RSA SecurID Ready Implementation Guide

Last Modified: December 6, 2007

Partner Information

Product Information	
Partner Name	OpenConnect Systems, Inc.
Web Site	www.oc.com
Product Name	WebConnect SSO
Version & Platform	7.0 for Sun Solaris 2.8+, IBM AIX 5.2+, HP-UX 11.11+, Windows 2000, Windows 2003, RedHat Linux Enterprise 3+, Linux for S/390 (Suse 390 8.0+)
Product Description	WebConnect SSO delivers secure single sign-on browser-based access to multiple mainframe applications with just one mouse click. Secure access is delivered through a single authentication process. With WebConnect SSO, user ids and passwords are stored within the glass house, thus eliminating serious security issues that result from passwords and login information being stored on the desktop. With its patented persistent, secure browser-based access only WebConnect SSO can support tens of thousands of concurrent Web-based users and at the same time provide organizations with the lowest total cost of ownership.
Product Category	Remote Access

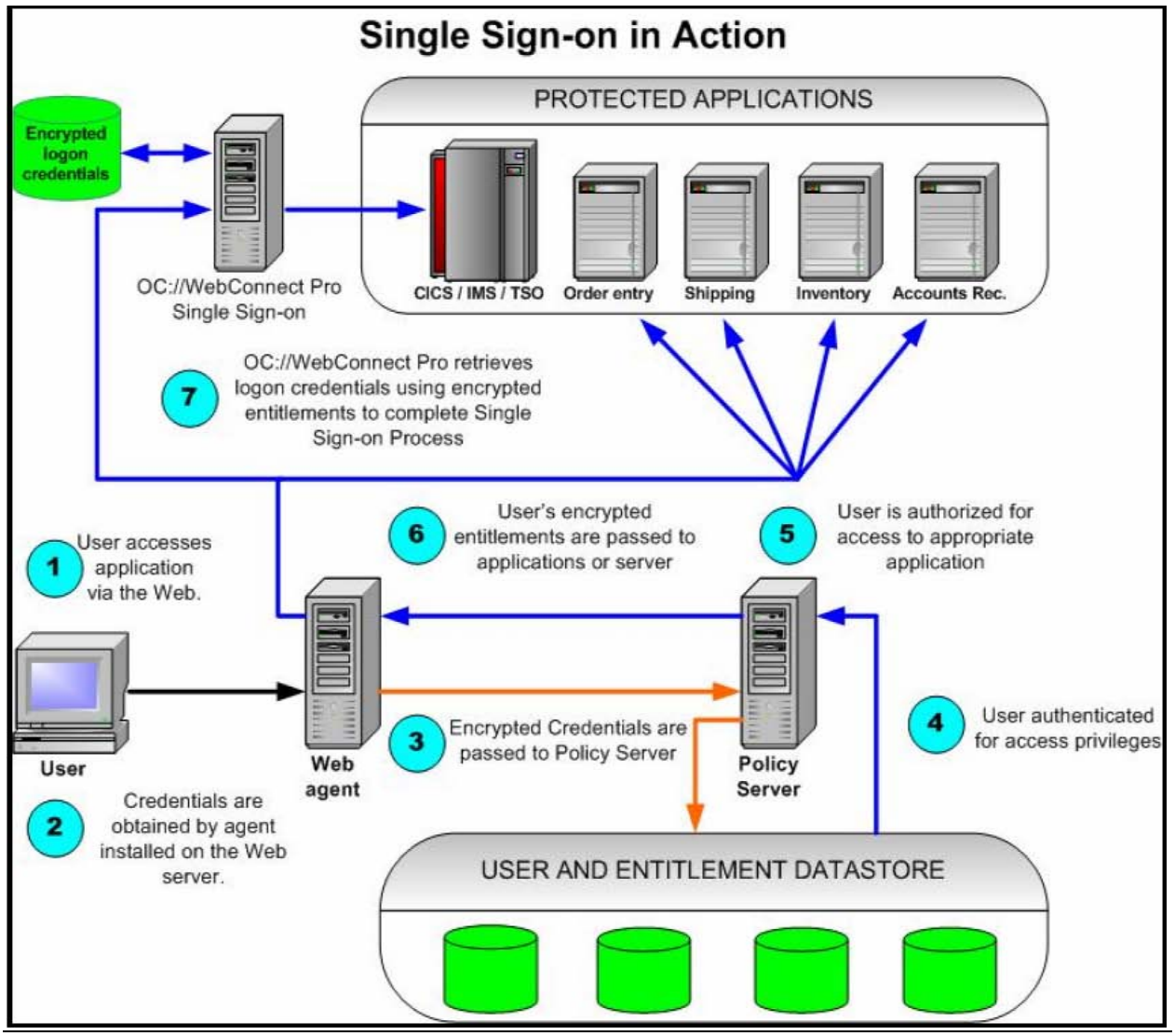
Solution Summary

WebConnect provides a secure software connectivity link that enables browser-based access to information residing on mainframe and other host computer systems. In addition to the numerous benefits provided by a secure, web-based emulation solution, WebConnect's Single Sign-On feature provides additional security by facilitating the automation of host application sign-on. Users are authenticated once by RSA Authentication Manager, and allowed access to host applications with user ids and passwords that are maintained within a secure data source. This automation eliminates security issues arising from desktop stored login information as well as monitor-attached post-it notes with logon information.

OpenConnect's WebConnect with Single Sign-on works in tandem with RSA SecurID authentication to provide secure, seamless access to legacy applications. RSA is uniquely positioned to provide the most comprehensive Trusted Identity and Access Management solution available today. Once a user has been authenticated and granted access by RSA Authentication Manager, WebConnect with Single Sign-on takes over seamlessly and securely completing the sign-on process into the host system and applications – all with one click on a web page!

Integration with RSA Authentication Manager for WebConnect is provided via an ISAPI plug-in provided with WebConnect. First, the RSA Authentication Agent for Web is installed into IIS and configured to provide authentication for IIS users. Next, the WebConnect plug-in is installed into IIS as well. To provide a general-purpose mechanism for integration into web-based security environments, the WebConnect server does not include direct integration with products such as RSA SecurID authentication. The WebConnect ISAPI plug-in obtains the authenticated user id from the web server and passes it to WebConnect. WebConnect generates an encrypted token, which is returned to the user's browser. This token is used as a bridge between web-based authentication systems and WebConnect via the ISAPI plug-in. When enabled, the WebConnect server honors only HTTP requests with the WebConnect token. This allows seamless single sign-on from initial web page to host application.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	RSA Authentication Agent for IIS Version 5.3
