eTrust® Single Sign-On

Release Summary

r8.1

Third Edition

CA Product References

This document references the following CA products:

- eTrust® Access Control (eTrust AC)
- eTrust® Directory
- Unicenter® Software Delivery
- eTrust® Audit

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 1: New Features

This section contains the following topics:

Offline Operation

Offline operation refers to the ability of the SSO Client to continue to work even when it can not establish a connection with the SSO Server or the authentication agent. When a user uses the SSO Client in offline mode, they can access specific applications that have been marked for offline use.

When to use offline operation

Offline operation is useful for two main reasons.

Ensuring uninterrupted service

You want your users to have uninterrupted access to SSO, even if the connection to the network periodically goes down. In this situation they can log onto SSO and launch all of their applications that you have marked for offline use, regardless of network connection.

Assisting laptop users

You want your laptop/remote users to use SSO when they are not connected to the network. This includes their ability to log onto Windows using the SSO GINA as well as their ability to access SSO-enabled applications. This is useful if you want users to connect to a remote network from home and therefore set up a VPN Client as an SSO-enabled application that can be launched offline and will then connect the user to the network.

Internationalization

eTrust SSO has been internationalized and now runs on non-English platforms. The product has not been translated.

SSO Client Usability Enhancements

The SSO Client has had a number of usability enhancements that allow SSO to be deployed on workstations in a multitude of different ways, and be configured to support individual company needs.

SSO Client Launchbar Interface

The SSO Client Toolbar has been replaced by the SSO Launchbar. This user interface displays all application types, including container applications and can be docked to any edge of the user's desktop.

SSO Client Status Icon

The SSO Client tray menu icon has been replaced by the SSO Status Icon. This persistent icon provides a visual indication of the Client state: user logged on, no user logged on, SSO Client offline.

The right-click menu functionality provided by the SSO Status Icon gives the end user access to the user interfaces and their SSO-enabled applications.

Active Directory Integration

eTrust SSO r8.1 provides greater integration and interoperability with Active Directory as a user datastore.

ADS Listener

When using Active Directory as the SSO user datastore, the ADS Listener "listens" for changes to user and user group information on Active Directory and sends notification of these changes to the SSO Server. This prevents the information in Active Directory and eTrust SSO from becoming out of sync.

ADS Listener enables mutual support for typical business scenarios in organizations when an employee is moved from one department (organization unit) to another or where an employee leaves a company.

Note: ADS Listener supports moving users and user groups, but does not support renaming or moving containers. (Deleting a container is supported).

MSCAPI Support

The Certificate Authentication Agent now provides support for MSCAPI certificate stores. MSCAPI certificate stores are where Windows stores digital certificates such as the My Certificates store. The Certificate authentication agent logs the user on using a certificate in the MSCAPI store, without requiring input from the user.

LDAP Authentication Agent ADS Integration

The LDAP authentication agent provides enhanced integration when using ADS as the datastore. The end user can change their domain password using the SSO Client, see notification messages such as Account Lockout and Password Expiry.

The LDAP authentication agent install has also been enhanced to provide connectivity to the ADS out-of-the-box, with no additional configuration required.

Bi-Directional Password Synchronization Agent

The Windows Password Synchronization Agent (PSA) provides password synchronization from the Domain Controller to SSO, and vice-versa. The PSA also provides the ability to change the SSO Server without requiring a reboot on the Domain Controller, as well as failover between SSO Servers.

Deployment Enhancements

eTrust SSO provides improved ease of deployment of SSO in the enterprise. This section outlines those improvements.

SSO Server Watchdog

The SSO Server Watchdog is a service that helps you monitor the status of the SSO Server. When you start the Watchdog, it runs constantly in the background and if it detects that the SSO Server is no longer responding it triggers a reboot of the SSO Server.

