IBM

WebSphere® software

IBM WebSphere Everyplace Connection Manager, Version 4.2

Highlights

■ *Delivers e-business applications to mobile users over wireless and wired networks*

■ *Ensures end-to-end network security by using strong authentication and data encryption*

■ *Drives productivity by allowing users to seamlessly roam across networks without breaking the application's end-to-end TCP/IP session*

■ *Integrates diverse wireless networks using a single industry standard interface*

■ *Includes a Java™ technology user interface to setup and configure easily across multiple platforms*

Delivering e-business on demand

In today's mobile business world, flexibility is key. Enterprises are looking for solutions that can extend their e-business to dispersed international work forces when and where they need to – over any network to any device. Simultaneously, Service Providers are looking for ways to provide these solutions with the scalability to handle larger numbers of subscribers, while they create new revenue generating services and expand their customer base.

IBM Pervasive Computing

IBM pervasive computing software empowers both enterprises and Service Providers to create and deploy applications for this new generation of mobile computing. With WebSphere® Everyplace Connection Manager, we have created a complete platform to enable you to easily extend e-business to mobile users over wired and wireless networks, now.

WebSphere Everyplace Connection Manager

IBM WebSphere Everyplace Connection Manager, Version 4.2 is a distributed, highly scalable, multi-purpose UNIX® communications platform. It supports optimized, security-rich data access by both Wireless Application Protocol (WAP) and non-WAP clients over a wide range of international wireless network technologies, local area networks (LANs) and wide area networks (WANs).

WebSphere Everyplace Connection Manager integrates data access from wireless and wired networks so that applications and data can be made available to a mobile workforce. With a Transmission Control Protocol/Internet Protocol (TCP/IP) interface, existing applications may use either wireless or wired networks to integrate communications. The interface shields network-specific details from the user application and provides network-specific authentication and data enhancements — such as compression, encryption and optimization.

Seamless cross-network roaming

WebSphere Everyplace Connection Manager allows mobile users to seamlessly roam from inside the intranet to the Internet or any public network and back. This dynamic roaming feature enables access across physical networks without breaking the application's end-to-end TCP sessions and provides mobile users with uninterrupted connectivity to critical applications.

WebSphere Everyplace Connection Manager components include:

- *Gatekeeper*
- *Mobility Client*
- *WAP proxy*
- *Messaging services*

Gatekeeper

IBM WebSphere Everyplace Connection Manager Gatekeeper provides a Java technology-based administrator console to the WebSphere Everyplace Connection Manager and to wireless resources. With the easy-to-use administrative interface in the Gatekeeper, you can remotely define and configure wireless gateways, register users and mobile devices, specify logging and tracing controls and perform routine administrative tasks. The administration and configuration data is stored conveniently in a Lightweight Directory Access Protocol (LDAP) directory.

Mobility Client

The Mobility Client software runs locally on mobile devices and provides a full-function interface to communicate with WebSphere Everyplace Connection Manager. With an authenticated network connection, you can assign a client Intranet or Internet IP address. IP applications can run on a wireless network using the standard TCP/IP provided by the operating system on the mobile device. The WebSphere Everyplace Connection Manager supports standard IP routing — even over non-IP wireless bearer networks — to help ensure unbroken, end-to-end TCP sessions between mobile devices and application servers.

WAP proxy

When you configure WebSphere Everyplace Connection Manager as a WAP gateway, you can provide connectivity for multi-vendor WAP 1.1 and WAP 1.2 client devices. WebSphere Everyplace Connection Manager fully supports the WAP Wireless Session Protocol (WSP) to link the microbrowser with cellular phones and Personal Digital Assistants (PDAs). When configured as a WAP gateway, WebSphere Everyplace Connection Manager performs a protocol conversion to provide communication with WAP clients and HyperText Transport Protocol (HTTP) Web servers.

Messaging services

You can use the Gatekeeper to configure WebSphere Everyplace Connection Manager as a messaging gateway. The messaging functions support delivery and receipt of short messages to and from client devices. When you configure the WebSphere Everyplace Connection Manager to be a messaging gateway, you allow a web application server to send messages to a client, such as a pager or a phone in a wireless network. The messaging gateway supports several types of messaging modes including Short Message Service (SMS), e-mail and Simple Network Paging Protocol (SNPP).

