CA Single Sign-On

Release Notes

r12.1 CR05

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 that you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following resources:

- 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

Providing Feedback About Product Documentation

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

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

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

Chapter 2: Changed Features in CA SSO r12.1 CR01

This section contains the following topics:

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*.

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*.

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.

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. Log in 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.

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.

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. Log in 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.

Chapter 3: Fixed Issues List

This section contains the following topics:

Issues Fixed in CA SSO r12.1 CR01

The following issues are fixed in this release:

Problem ID	Description	Resolution
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.
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.
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.

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*.
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 to the CA SSO Server topic in this guide.

Issues Fixed in CA SSO r12.1 CR02

The following issues are fixed in this release:

Problem ID	Description	Resolution
1066	The CA SSO interpreter is unable to type extended unicode character.	This issue is fixed.
1081	The AppWizard does not accept UTF-8 characters in script name.	This issue is fixed.
1075	Auto login to Windows in the shared workstation mode is not working.	This issue is fixed. For more information, see the *Implementation Guide*.
1045	CA SSO shell extension commands getscrape and waittext fail with Internet Explorer 8.0.	This issue is fixed.
1077	When [PasswordDialogLabels] section is empty in Client.ini, change password option is not working.	This issue is fixed.

Problem ID	Description	Resolution
1082	When smart card is removed Windows workstation is not locked.	This issue is fixed.
1083	SSO status window does not exit during Workstation shutdown.	This issue is fixed.

Issues Fixed in CA SSO r12.1 CR03

The following issues are fixed in this release:

Problem ID	Description	Resolution
1075	On Windows 7, fast user switching is delayed.	This issue is fixed. Code is modified to send a log out notification to the LogonUI.exe.
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 fully loaded, the script interpreter crashes.	This issue is fixed. All calls to Release() function on pointers to COM objects are now guarded.
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).
1105	When upgrading to 12.0 CR7, "EnforcePasswordPoliciesInLearn Mode" 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.

Problem ID	Description	Resolution
1107	When SSO 8.0 Clients connect to SSO Server 12.0, CPU use 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.
1117	On Windows, if you log in to an LDAP browser as an Administrator, you can deep copy existing LoginInfos and access credentials of an application.	This issue is fixed. The SSO Server is modified to support enhanced password encryption mechanism.
1118	During CA SSO installation, if the version of the existing JavaAccessBridge component is lower than 2.0.1 on the computer where SSO Client is installed, the SSO Interpreter fails.	This issue is fixed. The SSO Client Installer is modified to replace any lower version of JavaAccessBridge with JavaAccessBridge 2.0.1.
1119	The text is truncated on the CA SSO GUI of Swedish.	This issue is fixed. The GUI is modified to avoid text truncation.

Issues Fixed in CA SSO r12.1 CR04

The following issues are fixed in this release:

Problem ID	Description	Resolution
1107	In SSO r12, when the policyserver.exe is executed in farm server deployments, it results in high or critical CPU use.	This issue is fixed.
1141	When using x64 Windows LDAP environment, the ldap_explode_dn tokenizes UPN syntax user names which results in authentication failure.	This issue is fixed. DN separation is now performed for Distinguished Name syntax and not for UPN syntax user names.

Problem ID	Description	Resolution
1142	When Show Desktop is selected in Windows, the SSO Status or Toolbar hides completely.	This issue is fixed. The code is modified to handle *show desktop* event. The toolbar now appears in docking state after selecting Show Desktop.
1143	When Ctrl+R is entered in SSO r12.1 CR2, the 3270 script fails to execute.	This issue is fixed. The Ctrl+key combination virtual code has been added to the virtual code table *sso type*.
1146	When SSO Client users who are logged off, login to the application after eight hours, they see a re-authenticate request.	This issue is fixed. The new token replaces the expired token.
1147	Transaction Manager crashes when Policy Manager is run on a Windows 2008 x64 computer.	This issue is fixed. Transaction Manager picks up transactions from the Policy Manager without any errors.
1148	When watch list enabled applications are launched, they get executed twice.	This issue is fixed.
1149	The Connection Info Dialog in the Policy Manager displays error messages after successful connection.	This issue is fixed.
1151	On Windows 7, if one of the container applications contains an invalid icon file path then the container drop-down list does not open.	This issue is fixed.
1152	The memory occupied by the PolicyServer.exe increases when the Browser Helper Object calls SSOCLAPI.	This issue is fixed.
1153	In German versions of Windows Vista and Windows 7, Offline Data Cache get virtualized which denies access to folders.	This issue is fixed. In Windows Vista and Windows 7 cacls.exe is depreciated, and icacls.exe is used to grant permission to folders.
1156	On Windows 7, applications take more time to launch.	This issue is fixed.
1157	When using the x64 Windows LDAP environment, the ldap_explode_dn tokenizes user names which contain ".", which results in authentication failure.	This issue is fixed.

