CA Single Sign-On

Release Notes

r12.0

CA Product References

This document references the following CA products:

- CA® Single Sign-On (CA SSO)
- CA® Access Control
- CA® ACF2
- CA® Audit
- CA® Directory
- CA® Top Secret
- Unicenter® Software Delivery

Contact CA

Contact CA Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Welcome 9

Chapter 2: Fixed Issues List 11

Fixed Issues in r12 CR08 11
Fixed Issues in r12 CR07 12
Fixed Issues in r12 CR06 14
Fixed Issues in r12 CR04 14
Fixed Issues in r12 CR03 16
Fixed Issues in r12 CR02 17
Fixed Issues in r12 CR01 18

Chapter 3: New Features 21

Vista Support for CA SSO Client 21
SSO Credential Provider for Vista 21
Option for Identifying Elevated Applications in Vista 22
Tcl Tags Support for Elevated Applications 22
Installer Changes 23
FIPS 140-2 23
IPv6 Support 24
508 Compliance 24

Chapter 4: Changes to Existing Features 25

Changes to Existing Features in r12 CR08 25
Upgrades for the Server 25
Changes to Existing Features in r12 CR07 26
Support for Enforcing Password Policies 26
Enhancements to html_connect Extension 26
Changes to Existing Features in r12 CR06 27
Support for Modifying Password Labels 27
Hide PIN Field in the RSA Authentication Dialog 27
Enhancements to psgbc Utility 27
Changes to Existing Features in r12 CR05 28
Limit Number of Concurrent Sessions on a Workstation 28
Updated Version of Embedded Components in the CA SSO Server 28
Renaming of the New Password field 28

Update Version of CAPKI in CA SSO 29
Support for CRL as Fallback Revocation Method 30
Enhancements to html_connect Extension 31
Changes to Existing Features in r12 CR04 32
Display a Custom Name on the CA SSO GINA Dialog 32
CA Directory Version Updates in the CA SSO Server 32
Changes to Existing Features in r12 CR03 33
Changes to the CA SSO Integration Kit Documentation 33
Changes to the PSMaint Utility 33
Enhancements to Certificate Filtering 34
CA Access Control Version 34
Changes to Existing Features in r12 CR02 34
Changes to the CA SSO Integration Kit 34
Support for IE8 34
Changes to Existing Features in r12 CR01 35
Changes to the CA SSO Integration Kit 35
Changes to the Credential Provider 35
Changes to Session Administrator 35
Changes to Existing Features in r12 36
Support for Web Agents 36
Backward Compatibility with CA SSO Clients 36
Upgrading CA SSO Components 36

Chapter 5: Operating System Support 39

Platform Support 39

Chapter 6: System Requirements 41

CA SSO Server 41
CA SSO Client 42
ADS Listener 42
Authentication Agents 42
Password Synchronization Agent 43
Policy Manager 43
Session Administrator 43

Chapter 7: General and Installation Considerations 45

Sizing and Scaling Consideration 45
SSO Client Installer Consideration 45
Prerequisites for Silent Installation of Client 45
CA SSO Server Installation Consideration 45

Policy Manager Cannot Connect to the CA SSO Server When Different Modes of Operation Are Used 46
Installation Fails When Upgrading to r12 SSO Server 46
Server Upgrade from r8.1 GA to r12 Is Not Supported 46
Microsoft Windows Installation Consideration 46
Post Upgrade Configuration for Client.ini Files 47
Change Install Paths of Response Files 47

Chapter 8: Known Issues 49

CA SSO Server 49
Online Updates to the CA SSO Server Are Not Loaded after selang Updates 49
CA Directory Errors during CA SSO Server Startup 49
CA SSO Server Uninstall May Fail 50
CA SSO Server Data Migration Tools Do Not Support Non-English Characters from Pre-r12.1 Releases of CA SSO 50
Active Directory Object Limits on Microsoft Windows Platforms Affect CA SSO Server 50
Cannot Log into SSO Server from Policy Manager after Changing to Run in FIPS Mode 51
CA SSO Server Service Throws a EventLog Error After Reboot 51
Policy Manager 51
Alternative Languages not Supported 51
Policy Manager Registry Keys are Deleted After Upgrading the CA SSO Server 52
Authentication Agents 52
Windows Authentication Host Keyword <auto> Error 52
Authentication Agents Port Conflict 52
SSO Authentication Method Dialogs not Canceled 52
No Notification Given when Windows Authentication Fails 53
Cert Auth Authentication Does Not Work if the CA SSO Client is in FIPS-only Mode of Operation 53
Interpreter 53
Session Administrator 53
Internet Shortcut Is Not Created in Mozilla or Firefox 54
Navigating Using Interactive Mode 54
Support for FIPS 54
IPv6 Networking not Supported 54
Password Synchronization Agent (PSA) 54
PSA Modify/Repair Installation Functionality not Available 55
Application Wizard 55
Punctuation Characters must not be Used in Application Windows and Pages 55
Do Not Use Non-Standard Control Types on the Window You Are Automating 56
SSO Client 56
Dialogs Are Not Closed 56
Keep Servers Listed to a Minimum 56
Taskbar Right-Click Menu Does Not Work when Launchbar Is Docked 57

Taskbar Icon Does Not Disappear when Launchbar Application Is Exited . . . 57
Launchbar Screen Size Does Not Automatically Adjust . . . 57
Launchbar May Not Resize Correctly . . . 57
Application Names May Be Truncated . . . 57
Event Commands May Execute in Both Local and Remote Sessions . . . 58
Navigating Using Interactive Mode . . . 58
Remote Desktop Logon for GINA and Credential Providers Fails . . . 58
Icons for Disabled and Offline Applications Are Not Grayed Out . . . 58
Cannot Connect to IE7 without specifying an URL with the html_browse extension . . . 59
Cannot Connect to a URL using html_connect Extension if the Username is Administrator . . . 59

Chapter 9: International Support 61

Chapter 10: Accessibility Features 63

Product Enhancements . . . 64
Keyboard Shortcuts . . . 66
Hot Keys . . . 67

Chapter 11: Bookshelf 77

Chapter 12: Published Fixes 79

Appendix A: Third Party Acknowledgements 81

Softwares Under the Apache License . . . 82
Boost 1.40 . . . 85
TCL 8.4.13 . . . 86
Tclxml 2.6 . . . 87
OpenSSL 0.9.8.d and 0.9.8.h . . . 88
Zlib V1.2.3 . . . 90

Chapter 1: Welcome

Welcome to CA Single Sign-On (CA SSO). This document contains information about product installation considerations, operating system support, new features, changes to existing features, known issues, third-party acknowledgements, and information about contacting CA Technical Support.

Chapter 2: Fixed Issues List

This section contains the following topics:

Fixed Issues in r12 CR08 (see page 11)
Fixed Issues in r12 CR07 (see page 12)
Fixed Issues in r12 CR06 (see page 14)
Fixed Issues in r12 CR04 (see page 14)
Fixed Issues in r12 CR03 (see page 16)
Fixed Issues in r12 CR02 (see page 17)
Fixed Issues in r12 CR01 (see page 18)

Fixed Issues in r12 CR08

The following issues are fixed in this release:

Problem ID	Description	Resolution
1093	When ssoLaunchbar.exe is launched, the system crashes with a blue screen	This issue is fixed. SSOEvents is modified to make it thread-safe.
1094	Cert Authentication hangs during UPN name-mapping.	This issue is fixed. The local allocated memory is freed with corresponding free API.
1096	When the SSO Client service is started, it hangs.	This issue is fixed.
1098	When SSO launches the browser-based application and if you close the browser before the application is completely loaded, the script interpreter crashes.	This issue is fixed. All calls to Release() function on pointers to COM objects are now guarded.
1099	After the SSO Client r12.0 is installed, a significant delay is noticed in the startup of the Windows OS.	This issue is fixed. Now, winlogon.exe uses the SSO events asynchronously.
1103	The Watchdog service becomes unresponsive randomly. When the service is manually restarted, the problem does not reoccur.	This issue is fixed. The default value of WDOnlineChecksMode has been changed to zero (0).
1104	The system crashes while taking control of the "password change" screen from your Oracle web form application.	This issue is fixed. NULL check has been applied while taking control of the "password change" screen.

Problem ID	Description	Resolution
1105	When upgrading to 12.0 CR7, "EnforcePasswordPoliciesInLearnMode" option is not available in Policy Manager.	This issue is fixed. The required entries are added in the AccessControl database. Now, the “EnforcePasswordPoliciesInLearnMode” option is available in Policy Manager.
1106	A delay is observed when a fast user switching on Windows 7.	This issue is fixed. Code is modified to send a logoff notification to the LogonUI.exe.
1107	When SSO 8.0 Clients connect to SSO Server 12.0, CPU utilization of 12.0 Server is High, when compared to SSO 8.1 Server.	This issue is fixed.
1108	SSO installation fails due to the presence of same version of CA Directory, which is bundled with SSO Server installer.	This issue is fixed. A check is provided in the SSO Server installer to confirm whether CA Directory of the same version is already installed.

