Lotus® Expeditor Server

IBM

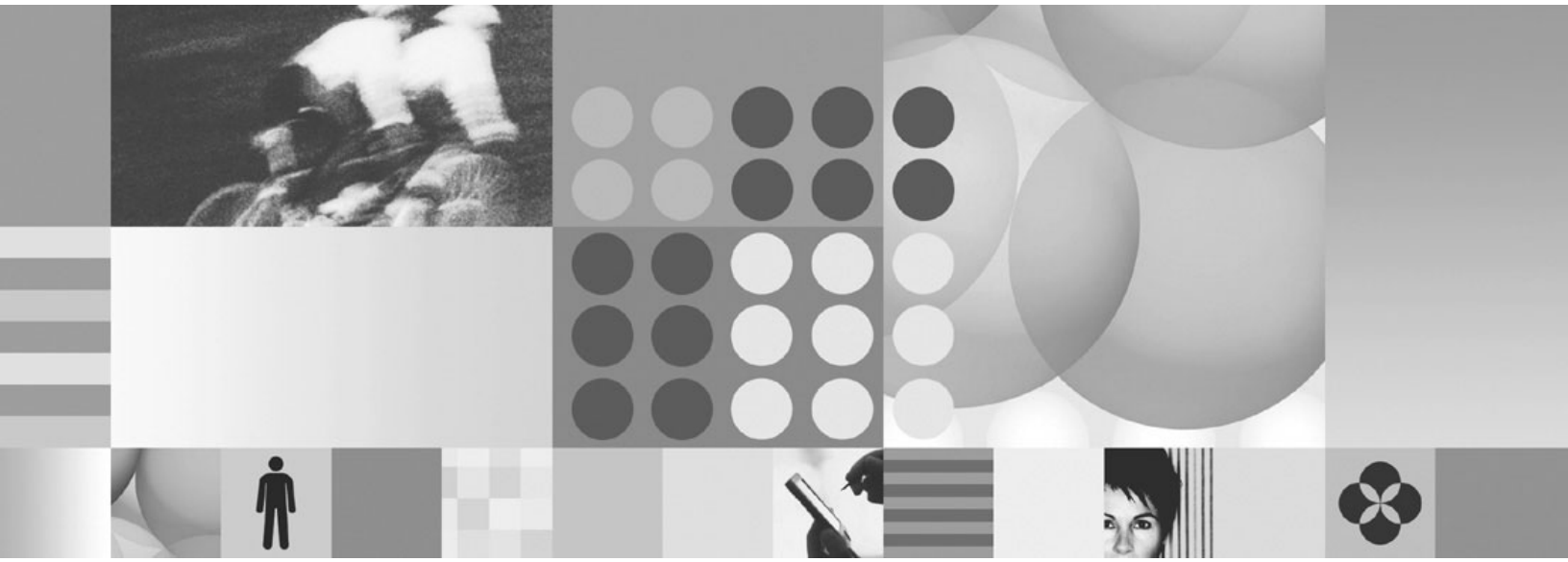
Version 6 Release 1

Using Lotus Expeditor Server

Lotus® Expeditor Server

IBM

Version 6 Release 1



Using Lotus Expeditor Server

Note
Before using this information and the product it supports, read the information in "Notices," on page 115.

Second Edition (November 2006)

This edition applies to Version 6, Release 1 of IBM Lotus Expeditor and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Introducing Lotus Expeditor Server

This topic introduces Lotus Expeditor Server, the corresponding Lotus Expeditor Client, and the end-to-end access services provided by these products.

Review these topics to better understand Lotus Expeditor Server and its associated components. Keep in mind that additional educational resources, such as product tutorials, demos, and technical overviews are available on the IBM® Education Assistant Web site.

Product overview

IBM Lotus Expeditor Server provides application management services and application connectors for the Lotus® Expeditor client. System Administrators can use the server application management services to deploy, configure and maintain applications running on the Lotus Expeditor client. Server application connectors are provided to enable client applications to securely perform assured transactions and database synchronization with Enterprise applications and data. An integrated installation and configuration program is provided to deliver these services.

Lotus Expeditor Client is a client middleware framework and tooling platform that enables connection, independent delivery, and management of applications and services. Because Lotus Expeditor Client extends the WebSphere® programming model by providing Java™ 2 Platform, Micro Edition (J2ME) services and Web Services to clients, you can move key components of your applications to the client. The client accesses enterprise data maintained on the server by using standard Application Programming Interfaces (APIs) and services. End users benefit from improved application response time because applications perform business operations locally on the client. As a result, network traffic might be reduced between clients and servers. Mobile end users can continue to productively use their applications even when they are at a location that does not have network connectivity, such as a customer site.

When you use the Lotus Expeditor Client client middleware framework in conjunction with Lotus Expeditor Server you can:

- Extend existing applications to new users, customers, and partners while utilizing current programming skills.
- Dynamically deploy, update, and maintain software on devices over a wireless connection.
- Access applications whether the device is connected, disconnected, or occasionally connected.
- Leverage standards-based middleware to connect applications to enterprise e-business applications.

Lotus Expeditor Server and supported clients provide a development environment for Independent Software Vendors (ISVs) and enterprise application developers to develop workforce mobile applications. The Lotus Expeditor Client solution enables you to start small and simple with the ability to deploy a robust set of mobile applications over time. Advanced features enable you to upgrade to a pilot or production environment that supports a larger number of client users.

What's new in this release

This topic describes new features and functionality included in this release.

New and changed features of Lotus Expeditor Server 6.1 include the following:

- Installation and configuration support of Lotus Expeditor Server on Red Hat Enterprise Linux®
- Ability to scale the Lotus Expeditor Server services across multiple servers using WebSphere Application Server clustering
- Support for additional LDAP servers

- Support for WebSphere Application Server configuration profiles

Device Manager 2.1 updates

This topic describes the latest updates to Device Manager Server.

New and changed features include the following:

- Direct management of Eclipse features and plug-ins

  A single feature or an entire update site can be registered for distribution.
- Retrieval and editing of Eclipse preferences and configuration properties
- New Eclipse device class for pure Eclipse device support (for example, Windows® Mobile)
- Package security, including verification of software packages to ensure that the packages were not altered after being registered
- Additional OSGi R4 support

Note: Eclipse is an award-winning, open source platform for the construction of powerful software development tools and rich desktop applications. Leveraging the Eclipse plug-in framework to integrate technology on the desktop saves technology providers time and money by enabling them to focus their efforts on delivering differentiation and value for their offerings. Full details on Eclipse are available at http://www.eclipse.org.

DB2 Everyplace 9.1 updates

This topic describes the latest updates in the DB2® Everyplace® 9.1 enterprise and database editions.

DB2 Everyplace Synchronization Server

Provides support for the following:

- Automatic replication statistics collection

  The DB2 Everyplace Sync Server automatically collects replication statistics to provide additional information to manage the replication performance and frequencies.
- Source schema consistency checking command

  Use the **dsycheck** command to check DB2 Everyplace Sync Server for inconsistencies between source databases and mirror databases. For more information, see command line scripts for DB2e Sync Server at: http://publib.boulder.ibm.com/infocenter/db2e/v9r1/index.jsp?topic=/com.ibm.db2e.doc/dbessr1301.html.
- Data filtering to reduce the amount of data transferred between the server and the client

For more information about DB2 Everyplace 9.1 features and updates, see the DB2 Everyplace 9.1 Enterprise Edition Release Notes.

DB2 Everyplace embedded database (ships with the Lotus Expeditor Client)

Provides support for the following:

- JDBC 3.0 Savepoint

  An application can set, release, or roll back a transaction to designated savepoints.
- 128-byte identifiers

  The maximum length of table names, column names and index names has been extended from 18 bytes to 128 bytes.
- Unique indexes
- New data types:
  - CHAR FOR BIT DATA—Allows you to store fixed-length byte strings.

– VARCHAR FOR BIT DATA—Allows you to store variable-length binary strings.

WebSphere MQ Everyplace 2.0.2 updates

This topic describes the latest updates to MQ Everyplace.

New and changed features include the following:

- Support for UTF-16 with surrogate characters has been added to the C Native code base
- Support for the native code base on Windows Mobile 5

Key features

This topic describes key features that expand the range, power, and usability of the entire solution.

Security

This topic provides details on enhanced security features for the Lotus Expeditor Server.

Lotus Expeditor Server security can be broken down into the following topics:

- "Transport layer security"
- "Authentication"
- "Enabling secure sockets layer (SSL)"

Transport layer security

Transport layer security ensures the privacy of data as it is transferred over public networks. Data encryption techniques prevent outsiders from eavesdropping sensitive data. Data encryption occurs between the client and server. You can use Secure Sockets Layer (SSL) as transport layer security for DB2 Everyplace and Device Manager. WebSphere MQ Everyplace has its own encryption capabilities to ensure message security; however, you must configure WebSphere MQ Everyplace to use encryption.

Authentication

The basis of all access control is to verify that you can identify the person or program requesting access. Lotus Expeditor Server exploits the security infrastructure provided by WebSphere Application Server. DB2 Everyplace and Device Manager rely upon WebSphere Application Server to provide a HTTP (401) basic authentication challenge to any request for a secure resource or to validate a supplied LTPA token. Lotus Expeditor services do not perform any additional user authentication, trusting the WebSphere Application Server authentication process. WebSphere Application Server data source service and DB2 Everyplace Synchronization Server subscription definitions provide authentication to back-end databases.

Enabling secure sockets layer (SSL)

To protect data transferred between the Expeditor Server and clients, the HTTP server, the application server, and the Expeditor Server client must be secure. Security is not enabled on your servers by default. You must SSL security on IBM HTTP Server and WebSphere Application Server. For complete details on enabling secure SSL, see "Securing Lotus Expeditor Server" on page 105.

Integrated installation and configuration

IBM Lotus Expeditor Server provides integrated installation and configuration of the server middleware components that provide access services for Lotus Expeditor clients.

These middleware components are DB2 Everyplace, Device Manager, and WebSphere MQ Everyplace. The installation and configuration programs are driven from a graphical user interface (GUI). The configuration program provides a recovery feature that enables you to resolve configuration problems

without uninstalling and reinstalling the server. If you encounter an error during the configuration phase you can pause, resolve the error condition, and resume the configuration from the point at which it was stopped.

WebSphere Application Server, the IBM HTTP Server, the IBM WebSphere Application Server HTTP plug-in, and DB2 are prerequisite software components. Lotus Expeditor Server media does not contain the prerequisite software. The Lotus Expeditor Server installation program performs prerequisite validation checking and do not proceed if the correct levels of the prerequisites are not installed.

Note: See the IBM Education Assistant Web site at http://www-306.ibm.com/software/info/education/assistant/ for information on how to obtain and install Lotus Expeditor Server prerequisite software.

Configuration Wizard

IBM Lotus Expeditor Server provides a Configuration Wizard that enables you to update the server configuration after the initial installation and configuration.

You can use the Configuration Wizard to complete the following tasks:

- Change the database administrator's password in the server configuration.
- Change the IBM Lotus Expeditor Server administrator's password in the server configuration.
- Change the server configuration to use Active Directory 2003 as the user registry.
- Change the server configuration to enable clustering of the services.

In addition, command line configuration update tools are provided to update the server configurations as follows:

- Change the server configuration to use an LDAP directory other than Active Directory 2003.
- Change the server configuration to reflect that a Web server has been moved or that a load-balancing proxy server added to the network configuration.

Scaling IBM Lotus Expeditor Server services

IBM Lotus Expeditor Server supports extending services across multiple physical systems and horizontal clustering of WebSphere applications.

Extend services across multiple physical systems

This task is accomplished by supporting WebSphere Application Server workload management. The application servers are defined in a horizontal cluster to provide workload distribution. Workload can be spread over the application server instances to provide more capacity. The installation program provides a method to quickly install and configure additional systems with minimal user input and manual intervention.

In a clustered environment, you must place the OSGi software bundles that are created to deliver software to the client on the Web server used to access Lotus Expeditor Server. This way, they are accessible from the clients.

Note: URLs for these software jobs reference the Web server host name and not the Lotus Expeditor Server host name.

MQ Everyplace is not a WebSphere Application Server application and, therefore, is not clustered. However, instances of WebSphere MQ Everyplace are installed on each server. Messaging can be administratively load balanced by configuring the clients to connect to a particular Lotus Expeditor Server.

High availability support

WebSphere Application Server clustering also provides high availability for application servers. Multiple instances of an application server (members) are available in a cluster. When one member

fails, WebSphere workload management stops sending requests to the failed member and routes them to the remaining active members. Since the three Lotus Expeditor application servers (Lotus Expeditor Core Services, DB2 Everyplace Synchronization Server, and Device Manager Server) can be clustered, WebSphere workload management provides failover support. This enables a high availability environment. Lotus Expeditor Server relies upon several services, each of which can become a single point of failure.

You should enable each of these services for high availability:

- LDAP server used to store Lotus Expeditor Client users and groups
- Database server where the Lotus Expeditor databases are stored
- Load balancer product to distribute workload across Web servers
- File system: Use of a shared, highly available disk storage system, such as RAID (Redundant Array of Independent Disks).
- Load balancers (optional) used to distribute workload across Lotus Expeditor Client Web servers

Note: For more information about high availability options, consult the product documentation shipped with your LDAP server, database server, Web server, disk storage system, or load balancing product.

Common user registry

IBM Lotus Expeditor Server reduces the overhead of creating and managing user IDs by providing a common user registry interface shared by Device Manager and DB2 Everyplace.

Each Lotus Expeditor Client must have a unique user ID and password to log in to Device Manager and DB2 Everyplace. WebSphere Application Server is configured to use this common user registry for all WebSphere applications installed on the local system. Because there is a common user registry, client users need only a single user ID to access both DB2 Everyplace and Device Manager.

IBM Lotus Expeditor Server creates a local database for the common user registry during installation that is intended for use in a development environment. When you are ready to upgrade to a pilot or production environment, you can change the server configuration to use an LDAP directory as the common user registry. A configuration wizard is provided to assist with configuring with Active Directory 2003. Other LDAP directories supported by WebSphere Application Server can be configured using a command line procedure.

Components overview

This topic describes each of the products and components that are shipped with Lotus Expeditor Server and explains the role each component plays in the overall solution.

Note: Consult the product license for specific terms of entitlement for the software products and components that are shipped with your edition of Lotus Expeditor Server. Usage restrictions apply for some software.

Prerequisite components

The following components are prerequisites to Lotus Expeditor Server:

- DB2

  Database server where Lotus Expeditor Client databases are created. This component is required.
- WebSphere Application Server (includes IBM HTTP Server)

  Provides the J2EE environment on which the Lotus Expeditor Server middleware is built. Runs the DB2 Everyplace and Device Manager application servers and provides Web servers used to access the Expeditor Servers. This component is required.

Note: WebSphere Application Server WebSphere Application Server Network Deployment provides the systems management and workload balancing support required to scale the Lotus Expeditor services.

- User Registry (LDAP)

  The LDAP server is used to provide user authentication and group membership information for the services of Lotus Expeditor Server. This component is optional.
- MQ Server, as needed. This component is optional.

Included components

The following components are included with Lotus Expeditor Server:

- Device Manager Server

  Provides software distribution and management for the supported Lotus Expeditor clients.
- DB2 Everyplace

  Provides database synchronization between application data stored on the Lotus Expeditor client and enterprise data stored on database servers.
- WebSphere MQ Everyplace

  Provides industry strength messaging optimized for the mobile environment with intermittent network connectivity.

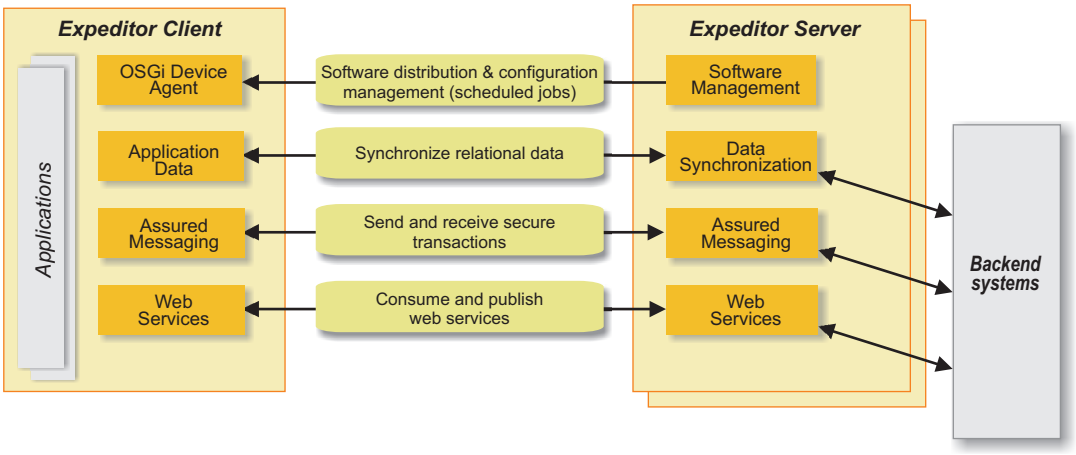
End-to-end access services

This topic describes the key products included with the Lotus Expeditor Server end-to-end solution. These components include: DB2 Everyplace, IBM WebSphere MQ Everyplace, and Device Manager Server.

The access services that comprise the Lotus Expeditor Server end-to-end solution model are as follows:

- Relational database synchronization users can access and update enterprise data from a database on their mobile devices and keep this data synchronized with other data sources in their enterprises. See “Relational database synchronization” on page 7.
- Transaction and messaging services using WebSphere MQ Everyplace enable messages and transactions to be queued up on the client for delivery as the client obtains a connection to a server. See “Transaction and messaging services” on page 8.
- Software management uses the Device Manager to administer both the Expeditor client as well as applications running on the client. See “Software management” on page 7.
- Web applications expose a set of Application Programming Interfaces (APIs) that you can use to create, test, and deploy server-managed software to semi-connected clients. See “Web applications” on page 9.

Lotus Expeditor End-to-end solution model



Relational database synchronization

With DB2 Everyplace, users can access and update enterprise data from a database on their mobile devices and keep this data synchronized with other data sources in their enterprises.

IBM DB2 Everyplace is a solution for mobile computing that enables mobile users to access the necessary information to perform their jobs, from any place, at any time.

The DB2 Everyplace solution consists of two main components:

- DB2 Everyplace or IBM Cloudscape™ database incorporated into Lotus Expeditor Client for Desktops and Mobile Devices.
- DB2 Everyplace Synchronization Server integrated into Lotus Expeditor Server

DB2 Everyplace database is a small footprint database engine installed on the Lotus Expeditor Client for Desktops and Mobile Devices client. DB2 Everyplace Synchronization Server carries out bidirectional synchronization of data between the database on the Expeditor Client and the source database on the server. DB2 Everyplace Synchronization is controlled by the DB2 Everyplace Synchronization Server component of Lotus Expeditor Server.

For synchronization of the relational database from the server to the Expeditor Client, Lotus Expeditor Server replicates the selected data periodically to a mirror (or mid-tier) database that serves as a temporary repository for the data. Lotus Expeditor Server moves a subset of the mirror data to the database on the Expeditor Client. For synchronization from the mobile client to the server, Lotus Expeditor Server moves data into the mirror database first and then replicates the data back to the server periodically.

To accommodate the security concerns of sensitive data stored on a mobile platform, DB2 Everyplace supports local encryption of the client-side database. When encrypted, the local database is also password protected. Additionally, DB2 Everyplace minimizes the synchronization data over the air by applying differencing techniques to the synchronized data and only sends necessary changes between the client and server. DB2 Everyplace accommodates the intermittent nature of wireless connections by supporting checkpoint restart, which enables the synchronization process to recover from a connection interruption without having to start synchronization from the beginning.

Software management

This topic describes how Lotus Expeditor Server uses Device Manager to deploy, configure and remove applications across multiple mobile clients on various platforms.

The Device Manager component of Expeditor Server provides a common software management function for the Expeditor Client and Expeditor Client applications running on a variety of desktop and mobile devices. Device management functions provided include:

- **Device enrollment**—Registering the client.
- **Client and application configuration**—Setting client and application parameters.
- **Software distribution**—Distributing, installing and uninstalling software on the client. Includes the ability to see the status of requests.
- **Inventory**—Collecting hardware and software information about the device (available only on certain client platforms).

Device Manager supports industry standards such as the Open Mobile Alliance Device Management and the Open Service Gateway Initiative (OSGi). Device Manager consists of a Web application and a relational database to store device management data. Managed clients require an agent to interact with the server. To manage an OSGi client, such as IBM Lotus Expeditor Client for Desktops and Mobile Devices, you need the plug-in and the device agent for OSGi devices. The OSGi Agent resides on the device and is responsible for running the commands sent by the Device Management Server. The OSGi Agent connects and interacts with the Device Management Server using the SyncML/DM protocol and is part of the Lotus Expeditor Client framework. The OSGi Agent does not have to be connected to the server all the time. When the agent connects, the server identifies the client and runs the jobs pending for the device.

Transaction and messaging services

IBM WebSphere MQ Everyplace provides the ability to integrate mobile clients to assured messaging systems, business integration systems, and financial transaction systems worldwide.

WebSphere MQ Everyplace enables messages and transactions to be queued on the client for delivery as the client obtains a connection to a server. The ability to queue data when the client obtains a connection to the server is important for intermittently-connected clients where financial transactions, medical information, or other critical data must be forwarded once, and only once, to a server. Examples of messages a program might send include: order entry, status updates, or requests for information.

A program can also receive messages with information on orders received, a list of things to be done, or replies to requests. Messages can be in any format as long as both the sender and receiver use the same format. A message can include simple text strings, or even serialized Java objects. WebSphere MQ Everyplace provides security capabilities for WebSphere MQ Everyplace applications that run outside the protection of an Internet firewall.

Lotus Expeditor Client integrates a subset of WebSphere MQ Everyplace functions that are applicable to the client platform. Lotus Expeditor Server includes the complete, licensed WebSphere MQ Everyplace product, including the function necessary for WebSphere MQ Everyplace to act as a gateway server to the WebSphere MQ products.

WebSphere MQ Everyplace is a member of the IBM WebSphere MQ family of business messaging products and integrates with other members of the WebSphere MQ family. To extend your messaging application to interact with your enterprise WebSphere messaging infrastructure, the server side of the solution requires you to install additional software. You must install the WebSphere MQ client on the Lotus Expeditor Server and configure WebSphere MQ Everyplace as a bridge to the WebSphere MQ network.

You can use the management tools in the WebSphere MQ Everyplace Server SupportPac™ in all phases of application development and rollout. They are more sophisticated than the utilities included with the licensed product and are an essential aid to getting started, configuring, inspecting pilot networks, and

managing production systems. If you intend to bridge to a WebSphere MQ family product, you must install the MQ client on Expeditor Server before you install the WebSphere MQ Everyplace Server SupportPac.

You can download the WebSphere MQ Everyplace Server SupportPac at: http://www.ibm.com/software/integration/support/supportpacs/

Web applications

Lotus Expeditor Client exposes a set of Application Programming Interfaces (APIs) that you can use to create, test, and deploy server-managed software to semi-connected clients.

The Enterprise Extensions leverage the enterprise developer community by using the same Java 2, Enterprise Edition (J2EE) programming model for Web application development. Embedded standard portlets (JSR 168 compliant), embedded servlets and embedded Java Server Pages (eJSPs) can enable local client browsers to render content, without the need of server connectivity. Embedded Web services enable you to integrate business applications and expand the applications running on enterprise servers. As a result, device users can access the applications from wireless and connected clients. In addition, you can use user interface Application Programming Interfaces (APIs) to deploy full function, rich client user interfaces to clients and avoid the network latency of constantly going back to a server. Client Services provides the platform integrity needed by enterprise Industrial Technology organizations to extend existing applications to server-managed clients because Extension Services is available on Java 2, Standard Edition (J2SE) and Java 2, Micro Edition (J2ME) platforms.

Planning for deployment

This topic explains how to plan your Lotus Expeditor Server environment.

Before you install Lotus Expeditor Server and associated components and products, review the following topics.

Planning considerations

This topic describes considerations for choosing the correct environment to install and configure Lotus Expeditor Server.

Lotus Expeditor Server supports the following environments:

- "Single system install with local database"
- "Single system install with remote database"
- "Multiple systems with a cluster of Lotus Expeditor Servers"
- "Using an LDAP registry" on page 12
- "High availability considerations" on page 12
- "Device Manager considerations" on page 12

Single system install with local database

For a single system install, select **local database** from the options offered during the Lotus Expeditor Server installation. As a result of this selection, all of the server components and databases are installed on a single system. This scenario is intended for developer or proof-of-concept installs. If you choose this install scenario, you will not be able to cluster the Lotus Expeditor Server. For the single system install, the default user registry for Lotus Expeditor Server is WebSphere Member Management. If you plan to use an LDAP directory, follow the instructions in "Upgrading to an LDAP user registry" on page 96. For instructions on installing a single system with a local database, see "Installing a single server" on page 38

Single system install with remote database

To use a remote database, select **remote database** from the options offered during the Lotus Expeditor Server installation. As a result of this selection, all the server components are installed on a single system and the databases are created on a separate system. This environment provides a path by which the Database Server can be made highly available as well as clustering the services of the Lotus Expeditor Server. The remote database server should use the same operating system as the Lotus Expeditor Server

Lotus Expeditor Server offers flexibility to grow from one single server to multiple systems. You must choose this option if you plan to grow your production environment from one single system to multiple physical systems. You can also use your local user registry for this scenario. To use an LDAP registry, follow the instructions in "Upgrading to an LDAP user registry" on page 96. For instructions on installing a single system with a remote database, see "Installing a single server" on page 38.

Multiple systems with a cluster of Lotus Expeditor Servers

You can create a cluster that would allow Lotus Expeditor Server to grow to multiple server systems. If you plan to install Lotus Expeditor Server on multiple systems, you must create a cluster on a single system installed with a remote database and configured for an LDAP user registry. This requires a WebSphere Application Server Deployment Manager. During the cluster creation, the Lotus Expeditor Server node is added to the Deployment Manager cell. After the cluster is created, a response file is generated that you can use when adding additional Lotus Expeditor Servers to the cluster. WebSphere

MQ Everyplace is not clustered because it is not an application server. To share MQe queues among multiple servers, you must create the queues on media that is accessible from all systems (for example, shared DASD). For instructions on setting up an initial cluster, see “Creating a cluster” on page 41.

In a high volume production environment, you might find it necessary to add additional Lotus Expeditor Servers to increase capacity or provide high availability for Lotus Expeditor Server services. After you have created the cluster from an initial installation, you can add additional Lotus Expeditor Server systems to the cluster. For instructions on how to add servers to your scaled environment, see “Adding an additional server” on page 43.

Using an LDAP registry

When you are ready to support a larger number of users, you can upgrade the server configuration for Lotus Expeditor Server to use an LDAP server as the user registry. After performing this upgrade, the User Management console is disabled. You must use the LDAP server’s management tools to manage users and groups.

To successfully configure Expeditor Server for LDAP, you must configure the user and group search paths at a point in the directory tree that covers all users. Specifically, you must provide the following directory search path information during the upgrade process: the directory root suffix, the top level users container under the directory suffix, and the top level groups container under the directory suffix. Refer to “Configuring the LDAP server” on page 93 and “Upgrading to an LDAP user registry” on page 96 for details on upgrading your system to LDAP.

High availability considerations

Consider the following when setting up a highly-available Lotus Expeditor Server system:

- Queues created with WebSphere MQ Everyplace must be on shared storage that is available to all systems. See the WebSphere MQ Everyplace section for more information.
- Consider other single points of failure in your system that might affect access to your IBM Lotus Expeditor system. Some components to consider are as follows:
  - LDAP server used to store IBM Lotus Expeditor users and groups
  - Web servers used to gain access to the IBM Lotus Expeditor servers
  - Load balancers (optional) used to distribute workload across WebSphere Everyplace Access servers
  - Database server where the IBM Lotus Expeditor databases are stored

Follow the instructions in “Installing Lotus Expeditor Server” on page 25 to install and configure systems in a IBM Lotus Expeditor environment.

Device Manager considerations

When defining software in Device Manager, make sure that the URL provided is accessible from both the server and clients that will install the software, regardless of which Device Manager Server is servicing the request. This means that you cannot use `localhost` or `127.0.0.1` as the host name for this software. Because the server accesses this URL when the software is created, it is possible for the software creation to succeed, even though the URL provided is not valid on the client. In this case, the software installation job will fail. Consider placing all the software bundles on a separate Web server to achieve this connectivity.

Operations for creating software include:

- Using the command line utility `dmaddsw`
- Using the Device Manager Console, new software operation

Software and hardware topologies

This topic provides information about software and hardware topologies to help plan your installation of Lotus Expeditor Server.

- "Software topology"
- "Hardware topology examples"

Software topology

Use the information in this section to understand how the software components interact. For a description of how different servers might be set up to support the software topology, see "Hardware topology examples."

Lotus Expeditor Server installs and runs as a collection of application servers on the WebSphere Application Server platform. For each installation of Lotus Expeditor Server, an installation of WebSphere Application Server is required. In addition, both the Lotus Expeditor Server and WebSphere Application Server installations must reside on the same system.

Note: Installing multiple Lotus Expeditor Server instances on a single WebSphere Application Server instance is not supported.

Hypertext Transfer Protocol (HTTP) is used as the transport protocol for the majority of the Lotus Expeditor Server services requests. It is required that the IBM HTTP server be installed locally with the first install of Lotus Expeditor Server. For a clustered environment, all Lotus Expeditor Server instances can share one or more remote Web servers.

Because IBM Lotus Expeditor administration and configuration are dependent on WebSphere Application Server, you might have to use the administrative tools that are provided with WebSphere Application Server to monitor or control activities that are related to the Lotus Expeditor Server. Additionally, if you configure an external Web server for use with Lotus Expeditor Server, you might need to use the Web server interface to administer Lotus Expeditor Server related activities.

Lotus Expeditor Server and WebSphere Application Server require access to a user registry. The following list provides different sources that the Lotus Expeditor Server can use to access a user registry:

- Lightweight Directory Access Protocol (LDAP) directory, such as IBM Tivoli® Directory Server, Domino® Directory, Active Directory, Novell eDirectory, or Sun ONE
- Database User registry (WebSphere Member Manager)

Lotus Expeditor Server automatically creates a database on the DB2 server to use for authentication. You can reconfigure Lotus Expeditor Server to use an LDAP directory to authenticate users and maintain user and group relationships.

Hardware topology examples

WebSphere Application Server supports a wide variety of ways to deploy in your computing environment. Commonly used topologies fall into one of the following broad categories:

- **Single-system topology**. The components are installed on the same system. This topology is useful for developer and proof of concept installations, but is not recommended for production environments.
- **Multi-system topologies**. The components (the Web server, application server, databases, and so forth) are physically separated onto different systems.
- **Vertical scaling topologies**. Multiple application servers running IBM Lotus Expeditor are created on a single physical system, usually by creating cluster members. Note that Lotus Expeditor Server does not support this topology.

- **Horizontal scaling topologies**. Members of a Lotus Expeditor Server cluster exist on multiple physical systems, effectively and efficiently distributing the workload of a single logical Lotus Expeditor Server. HTTP redirector products can also be used to implement horizontal scaling. Clustering is most effective in environments that use horizontal scaling because of the ability to build in redundancy and failover, to easily add new horizontal cluster members to increase capacity, and to improve scalability by adding heterogeneous systems into the cluster.
- **HTTP server separation topologies**. The Web (HTTP) server is located on a different physical system than WebSphere Application Server and Lotus Expeditor Server.
- **Demilitarized zone (DMZ) topologies**. Firewalls can be used to create demilitarized zones -- systems that are isolated from both the public Internet and other systems in the configuration. This improves security, especially for sensitive back-end resources, such as databases.

Note: It is important to remember that, in any topology, many resources and settings that are defined within WebSphere Application Server, like Global Security Settings, DataSources, and so on, are shared across all applications, including the Lotus Expeditor Server instances.