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	Designated Users, All Users, RSA SecurID as default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No


Single Sign-on in Action
PROTECTED APPLICATIONS
Encrypted logon credentials
OC://WebConnect Pro Single Sign-on
CICS / IMS / TSO
Order entry
Shipping
Inventory
Accounts Rec.
7
OC://WebConnect Pro retrieves logon credentials using encrypted entitlements to complete Single Sign-on Process
1
User accesses application via the Web.
6
User's encrypted entitlements are passed to applications or server
5
User is authorized for access to appropriate application
User
Web agent
Policy Server
3
Encrypted Credentials are passed to Policy Server
4
User authenticated for access privileges
2
Credentials are obtained by agent installed on the Web server.
USER AND ENTITLEMENT DATASTORE

Product Requirements

Partner Product Requirements: WebConnect SSO	
Memory	64MB of RAM is recommended for all platforms to run 1000 concurrent users, each with one session. On average, add 40MB for every additional 1000 unencrypted concurrent sessions.
HD space	300 MB
Operating System	
Platform	**Required Patches**
AIX	5.2 +
HP-UX	11.11+
SOLARIS	2.8+
LINUX	RedHat Enterprise 3.0+
Windows 2000	Service Pack 2 or higher
Windows 2003	Service Pack 2 or higher
Linux S390	SuSE Linux 390 8.0+
Additional Software Requirements	
Application	**Additional Patches**
MS Internet Explorer	Version 5.5+ w/ JVM Build 3802 or greater or Sun JRE as shown below
Netscape	Navigator version 7.0+ w/JRE 1.5x
Sun	JRE 1.5.x (Java Runtime Environment) required for Swing and .NET client types
	JRE 1.4.x (Java Runtime Environment) supported only with the Classic client type.
Safari	Version 1.2+ w/ JDK 1.4.2

Agent Host Configuration

No special configuration of Authentication Manager is required for integration with WebConnect. Only the configuration normally required to integrate IIS with RSA SecurID is necessary.

To facilitate communication between the WebConnect and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the RSA Authentication Agent for IIS within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the RSA Authentication Agent for IIS as NetOS. This setting is used by the RSA Authentication Manager to determine how communication with the RSA Authentication Agent for IIS will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	Subject to standard handling of the RSA Web Agent
Node Secret	Subject to standard handling of the RSA Web Agent
sdstatus.12	Subject to standard handling of the RSA Web Agent
sdopts.rec	Subject to standard handling of the RSA Web Agent

Note that WebConnect SSO uses the standard RSA Authentication Agent for IIS and all RSA SecurID files are handled as stated in the RSA documentation.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