Fixed Issues in r12 CR07

The following issues are fixed in this release:

Problem ID	Description	Resolution
1037	In the learn mode, the CA SSO Server does not enforce password policies.	This issue is fixed. You can now configure the CA SSO Server to enforce password policies in the learn mode. **Note:** For more information about how to configure the CA SSO Server to enforce password policies in the learn mode, see the Enhancements topic in this guide.
1045	The CA SSO tcl extensions getscrape and waittext do not support IE8.	This issue is fixed. The getscrape and waittext extensions now support IE8.

Problem ID	Description	Resolution
1048	The html_connect extension uses only the document title of a window to identify it. So, if you are using Window title as an input to the html_connect extension, you cannot connect to that window.	This issue is fixed. The html_connect extension is modified to connect to a window using both the window title and document title of a web page. By default, the html_connect extension uses the window title to identify a window. If you want to identify a window using the document title, use the newly added key, -doctitle, with the html_connect extension. **Note:** For more information about the newly added option, see the html_connect extension description in the *tcl Scripting Reference Guide*.
1049	During the CA SSO Server installation on Windows 2008, the DSAs fail to start with the following message: "DSA has multiple interfaces that resolve to the same address".	If the Windows 2008 Server is configured to use IPv4 and IPv6 interfaces, the DSAs fail to start as the hostname in the DSA configuration resolves to the IPv4 and IPv6 interfaces. This issue is fixed now. The DSA now resolves to only one interface.
1050	The CA SSO interpreter and the Application Wizard are unable to identify the controls from a web page.	This issue is fixed. If the web page does not have a window title, the CA SSO interpreter fails to connect to the web page. So, the Application Wizard cannot identify the controls on that web page. This issue is fixed. If the web page does not have a window title, the CA SSO interpreter uses the URL of the web page to connect to it.
1051	If you enter a noncompliant password in the learn mode, a progress window "Setting application password" appears in the background.	This issue is fixed.
1066	The CA SSO interpreter extension *type* does not support Unicode characters when you are using a remote desktop connection in a full screen mode.	This issue is fixed. You can now use the CA SSO interpreter to type Unicode characters.
1068	During user logout, the session tokens are not deleted from the memory. So, memory leaks in the CA SSO Server	This issue is fixed. During user logout, the session tokens are deleted from the CA SSO Server memory.
1075	CA SSO credentila provider does not automatically login users even if DefaultPassword value is specified in clear text in the following registry key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	This issue is fixed.

Problem ID	Description	Resolution
1076	The value for the Token code field in the RSA Authentication dialog is not masked.	This issue is fixed. To mask the Token code field value, set the value of the HidePinInputField in the Auth.ini file to Yes.
1077	If the [PasswordDialogLabels] section in the Client.ini file does not contain any parameters, the CA SSO interfaces such as the Launchbar, Tools, and GINA crash.	This issue is fixed.

Fixed Issues in r12 CR06

The following defects are fixed in this release:

Problem ID	Description	Resolution
884	After upgrading your version of Active Directory Listener to CR05, uninstalling it does not remove the libetpki*.dlls in the bin folder.	This issue is fixed.

Fixed Issues in r12 CR04

The following defects are fixed in this release:

Problem ID	Description	Resolution
948	Silent installation and upgrade of Policy Manager fails on Windows XP	This issue is fixed. Silent installation of Policy Manager no longer fails.
954	CA SSO must not prompt users to reauthenticate when Windows authentication method is configured with AutoNetworkAuth=yes.	A new configuration parameter "SuppressExpirationNotification" is added to the Client.ini. **Note:** For more information about this parameters, see the *Implementation Guide*.
955	Error invoking legacy 16-bit application from launchbar	This issue is fixed. The error in invoking legacy 16-bit application from launchbar is corrected.
956	The html_selectitem extension does not simulate mouse clicks.	This is issue is fixed. Added support to fire Onchange event for html_SelectItem.

Problem ID	Description	Resolution
958	In CA SSO-Citrix integration or in a remote session, CA SSO does not generate SSO TK cookies upon successful login. So, the CA SSO-SiteMinder integration fails.	This issue is fixed. CA SSO generates cookies for remote sessions for all agents except when the authentication method is set to Citrix.
959	PwdEncUtil.exe encrypts user information available in the default user directory only.	PwdEncUtil.exe encrypts user information available in all the user data stores.
960	If the smartcard used for authentication is removed during a login through GINA, the user is authenticated even if the option scremove is set to 1.	This issue is fixed. If you remove the smartcard during the Windows login process, the workstation is locked or logged off according to the settings of scremove option.
962	Increase in engsvc.exe memory usage.	Handle leak in engine service is corrected.
963	If you upgrade the CA SSO Server it breaks the unique IDs of the Watchdog service.	Watchdog Service now installed with a unique account ID in server farm setup. **Note:** Copying Access Control Databases from one server to another server in a farm setup will need the Watchdog credentials reset for authentication to SSO server. Please consult CA Support for resetting Watchdog credentials.
965	HTML_BROWSE -grab extenstion	Added a new option "grab" to html_browse command to specify whether to grab the html page. The default value is TRUE i.e the page will be scraped by default if -grab is not specified. Following values can be used: **Value:** [y|n] **Default:** y
966	HTML_BROWSE -size extenstion	A new extension "size" is added to html_browse command to specify how IE should be displayed when launched. Following values can be used min - Indicates that IE should be opened in minimized state max - Indicates that IE should be opened in maximized state same - Indicates that IE should be opened at the same size it was. open - Indicates that IE should be restored.

Problem ID	Description	Resolution
967	Pop-up disabled during offline	Added a new entry "DisplayOfflineModeConfirmation" in OfflineOperation section in the client ini file. If it is set to yes, user is prompted that server is offline and waits for user input to continue or abort the login process. If it is set to no, there will not be any prompt and user will work offline. **Note:** For more information about this parameters, see the *Implementation Guide*.
984	Retrieval of user application list using SSO Java SDK fails.	This issue is fixed. Information about JAVA SDK and its usage was provided to the users.
985	When you upgrade from CA SSO Client from r8.1 to r12, the installer prompts users to change the install folder. The installer does not upgrade the CA SSO Client to the same location.	This issue is fixed. The installer upgrade the CA SSO Client using the same folder structure as in earlier releases.
986	Policy Manager cannot connect to the CA SSO Server over non-default communication ports.	This issue is fixed. The Policy Manager can now connect to CA SSO Server over non-default ports.
987	The file C:\Program Files\CA\Single Sign-On\Client\cfg\Configuring the SSO Client.html contains information related to SSO r8.1.	This issue is fixed. The file is updated to reflect SSO r12 information.
988	The Application Wizard is unable to interpret controls on the CA Support portal.	
989	When you uninstall the Password Synchronization Agent, the SingleSignOn key is not removed from the registry.	This issue is fixed. Uninstalling the Password Sychronization Agent removes the SingleSignOn key from the registry.

Fixed Issues in r12 CR03

The following defects are fixed in this release:

Problem ID	Description	Resolution
926	When using certificate authentication, if you logoff Windows and insert smart card for reauthentication, CA SSO Client does not recognize the smart card.	This issue is fixed. CA SSO Client recognizes smart cards if you logoff Windows and re-insert the smart card.

Problem ID	Description	Resolution
928	CA SSO applications configured to launch on Windows startup fail to launch with the following error: cannot retrieve variables	This issue is fixed. CA SSO applications no longer fail to launch on Windows startup.
936	Winlogon.exe crashes when you install CA SSO Client on computers where SafeBoot is also installed.	This issue is fixed. winlogon.exe no longer crashes.
942	When users start a computer and insert their smart cards for authentication, the Authentication - Certificate dialog opens, but the cursor focus is not set to the password field.	This issue is fixed. When users insert a smart card, the Authentication - Certificate dialog opens and the cursor focus is set to the Password field.
945	Sample source code required for customizing namemapping DLL are not packaged.	This issue is fixed. The sample source code for customizing namemapping DLLs are packaged. Instructions for customizing the namemapping DLL are included in the ReadMe.txt at the following folder: *SampleNameMapping*

Fixed Issues in r12 CR02

The following defects are fixed in this release:

Problem ID	Description	Resolution
884	The maximum length of the Verify Password field for CA SSO Server administrator is 14 characters. So, if the CA SSO Server administrator password is longer than 14 characters the entries in the Password and Verify Password fields do not match and the installer aborts.	The maximum length for the Verify Password field related to CA SSO Server administrator is modified to accept long passwords.