Supported hardware and software

This topic provides hardware requirements and software product levels that are supported for Lotus Expeditor Server 6.1. This page also includes system requirements for optional software.

Lotus Expeditor Server has specific system requirements and component prerequisites that must be understood prior to installation. These requirements were accurate at the time this information was published and reflects what was used during testing and quality assurance. As newer versions of software are supported, information will be provided on the Lotus Expeditor Server Support page at: http://www-306.ibm.com/software/lotus/expeditor/support/. If you cannot find your required version, contact IBM Support before proceeding.

Hardware requirements

This topic provides data for hardware configurations that have been tested by IBM. Use the following information as a guide for your installation of IBM Lotus Expeditor Server. Also see "Installation requirements" on page 25 for more information.

Note: Installation times will vary based on system characteristics, including processor speed, available disk space, and physical memory size. Installation on systems with the minimum requirements takes several hours.

Linux Intel® systems

Refer to the following list for hardware requirements for Linux Intel systems:

- **Processor**: Pentium® 2GHz or equivalent at a minimum
- **Physical memory**: 2 GB or more per processor
- **Disk space**: The following values are required if you use the installation program to install WebSphere Application Server, extensions and fixes, and IBM Lotus Expeditor. These values do not account for any other products or components that could be installed on the IBM Lotus Expeditor system. See the documentation shipped with your products for additional hardware requirement information. The following list shows the space requirements by component:

Table 1. Disk space

Component	Install directory (/opt)	Temp directory (/tmp)
IBM Lotus Expeditor	1 GB	200 MB
WebSphere Application Server, plugin, and fixes	1.7 GB	300 MB
DB2	500 MB	10 MB
IBM HTTP Server and fixes	100 MB	10 MB
Total	3.3 GB	520 MB

Virtual memory/swap space: This value should be equal to double your physical memory. At a minimum, this value should be at least equal to your physical memory.

- **File system size**: The Linux ext2 file system, which is used by default, does not allow you to change the file system size. Therefore, you should carefully plan in advance for the size of your file system in order to avoid related problems. The following disk space is required for each directory:
  - /: 1.5 GB or more (root directory)
  - /opt: 2.5 GB or more. The default directory to install IBM Lotus Expeditor on Linux is /opt. By default, /opt is under / file system. If you choose to install IBM Lotus Expeditor under /usr, 3.5 GB or more is recommended.
  - /home: 500 MB or more (home directory)
- **Network connectivity**: The following elements are required for the server system:
  - Network adapter and connection to a physical network that can carry IP packets. For example, Ethernet, Token Ring, ATM, and so on.
  - Configured fully-qualified host name. The IBM Lotus Expeditor system must be able to resolve an IP address from its fully-qualified host name. To ensure that this is configured correctly, issue the ping command from a command line. For example, ping *hostname.yourco.com*, where *hostname.yourco.com* is the fully-qualified host name.

Windows systems

See the following list for hardware requirements for Windows systems:

- **Processor**: Pentium 2GHz or equivalent at a minimum
- **Physical memory**: 2GB or more per processor
- **Disk space**: The following values are required if you use the installation program to install WebSphere Application Server, extensions and fixes, and IBM Lotus Expeditor. These values do not account for any other products or components that could be installed on the IBM Lotus Expeditor system. See the documentation shipped with your products for additional hardware requirement information. You can perform a custom installation of the components. The following list shows the space requirements by component:

Table 2. Disk space

Component	Install directory (C:\Program Files\IBM\WebSphere or C:\Program Files\IBM\Lotus)	Temp directory (%TEMP%\IBM)
IBM Lotus Expeditor	1 GB (2.5 GB for a local database)	200 MB
WebSphere Application Server, plugin, and fixes	1.7 GB	300 MB
DB2	500 MB	10 MB
IBM HTTP Server and fixes	100 MB	10 MB
Total	3.3 GB	520 MB

- **Virtual memory/swap space**: This value should be equal to double your physical memory. At a minimum, this value should be at least equal to your physical memory.
- **File system**: NTFS file system is recommended.

  Note: Because the installation program does not check cluster sizes on a file system, install on an NTFS file system to ensure that you have enough disk space. If you intend to install on a FAT file system, make sure that you have enough disk space prior to installation. For information, see the Microsoft® support Web site, http://support.microsoft.com, and search for content about default cluster sizes for FAT file systems.
- **Network connectivity**: The following elements are required for the server system:
  - Network adapter and connection to a physical network that can carry IP packets. For example, Ethernet, Token Ring, ATM, and so on.
  - Configured fully-qualified host name. The Lotus Expeditor system must be able to resolve an IP address from its fully-qualified host name. To ensure that this is configured correctly, issue the ping command from a command line. For example, ping *hostname.yourco.com*, where *hostname.yourco.com* is the fully-qualified host name.

Software requirements

This topic provides the minimum product levels that you should install for IBM Lotus Expeditor. Because other products frequently ship fixes, updates, and new releases, every possible configuration has not been tested.

Notes:
- Required software is supported only on the platforms that IBM Lotus Expeditor supports.
- Usage restrictions apply for some software. Consult the product license for details.

Supported operating systems

One of the following operating systems is required on the system where IBM Lotus Expeditor will be installed:

Operating system	Notes	Additional information on fixes and support
Linux		
Red Hat Enterprise Linux Enterprise Server 4.0 for Intel (x86)	Supports 32-bit version only.	http://www.redhat.com/
Red Hat Enterprise Linux Enterprise Server 4.0 for Intel (x86) update 1, 2, or 3	Supports 32-bit version only.	http://www.redhat.com/
Red Hat Enterprise Linux Advanced Server 4.0 for Intel (x86)	Supports 32-bit version only.	http://www.redhat.com/
Red Hat Enterprise Linux Advanced Server 4.0 for Intel (x86) update 1, 2, or 3	Supports 32-bit version only.	http://www.redhat.com/
Windows		
Windows 2003 Enterprise	Supports 32-bit version only.	http://www.microsoft.com
Windows 2003 Enterprise SP 1	Supports 32-bit version only.	http://www.microsoft.com
Microsoft Windows 2003 Standard	Supports 32-bit version only.	http://www.microsoft.com
Microsoft Windows 2003 Standard SP 1	Supports 32-bit version only.	http://www.microsoft.com

Supported application server

WebSphere Application Server 6.0.2.11 and higher fix pack levels

Red Hat Linux 4 system users only: Prepare your system for WebSphere Application Server 6.0.2. Complete instructions at http://www-1.ibm.com/support/docview.wss?rs=180&=swg21201306

Note: WebSphere Application Server 6.1 is not supported.

Supported Web server (required)

IBM HTTP Server 6.0.2.11 and higher fix pack levels

Note: This is the HTTP server that is provided with WebSphere Application Server. For additional information on fixes and support, see http://www.ibm.com/software/webservers/httpservers/

Support for Remote Web servers

This statement only applies to Web servers running on a separate system than Lotus Expeditor Server. If you plan to run the Web server on the same system as Lotus Expeditor Server, you must use IBM HTTP Server 6.0.2.11 or a higher fix pack.

IBM Lotus Expeditor support for remote Web servers spans two categories:

- **Fully-tested and supported remote Web servers**: The list of fully tested Web servers for each release of IBM Lotus Expeditor is documented in the information center and in the supported hardware and software documentation for each release. IBM Lotus Expeditor support accepts problem reports for the appropriate IBM Lotus Expeditor releases using the tested Web servers. These problem reports receive high-priority attention.
- **Untested and partially supported remote Web servers**: In general, IBM Lotus Expeditor support makes a best effort to support remote Web servers that have not been tested with IBM Lotus Expeditor. IBM Lotus Expeditor support accepts problem reports for the appropriate IBM Lotus Expeditor releases using untested remote Web servers. If IBM Lotus Expeditor support can re-create the reported problem using a tested remote Web server, staff will attempt to fix the problem. If the support team is not able to re-create the problem on a tested remote Web server, customers are referred to the Web server provider for further assistance.

Submitting requests for additional Web server support:

IBM Lotus Expeditor Development accepts customer requirements for Web server support and functionality enhancements. Formal requirements are reviewed for consideration if they are submitted through the applicable IBM marketing or sales representative. Customer requirements must address one of the following areas:

- Formal Web server support for additional Web server products, platforms, or configurations not currently supported, as previously indicated.
- Functional enhancements that either extend or exploit IBM Lotus Expeditor Web server integration capabilities.

Supported databases (required)

You can use one of the following database products to store IBM Lotus Expeditor information.

Table 3. Supported databases

Database	Notes	Additional information on fixes and support
IBM DB2 Enterprise 9.1 for Linux, UNIX®, and Windows	Any fix pack provided for DB2 9.1 will be supported.	http://www.ibm.com/software/data/db2/
IBM DB2 Workgroup Server Edition 9.1 for Linux, UNIX, and Windows	Any fix pack provided for DB2 9.1 will be supported.	http://www.ibm.com/software/data/db2/

Notes:

- A database server is required for IBM Lotus Expeditor.
- If you install the database server on a different system from where IBM Lotus Expeditor is installed, the database server must be on the same operating system that is installed on the IBM Lotus Expeditor server system.

Supported LDAP directories (optional)

You can use one of the following software products as an LDAP directory to store user information.

Table 4. Supported LDAP directories

LDAP server	Notes	Additional information on fixes and support
IBM Tivoli Directory Server 6.0	Only supported using the custom LDAP configuration.	http://www.ibm.com/software/tivoli/products/directory-server/
IBM Lotus Domino Enterprise Server 7.0	Only supported using the custom LDAP configuration.	http://www.lotus.com/products/product4.nsf/wdocs/dominohomepage
IBM Lotus Domino Enterprise Server 6.5.*x*	Only supported using the custom LDAP configuration.	http://www.lotus.com/products/product4.nsf/wdocs/dominohomepage
Windows Active Directory 2003		http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

Notes:

1. Using an LDAP server is optional for IBM Lotus Expeditor.
2. Because you can install the LDAP server on a different system from where Lotus Expeditor Server is installed, you might be able to install the LDAP server on an operating system that is different from the operating system on the Lotus Expeditor system.

Support for LDAP servers

IBM Lotus Expeditor support for LDAP servers spans two categories:

- **Fully tested and supported LDAP servers**: IBM Lotus Expeditor support accepts problem reports for the appropriate IBM Lotus Expeditor releases using the tested directory servers. These problem reports receive high-priority attention. Features that are tested with these directories include relatively simple search and retrieval functions for user and group objects. Functions outside this scope, such as dynamic groups, referrals, or the Active Directory Global Catalog feature, are considered advanced features and have not been tested with IBM Lotus Expeditor. IBM Lotus Expeditor support encourages customers to work with their LDAP provider for additional support on these advanced features.
- **Untested and partially supported LDAP servers**: In general, IBM Lotus Expeditor support makes a best effort to support directory servers that have not been tested with IBM Lotus Expeditor. IBM Lotus Expeditor support accepts problem reports for the appropriate IBM Lotus Expeditor releases using untested directory servers. If IBM Lotus Expeditor support can recreate the reported problem using a tested LDAP server, staff will attempt to fix the problem. If the support team is not able to recreate the problem on a tested LDAP server, customers are referred to the LDAP provider for further assistance.

Submitting requests for additional LDAP support

IBM Lotus Expeditor Development accepts customer requirements for LDAP support and functionality enhancements. Formal requirements are reviewed for consideration if they are submitted through the applicable IBM marketing or sales representative. Customer requirements must address one of the following areas:

- Formal LDAP support for additional LDAP products, platforms, or configurations not currently supported, as previously indicated.
- Functional enhancements that either extend or exploit IBM Lotus Expeditor LDAP integration capabilities.

Supported Web browsers (required)

- The IBM Lotus Expeditor User Management console and WebSphere Application Server administration require a Web browser to access them. You can only work with the User Management console using a desktop browser.
- These Web browsers were tested by IBM on servers that support the following client operating systems or desktop products:
  - Red Hat Enterprise Linux WS v4.0/Red Hat Desktop
  - Microsoft Windows 2000
  - Microsoft Windows XP Professional

Behavior in Web browsers that are not listed, or in Web browsers that are listed but on client operating systems that are unlisted, is unknown.

Table 5. Supported Web browsers

Web browser	**Additional information on fixes and support**
Microsoft Internet Explorer 6.0 SP1	http://www.microsoft.com
FoxFire 1.5	http://www.mozilla.org/
Mozilla Web browser 1.0.6 **Note:** On Linux systems, the Mozilla Web browser is required for the operation of the First Steps console.	http://www.mozilla.org/
Netscape Communicator 8.0	http://www.netscape.com/
Opera Web Browser 7.23 (or higher)	http://www.opera.com/

Supported clients

- Lotus Expeditor Client for Desktops and Mobile Devices 6.1
  - Windows XP
  - Red Hat Linux
  - Windows Mobile 2003 SE and Windows Mobile 5 (PocketPC and Phone editions)
- IBM Workplace Client Technology™, Micro Edition Enterprise Offering (WCTME EO) 5.8.1
- WebSphere Everyplace Deployment 6.0.0 and 6.0.0.1
- IBM Workplace Client Technology, Micro Edition (WCTME) 5.7.1 and WCTME 5.7.2 for devices:
  - Windows Mobile 2003 2nd Edition with HP iPaQ Pocket PC h5550
  - Windows Mobile 2003 2nd Edition with HP iPaQ Pocket PC h4700
  - Windows Mobile 2003 2nd Edition with HP iPaQ Pocket PC h3715
- IBM Workplace Client Technology, Micro Edition (WCTME) 5.7.1 for devices:
  - Windows Mobile 2003 with HP iPaQ Pocket PC h5550

OSGi support

The Device Manager OSGi plug-in included with Lotus Expeditor Server supports all of the Windows Mobile clients listed in “Supported clients” on page 19. Do not install the OSGi plug-in included on the WCTME EO media. An IFix is required for WCTME 5.7.2 and WCTME 5.7.1 FP1 to obtain the OSGi support that will work with Lotus Expeditor Server 6.1. The *IFix required is 112818* and is available from the WCTME EO support Web site.

Compatible products

Separate enhancements are available that work with Lotus Expeditor Server.

- The Lotus Expeditor client package includes a Network Client Installer that provides for remote installation of the Lotus Expeditor client. It supports the following environments: Web server only, Portal Server, or Lotus Expeditor Server. For purchasing information of the client, contact your IBM representative.
- Performance planning data can be used to assist in scaling Lotus Expeditor Server. For purchasing information, contact your IBM representative.

Supported naming conventions

This topic provides naming conventions for directories, users, and groups that are supported for IBM Lotus Expeditor Server 6.1.

Lotus Expeditor Server authenticates the user with the value specified for the LDAP user login name. You must specify the LDAP user login name to log in as the Lotus Expeditor Server administrator. The user login name must be unique. Supported naming conventions for Expeditor Server users, groups, and containers created in LDAP, as well as the install directory name, are as follows:

- There must not be a space in the relative distinguished name of the administrative user. A container name can contain a space.
- Lotus Expeditor Server does not permit any users to have the following special characters in their distinguished names: "#", ",", "+", """, "\", "<", ">", ";", "(", ")", or "*".
- Names cannot include NON-ASCII characters, or diacritics, such as umlauts.
- Valid characters for user, group, and container names include a-z, A-Z, 0-9, and underscore.
- DB2 Everyplace requires that names do not begin with a numeric character.
- The container name must contain only single-byte characters. The container name does not support double-byte characters.
- The user login name must be unique.

Directory names

Valid characters for an installation directory are a-z, A-Z, 0-9, diacritics, '-' (dash), '_' (underscore), and space (Windows only). Double-byte characters are not valid.

Database User Registry Naming Limitations

Lotus Expeditor Server is configured to use a database user registry after the initial install. Expeditor Server provides an user management application to manage users in the database user registry. The following restrictions apply to user IDs, passwords, or group names defined in the database user registry.

Users and groups

Administrator user IDs and passwords:

User IDs: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore) Note that double-byte characters or diacritics, such as umlauts, are not valid for Administrator user IDs. Also the administrator user ID cannot begin with a numeric character (0-9), '-' (dash), '.' (dot), or '_' (underscore).

Passwords: Any characters except the following: spaces, non-ASCII characters (including double-byte characters or diacritics, such as umlauts), and the following special characters: % ^ &) ″ < > \ |

Attention: **Linux users**: ! and $ characters are also not supported in administrator passwords.

General user ID and passwords:

User IDs: Valid characters for user IDs include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore). Double-byte characters or diacritics, such as umlauts, are permitted. Also the user ID cannot begin with a numeric character (0-9), '-' (dash), '.' (dot), or '_' (underscore).

Passwords: Any characters except the following: spaces, and the following special characters: !@#$% ^ &*( ) ″ < > \ |=+, - . _

Group names:

Lotus Expeditor Client administrator group: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore) Note: Double-byte characters or diacritics, such as umlauts, are not valid for the administrator group.

Synchronization group: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore). Double-byte characters or diacritics, such as umlauts, are permitted.

DB2e user groups: Valid characters for user IDs include a-z, A-Z, 0-9, and special characters: !@#$% ^ &*( ) ″ < > \ |=+, - . _. Double-byte characters or diacritics, such as umlauts, are permitted.

LDAP Naming Limitations

The following restrictions apply to user IDs, passwords, or group names used by the Lotus Expeditor Server after reconfiguring the Lotus Expeditor Server to use an LDAP server.

Container restriction:

The container name must contain only single-byte characters. Expeditor Server does not support container names using double-byte characters.

Administrator user IDs and passwords:

User IDs: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore) Note: Double-byte characters or diacritics, such as umlauts, are not valid for administrator user IDs. Also the administrator user ID cannot begin with a numeric character (0-9), '-' (dash), '.' (dot), or '_' (underscore).

Passwords: Any characters accepted by the LDAP server with the following exceptions: spaces, non-ASCII characters (including double-byte characters or diacritics, such as umlauts), and the following special characters: % ^ &) ″ < > \ |

Attention: **Linux users**: ! and $ characters are also not supported in administrator passwords.

General user IDs and passwords:

User IDs: Any characters accepted by the LDAP server with the following exceptions: spaces. Also the user ID cannot begin with a numeric character (0-9).

Passwords: Any characters accepted by the LDAP server.

Group names:

Lotus Expeditor Client Administrator group: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore) Note: Double-byte characters or diacritics, such as umlauts, are not valid for the administrator group.

Synchronization users group: Valid characters include a-z, A-Z, 0-9, and '-' (dash), '.' (dot), and '_' (underscore). Double-byte characters or diacritics, such as umlauts, are permitted.

DB2e users groups: Any characters accepted by the LDAP server.

Planning for a clustered environment

This topic provides information you can use to plan your Lotus Expeditor Server in a clustered environment.

- "Before you begin"
- "Guidelines for implementing cluster environments"
- "Limitations" on page 23

Before you begin

Review "Planning considerations" on page 11 for the Lotus Expeditor Server environment before reviewing this section for planning considerations specific to clusters.

In WebSphere Application Server, a cluster is composed of multiple identical copies of an application server. A cluster member is a single application server in the cluster. Lotus Expeditor Server is installed as a collection of enterprise application services within the WebSphere Application Server infrastructure. The exception to this is WebSphere MQ Everyplace. The services provided by MQ Everyplace do not run as an enterprise application service. All of the clustering features available within the WebSphere Application Server infrastructure are also available and apply to Lotus Expeditor Server. Consequently, an Lotus Expeditor Server cluster is simply a collection of multiple Lotus Expeditor Servers that are identically configured.

When planning for Lotus Expeditor Server clusters, you must also take into account any cluster planning required for the WebSphere Application Server nodes. For further information, see product planning documentation for the version of WebSphere Application Server Network Deployment supported by the version of Lotus Expeditor Server that you are using.

Guidelines for implementing cluster environments

Cluster environments should be implemented according to the following guidelines:

- In WebSphere Application Server 6, there are additional requirements for properly configuring your Web server. If you do not follow these steps, the Web server plug-in might not work as expected. See "Updating the Lotus Expeditor Web server" on page 102 for more information.
- Ensure that WebSphere Application Server is installed properly on each node. Make sure that all appropriate interim fixes are applied to each node. The Deployment Manager (from WebSphere Application Server Network Deployment) should always be at the same fix level or higher than any managed WebSphere Application Server node.
- Ensure that the Lotus Expeditor Server is installed properly with databases on a remote database server and configured for an LDAP directory.
- The Deployment Manager node must be installed separately before the cells and clusters can be configured. See the WebSphere Application Server Network Deployment Information Center for details.
- Network Deployment must be configured with the same security settings as Lotus Expeditor Server before adding an Lotus Expeditor Server node to the cell. The Lotus Expeditor Server configuration wizard will automatically do this for you or you can choose to configure the Network Deployment security manually. You must manually enable custom security for WebSphere Network Deployment before attempting to configure to a custom LDAP. The configuration wizard will automatically configure Network Deployment security only if you are using Active Directory 2003. See the WebSphere Application Server Network Deployment Information Center for details on how to configure security for Network Deployment.

- Add the primary Lotus Expeditor Server node to the cell using the Lotus Expeditor Server configuration wizard. This wizard will prepare the Lotus Expeditor Server configuration for a cell environment and manage the addNode process automatically. Do not attempt to manually add an Lotus Expeditor Server node to a cell.
- Install additional secondary Lotus Expeditor Server nodes into the cluster. These nodes may already be members of the Deployment Manager cell to which the primary Lotus Expeditor Server belongs. If the nodes are unmanaged, the installation program will handle joining the node to the Deployment Manager cell.

Limitations

The following limitations apply when implementing an Lotus Expeditor Server cluster:

- Expeditor Server cannot coexist in the same WebSphere management cell as WebSphere Portal Server.
- You must install and configure the primary Lotus Expeditor Server on an unmanaged node (not already part of a cell).
- There can only be one primary Lotus Expeditor Server installation per cell. Additional nodes must be installed using the secondary node install process.
- Lotus Expeditor Server services cannot be configured for vertical clustering.
- Lotus Expeditor Server cannot be clustered using database server that is local to the Lotus Expeditor Server.
- Expeditor Server cannot be clustered using the database user registry. Use the Configuration Wizard to configure Expeditor Server to use an LDAP registry before clustering.
- Uninstallation of the primary node, when there are secondary nodes in the cluster, is not supported and should not be attempted. You must uninstall the secondary nodes before uninstalling the primary node.

Installing Lotus Expeditor Server

This topic provides instructions on how to install Lotus Expeditor Server successfully.

You can access information on the following installation topics.

Installation overview

This topic provides overview information about the Lotus Expeditor Server installation process.

The Lotus Expeditor Server installation program includes two distinct processes: installation and configuration. The installation process copies the required files to the system; the configuration process customizes these files for use in your production environment. Before you begin the installation process, you need to determine whether you require simple installation (all prerequisite products of Lotus Expeditor Server installed on one system) or a distributed environment (the database is installed on a remote system to allow clustering and greater productivity). See "Planning considerations" on page 11 to assist with determining your installation environment.

After the installation process is completed, Lotus Expeditor Server automatically invokes the Configuration Wizard to configure the server. During the configuration phase, the Configuration Wizard sets up component databases, configures services in WebSphere Application Server, and updates the server configuration files with the information collected from the installation panels. After the configuration phase is completed, the server is ready to use.

Getting started with the installation

Lotus Expeditor Server uses a graphical launchpad and installation wizard to guide you through the installation and configuration process. During this process, Lotus Expeditor Server performs the following steps:

- Checks for prerequisites and collects the necessary information for the installation and initial configuration.
- Performs validation checks using the information you specify.
- Installs the files for Lotus Expeditor Server core services, Device Manager, DB2 Everyplace, and WebSphere MQ Everyplace.
- Launches the Configuration Wizard automatically when the installation completes.

Lotus Expeditor Server provides a post-installation First Steps console as a convenient launching point from which to explore and start using the product. See "Using the First Steps console" on page 46 to see a list of options offered after completion of the installation process.

Review "Installation procedures and scenarios" on page 36 to better understand the Lotus Expeditor Server installation process.

Installation requirements

This topic identifies requirements and limitations for your server environment.

Before you install Lotus Expeditor Server, see the following information to ensure that you have correctly prepared your environment for installation.

- You cannot install Lotus Expeditor Server into a WebSphere managed node. After installation completes, Lotus Expeditor Server provides a configuration wizard to guide you through the process of

adding the Lotus Expeditor Server node into a Network Deployment cell. You cannot manually add the initial Lotus Expeditor Server node into a Network Deployment cell.

- WebSphere Portal Server cannot reside in the same management configuration cell as Lotus Expeditor Server.
- WebSphere Everyplace Access cannot reside in the same WebSphere Application Server management configuration (node or cell) as Lotus Expeditor Server.
- Standalone versions of DB2 Everyplace or products containing Device Manager cannot reside in the same WebSphere Application Server management configuration (node or cell) as Lotus Expeditor Server. Stand alone versions of WebSphere MQ Everyplace cannot reside on the same system as Lotus Expeditor Server. The Lotus Expeditor Server installation program does not support migrating from prior standalone versions of these components.
- All IBM Lotus Expeditor Client for Desktops and Mobile Devices and Workplace Client Technology, Micro Edition Enterprise Offering client components must reside on a separate system from the Lotus Expeditor Server components.
- Your Microsoft Windows 2003 server can be a member of a Windows domain; however, the user ID that you use to install Lotus Expeditor Server must be a local user ID. In addition, the person performing the installation must not be logged into the Microsoft domain during the installation process.
- You cannot install Lotus Expeditor Server on a system that is configured with the Arabic locale.
- Lotus Expeditor Server does not provide explicit support for clustering options provided by the operating system (for instance, Microsoft Cluster Server). Only WebSphere Application Server clustering is supported.

To continue preparing your production environment for the installation of Lotus Expeditor Server, complete instructions in one of the following sections to prepare your operating system.

Preparing a Windows operating system

Review this topic to make sure that your Microsoft Windows operating system is ready for the Lotus Expeditor Server installation and configuration process.

This topic includes prerequisite checks and setup instructions for:

- Checking the network setup
- Checking access rights for the system login user ID that is required during installation
- Disabling Microsoft Internet Information Services (IIS)
- Disabling any firewall products

Checking the network setup

This topic describes the network setup requirements. Proper network configuration is essential when installing Lotus Expeditor Server.

Checking for a static IP address

Lotus Expeditor Server requires your system to have a static IP address if the system will be used in production. A dynamic IP address is allowed for development environments. Use the following instructions to determine if the system's network is configured correctly:

1. Open your network connection.
2. Right-click the **LAN connection** for your network adapter and click **Properties**.
3. On the network adapter properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) is displayed.

4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the system has a dynamic IP address. If your system has a dynamic IP address and this installation is intended for production use, contact your network administrator to obtain and configure a static IP address.

Checking for a fully-qualified host name

Lotus Expeditor Server also requires the use of a fully-qualified host name, which is typically the host name of the server, along with its fully-qualified domain name. To ensure that the fully-qualified host name is configured correctly, use the ping command before you start the installation. For example, type the following command at the command prompt:

```
ping yourserver.yourcompany.com
```

Where *yourserver.yourcompany.com* represents the fully-qualfied host name of your system.

If a fully-qualified host name is not configured correctly, the request might time out. If necessary, contact your network administrator for assistance.

Note: Lotus Expeditor Server does not support the use of an IP address instead of a fully-qualified host name registered with your Domain Name Server (DNS).

Checking port bindings

Lotus Expeditor Server requires specific ports to complete the installation. If two applications attempt to use the same port, a port conflict results.

To ensure that port bindings are available, use the Netstat utility as follows:

1. Click **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type **netstat -an** at the command prompt.
3. Look at the numbers listed in the Local Address column. The fifth number is the port number. For example, if the IP address is 1.2.3.4:80, 80 is the port number.
4. Verify that the following list of port numbers, required by Lotus Expeditor Server, are not in use. If any of these port numbers are already in use you might experience port conflicts. Lotus Expeditor Server requires the following ports by default for Lotus Expeditor Server and related applications:
   - 80 (HTTP port)
   - 523 (DB2 Administration Server)
   - 8008 (IBM HTTP Server Administration port)
   - 50000 (DB2 instance connection port)
   - 50001 (DB2 instance interrupt port)
   - 50002 (DB2 Control Server)
   - 55555 (WebSphere Application Server database port)

Checking access rights for the system login user ID required during installation

You must log in to the system with an administrative user ID to perform the installation and configuration. To be an administrative user ID, it must belong to the administrator's group defined in the Windows operating system. You cannot install Lotus Expeditor Server while logged into a Microsoft Domain. You must log in using a local Administrative user with proper access rights before starting the installation and configuration. In addition, the user ID must have the following rights:

- Act as part of the operating system
- Create a token object
- Adjust memory quotas for a process

- Replace a process level token
- Log on as a Service

To access the interface for editing user rights:

1. Click **Start** → **Programs** → **Administrative Tools** → **Local Security Policy**.
2. Expand **Local Policies** and click **User Rights Assignment**.
3. Locate each Policy listed above and verify that the logon ID is listed in the **Security Setting** column.
4. To add the user, right-click the **Policy** and select **Properties**.
5. Click **Add User or Group...**.

Disabling Microsoft Internet Information Services

If Microsoft Internet Information Services (IIS) Web server is running on your system, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft Internet Information Services Web server.

To determine whether or not Internet Information Services is enabled, complete the following steps:

1. Click **Start** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**. If IIS is selected, it is enabled on the system.

To disable Internet Information Services, complete the following steps:

1. Click **Start** → **All programs** → **Administrative Tools**.
2. Open **Services**.
3. Locate and highlight **Internet Information Services Admin Service**.
4. Click on the **Action** menu.
5. Click **Properties**.
6. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
7. Click **Yes** to stop any services that are stopped as a result.
8. Locate the **World Wide Web Publishing Service** and also disable it at startup using the previous steps.

Disabling any firewall products

Before you start the Lotus Expeditor Server installation program, it is recommended that you disable any firewall products that are running. The Lotus Expeditor Server installation and configuration program will attempt to access local TCP/IP resources, such as the local Web server. No external resources will be accessed. If the firewall denies the access attempts made by the installation and configuration program, the installation will fail. The firewall might be re-enabled on completion of the installation and configuration program.

Preparing a Red Hat Linux operating system

Review this topic to make sure that your Linux operating system is ready for the Lotus Expeditor Server installation and configuration process.

This topic includes prerequisite checks and setup instructions for:

Checking the network setup

This topic describes the network setup requirements. Proper network configuration is essential when installing Lotus Expeditor Server.

Checking for a static IP address

Lotus Expeditor Server requires your system to have a static IP address if the system will be used in production. A dynamic IP address is allowed for development environments. Use the following instructions to determine if the system's network is configured correctly:

1. Click **Applications → System Settings → Network** to launch the Network Configuration application.
2. Click on the **Active** device in the **Devices** tab.
3. Verify that you have selected **Statically set IP addresses**. If **Automatically obtain IP settings with** is selected, the system has a dynamic IP address. If your system has a dynamic IP address and the system will be used in a production environment, contact your network administrator to obtain and configure a static IP address.

Checking for a fully-qualified host name

Lotus Expeditor Server also requires the use of a fully-qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). To ensure that the fully-qualified host name is configured correctly, use the ping command before you start the installation. For example, type the following command at the command prompt:

```
ping yourserver.yourcompany.com
```

Where `yourserver.yourcompany.com` represents the fully-qualfied host name of your system. If a fully-qualified host name is not configured correctly, the request might time out. If necessary, contact your network administrator for assistance.

Note: Lotus Expeditor Server does not support the use of an IP address instead of a fully-qualified host name registered with your Domain Name Server (DNS).

Checking port bindings

Lotus Expeditor Server requires specific ports to complete the installation. If two applications attempt to use the same port, a port conflict results.

