
- Windows v2 Passphrase User interface..... 25

Minimum length
 

- Proximity Card Authentication PIN settings.....37
- Windows v2 Authentication Passphrase.....26

Modified Default Values, Appendix 2..... 76

Multisession configuration, Kiosk Manager..... 66

**N**

Naming attribute string
 

- LDAP Authentication..... 33
- LDAP Authentication Connection information.....30

LDAP Synchronization Special Purpose .....52  
 LDAP v2 Authentication ..... 29  
 Node Modifications, Appendix 1 .....73  
 Number of times to process session termination.....66  
 Numeric characters, Password Change Allowed character sets..... 16

**O**

Obfuscate masked field length.....55  
 Only recognize Ctrl-Alt-Del, Kiosk Manager User Interface, Transparent screen lock....69  
 Optimize synchronization, Synchronization Behavior..... 39  
 Order, Authentication Manager..... 23

**P**

Passphrase Options, Windows v2 Authentication..... 26  
 Password change  
   behavior, User Experience Settings ..... 15  
   window subtitle  
     AD Synchronization User interface..... 45  
     ADAM Synchronization User interface..... 42  
     LDAP Authenticator User interface..... 31  
   window title  
     ADAM Synchronization User interface..... 42  
     LDAP Authentication User interface..... 31  
 PIN settings  
   Proximity Card Authentication..... 37  
   Proximity Card Options..... 36  
 PKCS#11 Library Path  
   Read-Only Smart Card Authentication Options..... 35  
   Smart Card Authentication Options.....34  
 Placement behavior, Kiosk Manager User Interface Background Image..... 70  
 Placement, Kiosk Manager User Interface Text Message..... 72  
 Polling interval, Host/Mainframe Applications Response..... 14

Pop-up dialog text after submission, Password change behavior..... 15  
 Pre-populate on startup, Kiosk Manager..... 67  
 Prepend Domain when naming  
   AD Data storage configuration objects.....43  
   ADAM Data storage configuration objects..... 40  
   user folders, File Synchronization Data storage configuration.....46  
 Prohibit canceling the addition of new accounts, Initial Credential Capture..... 8  
 Prohibit disabling the addition of new accounts, Initial Credential Capture..... 8  
 Prohibit excluding accounts from credential sharing groups, Initial Credential Capture... 8  
 Prompt when disconnected  
   AD Connection information.....44  
   ADAM Connection information.....41  
   File Synchronization Connection information.....47  
   LDAP Connection information..... 49  
 Protocol for sending messages, Syslog Server, Audit Logging..... 59  
 Provide dropdown menu, User Experience Title bar button.....6  
 Proximity Card  
   Authentication Manager  
     Enrollment .....21  
     Grade..... 22  
     Order.....23  
   Authentication Options..... 36

**R**

Read-Only Smart Card  
   Authentication Manager  
     Enrollment .....20  
     Grade..... 22  
     Order.....23  
   Authentication Options..... 35  
 Reader type, Proximity Card Authentication Options.....36  
 Reauthentication dialog, Windows v2 Authentication User interface..... 24  
 Reauthentication timer.....54

Recovery	
certificate object identifier	
Smart Card Authentication Recovery.....	35
certificate object identifier, Read-Only Smart Card Authentication.....	36
method, Read-Only Smart Card Authentication.....	36
method, Smart Card Authentication.....	35
Read-Only Smart Card Authentication.....	36
Smart Card authentication.....	35
Windows v2 Authentication.....	24
Removed Settings, Appendix 1.....	73
Reporting Server Options, Audit Logging.....	57
Require old password when Windows password changes, Windows Authentication User interface.....	26
Require reauthentication before upgrading account credentials.....	54
Require reauthentication to reveal masked fields.....	55
Reset with old password, Windows v2 Authentication Passphrase.....	26
Respond to hidden and minimized windows, User Experience Application Response.....	7
Respond to IE modal dialogs, Web Applications Behavior.....	10
Response control, Web Applications.....	11
Response delays, Java Applications.....	12
Resynchronize when network or connection status changes, Synchronization Behavior.....	39
Retry behavior, Java Applications.....	12
Retry interval	
Audit Logging general settings.....	57
Audit Logging Reporting Server Options.....	57
Audit Logging Windows Event Viewer.....	58
Database, Audit Logging.....	62
Syslog Server, Audit Logging.....	59
XML File, Audit Logging.....	61
Roaming Sync DLL location, Roaming Synchronization Required.....	53
Roaming Synchronization, Required.....	53
RSA SecurID	
Authentication Manager	
Enrollment.....	21