Problem ID	Description	Resolution
893	When users launch applications through a Citrix Metaframe Server, the memory usage of engsvc.exe increases incrementally.	This issue is fixed. engsvc.exe does not increase its memory usage when users launch applications through Metaframe server. The following new configuration section [SessionCleanup] is added to Client.ini to enable orphan token cleanup process in engine service: **Note:** For more information about this parameters, see the *Implementation Guide*.
911	During certificate authentication, CA SSO truncates all characters after the symbol '@' in the User Principal Name from the smart card, and maps this truncated attribute to the userPrincipalName in Active Directory. So, the mappings do not match and authentication fails.	This issue is fixed. CA SSO does not truncate the User Principal Name before comparing the attribute with the userPrincipalName in Active Directory.
912	Users can use their smart cards with only one smart card reader to authenticate with CA SSO Client. Users cannot use a smart card with more than one smart card reader to authenticate with CA SSO.	This issue is fixed. Users can use their smart cards with any Smart Card Reader to authenticate with CA SSO Client.

Fixed Issues in r12 CR01

Problem ID	Description	Resolution
832	Password filter blocks password changes to the Directory Services Restore Mode (DSRM) administrator account using ntdsutil command.	This issue is fixed. The password filter no longer blocks password changes for the DSRM administrator account.
836	If the certificate store path is invalid, the CA SSO Client displays inaccurate error messages during certificate authentication.	A new error message is included to reflect the validity of certificate path entries in the Auth.ini file.
842	The SSO PWDBOX extension displays an inaccurate and confusing error message when users change passwords and the new password and confirm password fields do not match.	This issue is fixed. The error message format is changed to the same format used in CA SSO r8.0.
850	Launchbar crashes when retrieving container applications that have only one application.	This issue is fixed. Upgrade your CA SSO client installation to CA SSO r12.0 CR01.

Problem ID	Description	Resolution
865	Unable to add the CA SSO Server performance counters to Windows Performance Monitoring service PerfMon.msc.	This issue is fixed. You can now add the CA SSO Server performance counters to PerfMon.msc.
868	CA SSO Client installation fails when you try to install the CA SSO client on a server with unsupported versions of Citrix MetaFrame Servers. The installation must not fail but must let you to continue the installation even with unsupported versions of the Citrix MetaFrame Server.	This issue is fixed. The CA SSO Client installation proceeds even with unsupported versions of Citrix MetaFrame Server.
870	In a Citrix environment, the CA SSO interpreter crashes with exceptions when users try to log in.	This issue is fixed. The CA SSO interpreter no longer crashes with exceptions when users try to log in.
871	CA SSO GINA is not displayed during a remote desktop session and the login fails with the following error: Workstation Login Failed Windows could not log you on (reported error 0x57) Win32 Error: The parameter is incorrect.	This issue is fixed. CA SSO GINA is available during a remote desktop session.
872	When CA SSO Server is installed on a server with a locale that is not certified, login to the Policy Manager fails with the following error: Failed to unpack data	This issue is fixed. If you install the CA SSO Server with a locale that is not certified, the locale is set to the default locale, ENU.
874	Application Wizard generates errors when scripts contain a "\" (backslash).	This issue is fixed. Application Wizard now handles scripts containing a "\" (backslash) appropriately and no longer generates errors.
876	Roaming user profiles are not deleted.	This issue is fixed. The roaming profiles are now deleted
877	Unable to authenticate using Windows Authentication agents due to named pipe timeouts.	This issue is fixed. A new entry, NamedPipeTimeout is added to Connection section of CA_wintga.ini file of the WinAuth Agent. **Note:** For more information about this parameters, see the *Implementation Guide*.
882	CA SSO Smartcard authentication does not support NetID software.	CA SSO Smartcard authentication now supports NetID software Two entries are added to [auth.CERT] section in auth.ini to address this issue. **Note:** For more information about this parameters, see the *Implementation Guide*.

Problem ID	Description	Resolution
884	The maximum length of the Verify Administrator Password field in the Active Directory Listener installer is 14 characters. So, if the administrator password is longer than 14 characters the entries in the Password and Verify Password fields do not match and the installer aborts.	The maximum length for the Verify Password field is modified to accept long passwords.
888	CA SSO GINA crashes when users try to unlock workstations that are not connected to a network domain.	This issue is fixed. The CA SSO GINA no longer crashes when users try to unlock workstations that are not connected to a network domain.
889	The following error is recorded in the CA SSO Interpreter logs when you use the Exit command in a login script: ERROR - error evaluating script	This issue is fixed. The CA SSO Interpreter no longer returns an error merely because you use an Exit command in a login script.

Chapter 3: New Features

This section contains the following topics:

Vista Support for CA SSO Client (see page 21)
FIPS 140-2 (see page 23)
IPv6 Support (see page 24)
508 Compliance (see page 24)

Vista Support for CA SSO Client

The CA SSO Client is supported on Windows Vista. Vista manages applications differently from other platforms; so, the CA SSO Client also behaves differently when you try to launch applications.

On Vista, applications are classified as standard applications and elevated applications. *Standard* applications are applications that do not need to modify or write to system files, including registry and program files folder. *Elevated* applications are applications that may need to modify or write to restricted system files. As a standard user on Vista, you can run standard applications only. To run elevated applications on Vista, you must have administrator privileges.

Note: For more information on how the CA SSO Client behaves on Vista, see the *CA SSO Administration Guide* and the *CA SSO Client Online Help*.

SSO Credential Provider for Vista

When Vista is the operating system, two new SSO credential providers are installed. One of the new credential providers provides interactive workstation logon support using local or SSO authentication methods and the other credential provider helps the user log onto the Windows workstation directly. When a user logs onto a Windows Vista computer, they enter their credentials using the SSO Credential Provider. When the operating system is Vista, the SSO Installer only shows Vista features. All other platform features are hidden. For example, the Credential Provider feature replaces GINA in the features dialog.

The SSO Credential Provider for Vista provides two new unlock station modes:

- Mode 4: Single SSO User per Windows Session Lock Option
- Mode 5: Multiple SSO Users per Windows Session Lock Option

For more information on the SSO Credential Provider for Vista, and the unlock station modes, see the *CA SSO Administration Guide.*

Option for Identifying Elevated Applications in Vista

The CA SSO Client is supported on Vista. Vista manages applications differently from other platforms; so, the CA SSO Client also behaves differently when you try to launch applications.

On Vista, applications are classified as standard applications and elevated applications. *Standard* applications are applications that do not need to modify or write to system files. *Elevated* applications are applications that may need to modify or write to restricted system files. As a standard user on Vista, you can run standard applications only. To run elevated applications on Vista, you must have administrator privileges.

To conform to these application types on Vista, the CA SSO Client must differentiate between standard applications and elevated applications. The CA SSO Server identifies whether to run the SSO interpreter in elevated mode, or not, by the "Run as administrator" attribute in the application properties. The following attribute is added to the Attributes dialog of Application Resources:

```
Run As Administrator
```

Note: For more information on the attribute, Run As Administrator, see the CA SSO Policy Manager Help.

Tcl Tags Support for Elevated Applications

Whenever you try to access an elevated application on Vista, the CA SSO Client must also run in an elevated mode. To run the CA SSO Client in an elevated mode, you must use the administrator privileges. So, when you try to launch applications on Vista, you may be required to provide the administrator credentials twice-first to run the CA SSO Client in an elevated mode and the second to launch the elevated application. Vista prompts for administrative privileges using the UAC prompts.

On Vista, an elevated application can launch another elevated application without any UAC prompts. So, the CA SSO Client if running in an elevated mode can launch elevated applications without prompting the user for administrative privileges. You can configure the CA SSO Client to suppress the second UAC prompt needed to launch elevated applications by configuring the following tags are added to the TCL extension *-sso run*:

- [-elevated y|n]
- [-suppressconsent y|n]

Note: For more information on -sso run TCL extension, see the *TCL Scripting Reference Guide*.

Installer Changes

The CA SSO Client supports Vista. Accordingly, the CA SSO Client installer is also updated to support Vista. The CA SSO Client installer includes a version of TCL interpreter for Vista that is different from the TCL interpreters for other Windows operating systems. The TCL interpreter for Vista must run in the elevated mode to handle elevated applications on Vista.

Also, the CA SSO Client installer includes a CA SSO Credential Provider for Vista in place of CA SSO GINA. When you install CA SSO Client, the installer checks for the underlying operating system and provides you the following options differently for Vista and other operating systems:

For Vista

SSO Credential Provider

For other Windows operating systems

SSO GINA

FIPS 140-2

CA SSO r12 supports FIPS 140-2 in new installations and upgrades. Also, CA SSO comes with a command line utility called PwdEncUtil, to:

- Generate new key encryption and password encryption keys (KEK and PEK) and expire/replace active keys. (The KEK and PEK are the keys that are currently being used by the SSO Server.)
- Re-encrypt all existing passwords after changing the PEK.
- Re-encryption of legacy passwords (After an upgrade from 8.1)

For more information on this utility, see the "FIPS 140-2 Appendix", in the C*A SSO Administration Guide*.