You can use the Netstat utility to ensure that port bindings are available:

1. Open a terminal.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the **Local Address** column. The fifth number is the port number. For example, if the IP address is 1.2.3.4:80, 80 is the port number.
4. Verify that the following list of port numbers, required by Lotus Expeditor Server, are not in use. If any of these port numbers are already in use you might experience port conflicts. Lotus Expeditor Server and related applications require the following ports by default for successful operation:
   - 80 (HTTP port)
   - 523 (DB2 Administration Server)
   - 8008 (IBM HTTP Server Administration port)
   - 50000 (DB2 instance connection port)
   - 50001 (DB2 instance interrupt port)
   - 50002 (DB2 Control Server)

Enabling database access for the root user

The root user must be able to access the database during installation and when running the WebSphere Application Servers. Follow these steps to ensure proper access:

1. Source the db2profile before running the install and add a line to setupCmdLine to source db2profile.
   a. Add the following lines to beginning of the /opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh. Be sure to insert these lines after the #!/bin/sh line:

      ```
      if [ -f /home/db2inst1/sqllib/db2profile ]; then
      . /home/db2inst1/sqllib/db2profile
      fi
      ```

      where db2inst1 is replaced by the DB2 instance owner used to install the software.
   b. Before running the launchpad.sh or install.sh, run the following command in the same terminal window you will use to launch the install:

      ```
      . /home/db2inst1/sqllib/db2profile
      ```

      where db2inst1 is replaced by the DB2 instance owner used to install the software.
2. Modify the root .bash_profile to source the db2profile. Add the following lines to end of the /root/.bash_profile:

   ```
   if [ -f /home/db2inst1/sqllib/db2profile ]; then
   . /home/db2inst1/sqllib/db2profile
   fi
   ```

   where db2inst1 is replaced by the DB2 instance owner used to install the software.

Disabling other Web servers

If other Web servers are running on your system, you will have a port conflict with IBM HTTP Server. Both Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the other Web server.

To determine whether or not Apache Web Server is enabled, complete the following steps:

1. Click **Application → Server Settings → Services**.
2. In the **Currently Running in Runlevel** column, scroll down and verify that **httpd** is not checked.
3. Click **httpd** to highlight it.
4. Verify that the **Status** windows says **httpd** is stopped. Verify that **httpd** is still not checked.

Disabling firewall products

Before you start the Lotus Expeditor Server installation program, it is recommended that you disable any firewall products that are running. The Lotus Expeditor Server installation and configuration program will attempt to access local TCP/IP resources, such as the local Web server. No external resources will be accessed. If the firewall denies the access attempts made by the installation and configuration program, the installation will fail. After configuration completes, you may re-enable the firewall.

Install the Mozilla browser

Download and install the Mozilla Web browser so that you can use the launchpad application on the product disc and the Firststeps application. If you do not have the Mozilla browser, download and install the browser from http://www.mozilla.org/products/mozilla1.x/.

Note: You might need to start the Mozilla browser from directories other than the one where you have installed Mozilla, so make sure Mozilla is in the path.

After you install the Mozilla browser, export the location of the Mozilla browser using a command that identifies the actual location of the browser. For example, if the Mozilla package is in the `/opt/bin/mozilla` directory, use the following command:

```
export BROWSER=/opt/bin/mozilla
```

Installation and configuration checklist

This topic provides a checklist that you can use to plan and store information that is required for the Lotus Expeditor Server installation and configuration process.

Print the checklist and use it to help you prepare for installing Lotus Expeditor Server. After you have completed the information in this checklist, see "Installation procedures and scenarios" on page 36.

Checklist for single server installation or a single server with a remote database

System preparation

____ Verify that your system meets the hardware and software requirements. For more information see, Hardware and software requirements.

____ Verify that your operating system meets the following requirements. For more information, see Preparing a Windows operating system or "Preparing a Red Hat Linux operating system" on page 28 for instructions.

- ____ Verify the network setup
- ____ Verify the access rights for the user ID used to log on to the system
- ____ Windows only: Disable Microsoft Internet Information Services (IIS)
- ____ Disable any firewall products

____ Verify that you are logged on as a local administrator on Windows or with root authority on Linux.

Record the following information:

Host name of the system where you want to install Lotus Expeditor Server:_____

DB2 preparation

To prepare for your DB2 installation, you need to decide whether you require a remote database.

Note: If you plan to cluster now or in the future, the answer must be yes or you must reinstall when you decide to cluster.

If you do not require a remote database:

____ Install the DB2 server, unless you plan to use an existing installation of DB2. The database server must be installed on the same system as Lotus Expeditor Server. For information about which versions are supported, see Hardware and software requirements.

Record the following information:

Database administrative ID:_____

Database administrative password:_____

If you do require a remote database:

____ Install the DB2 server, unless you plan to use an existing installation of DB2. The database server must be installed on a separate system from the system where Lotus Expeditor Server will be installed. For information about which versions are supported, see Hardware and software requirements.

____ Install the DB2 client on the systems where you will install Lotus Expeditor Server.

Record the following information:

Database administrative ID:_____

Database administrative password:_____

Database server host name:_____

Database server port number:_____

WebSphere Application Server and IBM HTTP Server preparation

____ Ensure that you have configured WebSphere Application Server with the correct hostname.

1. Open a command prompt and switch to the *profile_root*/bin directory.
2. Start **wsadmin** using the following command:
   Windows: wsadmin.bat
   Linux: ./wsadmin.sh
3. Enter the following commands at the **wsadmin** prompt to display the configured host name:
   ```
   wsadmin>set ns [$AdminConfig getid /Node:[$AdminControl getNode]/]
   wsadmin>$AdminConfig showAttribute $ns hostName
   ```
   If the response to the last command is not the fully-qualified host name, check that you have the host name configured correctly on the operating system and recreate the profile using the **wasprofile** command. See the WebSphere Application Server information center for information on the **wasprofile** command.
4. Enter exit to exit **wsadmin**:
   ```
   wsadmin>exit
   ```

____ Install WebSphere Application Server 6.0.2 with a minimum of fix pack 11 on the system where you have installed Lotus Expeditor Server. Create an Application Server profile.

Note: When you create an Application Server profile in a Windows environment, it is recommended not to select to have a Windows service automatically created.

____ Ensure that you have created a WebSphere Application Server profile and have not enabled WebSphere global security. You should be able to log in to the **Administrative** console without specifying a user ID and password.

____ Install IBM HTTP Server on the system where you will install Lotus Expeditor Server.

Note: IBM HTTP Server is only required on the same system as Lotus Expeditor Server for a single server or primary server installation.

____ Install and configure the Web server plug-in.

____ Verify that the IBM HTTP Server and Web server plug-in are operational by completing the following steps:

1. Use a browser on a remote system to access the Lotus Expeditor Server fully-qualified hostname.
2. Verify that the IBM HTTP Server Welcome Page is displayed. If the IBM HTTP Server Welcome Page is not displayed, verify that the HTTP server is running and validate your network connectivity.

____ Verify the WebSphere Application Server Web Server plug-in is installed and configured to run on port 80.

Note: If the server is configured correctly, you should be able to access the Snoop servlet from a remote browser without having to specify a port number. For example, you can enter `http://`*`expeditor_server_hostname`*`/snoop` in your browser and the Snoop Servlet sample application is displayed. (where *`expeditor_server_hostname`* represents the host name of your Lotus Expeditor Server.)

____ Verify that no other WebSphere applications reside on the local node. Lotus Expeditor Server configures global security and the user registry for the local node (in the profile specified). This might impact any existing applications configured for this node.

____ Verify that the local node is not a member of a WebSphere managed node.

Note: If you are installing with a remote database, you can only add the local node to a WebSphere cell after the Lotus Expeditor Server installation completes.

For the profile where Lotus Expeditor Server will be installed, record the following information:

Note: See "Determining WebSphere Application Server configuration" on page 35 for instructions on how to determine these values.

WebSphere Application Server profile name: _____

WebSphere Application Server node name:_____

WebSphere Application Server cell name:_____

File system location information

Record the following file system location information so that you can enter the information in the Lotus Expeditor Server installation program prompts.

File System location where DB2 is installed:_____

File System location where WebSphere Application Server is installed:_____

File System location where IBM HTTP Server is installed:_____

File System location where you want to install Lotus Expeditor Server:_____

Checklist for additional systems in a Lotus Expeditor Server cluster

System preparation

____ Verify that your system meets the hardware and software requirements. For more information see, Hardware and software requirements.

____ Verify that your operating system meets the following requirements. For more information, see Preparing a Windows operating system or "Preparing a Red Hat Linux operating system" on page 28 for instructions.

____ Verify the network setup

____ Verify the access rights for the user ID used to log on to the system

____ Windows only: Disable Microsoft Internet Information Services (IIS)

____ Disable any firewall products

____ Verify that you are logged on as a local administrator on Windows or with root authority on Linux.

Record the following information:

Host name of the system where you want to install Lotus Expeditor Server:_____

DB2 preparation

____ Install the DB2 client on the systems where you plan to install Lotus Expeditor Server.

WebSphere Application Server and IBM HTTP Server preparation

____ Install WebSphere Application Server Network Deployment 6.0.2 with a minimum of fix pack 11 on a system to be used for the Deployment Manager. Create a Deployment Manager profile. You can use an existing network Deployment Manager profile as long as the security configuration matches that of the Lotus Expeditor Server unmanaged node.

____ Verify that you have disabled security for Deployment Manager or that you will configure the security to an LDAP supported by Lotus Expeditor Server. For more information on supported LDAP servers, see Hardware and software requirements.

____ The WebSphere Application Server profile used for Lotus Expeditor Server on the additional system must be configured to satisfy one of the following options:

- Security is not configured for the WebSphere Profile and the profile is for an unmanaged node.
- The profile is configured with a managed node that is part of a cell managed by Deployment Manager. Security is configured to an LDAP supported by Lotus Expeditor Server and used by the primary Lotus Expeditor Server system. For more information on supported LDAP servers, see Hardware and software requirements.

____ (Optional) Install IBM HTTP Server on the additional systems where additional Lotus Expeditor Servers will be installed.

Note: IBM HTTP Server is only required on the local system for the initial install of Lotus Expeditor Server. The Web server can later be moved to a remote system.

____ Install and configure the Web server plug-in on each system where you installed IBM HTTP Server.

____ If you have IBM HTTP Server installed, verify that the IBM HTTP Server and Web server plug-in are operational on each system by completing the following steps:

1. Use a browser on a remote system to access the Lotus Expeditor Server fully-qualified host name.
2. Verify that the IBM HTTP Server Welcome Page is displayed. If the IBM HTTP Server Welcome Page is not displayed, verify that the HTTP server is running and validate your network connectivity.

____ Verify the WebSphere Application Server Web Server plug-in is installed and configured to run on port 80.

Note: If the server is configured correctly, you should be able to access the Snoop servlet from a remote browser without having to specify a port number. For example, you can enter `http://expeditor_server_hostname/snoop` in your browser and the Snoop Servlet sample application is displayed. (Where *expeditor_server_hostname* represents the host name of your Lotus Expeditor Server.)

For the profile where Lotus Expeditor Server will be installed, record the following information:

Note: See "Determining WebSphere Application Server configuration" for instructions on how to determine these values.

WebSphere Application Server node name:_____

WebSphere Application Server cell name:_____

File system location information

Record the following file system location information so that you can enter the information in the Lotus Expeditor Server installation program prompts.

File System location where DB2 is installed:_____

File System location where WebSphere Application Server is installed:_____

File System location where IBM HTTP Server is installed:_____

File System location where you want to install Lotus Expeditor Server:_____

Determining WebSphere Application Server configuration

The installation of Lotus Expeditor Server requires information about the WebSphere Application Server environment.

The following describes information about the WebSphere Application Server environment required to install Lotus Expeditor Server successfully, and how to obtain the information.

- **Deployment Manager SOAP port** - Used when configuring the initial Expeditor Server for a cell environment. To determine the SOAP port follow these steps:
  1. Log in to the **Deployment Manager** console.
  2. Select **System Administration → Deployment Manager**.
  3. Under **Additional Properties**, expand **Ports**.

     The value for the SOAP port is listed as **SOAP_CONNECTOR_ADDRESS**.
- **Profile name** - Identifies the instance of WebSphere Application Server where Lotus Expeditor Server will be installed. The profile must be created before Lotus Expeditor Server installation is started. To obtain a list of profile names:
  1. Open a command window and change to the *was_home*`/bin` directory.
  2. Issue the following command to display the list of profiles:
     - **(Linux)** `./wasprofile.sh -listProfiles`
     - **(Windows)** `wasprofile.bat -listProfiles`
- **Cell name** - Identifies the WebSphere Application Server administration cell for installation of Lotus Expeditor Server.

  Note: The user admin ID and password are only required if you have enabled security for Lotus Expeditor Server.

To obtain the cell name:

1. Open a command window and switch to the *profile_home*/bin directory.
2. Issue the following command to display the cell name:
   - **(Linux)** - ./wsadmin.sh -c '$AdminControl getCell' -user *admin_id* -password *admin_password*
   - **(Windows)** - wsadmin.bat -c "$AdminControl getCell" -user *admin_id* -password *admin_password*

- **Node name** - Identifies the node where Lotus Expeditor Server will be installed.

  Note: The user admin ID and password are only required if you have enabled security for Lotus Expeditor Server.

  To obtain the node name:

  1. Open a command window and switch to the *profile_home*/bin directory.
  2. Issue the following command to display the node name:
     - **(Linux)** ./wsadmin.sh -c '$AdminControl getNode' -user *admin_id* -password *admin_password*
     - **(Windows)** wsadmin.bat -c "$AdminControl getNode" -user *admin_id* -password *admin_password*

Installation procedures and scenarios

This topic includes the procedures and scenarios for Lotus Expeditor Server 6.1. Each scenario details what software must be configured and running to successfully complete the install.

Important: All of the procedures and scenarios assume that you have installed the necessary prerequisites and intend to complete the installation in one attempt by completing the information on each panel and continuing to the next panel. If errors occur during the installation of Lotus Expeditor Server, see Troubleshooting Lotus Expeditor Server in this information center. At any point during the installation, you can select **Back** to return to the previous panel or select **Cancel** to abort the installation. See Hardware and Software requirements for information about the prerequisites.

There are four scenarios for installing Lotus Expeditor Server:

- "Single system install with local database"
- "Single system install with remote database"
- "Creating a cluster" on page 37
- "Adding additional servers " on page 37

Single system install with local database

For a single system install, select **local database** from the options offered during the Lotus Expeditor Server installation. As a result of this selection, all of the server components and databases are installed and configured on a single system. This scenario is intended for developer or proof-of-concept installs. If you choose this install scenario, you will not be able to cluster the Lotus Expeditor Server. For the initial install, the default user registry for Lotus Expeditor Server is an internal, custom user registry shipped with Lotus Expeditor Server that uses a DB2 database as the data store. If you plan to use an LDAP directory, follow the instructions in "Upgrading to an LDAP user registry" on page 96. For instructions on installing a single system with a local database, see "Installing a single server" on page 38.

Single system install with remote database

To use a remote database, select **remote database** from the options offered during the Lotus Expeditor Server installation. As a result of this selection, all the server components are installed on a single system and the databases are configured on a separate system.

Note: The databases must be manually created before installing the server.

Lotus Expeditor Server offers flexibility to grow from one single server to multiple systems. You must choose this option if you plan to grow your production environment from one single system to multiple physical systems. You can use the default user registry provided with Lotus Expeditor Server for this scenario also. To use an LDAP user registry, follow the instructions in "Upgrading to an LDAP user registry" on page 96. For instructions on installing a single system with a remote database, see "Installing a single server" on page 38.

Creating a cluster

You can configure Lotus Expeditor Server to allow it to be scaled across multiple server systems. If you plan to install Lotus Expeditor Server on multiple systems, you must create a cluster on a single system installed with a remote database and configured for an LDAP user registry. This requires WebSphere Application Server Network Deployment Edition. During the cluster creation, the Lotus Expeditor Server node will be added to the Deployment Manager cell. After the cluster is created, a response file is generated that will be used when adding additional Lotus Expeditor Servers to the cluster. WebSphere MQ Everyplace is not clustered because it is not an application server. To share MQe queues among multiple servers, you need to create the queues on media that is accessible from all systems (for example, shared DASD). For instructions on setting up an initial cluster, see "Creating a cluster" on page 41.

Adding additional servers

In a high volume production environment, you might find it necessary to add additional Lotus Expeditor Servers to increase capacity or provide high availability for Lotus Expeditor Server services. After you have created the cluster from an initial installation, you can add additional Lotus Expeditor Server systems to the cluster. For instructions on how to add servers to your scaled environment, see "Adding an additional server" on page 43.

Review the following procedures for installing Lotus Expeditor Server.

Creating the databases (optional)

This topic describes how to create the Lotus Expeditor Server databases needed for a remote database environment.

These steps only have to be performed if you plan to use an environment which requires a remote database. See "Creating the databases (optional)"for information on environments which require a remote database.

1. Log in as DB2 Administrator on Windows system or if you're using a Linux system, switch to the DB2 instance using `su - db2inst1`, for instance.
2. Ensure that DB2 starts on the database system.
3. On the database server system, insert the product installation CD.

   Note: You might need to manually mount the product installation CD on Linux.
   If the Launchpad starts, click **Exit** to close it.
4. Open a command window using the following:
   - (Windows) Open a command window.
   - (Linux) Open an XTERM window or console.
5. In the DB2 command window, change the directory to \scripts\remotedb (Windows) or /scripts/remotedb (for Linux) on the product CD.
6. If the Lotus Expeditor Server databases exist from a previous installation, you will need to drop them before you create new databases. Run the following command to drop the existing databases:
   - **(Windows)** `dropDBs.bat`

- **(Linux)** `./dropDBs.sh`

7. Run the following command to create the databases:
   - **(Windows)** `createDBs.bat` *database_admin_id database_admin_password*
   - **(Linux)** `./createDBs.sh` *database_admin_id database_admin_password*

   Note: You can copy the script from the CD and run it locally if the script needs to be modified. If you want to create databases in different or separate drive(s) or file systems, you can change the property values in the script to one of the following: `DEFAULT_DRIVE`, `DEFAULT_WMM_DRIVE`, `DEFAULT_DB2E_DRIVE`, and `DEFAULT_DMS_DRIVE`.
8. Verify that there are no error messages in the command window.

Installing a single server

This topic describes how to install a single Lotus Expeditor Server.

Based on which operating system you currently own, use the following procedures for instructions on installing Lotus Expeditor Server on a single server. The following instructions include instructions for a Windows or Linux operating system.

Important: These steps assume that you have installed the necessary prerequisites and intend to complete the installation in one attempt by completing the information on each panel and continuing to the next panel. At any point during the installation, you can select **Back** to return to the previous panel or select **Cancel** to abort the installation. See Hardware and Software requirements for information about the prerequisites and "Installation requirements" on page 25 for information on preparing your system for the install.

Installing IBM Lotus Expeditor

1. Ensure that IBM HTTP Server and WebSphere Application Server plug-ins have been installed and are functioning properly. Open a Web browser and go to the following URL, http://hostname:port/snoop, where hostname:port is the host name of the system where you will install the Lotus Expeditor Server and port is the web server HTTP port. Note that server1 must be started before performing this test. You should see a Web page containing information about your Web browser client.
2. **(Windows)** Log in as an administrator user in the local server domain (not part of a Windows domain).
3. Insert the Lotus Expeditor Server CD in the CD drive.

   Note: You might need to manually mount the product installation CD on Linux.
4. Open a command window, change to the root directory on the CD and enter the following command to start the installation:
   - **(Windows)**`launchpad.exe`
   - **(Linux)** `./launchpad.sh`
5. Select **Install IBM Lotus Expeditor**.
6. Under **Install IBM Lotus Expeditor**, select **Launch the installation wizard for Lotus Expeditor Server**.

   Notes:
   a. InstallShield does not accept bi-directional characters as input.
   b. If you are installing from a network drive, there might be a delay before the installation program starts.
7. Review the text on the **Welcome** panel and click **Next**. The Lotus Expeditor Server installation program completes the following actions:

- Verifies that Lotus Expeditor Server supports the operating system that resides on your system.
- Verifies that you have enough memory and disk space to support the Lotus Expeditor Server installation.
- Verifies that you do not have a previous version of any of the Lotus Expeditor Server components installed on your system.

If your system passes the verifications check described, the **License** panel is displayed.

8. Review the terms of the license and select "**I accept the terms of the license agreement**" if you agree to the terms and click **Next**.

   Note: If you select "**I do not accept the terms of the license agreement**", the installation program prevents you from continuing any further.

   If you accepted the terms of the license, the **Prerequisite Software** panel is displayed.
9. Specify the directories where DB2, IBM HTTP Server, and IBM WebSphere Application Server are installed or accept the default directories listed, and click **Next**.
10. Specify the WebSphere Application Server profile name, cell name and node name into which your Lotus Expeditor Server will be configured, if necessary. The installation program supplies default values. If you want to use a different profile than the profile selected by the installation program, you need to update the profile name and the corresponding cell name and node name before continuing. After you specify a value for each field, click **Next**.

    Notes:

    a. See "Determining WebSphere Application Server configuration" on page 35 for more information on determining the profile name, cell name and node name.
    b. The installation program verifies you have the prerequisite software installed at a version level that Lotus Expeditor Server supports.
    c. The installation program also verifies that WebSphere security is not currently enabled and the node is unmanaged.

    The Lotus Expeditor Server **Host Information** panel is displayed.
11. Complete the following fields on the Lotus Expeditor Server **Host Information** panel:
    - **Host name:** Specify the fully-qualified host name of the system where you are installing Lotus Expeditor Server. This value must be a fully-qualified name registered with your Domain Name System (DNS). You cannot specify an IP address instead of a host name.
    - **Create Lotus Expeditor Server Administrator ID**: Specify the administrator user ID you want to give to your Lotus Expeditor Server administrator. Your administrator user ID does not have to be the Windows login user. Lotus Expeditor Server will create the administrator ID in the local user registry during the installation.

      Lotus Expeditor Server has limitations for the **Create Lotus Expeditor Server Administrator ID**. See "Supported naming conventions" on page 20 for information on restrictions on administrator ids.
    - **Create Lotus Expeditor Server Administrator Password**: Specify the password you want your Lotus Expeditor Server administrator to use. See "Supported naming conventions" on page 20 for information on restrictions on administrator password.
    - **Confirm Lotus Expeditor Server Administrator Password**: Retype the password you specified in the previous step.
12. Click **Next**. The **Database Location** panel is displayed.

    Note: If you are not the Lotus Expeditor Server administrator, provide the administrator with the administrator user ID and password.
13. On the **Database Location** panel, select the location of the Lotus Expeditor Client databases. To use a local database server installed on this system, select **Local**. To use a database server on another system, select **Remote**.

Important: If you plan to cluster Lotus Expeditor Server at a later time, you must select **Remote**. Clustering Lotus Expeditor Server requires a remote database and you cannot reconfigure Lotus Expeditor Server to use a remote database after the install.

14. Click **Next**. The **Database Login** panel is displayed.
15. If you are using a local database, complete the following fields on the Lotus Expeditor Server **Database Login** panel:
    - **Database Administrator ID**: Specify the administrator user ID configured for the database server.
    - **Database Administrator Password**: Specify the password used for the database administrator id.

    Complete the following fields if you are using a remote database:
    - **Host name**: Specify the fully-qualified host name of the system where the database server is installed. This value must be a full-qualified name registered with your Domain Name System (DNS). You cannot specify an IP address instead of a host name.
    - **Port number**: Specify the database port number. The default port number for DB2 is 50000.

    Note: The installation program verifies that this administrator user ID already exists. You will not be able to proceed until you enter a valid database administrator user ID and password. If you specified **Remote** for the database location, the product databases must already exist. See "Creating the databases (optional)" on page 37 for information on creating databases on the remote database server.
16. Click **Next**. The database information is validated. There may be a delay when validating a remote database. The **Installation Location** panel is displayed next.
17. On the Lotus Expeditor Server **Installation Location** panel, specify the location where you want to install Lotus Expeditor Server. You can type the directory location in the field or go to the location by selecting **Browse** and navigating to a directory. Click **Next**.

    Note: See "Supported naming conventions" on page 20 for information on restrictions for the installation directory.
18. Click **Next**. The **Installation Summary** panel is displayed.
19. (Optional) If you need to apply updates to the files already installed, click on the check box to pause between the end of the installation process and the beginning of the configuration process. Follow the update instructions to apply any required fixes. Then, click **Next** to continue with the configuration.
20. Verify that the information on the **Installation Summary** panel is correct and click **Next**.

    Note: Installing Lotus Expeditor Server is a two phase process. During the installation phase, the installation program copies files to your local system. In the configuration phase, the installation program creates databases and Web applications.

    After the installation program completes, Lotus Expeditor Server launches the **Configuration Wizard**.

    Tip: If you encounter an error during the configuration phase, see Troubleshooting in this information center.
21. On the final configuration panel, click **Finish** to complete the configuration. See "Verifying the installation" to ensure you have properly installed Lotus Expeditor Server.
22. See "Using the First Steps console" on page 46 to get started using the product.

Verifying the installation

1. To verify your installation, launch the **First Steps** console.
2. Select **Verify Install** from the **First Steps** panel.
3. Verify that you receive the message, **CWPSF1535I Verification of Lotus Expeditor Server Completed SUCCESSFULLY** is issued at the end of the verification.

Creating a cluster

This topic describes how to cluster a single Lotus Expeditor Server.

Prerequisite setup

The following steps must be performed before proceeding with clustering Lotus Expeditor Server:

Note: If you have already clustered Lotus Expeditor Server and need to add an additional server, see "Adding an additional server" on page 43.

1. Ensure that Lotus Expeditor Server has been installed and configured on a single system with a remote database. See "Installing a single server" on page 38 for more information about installed and configured Lotus Expeditor Server on a single system with remote databases.

   Note: It is important that you install Lotus Expeditor Server with a remote database. You cannot cluster a server that is using a local database. Verify that the single server is working before continuing.
2. Upgrade the Lotus Expeditor Server to use an LDAP server for the user registry. See "Updating the configuration" on page 92 for information on configuring Lotus Expeditor Server to use an LDAP server.
3. Install and configure a WebSphere Application Server Deployment Manager node. This step is optional if you are adding Lotus Expeditor Server to an existing cell. See the WebSphere Application Server Network Deployment Infocenter for information on installing and configuring a Deployment Manager node.

   Note: If you enable **Security** on the Deployment Manager node, it must match the security settings for the Lotus Expeditor Server single system installation.
4. Change the time-out request for the Simple Object Access Protocol (SOAP) client. Edit the file *was_home*/profiles/profile_name/properties/soap.client.props and change the **com.ibm.SOAP.requestTimeout** value to `6000`. Ensure there is no whitespace following `com.ibm.SOAP.requestTimeout=6000`.

   Note: This needs to be done on both the Lotus Expeditor Server node and the Deployment Manager node before you start the clustering process.

Configuring the Lotus Expeditor Server as a managed node

The following section provides instructions on how to configure a Lotus Expeditor Server as a managed node.

Caution: Do not attempt to manually add the Expeditor Server node to a Deployment Manager cell.

Pre-install steps

1. Start with a remote database installation of Lotus Expeditor Server. See "Installing a single server" on page 38, beginning at step 13.
2. Upgrade to LDAP. See "Upgrading to an LDAP user registry" on page 96.
3. Use the WebSphere Application Server **backupconfig** command to create a backup of the default profile config tree. You may need this to recover definitions lost when joining the server to the cell.
4. Install WebSphere Application Server Network Deployment edition 6.0.2 with a minimum of fix pack 11 applied on the Network Deployment system. The server that will contain the deployment manager must be at the same or higher fix pack level than the Lotus Expeditor Server systems.
5. Create profile for WebSphere Application Server Deployment Manager on the Network Deployment system. See the Creating and deleting profiles topic in the in the WebSphere Application Server Network Deployment Infocenter.

Note: You do not need to complete this step if a profile already exists.

6. Ensure that system clocks on the Lotus Expeditor Server system and WebSphere Application Server Network Deployment system are syncronized within 5 minutes of each other.
7. Start the Deployment Manager on the Network Deployment system. If you have enabled security on the Deployment Manager node, ensure that the settings remain consistent with the settings used on the Lotus Expeditor Server node.
8. Ensure that the Lotus Expeditor Server node can ping the Network Deployment system by short name only. Otherwise, adding the Lotus Expeditor Server node to the Network Deployment cell results in failure during the clustering process.
9. Ensure that the Deployment Manager system can ping the fully-qualified host name of the Lotus Expeditor Server.
10. If you are installing on Linux, create a group on the Linux server and add the DB2 instance user (for example, db2inst1) and the root user as members of the group. You are prompted to enter this group name during the configuration process.

Configuration steps

1. Launch the **First Steps** console. See "Using the First Steps console" on page 46.
2. Launch the configurator from the **First Steps** console.
3. Click **Next** at the **Welcome** panel.
4. Select **Advanced Clustering Services** and click **Next**.
5. Select **Configure Node for Cell Environment** and click **Next**.
6. Enter **WebSphere Deployment Manager Hostname** and **Port** (SOAP Port, generally 8879) and click **Next**. The WebSphere Deployment Manager information will be validated.

   Note: To determine the SOAP port used by the deployment manager, see "Determining WebSphere Application Server configuration" on page 35.
7. On Linux systems only: Enter the name of the group containing the DB2 instance user and the root user and click **Next**.
8. The Summary panel is displayed. Click **Next** to start the configuration.
9. Click **Next** to start the configuration.
10. Restart the Deployment Manager if prompted to do so. You will be prompted to restart if the Deployment Manager node was not already configured for security. To restart the Deployment Manager, run the following commands on the deployment manager system:
    a. Open a command window and change directory to dmgr_profile_root /bin.
    b. Run the following command:

       Windows: **stopManager.bat**

       Linux: **./stopManager.sh**
    c. Run the following command:

       Windows: **startManager.bat**

       Linux: **./startManager.sh**
11. After the Deployment Manager is restarted, click **OK** to continue the configuration.
12. At the **Configuration Successful Summary** panel, select **Next** to return to the configuration options.
13. Select **Advanced Clustering Options** and click **Next**.
14. Select **Create Cluster** and click **Next**.
15. The **Summary** panel is displayed.

A response file also is created that can be used for installing additional Lotus Expeditor Servers in the cluster.

Verifying the cluster

1. Start **First Steps**. See "Using the First Steps console" on page 46.
2. Click **Installation verification** to validate that the servers have started.
3. Log in to the **Network Deployment Administration** console using the Lotus Expeditor Server admin ID and password.
4. Select **Servers** then **Clusters** and verify the following clusters exist:
   - coreServicesCluster
   - IBMDB2eServerCluster
   - DMS_AppServerCluster

To add additional servers to the cluster, see "Adding an additional server."

Adding an additional server

This topic describes how to add additional Lotus Expeditor Servers to an existing Lotus Expeditor Server cluster.

Prerequisite setup

You must complete the following requirements prior to adding an additional Lotus Expeditor Server.

- You must create an Lotus Expeditor Server cluster. See "Creating a cluster" on page 41 for more information on creating an Lotus Expeditor Server cluster.
- Install the Lotus Expeditor Server prerequisite software on the system, which will contain the additional Lotus Expeditor Server. If you are installing Lotus Expeditor Server on an existing server, verify that it meets the software prerequisites. Refer to "Supported hardware and software" on page 14 for information about the prerequisites and "Installation requirements" on page 25 for information on preparing your system for the install.
- Change the time-out request for the Simple Object Access Protocol (SOAP) client . Edit the file *was_home*/profiles/profile_name/properties/ directory/soap.client.props and change the **com.ibm.SOAP.requestTimeout value** to `6000`. Ensure there is no whitespace following `com.ibm.SOAP.requestTimeout=6000`.
- If you are utilizing the services of the DB2 Everyplace Synchronization Server, you must catalog any source and mirror databases associated with DB2 Everyplace JDBC Subscription definitions ***before*** you add the additional Expeditor Server on this server. When the installation process has completed, this server is available to service client synchronization requests. If the databases are not cataloged, synchronization requests fail.

