

OC://WebConnect

OC://WebConnect Single Sign-On

a Whitepaper prepared by

OpenConnect Systems, Inc.

January 29, 2003

Table of Contents

Introduction 3

Single Sign-On Architecture 4

Single Sign-On Process 7

What's New? 8

Technical Specifications 9

Summary 10

Contact Information 11

Introduction

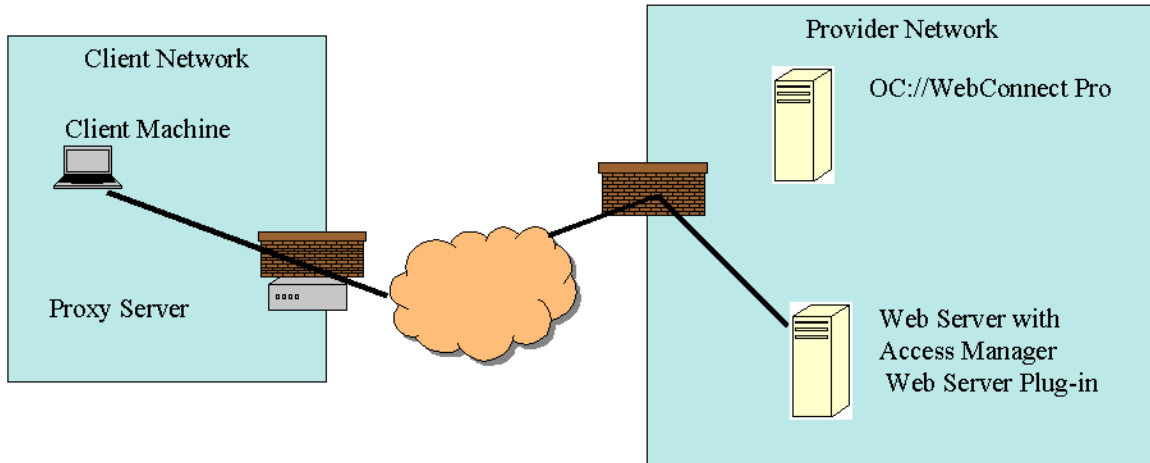
OC://WebConnect is client-server based software that provides browser based emulations to 3270, 5250 and VT data streams. In 1996, OpenConnect created the Web-to-Host market by introducing it's premier connectivity software, **OC://WebConnect**, to provide a secure software connectivity link that enables browser-based access to information residing on mainframe and other host computer systems.

OpenConnect's Web-to-Host technology is covered by U.S. Patent No. 5,754,830, which enables an SNA-style persistent connection to host applications over the Internet. This allows traditional information sources over corporate intranets to be shared with business-to-business extranets created from Internet technology. Mainframe and other client server host applications can be easily enabled for Web-to-Host access, without changing a single line of source code. Once enabled, the user can access commercial information through a Web Browser.

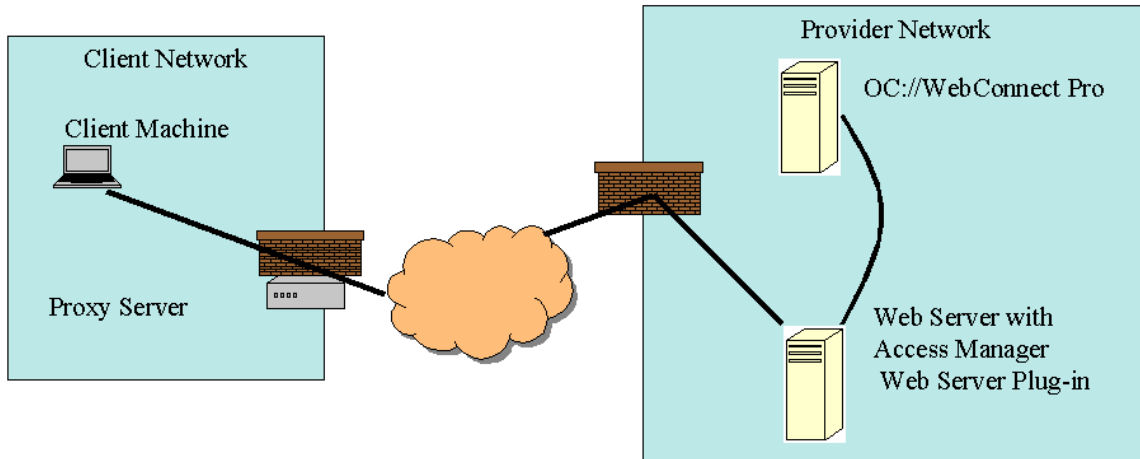
OC://WebConnect's newest feature, **Single Sign-On** facilitates the automation of host application sign-on, by allowing users to login once to the **OC://WebConnect** server or 3rd party web server, then access their host applications with a single mouse-click. The host user ids and passwords are stored on the **OC://WebConnect** server, eliminating security issues arising from desktop stored login information. See OpenConnect's Whitepaper "*OC://WebConnect 6.2*" for a full discussion of our award-winning software.