Issues Fixed in CA SSO r12.1 CR05

The following issues are fixed in this release:

Problem ID	Description	Resolution
1182	On SSO Server x64, when user name contains special characters (extended ASCII /ANSI), login through SSO client fails.	This issue is fixed. The CA SSO Server now uses CA LDAP x64 library to interact with all types of directories.
1183	When setting CertStore to PKCS11 the Pkcs11TokenAbsenceBehavior is honored, but it is not honored while setting the CertStore to MSCAPI. When you remove the MSCAPI Smart card from the card reader Logoff does not work as expected.	This issue is fixed. A condition has been added to make the Sign on state to be set for MSCAPI Smart Cards also.
1184	On Windows 2008, Sample Authentication Agent fails to start.	This issue is fixed. CA SSO Sample Authentication Agent will use newly created DLL wraps for SSOCOMMS library to work around the access violation problem.
1185	When the SSO Client is running in a non-English Windows box during Windows authentication, the following error message appears: LookupAccountName("NT AUTHORITY\NETWORK") failed. Error: 1332.	This issue is fixed.CA SSO Client now uses well know SID S-1-5-2 corresponding to account ("NT AUTHORITY\NETWORK"). This SID is independent of the location of the operating system.
1186	SSO and Site Minder Integration fails for x64 SSO Client.	This issue is fixed.
1188	The “sso waittext” extension does not work properly on x64 bit machines. It returns true even when it does not find the given string.	This issue is fixed. The code is modified and INVALID_HANDLE_VALUE is now passed to the API.
1189	On the x64 platform the extension sso html_connect with -title option does not work as expected	This issue is fixed. The string is allocated using SysAllocString, so that the the sso html_connect with option –title works as expected on both x64 and x86 platforms
1191	Windows Authentication agent does not start automatically at system startup if it is installed on Windows 2008 r2, where the SSO Server is installed.	Issue is fixed with delay start option. WinAuth service startup type on Windows 2008 R2 is updated to Delayed Start as part of fixing this issue.

Problem ID	Description	Resolution
1192	When creating an (AD) userDIR containing '-' character in its name, SSO prefixes the trailing string to the $_Password and $_Nextpwd.	This issue is fixed.
1193	While setting up the psbgc utility on SSO servers running r12.1, an error appears in the log. This error occurs when it tries to generate the cache for the "ldap-pers" user in each of the OU's that you run the psbgc utility against. The error says that "Target user not found", indicating that the "ldap-pers" user does not exist in any of the OU's.	This issue is fixed.
1194	In SSO r12.1 CR4 on Solaris zone, errors occur when the application is not active during a period of time.	This issue is fixed.
1195	SSO and SiteMinder integration breaks when SiteMinder points to a different SSO Server other than the localhost.	This issue is fixed. The incoming timeout in timeval structure is represented appropriately.
1199	When you use Windows 7 32-bit (x86) a problem occurs with the command waittext in a script. The following error message appears : "The SSO TCL interpreter can't execute sso waittext time expired : the text not found".	This issue is fixed.
1202	When you startup or shutdown SSO r12.1 CR4, RHEL r5.5/5.6 x64, the PolicyServer process crashes intermittently, and the syslog is revealed.	This issue is fixed.
1205	When you enable “EnforcePasswordPoliciesInLearnMode”, Server throws an error message which says the password has been already used indicating that the new password is part of password history.	This issue is fixed.