Install and configure the additional server

1. Ensure that core services is running on the primary node. DB2 Everyplace server configuration will fail without it. Check that you can access http://*webserverhost*/UserGroupInfoWebService/servlet/rpcrouter. If not, you may need to regenerate the plug-in and restart IHS on the primary node.
2. Copy the cluster.rsp file from the primary node to the secondary node. You may generate a new response file by running the Configuration Wizard on the primary node and selecting the **Advanced Clustering Services → Create a Cluster reponse file** option.
3. Start the launch pad application on the installation CD.
4. Select **Install Lotus Expeditor Server**.
5. Under **Install Lotus Expeditor on an additional server**, click **Launch the installation wizard for Lotus Expeditor Server**.
6. Click **Next** at the Welcome panel.
7. Accept the license agreement and click **Next**.
8. On the prerequisite installation panel, fill in the installation directories for the prereqs and click **Next**.
9. Enter the location of the response file copied from the primary node and click **Next**.

10. Enter the Expeditor administrator and database passwords and click **Next**.
11. Specify the **hostname**, **WAS profile name**, and **WAS node name** , and click **Next**.
12. Enter the **Lotus Expeditor installation directory** and click **Next**.
13. The summary panel is displayed. Click **Next** to start the installation.

Important:

- You will get a popup during the configuration that states you must regenerate and propagate the Web server plugin. Use the WebSphere Administration console to regenerate and propagate the Web server plugin. Then restart IBM HTTP Server before clicking OK.
- After the server installation completes, perform any setup that may be needed for applications you installed on other nodes in the cluster, such as cataloging databases.

Verify the additional server and cluster

1. Start **First Steps**. See "Using the First Steps console" on page 46.
2. Click **Verify Install** to validate that the servers have started.
3. Log in to the **Network Deployment Administration** console using the Lotus Expeditor Server **admin ID** and **password**.
4. Select **Servers** then **Cluster Topology**.
5. Expand the following clusters and verify that the new Lotus Expeditor Server node is listed under **Nodes** along with the following:
   - coreServicesCluster
   - IBMDB2eServerCluster
   - DMS_AppServerCluster

Installing IBM Tivoli License Compliance Manager

This topic provides information about the IBM Tivoli License Compliance Manager.

What is IBM Tivoli License Compliance Manager?

IBM Tivoli License Compliance Manager 2.2 monitors license compliance for sub-capacity and capacity-on-demand pricing options. Basically, it recognizes and monitors what product offerings and their versions, releases, fix packs are installed and used on a system. That allows IBM to communicate updates for products installed in its customer base, and appropriately bill for the product and the amount of usage. It also prevents billing for multiple installations of the same product that is bundled with various IBM software packages.

How IBM Tivoli License Compliance Manager works

The product that enables IBM Tivoli License Compliance Manager works in conjunction with it. A product like Lotus Expeditor that enables IBM Tivoli License Compliance Manager chooses one or more executables that appear on the system when the product is running, and submits the names of those executables (called usage signatures) to IBM Tivoli License Compliance Manager. This happens before a product release. Those signatures predefine its product offering to IBM Tivoli Compliance License Manager. Lotus Expeditor Server installs its inventory signature file in the TIVREADY subdirectory of one of the enterprise applications deployed with Lotus Expeditor. Then, after installed and activated, IBM Tivoli License Compliance Manager recognizes the product offering's signature as it looks for one or more predefined product processes when determining whether the product offering is installed and running. IBM Tivoli License Compliance Manager also identifies the product offering's version, release, and fix pack levels.

When IBM Tivoli License Compliance Manager recognizes a product offering, it allows you to take advantage of IBM's pricing options and product update notifications.

What is required

1. Install the Lotus Expeditor Server 6.1 or higher product.
2. Follow these directions for installing and enabling IBM Tivoli License Compliance Manager 2.2 agent.

Enabling IBM Tivoli License Compliance Manager

IBM Tivoli License Compliance Manager monitors license compliance. Basically, it recognizes and monitors what product offerings and their versions, releases, and fix packs are installed, and used, on a system.

Before beginning the enabling process, Lotus Expeditor Server 6.1or later must be installed. Lotus Expeditor Server is preset to work with IBM Tivoli License Compliance Manager.

To install and enable IBM Tivoli License Compliance Manager, you must:

1. Download the IBM Tivoli License Compliance Manager 2.2 agent and install it on each system that requires it. Instructions for downloading the IBM Tivoli License Compliance Manager agent, prerequisites and licensing process are documented on the Passport Advantage® Web site.
2. Download and install Fix Pack 1 for IBM Tivoli License Compliance Manager 2.2. Link to this software support site to begin the download process.
3. Security must be enabled to continue with these steps. Lotus Expeditor runs with WebSphere Application Server Security enabled. Credentials must supplied to IBM Tivoli License Manager to allow the monitoring of Lotus Expeditor Server usage. Credentials can be provided to IBM Tivoli License Manager as follows. First find the IBM Tivoli License Manager install directory for your operating system:
   - **Windows**: C:\WINNT\itlm\wasagent
   - **UNIX**: /var/itlm/wasagent
4. Next, complete each of these steps:
   a. Run **WASAgentClient.{bat|sh}**
   b. Type `servers` on the **WASAgentClient** console to list all the application server IDs and the profile where each resides.
   c. From this list, locate the ID for the application server named **coreServices**.
   d. Provide credentials for this server by typing:

      `credentials id userid password`

      where `id` is the server ID of the coreServices application server, `userid` and `password` are for the Lotus Expeditor administrator.

      Note: Whenever the IBM Tivoli License Compliance Manager agent is stopped, then **WASAgentClient.{bat|sh}** must be run again and the credentials must be reissued.
5. To complete the enablement of the IBM Tivoli License Compliance Manager licensing feature for Lotus Expeditor Server 6.1, follow the IBM Tivoli License Compliance Manager instructions provided with your customer agreement.
6. **Optional**: To troubleshoot problems encountered during enabling, check the following:
   a. Ensure that the correct inventory signature file exists in the directory path indicated in the table below.

Note: The required signature file is available on its product installation CD.

Table 1. Product signature files		
Product offering / Component name	**IBM Tivoli License Manager signature file**	**Signature file's directory path**
IBM Lotus Expeditor Server 6.1	COREUGI0601.sys2	**Note:** This signature file is placed in the EAR directory during installation. • **Windows**: `C:\`*`WebSphere profile path \profile name`*`\installedApps\`*`nodename`*`\UserGroupInfoWebService.ear\TIVREADY` • **UNIX:** */`*`WebSphere Profile Path`*`/`*`profile name`*`/installedApps/`*`nodename`*`/UserGroupInfoWebService.ear/TIVREADY`

b. From the WASAgentClient prompt, run the **servers** command. Verify that for the coreServices application server, the status appears as **MANAGED PRODUCT**. If the status shows as **UNMANAGED PRODUCT**, then the credentials must supplied.

IBM Tivoli License Compliance Manager is now installed and enabled.

Using the First Steps console

The First Steps console provides a launching point from which you can access IBM Lotus Expeditor Server features. This topic describes the options available on the First Steps console.

After installation, you can open the **First Steps** window by one of the following ways:

- Select **Start** → **All Programs** → **Lotus Expeditor** → **First Steps**
  OR
- Run *`expeditor_home`* `\FirstSteps\firststeps.bat/sh`.
  Where *`expeditor_home`* represents the directory where you installed IBM Lotus Expeditor Server.

First Steps provides the following options:

Start and Stop Lotus Expeditor Server

IBM Lotus Expeditor Server is installed and configured with three Web application servers. Before you access the User Management console or using software management or database synchronization services, you must start these application servers. The Lotus Expeditor Server configuration wizard will automatically handle stopping and starting the servers as necessary for any reconfiguration steps.

Note: In a cluster environment, this option will only start the servers on the node where you run **First Steps**.

When you launch the First Steps application, only the **Start Lotus Expeditor Server** will appear, regardless of whether the Lotus Expeditor Server services are already running. After you select the **Start Lotus Expeditor Server** option, an output screen displays with status messages. The success message informs you that the servers have started successfully. Then the menu item changes to **Stop Lotus Expeditor Server**. For Windows, the options to start and stop the Lotus Expeditor Server are available from the start menu.

In a cluster environment, the start/stop server option does not start or stop the node agent running on the system. You need to manually start or stop the node agent using the following commands:

- To start the node agent run:
  - **(Windows)** *was_profile_root*/bin/startNode.bat
  - **(Linux)** *was_profile_root*/bin/startNode.sh
- To stop the node agent run:
  - **(Windows)** *was_profile_root*/bin/stopNode.bat -username admin_id -password admin_password
  - **(Linux)** *was_profile_root*/bin/stopNode.sh -username admin_id -password admin_password

If errors occur starting or stopping the Lotus Expeditor Server, see Troubleshooting in this information center.

Verify Installation

This option confirms your server is installed and started properly.

Verify installation messages display in a separate window. When the verification has finished, you will see the following message: ***CWPSF1535I Verification of Lotus Expeditor Server Completed SUCCESSFULLY***

Note: If the verification fails, see the log file displayed in the verification output window to determine the cause of the failure.

Start User Management Console

This option accesses the Lotus Expeditor Server User Management console. You must start Lotus Expeditor Server to be able to use the User Management console. If you upgrade the server configuration to use LDAP as the user registry, the User Management console is disabled. You must use the administration tools associated with the LDAP directory to manage users and groups. For Windows, the User Management Console can be launched from the start menu.

View information center

This option allows you to view this information center and requires an internet connection.

Start Configuration Wizard

This option launches the Configuration Wizard, which enables you to update your configuration to use Active Directory 2003 as your user registry. The Configuration Wizard also enables you to change your Lotus Expeditor Server administrator password, your database administrator password in the server configuration files, or cluster your Lotus Expeditor Server. For Windows, you can also launch the Configuration Wizard from the Windows Start Menu. For detailed information to use the Configuration Wizard, see the topics in "Updating the configuration" on page 92.

Exit

This option closes the First Steps console.

Enabling Client Deployment over the network

This topic describes how to deploy the IBM Lotus Expeditor Client for Desktops and Mobile Devices using a Web server.

The Network Client Installer allows you to deploy the Lotus Expeditor Client from a Web server. The Network Client Installer allows Lotus Expeditor Server users to download and install the Lotus Expeditor Client using a Web browser on the device without requiring access to the Lotus Expeditor Client installation CD. This can be the same Web server used by the Lotus Expeditor Server. See Installing with the Network Client Installer for detailed information on the Network Client Installer.

Uninstalling IBM Lotus Expeditor Server

This topic describes how to uninstall Lotus Expeditor Server from your system.

Lotus Expeditor Server provides an integrated uninstallation program that is similar to the installation program in that removal of configuration and removal of the components are two separate and distinct phases of the uninstallation process. The configuration removal deletes the Lotus Expeditor Server application servers and associated configuration from WebSphere Application Server. If the database server is on the same system as Lotus Expeditor Server, the DB2 server drops the DMS and WMM databases. The component uninstallation removes all component files and registry entries. If the configuration removal is successful, the uninstallation phase launches automatically.

Note the following exceptions:

- The DB2 Everyplace databases are not dropped.
- Log files and other files generated after the initial installation will not be removed.
- Databases on remote database systems are not dropped. These database can be dropped manually after the Lotus Expeditor Server uninstall completes.

Important:

- For a clustered environment, ensure that the Deployment Manager and node agent are started before you start to uninstall the product.
- Ensure that the DB2 server is started before you start to uninstall the product. If the product databases are on a remote system, that database server must be running before starting the product uninstall.
- The uninstallation program removes the configuration before removing all of the components completely. See the following steps to uninstall Lotus Expeditor Server from your system. In a cluster environment, these steps must run on each Lotus Expeditor Server system. The first Lotus Expeditor Server node that was added to the cluster (the primary node) must be uninstalled last. The uninstaller will block the uninstall of the Lotus Expeditor Server primary node until you successfully uninstall all the secondary nodes in the cluster.

Note: At any point during the uninstallation, you can click **Back** to return to the previous panel or click **Cancel** to abort the uninstall program.

Uninstalling Lotus Expeditor Server

1. Start the uninstall program as follows:

   (Windows)

   a. Go to the Windows control panel and double-click on **Add or Remove Programs** to begin the uninstallation.

   b. Select **IBM Lotus Expeditor Server**.

   c. Click **Change / Remove**.

   (Linux)

   a. Run `install_root/Expeditor/_uninst/uninstall.bin`

2. The **Welcome Panel** is displayed.
3. Click **Next**.

4. The uninstall response file is loaded and the database connections will be validated. This may take a few minutes.
5. The **Uninstallation Summary** panel is displayed.
6. Verify the information on the uninstallation summary panel is correct, and click **Next**.

   The configuration removal phase displays progress panels that indicate the level of completeness of the configuration removal.

   When the configuration removal completes, the uninstallation program is automatically launched. The progress panels displayed indicate the level of completeness of the uninstallation phase.
7. Click **Finish** to complete the uninstallation process.

In the event that you uninstalled the Lotus Expeditor Server from a managed environment and performed a WebSphere remove node operation, it is recommended that you delete the current WebSphere profile and create a new one before performing any further modifications to this profile. Creating the new profile ensures that all remnants of the Lotus Expeditor Server configuration are removed. WebSphere provides a command line interface (wasprofile) for managing profiles. In addition, WebSphere provides a wizard for creating a new profile.

Do not remove the profile if there are other applications configured within the profile that cannot easily be reconfigured. To manually clean up the IBM Lotus Expeditor configuration, see Troubleshooting in this information center.

Migrating to Lotus Expeditor Server

This topic provides instructions on migrating from an operational WebSphere Everyplace Deployment 6.0 system to a Lotus Expeditor Server 6.1 system.

Migration overview

This topic provides a general overview of migrating from a WebSphere Everyplace Deployment 6.0 system to Lotus Expeditor Server 6.1.

The migration strategy for moving a WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1 involves installing and configuring a working Lotus Expeditor Server 6.1 system that is parallel to your existing WebSphere Everyplace Deployment 6.0 system and then migrating the desired data from the 6.0 system into the 6.1 system using the tools and documentation provided with the 6.1 system. The WebSphere Everyplace Deployment 6.0 system data will not be modified in any way that would prevent it from working or attempting the WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1 migration again. You can repeat the migration several times if necessary. Repeating allows you the opportunity to test the migration before you complete the final migration to permanently move to the new Lotus Expeditor Server 6.1 system.

You can migrate all components of WebSphere Everyplace Deployment 6.0 with the exception of MQ Everyplace. Migration requires you to redeploy your MQ Everyplace application on the Lotus Expeditor Server 6.1 system. This requires you to recreate any MQ Everyplace queues you created on your WebSphere Everyplace Deployment 6.0 system on your newLotus Expeditor Server 6.1 system.

Similar environments

Migration from a WebSphere Everyplace Deployment 6.0 system to a Lotus Expeditor Server 6.1 system can only occur when the environments for each system are similar. The following lists aspects of each system that must be similar to achieve successful migration:

- Operating system - Since WebSphere Everyplace Deployment 6.0 only supports the Windows 2003 operating system, you can only perform migration from a WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1 on a Windows 2003 operating system. Migration to Linux is not supported.
- User registry - You must use the same user registry for the Lotus Expeditor Server6.1 as you used for the WebSphere Everyplace Deployment 6.0 server.
  - Database user registry - If your current WebSphere Everyplace Deployment 6.0 uses the database user registry, you must still configure your Lotus Expeditor Server 6.1 server with the database user registry to proceed with migration of data.

    Note: You can reconfigure the Lotus Expeditor Server 6.1 system to use an LDAP user registry after you have completed migration.
  - Active Directory 2003 - If your WebSphere Everyplace Deployment 6.0 has been reconfigured to use an Active Directory 2003 LDAP user registry, then the Lotus Expeditor Server 6.1 system must be reconfigured to use the same Active Directory 2003 LDAP user registry before proceeding with migration of data. Migration to a different Active Directory 2003 server or any other LDAP server is not supported.
- Userid and groups - You must use the same userid and groups for the Lotus Expeditor Server 6.1 as you used for the WebSphere Everyplace Deployment 6.0 server to ensure successful migration.
- The Lotus Expeditor Server 6.1 system must not be a member of a Network Deployment cell to proceed with the migration of data.

Migration planning

Review the following information to successfully plan your migration from WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1.

The following sections includes information you need to prepare for migrating to Lotus Expeditor Server 6.1.

Important: You must use the same userid and groups for the Lotus Expeditor Server 6.1 as you used for the WebSphere Everyplace Deployment 6.0 server to ensure successful migration.

Remote Database support

Lotus Expeditor Server 6.1 only supports clustering if it is configured using a remote DB2 server. The previous version of WebSphere Everyplace Deployment 6.0 only supported an environment in which DB2 was installed on the same server as the WebSphere Everyplace Deployment 6.0 product. Note that to migrate from a 6.0 system and then cluster it, you must configure the Lotus Expeditor Server 6.1 environment for a remote DB2 server. You may only cluster your 6.1 system after the final migration is complete.

Unsupported Scenarios

Migration is not supported in the following scenarios:

- In place, same system migration or upgrade.
- Migration from any WebSphere Everyplace Access system.
- Migration to a Lotus Expeditor Server 6.1 system that is configured to a different LDAP server than the WebSphere Everyplace Deployment 6.0 server from which you are migrating.
- Migration to a Lotus Expeditor Server 6.1 system that has been added into a Network Deployment cell.
- Migration to an operating system different than that of the WebSphere Everyplace Deployment 6.0 system.
- Migration from a beta release of IBM Lotus Expeditor Server 6.1.

Migration process

This topic includes the overall process for migrating from WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1.

Use the following instructions to migrate from WebSphere Everyplace Deployment 6.0 to Lotus Expeditor Server 6.1. If your 6.0 system was configured with a local user registry, see “System configured with local user registry” to successfully migrate from 6.0 to 6.1. If your 6.0 system was configured with Active Directory 2003, see “System configured with Microsoft Active Directory 2003” on page 53.

Also, you must use the same userid and groups for the Lotus Expeditor Server 6.1 as you used for the WebSphere Everyplace Deployment 6.0 server to ensure successful migration.

System configured with local user registry

Follow the procedure to migrate a WebSphere Everyplace Deployment 6.0 system that is configured using the database user registry.

1. Install Lotus Expeditor Server 6.1 on a separate system. If clustering is in your future plans, select the **Remote Database** server install option to create the 6.1 databases on a remote database server. Do not reconfigure the new system to use LDAP.
2. Test and confirm the system works as expected, then shut down the Lotus Expeditor Server 6.1 application servers after the installation is complete.

3. Quiesce the WebSphere Everyplace Deployment 6.0 server, shut down application servers, and back up the WebSphere Everyplace Deployment 6.0 and the Lotus Expeditor Server 6.1 databases. The following databases should be backed up for both WebSphere Everyplace Deployment 6.0 and Lotus Expeditor Server 6.1:
   - DMS
   - DSYCSTAT
   - DSYMSGDB
   - DSYCTLDB
   - WMM

   See Backing up and restoring databases for instructions on how to back up the databases.
4. Migrate WebSphere Member Manager user registry if necessary. See "Migrate WebSphere Member Management database" on page 54 to determine whether you need to migrate WebSphere Member Manager migration.
5. Migrate DB2 Everyplace component data if necessary. See "Migrate DB2 Everyplace data" on page 55 to determine whether you need to migrate DB2 Everyplace data.
6. Migrate DMS component data. See "Migrate Device Management Services data" on page 64 to determine whether you need to migrate Device Manager Services data.
7. You can restart WebSphere Everyplace Deployment 6.0 and use it while migration testing of the Lotus Expeditor Server 6.1 server proceeds.

   Note: Keep in mind that any changes to back end data on the WebSphere Everyplace Deployment 6.0 system will not be reflected in the Lotus Expeditor Server 6.1 system unless migration is performed again.
8. Deploy any application from the 6.0 system to the 6.1 system. For the MQ Everyplace application, you need to create any necessary queues.
9. Test the Lotus Expeditor Server 6.1 server to ensure a successful migration of data.
10. If this is the final migration, perform additional final migration steps to route all request to your Lotus Expeditor Server 6.1 system. See Final Steps for Migration.
11. Upon migration completion, you can reconfigure the Lotus Expeditor Server 6.1 system with an LDAP user registry if desired.

System configured with Microsoft Active Directory 2003

Follow the procedure to migrate a Lotus Expeditor Server 6.0 system that is configured using Microsoft Active Directory 2003 or other customized LDAP.

1. Install Lotus Expeditor Server 6.1 on a separate system. If clustering may be desired in the future, select the **Remote Database** server install option to create the 6.1 databases on a remote database server.

   Important:
   Reconfigure the new system to use the same Active Directory 2003 server as the one you used on your Lotus Expeditor Server 6.0 server.
2. Test and confirm system works as suspected , then shutdown the Lotus Expeditor Server 6.1 application servers after the install is complete.
3. Quiesce the WebSphere Everyplace Deployment 6.0 server, shut down application servers, and backup the WebSphere Everyplace Deployment 6.0 and Lotus Expeditor Server 6.1 databases. The following databases should be backed up for both WebSphere Everyplace Deployment 6.0 and Lotus Expeditor Server 6.1:
   - DMS
   - DSYCSTAT
   - DSYMSGDB

- DSYCTLDB

See Backing up and restoring databases for instructions on how to backup the databases.

4. Migrate DB2 Everyplace component data if necessary. See "Migrate DB2 Everyplace data" on page 55 to determine whether you need to migrate DB2 Everyplace data.
5. Migrate DMS component data. See "Migrate Device Management Services data" on page 64 to determine whether you need to migrate Device Management Services data.
6. You can restart the WebSphere Everyplace Deployment 6.0 now and use it, if desired, while migration testing of Lotus Expeditor Server 6.1 proceeds.

   Note: Keep in mind that any changes to back end data on the WebSphere Everyplace Deployment 6.0 system will not be reflected in the Lotus Expeditor Server 6.1 system unless migration is performed again.
7. Deploy any application from the 6.0 system to the 6.1 system. For the MQ Everyplace application, you need to create any necessary queues.
8. Test the Lotus Expeditor Server 6.1 server to ensure a successful migration of data.
9. If this is the final migration, perform addition final migration steps to route all request to your Lotus Expeditor Server 6.1 system. See Final Steps for Migration.

Backing up and restoring databases

This topic provide instructions on backing up and restoring databases used by WebSphere Everyplace Deployment 6.0 and Lotus Expeditor Server 6.1.

To backup a database follow these instructions:

1. Make sure that you have stopped all applications that use the database.
2. On the database server, open a command prompt.
3. Issue `db2cmd` to open a DB2 command window.
4. Issue the following command to backup the database:

   ```
   DB2 BACKUP DATABASE db_name TO backup_dir WITH 2 BUFFERS BUFFER 1024 PARALLELISM 1 WITHOUT PROMPTING
   ```

   Where `db_name` refers to the name of the database and `backup_dir` refers to the location to store the database backup.

To restore a database follow these instructions:

1. Make sure that you have stopped all applications that use the database.
2. On the database server, open a command prompt.
3. Issue **db2cmd** to open a DB2 command window.
4. Issue the following command to back up the database:

```
DB2 RESTORE DATABASE db_name FROM backup_dir WITH 2 BUFFERS BUFFER 1024 PARALLELISM 1 WITHOUT PROMPTING
```

   Where *db_name* refers to the name of the database and *backup_dir* refers to the location to store the database backup.

Migrate WebSphere Member Management database

This topic provides instructions on migrating WebSphere Member Management data from WebSphere Everyplace Deployment 6.0.

Migration of the WebSphere Member Management database is not required. If you have reconfigured your WebSphere Everyplace Deployment 6.0 system to use Active Directory 2003 for its user registry, you do not need to migrate the WebSphere Member Manager database to the Lotus Expeditor Server 6.1

system. If you have not reconfigured your 6.0 system to use Active Directory 2003, you should only consider migrating the WebSphere Member Management database if you plan to migrate DB2 Everyplace data. Follow the procedure to migrate WebSphere Member Management data.

1. Shutdown the coreServices application servers on both the WebSphere Everyplace Deployment 6.0 system and the Lotus Expeditor Server 6.1 system.
2. Use the DB2 backup command to backup the WebSphere Member Manager database named WMM on the WebSphere Everyplace Deployment 6.0 server. See Backing up and restoring databases for instructions on how to backup the database.
3. Copy the backup to the DB2 server that the Lotus Expeditor Server 6.1 system is currently using.
4. Use the DB2 `restore` command to restore the backed up WebSphere Member Manager database onto the Lotus Expeditor Server 6.1 system's DB2 server. See Backing up and restoring databases for instructions on how to restore the database.
5. Update the security role for the User Management application:
   a. Log on to the WebSphere Application Server administration console and browse to **Applications → Enterprise Applications**.
   b. Select **User Management Servlet**.
   c. Under **Addition Properties** select **Map security roles to users/groups**.
   d. Check **um-security-role** and click **Lookup groups**.
   e. Search String should be * and click on **Search**.
   f. Select the WebSphere Everyplace Deployment 6.0 admin group name (for instance, edsdadmins) under **Available** and click **>>** to move it to **Selected**.
   g. Select any groups under **Selected** that did not exist on the WebSphere Everyplace Deployment 6.0 Server and click **<<** to remove it. Then click **OK**.
   h. Click **OK**, then save the changes.
6. Update the DB2e synchronization group:
   a. Log in as the administrator.
   b. Change to the *expeditor_home*\DB2Everyplace\config directory.
   c. Edit **dsyconfig.properties** and change the value of **syncgroup** to the name of the syncgroup used by WebSphere Everyplace Deployment 6.0 (for example, edssycngroup). Save the changes.
   d. Issue the following command: `DSYconfig.bat update-syncgroup`
7. Update the DMS administrator group:
   a. Log in as the administrator.
   b. Change to the *expeditor_home*\DMS\config directory.
   c. Edit **DMSconfig.properties** and change the value of **instDMAdminGroup** to the name of the administrator group used by WebSphere Everyplace Deployment 6.0 (for example, edsadmins). Save the changes.
   d. Issue the following command: `DMSconfig.bat -target ext-update-UserServices-pw`
8. Start the Lotus Expeditor Server 6.1 application servers and use the User Management Console to see if the migration was successful.

Migrate DB2 Everyplace data

This topic describes how to migrate DB2 Everyplace data.

Migration of DB2 Everyplace is not required. You should only consider migrating DB2 Everyplace if you are using the DB2 Everyplace services in a WebSphere Everyplace Deployment 6.0 production environment in which you have created a large number of subscriptions that you do not want to manually recreate on the Lotus Expeditor Server 6.1 system.

You may only migrate from DB2 Everyplace 8.2 included with WebSphere Everyplace Deployment 6.0. Migration from a standalone version of DB2 Everyplace is not supported.

If you need to migrate DB2 Everyplace, you can only migrate from DB2 Everyplace 8.2 included with WebSphere Everyplace Deployment 6.0. Migration from a standalone version of DB2 Everyplace is not supported. Using parallel migration allows you to test, evaluate, and move users to the new DB2 Everyplace 9.1 server gradually by migrating one group at a time.

Performing parallel migration to DB2 Everyplace

You can now create or edit subscriptions on the DB2 Everyplace 9.1 server. If you have not done so already, you can also choose to upgrade client device software to DB2 Everyplace 9.1 after you complete the migration.

To perform parallel migration, follow these steps:

1. Make sure that you meet the requirements described in "Requirements for parallel migration."
2. *Optional*: If you want to test the new DB2 Everyplace 9.1 configuration before allowing it to write to the source databases, duplicate the source databases by copying them to a test server. This test is supported only for JDBC subscriptions.

   When migrating to DB2 Everyplace 9.1, both the DB2 Everyplace 8.2.x server and the DB2 Everyplace 9.1 server can write to the production source databases
3. Prepare the DB2 Everyplace 8.2.x server for migration. See "Preparing the DB2 Everyplace 8.2.x server for migration" on page 57.
4. Prepare the DB2 Everyplace 9.1 server for migration. See "Preparing the DB2 Everyplace server for migration" on page 58.
5. Export the DB2 Everyplace 8.2.x configuration. If you have both DataPropagator™ and JDBC subscriptions, you must export each type of subscription separately. See "Exporting the DB2 Everyplace 8.2.x configuration" on page 58.
6. Import the DB2 Everyplace 8.2.x configuration into the DB2 Everyplace 9.1 server. If you have both DataPropagator and JDBC subscriptions, you must import each type of subscription separately. See "Importing the DB2 Everyplace 8.2.x configuration" on page 60.
7. Synchronize client devices with the DB2 Everyplace 9.1 server. See "Synchronizing client devices with the DB2 Everyplace 9.1 server" on page 62.
8. Disable the DB2 Everyplace 8.2.x system:
   a. Make sure that no applications are connected to the source database, including the DB2 Everyplace 9.1 Sync Server.
   b. Delete all the subscriptions that are using the DB2 Everyplace 8.2.x Mobile Devices Administration Center.
9. Test the compatibility mobile devices that are running different versions of DB2 Everyplace. See "Testing compatibility of different versions of DB2 Everyplace client devices" on page 63.

Requirements for parallel migration

This topic lists requirements for parallel migration.

Before you can perform parallel migration to DB2 Everyplace 9.1, you must meet the following requirements.

- You must be migrating from DB2 Everyplace 8.2.x to DB2 Everyplace 9.1.
- You will need a separate physical server for DB2 Everyplace 9.1. UNIX and Linux servers support parallel migration on the same physical server, but DB2 Everyplace 9.1 must be a separate instance from the older version of DB2 Everyplace.
- Parallel migration to DB2 Everyplace 9.1 is supported for the following source databases:

– DB2 for zSeries®
– DB2
– DB2 for iSeries™
– Oracle
– SQL Server

For the supported versions of each source database, see Source databases supported by DB2 Everyplace.

DB2 Everyplace 9.1 does not support parallel migration for configurations with Informix® source databases on any operating system. For information about the migration steps for this unsupported database, contact IBM Software Support.

- If your source database is DB2 UDB 7, migrate your source database to DB2 UDB 8. You cannot add, modify, or delete any DB2 Everyplace subscriptions if the source database is DB2 UDB 7.

  Attention: To migrate to UDB 8, ensure that the 7 source database has fix pack 4 or later installed. In addition, be sure that replication is running normally for at least a week after fix pack 4 is installed.
- If you have JDBC subscriptions with an Oracle source database, and the tables in the subscriptions have LONG or LONG RAW columns, do not migrate to DB2 Everyplace 9.1. Contact IBM Software Support for assistance.

Restrictions:

- Do not change user IDs or passwords during migration. Make these changes only after you have completed migration and you have verified that DB2 Everyplace is functioning properly.
- Do not create or edit subscriptions on any server during migration. You must clean up and disable the DB2 Everyplace 8.2.x server before you edit or create subscriptions on the DB2 Everyplace 9.1 server.
- If you have both JDBC and DataPropagator subscriptions, you must import each type of subscription separately.
- The new DB2 Everyplace 9.1 server can write to the production source databases at the same time as the older version of DB2 Everyplace. If this is a concern, duplicate the source databases before beginning the migration process and test the new DB2 Everyplace 9.1 configuration with the test source databases. This test is supported only for JDBC subscriptions.
- DB2 Everyplace 9.1 supports 8.2.x mobile devices. Therefore, you can choose whether to upgrade the mobile devices.
- If you have DataPropagator subscriptions, you must follow special instructions for importing and exporting DataPropagator subscriptions.

Preparing the DB2 Everyplace 8.2.x server for migration

This topic describes how to prepare the DB2 Everyplace 8.2.x server for migration.

Important: Before you perform parallel migration to DB2 Everyplace 9.1, you must create a backup of the data on your system.

To prepare the DB2 Everyplace 8.2.x server for migration:

1. Replicate each mirror database with the dsyreplicate command.
   a. Log in as the administrator.
   b. Go to the <DSYPATH>\Server\bin directory.
   c. Issue the following command: `dsyreplicate` *`mirror_db`*`_name`

      where *mirror_db_name* is the name of the mirror database that you want to replicate.
2. Stop the DB2 Everyplace 8.2.x Sync Server servlet.