You can configure the Watchdog to automatically:

- Send you a message before it reboots the SSO Server
- Perform commands before or after it reboots the SSO Server

You can also manually check the status of the SSO Server by connecting to the Watchdog using a web browser. The SSO Server's Watchdog service is now capable of restarting the SSO Server when it detects that the server is down. In addition, the Watchdog's ability to report on the status of the SSO Server includes Telnet and HTTP. Using the Watchdog in conjunction with a Hardware Load Balancer greatly improves SSO Server uptime and failover.

Mixed Version Server Farm Upgrades

eTrust SSO r8.1 Server supports the operation of different versions of SSO Servers in a server farm.

This means you can have users operating in both an eTrust SSO 6.5/7.0/r8 environment and in eTrust SSO r8.1 at the same time. This is particularly useful when upgrading to the latest version of SSO: you can set up the eTrust SSO r8.1 environment and gradually migrate users to the new platform. In this scenario, users on earlier releases of the SSO Client can continue to work with older SSO Server releases while users who have been upgraded to the r8.1 SSO Client work with the new SSO Server. This allows for a phased migration to eTrust SSO r8.1, as well as a potential downgrade path.

Note: Mixed Version Server Farms is defined as servers from different versions working together, while backward compatibility is defined as clients and servers from different versions working together.

Backward Compatibility with SSO r8 Clients

SSO r8.1 Server supports SSO r8 Clients. This allows you to first upgrade all SSO Servers, leaving existing SSO r8 Clients to work with r8.1 Servers in backward compatibility mode, then gradually migrate r8 clients to SSO r8.1.

Note: r8 Clients must use r8 Authentication Agents to authenticate to an r8.1 Server.

Note: Mixed Version Server Farms is defined as servers from different versions working together, while backward compatibility is defined as clients and servers from different versions working together.

Migration

eTrust SSO provides tools to migrate your user and resource information from earlier releases. This includes a tool to migrate directly to your Active Directory implementation, as well as migrating user’s login and other SSO-specific information.

Scalability and Performance Enhancements

eTrust SSO can now be configured to support 125,000 users logging on within a defined period.

The SSO Performance Measurement Module allows you to simulate a user load to replicate the performance and scalability that CA has produced in the lab, in your enterprise. In addition, the Performance Measurement Report included in the module explains how to tune the performance of your implementation to meet your internal performance and scalability needs.

SSO Servers on UNIX

The SSO Server is supported on UNIX as well as on Windows.

The Application Wizard

The SSO Application Wizard lets you add your applications to SSO without the need to learn Tcl scripting for basic scripting tasks.

Use the SSO Application Wizard to create SSO application scripts for browser-based applications and Windows applications, such as login scripts and scripts that automate post-login tasks. For example, navigating to a specific screen or dialog in an application, or navigating to a specific web page. You can perform more complex application integration or task automation processes by writing Tcl scripts manually.

Note: The SSO Application Wizard is a standalone Windows application that does not require any other SSO components to generate scripts. However, to test Tcl scripts generated by the Application Wizard, you must install the SSO Client on the local computer.For more information on the Application Wizard, see the chapter "Adding Applications to SSO" in the *Implementation Guide*.

Chapter 2: Changes to Existing Features

This section contains the following topics:

Enhancements

This section describes what has been since the previous release.

Update Application List Cache Utility (psbgc)

The psbgc utility keeps users' applications lists up-to-date on the SSO Server. The psbgc has been enhanced to use paging access for user datastores, overcoming the limitation on the number of entries returned by a single LDAP query. The command-line interface has been extended to support additional scoped parameters: to run the psbgc for a single user, user group or container within the datastore.

SSO Scripting Improvement

eTrust SSO provides new SSO extensions, as well as enhancements to existing extensions.

Specify Position for Box

SSO Statusbox, Msgbox and Inputbox have been enhanced to provide the ability to specify their position.

Specify Window Title

SSO Statusbox and Msgbox window titles can now be specified in a script.

Text Wrapping Enhancement

The SSO Statusbox and Inputbox have been enhanced to provide text wrapping.