IPv6 Support

When configuring CA SSO, you can enter both IPv4 and IPv6 addresses.

CA SSO supports IPv6 on the following operating systems:

- Vista
- Server 2003 Enterprise Edition and Standard Edition SP2
- XP SP2

Note: The Windows Authentication method is not supported for CA SSO and GINA clients in a pure IPv6 environment; this limitation is valid for Windows XP and Windows 2003 Server.

508 Compliance

For this release of CA SSO, the SSO Client has been updated to comply with Section 508 standards in the following categories:

- Software Applications and Operation Systems
- Functional Performance Criteria and Information
- Documentation
- Support

More information:

Accessibility Features (see page 63)

Chapter 4: Changes to Existing Features

This section contains the following topics:

Changes to Existing Features in r12 CR08 (see page 25)
Changes to Existing Features in r12 CR07 (see page 26)
Changes to Existing Features in r12 CR06 (see page 27)
Changes to Existing Features in r12 CR05 (see page 28)
Changes to Existing Features in r12 CR04 (see page 32)
Changes to Existing Features in r12 CR03 (see page 33)
Changes to Existing Features in r12 CR02 (see page 34)
Changes to Existing Features in r12 CR01 (see page 35)
Changes to Existing Features in r12 (see page 36)

Changes to Existing Features in r12 CR08

Upgrades for the Server

The following upgrades are done in CR08 for the Server:

- Upgraded AccessControl kit in SSO Server installer to r12.5 SP3.
- Upgraded CA Directory to r12.0SP5.

Changes to Existing Features in r12 CR07

Support for Enforcing Password Policies

A new property EnforcePasswordPoliciesInLearnMode is added to the Policy Manager properties to let you enforce password policies in the learn mode.

To configure the CA SSO Server to enforce password policies

1. Login to the Policy Manager.
2. Select the Resources icon in the program bar.

   The Resources window appears.
3. Expand the Configuration Resources folder, and select Policy Server Settings.

   The list of Policy Server settings opens in the right pane.
4. Double-click the General settings.

   The View or Set GPSCONFIGPROPERTY Properties - Settings dialog opens.
5. Select the EnforcePasswordPoliciesInLearnMode property and click the  icon to edit the property.
6. Set the property value to Yes, and click OK.

   Note: The default value of this property is set to Yes. If you set this property value to No, the CA SSO Server does not enforce password policies during the learn mode.
7. Click OK.

   The CA SSO Server is configured to enforce password policies.

Enhancements to html_connect Extension

You can now use the html_connect extension to connect to a window using the window title or the document title. To support this enhancement the following key is added to the html_connect extension:

-doctitle

Specifies that the CA SSO interpreter matches the value of the doctitle with the document title of the web page.

Changes to Existing Features in r12 CR06

Support for Modifying Password Labels

You can now configure the Password and Verify Password field labels in the Set Login Information and the Change Password dialogs of the CA SSO Client. The following options are added to the [PasswordDialogLabels] section in the Client.ini file:

- PasswordFieldLabel
- VerifyPasswordFieldLabel

Note: For description about these entries, see the Client.ini file section in the Administration Guide.

You can also set these password labels using the following keys added sso tcl extension pwdbox:

- –pswd_label
- –vrfy_pswd_label

Note: For description about these keys, see the pwdbox extension description in the *tcl Scripting Reference Guide*.

Hide PIN Field in the RSA Authentication Dialog

You can configure the CA SSO Client to hide the PIN field in the RSA Authentication dialog. The following new entry is added to the Auth.RSA section in the Auth.ini file:

- HidePinInputField

Note: For more information about the HidePinInput field, see Auth.ini section the *Administration Guide*.

Enhancements to psgbc Utility

The psbgc utility is enhanced to request the CA SSO Server to cache authorization rules to build the application lists. You can configure the psbgc to support this functionality using the following entry in the psbgc.ini file:

- CreateUserAPPLCache

Note: For a description of this entry, see the psbgc.ini file section in the Administration Guide.

Changes to Existing Features in r12 CR05

Limit Number of Concurrent Sessions on a Workstation

Note: The following enhancement is valid on Windows Vista and Windows 7 in workstation modes 4 and 5 only.

You can now configure the CA SSO Client to limit the number of concurrent sessions on a workstation. To create a session, the CA SSO Client does the following during a user login process:

1. Verifies if the number of concurrent sessions has reached the specified limit. If the limit is not reached, a new session is created.
2. If the specified limit is reached, the CA SSO Client verifies each of the existing sessions starting from the oldest session for any active monitored applications. The CA SSO Client will log off a session that has no active monitored applications. If all the existing sessions have active monitored applications, the CA SSO Client does not create a new session.

   Note: Monitored applications are your preferred applications that are mentioned in the MonitorAppExes in the Client.ini file.

The following entries in the [CredentialProvider] section of the Client.ini file controls this CA SSO Client behavior.

- MaxConcurrentSessions
- LimitChoice
- MonitorAppExes

Note: For more information about these entries, see the Client.ini file description in the *Administration Guide*.

Updated Version of Embedded Components in the CA SSO Server

From this release, the CA SSO Server embeds the following components:

- CA Access Control r12.5 build number: 12.51.543
- CAPKI r4.1.3

Renaming of the New Password field

In the Set Login Information dialog in the CA SSO Client, the New Password field is renamed to Password.

Update Version of CAPKI in CA SSO

The following CA SSO components are upgraded to embed CAPKI r4.1.3:

- Policy Manager
- PSLang
- Session Administrator
- CA SSO Integration Kit
- CA SSO Application Wizard
- Password Synchronization Agent
- Active Directory Listener
- Windows Authentication Agent
- RSA Authentication Agent
- LDAP Authentication Agent

Support for CRL as Fallback Revocation Method

The following enhancements are made to the Certificate Authentication Agents to support the following features:

- CRL as fallback revocation method
- Fixed OCSP and CRL revocation methods for multiple certificate authentication agents

Support for fallback revocation method

New values added for the RevocationMeth parameter, in the CA_certtga.ini, to have a fallback mechanism are as follows:

- FIXED_OCSP_FALLBACK_TO_CRL
- FIXED_OCSP_FALLBACK_TO_CRLDP
- AIA_OCSP_FALLBACK_TO_CRL
- AIA_OCSP_FALLBACK_TO_CRLDP
- CRLDP_FALLBACK_TO_CRL

For the previously mentioned methods, the user certificate is initially verified using first method (FIXED_OCSP or AIA_OCSP or CRLDP). If the OCSP/CRLDP methods are unavailable, the certificate authentication agent uses the CRL/CRLDP methods. For example, FIXED_OCSP_FALLBACK_TO_CRL first verifies the user certificate using FIXED_OCSP and if OCSP is not available, then only it verifies with the CRL.

Support for multiple CAs

To support multiple values for FIXED_OCSP add different sections for OCSP in the CA_certtga.ini as follows:

[OCSPresponder1]

OcspSignCert=

OcspSignCertPass=

OcspResponder=

TrustedPath=

TrustedNames=

[OCSPresponder2]

OcspSignCert=

OcspSignCertPass=

OcspResponder=

TrustedPath=

TrustedNames=

To support multiple CRLs, add different sections for CRL in the CA_certtga.ini as follows:

[CRL1]

CrlFileName=

CrlIssuerCert=

[CRL2]

CrlFileName=

CrlIssuerCert=

Enhancements to html_connect Extension

You can now use the html_connect extension to connect to a window using the window title or the document title. To support this enhancement the following key is added to the html_connect extension:

-doctitle

Specifies that the CA SSO interpreter matches the value of the doctitle with the document title of the web page.

Changes to Existing Features in r12 CR04

Display a Custom Name on the CA SSO GINA Dialog

The user data store is enhanced to include a new property DisplayName_USER@<datastore>. This property identifies the user attribute that is displayed on the CA SSO GINA when a user locks a workstation.

Notes:

- To display a user attribute on the CA SSO GINA dialog, identify the attribute using the DisplayName_USER@<datastore> property and also set the *DisplayCustomName* attribute in the Client.ini file.
- For more information about the DisplayCustomName attribute, see the Client.ini file section of the *Administration Guide*.

To add DisplayName_User property in the CA SSO Server

1. Login to the Policy Manager.
2. Select the Resources icon in the program bar.

   The Resources window appears.
3. Expand the User Resources folder, right-click User Attributes and select New.