3. Back up all source and mirror databases and the DSYCTLDB control database. For details about backing up DB2 databases, see the DB2 Information Center. For details about backing up non-DB2 databases, see the documentation for the non-DB2 database.
4. Restart the DB2 Everyplace 8.2.x Sync Server servlet so that client devices can resume synchronization.

Preparing the DB2 Everyplace server for migration

This topic describes how to prepare the DB2 Everyplace server for migration.

Prerequisites are as follows:

- Make sure that you meet the "Requirements for parallel migration" on page 56.
- Install the DB2 Everyplace 9.1 Sync Server and test it by running the VNurse sample.
- Install DB2 UDB 8.1.6a with the hotfix that is shipped with WebSphere Application Server 5.1.
- Migrate all users from the WebSphere Everyplace Deployment 6.0 to the Lotus Expeditor 6.1. See "Migrate WebSphere Member Management database" on page 54 for more information on migrating users.
- Use the system user IDs and passwords from the WebSphere Everyplace Deployment 6.0 server.

To prepare the DB2 Everyplace 9.1 server for migration, follow these steps:

1. Stop the DB2 Everyplace 9.1 Sync Server servlet.
2. Create mirror databases for all JDBC subscriptions that you want to migrate. Do not create mirror databases for DataPropagator subscriptions. You will back up and restore mirror databases for DataPropagator subscriptions at a later time.
3. Catalog the source databases.

   If you are using a DB2 series source database, you must catalog the source databases to make it accessible. See the DB2 Information Center for catalog steps.

   If your source database is non-DB2, enter the correct information for the JDBC driver while you are creating a subscription so that it can connect to the source database correctly. For more information about connecting to non-DB2 source databases while creating subscriptions, see the Subscriptions topic of the Sync Server Administration Guide.

   If you are using test source databases, make sure that this database is accessible instead of the production source database. You can use test source databases only with JDBC subscriptions.
4. For file subscriptions only, copy the subscribed files that have the same directory path as the DB2 Everyplace 8.2.x server to the new DB2 Everyplace 9.1 server.

Exporting the DB2 Everyplace 8.2.x configuration

This topic describes how to export the DB2 Everyplace 8.2.x configuration.

Part of the process of parallel migration involves exporting your current DB2 Everyplace 8.2.x configuration into an XML script. There are separate instructions for JDBC and DataPropagator subscriptions.

Topics are as follows:

- "Exporting the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions" on page 59
- "Exporting the DB2 Everyplace 8.2.x configuration for JDBC subscriptions" on page 59

Exporting the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions

Follow these steps to export the configuration of your DB2 EveryplaceDataPropagator subscriptions.

Prerequisites:

- If your DataPropagator subscriptions access a source database that is running on an AS/400® server, create a new index on the prune control table on the source database. Use the following SQL statement to create the index:

```
CREATE UNIQUE INDEX ASN.IBMSNAP_PRUNCNTLX
    ON ASN.IBMSNAP_PRUNCNTL (
    SOURCE_OWNER,
    SOURCE_TABLE,
    SOURCE_VIEW_QUAL,
    APPLY_QUAL,
    SET_NAME,
    TARGET_SERVER,
    TARGET_TABLE,
    TARGET_OWNER);
```

- Make sure that you meet the "Requirements for parallel migration" on page 56.

To export the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions, complete these steps.

Attention: The coreServices application server must be started before you can export the IBM DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions.

Note:

1. Run the XML scripting tool, dsyadminxml.
   a. Log in as the administrator.
   b. Change to the <DSYPATH>\Server\bin\ directory.
   c. Issue the following command: `dsyadminxml -x outputFile`.

      where *outputFile* is the output file to which you want to store the configuration for DataPropagator subscriptions.
2. Remove all tags that apply to JDBC subscriptions. You must export JDBC subscriptions separately.
3. Transfer the output file to the DB2 Everyplace 9.1 server.

Exporting the DB2 Everyplace 8.2.x configuration for JDBC subscriptions

Follow these steps to export the configuration of your DB2 Everyplace JDBC subscriptions.

Prerequisite: Make sure that you meet the "Requirements for parallel migration" on page 56.

To export the DB2 Everyplace 8.2.x configuration for JDBC subscriptions:

Attention: The coreServices application server must be started before you can export the DB2 Everyplace 8.2.x configuration for JDBC subscriptions.

1. Run the XML scripting tool, dsyadminxml.

   Windows

   a. Log in as the administrator.
   b. Change to the <DSYPATH>\Server\bin\ directory.
   c. Issue the following command: `dsyadminxml -x outputFile`

   UNIX and Linux

   a. Log in as the DB2 Everyplace Sync Server instance.

b. Change to the $DSYINSTDIR/Server/bin/ directory.
c. Issue the following command: `./dsyadminxml -x outputFile`

where *outputFile* is the output file to which you want to store the configuration for JDBC subscriptions.

2. Remove all tags that apply to DataPropagator subscriptions. You must export DataPropagator subscriptions separately.
3. **Optional:** If you are using a test source database, edit the `Database` and `MasterDb` tags in the output file to point to the test source database instead of to the production source database.

   Example:

```
<AddJdbcMaster>
...
 <Database>jdbc:db2:testSourceDb</Database>
...
</AddJdbcMaster>
<AddJdbcSubscription>
...
 <MasterDb>jdbc:db2:testSourceDb</MasterDb>
...
</AddJdbcSubscription>
```

   where *testSourceDb* is the name of the test source database. Be sure to edit the `MasterDb` tag for all of your subscriptions.
4. Transfer the output file to the DB2 Everyplace 9.1 server.

Importing the DB2 Everyplace 8.2.x configuration

This topic describes how to import the DB2 Everyplace 8.2.x configuration.

Part of the process of parallel migration involves importing your current DB2 Everyplace 8.2.x configuration into a DB2 Everyplace 9.1 configuration. There are separate instructions for JDBC and DataPropagator subscriptions.

Topics are as follows:

- "Importing the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions"
- "Importing the DB2 Everyplace 8.2.x configuration for JDBC subscriptions" on page 62

Importing the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions

Follow these steps to import the configuration of your DB2 Everyplace DataPropagator subscriptions.

Prerequisites:

- Make sure that you meet the "Requirements for parallel migration" on page 56.
- Ensure that the LogFileSize setting of the mirror database is at least 1000 4KB.
- Create a backup image of the mirror database that is used in DataPropagator table subscriptions on the DB2 Everyplace 8.2.x server.
- Verify that the database user IDs and passwords in the output file on the DB2 Everyplace 9.1 server are correct.
- Ensure that no applications are connected to the source databases and that DB2 Everyplace 8.2.x does not perform a replication to the source database.

To import the DB2 Everyplace 8.2.x configuration for DataPropagator subscriptions, complete these steps.

Attention: The coreServices application server must be started before you can export the DB2 Everyplace 8.2.x configuration for JDBC subscriptions.

1. Stop the DB2 Everyplace 9.1 Sync Server servlet. Do not open the Mobile Devices Administration Center after you have stopped the DB2 Everyplace 9.1 Sync Server servlet. If you open the Mobile Devices Administration Center, the next import step will result in errors.
2. Restore the mirror database backup image from the DB2 Everyplace 8.2.x server. If the restored database is in a rollforward-pending state and does not allow connections, enter the following command in a DB2 command window to bring the database into a defined state:

   `db2 rollforward database DB_name to end of logs and complete`

   where *DB_name* is the name of the restored database.
3. Catalog the source database.
4. Edit the DSYDPMIG8ENV file and supply values for the environment variables that are listed in the file.
   - On Windows systems, edit the DSYDPMIG8ENV.bat script that is located in the <DSYPATH>\config\work\migrate\ directory.
   - On UNIX and Linux systems, edit the DSYDPMIG8ENV.sh script that is located in the $DSYINSTDIR/config/work/migrate/ directory.
5. Run the DSYPREASNMIG8 command.

   If you receive the error `DB2Exception: SQL1117N A connection to or activation of database dbname cannot be made because of ROLL-FORWARD PENDING` (SQLSTATE = 57019), issue the rollforward command to bring the database into a defined state as described in step 2.
6. Edit the XML output file that contains the DB2 Everyplace DataPropagator configuration and make the following changes:
   a. Make sure that the Replicate attribute is set to FALSE.

      Example:

      ```
      <AddDproprSubscription Replicate = "FALSE">
      ```

   b. Remove all the `<AddAdapter>` and `</AddAdapter>` tags and their contents. If you do not remove the tags, you will receive the following error message: `Error processing XML: Adapter already exists in the next import step`
7. Import the DB2 Everyplace 8.2.x configuration by using the XML Scripting tool.
   a. Log in as the administrator.
   b. Change to the <DSYPATH>\Server\bin\ directory.
   c. Issue the following command: `dsyadminxml -d outputFile`.where *outputfile* is the output file to which you want to store the configuration for DataPropagator subscriptions.

   If the import operation results in filter and parameter syntax errors, fix them in the output file before you import the configuration again. See the table filters topic in DB2 Everyplace Sync Server Administration Guide for more information about filter syntax.

   Note: This step will not import a non-LDAP user. The users in the imported XML need to be defined in the LDAP SyncGroup group already. If the users are not defined in the SyncGroup, you will receive the following error message: `Error processing XML: DSYT030E Error creating an LDAP user and associating it with Sync Server`
8. Run DSYPOSTASNMIG8.
9. Disable all groups that are using the DB2 Everyplace 9.1 Mobile Devices Administration Center.
10. Replicate each mirror database:
    a. Log in as the administrator.
    b. Change to the <DSYPATH>\Server\bin\ directory.
    c. Issue the following command: `dsyreplicate mirror_db_name`.

where *mirror_db_name* is the name of the mirror database that you want to replicate. If there is an error, fix the error and rerun the script.

11. Verify that the DB2 Everyplace 8.2 mirror database is correctly migrated and that it properly supports the DataPropagator table subscriptions.
12. Drop the BACKUPTS table space and all of the other tables in the schema BACKUP (substitute your own table space and schema names if you did not use the default names).
13. Start the DB2 Everyplace 9.1 Sync Server servlet.

Importing the DB2 Everyplace 8.2.x configuration for JDBC subscriptions

Follow these steps to import the configuration of your DB2 Everyplace JDBC subscriptions.

Prerequisites:

- Make sure that you meet the "Requirements for parallel migration" on page 56.
- Verify that the database user IDs and passwords in the output file on the DB2 Everyplace 9.1 server are correct.
- Ensure that no applications are connected to the source databases. Make sure that DB2 Everyplace 8.2.x does not perform a replication to the source database.

To import the DB2 Everyplace 8.2.x configuration for JDBC subscriptions, complete these steps.

Attention: The coreServices application server must be started before you can export the DB2 Everyplace 8.2.x configuration for JDBC subscriptions.

1. Stop the DB2 Everyplace 9.1 Sync Server servlet. Do *not* open the Mobile Devices Administration Center after you have stopped the DB2 Everyplace 9.1 Sync Server servlet. If you open the Mobile Devices Administration Center, the next import step will have errors.
2. Remove all the `<AddAdapter>` and `</AddAdapter>` tags from the output file. If you do not remove the tags, you will receive the following error message: `Error processing XML: Adapter already exists in the next import step`.
3. Import the DB2 Everyplace 8.2.x configuration by using the XML Scripting tool.
   a. Log in as the administrator.
   b. Change to the <DSYPATH>\Server\bin\ directory.
   c. Issue the following command: `dsyadminxml -d outputFile`.

      where *outputFile* is the output file to which you want to store the configuration for DataPropagator subscriptions. If the import results in filter and parameter syntax errors, fix them in the output file before you import the configuration again.

      Note: This step will not import a non-LDAP user. The users in the imported XML must be defined in the LDAP SyncGroup group already. If the users are not defined in the SyncGroup, you will receive the following error message: `Error processing XML: DSYT030E Error creating an LDAP user and associating it with Sync Server`.
4. Replicate each mirror database:
   a. Log in as the administrator.
   b. Change to the <DSYPATH>\Server\bin\ directory.
   c. Issue the following command: `dsyreplicate mirror_db_name`.

      where *mirror_db_name* is the name of the mirror database that you want to replicate. If there is an error, fix the error and rerun the script.
5. Start the DB2 Everyplace 9.1 Sync Server servlet.

Synchronizing client devices with the DB2 Everyplace 9.1 server

This topic describes how to synchronize client devices with the DB2 Everyplace 9.1 server.

By using parallel migration, you can migrate a small subset of your client devices that synchronize to the DB2 Everyplace 8.2.x server to synchronize to the DB2 Everyplace 9.1 server.

Prerequisite: Make sure that you meet the "Requirements for parallel migration" on page 56.

To synchronize the client devices with the DB2 Everyplace 9.1 server:

1. On the DB2 Everyplace 8.2.x server:
   a. Identify a synchronization group to migrate.
   b. Synchronize all of the client devices that are in the group with the DB2 Everyplace 8.2.x server and ensure that synchronization is successful.

      Important: A client device must not make any changes to data during the time after this synchronization and before it synchronizes with the DB2 Everyplace 9.1 server. If it does, those changes are lost because the client device refreshes when it synchronizes with the DB2 Everyplace 9.1 serverfor the first time.
   c. Replicate each mirror database and ensure that replication is successful.
   d. Disable this synchronization group in the Mobile Devices Administration Center.
   e. Remove the association that these client devices have with the subscription sets and groups.
2. On the DB2 Everyplace 9.1 server:
   a. Replicate each mirror database and ensure that replication is successful.
   b. Enable the same synchronization group that you disabled on the DB2 Everyplace 8.2.x server in the Mobile Devices Administration Center.
   c. Open the DB2 Everyplace 9.1 Mobile Devices Administration Center. Check the group that these clients belong to and ensure that the subscription sets are associated with this group. If the subscription sets are not associated with the group, edit the group and associate the subscription sets with the group.
   d. **Optional:** Upgrade the group of client devices to DB2 Everyplace 9.1. DB2 Everyplace 9.1 is compatible with 8.2.x client devices, so you can choose to do this at a later time.
   e. Update the server IP address in the server settings of the synchronization client program to the IP address of the DB2 Everyplace 9.1 Sync Server. Do this for all client devices in the group.
   f. Synchronize the group and ensure it is successful.

      Important: The client devices that are in the group are refreshed because they are now synchronizing to the new DB2 Everyplace 9.1 system. Any changes that a client device made after synchronizing for the last time with the DB2 Everyplace 8.2.x system are lost after this refresh.
   g. Compare all of the clients' table data with the source table data and make sure they are the same.
3. Repeat steps 1 and 2 until you migrate all of the client devices to the DB2 Everyplace 9.1 server.

Testing compatibility of different versions of DB2 Everyplace client devices

This topic describes how to testing compatibility of different versions of DB2 Everyplace client devices.

Because DB2 Everyplace 9.1 supports DB2 Everyplace 8.2.x client devices, you can test to see if the two types of client devices receive changes from each other. This test is optional.

To test the compatibility of different versions of DB2 Everyplace client devices:

1. On a DB2 Everyplace 8.2.x client device:
   a. Insert, update, and delete rows from the client device.
   b. Synchronize the client device.

c. Replicate each mirror database and ensure that the replication is successful.
d. Compare the client device data with the source table data and ensure that they are the same.

2. On a DB2 Everyplace 9.1 client device:
   a. Synchronize the client device.
   b. Replicate each mirror database and ensure that the replication is successful.
   c. Synchronize the client device and ensure that the replication is successful.
   d. Compare the client device data and the source table data and ensure that they are the same.
   e. Insert, update, and delete rows from a client device.
   f. Synchronize the client device.
   g. Replicate each mirror database and ensure that the replication is successful.
   h. Compare the client device data with the source table data and ensure that they are the same.
3. On a DB2 Everyplace 8.2.x client device:
   a. Replicate each mirror database and ensure that the replication is successful.
   b. Synchronize the client device and ensure that the replication is successful.
   c. Compare the client device data and the source table data and ensure that they are the same.

Migrate Device Management Services data

This topic provides instructions on how to migrate from Device Manager 1.8 to Device Manager 2.1.

Migration of Device Manager is not required. You should only consider migrating Device Manager if you are using the Device Manager in a WebSphere Everyplace Deployment 6.0 production environment where you want to preserve your inventory data about your existing devices.

To migrate the data from Device Manager 1.8 to Device Manager 2.1, complete the following required steps:

1. Read the migration introduction, assumptions, and restrictions.
2. Perform the prerequisite tasks.
3. Prepare for the database migration.
4. Migrate the data.

After the required migration steps are complete, some of the following tasks may be required depending on your environment:

- Upgrade the clients. You can upgrade the clients over a period of time.
- "Replacing the Device Manager console" on page 78
- Migrate the Administration API (optional)

This migration document refers to Device Manager 1.8 and Device Manager 2.1, which were included with WebSphere Everyplace Deployment 6.0, and Lotus Expeditor Server 6.1, respectively. You can only migrate from Device Manager 1.8 to Device Manager 2.1.

Introduction to Device Manager migration

This topic provides an overview to migrating from Device Manager 1.8 to Device Manager 2.1.

The following topics are described in this section:

- Introduction
- Overview of the migration process
- Migration assumptions
- Differences between Device Manager Services 1.8 and 2.1

- Incompatibilities between the Device Manager versions
- URLs for software distribution jobs
- Migration restrictions

Introduction

The purpose of migrating to Device Manager 2.1 is to retain relevant device data from a previous release of Device Manager and to have that data work with the new release of Device Manager. The data migration copies the device data, such as data for OSGi devices and Windows 32-bit devices, from the old database schema to the new database schema. The device data from the previous version is not changed during the data migration.

The Device Manager database 2.1 and the Device Manager database 1.8 are independent of each other. There should be no corruption of data or extended downtime for the Device Manager server 1.8. **However, it is recommended that you make a backup copy of your data on a regular basis and before you start the data migration process.**

You can perform "practice migrations" prior to migrating your production data to Device Manager 2.1. After the Device Manager 2.1 environment has passed your acceptance test, the migration process can be repeated for the final migration to the new Device Manager Services.

Before completing the final migration:

1. You must take the Device Manager server 1.8 off-line.
2. The backup of the production system database must be done after it has been disabled.

With the Device Manager server off-line, ensure that the most recent data is migrating to Device Manager 2.1. You must prevent users from accessing either system until the final migration is complete and the new system is placed in production.

The migration from Device Manager 1.8 to Device Manager 2.1 affects the following Device Manager components:

- Device Manager device data

  The major differences between Device Manager 1.8 and Device Manager 2.1 are the changes to the database schema. Data for the following devices classes are migrated:

  – Linux
  – OSGi
  – Win32
- Device Manager device agents

  The Linux, OSGi, and Windows 32-bit device agents for Device Manager 1.8 do work with a Device Manager 2.1 server. The new functions cannot be used with Device Manager 2.1 until the device agent is upgraded to the Device Manager 2.1 level.

  It is recommended that you upgrade all of your device agents.
- Device Manager console, if used

  Due to the changes in the supported database levels and database schema, the older Device Manager console does not function with the Device Manager 2.1 server and database.

  Using the previous console or database client with Device Manager 2.1 may destroy data and have unpredictable results.

  After Device Manager 2.1 is in full production, you can delete the console files from Device Manager 1.8.
- Device Manager Administration API (optional)

The Administration APIs that are based on the Apache SOAP run-time will continue to be supported with Device Manager 2.1. However, the use of the Apache SOAP run-time classes in the Administration APIs will be deprecated in a future release of Device Manager.

Before you migrate the device data from Device Manager 1.8 to Device Manager 2.1, you must install and configure Device Manager 2.1. Device Manager 2.1 must be a new installation.

Only the device data migrates to Device Manager 2.1. The Device Manager server binary files are not migrated from Device Manager 1.8 to Device Manager 2.1. Any customized changes to the configuration of Device Manager server 1.8 must be manually migrated to the Device Manager 2.1 server installation.

The migration process that follows is only valid for migrating from Device Manager 1.8 to Device Manager 2.1.

Overview of the migration process

To migrate your data to Device Manager 2.1, complete the following tasks:

1. Complete a new installation of Device Manager 2.1.
2. Backup your Device Manager 1.8 database, then restore that database to the Device Manager 2.1 database server.

   Note: The Device Manager 1.8 database and Device Manager 2.1 database might be on the same system or on different systems. If the databases are on the same system, the names must be different.
3. Use the data migration command to move the device data from the previous version of Device Manager to the database for Device Manager 2.1.
4. Upgrade the device agents on your devices by using software distribution jobs.
5. Upgrade the Device Manager console.
6. Upgrade your applications that use the Administration APIs.

Step-by-step instructions for these migration tasks are provided.

Post Migration steps

After Device Manager migration is complete, review the topics in After installing Device Manager for a list of post-migration tasks that may be required for your environment.

Migration assumptions

When migrating from Device Manager 1.8 to Device Manager 2.1, the following assumptions are made:

- Your database system for Device Manager 2.1, must have adequate disk space to store two copies of the database for the exported files.

  If you want to backup the Device Manager 2.1 database during the migration testing period (recommended), then your database system must have adequate disk space to store three copies of the database.

  Since the Device Manager 2.1 database has not been used in a production environment, it should be small in size.
- The system where you install and configure Device Manager server 1.8 must not have Device Manager 2.1 server installed on it.

  Device Manager 1.8 and Device Manager 2.1 cannot coexist on the same systems.
- You cannot migrate to or from an Oracle database.
- You cannot migrate between a DB2 database and an Oracle database.

- The only supported operating system for the Device Manager servers for this migration is Windows.
- The migration of the device data must be done before any devices are registered or jobs created for Device Manager 2.1. Any device data in the Device Manager 2.1 database is deleted when the Device Manager 1.8 data is migrated.
- The initial inventory jobs (with default job attributes) created during the installation of Device Manager 2.1 are deleted. The initial inventory jobs from Device Manager 1.8 are migrated to replace default initial inventory jobs that were deleted.

  If the administrator deleted an initial inventory job from Device Manager 1.8 after the migration there will not be an initial inventory job for that device class for Device Manager 2.1.
- The device notification data is migrated so the devices will continue to be notified about the migrated jobs.
- You cannot migrate from Device Manager 1.3, 1.4, 1.5, 1.5.1, 1.6, or 1.7, to Device Manager 2.1.

Differences between Device Manager Services 1.8 and 2.1

The major differences between Device Manager 1.8 and Device Manager 2.1 are as follows:

- The database schema has undergone changes.
- Device Manager 2.1 server requires DB2 9.1.
- Device Manager 2.1 server requires WebSphere Application Server 6.0.2.11.

Incompatibilities between the Device Manager versions

The database schema for Device Manager 1.8, is different from the database schema used for Device Manager 2.1. Therefore, the following incompatibilities exist between those versions:

Incompatibilities with server and database

- Device Manager server 1.8 does not work with the Device Manager database 2.1.
- Device Manager database 1.8 does not work with the Device Manager server 2.1.

Incompatibilities with the console

- Device Manager console 1.8 does not work with the Device Manager database 2.1.
- Device Manager database 1.8 does not work with the Device Manager console 2.1.

Incompatibilities with the device agents:

- The device agents for Device Manager 2.1 do not work with a Device Manager server 1.8.

URLs for software distribution jobs

When an administrator creates a software distribution job or a software removal job with the Device Manager console, Administration APIs, or Device Manager commands, the URL for the software package, OSGi bundle, or Eclipse feature is entered in the **Software URL** field.

If software files associated with migrated jobs are relocated, then the software URLs for those jobs within the migrated database must be manually updated.

You must verify that the value for the software URL remains valid for Device Manager 2.1. No migration for the value of the software URL occurs.

Migration restrictions

For the following features, there are migration restrictions:

- No migration for Palm OS and Windows CE devices

The device data for Palm OS and Windows CE devices is not migrated to Device Manager 2.1.

- Reregistered Eclipse features that were wrapped and delivered via the NativeAppBundle tool

  If you delivered Eclipse features that were wrapped with the NativeAppBundle tool, those Eclipse features must be reregistered as Eclipse feature distribution jobs. Use the Eclipse feature control job to manage the Eclipse features.

  You cannot wrap and deliver Eclipse features with the NativeAppBundle tool.
- Recreate all NativeAppBundles

  All NativeAppBundles from the previous release containing native content (not Eclipse features) must be recreated using the updated NativeAppBundle tool in the current release.

  You must use the new NativeAppBundle tool to create the NativeAppBundle again before distributing it with the current release.

Prerequisite tasks for Device Manager migration

This topic provides a list of tasks that must be completed before you migrate to Device Manager 2.1

You can install the new version of Device Manager as a single, unmanaged server deployment, an unmanaged Device Manager server with a remote database deployment, or a managed server deployment.

You must complete the following tasks before you migrate the database:

1. Install and configure Device Manager database 2.1.
2. Ensure your version of DB2 is supported by Device Manager 2.1.
3. Install and configure Device Manager server 2.1.
4. Ensure your version of WebSphere Application Server is supported by Device Manager 2.1.
5. Manually migrate any customized changes to the configuration of Device Manager server 1.8 to the Device Manager 2.1 server installation.

   For example, custom changes to **Transaction.properties**, **ConsoleTransaction.properties**, **push.properties**, and **web.xml files** must be manually migrated (refer to the Troubleshooting topic).

   If you do not have any customized changes to the configuration of Device Manager server, you can use the default configuration for Device Manager 2.1 server.

Preparing for the database migration

See this section for tips on how to plan for migrating your Device Manager 1.8 to Device Manager 2.1.

The following topics are described in this section:

- Preparing the databases
  - System with Device Manager 1.8 database
  - System with Device Manager 2.1 database
- Preparing a properties file for migration
- Sample properties file for migration

Preparing the databases

System with Device Manager 1.8 database

To prepare the Device Manager 1.8 database for migration, do the following steps on the system with Device Manager 1.8 database:

1. As appropriate, clean up expired jobs, delete obsolete devices, delete obsolete jobs, and so on. You want to remove all obsolete data from your Device Manager 1.8 database before you run the data migration command so you have less data to migrate.

As appropriate, increase the size of the DB2 logs. The log sizes can be reduced to your normal size after the migration.

2. Gather information about the Device Manager 1.8 database by running the DB2 snapshot command:

```
db2start
db2 update monitor switches using bufferpool on
db2 activate db dms
db2 get snapshot for tablespaces on dms
```

The snapshot command provides the directories for the database table space. When you install Device Manager 2.1, you must use different directories for the database table space.

Note: The restored Device Manager 1.8 database and new Device Manager 2.1 database cannot have the same name or be in the same directory.

3. Create a directory on the Device Manager 1.8 system for the backup of the existing Device Manager database.
   a. Change to the *dms_home* directory, where *dms_home* is the installation directory of the Device Manager server application.
   b. Create a backup directory named DMS_18_DB_BACKUP.

```
mkdir data/DMS_18_DB_BACKUP
```

4. Shutdown the DMS_AppServer from WebSphere Application Server console.

The data backup process requires that the DMS_AppServer be stopped while the backup occurs. The amount of time to do the backup depends on the size of the database, but it should be brief. This shutdown of WebSphere Application Server should not affect users anymore than a regular maintenance backup of the data on the production system.

Note: Shutting down the DMS_AppServer also disables other applications, such as Device Manager applications and WebSphere Application Server applications.

   a. Change to the *was_home*/bin directory, where *was_home* is the installation directory of the WebSphere Application Server is running.
   b. Use the command for your operating system (assumes DMS as the database name):

      Windows:

```
stopServer.bat DMS_AppServer -user was_admin_user -password was_admin_password
```

5. Back up the database for Device Manager 1.8 to the DMS_18_DB_BACKUP directory.

The backed-up 1.8 database file is the basis for the data migration and will be restored as the Device Manager 2.1 database. The restored database name and directory name must be different from the Device Manager 1.8 names.

Make a note of the timestamp for the backup output file. The timestamp value will be used when you restore the database.

For Windows, you must be logged in with Administrator privileges:

```
db2stop force
db2start
db2 backup database dms to /data/DMS_18_DB_BACKUP
```

6. Start the DMS_AppServer from WebSphere Application Server console.
   a. Change to the *was_home*/bin directory, where *was_home* is the installation directory of the WebSphere Application Server is running.
   b. Use the command for your operating system (assumes DMS as the database name):

      Windows:

```
startServer.bat DMS_AppServer -user was_admin_user -password was_admin_password
```

System with Device Manager 2.1, database

To prepare the Device Manager 2.1 database for migration, do the following steps on the system with Device Manager 2.1 database:

1. Even though the Device Manager 2.1 is a new installation, you should back up the Device Manager 2.1 database to the DMS_21_ORIGINAL_DB directory.

   If you want to do practice migrations, you can use this backup database to restore the Device Manager 2.1 database to the original state right before the final migration occurs without having to reinstall Device Manager. You may never need the backup of the original Device Manager 2.1 database, but it is a good practice to back up the original database.

   It is recommended that you do practice migrations. You can always restore back to the database in the DMS_21_ORIGINAL_DB directory (see steps 3 below).
2. Create a directory on the Device Manager 2.1, system for the database backup.
   a. Change to the *dms_home* directory. where *dms_home* is the installation directory of the Device Manager server application.
   b. Create a backup directory named DMS_21_ORIGINAL_DB.

      ```
      mkdir data/DMS_21_ORIGINAL_DB
      ```
3. While you are doing the practice migrations, you can always restore the Device Manager 2.1 database to the original state with this backup of the database.

   For Windows, you must be logged in with Administrator privileges:

   ```
   db2stop force
   db2start
   db2 backup database dms to /data/DMS_21_DB_ORIGINAL
   ```
4. Start the DMS_AppServer from WebSphere Application Server console.
   a. Change to the *was_home*/bin directory, where *was_home* is the installation directory of the WebSphere Application Server is running.
   b. Use the command for your operating system (assumes DMS as the database name):

      Windows:

      ```
      startServer.bat DMS_AppServer -user was_admin_user -password was_admin_password
      ```
5. When the Device Manager 1.8 database is restored, the database name and database schema name must match the values for **instDBName** and **instDBUserId** that were used during the installation of Device Manager 2.1.
6. Make sure the migration of the device data is done before any "production" devices are registered or jobs created. Any device data in the Device Manager 2.1 database is deleted when the Device Manager 1.8 data is migrated.

Preparing a properties file for migration

The properties file for migration uses keyword=value pairs. By inserting values after keywords or changing the values for the keywords, you specify the migration properties.

The properties file name is:

```
dms_home/config/DMSmigration.properties
```

The keywords in the properties file are grouped as follows:

- Device classes for data migration
- Network and database environment
- Connecting to the source database
- Connecting to the destination database

Use the sample properties file as a guide. Edit the values in the config/DMSmigration.properties file for your environment. Use a text editor to edit the values. The values in the properties file are validated when you run the data migration command. If the values are not valid, the data migration stops.

Identify device classes for data migration

Table 6. Keywords that Identify Device Classes for Data Migration

Keyword	Description	Allowed Values, Samples, and Notes
Linux	Device class for Linux devices. Use true to migrate data. Valid values are: • true • false	If a true or false value is not specified, or the line is deleted, false is assumed. If set to true and the device class does not exist, an error occurs.
OSGi	Device class for OSGi devices. Use true to migrate data. Valid values are: • true • false	If a true or false value is not specified, or the line is deleted, false is assumed. If set to true and the device class does not exist, an error occurs.
Win32	Device class for Windows 32-bit devices. Use true to migrate data. Valid values are: • true • false	If a true or false value is not specified, or the line is deleted, false is assumed. If set to true and the device class does not exist, an error occurs.

Network and database environment

Table 7. Keywords for the Network and Database Environment

Keyword	Description	Allowed Values, Samples, and Notes
instDBType	Identifies the database type. The valid values is: db2	The source and destination database types must be the same.

instDBPath	Directory path where the DB2 database software is installed.	`/home/db2inst1/sqllib`
		
		`c:/Program Files/IBM/SQLLIB`

instDBInstance	Identifies the database instance.	db2

instJavaPath	Directory path to the JAVA_HOME to use for the installations. The directory must contain `bin/java` (or `bin/java.exe`).	`/usr/java130`
		
		`c:\Program Files\IBM\ DeviceManager\java\jre`

instExportPath	Identifies the directory where some data is exported to before the data is imported to the new database. The default location is within the Device Manager installation directory. However, if disk space is insufficient, instExportPath can be used to point to a location with more disk space. This keyword is optional.	`/files` If instExportPath is specified and the directory does not exist, the directory will be created.