Problem ID	Description	Resolution
1209	On x64 platforms, when SSO Server and Policy Manager are installed on the same x64 machine the following problems are seen: Error messages do not have descriptive text When you click Help Menu,and select the About option, error messages are displayed No logo is displayed	This issue is fixed.

Chapter 4: New Features in CA SSO r12.1

This section contains the following topics:

Support for Java Applications

CA SSO now supports Java applications. The following CA SSO components are enhanced to provide single sign-on capability to java applications.

CA SSO Client

Use the CA SSO Client to provide single sign-on capabilities for Java applications.

Application Wizard

Use the Application Wizard to generate login scripts for Java applications.

CA SSO Interpreter

The CA SSO Tcl extensions are modified to support Java applications.

Changes to Client.ini File

A new section [WindowWatcher] is added to the Client.ini file. The following keys are part of the [WindowWatcher] section:

- EnableWindowWatcher
- EnableCaseInsensitiveMatch
- PollInterval

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

Support for Window Watching Capability

CA SSO is enhanced to include window watching capability. Window Watcher is a component of the CA SSO Client that continuously monitors the windows or applications that a user launches outside of CA SSO Client. When users launch applications from their computer, the CA SSO Client compares the application attributes with a Watchlist stored in the CA SSO Server. If the application attributes match the attributes of any CA SSO enabled application in the Watchlist, the CA SSO Client supplies the login credentials for the user and logs the user into the application. Window Watcher extends CA SSO functionality to applications that are not launched using the CA SSO Client.

To support window watching capability, the following changes are made to the CA SSO components:

CA SSO Client

The CA SSO Client is enhanced to include the window watcher. To enable or disable window watching capability in the CA SSO Client, a new section [WindowWatcher] section is added to the Client.ini file.

Note: For more information on configuring the window watcher capability, see the *Implementation Guide*.

Application Wizard

The Application Wizard is enhanced to generate a Watchlist. This Watchlist is used by Window Watcher to monitor applications.

Note: For more information about how to generate Watchlist, see the Adding Applications chapter in the *Implementation Guide*.

Policy Manager

The Policy Manager lets you upload the Watchlist generated by Application Wizard to The CA SSO Server. The CA SSO Server in turn passes on this list to the CA SSO Client.

Enhancements to the Application Wizard

The following new features are added to the Application Wizard:

Support for Java applications

Use the Application Wizard to generate Tcl login scripts for Java applications.

Support for HLL applications

Use the Application Wizard to generate Tcl login scripts for HLL applications.

Support for editing and testing Tcl scripts

When you generate a Tcl script, you can test or edit the generated script before uploading the script to the CA SSO Server.

Support for IE tabs

The Application Wizard lets you generate scripts to accommodate the tabs feature in IE7 and IE8.

Generate Watchlist

Use the Application Wizard to generate watchlists and upload them to the CA SSO Server. A watchlist is a set of application attributes such as the application name, application executable path, window title, and application class name. The CA SSO Client uses the watchlists to monitor applications that the users launch directly from their desktops. If a user launches an application directly from the desktop, the CA SSO Client matches the application attributes with the watchlist. If the match is successful, the CA SSO Client provides single sign-on capability by logging in the users to the application.

Enhancements to the Policy Manager

To support window watcher capability of CA SSO, the Policy Manager is enhanced to let users enable window watcher capability for an application and upload the Watchlist, containing application attributes, to the CA SSO Server. If you want your users to launch and use their CA SSO-enabled applications without using CA SSO Client, enable window watcher capability for an application using the Policy Manager. The following new options are added to the Attributes section of Application Resources in Policy Manager:

Upload Watchlist

Lets you upload watchlists generated using Application Wizard to the CA SSO Server.

Enable Window Watcher

Select this checkbox to enable the CA SSO interpreter to detect the launch of CA SSO enabled applications from their desktop (outside of the CA SSO Client), provide login credentials to the application, and log in users.