   The Create New USER_ATTR Resource - General dialog appears.
4. Enter the following values:

   Name

   Specify DisplayName_USER as the name of the attribute.

   Data Store

   Specify a user directory where the user attributes are stored. Click Browse to select the user directory.

   DBField

   Specify the user attribute that you want to display on the CA SSO GINA dialog.
5. Click OK.

   The user attribute is created.

CA Directory Version Updates in the CA SSO Server

From this release, the CA SSO Server embeds CA Directory r12 SP1 build number: 12.0.4076.

Changes to Existing Features in r12 CR03

Changes to the CA SSO Integration Kit Documentation

The CA SSO integration kit build release no. 12.0.0.54 is enhanced to include the following documentation:

- A new API ssoclapi_GetUserTokenEx() is added to the CA SSO Integration Kit. Use this API to retrieve the token status from CA SSO Server.
- The SSOCLAPI error codes are included in the CA SSO Integration Kit.

Note: For more information about the new API and SSOCLAPI error codes, see the *CA SSO Integration Kit*.

Changes to the PSMaint Utility

The PSMaint utility is enhanced to include the following functionality in CA SSO Server build release no. 12.0.0.5056:

- A switch 'WD' is added to start and stop the Watchdog services. To start and stop the Watchdog service, use the following commands:

  ```
  PSMaint.cmd -start WD
  PSMaint.cmd -stop WD
  ```

- An option to accept archive directory names that have spaces. If the directory name contains spaces, the directory name must be enclosed within double quotes. For example, if directory name is Archival Directory, it must be modified as "Archive Directory" for input to the PSMaint utility.
- The archive files are copied to a temp folder, zipped, and only on confirmation that the zipping was successful that the logs are deleted.

Enhancements to Certificate Filtering

CA SSO Client is enhanced to include certificate filtering. Certificate filtering helps you to filter user certificates based on certain certificate parameters and display only the filtered certificates to the users. This certificate filtering is useful when users have more than one certificate to authenticate using smart cards and users do not know which certificate to use. The following entries are added to the Auth.Cert section of the Auth.ini file to configure certificate filtering:

- AutoCertSelection
- FilterDLLPath
- MappingMethod
- ExpectedValue
- ShowFilteredCertificates
- FilteringPattern

Note: For description about these entries, see the Auth.ini file section in the *Administration Guide*.

CA Access Control Version

From this release, the CA SSO Server includes CA Access Control r12.0 build release no.12.1.0812.

Changes to Existing Features in r12 CR02

Changes to the CA SSO Integration Kit

The CA SSO Integration Kit is enhanced to include the following:

- Samples for implementing a sample authentication using Credential Provider. The SampW32.dll is enhanced to handle authentication calls from Credential Providers.
- Support for FIPS140-2 and IPv6.

Support for IE8

The CA SSO Client now supports IE8; but support does not include tabs functionality in IE8.

Changes to Existing Features in r12 CR01

Changes to the CA SSO Integration Kit

The CA SSO Integration Kit consists of the following components:

- CA SSO Sample Authentication Method for Windows operating system.
- CA SSO Client API, SSOCLAPI, for Windows operating system.
- CA SSO Server API in C and Java SDK for Windows operating system.

Changes to the Credential Provider

The following enhancements are made to Credential Provider:

- If a user login through the Credential Provider fails, CA SSO displays all the Credential Provider tiles. In CA SSO r12.0, CA SSO displayed only the Windows Logon tile for any login failures.
- In shared workstation modes 0 through 3, Credential Provider is enhanced to let Windows administrators log in to CA SSO even when another user is logged into CA SSO. The administrator can log in to CA SSO using CA SSO agents from a Windows desktop. As shared workstations mode 0 through 3 support only one CA SSO session, CA SSO prompts the administrator to log off the current CA SSO user before logging in.
- In shared workstation modes 4 and 5, Credential Provider is enhanced to let Windows administrators log in to CA SSO using an actively logged in CA SSO user. As shared workstation modes 4 and 5 support only one CA SSO session per user, CA SSO prompts the administrator to log off the existing session for the CA SSO user before logging in.
- If a Windows user tries to unlock a workstation locked by another Windows user, Credential Provider prompts the Windows user to perform a Windows Switch User before logging in. This is valid for shared workstation mode 5.

Changes to Session Administrator

From this release, the Session Administrator is FIPS140-2 and IPv6 compliant.

Changes to Existing Features in r12

Support for Web Agents

If using the CA SSO Web Agents for forms-based authentication, these agents are not provided in this release. Instead, use the CA SSO r8 versions of these agents.

For Web access protection, CA® SiteMinder Web Access Manager is the chosen upgrade path. For more information on this contact your local SSO Support Representative.

Backward Compatibility with CA SSO Clients

The following points on backward compatibility must be noted before upgrading CA SSO r12 components:

- CA SSO r12 servers are backward compatible with CA SSO r8.1 clients.
- CA SSO r12 client is not backward compatible with earlier versions of CA SSO components.
- CA SSO r12 authenticating agents are compatible only with r12 clients.
- CA SSO r8.1 clients are compatible with r8.1 or r12 authentication agents.

Note: For more information on backward compatibility with CA SSO clients, see the *Implementation Guide*.

Upgrading CA SSO Components

CA SSO r12 supports upgrade of all components from CA SSO r8.1. CA SSO does not support a direct upgrade from r8.0 to r12. You can only upgrade the r8.0 client component to r12 directly. To upgrade from CA SSO r8.0 to CA SSO r12, you can either:

- Set up a new CA SSO r12 environment. This involves:
  - Installing r12 Servers.
  - Migrating all data from r8 to r12.

- Upgrade to r8.1 Servers and then to r12 Servers.

You must use the data migration upgrade paths to ensure that the data from the user and policy stores from r8.0 or r8.1 are migrated to the CA SSO r12 during upgrade in the following scenarios:

- CA SSO Server is installed on the same machine; however use of the upgrade wizard is not possible, for instance in SSO r8 to r12 scenario.
- CA SSO Server r12 is installed on a separate machine from existing 8.0 or 8.1 Server and the existing configuration needs to be migrated to a new machine.

Note: For more information on upgrading to r12, see the *Implementation Guide.*

Chapter 5: Operating System Support

The following describes the operating system support for each component.

This section contains the following topics:

Platform Support (see page 39)

Platform Support

For more information about platforms, CA products, and third-party software that CA SSO components support, see the Compatibility Matrix(Document ID: TEC267840) on the Technical Support site: https://support.ca.com.

For latest updates about platforms for SSO, see the *Readme*(Document ID: G00857-1E).

Chapter 6: System Requirements

The following describes the system requirements for each component.

This section contains the following topics:

CA SSO Server (see page 41)
CA SSO Client (see page 42)
ADS Listener (see page 42)
Authentication Agents (see page 42)
Password Synchronization Agent (see page 43)
Policy Manager (see page 43)
Session Administrator (see page 43)

CA SSO Server

The following are the minimum requirements for the system that hosts the CA SSO Server:

- Pentium 2 GHz or greater
- 2 GB RAM or greater
- 2 GB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Note: Requirements vary depending on the number of users in your data store, and other variables. CA recommends planning your architecture, which will help you to determine the appropriate sizing and scaling requirements of your servers for your environment.

CA SSO Client

The following are the minimum requirements for the system that hosts the CA SSO Client:

- Pentium 266 MHz or greater
- 256 MB RAM or greater
- 200 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

ADS Listener

The following are the minimum requirements for the system that hosts the ADS Listener:

- Pentium 512 MHz or greater
- 1 GB RAM or greater
- 500 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Authentication Agents

The following are the minimum requirements for the system that hosts the Authentication Agents:

- Pentium 512 MHz or greater
- 512 MB RAM or greater
- 500 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Password Synchronization Agent

The following are the minimum requirements for the Password Synchronization Agent:

- Pentium 512 MHz or greater
- 512 MB RAM or greater
- 500 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Policy Manager

The following are the minimum requirements for the system that hosts the Policy Manager:

- Pentium 266 MHz or greater
- 256 MB RAM
- 20 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Session Administrator

The following are the minimum requirements for the system that hosts the Session Administrator:

- Pentium 266 MHz or greater
- 256 MB RAM
- 20 MB free disk space
- DVD-ROM drive (The installation package is provided in DVD format only.)
- Active network connection
- TCP/IP

Chapter 7: General and Installation Considerations

The following should be considered when installing CA SSO.

Sizing and Scaling Consideration

CA recommends sizing and scaling your CA SSO environment for your enterprise's requirements. CA has provided tools to assist with this. For more information see, the *CA SSO Performance Measurement Module* on Support Connect.

SSO Client Installer Consideration

The CA SSO Client installer uses the Windows cacls.exe program to set directory permissions. This tool is subject to a known issue described in the Microsoft Knowledge Base article 834721. To work around this issue, apply the operating system hotfix supplied by Microsoft.