Single Sign-On Architecture

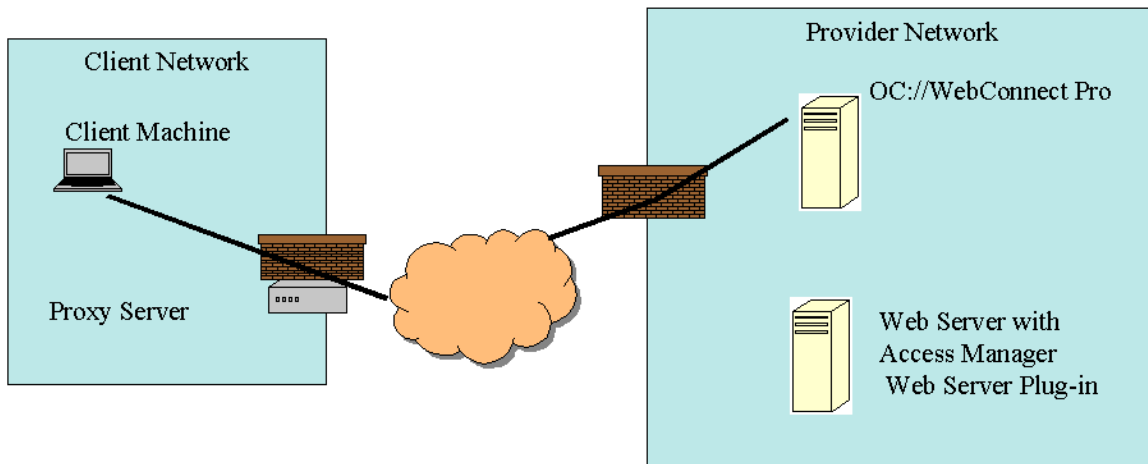
OC://WebConnect's Single Sign-On feature is designed to work with any 3rd-party policy manager and web server.



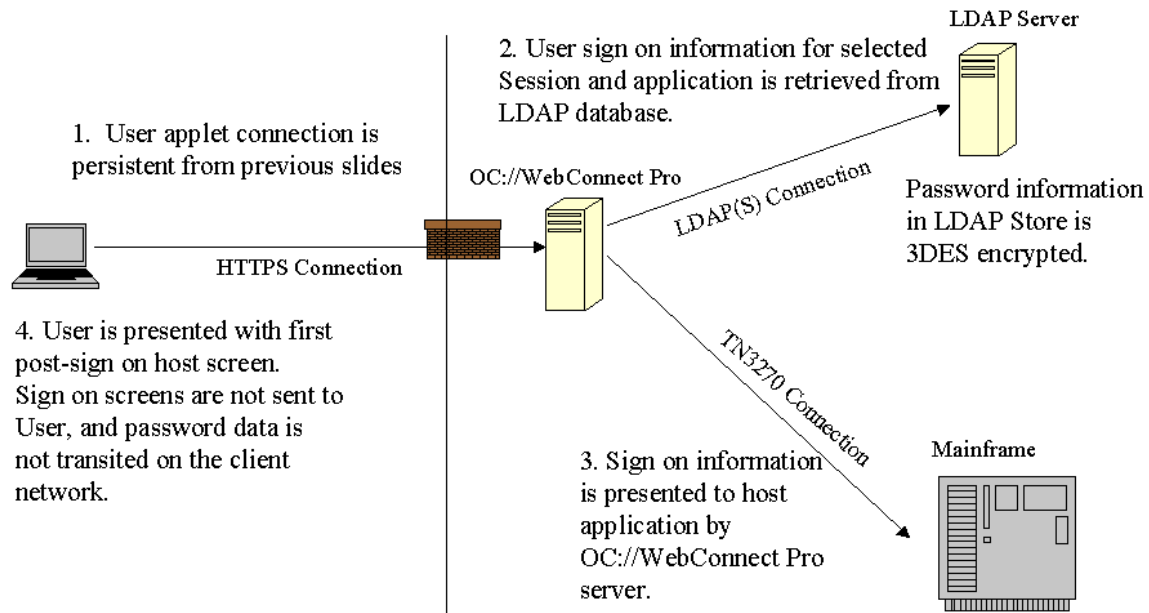
- First, the user accesses your company's web-site either through the Internet, intranet or extranet.
- The user then clicks on a link on your company's web-site that will launch an emulation session.
- Clicking on the emulation link invokes a Policy Manager to challenge the user for authentication.
- If authenticated, the Policy Manager then authorizes the user access to the emulation session.