Enhancements to TCL Scripts

The CA SSO TCL extensions are enhanced to support the following new features:

Support for Java applications

Existing TCL extensions are enhanced to support java applications. The following variable is enhanced to identify a target application as Java application:

`_Mode`

You must identify a Java application in the first line of the TCL script before scripting other functionality. Include the following line of code before writing any script for Java applications:

```
set _Mode Java
```

Support for tabs in IE7 and above

A new argument -newtab is added to the html_browse TCL extension to support tabs in IE7 and above.

-newtab

Specifies if the URL is opened in a new tab of the existing IE instance. For IE 7 or IE 8, if the value is set to Y (Yes), the specified URL is opened in a new tab. If the value is set to N (No), the specified URL is opened in a new IE instance. For IE 6 and earlier versions of IE, the specified URL is always opened in a new IE instance irrespective of the value for this key.

Chapter 5: New Features in CA SSO r12.1 CR02

This section contains the following topics:

New Command Line Option to Check Client Availability Status

New command line option, *--check_status* has been added to let you check the availability status of the client. If the client is offline, this option automatically changes the status of the client from offline to online when the server is available.

Chapter 6: New Features in CA SSO r12.1 CR03

This section contains the following topics:

Support for Oracle Jinitiator

CA SSO is enhanced to support Oracle Jinitiator to launch CA SSO.

CA SSO Integration Kit

CA SSO now delivers an integration kit that lets you customize your applications. The CA SSO integration kit contains the following components:

- Sample authentication agent for Windows
- Server SDK for servers on Windows, Linux, and Solaris, and clients on Windows
- SSO clapi library for Windows
- Sample code APIs

Support for Microsoft Windows 2008 R2

CA SSO is enhanced to support Microsoft Windows 2008 R2.

Chapter 7: New Features in CA SSO r12.1 CR04

This section contains the following topics:

Enhancement to the TCL Script

The CA SSO TCL extension has been enhanced to hide sensitive data like the username and password for script variables in error dialogues.

Changes to SSO Token Cookie

The SSO token cookie is deleted when a user goes offline. A new cookie is created when the user returns online.

Set the *ExpireCookiesWhenOffline* value to true to enable this setting.

Enhancements to SSOLaunchBar

The CA SSO launch bar is enhanced to support the following new features when HideOnMinimize parameter in the LaunchBar section is set to *yes* in the Clinet.ini:

- Launch bar hides when minimized.
- Launch bar appears when you double-click SSO Status icon.

Support for Citrix

CA SSO is enhanced to support Citrix XenApp 5.0 and 6.0.

AD Configuration Wizard

The Active Directory configuration wizard takes you through the process of configuring and creating the Active Directory as the user data store for CA SSO.

The Active Directory configuration wizard has the following limitations:

- You cannot edit configurations of user data stores through the Active Directory configuration wizard.
- SSL communication configuration cannot be performed through the Active Directory configuration wizard.

Support for Microsoft Windows 2008 R2 SP1 (64-bit)

CA SSO is enhanced to support Microsoft Windows 2008 R2 SP1 (64-bit).

Support for Microsoft Windows 7 SP1

CA SSO Client is enhanced to support Microsoft Windows 7 SP1.

Support for Windows 2008 R2 Hyper-V

CA SSO is enhanced to support Windows Server 2008 R2 Hyper-V.

Enhancement to CAPKI

CA SSO has upgraded CAPKI to version 4.2.2 (Linux and Solaris) and 4.2.3 for all components.

Enhancements to SSO and SiteMinder Integration

CA SSO has been upgraded to support .NET Request Validator on the IIS Server. The SSO Client can now encode characters '<' and '>' in the SSO cookie and does not cause any authentication failures.

To generate the encoded cookie, set the SSOTokenVersion value to 12 in [WebAgentIntegration] section in Client.ini file.

Note: SiteMinder version r12.0 SP3 CR7 or above supports SSOTokenVersion value 12.

Chapter 8: New Features in CA SSO r12.1 CR05

This section contains the following topics:

Disable Windows PSA

The CA SSO Windows Password Synchronization Agent has been enhanced so that the user can disable it without having to reboot or uninstall the product. The support code that enables the functionality has been added. Poll configuration is set to default. The default poll interval has been changed to allow changes made to PSA Configuration to be picked up with a reboot even in the first instance. This enhancement enables business needs outside of the SSO environment to continue to function, and limits the involvement of Active Directory Administrators in cases where CA SSO cannot retrieve password updates.