Grade.....	22
Order.....	23

**S**

Scroll into view, Web Applications Behavior.....	10
Secure Data Storage, Authentication.....	37
Security Settings	
Default encryption algorithm.....	54
Masked field options	
Allow revealing.....	55
Obfuscate length.....	55
Require reauthentication to reveal.....	55
Reauthentication timer.....	54
Require reauthentication before updating account credentials.....	54
Store user data on disk in encrypted file.....	54
Security version, LDAP Synchronization Administrative security.....	50
Selected authenticator, Setup Wizard.....	18
SendKeys event interval, User Experience Application Response.....	7
Server(s)	
AD Connection information.....	44
ADAM Connection information.....	41
Database Synchronization.....	46
Database, Audit Logging.....	62
Default, Database, Audit Logging.....	62
File Synchronization Connection information.....	47
LDAP Synchronization Connection information.....	49
LDAP v2 Authentication Connection information.....	27
Setup Wizard, User Experience.....	18
Share credentials	
with authenticators, AD Synchronization.....	45
with authenticators, ADAM Synchronization.....	42
with authenticators, LDAP Synchronization.....	51
with other authenticators, LDAP Authentication.....	32
with other authenticators, LDAP v2 Authentication.....	28

with other authenticators, Windows Authentication.....	27
with other authenticators, Windows v2 Authentication.....	25
with synchronizers, LDAP Authentication.....	32
with synchronizers, LDAP v2 Authentication.....	28
with synchronizers, Windows Authentication.....	27
with synchronizers, Windows v2 Authentication.....	25
Show border, Web Applications Credential field identification.....	9
Show confirmation message	
when restarting kiosk, Kiosk Manager User Interface.....	68
when shutting down kiosk, Kiosk Manager User Interface Options.....	68
Show desktop status window, Kiosk Manager User Interface Status window.....	69
Show first-time-use (FTU) wizard, Setup Wizard.....	18
Show system name, User Experience System tray icon.....	6
Show title bar button, User Experience Title bar button.....	6
Show user path	
LDAP Authenticator User interface.....	31
LDAP Synchronization user interface.....	50
Size automatically, Kiosk Manager User Interface Text Message Placement.....	72
Smart Card	
Authentication Manager	
Enrollment.....	20
Grade.....	22
Order.....	23
Authentication Options.....	34
library, Smart Card Authentication Options.....	34
Recovery, Authentication.....	35
Special characters, Password Change Allowed character sets.....	16
Special Purpose	
LDAP Authentication.....	33
LDAP Synchronization.....	52
LDAP v2 Authentication.....	29
Status window, Kiosk Manager User Interface.....	69
Storage path	
Kiosk Manager.....	67

Store synchronization credentials	
Read-Only Smart Card Authentication.....	35
Smart Card Authentication Options.....	34
Store the PIN	
Smart Card Authentication Options.....	34
Store user data on disk in encrypted file.....	54
Stored procedure, Audit Logging Reporting Server, Database.....	57
Strong authentication options, Kiosk Manager.....	67
Synchronization	
AD.....	42
Connection information.....	44
Credential sharing.....	45
Data storage configuration.....	43
File mode configuration.....	45
User interface.....	45
ADAM.....	39
ADAM Sync DLL location.....	39
Base location(s) for configuration objects.....	40
Connection information.....	41
Credential sharing.....	42
Data storage configuration.....	40
User interface.....	42
Behavior.....	39
Interval for automatic resynchronization.....	39
Optimize synchronization.....	39
Resynchronize when network or connection status changes.....	39
Use aggressive synchronization.....	39
Wait for synchronization at startup.....	39
Database.....	46
Append Domain when naming objects.....	46
DBSync DLL location.....	46
Servers.....	46
File.....	46
Connection information.....	47
Logon attempts.....	47