Tcl Status Box Enhancement

SSO script developers use the statusbox extension to display information to the end user about the progress of the Tcl script. It has been enhanced to:

- Be persistent
- Provide cancel ability
- Add checks to see what caused the statusbox to close.

SSO getmode Extension

There is a new SSO getmode extension, to return the current state of the SSO Client. This includes modes such as the SSO Client logged on, logged off and offline, as well as SSO Client logging off, SSO Client logging on and Windows station being locked.

HTML_link

An html extension to select a dynamic link within an HTML web page is now available.

Application Password Length Limitation

The application password length limitation has been extended from 21 characters to support application passwords of 254 characters.

Auditing and Logging

The auditing and logging of events which take place on the SSO Server have been improved for this release.

Silent Installation Changes

Silent installation commands have changed and been extended and now include response files.

Script Caching to Reduce Network Traffic

The SSO Client has been enhanced to store logon scripts in a local cache. This reduces the load on the network.

Support

Password Exits

The Password exit functionality has been enhanced. Existing Password Exit implementations must be rewritten to work with eTrust SSO r8.1.

Third-Party Authentication Agents

The SSO authentication agent has been enhanced to support Internationalization. Existing third-party authentication agent implementations must be rewritten to work with eTrust SSO r8.1.

The Sample Authentication Agent describes how to write a third-party authentication agent to work with eTrust SSO r8.1.

SSO Client Windows Platforms

The SSO Client for this release is no longer supported on Windows NT and 98.

Session Administrator

The Session Administrator is now a stand alone installation rather than being part of the IA Manager.

Authentication Agents

The following authentication agents are not supported for this release: Entrust, Novell, Safeword.

IAM Integration Dropped

eTrust SSO does not come as part of the eTrust IAM suite for this release. This means that the IA Manager interface is not supported for this release and the SSO Server installation is no longer done using the IAM Common Components CD.

MetaFrame Application Manager

The MetaFrame application manager is no longer necessary for Citrix Application Migration.

Upgrading and Data Migration

The SSO Server data migration tools do not support migration of data which contains characters other than those of the English locale from previous versions of SSO to SSO r8.1. Likewise, Mixed Version Server Farms do not support synchronization of data which contains characters other than those provided in the English locale between previous versions of SSO and SSO r8.1.

Mainframe Password Synchronization Agent

The Mainframe Password Synchronization agent is not provided in this release.

One-Time Password Agent

The SSO One-Time Password (OPT) Agent is not provided in this release. Instead, the eTrust SSO r8 OTP agent has been certified to work with r8.1.

Policy Server Renamed SSO Server

The Policy Server has been renamed the SSO Server.

User Data Store

eTrust Access Control is no longer supported as the user data store. It is still the administrative data store and contains information about administrators, resources and all policies.

You should use your existing LDAP user data store such as Active Directory as your user data store. If you do not have an LDAP datastore already, you can use eTrust Directory as your user datastore.

Web Agents

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

For Web access protection, eTrust Siteminder is the chosen upgrade path. For more information on this contact your local SSO Support Representative.

Resolved Issues

This section lists all the major issues that have been raised in the CA bug and issue tracking system since eTrust SSO r8.

Issues Resolved for eTrust SSO r8.1

This table lists all the major bugs and issues that were resolved since the previous release:

STAR or Patch/Testfix Number	Component	Description
QO71779	Win PSA	Agent not upgrading correctly
QO69060	Win PSA	Quoted registry ImagePath for Service
QO69099	RSA Auth Agent	Quoted registry ImagePath for Service
Q069065	Cert Auth Agent	Removal of smart card after changing authentication methods does not lock the workstation
QO69065	Cert Auth Agent	Sample NameMapping Dll added
QO69065	Cert Auth Agent	Installer updated to address configuration issues
QO69065	Cert Auth Agent	Quoted Registry ImagePath for service
QO71777	Win Auth Agent	Win auth agent install detects existing LDAP auth agent and attempts to upgrade
QO78499	Client	Access rights for Citrix/Terminal service
QO78499	Client	Access rights for Citrix/Terminal Services
QO78499	Client	GINA Unlock different user delay with UnlockStation Mode=3
QO78499	Client	GINA RDP Client refresh problem
QO78499	Client	SSO GINA, Windows Group Policy and Disable Password Change Button
QO78499	Client	Cannot login after RDP logoff
QO78499	Client	RDP Client reauth on startup
QO78499	Client	ssochlapi_getapplist fails with Client on Citrix

STAR or Patch/Testfix Number	Component	Description
QO78499	Client	SSO GINA unlock issue
QO78499	Client	SSO GINA and autostart of Client from Startup folder inconsistent
QO78499	Client	GA upgrade issues
QO78499	Client	SSO GINA unavailable after installer modify
QO78499	Client	Current username doesn't show on SSO GINA unlock window
QO78499	Client	SSO GINA windows logon error with terminal services
QO78499	Client	SSO Client/Application startup
QO78499	Client	SSO Client silent install options
QO78499	Client	AuthNT (now AuthWIN) attribute 'auto' doesn't work with NearestDomainController attribute
QO71773	Client	Threading issue with integrated Siteminder code
QO71773	Client	Citrix server Client log file settings
QO71773	Client	Inappropriate termination of shared memory library
QO71773	Client	Client not setting auth method in cookie correctly
QO71773	Client	Possible crash when CFileDialog times out
QO71773	Client	Client crash with UserLogoff command
QO71773	Client	Client crashing constantly: tcl library updated
QO71773	Client	Error in WaitText function
QO70074	Client	Denial of login if GinaPassThrough enabled
QO70074	Client	sso type extension can't handle German characters
QO70074	Client	GINA blue screen on Win XP
QO70074	Client	GINA blue screen after several workstation logoffs
QO70074	Client	CookieExp attribute not applied with ETWAC cookie
QO70074	Client	Allow multiple domains so that multiple WAC cookies are generated
QO68853	Client	Cookie contains nonHTTP compliant characters
QO68853	Client	Applist cache name mangling
QO68853	Client	Citrix + SSO GINA + Session Management enabled results in session management error

STAR or Patch/Testfix Number	Component	Description
QO68853	Client	Improved SSO Tcl support for German, French and Brazilian Portuguese input locales
QO68853	Client	Interpreter crash when getting OS version on Windows XP sp2
QO68853	Client	Exiting the Client through the system tray icon before logging in prevents the user from logging onto SSO and prevents Client restart
QO68853	Client	NT authentication error causing authentication loop
QO68853	Client	Getlogin extension doesn't parse variables correctly
QO68853	Client	MSI shortcuts not working with sso run extension
QO68853	Client	Cookie generated with GINA windows logon has incorrect username
QO78393	Server	Improved password generation algorithm for ps-pers account
QO78393	Server	Station unlock process fails to unlock workstation
QO78393	Server	PSMP OutOfMemory error when upgrading large databases
QO78393	Server	Configuration values reset upon upgrade
QO78393	Server	Dollar signs not recognized in ps-admin installed password
QO78393	Server	Upgrade on Windows 2003 sp1
QO78393	Server	Server language configuration changes
QO71780	Server	Support application scripts with 'extended' characters
QO71780	Server	Setup automatic service recovery for the Server
QO71780	Server	Etwac_Adm_GetObjectTimeDateRes fails
QO71780	Server	Ps-bgc improvements when working with large data stores
QO71780	Server	Server supported on Windows 2003 sp1
QO71780	Server	Access Control group authorization and 255 rules ACL limit problem
QO71780	Server	Some Policy Manager operations or DSA restarts cause the Server service to stop
QO71780	Server	Problem with large application scripts
QO71780	Server	Server crash when retrieving terminal object