Double-click on CA SSO Launchbar

The CA SSO launchbar is enhanced so that the script does not lose focus while launching applications from the browser on double-click. The DoubleClickInterval parameter has been added to Client.ini file. The customer can now launch applications on double-click from the SSO launchbar without causing TCL to fail.

CA SSO PSA Installer Option Added

CA SSO PSA Installer has been enhanced. A check box is added for "AllowPasswordChangeOnServerdown" to make it a parameter to set during the SSO PSA Install.

IE9 Certified for CA SSO

Internet Explorer 9 has been certified for CA SSO.

CA Directory R12SP8 Certified for CA SSO

The functionality of CA Directory r12SP8 has been verified for CA SSO r12.1.

Windows 2008 R2SP1 Certified for CA SSO

CA SSO r12.1 has been certified with Windows 2008 r2 SP1 Standard Edition.

Application Wizard Support for x64 Windows Platforms

The CA SSO Application Wizard now supports x64 windows platforms and generates the TCL scripts for the required applications.

CA License Upgrade

CA SSO has been enhanced to to CA License version which has vulnerabilities fixed

The following upgrades have been made:

- CA Licensing in SSO Server Linux has been replaced with version 1.90.04
- CA Licensing in SSO Server Solaris has been replaced with version 1.90.03
- CA Licensing in SSO Server Windows x32/x86 has been replaced with version 1.90.03
- CA Licensing in SSO Server Windows x64 has been replaced with version 1.90.03

Extension Added for Protected Mode Compatibilty

A new extension html_getscrape, has been written to make sure that CA SSO's screen scraping calls do not fail when the web browser is running in "Protected Mode". The html _getscrape extension returns the text content in the html page.

For more information, refer to the *CA SSO Tcl Reference Guide*.

Enhancement to the TCL Script

An extension, html_searchtext, has been added to the TCL Script to search for the presence of texts in a webpage.

For more information, refer to the *CA SSO Tcl Reference Guide*.

Chapter 9: Operating System Support

The following describes the operating system support for each component.

This section contains the following topics:

CA SSO Server

CA SSO only supports server farms that have all CA SSO Servers installed on computers with the same operating system. For example, you cannot have a server farm with one CA SSO Server installed on Solaris, another installed on Windows, and a third installed on HP-UX.

Note: The CA SSO Server runs in 32-bit mode on UNIX 64-bit platforms. The CA SSO Server runs as a 64-bit application on a 64-bit Windows operating system.

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2008 Enterprise Edition SP1 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

Solaris (SPARC)

- 10 including zone and LDOM support

You can install the CA SSO Server on Solaris 10 in a global zone, a non global zone, or both. Each installation is a separate instance of a CA SSO server. If you are not running a standard Solaris 10 installation, verify that you have the following Sun packages installed before you install the CA SSO Server:

- SUNWbcp
- SUNWscpr
- SUNWscpu
- SUNWscpux
- SUNWsra
- SUNWsrh
- SUNWipc

- SUNWcsu
- SUNWnisu

Apart from the preceding requirements, the following additional requirements are required to install the CA SSO Server in non global zones:

- CA Access Control kernel module (SEOS_load) must be installed and loaded in the global zone before installing CA SSO Server in a non global zone.
- Use install_base script when installing CA Access Control in the global zone.

Note: If the CA SSO server is installed in both global and non global zone, the two installations must be in a similar mode of operation--non-FIPS, FIPS, or mixed mode.