Connecting to the source database

Table 8. Keywords for Connecting to the Source Database

Keyword	Description	Allowed Values, Samples, and Notes
srcVersion	Identifies the Device Manager version of the source database.	The valid value is: 1.8
srcDBUserId	User name for connecting to the source database. Must be a valid user ID on the system that has the DB2 database that was used with Device Manager 1.8.	db2admin
srcDBPassword	Password for the user name specified by srcDBUserId.	secret
srcDBName	Database name of the source database.	dms18
srcJDBCDriver	Driver name to use for the database connections.	`com.ibm.db2.jcc.DB2Driver`

Connecting to the destination database

Table 9. Connecting to the destination database

destVersion	**Identifies the Device Manager version of the destination database.**	**The valid value is:** **2.1**
destDBUserId	User name for connecting to the destination database. Must be a valid user ID on the system that has the DB2 database that will be used with Device Manager 2.1.	db2admin
destDBPassword	Password for the user name specified by destDBUserId.	secret
destDBName	Database name of the destination database.	dms
destJDBCDriver	Driver name to use for the database connections.	`com.ibm.db2.jcc.DB2Driver`

Sample properties file for migration

```
# Device Manager 2.1 - - - Migration properties file

#     Currently supported migration path:

#     Device Manager version 1.8 to version 2.1
```

Table 10. Sample properties file for migration

```
#################################################################################################

#####                              Keywords that Identify Device    #####
                                    Classes for Data Migration

#####                             - - - - - - - - - - - - - - - -  #####
                                              - - - -
```

Table 10. Sample properties file for migration (continued)

```
#################################################################################################
#####                              Options for each keyword: true or   #####
                                   false
#####                                  true = Device class will be     #####
                                     migrated.  If the device class
                                      does not exist, an error is
                                                logged.
#####                                 false = Device class will NOT be  #####
                                           migrated if it exists
#####                              If a true or false value is not     #####
                                   specified or the line is deleted,
                                   false is assumed, Data for that
                                   device class will not be migrated.
#################################################################################################


Linux=false

OSGi=false

Win32=false
```

Table 11. Sample properties file for migration

```
#################################################################################################
#####                                                                #####
#####                          Keywords for Network and Database     #####
                                        Environment Setup
#####                                                                #####
#################################################################################################


# Set to indicate database type (only "db2" is valid)#
# The source and destination database types must be the same.
instDBType=db2
# instDBPath - Root directory path to where DB2 database software is installed
# Example for Windows:  instDBPath=c:\Program Files\IBM\SQLLIB
 instDBPath=c:/Program Files/IBM/SQLLIB
# instDBInstance - DB instance for db2
# Example for Windows:  db2
instDBInstance=db2
# instJavaPath - Location of JAVA_HOME to use for the installation.
# The directory must contain bin/java (or bin/java.exe)
#Example for Windows:  instJavaPath=C:\Program Files\IBM\DeviceManager\java\jre
instJavaPath=
# instExportPath - During the installation, some data is exported to files
# before being imported to the new database.  The default location is
# within the IBM\DeviceManager installation directory. However, if disk space
# is insufficient, instExportPath can be used to point to a location
# with more disk space. If instExportPath is specified and the directory
# does not exist, the directory will be created.
# Example for Windows:  instExportPath=D:\files
# This keyword is optional.
instExportPath=
```

Table 12. Sample properties file for migration

```
#################################################################################################
```

Table 12. Sample properties file for migration (continued)

```
#####                                                                                  #####
#####                                Keywords for Connecting to the                    #####
                                            Source Database
#####                                                                                  #####
##########################################################################################################

# destVersion - Device Manager version of the destination database
# Only 2.1 is valid
destVersion=2.1

# destDBUserId - Username for connecting to the destination database
# Example:  destDBUserId=dmsadmin
destDBUserId=db2admin

# destDBPassword - Password for destDBUserId
destDBPassword=

# destDBName - Database name of the destination database
destDBName=dms

# destJDBCDriver - Driver name to use for the database connections
# Options:  com.ibm.db2.jcc.DB2Driver
destJDBCDriver=com.ibm.db2.jcc.DB2Driver
```

Migrating the data

This topic provides specific instructions on how to migrate your data from your Device Manager 1.8 to Device Manager 2.1.

The following steps must be completed to migrate the data:

1. Setting up access to required databases
2. Stopping WebSphere Application Server
3. Running the data migration command
4. After migrating your device data

Setting up access to required databases

The Device Manager 2.1 system needs access to the Device Manager 1.8 database to migrate the 1.8 data to the 2.1 database. To ensure proper access to the required databases during migration complete the following steps:

1. Catalog the Device Manager 1.8 database on the Device Manager 2.1 system:
   a. Open a DB2 command window by running the **db2cmd** command.
   b. Issue the following commands to catalog the Device Manager 1.8 database:

      ```
      db2 catalog tcpip node dms_1.8_node remote dms_1.8_hostname server dms_1.8_port
      db2 catalog db DMS as DMS18 at node dms_1.8_node
      ```

      where *dms_1.8_node* is a name to use for the Device Manager 1.8 host, *dms_1.8._hostname* is the fully-qualified Device Manager 1.8 hostname, and *dms_1.8_port* is the port number used to access the Device Manager 1.8 database (default is 50000).
2. If the Device Manager 2.1 database is on a remote database server, catalog the Device Manager 2.1 database on the Device Manager 2.1 system:
   a. Open a DB2 command window by running the **db2cmd** command.
   b. Issue the following commands to catalog the Device Manager 2.1 database:

      ```
      db2 catalog tcpip node dms_2.1_node remote dms_2.1_hostname server dms_2.1_port
      db2 catalog db DMS as DMS at node dms_2.1_node
      ```

where *dms_2.1_node* is a name to use for the Device Manager 2.1 host, *dms_2.1._hostname* is the fully-qualified Device Manager 2.1 hostname, and *dms_2.1_port* is the port number used to access the Device Manager 2.1 database (default is 50000).

3. Shut down the DMS_AppServer from WebSphere Application Server console. There must be no other connections to the database during migration.

   The data backup process requires that the DMS_AppServer be stopped while the backup occurs. The amount of time to do the backup depends on the size of the database, but it should be brief.

   a. Change to the *was_home*/bin directory.

      where *was_home* is the installation directory of the WebSphere Application Server is running.

   b. Use the command for your operating system (assumes DMS as the database name):

      Windows:

      ```
      stopServer.bat DMS_AppServer -user was_admin_userid -password was_admin_password
      ```

      All Device Manager 2.1 application servers must be stopped before attempting to migrate the device data. There must be no other connections to the database during migration.

4. On the system with Device Manager 2.1 database, restore the binary database file (the backed-up database that you copied from the /data/DMS_18_DB_BACKUP directory in step 2.

   Replace the bogus number below (20060519140222) with the timestamp number from the backup file. If you do not have the timestamp number, refer to the DB2 documentation or check the file structure.

   The DB2 restore command below changes the Device Manager 1.8 database name to dms18. This database name will be referenced in migration properties file. The database directories remain the same.

   For Windows, you must be logged in with Administrator privileges.

   ```
   db2 restore database dms user dmsadmin using your_password from /data/DMS_18_DB_BACKUP
   taken at 20060519140222 into dms18 with 2 buffers buffer 1024 ;
   ```

Stopping the WebSphere Application Server

The data migration process requires that the DMS_AppServer be stopped on both systems while the backup occurs. From WebSphere Application Server console on the system with Device Manager 1.8 database, do the following steps:

1. Change to the *was_home*/bin directory.

   where *was_home* is the installation directory of the WebSphere Application Server is running.

2. Use the command for your operating system (assumes DMS as the database name):

   Windows:

   ```
   stopServer.bat DMS_AppServer -user was_admin_user -password was_admin_password
   ```

Running the data migration command

The command to implement the values in the "Preparing a properties file for migration" on page 70 for migrating the device data is run manually from a command prompt. Use the following command, which is located in the *dms_home* directory (DeviceManager/config), to migrate your device data from Device Manager 1.8 to Device Manager 2.1:

Windows:

```
DMSmigrate.bat required_parameter  optional_parameters
```

Note: The migration command requires the use of both JDBC and a DB2 client to perform the migration steps. The DB2 client must have access to both the Device Manager 1.8 and Device Manager 2.1 databases. The JDBC is also used to communicate between the old and new Device Manager databases.

Test the connection and environment, then migrate

It is recommended that you use the DMSmigrate command in the following order:

1. Test your connection to the database with the **–testconnect** parameter.

   If an error occurs, review the properties files or the database setup, fix the error, and rerun this command.

   ```
   DMSmigrate -testconnect
   ```

2. Test the existence of the device classes and the contents of the database with the -testmigrate parameter.

   ```
   DMSmigrate -testmigrate
   ```

   If an error occurs, review the log file to determine which device class is not ready to migrate.

   The possible errors include the specified device class is not installed in Device Manager 2.1 database or the restored Device Manager 1.8 database, or Device Manager 2.1 has unexpected devices, jobs, or software. You should fix the error and rerun this command.

3. Migrate your data with the **–migrate** parameter.

   ```
   DMSmigrate -migrate
   ```

   You can run the DMSmigrate command with one or more device classes. You can change the properties file, and rerun the DMSmigrate command.

   When migrating data, messages are written to the dms_migrate_trace.log file. If there is an error, you should restore the Device Manager 2.1, database, fix the error, and run this command.

List of Parameters for DMSmigrate Command		
Parameter	**Description**	**Required or Optional**
–migrate **–testmigrate** **–testconnect**	Identifies the action. **–migrate** Migrates your data for one or more device classes. **–testmigrate** Connects to the databases, tests the existence of the device classes, and tests the contents of the database (no data is actually migrated). **–testconnect** Tests the connection to the source and destination databases.	required You must use one, but only one, of these parameters with each **DMSmigrate** command.
-file *properties_file*	Identifies the fully-qualified path for the properties file. The default properties file is: *dms_home*/config/DMSmigration.properties	optional
-showtrace	Trace information is written to the log file and directed to std out. The default file for the trace configuration information is: dms_migrate_trace.log	optional
-? -h -help	Displays the usage statement for the command.	optional

Error reporting

If an error occurs when the properties file is run with the command, the migration stops. Trace information is written to the dms_migrate_trace.log file. For example, if a value for a property is not valid, an error message is displayed and the migration stops. Fix the error and run the data migration command again.

SQL exceptions while migrating the data

New database is too small

If you did not make the Device Manager 2.1 database large enough to contain the data being migrated from Device Manager 1.8, you can receive an SQL exception. For example:

```
[exec] SQL3109N  The utility is beginning to load data from file
[exec] "C:\MigrationExports\Win32_JOB_NOTIFICATION.ixf".

[exec] SQL3306N  An SQL error "-289" occurred while inserting a row into the table.

[exec] SQL0289N  Unable to allocate new pages in table space "ISPB_INDEX".
[exec] SQLSTATE=57011
```

In this example message, there is a problem with the ISPB_INDEX tablespace. You must increase the tablespace that holds the Device Manager indexes, then you must increase the tablespace that holds our data (ISPB_DATA).

DB2 warning message

The migration log may contain a DB2 EXPORT warning message. Do not be concerned if you receive a message similar to the DB2 message below because the Device Manager migration does not use the **IMPORT CREATE** mode.

```
[exec] EXPORT TO 'C:\tmp\expath\FILE_PATH.ixf' OF IXF METHOD N (FILE_PATH_ID, PATH) SELECT DISTINCT
(a.FILE_PATH_ID), a.PATH FROM FILE_PATH a, UNMATCHED_FILES f, DeviceIDView d WHERE
a.FILE_PATH_ID=f.INST_PATH_ID AND f.DEVICE_ID=d.DEVICE_ID AND d.DEVICE_CLASS_NAME != 'Wince'
[exec] SQL3104N  The Export utility is beginning to export data to file
[exec] "C:\tmp\expath\FILE_PATH.ixf".

[exec] SQL27984W Some information has not been saved to the PC/IXF file during
[exec] Export. This file will not be supported in Import CREATE mode. Reason code="7,
[exec] 8".

[exec] SQL3105N  The Export utility has finished exporting "10" rows.
```

A DB2 table can be saved by using the export utility and specifying the IXF file format. The saved table (including its indexes) can then be recreated using the import utility. See the DB2 documentation for further information.

After migrating your device data

After you have successfully migrated your device data, complete the following steps:

1. On the system with Device Manager 2.1, database, start the **DMS_AppServer** from **WebSphere Application Server** console.
   a. Change to the *was_home*/bin directory.
      where *was_home* is the installation directory of the WebSphere Application Server is running.
   b. Use the command for your operating system (assumes DMS as the database name):
      Windows:
      startServer.bat DMS_AppServer -user *was_admin_user* -password *was_admin_password*
2. Enable security in WebSphere Application Server for Device Manager 2.1. See "Device Manager server security" on page 109.

3. You must determine how you switch the device connections to the new version of the Device Manager server. Some typical scenarios include the following:
   - Change the DNS and IP addresses so the new server replaces the old server.
   - Redirect the traffic from the old server to the new server.

     The new server name or address can be updated on the client when the device agent is upgraded.
   - Run a device configuration job to update the server name or address on the devices.
4. If appropriate, manually migrate any customized configuration values from the Device Manager server 1.8 to Device Manager server 2.1.
5. Run the following command to drop the restored Device Manager 1.8 database:

   ```
   db2 drop db dms18
   ```
6. The system with Device Manager 1.8 database should have the DMS_AppServer stopped from a previous step. If DMS_AppServer is started, do the following steps on the system with Device Manager 1.8 database:
   a. Change to the *was_home*/bin directory.

      where *was_home* is the installation directory of the WebSphere Application Server is running.
   b. Use the command for your operating system (assumes DMS as the database name):

      Windows:

      ```
      stopServer.bat DMS_AppServer -user was_admin_user -password was_admin_password
      ```
7. After the final migration is complete, the Device Manager 1.8 server must be taken off-line or disabled.
8. It is optional to upgrade the device agents, but it is recommended.

   You can upgrade the devices over a period of time with software distribution jobs. For Device Manager 2.1, there is a change in behavior for the DMS_REDIRECT_TO_DEVICE_MANAGEMENT_SERVER_USING_ORIGINAL_CLIENT_URL environment variable compared to previous releases. For Device Manager 2.1, set this variable to true.

   For prior Device Manager version (versions before 2.1), this environment variable has the following meaning. If you are using prior versions of the device client, use the following information for this environment variable:
   - When this environment variable is set to true, the device is redirected to the Device Manager server using the original device (client) URL. The default value is true.
   - When this environment variable is set to false, the Device Manager server uses the server redirect URL, which is the URL that a device is directed to so work can be performed. The basic flow is that the device agent connects to the server URL as configured on the client and is then redirected to the server redirect URL to actually perform the work. The allowed values are:
     – true
     – false
   - Device clients that are older than 2.1 will need to confirm that DMS_PROXY_HOSTNAME is configured correctly in the Device Manager 2.1 installation for older device clients to connect properly.
9. Replace the older Device Manager console.
10. Migrate the Administration API (optional).

Replacing the Device Manager console

This topic provides instructions on how to replace your older version Device Manager console with the new Device Manager console.

The Device Manager console is a graphical user interface (GUI) for administering device management operations. The installing tasks in this section must be performed on every Device Manager GUI client system.

Note: The Device Manager server must already be installed before installing and starting the Device Manager console.

The Device Manager console must communicate with the Device Manager database server. When the Device Manager console is installed on a different system (Device Manager GUI client system) than the Device Manager database system (unmanaged server with remote database deployment or managed server deployment configuration), the database client software with the JDBC driver will be installed on the system that runs the Device Manager console so data flows between the Device Manager console and the database.

To download and install the Device Manager console:

1. Open a Web browser on the system where you will install the Device Manager console.

   Note: The Device Manager console is only supported on Windows platforms.
2. Point your Web browser to the following Web page:

   `http://server_name/dmserver/DMconsole`

   server_name is the hostname.domain of the system handling the Device Manager server HTTP requests (for example: dmserver.raleigh.ibm.com).
3. Click the **Download DMconsole.zip** message to download the Device Manager console ZIP file.
4. When prompted, save the file to a temporary directory, such as C:\temp.
5. Create a new folder, such as C:\IBM_DM. This new folder is referred to as *console_install_dir*.

   Do not include double-byte characters in the directory name.

   Second and additional instances of the console log stdout and stderr messages to the command shell, and not to the log file.
6. Unzip the DMconsole.zip file into the *console_install_dir* folder.

   The **DMconsole.zip** file contains the files for the Device Manager console and the database client, so the system with the console can access the database on the Device Manager database system.
7. From the *console_install_dir* folder, right-click **DMconsole.bat** and select **Create Shortcut**.
8. Rename the shortcut `Device Manager Console`.
9. Copy the new shortcut to the Windows desktop, the Windows Start Menu, or a folder that contains shortcuts that you use often.

To run the Device Manager console, click the shortcut created in step 9.

You will be prompted for a user id, password, and Device Manager server. Specify the Lotus Expeditor Server administrator id and password and the host name of a Web server that services the Lotus Expeditor Server requests. The hard-coded values are:

Default user ID:	dmadmin
Default password:	dmadmin

Changing the default port number

Port 80 is the default port for IBM HTTP Server used by Device Manager. Before installation of a Device Manager server, the default port for the Web server can be changed. If the port number was changed, then you will have to include the new port number in the *server_name* portion of the URL of the above Web page. For example, you will have to type a URL such as:

`http://dmserver.raleigh.ibm.com:8080/dmserver/DMconsole`

The `:8080` references the changed port number.

Relocating a DB2 database

See this section to rename and relocate the DB2 database to another directory.

Your objective is to rename the DB2 database and relocate the DB2 database to another directory. For example, the database is currently named `dms` and is located in the `/dms/db2` directory, and you want to rename the database to `dms18` and relocate the database to the `/data/tempdm18/dmsdb` directory.

For this scenario to relocate a DB2 database, make the following assumptions:

- The steps provided are one way to relocate a DB2 database. See the DB2 documentation for further information.
- The steps provided to relocate a DB2 database are for a UNIX operating system only.
- You are migrating data from a DB2 database on Device Manager 1.8 system to a DB2 database on a system that will have Device Manager 2.1.
- You have backed up the database for Device Manager 1.8.
- You have copied the binary file (backed-up database) from the `/data/dm1.8_backup` directory on the Device Manager 1.8 system to the `/data/dm1.8_backup` directory on the system that will have Device Manager 2.1.
- On the system that has the DB2 database for Device Manager 2.1, you have restored the binary file (the backed-up database you copied) in the `/data/dm1.8_backup` directory.
- You have not yet installed Device Manager 2.1.

To rename the DB2 database and relocate the database to another directory, complete the following steps:

1. On a system with DB2 database for Device Manager 2.1, restore the binary file (the backed-up database you just copied) in the `/data/dm1.8_backup` directory (For Windows, you must be logged in with Administrator privileges):

   ```
   su - db2inst1          (UNIX only)
   mkdir /data/tempdm18
   db2 restore database dms user dmsadmin using your_password from /data/dm1.8_backup
   taken at 20060519140222 to /data/tempdm18 into dms18 with 2 buffers buffer 1024 ;
   ```

   The DB2 restore command above changes the Device Manager 1.8 database name to dms18 and changes the directories.

2. Gather information about the database by running the DB2 snapshot command:

   ```
   db2start
   db2 update monitor switches using bufferpool on
   db2 activate db dms
   db2 get snapshot for tablespaces on dms
   ```

   Below is a summary of the information that the snapshot command provides. Use this sample as a guide. Your information will be somewhat different. The table spaces which are bold text will be relocated.

SYSCATSPACE	0	/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0000.0 (path)
TEMPSPACE1	1	/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0001.0 (path)
USERSPACE1	2	/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0002.0 (path)
USER_TEMPTS1	**3**	**/db/db2/dms/tempspace (path)**
ISPB_DATA	**4**	**/dmsdb/dms/data001 (file)**
ISPB_INDEX	**5**	**/dmsdb/dms/index001 (file)**
ISPB_DATA16	**6**	**/dmsdb/dms/data002 (file)**
TEMPTS16	**7**	**/db/db2/dms/ts16 (path)**

3. Make a copy of the table spaces that will be relocated. Use the following commands to copy the table spaces to the `/data/tempdm18` directory:

```
db2stop force
cd /data/tempdm18
cp -r /db/db2/dms/tempspace .
cp -r /db/db2/dms/ts16 .
cp /dmsdb/dms/data001 .
cp /dmsdb/dms/index001 .
cp /dmsdb/dms/data002 .
```

4. Use a text editor to create a config.file to identify the new container locations.

   The following example is for UNIX:

```
DB_NAME=dms18
DB_PATH=/data/tempdm18/dmsdb
INSTANCE=db2inst1
NODENUM=0
#CONT_PATH=/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0000.0
#CONT_PATH=/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0001.0
#CONT_PATH=/data/tempdm18/dmsdb/db2inst1/NODE0000/SQL00001/SQLT0002.0
CONT_PATH=/db/db2/dms/tempspace,/data/tempdm18/tempspace
CONT_PATH=/dmsdb/dms/data001,/data/tempdm18/data001
CONT_PATH=/dmsdb/dms/index001,/data/tempdm18/index001
CONT_PATH=/dmsdb/dms/data002,/data/tempdm18/data002
CONT_PATH=/db/db2/dms/ts16,/data/tempdm18/ts16
```

   The following example is for Windows to move from the `c:\dms` directory to the `c:\migration\tempdm18` directory. Assume that the table spaces directory are moved from `c:\dms` to `c:\tempdm18`.

```
DB_NAME=dms18
DB_PATH=C:
INSTANCE=db2
NODENUM=0
CONT_PATH=c:\dms\ispbdata,c:\tempdm18\ispbdata
CONT_PATH=c:\dms\tempspace_user,c:\tempdm18\tempspace_user
CONT_PATH=c:\dms\tempspace_system,c:\tempdm18\tempspace_system
CONT_PATH=c:\dms\ispbindex,c:\tempdm18\ispbindex
```

5. Run the DB2 relocate command using the container locations in `config.file`:

```
db2relocatedb -f config.file
```

6. To verify the relocation, run the DB2 snapshot command and make sure the container names have changed to the `/data/tempdm18/dmsdb` directory:

```
db2 get snapshot for tablespaces on dms18
```

7. Remove the old table space containers:

```
rm -r /db/db2/dms/tempspace
rm -r /db/db2/dms/ts16
rm -r /dmsdb/dms/data001
rm -r /dmsdb/dms/index001
rm -r /dmsdb/dms/data002
```

This completes the steps to relocate the Device Manager 1.8 database to another directory and change the database name to dms18.

Migrating applications written to the Apache SOAP based Administration API

See this section if you use the Device Manager Administration API.

For Device Manager 1.8 the Administration APIs that are based on the Apache SOAP run-time will continue to be supported with Device Manager 2.1. However, the use of the Apache SOAP run-time classes in the Administration APIs will be deprecated in a future release of Device Manager.

It is recommended that you use the Administration API classes that are based on the Web Services for J2EE and JAX-RPC specifications. This is the strategic Web services run-time and API for WebSphere.

Note: If you are not using the Device Manager Administration API, this task can be skipped.

Migration issues

If you want to continue using your existing application that was developed with Device Manager 1.8, consider the following:

- If you used the dmapi.jar in Device Manager 1.8 there are no changes required in your application. However, you must use the dmapi.jar file that is shipped with Device Manager 2.1.

  You cannot use the dmapi.jar file that was shipped with Device Manager 1.8 with Device Manager 2.1.
- If you generate the Administration API from Apache SOAP WSDL files, the XML data that is transported over HTTP uses RPC/SOAP style and encoding. If you use the WSDL files based on the Web Services for J2EE, document/literal style and encoding are used.

Some features perform differently in Device Manager 2.1 than in Device Manager 1.8.

Note: Run your Java code that implemented the Administration API and compare the results. Make appropriate modifications to your code when you migrate to Device Manager 2.1.

Running a standalone Java application (Web services client) now requires a different method of setting up the classpath. WebSphere Application Server 6 supports both managed and unmanaged client applications. To invoke an unmanaged client application that runs outside of a Web container, such as a stand-alone Java application, you should follow the instructions in the WebSphere Information Center section on developing Web service clients. That information describes the supported method of setting the Java classpath. You can also see Building an application using the Administration API in the Device Manager Information Center.

Migration changes that must be made

Changes that must be made when you migrate your Device Manager 1.8 Apache SOAP-based application to Web Services for J2EE include the following:

- The proxy package changes from `soap.proxy` to `com.tivoli.dms.api.proxy`.
- The proxy classes change from JobProxy to JobManagerProxy, and so on.
- The exception that the methods throw changes from SOAPException to com.tivoli.dms.api.DeviceManagerException.
- The default endpoint URL changes from http://*local_host*/dmserver/servlet/rpcrouter to http://*host_name*/dmserver/services/DeviceManagerService (or /JobManagerService, as appropriate for the Web service you are using).
- Hashtable attributes are changed to HashMap in Device.java and Job.java.

  For example: Use `Device.deviceClassAttributesMap` instead of `Device.deviceClassAttributes`.
- Date attributes are changed to Calendar.

  For example: Use `Job.activationTime` instead of `Job.activationDate`.

Client migration

This topic provides instructions on upgrading the network configuration of all existing clients to the Lotus Expeditor Server 6.1.

After the Lotus Expeditor Server 6.1 server comes online, you need to initiate the process upgrading and updating the network configuration of all existing clients to the Lotus Expeditor Server 6.1 server. You have the option of using one or more of the following methods to upgrade your users:

- New Device Manager Services jobs - You can create Device Manager jobs to update the device management server host name configured in existing clients. Perform the following steps to create a job to update the device management server host name:
  1. Start the Device Management console and log into the Lotus Expeditor Server 6.1.

2. Select **Device Classes**.
3. Right click on the device class for your target devices (for instance, Win32, Linux, OSGi) and select **Submit job**.
4. On the target device panel, select the option to target the job to all devices in the device class (for instance, Win32, Linux, OSGi) and select the status of currently enrolled devices.
5. Click **Next** to continue.
6. On the job attribute panel, fill in the following information:

   Job Type: Device Configuration

   Description: *Description of the job* (for example, Update Server host name for Win32 devices)
7. Click **Next** to continue.
8. On the job parameters panel, select DM Account, click on Add Group and fill in the following information:

   Action: Modify

   Name: *Name of the OSGi account on the client. The default is SampleAccount.*

   Address: Device Management server URL with new host name (for instance, http://newhost/dmserver/SyncMLDMServletAuthRequired)
9. Click **Next** to continue.
10. On the **Summary** panel, click **OK**.
11. Click **Close** on the window showing the job was created successfully.

- The Lotus Expeditor administrators can contact users, informing them of the need to:
  - Reconfigure their devices with the new host name and confirm that Device Management is enabled.
  - Install the client upgrade to Lotus Expeditor 6.1 manually.

See Developing Applications for Lotus Expeditor for more information on the client migration.

Final steps for migration

This topic describes how the users on the production WebSphere Everyplace Deployment 6.0 system will be moved onto the Lotus Expeditor Server 6.1 system, after you have performed and tested the migration.

Migration Testing

Before final migration from the WebSphere Everyplace Deployment 6.0 production system to the new Lotus Expeditor Server 6.1, you must confirm success of the following items:

- Installation and configuration of the target Lotus Expeditor Server 6.1 system
- Identification of all components to be migrated
- Successful migration of components from Lotus Expeditor Server 6.0 system to Lotus Expeditor Server 6.1 system
- Testing and confirmation that you have migrated all functionality required and met QA exit criteria using a limited test user subset. Testing should cover:
  - When using the database user registry, ensure the User Management console functions properly. Verify users and groups from the WebSphere Everyplace Deployment 6.0 system can be viewed.
  - Verify security is correctly configured by logging on the WebSphere Application Server administration console with the Lotus Expeditor admin user ID and password.
  - DB2 Everyplace client applications sync successfully with the server.
  - Test clients can register with Device Manager Services, inventory jobs run successfully, and software jobs can be distrusted to test clients.
  - MQ Everyplace applications work successfully.

- Scheduling of a maintenance window of WebSphere Everyplace Deployment 6.0 that enables the final migration to Lotus Expeditor Server 6.1.

Production Migration

At the scheduled WebSphere Everyplace Deployment 6.0 maintenance window, the following occurs:

- The WebSphere Everyplace Deployment 6.0 system will be taken offline, preventing any further changes to the component user data.
- The components targeted for migration will be migrated again from the WebSphere Everyplace Deployment 6.0 system.
- The user data of each component will be the most current available data, and the starting point for the user data of the Lotus Expeditor Server 6.1 system. (All test data currently contained on the Lotus Expeditor Server 6.1 system will be replaced by this migration procedure)
- The Lotus Expeditor Server 6.1 server will be brought online and access will be allowed.
- At this point, WebSphere Everyplace Deployment 6.0 clients will must redirected to the LE Server 6.1 system. There are two options to enable this:
  - Option 1: Update DNS entry for the WebSphere Everyplace Deployment 6.0 host to point to the IP address of the Lotus Expeditor Server 6.1 host. Use this option if you want to recycle the WebSphere Everyplace Deployment 6.0 system and do not want to keep it for emergency switch back. Also, if you are using MQ Everyplace application and you do not want to update the host name used by your MQ Everyplace client applications.
  - Option 2: Update the HTTP server plug-in on the WebSphere Everyplace Deployment 6.0 host to route requests to the Lotus Expeditor Server 6.1 system. Use this option if you want to keep the WebSphere Everyplace Deployment 6.0 system around for emergency switch back. This option is not available if you are using MQ Everyplace applications since MQ Everyplace does not utilize HTTP. To update the HTTP server plug-in on the WebSphere Everyplace Deployment 6.0 system, follow these steps:
    1. Apply the same fix pack level being used by the Lotus Expeditor Server 6.1 system to the WebSphere Application Server 6 HTTP server and plug-in on the original WebSphere Everyplace Deployment 6.0 HTTP server.
    2. Copy the plugin.xml file from the Lotus Expeditor Server 6.1 system to the WebSphere Everyplace Deployment 6.0 system.
    3. Make a backup of the `httpd.conf` file used by the HTTP server.
    4. Edit the `httpd.conf` file used by the HTTP server on the WebSphere Everyplace Deployment 6.0 system and change the **WebSpherePluginConfig** statement to point to the `plugin.xml` file copied from the Lotus Expeditor Server 6.1 system.

Sunsetting of the WebSphere Everyplace Deployment 6.0 Server

If you chose option 1 in the final migration steps above, you can recycle it for other uses after your final migration testing is completed and your Lotus Expeditor 6.1 system is working as desired.

If you chose option 2 in the final migration steps above, you should wait to recycle the 6.0 system after all clients have started using the Lotus Expeditor 6.1 system directly. You can check the HTTP server access log to determine how much traffic your HTTP server is seeing from 6.0 clients. Also, you may schedule a device management job to update the host name for the 6.0 client being managed by the 6.0 server. See “Client migration” on page 82 for instructions on how to configure the host name update job. After the clients connect to the server and process this job, they should connect directly with the Lotus Expeditor 6.1. You can use the Device Management console to view clients that have successfully ran the job.

Switch back to WebSphere Everyplace Deployment 6.0

Option 2 allows the WebSphere Everyplace Deployment 6.0 server to stay intact, allowing for emergency switch back to the previous configuration in the event of a Lotus Expeditor Server 6.1 problem.

Note: Any switch back performed is expected to be done in a short amount of time after the final migration. After clients have migrated to the Lotus Expeditor Server 6.1 client, they will need to reinstall the WebSphere Everyplace Deployment 6.0 client if a switch back is performed.