Prompt when disconnected.....	47
Server.....	47
Data storage configuration.....	46
Prepend Domain when naming user folders.....	46
FileSync DLL Location.....	46
User interface.....	47
Descriptive name.....	47
LDAP.....	48
Administrative security.....	50
Administrative group DN.....	50
Security version.....	50
Connection information.....	49
Directory type.....	49
Prompt when disconnected.....	49
Servers.....	49
Use SSL.....	49
User paths.....	49
Credential sharing.....	51
Share credentials with authenticators.....	51
Data storage configuration.....	48
Base location(s) for configuration objects.....	48
Special Purpose.....	52
Alternate user ID location.....	53
BIND timeout.....	52
BIND user DN.....	52
BIND user password.....	52
Enable directory search for users.....	53
Naming attribute string.....	52
User interface.....	50
Descriptive name.....	50
Logon attempts.....	50
Show user path.....	50
LDAP Sync DLL location.....	48
Options.....	38
Allow disconnected operation.....	38
Delete local cache.....	38

Location of entlist.ini file.....	38
Synchronizer order.....	38
Use configuration objects.....	38
Roaming	
Required.....	53
Roaming Sync DLL location.....	53
Synchronizer order, Synchronization Options.....	38
Syslog Server, Audit Logging.....	59
System tray icon, User Experience.....	6

**T**

Time allowed for Java applets to load, Java Applications Response delays.....	12
Timeout	
for authentication prompt, Kiosk Manager User Interface Options.....	68
for locked session.....	66
TimeStamp, Database Event Fields Audit Logging.....	64
Title bar button, User Experience.....	6
Tooltip text	
User Experience System tray icon.....	6
User Experience Title bar button.....	6
Track memory consumption, Kiosk Manager.....	66
Transparent screen lock, Kiosk Manager User Interface.....	69
Type, Database Event Fields Audit Logging.....	64

**U**

Uppercase characters, Password Change Allowed character sets.....	16
URL matching precision, Web Applications Behavior.....	10
Use aggressive synchronization, Synchronization Behavior.....	39
Use cached credentials, Kiosk Manager.....	67
Use configuration objects, Synchronization Options.....	38
Use default certificate for authentication, Smart Card Authentication Options.....	34



- Use server icon, User Experience System tray icon ..... 6
- Use SSL
  - AD Connection information ..... 44
  - ADAM Connection information ..... 41
  - LDAP Synchronization Connection information ..... 49
  - LDAP v2 Authentication Connection information ..... 27
- Use transparent lock, Kiosk Manager User Interface Transparent screen lock ..... 69
- Use Windows Data Protection (DPAPI), Windows v2 Authentication Recovery ..... 24
- User can change passphrase, Windows v2 Authentication Passphrase ..... 26
- User domain name to use, ADAM Data storage configuration ..... 40
- User Experience
  - Application Response ..... 7
    - Applications that hooks should ignore ..... 7
    - Host/Mainframe Applications ..... 14
      - 16-bit screen capture attempts ..... 14
      - Credential request delay interval ..... 14
      - Polling interval ..... 14
  - Initial Credential Capture
    - Limit response to predefined applications for ..... 9
      - All application types ..... 9
      - Allowed Web pages ..... 9
      - Web applications ..... 9
      - Windows applications ..... 9
  - User Interface ..... 8
    - Allow creating multiple accounts during credential capture ..... 8
    - Credential capture mode ..... 8
    - Enable Auto-Enter ..... 8
    - Enable Auto-Prompt ..... 8
    - Enable Auto-Recognize ..... 8
    - Prohibit canceling the addition of new accounts ..... 8
    - Prohibit disabling the addition of new accounts ..... 8
    - Prohibit excluding accounts from credential sharing groups ..... 8
- Java Applications
  - Exclusions ..... 12
    - Excluded Java vendors ..... 12