- A CGI program bundled with **OC://WebConnect** and installed on the 3rd-party Web Server is then launched which connects to the **OC://WebConnect** server and builds the applet page for the session specified. The CGI program passes the user credentials that will be used to “look up” the host user id and password on the **OC://WebConnect** server.
- A time limited session token is generated by the **OC://WebConnect** server and returned with the page to the client.
- The Java applet is downloaded to the user’s browser if it is not already cached on the Client Machine.



- The applet initializes on the Client Machine and makes a persistent connection to the **OC://WebConnect** server. The session token is validated and the session is started to the host.



- Once a host session has been started and a persistent connection established, the **Single Sign-On** process defined for that session is invoked.
- Based on the user's authentication credentials, the host sign-on information is retrieved from an LDAP database, or **OC://WebConnect's** secure files. Password information is always stored in a 3DES encryption.
- The session's **Single Sign-On** process then navigates through the host sign-on screens, presenting the appropriate user information and static information to each screen.
- Once the **Single Sign-On** process is complete, the user is presented with the first post sign-on host screen.

Single Sign-On Process

Enabling the **Single Sign-On** process for a host session is a three step process:

1. Create a **Single-Sign-on** Definition (container for **Single-Sign-on** information)
2. Record **Single-Sign-on** Sequences (navigate through logon process - success and failure)
3. Annotate Sequences (define user variables, messages, branching, etc.)

For every Sequence in the **Single Sign-On** definition, determine:

- How Sequence is triggered
- What to do when Sequence is complete

For every Host screen in each Sequence:

- Define what to display to user
- Define user variables (user id, password, CICS region, etc.)
 - The **OC://WebConnect** Administrator can populate user variable database -or-
 - User variables can be captured when the user types them in the first time (or changes it due to expiration.)
- Define which host screen should follow the current screen
- Define Identifiers so host screens can be recognized

What's New?

OC://WebConnect 6.2, OpenConnect's latest version of its award-winning software offers a long list of new features, including:

Single Sign-On Enhancements

- The **Single Sign-On** process can optionally automatically generate random passwords to be used when a host password expires. This feature addresses two security issues:
- Mainframe Security Managers do not have to change their current procedures, passwords can still expire at a determined interval
- End users are freed from knowing or remembering passwords – suppliers and partners can now be allowed secure access to host systems without assigning original passwords and transmitting those passwords across the Internet, intranet or extranet.

Technical Specifications

OC://WebConnect Server

- Operating System
 - AIX 4.1.4+
 - HP-UX 10.10+
 - SOLARIS 2.5+
 - LINUX (RedHat 6.2)
 - Windows NT 4.0 w/minimum of SP/6 (for Y2K)
 - WINDOWS 2000
 - AS400 - OS400 V4R1
- 135 MB hard disk
- Memory Utilization
 - Minimum 64 MB of RAM available for platforms to run 1000 concurrent users, each with one host session.
 - Add 36 MB RAM for every additional 1000 concurrent host sessions.
- Session Limitations
 - UNIX - Maximum 5000 host sessions
 - WinNT and WINDOWS 2000 - Maximum 3000 host sessions
 - Minimum 400 MHz processor for 3000 host sessions
 - Microsoft recommends 128-MB memory, 256 MB for WINDOWS 2000

Client Platform requirements

- CPU – Minimum 200 MHz, 300+ recommended
- RAM – 32 MB for WIN, 64 MB for NT, 128 MB for WINDOWS 2000
- OS – Y2K compliant Intel

Browser Requirements

- Netscape Navigator v 4.08+
- Microsoft Internet Explorer 4.0 w/JVM Build 2436 or
- Microsoft Internet Explorer 5.0 w/JVM Build 3167

Summary

OC://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, **OC://WebConnect**'s feature, **Single Sign-On**, provides additional security by facilitating the automation of host application sign-on. Users are authenticated once by a 3rd-party Policy Manager, and allowed access to host applications with user ids and passwords that are stored on the **OC://WebConnect** server. This automation eliminates security issues arising from desktop stored login information as well as monitor-attached post-it notes with logon information.



Contact Information

For more information about **OC://WebConnect**, **Single Sign-On**, or any of OpenConnect Systems' award-winning software, please contact:

Corporate Sales – U.S.: 972-888-0470
Corporate Sales – U.K.: +44 0870 420 2765

Corporate Fax: 972-484-6100

Email: sales@oc.com

OpenConnect Systems, Inc.

2711 LBJ Freeway, Suite 700
Dallas, TX 75234