LINUX (x86 and X64)

- Red Hat Enterprise Linux 5

CA SSO Client

The CA SSO Client is supported on the following operating systems:

Microsoft Windows (32-bit)

- 7
- 7 SP1
- 2008 Enterprise Edition SP1 and SP2
- 2008 Enterprise Edition SP1 and SP2 on VMware ESX Server 3.5
- Vista SP2
- Vista SP2 on VMware ESX Server 3.5
- Server 2003 Enterprise Edition and Standard Edition R2 SP2
- Server 2003 Enterprise Edition and Standard Edition R2 SP2 on VMware ESX Server 3.5
- Server 2003 Enterprise Edition and Standard Edition SP2
- Server 2003 Enterprise Edition and Standard Edition SP2 on VMware ESX Server 3.5
- XP SP3
- XP SP3 on VMware ESX Server 3.5

Microsoft Windows (64-bit)

- 7 SP1
- 2008 Enterprise Edition R2 SP1
- Vista SP2

ADS Listener

The ADS Listener is supported on the following operating systems:

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

Authentication Agents

Authentication Agents are supported on the following operating systems:

Note: The authentication agents run as 32-bit applications on 64-bit operating systems.

Certificate Agent

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

LDAP Agent

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

RSA Agent

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

SSO Agent

The SSO Auth Agent is part of the CA SSO Server. See the CA SSO Server supported platforms in the previous topic.

Windows Agent

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

Password Synchronization Agent

The Password Synchronization Agent is supported on the following operating systems:

Microsoft Windows (32-bit and 64-bit)

- 2008 Enterprise Edition SP1
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition SP2 on VMWare ESX Server 3.5
- 2003 Enterprise Edition and Standard Edition R2 SP2 on VMWare ESX Server 3.5

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

LINUX (x86 and x64)

- Red Hat Enterprise Linux 5

Solaris (SPARC)

- 10 including zone and LDOM support

For CA SSO Server plug-in specifications, see the SSO Server (see page 44).

Application Wizard

The CA SSO Client is supported on the following operating systems:

Microsoft Windows (32-bit)

- 2008 Enterprise Edition SP1 and SP2
- Vista SP2
- Server 2003 Enterprise Edition and Standard Edition R2 SP2
- Server 2003 Enterprise Edition and Standard Edition SP2
- XP SP3

Policy Manager

The Policy Manager is supported on the following operating systems:

Note: The Policy Manager runs as a 32-bit application on 64-bit operating systems.

Microsoft Windows

- 2008 Enterprise Edition SP1 and SP2 (32-bit and 64-bit)
- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1 (64-bit)
- Vista SP2 (32-bit)
- 2003 Enterprise Edition and Standard Edition SP2 (32-bit)
- XP SP3 (32-bit)
- 2008 Enterprise Edition R2 SP1 (64-bit)
- Windows 7 SP1 (32-and 64-bit)
- Vista SP2 (64-bit)

Session Administrator

The Session Administrator is supported on the following operating systems:

Microsoft Windows (32-bit)

- 2003 Enterprise Edition and Standard Edition SP2
- 2003 Enterprise Edition and Standard Edition R2 SP2

Microsoft Windows (64-bit)

- 2008 Enterprise Edition R2 on VMWare ESX Server 4.0 and VMWare ESX Server 4.1
- 2008 Enterprise Edition R2 SP1

Chapter 10: System Requirements

The following describes the system requirements for each component.

This section contains the following topics:

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 11: 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.

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 on SUN Solaris and Red Hat Linux

After installing the CA SSO Server, reboot the computer to complete the installation.

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

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

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

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 r12.1:

`<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 r12.1 Client, the information in *.ini files of previous releases is migrated to the *.ini files of CA SSO r12.1. So, the entries for IdentityFile and TrustFile entries in CA SSO r12.1 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 r12.1, 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 r12.1.

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 12: Known Issues

This section contains the following topics:

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

Symptom:

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

Symptom:

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

Symptom:

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 r12.1.

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

Symptom:

After upgrading from an r8.1 CA SSO Server (at least CR6) to r12.1 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.

Issue with CA SSO Server on some Windows 2008 R2 Systems

Symptom:

On select Windows 2008 R2 boxes LogWatNT.exe (CA License component) and dxadmind.exe (CA Directory Administration Service) crash with access violation when you reboot. The following errors occur:

EventViewer shows event id 1001 for LogWatNT.exe after reboot.

EventViewer shows event id 1001 for dxadmind.exe after reboot.