Prerequisites for Silent Installation of Client

Before you run a silent installation of CA SSO r12 client on a Windows 2000 Server operating environment, ensure that you have Microsoft Visual C++ 2005 redistributable package installed on that computer.

CA SSO Server Installation Consideration

The CA SSO Server cannot be installed in a location that contains non-ASCII characters anywhere in the path.

Policy Manager Cannot Connect to the CA SSO Server When Different Modes of Operation Are Used

When the CA SSO Server is installed in mixed mode of operation and the Policy Manager is installed in FIPS-only mode of operation, the Policy Manager cannot connect to the CA SSO Server.

Change the CA Access Control registry entries to FIPS-only mode of operation. Also, change the CA SSO Server mode to FIPS-only mode of operation.

Note: For more information on how to change the mode of operation of CA Access Control and CA SSO Server, see the *CA SSO Implementation Guide*.

Installation Fails When Upgrading to r12 SSO Server

If the existing r8.1 Server has been upgraded from r8.0 and then upgraded to r12, the installation does not proceed. Verify that the upgrade from r8.0 to r12 in the following order:

1. Upgrade Ingres version from r2.6 to at least r3.0 on the computer that hosts the r8.0 server installation.
2. Upgrade the SSO Server from r8.0 to r8.1.
3. Upgrade the SSO Server from r8.1 to r12.

Server Upgrade from r8.1 GA to r12 Is Not Supported

You cannot upgrade directly from r8.1 GA version ofthe CA SSO Server to r12.

To work around this issue, upgrade r8.1 with r8.1 CR6 or greater and then upgrade to r12.

Microsoft Windows Installation Consideration

On some computers, the timestamp for the install and un-install log file is in GMT time rather than local time. This is a known problem with Java when the Windows locale and time zone is not properly set.

To work around this issue, reset your Windows system locale and time zone. This can be done by setting your time zone to another time zone and applying it, then changing it back to the correct time zone.

Post Upgrade Configuration for Client.ini Files

The CA SSO Client uses the IdentityFile and TrustFile entries in the [Auth.Win] section of Auth.ini file to connect to a Windows authentication agent. The IdentityFile and TrustFile files are stored in the following location for r12:

<*Install_folder*>\ca\Single Sign-On\client\cfg

In previous releases of the CA SSO Client the IdentityFile and TrustFile entries pointed to files in the following location:

<install_folder>\ca\etrust sso\client\cfg

When you upgrade from previous releases of CA SSO to r12 Client, the information in *.ini files of previous releases is migrated to the *.ini files of CA SSO r12. So, the entries for IdentityFile and TrustFile entries in CA SSO r12 after upgrade refer to the configuration folder of previous releases. So, the client cannot connect to a Windows authentication agent after an upgrade.

Post upgrade to r12, manually edit the IdentityFile and TrustFile entries in [Auth.Win] section of Auth.ini file to reflect the path of the client configuration folder for r12.

Change Install Paths of Response Files

For silent upgrade, the install paths for response files of CA SSO components (clients, authentication agents, and password synchronization agents) must be different from the install paths specified for earlier releases.

Chapter 8: Known Issues

This section contains the following topics:

CA SSO Server (see page 49)
Policy Manager (see page 51)
Authentication Agents (see page 52)
Session Administrator (see page 53)
Password Synchronization Agent (PSA) (see page 54)
Application Wizard (see page 55)
SSO Client (see page 56)

CA SSO Server

The following are the CA SSO Server known issues.

Online Updates to the CA SSO Server Are Not Loaded after selang Updates

Problem:

When updating large numbers of objects in the database from a batch selang script, some of the online updates to the CA SSO Server might not get loaded.

Solution:

To work around this issue and ensure the new information is fully loaded into the CA SSO Server, you must restart the server service after the selang updates complete.

CA Directory Errors during CA SSO Server Startup

Problem:

When there is a large amount of data in the CA Directory, it might report the following errors during the startup phase:

```
Out of memory. Cache disabled.
```

CA Directory disables caching and may crash while trying to serve the next request.

Solution:

To resolve this problem, we recommend that you disable caching by setting the following parameter in the PS DSA dxi file:

```
set lookup-cache=false
```

CA SSO Server Uninstall May Fail

Problem:

The CA SSO Server uninstall process may fail due to the lack of space in the temp directory.

Solution:

Make sure the temporary directory has at least 100 MB of free space.

CA SSO Server Data Migration Tools Do Not Support Non-English Characters from Pre-r12.1 Releases of CA SSO

The CA SSO Server data migration tools do not support the migration of data that contains characters other than those of the English locale, from previous versions of CA SSO to CA SSO r12.

Active Directory Object Limits on Microsoft Windows Platforms Affect CA SSO Server

There is a limit of 1500 objects for Active Directory running on Windows 2003. These limits affect CA SSO in several ways. The following issues apply to configurations using Active Directory as the SSO primary user data store:

- If a user group has more than 1500 members in Active Directory running Windows 2003, the Policy Manager is not able to show all users that are members of this group.
- The psbgc utility does not calculate background application list cache files for all users in a group if this group has more than 1500 members in Active Directory running on Windows 2003.
- If a user is a member of more than 1500 user groups in Active Directory running on Windows 2003, not all of these groups are considered for authorization purposes. As such, a user might have access denied to SSO applications (that is, these applications do not appear on a user's application list) even if there are explicit authorization rules granting some of the user groups which the user is a member of access to these applications.

Note: This limitation is based on the Microsoft Active Directory limitation imposed by the MaxPageSize setting. The MaxPageSize is noted in knowledge article 315071 http://support.microsoft.com/kb/315071.

Cannot Log into SSO Server from Policy Manager after Changing to Run in FIPS Mode

Problem:

After upgrading from an r8.1 CA SSO Server (at least CR6) to r12 and changing the Server mode of operation to FIPS mode, you cannot log into the Policy Manager with administrative accounts.

Solution:

Reset the admin password after upgrading.

CA SSO Server Service Throws a EventLog Error After Reboot

Problem:

I receive the following error when I reboot my computer on which CA SSO Server is installed:

```
At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.
```

I see the following description for the preceding error in the Event Viewer:

```
The CA Single Sign-On Server service hung during on starting.
```

Solution:

Ignore the error message and start the CA SSO services.

Policy Manager

The following are the CA SSO Policy Manager known issues.

Alternative Languages not Supported

The Policy Manager presents the options to install in one of the following languages:

- English
- Japanese
- Simplified Chinese
- Korean

However, only English must be used. Japanese, Simplified Chinese, and Korean are not supported.

Policy Manager Registry Keys are Deleted After Upgrading the CA SSO Server

Symptom:

When I upgrade the CA SSO Server from an earlier CR build to the current release, the Policy Manager registry key entries in the AccessControl – ClientType node are deleted and the Policy Manager does not work.

Solution:

Reinstall the Policy Manager after upgrading the CA SSO Server.

Authentication Agents

The following are the CA SSO Authentication Agents known issues.

Windows Authentication Host Keyword <auto> Error

Use of the authentication host keyword <auto> does not work if the Windows authentication method's PDCFallback property is set to No. Even when successful, the client logs an error for failure to find the authentication host <auto>.

Authentication Agents Port Conflict

For performance reasons, authentication agents do not prevent socket re-use on their listen ports. If administrators configure multiple instances of an authentication agent to run on one computer, they must ensure that they do not listen on the same port.

SSO Authentication Method Dialogs not Canceled

Problem:

The SSO authentication method checks to ensure that user names and passwords over 254 characters are not entered. The associated warning dialog is not always canceled when exiting CA SSO using the ssostatus exit menu item, or when changing a user as part of the SSO GINA workstation unlock.

Solution:

Close this dialog and any other related dialogs that are not automatically closed.

No Notification Given when Windows Authentication Fails

If you use the Windows authentication method and specify AutoNetworkAuth=yes, and the authentication fails for a reason other than the host being offline (for example, your password has expired), you are not informed of the error. It appears as though the authentication was not performed.

Cert Auth Authentication Does Not Work if the CA SSO Client is in FIPS-only Mode of Operation

Problem:

Cert Auth authentication does not work if the CA SSO Client is in FIPS-only mode of operation because the PKCS#12 certificate and PBE certificates being used for authentication are not FIPS compliant.

Solution:

If a Cert Auth agent must be used for authentication, the SSO Client must be installed in non-FIPS or TLS mode of communication. In TLS mode of communication, PKCS certificates, which are generated with the FIPS Compliant algorithms, must be used for proper authentication.

Interpreter

The following are the Interpreter known issues.

Lycos and Hotbot Do Not Work with sso html_search Extension

The search engines Lycos and Hotbot do not work with the Interpreter extension sso html_search.