The procedure for switching back to the WebSphere Everyplace Deployment 6.0 server is:

1. Shutdown the HTTP server.
2. Uninstall any fix pack maintenance applied to the HTTP server and plug-in.
3. Restore the backup of the `httpd.conf` file.
4. Restart the HTTP Server.
5. Start all WebSphere Everyplace Deployment 6.0 component servers.

Administering Lotus Expeditor Server

This topic describes how to administer Lotus Expeditor Server. Lotus Expeditor Server administration tasks include starting and stopping the servers and administering users and groups.

Starting and stopping the servers

This topic describes how to start and stop the Lotus Expeditor Server.

Lotus Expeditor Server is installed and configured with three Web application servers. Before accessing the services of Lotus Expeditor Server, you must start these servers.

Required Windows and Linux operating system privileges

To start or stop the servers, you must have the Windows operating system privileges described in this section. You must also log in to the server, or if running as a service, you must be the **Log On As** user. The access requirements vary depending whether your system is a standalone system, part of a domain, or is the domain controller.

If you are operating on a Linux platform ensure you have root authorization.

For a standalone system on Windows, you must meet the following privileges:

- Be a member of the administrative group.
- Have the **Act as part of the operating system** privilege.
- Have the **Log on as a service** privilege, if the server is running as a service.

On Windows, if your system is a member of a domain and you are logged on to that system as a domain user, you must meet the following privileges:

- Be a member of the domain administrative groups in the domain controller.
- Have the **Act as part of the operating system** privilege in the Domain Security Policy on the domain controller.
- Have the **Act as part of the operating system** privilege in the Local Security Policy on the local system.
- Have the **Log on as a service** privilege on the local system, if the server is run as a service.

For a single Lotus Expeditor Server, you can use the methods described under “Starting and stopping on a single system” on page 88 to start and stop the Lotus Expeditor application servers. If your Lotus Expeditor Server is part of a cluster, you should use the method described under “Starting and stopping clusters” on page 89 to start and stop the Lotus Expeditor application servers.

Note: If you have clustered Lotus Expeditor Server, you may also start and stop servers on an individual node using the methods described under “Starting and stopping on a single system” on page 88. This would only affect the Lotus Expeditor application servers on that node. You must start the WebSphere Application Server node agent before you start or stop Lotus Expeditor application servers from the node.

Important: The servers cannot start automatically when you restart the operating system. Because the coreServices Server must be started before the Device Management and DB2 Everyplace application servers, starting Windows services automatically for each application server is not recommended.

Starting and stopping on a single system

This topic describes how to start and stop the Lotus Expeditor Servers from a single node.

If you have clustered the Lotus Expeditor Server, see "Starting and stopping clusters" on page 89 for information on starting and stopping IBM Lotus Expeditor servers in a cluster.

Note: If you have clustered Lotus Expeditor Server, you may also start and stop servers on a individual node using the methods described in this topic. This would only affect the IBM Lotus Expeditor application servers on that node. You must start the WebSphere Application Server node agent before you start or stop IBM Lotus Expeditor application servers from the node in a cluster.

Lotus Expeditor Server is installed and configured with three Web application servers. Before accessing the User Management console, Device Management services, or DB2 Everyplace, you must start these servers. The Stop Servers command also stops server1, which is the server that provides the WebSphere Application Server Administrative console. See Starting and stopping the servers for information on required operating system privileges needed to start or stop IBM Lotus Expeditor servers.

Note: server1 does not have to be running to access the services of Lotus Expeditor Server.

Methods to start and stop the servers

You can start or stop the servers using one of the following methods.

- From the Windows Start menu:
  - Select **Start → All Programs → Lotus Expeditor → Start Servers**.
  - Select **Start → All Programs → Lotus Expeditor → Stop Servers**.

    Note: This method of stopping the servers prompts for the Lotus Expeditor Administrator ID and password.
- From the System Command prompt:
  - *expeditor_home*/bin/startServers.bat | .sh
  - *expeditor_home*/bin/stopServers.bat | .sh

  Note: This method of stopping the servers prompts for the Lotus Expeditor Administrator ID and password
- From the First Steps console:
  1. Select **Start → All Programs → Lotus Expeditor → First Steps** to launch the First Steps menu.
  2. Then, select the **Start Lotus Expeditor Server** or **Stop Lotus Expeditor Server** option.
- You can start or stop the servers individually from a command prompt using the Application Server startServer and stopServer commands.

  See the following sample commands that starts and stop the Application Server administrative console, server1:
  - *profile_home*/*profile_name*/bin/startServer.bat server1
  - *profile_home*/*profile_name*/bin/stopServer.bat server1 –username *administrator_id* –password *administrator_password*

    Where *profile_home/profile_name* represents the directory where you created the WebSphere configuration profile in which Lotus Expeditor is configured. *administrator_password* represents your Lotus Expeditor Server administrator password.

Notes:

- You might have to issue the stop server command more than one time for the command to take effect.

- It is recommended that you do not use the Windows Service panel to start or stop WebSphere Application Server server1. Instead, use the Lotus Expeditor Server stopServers program shortcut or issue the WebSphere Application Server stopServer command from the command line.

See the following list of Lotus Expeditor application servers. You must start the coreServices Server before you start the Device Management or DB2 Everyplace application servers.

- coreServices
- DMS_AppServer
- IBMDB2eServer

If errors occur starting or stopping the Lotus Expeditor Servers, see Troubleshooting in this information center.

Important: The servers are not started automatically when you restart the operating system. Because the coreServices Server must be started before the Device Management and DB2 Everyplace application servers, creating Windows services to automatically start each application server is not recommended.

Starting and stopping clusters

This topic provides information about how to start IBM Lotus Expeditor services and in what order for a network deployment environment. IBM Lotus Expeditor services are dependent on other services, such as the WebSphere Application Server node agent. You must start the prerequisites services first and then start the IBM Lotus Expeditor services.

In a Network Deployment environment, Lotus Expeditor Servers are installed on nodes managed by a Deployment Manager node. While servers may be started on the individual managed nodes, all nodes might be managed using the Deployment Manager console. The Deployment Manager console provides a central administration point for starting and stopping servers for the entire Network Deployment environment. The following instruction describe how to use the Deployment Manager console to startup the Network Deployment environment.

To start Lotus Expeditor Server:

1. Start the database server and database clients running on the nodes in the cell.
2. Start your LDAP server.
3. If you are using an external Web Server or load balancer, start it.
4. Start the Deployment Manager. Run the following command on the deployment manager system from *dmgr_home*/bin:

   Windows: `startmanager.bat`

   Linux: `./startmanager.sh`
5. Start the node agent on each node that is managed by the Deployment Manager. Run the following command on the node system from *was_profile*/bin:

   Windows: `startnode.bat`

   Linux: `./startnode.sh`
6. Go to http://*dmgr_host*:*port*/ibm/console and log in, where *dmgr_host* is the fully-qualified host name of the Deployment Manager and *port* is the Deployment Manager administration port.
7. Under **Servers**, select **Application Servers**. This will display a list of all application servers in the cell.
8. Start **Core Services**. Go to **Servers** → **Clusters**, select **coreServicesCluster**, and click the **Start** button to start all servers in the cluster. Wait until the coreServicesCluster is started before you proceed.

9. Start the **DB2 Everyplace** servers. Go to **Servers** → **Clusters**, select **IBMDB2eServerCluster**, and click the **Start** button to start all servers in the cluster. Wait until the IBMDB2eServerCluster is started before you proceed.
10. Start the **Device Manager** servers. Go to **Servers** → **Clusters**, select **DMS_AppServerCluster**, and click the **Start** button to start all servers in the cluster. Wait until the DMS_AppServerCluster is started before you proceed.

Alternatively you can start and stop the servers using the start and stop scripts provided on each IBM Lotus Expeditor node, although using the Deployment Manager console is the preferred method. See "Starting and stopping on a single system" on page 88 for information on running the scripts.

Note: The scripts are not cluster-aware and only affect cluster members on that node. Also, you must manually start and stop the node agent if the node has been clustered. Make sure to start the node agent before starting any IBM Lotus Expeditor services.

Verification Steps

To verify the servers are started correctly, go to `http://dmgr_host:port/ibm/console` and log in. Where *dmgr_host* is the fully-qualified host name of the Deployment Manager and *port* is the Deployment Manager administration port. Under **Servers**, select **Application Servers** and ensure all the coreServices, DB2Everyplace, and DeviceManagement application servers show a status of started. In addition, you can test access to the service as follows:

1. Verify Core Services is started.

   Open a Web browser and go to the following URL: `http://access_host : access_port/UserGroupInfoWebService/servlet/rpcrouter` where *access_host* and *access_port* is the host name and port used to gain access to the servers in the cluster. This is normally the hostname of the external Web Server or load balancer. If prompted for a user ID and password enter your IBM Lotus Expeditor administrator user ID and password. The following message is displayed: `SOAP RPC Router Sorry, I don't speak via HTTP GET- you have to use HTTP POST to talk to me.`
2. Verify DB2 Everyplace is started.

   Open a Web browser and go to the following URL: `http://access_host : access_port/db2e/db2erdb` where *access_host* and *access_port* is the host name and port used to gain access to the servers in the cluster. This is typically the host name of the external Web Server or load balancer. If prompted for user ID and password, enter your IBM Lotus Expeditor administrator user ID and password. You should see a message similar to this with the current date and time: `DB2e SyncServer (Mon Jun 26 15:31:16 EDT 2006).`
3. Verify Device Management is started.

   Open a Web browser and go to the following URL: `http://access_host : access_port/dmserver/DMconsole` where *access_host* and *access_port* is the host name and port used to gain access to the servers in the cluster. This is typically the host name of the external Web Server or load balancer. If successful, you are redirected to the information center for Lotus Expeditor. A download page for the Device Manager console is displayed.

Administering users and groups

This topic provides information to help you manage users and groups for Lotus Expeditor Server. Lotus Expeditor Server offers centralized administration of users and user groups, which enables you to define and manage synchronization and device management users.

Each client must have a unique user ID and password to log in to Device Manager and DB2 Everyplace. Lotus Expeditor Server reduces the overhead of creating and managing user IDs by providing integrated user management for Device Manager and DB2 Everyplace. During the installation, Lotus Expeditor Server creates a database for the user registry. Lotus Expeditor Server configures WebSphere Application Server to use this common user registry for all application servers installed on the local system. Because

there is a common user registry, the Expeditor Client services needs only a single user ID to access both DB2 Everyplace services and Device Manager services.

Required administrative user ID and password

The installation program will prompt you to specify an administrative user ID and password. The User Management console, the Device Manager console, and the DB2 Everyplace Mobile Device Administration Center require the Lotus Expeditor Server administrative user ID to log in. Because Lotus Expeditor Server configures security for the local system, the WebSphere Application Server administrative console also requires you to use the Lotus Expeditor Server administrative user ID and password to log in.

Note: The Lotus Expeditor Server administrative ID only supports alphanumeric characters. See "Supported naming conventions" on page 20 for a complete list of supported characters.

Lotus Expeditor Server creates the administrative user ID and password in the database user registry. The administrative user ID that you specify does not have to be a local operating system user.

Required groups

The Lotus Expeditor Server installation creates the following two groups in the local database user registry:

- The **xpdadmins** group contains the Lotus Expeditor Server administrative users.
- The **xpdsyncusers** group contains all DB2 Everyplace synchronization users. All users that need to use DB2 Everyplace synchronization services must belong to exactly two groups: one user group and the **xpdsyncusers** synchronization group. The DB2 Everyplace user group must start with a prefix of `DB2e`.

User Management console

The Lotus Expeditor Server User Management console provides a Web-based interface for the local database user registry. The console functions provide the minimal function required to develop and test DB2 Everyplace and Device Manager applications. You can use the console to create users and groups and manage group memberships for your test users. The User Management console is secured and accessible only by an Lotus Expeditor Server administrative user ID.

You can use the User Management console to complete the following tasks:

- Create an Lotus Expeditor Server user
- Create an Lotus Expeditor Server group
- Assign an Lotus Expeditor Server user to a group
- Change an Lotus Expeditor Server user's password
- Remove an Lotus Expeditor Server user from a group
- Delete an Lotus Expeditor Server user
- Delete an Lotus Expeditor Server group

Launching the User Management console

You can start the User Management console in one of the following ways:

1. From the Windows Start menu:
   - Select **Lotus Expeditor → User Management Console**.
2. From the First Steps menu:
   - Select **Lotus Expeditor → First Steps** to launch the First Steps menu and select **Start User Management Console**.

- Linux users can access the first steps menu from the command line.

3. From a Web browser:
   - Type the following into the address field:

     `http://`*`expeditor_hostname`*`/user-management`

     Where *expeditor_hostname* represents the host name of the server where you installed Lotus Expeditor Server.

After you start the User Management console, you will be prompted to enter your Lotus Expeditor Server administrative user ID and password to log in to the console.

Limitations of the User Management console

The Lotus Expeditor Server User Management console is not intended to be used in a production environment. It has the following limitations:

1. All users and groups must be created by an Lotus Expeditor Server administrative user. Self-registration is not supported.
2. The User Management console is intended to enable you to create users and groups for a development environment. Bulk load of users and groups is not provided.
3. The user attributes supported are user ID, password, first name, and last name.
4. After you create the user, the only user attribute you can edit is the password.
5. Nested groups are not supported.
6. The User Management console is not intended to scale to a large number of users. You should upgrade your server configuration to use an LDAP server before starting a test environment or pilot with more than 50 users.

Upgrading to LDAP

When you are ready to support more than 50 users, you can upgrade Lotus Expeditor Server to use an LDAP server as the user registry. After you perform this upgrade, the User Management console is disabled. You must use the LDAP server management tools to manage users and groups.

The users and groups that you created in the local database user registry with the User Management console will not be migrated to the LDAP server. After you have upgraded to LDAP, you will *not* be able to revert back to the local database user registry.

For more information on using LDAP as the user registry see topic Configuring your LDAP server.

Updating the configuration

This topic describes how to use the Configuration Wizard to update your server configuration.

The Configuration Wizard supports the following configuration update scenarios:

- Update the Lotus Expeditor Server configuration to use Active Directory 2003 as the user registry. The Configuration Wizard will not migrate the users in the local database user registry to Active Directory 2003.

  Important: Lotus Expeditor Server does not support converting your user registry from Active Directory 2003 back to a local DB2 database.
- Change the Lotus Expeditor Server administrator password in the server configuration.
- Change the database administrator password in the server configuration.

Review the following topics to upgrade your Lotus Expeditor Server configuration.

Note: Before you run a configuration task, use the WebSphere Application Server **backupConfig** command to save the configuration. If a failure occurs during the configuration task, you can use the **restoreConfig** command to restore the WebSphere Application Server configuration.

Command line support is provided for the following configuration update scenarios:

- "Upgrading to an LDAP user registry" on page 96
- "Updating the Lotus Expeditor Web server" on page 102

Using the Configuration Wizard

The Configuration Wizard provides an interface to allow certain features of your Lotus Expeditor Server environment to be reconfigured. This topic describes the options available on the Configuration Wizard.

After installation, you can open the Configuration Wizard window in one of the following ways:

- Select Configuration Wizard from the First Steps application menu.
- Run the following command:
  - Windows: *expeditor_home*\Expeditor\config\config.bat
  - Linux: *expeditor_home*/Expeditor/config/config.sh

    Where *expeditor_home* is the directory where you installed Lotus Expeditor Server.
- Windows only: Select **Start** → **All Programs** → **Lotus Expeditor** → **Configuration Wizard**.

Use the Configuration Wizard to access the following options:

Upgrade to Active Directory 2003

Lotus Expeditor Server is installed and configured with a database user registry. This option allows you to reconfigure Lotus Expeditor Server to use Active Directory 2003 server as the user registry. See "Upgrading to Active Directory 2003" on page 98 for details.

Update existing IBM Lotus Expeditor Administrator's Password

This option allows you to update the Lotus Expeditor Server administrator's password. See "Updating the Lotus Expeditor Server administrator password" on page 100 for details.

Update existing Database Administrator Password

This option allows you to update the Lotus Expeditor Server database administrator's password. See "Updating the database administrator password" on page 101 for details.

Advanced Clustering Services

This option allows you to prepare an Lotus Expeditor Server for clustering, create the Lotus Expeditor Server cluster, and the response file used when adding additional servers to an existing cluster. See "Creating a cluster" on page 41 for details.

Configuring the LDAP server

IBM Lotus Expeditor supports a configuration upgrade to an LDAP server as the user registry. The LDAP server must be installed, configured, and running before you can perform the upgrade. See the information in this topic for the required LDAP configurations.

IBM Lotus Expeditor reduces the amount of time needed to create and manage user IDs by providing integrated user management for Device Manager and DB2 Everyplace. Expeditor client services need only a single user ID to access the services of both DB2 Everyplace and Device Manager.

During installation, IBM Lotus Expeditor creates a database for the user registry. The database user registry is intended for use in a development environment. It is not intended to scale into a production environment with a large number of users and groups. When you are ready to support a larger number of users, you can upgrade the server configuration to use an LDAP server as the user registry. After performing this upgrade, the User Management console is disabled. You must use the LDAP server's management tools to manage users and groups.

You must perform special configuration steps to enable LDAP to work with Lotus Expeditor Server. Use the following topics as a guide when configuring your directory server.

General directory requirements

This topic discusses general directory requirements.

See the following list of general directory requirements:

- The LDAP cannot be installed on the same system as IBM Lotus Expeditor. You must install and configure the LDAP server on a remote server before you configure Lotus Expeditor Server.
- The user login name in LDAP is used to authenticate to the Lotus Expeditor Server services. When you configure DB2 Everyplace synchronization and the Enterprise Management agent in the client, specify the user logon name, not the distinguished name (DN).

  Note: The attribute for the user logon name will vary depending on the type of LDAP server being used. For example, the attribute is known as the sAMAccountName attribute in Active Directory 2003. Although the user authenticates with the login name, the distinguished name (DN) might display in component trace files.
- Expeditor Server requires read-only access to the directory. Because the Expeditor Server does not write to the LDAP directory, the users and groups required by Expeditor Server are not created during the upgrade process. You must create the required users and groups in the directory before you begin the upgrade process. For more information, see Required Users and Groups.

  Note: To enable Lotus Expeditor Server to connect to the directory, do not enable Simple LDAP Bind operations.
- The Lotus Expeditor Server LDAP upgrade process does not support Secure Sockets Layer (SSL) connections to the LDAP server. If you want to secure the connection between the LDAP server and WebSphere Application Server, you can do so after you have successfully upgraded the server configuration to use a LDAP server.
- You must organize the directory tree so that you can configure Lotus Expeditor Server to find users and their group memberships. For more information see Directory organization requirements.

Directory organization requirements

IBM Lotus Expeditor must be able to search the directory for users and their group memberships. This topic discusses the requirements for organizing your directory and describes how to select the appropriate search starting points in your directory tree to use in the configuration.

To successfully configure Lotus Expeditor Server for LDAP, you must configure the search paths at a point in the directory tree that will cover all of the users. Specifically, you must provide the following directory search path information during the upgrade process:

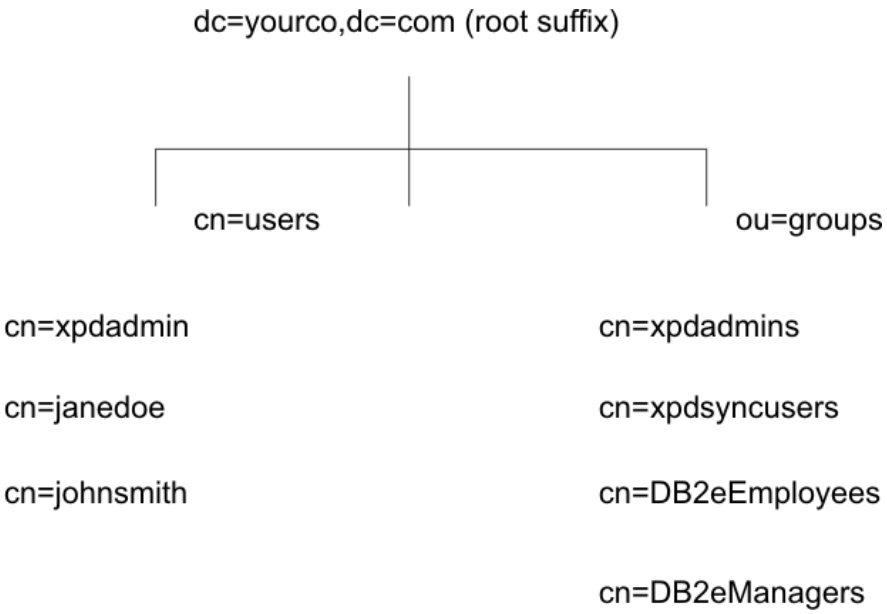
- the directory root suffix,
- the top level users container under the directory suffix, and
- the top level groups container under the directory suffix.

The LDAP upgrade process supports two separate directory containers under the root suffix for users and groups. In most LDAP servers, the user container and group container can be in the same directory container in LDAP. If the group container differs from the user container, you can nest groups under the

top level group container configured for Lotus Expeditor Server. Lotus Expeditor Server does not support the configuration of multiple containers for users or groups.

The sample in the following graphic shows the users and groups in separate containers.

- The directory root suffix is dc=yourco,dc=com.
- The users container is cn=users and the groups container is ou=groups.
- The fully-qualified distinguished name (DN) for the xpdadmin user is cn=xpdadmin,cn=users,dc=yourco,dc=com.
- The fully-qualified DN for the xpdadmins group is cn=xpdadmins,ou=groups,dc-yourco,dc=com.



Required users and groups

This topic provides instructions to help you configure the users and groups required by the LDAP server.

Lotus Expeditor Server features require an administrative user, an administrative group, and a synchronization users group. The Lotus Expeditor Server administrative user also serves as the DB2 Everyplace and Device Management administrator. Because Lotus Expeditor Server does not write to the directory, the administrative user does not have to be an LDAP administrator. The administrative user can be any user in the configured users container that is a member of the Lotus Expeditor Server administrators group. To create new users and groups to administer Lotus Expeditor Server and features, use your directory server administration tools.

The administrative user and the following groups must exist in your LDAP server before running the configuration program. You can customize the administrative ID, administrator group name, and synchronization users group during the LDAP upgrade process.

- Lotus Expeditor Server administrator, such as xpdadmin.
- Lotus Expeditor Server administrator group, such as xpdadmins. (IBM Lotus Expeditor administrator must belong to this group.)
- DB2 Everyplace synchronization group, such as xpdsyncusers. (All DB2 Everyplace synchronization users must belong to this group.)
- At least one DB2 Everyplace user group that begins with the prefix “DB2e”, such as DB2eEmployees.

  Notes:

  – Administrator IDs require that the value for common name (for instance, CN) be the same as the value for account ID (for example, logon name). You can configure this by setting the first name to the value of account ID and leaving the last name and middle initial blank.

– For information on the allowed values for the required users and groups, see “Supported naming conventions” on page 20.

LDAP server configuration checklist

During the configuration upgrade to an LDAP server, you must provide information. Use this checklist to gather the information you need about the directory server to upgrade the configuration.

Print the checklist and use it to help you prepare for upgrading to an LDAP server.

____ Install an LDAP server, unless you plan to use an existing LDAP server. The LDAP server cannot reside on the same system as IBM Lotus Expeditor.

____ The LDAP server must be configured to allow a non-SSL connection during the Lotus Expeditor Server configuration update.

____ Access the LDAP server from a remote system using a LDAP browser to ensure that you can connect to the directory remotely before you start the configuration upgrade. Do not use the Microsoft LDAP browser because the Microsoft LDAP browser does not detect potential connectivity problems between the LDAP server and the Lotus Expeditor server. Freeware LDAP browsers are available from the Web.

____ Determine the suffix, user container, and group container for the Lotus Expeditor Server users. See Directory organization requirements for more information.

____ Create the required user groups and users in your LDAP server before you begin the configuration upgrade. See Required Users and Groups for more information.

Gather the following information for use when upgrading the configuration to the LDAP server.

____ Fully-qualified host name of the system where you installed the LDAP server
____ Port number used to access the LDAP server; the default value is 389
____ Root suffix of directory tree
____ Lotus Expeditor Server administrative ID
____ Password for the Lotus Expeditor Server administrative ID
____ Lotus Expeditor Server administrative group name
____ Lotus Expeditor Server synchronization user group name
____ Name of the users container
____ Name of the groups container

____ When you provide input parameters during the upgrade process, enter user registry Relative Distinguished Name (RDN) prefixes, such as cn=, uid=, or ou=, in lowercase letters. Uppercase or mixed case letters can cause problems with subsequent case-sensitive queries.

Upgrading to an LDAP user registry

This topic describes how to modify the Lotus Expeditor Server user registry configuration using an LDAP server.

Review the following topics to better understand the process of upgrading the server configuration to use an LDAP as the common user registry.

Upgrading to a custom LDAP server

This topic provides information on how to upgrade the Lotus Expeditor Server configuration to use an LDAP server other than Active Directory 2003 as the common user registry.

For a list of supported LDAP servers, see “Supported hardware and software” on page 14. If you are using Active Directory 2003, see “Upgrading to Active Directory 2003” on page 98.

Use the information that you completed in the “LDAP server configuration checklist” on page 96 as input in the configuration process.

Important: Before you begin this configuration upgrade, verify that you have read and understand the “Existing user data considerations” on page 99. After you have successfully configured Lotus Expeditor Server for the LDAP server, you cannot modify the user registry configuration.

Use the following steps to upgrade to a custom LDAP:

1. Stop the Lotus Expeditor application servers before beginning the upgrade. For more information, see “Starting and stopping the servers” on page 87.
2. Back up the configuration using the WebSphere Application Server **backupconfig** command.
3. Reconfigure WebSphere Application Server Security to use the LDAP server. For instructions, see the WebSphere Application Server Information Center at: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_ldap.html.
4. After configuring WebSphere Application Server for LDAP, restart server1 and ensure that you can log into the WebSphere Application Server administration console.

   Note: If you have problems logging into the WebSphere Application Server console, you can restore your previous WebSphere Application Server configuration using the **restoreconfig** command.
5. Modify the *expeditor_home*\Expeditor\core\config\ldap\templates\wmm.xml template for your LDAP configuration as follows:
   a. Replace every `o=YourDomain` with your LDAP domain.
   b. Replace `cn=yourbindid` with the ID of the user to bind to LDAP.
   c. Replace `yourbindPassword` with the password of the user to bind to LDAP.
   d. Replace `your.ldap.server` with the fully-qualified host name for your LDAP server.
6. Back up the existing *was_profile_home*\config\wmm\wmm.xml file.
7. Copy the *expeditor_home*\Expeditor\core\config\ldap\templates\wmm.xml file to *was_profile_home*/config/wmm/wmm.xml.
8. Modify the *expeditor_home*\Expeditor\core\config\ldap\ldap.properties file as follows:
   a. Ensure that `ldap.admin.uid` is the short name of the Lotus Expeditor Client administrator account.
   b. Ensure that `ldap.admin.password` is the password for the Lotus Expeditor Client administrator account.
   c. Ensure that `ldap.admin.group` is the short name for the Lotus Expeditor Client administrator’s group.
   d. Ensure that `ldap.sync.group` is the short name for the sync group for DB2e.
9. To start the core services application server, run the following command:
   - Windows: *was_profile_home*\bin\startServer.bat coreServices
   - Linux: *was_profile_home*/bin/startServer.sh coreServices

   .
10. To verify the WMM settings, run the following command. If this script has errors, check the wmm.xml and ldap.properties files for errors. Also ensure that the core services server is running.
    - Windows: *expeditor_home*\Expeditor\core\config\ldap\verifyLDAP.bat
    - Linux: *expeditor_home*/Expeditor/core/config/ldap/verifyLDAP.sh
11. To apply the new LDAP settings to the Lotus Expeditor Server components, run the following command:

- Windows: *expeditor_home*\Expeditor\core\config\ldap\registerCustomLDAP.bat
- Linux: *expeditor_home*/Expeditor/core/config/ldap/registerCustomLDAP.sh

Note: If there are problems running this script, use the **–Ddebug=true** command line option to view additional information about the failure.

12. Restart the Lotus Expeditor servers. See "Starting and stopping the servers" on page 87 for information on stopping and starting the servers.

Upgrading to Active Directory 2003

This topic provides information to use the Configuration Wizard to upgrade the Lotus Expeditor Server configuration to use Active Directory 2003 as the common user registry.

Use the information that you completed Checklist for Active Directory 2003 as input in the Configuration Wizard.

Important: Before you begin this configuration upgrade, verify that you have read and understand Existing user data considerations. After you have successfully configured Lotus Expeditor Server for Active Directory 2003, you cannot modify the user registry configuration again.

Perform the following steps to upgrade to Active Directory 2003:

1. Stop all of the Lotus Expeditor Server application servers before beginning the upgrade to Active Directory 2003. For more information see Start and stopping the servers.
2. Run the WebSphere Application Server **backupConfig** command to back up the WebSphere Application Server configuration.
3. To launch the Configuration Wizard, see "Using the Configuration Wizard" on page 93.
4. Click **Next** on the **Welcome** panel to continue the configuration. The **Configuration Mode Selection** panel is displayed.
5. Select **Upgrade to Active Directory 2003**. Click **Next**. The **Directory Connection Server Information** panel is displayed.
6. 6. Complete the following fields:
   - **Host name**: Specify the fully-qualified host name of the Active Directory 2003 server you want to use.
   - **Port**: Specify the port number of the Active Directory 2003 server you want to use.
   - **Suffix**: Specify the directory suffix, such as, `dc=yourco,dc=com`, that will serve as the root directory for your user registry.
   - **IBM Lotus Expeditor Administrator ID**: Specify a directory administrator user ID that will be used to access the directory. Because the directory is accessed in read-only mode, this user does not have to be an Active Directory 2003 administrator. The administrator ID must be a fully-qualified distinguished name (DN).
   - **IBM Lotus Expeditor Password**: Specify a password for the directory user specified for the Lotus Expeditor Server administrator user ID.
7. Click **Next** to proceed to the **User and Groups Information** panel.

   Note: The Configuration Wizard connects to the directory using the information collected on the panel. You cannot proceed if any of the values are not validated.
8. Complete the following fields:
   - **Synchronization User Group Name**: Specify the name of the group in Active Directory 2003 where the Lotus Expeditor Server database synchronization users reside.
   - **Administrative Group Name**: Specify the name of the group in Active Directory 2003 where the Lotus Expeditor Server administrator user ID resides.
   - **User container**: Specify the name of the container in Active Directory 2003 where the users reside.

- **Group container**: Specify the name of the container in Active Directory 2003 where the groups reside.

9. Click **Next** to proceed to the **Configuration Summary** panel.

   Note: The Configuration Wizard attempts to access the user and group containers using the information collected on the panel. You cannot proceed if any of the values are not valid.

10. Review the changes that you configured and click **Next**.

    The **Configuration Progress** panels are displayed.

11. When the configuration completes, click **Finish**.

Note: If the configuration task fails, use the WebSphere Application Server **restoreConfig** command to restore the WebSphere Application Server configuration.

Existing user data considerations

This topic discusses considerations for the existing Lotus Expeditor Server user data. Review the information in this topic before you upgrade to an LDAP server.

The database user registry created during the Lotus Expeditor Server installation is intended to support a development environment. The only information Lotus Expeditor Server maintains in the user registry is the userid, password, first name, and last name. The users and groups that have been created in the database user registry with the User Management console will **not** be migrated to the LDAP server when you upgrade the configuration.

Lotus Expeditor Server interfaces with the directory in read-only mode and does not create users and groups. If it is important to recreate in the LDAP server the existing database registry users and groups, you must do so before updating the server configuration to use the LDAP server. The LDAP configuration upgrade deletes the user and group information maintained in the database user registry.