Solution:

This is a known issue that does not affect the functionality of the CA SSO Server. Disable instrumentation for above two processes by applying fix T5P7031 to CA Access Control. Add LogWatNT.exe and dxadmind.exe as data to the “ExcludeProcess” value for the registry key mentioned in the above fix.

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.

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

Symptom:

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

Symptom:

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.

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.

Getscrape and Waittext Extension Failure

The SSO Extensions Getscrape and waittext do not work with a 32 bit process (that includes a 32 bit Internet explorer) on a 64 bit system. Due to the enhanced security in Internet explorer 9, these extensions do not work with IE9 on either 32 bit or 64 bit versions. As an alternative to these extensions, two new html extensions html_getscrape and html_searchtext have been created. which can be used with Internet explorer applications.

For more information about the new html extensions, see the *CA SSO TCL Reference Guide*.

Session Administrator

The following are the Session Administrator known issues.

Internet Shortcut Is Not Created in Mozilla or Firefox

Symptom:

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

Symptom:

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.

Password Synchronization Agent (PSA)

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

PSA Modify/Repair Installation Functionality not Available

Symptom:

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 r12.1 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

Symptom:

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

Symptom:

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

Symptom:

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

Symptom:

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

Symptom:

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

Symptom:

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

Symptom:

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.

Change Password Fails When Using LDAP Authentication Agent

Valid in IPv6 environment

You cannot change your password in the CA SSO Client using an LDAP authentication agent to authenticate with an Active Directory.

Citrix Application Fails to Start

Symptom:

When I launch a Citrix Application using CA SSO Client, the application fails to start, and the following messages appear:

- There is no script engine for file extension ".js".
- There is no script engine for file extension ".vbs".

Solution:

The Content Redirection properties of the application published on the Citrix Server have registered the extensions .vbs and .js. Hence, the .vbs and .js files on the Citrix Client are executed with the application instead of the default or Windows Script Host (wscript.exe).

Follow these steps:

1. On the Citrix Server, modify the Content Redirection properties for each published application by clearing the .vbs and .js file extensions.
2. On the CA SSO Client, perform one of the following tasks to re register .vbs and .js extensions with the windows script host.
   - Install the windows script engine from Microsoft. See Microsoft documentation for more information.
   - Disable program neighborhood agent file type association redirection. See Citrix Support, document ID CTX126978 for more information.
   - Patch the registry to re register .vbs and .js to windows script host.

Citrix Terminal Session Ends

Symptom:

If I publish a browser-based application using an html_browse extension to the Citrix XenApp Server 5, then the Citrix terminal session ends. This occurs if the Citrix XenApp Server 5 is installed on a Windows 2008 (32-bit or 64-bit) server.

Solution:

This is a known issue. Upgrade your Windows 2008 server (32-bit or 64-bit) and verify if OLEACC.DLL is present in the *%windir%\System32* folder.

Note: For more information about upgrading your Windows 2008 server, refer Microsoft Support website and search for KB971513 article.

SSO Client (64-bit) Cannot Launch Citrix Applications

The CA SSO Client (64-bit) cannot be used to launch Citrix Applications, as the Citrix ICA Client for native x64 platform is unavailable.

SSO Client (64-bit) Does Not Support Smart Cards

Smart cards are not supported on the SSO Client (64-bit) due to compatibility issues on native 64-bit applications.

Chapter 13: 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 r12.1 CR02 Client is localized into the following languages:

- French
- German
- Italian
- Spanish
- Swedish

Chapter 14: 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

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 it's 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 15: 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 16: 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

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.

Java Access Bridge v2.0.2

Java Access Bridge v2.0.2

This Product is distributed with Java Access Bridge v.2.0.2. Use of the Commercial Features of the Java Access Bridge for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. Oracle has provided additional copyright notices and information that may be applicable to portions of the Java Access Bridge in the THIRDPARTYLICENSEREADME.txt file that accompanies the Java Access Bridge files and at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

TCL 8.4.19

This product includes TCL 8.4.19 ,which is distributed in accordance with the following terms:

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.

A portion of tcl software was obtained under the following terms:

Copyright (c) 1988, 1989, 1993, 1994

The Regents of the University of California. 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 acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``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 REGENTS 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.

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.