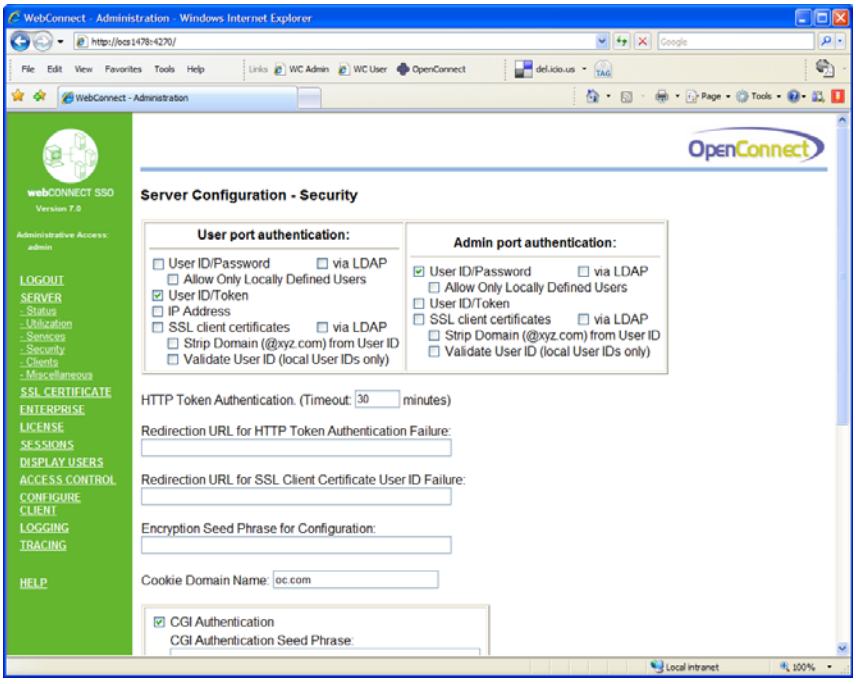
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration

To integrate WebConnect with RSA SecurID, it is necessary to use the WebConnect Token Authentication feature to bridge the authenticated userid from IIS to WebConnect. Configuration of WebConnect Token Authentication is described in Appendix G of the WebConnect *Configuration and Administration Guide*. To summarize, the steps are:

1. Install WebConnect IIS plug-in
2. Create HTML page(s) to start WebConnect host sessions via the plug-in
3. Configure WebConnect user port to use User ID/Token Authentication



Once WebConnect token authentication is enabled, only users with the tokens provided via the WebConnect plug-in will be allowed to access the WebConnect server. Access to the HTML page to generate the WebConnect token and start the session is protected via the RSA Authentication Agent for Web on the IIS machine, providing the seamless transition from RSA SecurID authentication to WebConnect.

Certification Checklist For RSA Authentication Manager

Date Tested: December 6, 2007

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2000 SP4
RSA Authentication Agent	5.3.3	Windows 2003 SP2
WebConnect SSO	7.0	Solaris 2.10

Mandatory Functionality				
RSA Native Protocol			**RADIUS Protocol**	
New PIN Mode				
Force Authentication After New PIN	✓		Force Authentication After New PIN	N/A
System Generated PIN	✓		System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓		User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓		User Defined (5-7 Numeric)	N/A
User Selectable	✓		User Selectable	N/A
Deny 4 and 8 Digit PIN	✓		Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓		Deny Alphanumeric PIN	N/A
Passcode				
16 Digit Passcode	✓		16 Digit Passcode	N/A
4 Digit Password	✓		4 Digit Password	N/A
Next Tokencode Mode				
Next Tokencode Mode	✓		Next Tokencode Mode	N/A
Load Balancing / Reliability Testing				
Failover (3-10 Replicas)	✓		Failover	N/A
Name Locking Enabled	✓		Name Locking Enabled	
No RSA Authentication Manager	✓		No RSA Authentication Manager	N/A

Additional Functionality				
RSA Software Token Automation				
System Generated PIN	N/A		System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A		User Defined (8 Digit Numeric)	N/A
User Selectable	N/A		User Selectable	N/A
Next Tokencode Mode	N/A		Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation				
System Generated PIN	N/A		System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A		User Defined (8 Digit Numeric)	N/A
User Selectable	N/A		User Selectable	N/A
Next Tokencode Mode	N/A		Next Tokencode Mode	N/A
Credential Functionality				
Determine Cached Credential State	N/A		Determine Cached Credential State	
Set Credential	N/A		Set Credential	
Retrieve Credential	N/A		Retrieve Credential	

SWA / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Note: Authentication feature set relies on standard RSA Authentication Agent for IIS. Testing performed was used to validate that the UserID credential was properly extended from the RSA SecurID Authentication for IIS into the WebConnect SSO server