SSO Waittext Extension Failure

If the text that the sso waittext is waiting for is selected in the target window, the sso waittext fails and you receive an error message.

Session Administrator

The following are the Session Administrator known issues.

Internet Shortcut Is Not Created in Mozilla or Firefox

Problem:

The Session Administrator's Internet shortcut is not created in Mozilla or Firefox bookmarks when it is used as the default browser.

Solution:

Import the Session Administrator's Internet shortcut from Microsoft Internet Explorer Favorites into Mozilla or Firefox Bookmarks.

Navigating Using Interactive Mode

Problem:

If you install using interactive mode, and you progress past the install location screen and then navigate back to that screen and change the install location, all information you have entered during the install may revert to the default values.

Solution:

Re-enter all values.

Support for FIPS

Session Administrator does not support FIPS 140-2. To use Session Administrator, install the CA SSO server in a non-FIPS mode or mixed mode.

IPv6 Networking not Supported

Problem:

Session Administrator does not support IPv6 networking.

Solution:

To use Session Administrator, enable IPv4 communications between machines on which the SSO Server and SSO Session Administrator are installed.

Password Synchronization Agent (PSA)

The following are the Password Synchronization Agent (PSA) known issues.

PSA Modify/Repair Installation Functionality not Available

Problem:

The PSA modify/repair installation functionality is not available.

Solution:

Use the Windows Add/Remove Programs to remove the previous version of the Windows PSA, then re-install the r12 PSA.

Application Wizard

The following are the Application Wizard Known Issues.

Punctuation Characters must not be Used in Application Windows and Pages

Your automation script may fail to correctly identify application windows and pages if punctuation characters are used to identify the application window or page. Do not use punctuation characters to identify application windows and pages.

For Windows applications:

- Identify any punctuation characters in the window title that may be causing your automation script to fail to find the window.
- On the Automating windows dialog, replace any punctuation characters in the Title or Text fields with '*' wildcard characters.

For browser-based applications:

- Identify any punctuation characters in the page title that may be causing your automation script to fail to find the web page.
- On the Automating forms dialog, in the Page Title field, use only an initial substring of the page title that does not contain punctuation characters.
- In the Unique Text field, use only alphanumeric and whitespace characters.

Do Not Use Non-Standard Control Types on the Window You Are Automating

Problem:

The Application Wizard may not detect some controls on the window you are automating if the Windows application uses non-standard control types or renders its own GUI elements.

Solution:

If a control does not appear in the table of controls on the bottom of the Automating window dialog:

- Select the Show All check box.
- Examine the table to see if the control has been listed as an unrecognized control type and assign an action to it.

Note: You can only assign the Click, Click exact point, and Type other text actions to these types of controls.

SSO Client

The following are the SSO Client known issues.

Dialogs Are Not Closed

Problem:

Some third-party dialogs are not always canceled when exiting CA SSO using the ssostatus Exit menu item, or when changing a user as part of the SSO GINA workstation unlock.

Solution:

Close these dialogs and any other related dialogs that are not automatically closed

Keep Servers Listed to a Minimum

Problem:

The SSO Client takes longer to authenticate a user and launch applications if there are numerous host names specified in the current server set.

Solution:

Keep the number of servers listed in your server set to a minimum, and avoid host names that do not currently resolve.

Taskbar Right-Click Menu Does Not Work when Launchbar Is Docked

Problem:

When the Launchbar is docked, the right-click menu does not work.

Solution:

Un-dock the Launchbar.

Taskbar Icon Does Not Disappear when Launchbar Application Is Exited

Problem:

If you exit the Launchbar application when it is docked, the taskbar icon does not immediately disappear.

Solution:

Click the taskbar icon.

Launchbar Screen Size Does Not Automatically Adjust

Problem:

The width of the docked Launchbar is determined as a percentage of the screen size. If you change the resolution on your screen, the Launchbar does not automatically adjust accordingly. You may therefore not see all of the Launchbar if you lower the screen resolution.

Solution:

Adjust the Launchbar size after the resolution has changed.

Launchbar May Not Resize Correctly

If you configure automatic button size (ButtonSize=auto) in the Client.ini file, the Launchbar may not resize as expected when you log off.

Application Names May Be Truncated

Application names can be truncated and a garbage character placed at the end if very long application names are used.

Event Commands May Execute in Both Local and Remote Sessions

If a remote desktop connection is used to access the local host, the SSO sign on and sign off event commands may execute in both the local and remote session.

Navigating Using Interactive Mode

Problem:

If you install using interactive mode, and you progress past the install location screen and then navigate back to that screen and change the install location, all information you have entered during the install may revert to the default values.

Solution:

Re-enter all values.

Remote Desktop Logon for GINA and Credential Providers Fails

The Remote desktop logon for GINA and credential provider fail the first time if the remote logon is preceded by a local logon to the workstation.

Icons for Disabled and Offline Applications Are Not Grayed Out

Symptom:

The icons for disabled and offline applications are highlighted and are not grayed out in my application list.

Solution:

To gray out icons for disabled or offline applications, use the default CA SSO application icon. Use the following entry in the Launchbar section of Client.ini to set the CA SSO application icon as default for disabled applications:

DisplayDefaultIconForDisabledApp

Specifies that the default icon is displayed for disabled applications.

Value: [yes|no]

Default: no

Cannot Connect to IE7 without specifying an URL with the html_browse extension

Valid on IE7 in protected mode on Windows Vista with UAC enabled

Symptom:

I cannot connect to IE7 without specifying an URL with the html_browse extension when IE7 is in a protected mode on a Windows Vista machine with UAC enabled.

Solution:

When you do not specify a URL with html_browse extension, CA SSO tries to open IE with the default home page. If the default home page is an unprotected URL and IE is set to work in a protected mode, html_browse cannot launch the URL. To launch the URL, add a protected URL as the default home page.

Cannot Connect to a URL using html_connect Extension if the Username is Administrator

Valid on IE7 in protected mode on Windows Vista with UAC enabled

You cannot connect to a browser window using the html_connect extension if you are logged in as a user with the username Administrator when UAC and Protected mode are on with IE7 on Windows Vista.

Chapter 9: International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

CA SSO is internationalized and now runs on the following non-English platforms:

- French
- German
- Italian
- Spanish
- Swedish

Note: If you run the product in a language environment *not* listed in the above-mentioned list, you may experience problems.

The CA SSO r12 CR02 Client is localized into the following languages:

- French
- German
- Italian
- Spanish
- Swedish

Chapter 10: Accessibility Features

CA is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of CA SSO.

Note: For more information about CA's accessibility initiatives, go to www.ca.com.

This section contains the following topics:

Product Enhancements (see page 64)
Keyboard Shortcuts (see page 66)
Hot Keys (see page 67)

Product Enhancements

SSO Client offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse
- Support

Note: The following information applies to Windows-based and Macintosh-based applications. Java applications run on many host operating systems, some of which already have assistive technologies available to them. For these existing assistive technologies to provide access to programs written in JPL, they need a bridge between themselves in their native environments and the Java Accessibility support that is available from within the Java virtual machine (or Java VM). This bridge has one end in the Java VM and the other on the native platform, so it is slightly different for each platform it bridges to. Sun is currently developing both the JPL and the Win32 sides of this bridge.

Display

To increase visibility on your computer display, you can adjust the following options:

- Font style, color, and size of items

  Lets you choose font color, size, and other visual combinations.

- Screen resolution

  Lets you change the pixel count to enlarge objects on the screen.

- Cursor width and blink rate

  Lets you make the cursor easier to find or minimize its blinking.

- Icon size

  Lets you make icons larger for visibility or smaller for increased screen space.

- High contrast schemes

  Lets you select color combinations that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

- Volume

  Lets you turn the computer sound up or down.

- Text-to-Speech

Lets you hear command options and text read aloud.

- Warnings

  Lets you display visual warnings.

- Notices

  Gives you aural or visual cues when accessibility features are turned on or off.

- Schemes

  Lets you associate computer sounds with specific system events.

- Captions

  Lets you display captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

- Repeat Rate

  Lets you set how quickly a character repeats when a key is struck.

- Tones

  Lets you hear tones when pressing certain keys.

- Sticky Keys

  When a shortcut requires a key combination, lets you press a modifier key, such as Shift, Ctrl, Alt, or the Windows Logo key, and have it remain active until another key is pressed.

Mouse

You can use the following options to make your mouse faster and easier to use:

- Click Speed

  Lets you choose how fast to click the mouse button to make a selection.

- Click Lock

  Lets you highlight or drag without holding down the mouse button.

- Reverse Action

  Lets you reverse the functions controlled by the left and right mouse keys.

- Blink Rate

  Lets you choose how fast the cursor blinks or if it blinks at all.