If you have synchronized data or distributed software jobs for users in the local database user registry, there is data associated with those users in the DB2 Everyplace and Device Manager databases. When you log in to the DB2 Everyplace Mobile Device Administration console, the list of users and groups will be reset based on the new LDAP registry. You will be prompted to delete the old users and groups that existed in the database. The DB2 Everyplace subscriptions and subscription sets still exist with the exception that the group to subscription set association is deleted. You must reassociate the groups with the subscription sets to synchronize the data to the LDAP users.

Device Manager keeps track of the owner of a device by storing the user ID in the Device Manager database. If a currently enrolled device attempts to connect to the Device Manager using a different user ID than the owner, the connection is not allowed. Therefore, the administrator should verify that for each device that is enrolled in Device Manager, the owners user ID exists in the LDAP server. The administrator can either modify the owner of the device using the Device Manager console or delete the device and allow it to re-enroll later.

Important: Lotus Expeditor Server permits you to upgrade to an LDAP as the user registry. However, after you have upgraded to LDAP, you will **not** be able to return to the local database user registry.

Reconfiguring the DB2 Everyplace VNurse sample

After you update your configuration from the local database user registry to LDAP, see this topic for instructions to reconfigure the VNurse sample provided by DB2 Everyplace.

Attention: The VNurse sample configuration is automatically set up only in the single server with local database installation scenario.

Complete the following steps to reconfigure the VNurse sample:

1. Create the users and groups in the LDAP server that were created in the original configuration in the local database user registry.
   a. Create users named: `nurse1`, `nurse2` and `nurse3`.
   b. Create a group whose name begins with `DB2e`.
2. Verify that the `nurse1`, `nurse2`, and `nurse3` users are members of both groups.
3. (Optional) Depending on whether or not you created the users and groups in the LDAP server after opening the DB2 Everyplace Mobile Devices Administration Center console, you might be required to refresh the list of users and groups in the Users and Groups folders in the console. To refresh the list of users and groups, log in to the console and right-click on the Users and Groups folders. Then, select **Refresh WPS LDAP Users**.
4. Edit the SUBSCRIPTION_SET1 subscription set in the console to assign the subscription set to the `DB2e` group you created. To edit the SUBSCRIPTION_SET1 subscription set, see Making the subscription set available to a group.

   You can now successfully perform a DB2 Everyplace synchronization with the VNurse sample.

Updating the Lotus Expeditor Server administrator password

This topic describes how to update the Lotus Expeditor Server administrator password in the server configuration.

Important: Follow these steps in order. If you have upgraded your configuration to LDAP, you must stop the servers before you change your password in LDAP. If your password has expired, end the server processes or restart the system to verify that the servers are stopped.

Follow these steps to update the Lotus Expeditor Server administrator password.

Attention: If you are operating in a clustered environment, perform these steps on every node.

1. Stop the IBM Lotus Expeditor application servers before beginning the administrator password update. See Start and stopping the servers for instructions.
2. If the server is configured to use LDAP as the user registry, change the Lotus Expeditor Server administrator password in LDAP.
3. **Windows only**: If you created services for any WebSphere Application Server using the **WASService** command, you must update the password for the `stopArgs`. For more information about the **WASService** command, see the WebSphere Application Server Information Center. If you specified to run the application server process as a service during WebSphere Application Server profile creation, you must update the password for `server1`.
4. Launch the Configuration Wizard. See “Using the Configuration Wizard” on page 93 for further instructions.
5. Click **Next** on the **Welcome** panel to continue the configuration. The **Configuration Mode Selection** panel is displayed.
6. Select **Update IBM Lotus Expeditor Administrator Password** and click **Next**. The Lotus Expeditor Server login panel is displayed.
7. Complete the following fields:
   - **Lotus Expeditor Server Administrator ID**: Specify the Lotus Expeditor Server administrator user ID. If you upgraded your configuration to LDAP, specify the administrator ID that exists in that directory.
   - **Password**: Specify the password.
   - **Confirm password**: Re-type your Lotus Expeditor Server administrator password for confirmation.

   Note: You are prompted to confirm your password only if the user registry is a local database. If you are using a remote user registry, you are not prompted to confirm your password.
8. Click **Next**. The **Configuration Summary** panel is displayed.

9. Review the changes that you configured and click **Next** to start the configuration update. The progress bar indicates the status of the server configuration update.
10. When the configuration completes, click **Finish**. You can verify the server configuration using the **Verify Installation** option from the First Steps menu. For more information, see Using the First Steps console.

Updating the database administrator password

This topic describes how to update the database administrator password.

Important: Follow these steps in order. You must stop the servers before you change your password in DB2. If your password had expired you might need to terminate the server processes or restart the system to verify that the servers are stopped.

Note: The Lotus Expeditor Server update process for the DB2 administrator password does not automatically update DB2 Everyplace subscriptions configured with the same administrator ID and password. You must modify db administrator passwords manually for any existing subscriptions.

Use the following steps to update the database administrator password.

Attention: If you are operating in a clustered environment perform these steps on every node.

1. Stop all of the Lotus Expeditor Server application servers before beginning the database administrator password change. For more information, see Start and stopping the servers.
2. On the database server, change the database administrator password in the local operating system and in DB2. Verify that you have changed the password in the DB2 Windows services that use this user ID to log in, and verify that those services can start successfully after the password has been changed.
3. Launch the Configuration Wizard. See "Using the Configuration Wizard" on page 93 for further instructions.
4. Select a language and click **OK**.
5. Click **Next** on the **Welcome** panel to continue the configuration. The **Configuration Mode Selection** panel is displayed.
6. Select **Update existing Database Administrator Password** and click **Next**.
7. Specify the new password that you want to assign to the database administrator.
8. Click **Next**. The **Configuration Summary** panel is displayed.
9. Review the changes that you configured and click **Next** to start the configuration update. The progress bar indicates the status of the server configuration update.
10. When the configuration completes, click **Finish**.
11. Update the password used to access the DB2e Message Store Database. Select one of the following:
    - Windows:
      a. Open a command window.
      b. Change to the *expediter_home*\DB2Everyplace\Server\bin directory.
      c. Run **dsysetproperty.bat DSYIdflt messagestore.db.pswd=*new_password*** where *new_password* is the new database administrator password.
    - Linux:
      a. Open a command window.
      b. Switch to the database instance user. For example, run **su - db2inst1**
      c. Change to the /home/db2inst1/db2everyplace91/Server/bin directory, where db2inst1 is database instance user name.
      d. Run **./dsysetproperty.sh DSYIdflt messagestore.db.pswd *new_password***, where *new_password* is the new database administrator password.

Note: Use a space between **messagestore.db.pswd** and the new password, not an equal sign.

12. *Optional*: Verify the server configuration using the **Verify Installation** option from the First Steps menu. For more information, see "Using the First Steps console" on page 46.

Updating the Lotus Expeditor Web server

This topic describes how to update the Web server used by a Lotus Expeditor Server installation (standalone environment) or add an additional Web server (clustered environment).

By default,Lotus Expeditor Server is configured to use the local IBM HTTP Server installed on the Lotus Expeditor Server system. If you cluster Lotus Expeditor Server, the cluster is configured by default to use the IBM HTTP Server on the primary Lotus Expeditor Server node.

Standalone environment:

To update the Web server used in a standalone environment, follow these steps:

1. Install a new Web server. For information about supported Web servers, see "Supported hardware and software" on page 14.
2. Install the WebSphere Application Server plug-in. When prompted for the Web server name, use the same name as the existing local IBM HTTP Server.
3. Create an administrator user ID and password in the *ihs_root*/conf/admin.passwd file, where *ihs_root* specifies the IBM HTTP Server installation directory. For example:

   ```
   c:\ws\ihs60\bin\htpasswd -cb c:\ws\ihs60\conf\admin.passwd adminUser adminPassword
   ```

4. Log on to the WebSphere Application Server administration console and browse to **Servers > Web servers**.
5. Click the existing Web server definition.
6. Enter Web server properties as follows:
   - **Type**: Specifies the Web server vendor type.
   - **Port**: Specifies the existing Web server port. The default value is **80**.
   - **Installation Path**: Specifies the Web server installation path. This field is required for IBM HTTP Server only.
   - **WINDOWS Service Name**: Specifies the Windows operating system service name of the Web server. The default value is **IBMHTTPServer6.0**.
   - **Use secure protocol**: Use the HTTPS protocol to communicate with the Web server. The default value is **HTTP**.
   - **Plug-in installation location**: Specifies the directory path where the plug-in is installed.
7. Enter the remote Web server properties. The properties for the IBM HTTP Server administration server are as follows:
   - **Port**: Specifies the administration server port. The default value is **8008**.
   - **User ID**: Specifies the user ID that is created using the htpasswd script.
   - **Password**: Specifies the password that corresponds to the user ID created with the htpasswd script.
   - **Use secure protocol**: Use the HTTPS protocol to communicate with the administration server. The default value is **HTTP**.
8. Save the configuration changes.
9. Stop all Lotus Expeditor Server application servers. For instructions, see "Starting and stopping the servers" on page 87.
10. Edit the *expeditor_home*/Expeditor/core/config/webserver/webserver.properties file and set **remote.webserver.hostname** to the fully-qualified host name of the new Web server system.
11. From a command prompt, enter the following command to update the Lotus Expeditor Server configuration to use the new Web server host name:

On Linux systems: **./updateWebServer.sh**

On Windows systems: **updateWebServer.bat**

12. Restart the Lotus Expeditor Servers. For instructions, see "Starting and stopping the servers" on page 87.

Clustered environment:

Before you begin:

Select from the following scenarios:

- If you are moving a Web server, or adding a load balancer to control incoming traffic to the Web servers, complete *all* steps in this procedure.
- If you are adding an additional Web server to supplement an existing configuration, complete steps 1 through 5 only.

To update the Web server in a clustered environment, follow these steps:

1. Install a new Web server. For information about supported Web servers, see "Supported hardware and software" on page 14.
2. Install the WebSphere Application Server plug-in.
3. See information about configuring a remote Web server in the WebSphere Application Server Information Center.
4. Log on to the WebSphere Application Server administration console and map the following Lotus Expeditor Server Enterprise Applications to the new Web server and the cluster:
   - Map the DB2 Everyplace Enterprise 9.1 application to the Web server and the IBMDB2eServerCluster.
   - Map the DMS_WebApp application to the Web server and the DMS_AppServerCluster.
   - Map the following applications to the Web server and the CoreServicesCluster:
     - User Group Info Web Service
     - User Management Servlet
     - wmmApp

   See information about mapping modules to servers in the WebSphere Application Server Information Center.

   Note: If you have other applications installed, you can also map them to the new Web server using the same procedure.
5. From the WebSphere Application Server administration console, regenerate and propagate the Web server plug-in.
6. Stop all Lotus Expeditor application servers. For instructions, see "Starting and stopping the servers" on page 87.
7. If the Web server will be used as the external IP address to access the Lotus Expeditor servers in the cluster, complete the following steps on each Lotus Expeditor Server system:
   a. Edit the *expeditor_home*`/Expeditor/core/config/webserver/webserver.properties` file and set **remote.webserver.hostname** to the fully-qualified host name of the new Web server system.

      Note: When two or more Web servers are involved, set up a load balancer to control incoming traffic to the Web servers. Also make sure to use the load balancer external IP address.
   b. From a command prompt, enter the following command to update the Lotus Expeditor Serverconfiguration to use the new Web server host name:

      On Linux systems: **./updateWebServer.sh**

      On Windows systems: **updateWebServer.bat**

8. Restart the Lotus Expeditor servers. For instructions, see “Starting and stopping the servers” on page 87.

Securing Lotus Expeditor Server

To protect data transferred between the Lotus Expeditor Server and clients, the HTTP server, the application server, and the Lotus Expeditor Client must be secure. Security will not be enabled on your servers by default. This topic describes how to enable Secure Sockets Layer (SSL) security on IBM HTTP Server and WebSphere Application Server. For more information or other implementations, see your HTTP server and WebSphere Application Server documentation.

The following topics describe how to enable SSL between the Lotus Expeditor Server client and server. After you enable security, Lotus Expeditor Server encrypts all requests, including logging in to the user management console. However, you must complete additional steps to configure the Device Manager and DB2 Everyplace administration consoles to use SSL. To secure Lotus Expeditor Server, complete the steps in the following sections in the order listed.

Obtaining a certificate

This topic provides instructions on how to obtain a certificate from a Certificate Authority for the Lotus Expeditor Server.

Production Web servers must use signed certificates purchased from a Certificate Authority that supports IBM HTTP Server, such as VeriSign or Thawte. You can use the IKEYMAN Key Management utility provided with IBM HTTP Server to create self-signed certificates. Self-signed certificates are useful for test purposes but should not be used in a production Web server.

To create a self-signed certificate, perform the following steps:

1. Use the IKEYMAN Key Management utility to create a new key database of type CMS.
2. Save the password to a file.
3. Create a new self-signed certificate in this keystore.
4. Extract the certificate that you just created to a file.

   Later, you will import this file into the Application Server Virtual Machine truststore file.

   Tip: See the SSL Certificates topic in the IBM HTTP Server Information Center for detailed instructions.

Configuring SSL

This topic describes how to secure your Lotus Expeditor Server and clients by configuring SSL.

Secure Socket Layer (SSL) technology allows Web browsers and Web servers to communicate over a secure connection. In this secure connection, the data that is being sent is encrypted before being sent and then is decrypted upon receipt and before processing. Both the browser and the server encrypt all traffic before sending any data. Review the following topics to better understand how to configure SSL.

Configuring the IBM HTTP Server for SSL

This topic provides instructions on configuring the IBM HTTP Server for SSL.

To configure the IBM HTTP Server for SSL, you must configure port 443 to accept HTTPS requests. Complete these steps to configure the IBM HTTP Server for SSL:

1. Open the httpd.conf configuration file so that you can enable the SSL directives.
2. Change any ″Listen″ directives to 443 from 80.

3. Uncomment or add the `LoadModule ibm_ssl_module modules/mod_ibm_ssl.so` configuration directive.
4. Create an SSL virtual host stanza in the httpd.conf file using the examples and directives documented in the IBM HTTP Server Information Center.

   Tip: See Quick start: Setting up Secure Sockets Layer.

   Note: Use a colon (:) instead of a period (.) before the port number as documented in Quick start: Setting up Secure Sockets Layer. For example, type **<VirtualHost *:443>** instead of **<VirtualHost *.443>**.
5. Save and close the IBM HTTP Server httpd.conf configuration file.
6. Restart the IBM HTTP Server.
7. Open a browser window and point to https://*hostname* to verify that the changes you made are functioning properly. (Where *hostname* refers to the host name of your IBM HTTP Server.)

Configuring WebSphere Application Server for SSL

This topic provides instructions on how to configure the WebSphere Application Server plug-in for the Web server to forward SSL requests to WebSphere Application Server.

You must configure the WebSphere Application Server plug-in for the Web server to forward SSL requests to WebSphere Application Server. Complete the following steps to configure the WebSphere Application Server for SSL:

1. Update the virtual host list for WebSphere Application Server to include the correct host name and SSL port number. Then regenerate the plug-in configuration. See "Adding a host alias" for instructions.
2. If you are using a self-signed certificate, add the certificate file that you created in "Obtaining a certificate" on page 105 to the Application Server Virtual Machine truststore file. See "Importing a self-signed certificate to the Application Server" on page 107 for instructions.

Adding a host alias

Complete the following steps to add a host alias for SSL port 443 to WebSphere Application Server:

1. Open the WebSphere Application Server Administrative Console and click **Environment** → **Virtual Hosts**.
2. Select the default host.
3. Select **Host Aliases** under **Additional Properties** and click **New** to create a host alias.
4. Specify 443 in the **Port** field under **General Properties** and click **Apply**.
5. Click **Save** to apply the changes to the Application Server master configuration.
6. To regenerate the Web server plug-in configuration select **Servers** → **Web Servers** and select the check box next to your Web server in the list. Select **Generate Plug-in**.
7. Restart the Web server and all the application servers.

   Remember: You can stop and start all Lotus Expeditor Server application servers through the Windows Start Menu. For instructions, see "Starting and stopping the servers" on page 87.
8. Open a browser window and point to `https://yourserver/user-management` to verify the SSL server configuration update was successful. (Where *yourserver* represents the host name of your Lotus Expeditor Server.)

   Tip: For a full description of the virtual hosts function of WebSphere Application Server, see the WebSphere Application Server documentation.

Importing a self-signed certificate to the Application Server

If you are using a self-signed certificate you must add that certificate to the Application Server Virtual Machine truststore file.

Complete the following steps to import the certificate:

1. Locate the Application Server Virtual Machine truststore file.

   Tip: In most cases, the truststore file resides in the *was_home*\java\jre\lib\security\cacerts directory. (Where *was_home* represents the directory where you installed WebSphere Application Server.)

2. Open a command prompt window and type the following:

   ```
   keytool -import -keystore "c:\JAVA_HOME\jre\lib\security\cacerts" -alias
   hostname -file "c:\path_to_exported_ssl_certificate\cert.arm"
   ```

   (Where *JAVA_HOME* represents the directory where the Java Runtime Environment resides, *hostname* represents the host name of your system, and *path_to_exported_ssl_certificate* represents the path to the certificate that you exported in "Obtaining a certificate" on page 105.

   Note: When you run the keytool command, verify that *JAVA_HOME*\bin is included the path or change to the directory where the Java Runtime Environment resides before you run the command.

3. When the keytool command prompts you, enter the keystore password. The default Virtual Machine cacerts keystore password is changeit.
4. When prompted "Trust this certificate?", type yes and press Enter.

   After you complete these steps, Java programs that use this Virtual Machine can open HTTPS connections to your SSL enabled Web server.

Configuring DB2 Everyplace for SSL

This topic provides instructions on configuring DB2 Everyplace for SSL connections.

To configure DB2 Everyplace for SSL connections, you must perform the following steps:

1. Make sure that you have configured the WebSphere Application Server for SSL before completing this procedure. For instructions, see "Configuring WebSphere Application Server for SSL" on page 106.
2. Modify the Uniform Resource Locator (URL) that you use to access the Lotus Expeditor Server common user registry. See "Modifying the URL for the common user registry for DB2 Everyplace" for instructions.
3. If you are using a self-signed certificate, add that certificate to the DB2 Everyplace Virtual System truststore file. See "Importing a self-signed certificate to DB2 Everyplace" on page 108 for instructions.

Modifying the URL for the common user registry for DB2 Everyplace

To modify the URL that you use to access the Lotus Expeditor Server common user registry, complete the following steps:

1. Open the DSYLDAP.properties file in a text editor. The DSYLDAP.properties file resides in the *dsypath*\Server\properties\com\ibm\mobileservices\DSYLDAP.properties directory. (Where *dsypath* represents the path where DB2 Everyplace is installed.
2. Modify the DSYLDAP.properties file to use secure HTTP for the WEBSERVICE_SOAP_ROUTER. For example, type:

   ```
   WEBSERVICE_SOAP_ROUTER=https://hostname/UserGroupInfoWebService/servlet/rpcrouter
   ```

   (Where *hostname* represents the host name of your system.)

3. Save and close the DSYLDAP.properties file.
4. Restart the IBMDB2eServer application server for the change to take effect.

Importing a self-signed certificate to DB2 Everyplace

If you are using a self-signed certificate, you must add that certificate to the DB2 Everyplace Virtual System truststore file.

Complete the following steps:

1. Make sure that you have configured the WebSphere Application Server for SSL before completing this procedure. For instructions, see "Configuring WebSphere Application Server for SSL" on page 106.
2. Locate the DB2 Everyplace Virtual System truststore file.

   Tip: In most cases, the truststore file resides in the *DSYPATH*\jre\lib\security\cacerts directory. (Where *DSYPATH* represents the path where DB2 Everyplace is installed.
3. Open a command prompt window and type the following:

   ```
   keytool -import -keystore "DSYPATH\jvm\jre\lib\security\cacerts" -alias hostname
   -file "path_to_exported_ssl_certificate\filename.cer"
   ```

   (Where *hostname* represents the host name of your system, *path_to_exported_ssl_certificate* represents the path to the certificate that you exported in "Obtaining a certificate" on page 105 and *filename.cer* represents the name of the certificate file.)
4. When the **keytool** command prompts you, enter the keystore password. The default Virtual Machine cacerts keystore password is **changeit**.
5. When prompted to `Trust this certificate?`, type **yes** and press **Enter**.
6. Restart server1 and the IBMDB2Server application server for the changes to take effect.

Configuring Device Manager for SSL

This topic provides instructions on how to configure Device Manager for SSL.

To configure Device Manager for SSL connections, you must perform the following steps:

1. Make sure that you have configured the WebSphere Application Server for SSL before completing this procedure. For instructions, see "Configuring WebSphere Application Server for SSL" on page 106.
2. Modify the URL used by the Subscription Manager to access the Lotus Expeditor Server common user registry. See Modifying the URL for the Common User Registry for Device Manager for instructions.
3. Configure the keystore file for the Device Manager console. See Configuring the console keystore file for instructions.
4. Add a new host alias for the Device Manager console. See Adding a host alias for the Device Manager console for instructions.

Modifying the URL for the common user registry for Device Manager

To modify the URL used by the Subscription Manager to access the Lotus Expeditor Server common user registry, complete the following steps:

1. Open the UserServicesSubscriptionManager.properties file in a text editor. The UserServicesSubscriptionManager.properties file resides in the *was_profile*\installedApps*cell_name*\DMS_WebApp.ear\dmserver.war\WEB-INF\classes\ directory. (Where *was_profile* represents the directory where you created the WebSphere Application Server configuration profile being used by Lotus Expeditor.)
2. Change **http://** to **https://** in the values for the WEBSERVICE_SOAP_ROUTER and WEBSERVICE_ALT_SOAP_ROUTER properties.
3. Save and close the file.

Configuring the console keystore file

To configure the keystore file for the Device Manager console, complete the following steps:

Tip: For more detailed information about configuring the console keystore file, see "Using HTTPS protocol with software distribution" in the Software distribution job topic.

1. Open the dmstart.bat file in a text editor. The dmstart.bat file resides in the *expeditor_root*\DMS\console\dm directory, where *expeditor_root* represents the location where you installed Lotus Expeditor Server.

   Note: For Linux server, there should be a remote DM console on Win OS, not the Expeditor Server installation path.

2. Modify the following lines in the dmstart.bat file:

   ```
   SET KEYSTOREPATH=c:\progra~1\IBM\WebSphere\AppServer\java\jre\lib\security\cacerts
   SET KEYSTOREPASSWORD=changeit
   ```

3. Save and close the file.

Adding a host alias for the Device Manager console

To add a host alias for SSL connections to the Device Manager console, use the internal HTTP transport for the Device Manager application server. Then, locate the internal HTTP port used by the Device Manager application server and add a host alias for that port. Follow these steps to add a host alias for the Device Manager console:

1. Open the WebSphere Application Server Administrative Console and click **Servers** → **Application Servers** → **DMS_AppServer**.
2. Scroll down to **Communications** and expand the list under **Ports**.
3. Find the port number associated with WC_defaulthost and record the number for later use.
4. Restart the DMS_AppServer application server.
5. Click **Environment** → **Virtual Hosts**.
6. Select the default host.
7. Select **Host Aliases** under **Additional Properties** and click **New** to create a host alias.
8. Specify the value associated with WC_defaulthost, which you recorded in step 3, in the **port** field under **General Properties** and click **Apply**.
9. Click **Save** to apply the changes to the Application Server master configuration.
10. To regenerate the Web server plug-in configuration, select **Servers** → **Web Servers** and use the check box to select your Web server from the list displayed. Then, select **Generate Plug-in**.
11. Restart the Web server and all the application servers.

    Remember: You can stop and start all Lotus Expeditor Server application servers through the Windows Start Menu. For instructions, see "Starting and stopping the servers" on page 87.

    For a full description of the virtual hosts function of WebSphere Application Server, refer to the WebSphere Application Server documentation.

Configuring the client device agent to use SSL

There are additional steps required to configure the client device agent to use SSL. See Configuring SSL for the Enterprise Management Agent for information on configuring the device agent for SSL.

Device Manager server security

This topic provides information on enabling SSL for the Device Manager server.

To enable SSL for the Device Manager server, use IBM HTTP Server.

Application server security

This topic describes application server security for Device Manager.

If the software is accessed with HTTPS protocol, the application server for Device Manager must be able to access that software on the HTTP server using SSL. The Software URL field for the software package specifies if HTTP or HTTPS protocol is used during the software distribution.

Device Manager console security

This topic provides information on enabling optimal security for the Device Manager console.

The Device Manager console uses JDBC to communicate with the Device Manager database. Optimal security is achieved only when the Device Manager console is contained within the same firewall as the Device Manager database and the Device Manager server. You want to avoid exposure of the Device Manager data to the Internet.

Device Manager requires the users of the Device Manager console to log in with a user ID and password. An authenticated user is authorized to use the console by virtue of being in the Expeditor Server administrators group. Once authorized, a user of the Device manager console can perform any operation on any Device Manager object (device, job, software, and so on). There is no finer-grained authorization that limits an administrator to certain operations or to certain objects.

Device security

This topic provides information on device security.

Devices connect to the Device Manager server using HTTP or HTTPS. The device is authenticated by the Web server, using HTTP basic authentication, with the device owner's ID and password as the security tokens. This authentication happens outside of Device Manager, and before the Device Manager server is invoked.

HTTPS can be used to protect sensitive data passing between the device and the server.

Using HTTPS with software distribution

This topic provides information on using HTTPS with software distribution.

When software is registered and made available for distribution with Device Manager, the software is copied to an HTTP server (IBM HTTP Server) and distributed to devices from the HTTP server. If the administrator uses HTTPS protocol to specify the location of the software in the Server URL field, the following configuration steps must be done:

1. Enable SSL using HTTPS for the application server.
2. Make path to the JKS file accessible on the system running the Device Manager console.
3. Open the DMstart.bat file in a text editor.

   Note: This file is located on the system running the Device Manager console in the console_install_dir \dm\ directory, where console_install_dir is the directory specified when you installed the Device Manager console.
4. Change the values for the **KEYSTOREPATH** and **KEYSTOREPASSWORD** parameters to the following values: set KEYSTOREPATH=path_to_JKS_file set KEYSTOREPASSWORD=password

   Note: The **KEYSTOREPATH** value is the fully-qualified path, or relative path to the location of the JKS format SSL certificates file.

   Note: If you use a % symbol in your password, the parser rules for **KEYSTOREPASSWORD** require that you double that % symbol, for example %%, when you use that symbol.

5. Save the changes to the DMstart.bat file.
6. Restart the Device Manager console.

Encrypted DB2 Everyplace Sync Server passwords

This topics introduces how different types of passwords are encrypted and where they are saved.

DB2 Everyplace Sync Server passwords appear in properties files and XML scripts

Two properties files contain passwords used by the DB2 Everyplace Sync Server:

- DSYIdflt.properties contains the password for the control database, DSYCTLDB.
- DSYLDAP.properties contains the password for the SOAP router HTTP connection.

DB2 Everyplace Sync Server passwords can also appear in XML scripts, and they can be specified using the Mobile Devices Administration Center.

To prevent accidental or unauthorized access to these resources, passwords can be encrypted.

DSYEncrypt utility encrypts passwords

DB2 Everyplace provides a command-line utility that encrypts passwords. Given a password, the utility returns an encrypted version of that password. The utility, named dsyencrypt.bat, is installed by default in the *dsypath*\Server\bin directory, where *dsypath* is the directory where DB2 Everyplace is installed.

Here's an example of how to use the tool to encrypt the password **db2admin**.

1. From the command line, enter **dsyencrypt db2admin**. A message is displayed similar to the following:

```
Encrypted form of your input text is: nw4SCU6x1ok=
If this is an encrypted password you want to place in a properties file,
then the value you should place in the properties file is: {DSY}nw4SCU6x1ok=
```

2. Use the generated value (prefixed by {DSY} in a properties file instead of the plain text password. For example, in DSYIdflt.properties, instead of using this:

   SSDB2.Password=db2admin use this:

   SSDB2.Password={DSY}nw4SCU6x1ok=

   Similarly, in DSYLdap.properties, instead of using this:

   WEBSERVICE_HTTP_PASSWORD=db2admin

   use this:

   WEBSERVICE_HTTP_PASSWORD={DSY}nw4SCU6x1ok=

DB2 Everyplace Sync Server passwords in XML scripts are encrypted in the database

When creating XML scripts manually, you can specify passwords for the DB2 Everyplace Sync Server in plain text, for example, <Password>db2admin<Password>. Such plain text passwords are automatically encrypted when stored in the control database.

In XML scripts generated by the XML Scripting Tool, master and mirror database passwords are encrypted automatically, with output similar to the following examples:

```
<AddJdbcMaster>
  <Databasej>dbc:db2:VNURSE</Database>
  <Driver>COM.ibm.db2.jdbc.app.DB2Driver<Driver>
  <Userid>db2admin<Userid>
  <Password Encryption="DSY">QmlUOzeUngArzGq1xptlhA==</Password>
<AddJdbcMaster>
```

```
<AddJdbcMirror>
  <Databasej>dbc:db2:M_VN2</Database>
  <Driver>COM.ibm.db2.jdbc.app.DB2Driver<Driver>
  <Userid>db2admin</Userid>
  <Password Encryption="DSY">bbRtum49DRuMMRxwD5eSlAA==</Password>
  <SyncWindow>5000</SyncWindow>
<AddJdbcMirror>
```

Mobile Devices Administration Center encrypts passwords for master and mirror databases

When you use the Mobile Devices Administration Center to specify passwords for master and mirror databases, they are saved in encrypted form. If you forget your passwords, you can't retrieve them by looking into these tables.

Note: Only new records and updated records are encrypted. Existing data in DSYCTLDB, specifically DSY.REPL_MIRROR.PASSWORD, DSY.REPL_MASTER.PASSWORD, DSY.JDBC_MIRROR.PASSWORD, and DSY.JDBC_MIRROR.PASSWORD, is not encrypted when migrated.

Reference

This topic provides reference information designed to help you find additional documentation about Lotus Expeditor Server and related products.

Review the following reference topics.

Lotus Expeditor Server TCP/IP ports

Review this topic to see which TCP/IP ports Lotus Expeditor Server uses.

Table 13. Lotus Expeditor Server TCP/IP ports. The following table lists the TCP/IP ports used by Lotus Expeditor Server.

Port number	Description
Lotus Expeditor Server	
389	Lotus Expeditor Server access to external LDAP server
50000	Lotus Expeditor Server access to DB2
Device Manager	
80	HTTP access to Device Manager servlets
443	HTTPS access to Device Manager servlets (optional)
DB2 Everyplace	
80	HTTP access into DB2 Everyplace servlets
443	HTTPS access into DB2 Everyplace servlets (optional)
WebSphere MQ Everyplace	
1881	WebSphere MQ Everyplace listens for incoming messages on this port

Accessibility features

This topic provides information about the Lotus Expeditor Server accessibility features.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

The following accessibility features are available in Lotus Expeditor Server.

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen.

  Note: This feature is not applicable for the Lotus Expeditor Server installation program.
- You can use the keyboard instead of the mouse to navigate the installation program and User Management Graphical User Interface.
- You can magnify the information displayed on the screen.
- All information is communicated independently of color.
- The Lotus Expeditor Server documentation is provided in an accessible format.

Lotus Expeditor Server installation program shortcut keys

The Lotus Expeditor Server installation program provides the following shortcut keys:

Alt+B Use this shortcut key combination to go back to the previous panel.

Alt+N Use this shortcut key combination to go forward to the next panel.

Alt+C Use this shortcut key combination to cancel the installation program.

Tab You can use the Tab key to go forward to the next panel.

Shift+tab
You can use this shortcut key combination to go back to the previous panel.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Intellectual Property Law

Department LZMS
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AS/400
Cloudscape
DataPropagator
DB2
Domino
Everyplace
IBM
IBM logo
Informix
iSeries
Lotus
Passport Advantage
Rational
SupportPac
Tivoli
WebSphere
Workplace Client Technology
zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linux Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product or service names may be trademarks or service marks of others.

Program Number:

Printed in USA