Supported Software Platforms

WebSphere Everyplace Connection Manager
- IBM AIX®, Version 4.3.3 or IBM AIX, Version 5.1
- SUN Solaris, Version 7 or higher

Client platforms
- Microsoft Windows XP, Windows 2000, PocketPC® 2002
- Windows ME, Windows 98
- Windows 95*, Windows NT 4.0*, WinCE 2.1* or higher
- Palm OS*, embedded RTOS*

Open database connectivity (ODBC)-compliant relational database
- IBM DB2 Universal Database, Version 7.1
- Oracle, Version 8.1.5 or Oracle, Version 8.1.6

LDAP database both server and client
- IBM SecureWay Directory Server, Version 3.2 or higher
- Netscape, Version 4.1.x

IPv4 or IPv6 networks and clients
- LAN & WAN, 802.11, Ethernet, 3G CDMA, 2.5G, CDPD, PDC-P, iDEN
- Support of several non-IP wireless WANs

* Not all EWG OS platforms include roaming support today

Mobile Access Services

An encrypted tunnel secures wireless connections between the WebSphere Everyplace Connection Manager and the Everyplace Wireless Client. Everyplace Wireless Client, in conjunction with WebSphere Everyplace Connection Manager, offers enhanced functionality, improved performance and security-rich operations. WebSphere Everyplace Connection Manager supports applications using industry-standard sockets programming interfaces, so developers don't need to learn special programming interfaces or proprietary tools and protocols. TCP/IP applications can run unchanged with a wireless network.

Security

WebSphere Everyplace Connection Manager provides strong authentication and supports the RSA Secure ID authentication solution. Customers can choose from an extensive cryptographic library, which includes DES, Triple DES, RC5[1] and AES[2], to provide end-to-end encryption of all data between the mobile device and the intranet network.

Data optimization

WebSphere Everyplace Connection Manager reduces data transmission costs over wireless networks since it provides very efficient data compression and optimizes session transport for IP-based wireless networks, including 2.5G and 3G networks. WebSphere Everyplace Connection Manager enables optimized IP transport over non-IP wireless packet networks, thereby improving data throughput, enhancing reliability of wireless communication and improving the end user experience.

Reliability of WebSphere Everyplace Connection Manager is further improved by gateway clustering and distribution of the load across multiple sites, in peak times. WebSphere Everyplace Connection Manager supports High Availability Cluster Multiprocessing (HACMP) to provide 24x7 availability and reliability.

IBM stands ready to help

At IBM, we understand your business and can provide custom pervasive computing solutions to expand your portfolio of services and speed your time to ROI. With worldwide resources and an extensive Business Partner network, IBM stands ready to help.

For more information

To learn more about IBM pervasive computing software solutions visit ibm.com/pvc or call your local IBM representative.