- Excluded Java versions ..... 12
- Java events to respond to
  - Component events ..... 13
  - Hierarchy events ..... 13
  - Injection type ..... 14
  - Window events ..... 13
- Response delays
  - Delay after Java runtime startup ..... 12
- Response delays' ..... 12
  - Delay between retries ..... 12
  - Time allowed for Java applets to load ..... 12
- Retry behavior ..... 12
  - Maximum times to retry credential injection ..... 12
- Log on to waiting applications upon Agent startup ..... 7
- Respond to hidden and minimized windows ..... 7
- SendKeys event interval ..... 7
- Web Applications
  - Allowed dynamic Web pages ..... 11
  - Behavior ..... 10
    - Activate tab ..... 10
    - Respond to IE modal dialogs ..... 10
    - Scroll into view ..... 10
    - URL matching precision ..... 10
  - Credential field identification ..... 9
    - Border appearance ..... 9
    - Show border ..... 9
  - Response control ..... 11
    - Applications to ignore ..... 11
    - Web pages to ignore ..... 11
  - Windows Applications ..... 11
    - Allow fallback from control IDs to SendKeys ..... 11
- Application ResponseJava Applications
  - Java events to respond to ..... 13
- Password Change
  - Allowed character sets ..... 16
    - Lowercase characters ..... 16

Numeric characters.....	16
Special characters.....	16
Uppercase characters.....	16
Password change behavior.....	15
Allow user to exclude accounts from credential sharing groups.....	15
Change passwords automatically.....	15
Default password policy.....	15
Manual password change behavior.....	15
Pop-up dialog text after submission.....	15
Setup Wizard.....	18
Selected authenticator.....	18
Show first-time-use (FTU) wizard.....	18
System tray icon.....	6
Display icon in system tray.....	6
Show system name.....	6
Tooltip text.....	6
Use server icon.....	6
Title bar button.....	6
Always show for.....	6
Provide dropdown menu.....	6
Show title bar button.....	6
Tooltip text.....	6
User Interface.....	17
Allow refresh in My Accounts.....	17
Columns in "Details" view of My Accounts.....	17
Columns in Logon Chooser.....	18
Language.....	17
Logon animation's duration.....	18
User Experience Settings.....	6
User Interface	
AD Synchronization.....	45
File Synchronization.....	47
Initial Credential Capture.....	8
Kiosk Manager.....	68
Kiosk Manager Text Message	
Font Name.....	71

Font Size.....	71
Font Style.....	71
LDAP Authentication.....	31
Custom image for authentication prompt.....	31
Password change window subtitle.....	31
Password change window title.....	31
Show user path.....	31
Window title.....	31
LDAP Synchronization.....	50
LDAP v2 Authentication.....	28
Passphrasae, Windows v2 Authentication.....	25
Smart Card Authentication.....	34
User Experience.....	17
Windows Authentication.....	26
Windows v2 Authentication.....	24
User path(s)	
AD Synchronization Connection information.....	44
LDAP Synchronization Connection information.....	49
LDAP v2 Authentication Connection information.....	27

**W**

Wait for synchronization at startup, Synchronization Behavior.....	39
Web Applications, Initial Credential Capture, Limit response to predefined Web applications.....	9
Web pages to ignore, Web Applications Response control.....	11
When logons are deleted, Custom Actions.....	56
When logons change, Custom Actions.....	56
Width, Kiosk Manager User Interface Background Image.....	70
Width, Kiosk Manager User Interface Text Message Placement.....	72
Window events, Java events to respond to.....	13
Window subtitle	
Password change, LDAP Authentication.....	31
Smart Card Authentication User interface.....	34
Windows Authentication User interface.....	26

Window title	
LDAP Authentication User interface.....	31
Password change, LDAP Authentication.....	31
Smart Card Authentication User interface.....	34
Windows Authentication User interface.....	26
Windows v2 Authentication User interface.....	24
Windows	
Authentication Manager	
Enrollment.....	20
Grade.....	22
Order.....	23
Windows Applications	
Application Response.....	11
Initial Credential Capture, Limit response to predefined Windows applications.....	9
Windows event logging server, Windows Event Viewer Audit Logging.....	58
Windows Event Viewer, Audit Logging.....	58
Windows v2	
Authentication Manager	
Enrollment.....	20
Grade.....	22
Order.....	23

**X**

X coordinate	
Kiosk Manager User Interface Background Image.....	70
Kiosk Manager User Interface Status window.....	69
Kiosk Manager User Interface Text Message Placement.....	72
XML File, Audit Logging.....	61

**Y**

Y coordinate	
Kiosk Manager User Interface Background Image.....	70
Kiosk Manager User Interface Status window.....	69

Kiosk Manager User Interface Text Message Placement.....	72
--	----