- Pointer Options

  Let you do the following:

  - Hide the pointer while typing
  - Show the location of the pointer

- Set the speed that the pointer moves on the screen
- Choose the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Support

You can use the following options to receive SSO support.

- Online and email support

  Lets you receive help if you are hard of hearing.

  Note: Online support is partially accessible for those with visual disabilities.

- Phone Support

  Lets you receive help if you have visual disabilities.

Keyboard Shortcuts

The following table lists the keyboard shortcuts that SSO supports:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+K	Find Next
Ctrl+F	Find and Replace
Ctrl+V	Paste
Ctrl+S	Save
Ctrl+Shift+S	Save All
Ctrl+D	Delete Line
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End

Hot Keys

Following are the SSO Dialogs and the hot keys that are available for the controls:

Set Login Information Dialog

- Login Name

  Alt+L

- New Password

  Alt+N

- Verify Password

  Alt+V

- Advanced

  Alt+A

Close SSO Session

- Close & Selection Session

  Alt+S

- Continue Login

  Alt+O

- Cancel Login

  Alt+C

My Applications

- Open

  Alt+O

- Change Password

  Alt+P

- Startup Group

  Alt+G

- Desktop

  Alt+D

- Refresh

  Alt+F

My Details

- Change Authentication Details

  Alt+A

Advanced Password Options

- Set Login Information

  Alt+L

- Cancel Pending Password Change

  Alt+P

End-User License Agreement

- Print

  Alt+P

About CA Single Sign-On

- Third Party Notices

  Alt+T

- System Info

  Alt+I

- Tech Support

  Alt+S

Server Set Selection

- Server Set

  Alt+S

- Auth. Method

  Alt+A

- Domain

  Alt+D

- Log on

  Alt+L

Server Set Selection (GINA configuration)

- Windows Only Logon

  Alt+W

- Logoff

  Alt+O

- Shutdown

  Alt+U

Authentication - SSO

- User Name

  Alt+U

- Password

  Alt+P

- Change

  Alt+C

- (GINA configuration controls) Domain

  Alt+D

Change Credentials - SSO

- User Name

  Alt+U

- Old Password

  Alt+O

- New Password

  Alt+N

- Verify Password

  Alt+V

- (GINA configuration controls) Domain

  Alt+D

Authentication - RSA SecurID

- Existing User

  Alt+E

- New User

  Alt+N

- Username

  Alt+U

- PIN

  Alt+P

- Token Code

  Alt+T

- (GINA configuration controls) Domain

  Alt+D

Pin Request - RSA SecurID

- System generation

  Alt+S

- User generation

  Alt+U

New PIN Entry - RSA SecurID

- New PIN

  Alt+N

- Confirm PIN

  Alt+C

Next Token - RSA SecurID

- Token code

  Alt+T

Authentication - LDAP

- User Name

  Alt+U

- Password

  Alt+P

- Change

  Alt+C

- (GINA configuration controls) Domain

  Alt+D

Change Credentials - LDAP

- User Name

  Alt+U

- Old Password

  Alt+O

- New Password

  Alt+N

- Verify Password

  Alt+V

- (GINA configuration controls) Domain

  Alt+D

Authentication - Certificate

- PKCS#11 Token

  Alt+T

- PKCS#12 File

  Alt+M

- Change

  Alt+C

- (GINA configuration controls) Domain

  Alt+D

Certificate

- Select a certificate for authentication

  Alt+S

- Details

  Alt+D

Authentication - WIN

- User Name

  Alt+U

- Password

  Alt+P

- Change

  Alt+C

- (GINA configuration controls) Domain

  Alt+D

Change Credentials - WIN

- User Name

  Alt+U

- Old Password

  Alt+O

- New Password

  Alt+N

- Verify Password

  Alt+V

- (GINA configuration controls) Domain

  Alt+D

Error Message Box

- Yes

  Alt+Y

- No

  Alt+N

- Retry

  Alt+R

- Details

  Alt+D

Unlock Computer

- User Name

  Alt+U

- Password

  Alt+O

- Domain

  Alt+D

Log Off Windows

- Log Off

  Alt+L

- No

  Alt+N

Log On to Windows

- User Name

  Alt+U

- Password

  Alt+O

- Domain

  Alt+D

- Shutdown

  Alt+S

CA Single Sign-On Security

- Lock Computer

  Alt+K

- Log Off

  Alt+L

- Shut Down

  Alt+S

- Change Password

  Alt+C

- Task Manager

  Alt+T

Change Password (Windows)

- User Name

  Alt+U

- Domain

  Alt+D

- Old Password

  Alt+O

- New Password

  Alt+N

- Confirm New Password

  Alt+C

Shutdown Computer

- What do you want the computer to do?

  Alt+W

The following are the context menu items and the hot keys that are available:

- Log On

  Alt+N

- Log Off

  Alt+F

- Refresh Application List

  Alt+R

- Applications

  Alt+A

- Open SSO Tools

  Alt+T

- Open LaunchBar

  Alt+L

- Lock Computer

  Alt+C

- About

  Alt+B

- Exit

  Alt+E

Chapter 11: Bookshelf

The Bookshelf provides access to all CA SSO documentation from a central location. The Bookshelf includes the following:

- Single expandable list of contents for all guides in HTML format
- Full text search across all guides with search terms highlighted in the content and ranked search results
- Breadcrumbs that link you to higher level topics
- Single index across all guides
- Links to PDF versions of guides for printing

Viewing the Bookshelf requires Internet Explorer 6 or 7 or Mozilla Firefox 2. For bookshelf links to PDF guides you can print, Adobe Reader 7 or 8 is required. You can download a supported version of Adobe Reader at www.adobe.com.

The PDF guides for this product are as follows:

- Administration Guide
- CA SSO Client Online Help
- Implementation Guide
- CA SSO Policy Manager Help
- Release Notes
- Tcl Scripting Guide

To use the Bookshelf

1. Locate and open the documentation folder from the product installation folder.
2. Choose one of the following methods to open the bookshelf:
   - Open the Bookshelf.hta file if the bookshelf is on the local system and you are using Internet Explorer.
   - Open the Bookshelf.html file if the bookshelf is on a remote system or if you are using Mozilla Firefox.

Chapter 12: Published Fixes

The complete list of published bug fixes for this product can be found through Published Solutions on CA Support Online.

Appendix A: Third Party Acknowledgements

This section contains the following topics:

Softwares Under the Apache License (see page 82)
Boost 1.40 (see page 85)
TCL 8.4.13 (see page 86)
Tclxml 2.6 (see page 87)
OpenSSL 0.9.8.d and 0.9.8.h (see page 88)
Zlib V1.2.3 (see page 90)

Softwares Under the Apache License

Portions of this product include software developed by the Apache Software Foundation (http://www.apache.org/).

- Log4cplus 1.0.2
- Tomcat 5.5.12

The Apache software is distributed in accordance with the following license agreement:

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Boost 1.40

Boost Software License - Version 1.0 - August 17th, 2003

This product includes software distributed under the following license agreement:

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

TCL 8.4.13

This product includes TCL v.8.4.13, which is distributed in accordance with the following license: This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files. The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply. IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS. GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Tclxml 2.6

Portions of this product include software developed by the Zveno Pty Ltd. The Tclxml software is distributed in accordance with the following license agreement:

Copyright (c) 1998-2003 Zveno Pty Ltd http://www.zveno.com/ Zveno makes this software available free of charge for any purpose. This software may be copied, and distributed, with or without modifications; but this notice must be included on any copy. The software was developed for research purposes only and Zveno does not warrant that it is error free or fit for any purpose. Zveno disclaims any liability for all claims, expenses, losses, damages and costs any user may incur as a result of using, copying or modifying this software. Copyright (c) 1997 ANU and CSIRO on behalf of the participants in the CRC for Advanced Computational Systems (|&&|ACSys|&&|). ACSys makes this software and all associated data and documentation (|&&|Software|&&|) available free of charge for any purpose. You may make copies of the Software but you must include all of this notice on any copy. The Software was developed for research purposes and ACSys does not warrant that it is error free or fit for any purpose. ACSys disclaims any liability for all claims, expenses, losses, damages and costs any user may incur as a result of using, copying or modifying the Software.

OpenSSL 0.9.8.d and 0.9.8.h

This product includes software developed by the OpenSSL Project 0.9.8.d and 0.9.8.h for use in the OpenSSL Toolkit (http://www.openssl.org/). This product also includes libraries from an SSL implementation written by Eric Young (eay@cryptsoft.com).

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Terms and Conditions for the Use of xmlsec-openssl:

OpenSSL License

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This product includes software written by Eric Young (eay@cryptosoft.com). Terms and Conditions for the Use of xmlsec-openssl:

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Zlib V1.2.3

This product includes zlib developed by Jean-loup Gailly and Mark Adler.