Wireless LAN components and security solutions
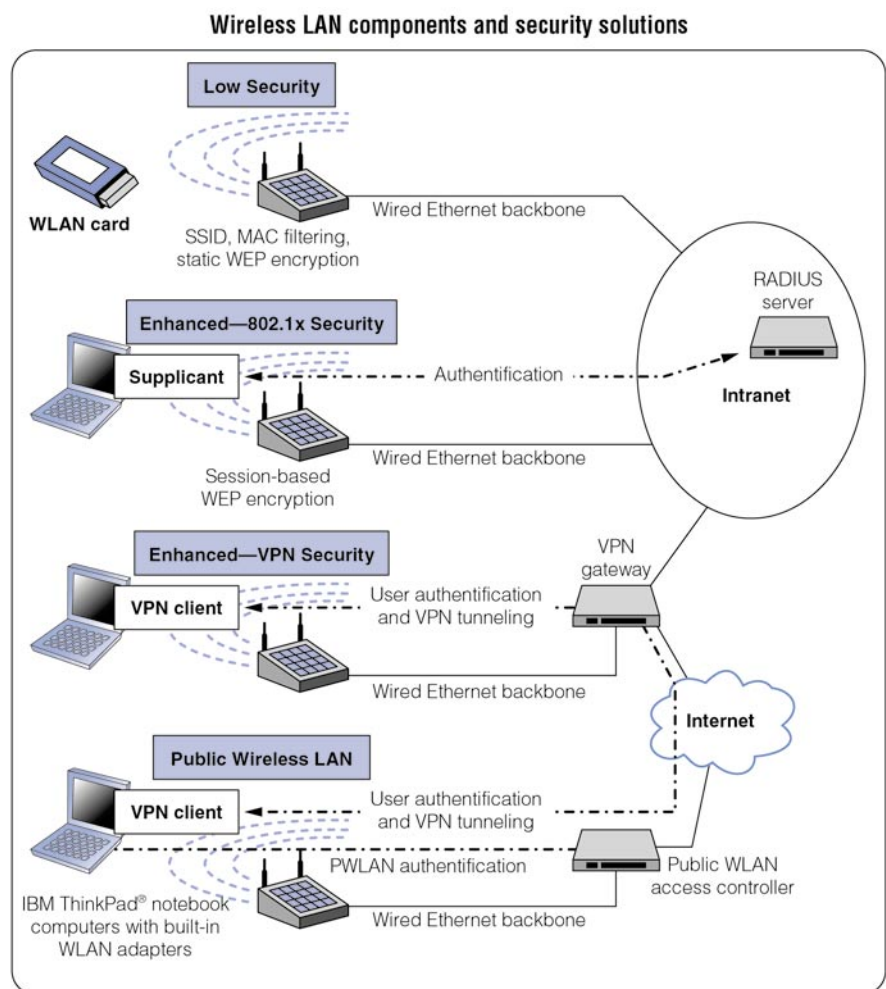
WECM hardware requirements

IBM AIX operating environment
- IBM RS/6000® 7043-150 tower
- 250MHz 32-bit 604e processor
- 128MB memory
- 9.1GB internal disk storage

Sun Solaris operating environment
- Ultra 10
- 1GB RAM
- CD-ROM
- Minimum 9GB hard disk drive

WECM software requirements

IBM AIX and Sun Solaris operating environments
- IBM AIX, Version 4.3.3 or IBM AIX, Version 5.1 plus AIXLink 1.1.3.0 or higher to use an X.25 adapter
- Sun Solaris operating environment, Version 7 or higher
- Open database connectivity (ODBC)-compliant relational database
- IBM DB2 Universal Database™, Version 7.1 or Oracle, Version 8.1.5 or Oracle, Version 8.1.6
- Merant DataDirect Connect ODBC, Version 3.6.0
- Oracle, Version 8.1.7
- Merant DataDirect Connect ODBC, Version 3.7.0
- LDAP database, both server and client (IBM SecureWay® Directory Server, Version 3.2 or higher), Netscape, Version 4.1.X
- HTTP Proxy Server (if using WAP function)

Gatekeeper at a glance

Gatekeeper hardware requirements

- On Intel® platforms, 400MHz or greater Pentium® processor
- On RS/6000 platforms, 250MHz or greater processor
- Minimum of 128MB RAM
- Minimum of 30MB disk space

Gatekeeper software requirements

- TCP/IP protocol installed
- IBM AIX, Version 4.3.3; IBM AIX, Version 5.1
- Microsoft® Windows® 95, Windows 98, Windows NT®, Windows 2000, Windows Me
- Sun Solaris operating environment
- Linux, Version 6.0 or later (with glibc2.1 or later)[1]

Mobility Client at a glance

Minimum disk space requirements

- TCP/IP protocol installed

- 1 to 3MB available disk space on Windows 95, Windows 98, Windows NT, Windows Me or Windows 2000 platforms

- 1.5MB available disk space on Windows CE

[1] Requires Java Runtime Environment (JRE), Version 1.2.2_006 (or later 1.2) but not Version 1.3 or later

1 RC5 is a fast block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security) in 1994. It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds.

2 Advanced Encryption Standard (AES) - is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

business software