Novell iFolder®

3.x

www.novell.com

ADMINISTRATION GUIDE

December 23, 2005

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Third-Party Materials

Contents

10 Managing iFolder Users 103

11 Managing iFolders 109

A Configuration Files 117

B Clustering iFolder 3.*x* with Novell Cluster Services for Linux 125

About This Guide

This guide describes how to install, configure, and manage the Novell® iFolder® 3.*x* enterprise server, the iFolder 3.*x* Web Access server, and the iFolder™ Client. This guide is divided into the following sections:

Audience

This guide is intended for system administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell iFolder 3.x Administration Guide*, visit the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/ifolder3/index.html).

For emerging issues with Novell iFolder 3.*x* and the iFolder client, see the *Novell iFolder 3.x Readme* (http://www.novell.com/documentation/ifolder3/readme/data/readme.html).

Additional Documentation

For information, see the following:

- *Novell iFolder 3.x Security Administrator Guide* (http://www.novell.com/documentation/ifolder3/security/data/front.html)
- *iFolder User Guide for Novell iFolder 3.x* (http://www.novell.com/documentation/ifolder3/user/data/front.html).
- Novell iFolder 3.*x* documentation (http://www.novell.com/documentation/ifolder3/index.html)
- Novell Open Enterprise Server product site (http://www.novell.com/products/openenterpriseserver)
- Novell Open Enterprise Server documentation (http://www.novell.com/documentation/oes/index.html)
- Novell eDirectory™ 8.7.3 documentation (http://www.novell.com/documentation/edir873/treetitl.html)
- Novell iManager 2.5 documentation (http://www.novell.com/documentation/imanager25/treetitl.html)
- Novell Linux Desktop 9 product site (http://www.novell.com/products/desktop/)
- Novell Linux Desktop 9 documentation (http://www.novell.com/documentation/nld/treetitl.html)
- Novell Technical Support (http://www.novell.com/support)

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview of Novell iFolder 3.*x*

1

Novell® iFolder® 3.*x* is the next generation of iFolder, supporting multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution. With iFolder, users' local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and share each iFolder with a different group of users. Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.

This section familiarizes you with the various benefits and features of iFolder and its main components:

- Section 1.1, "Benefits of iFolder for the Enterprise," on page 13
- Section 1.2, "Benefits of iFolder for Users," on page 15
- Section 1.3, "Enterprise Server Sharing," on page 17
- Section 1.4, "Key Components of iFolder," on page 17
- Section 1.5, "What's Next," on page 20

1.1 Benefits of iFolder for the Enterprise

Benefits of iFolder to the enterprise include the following:

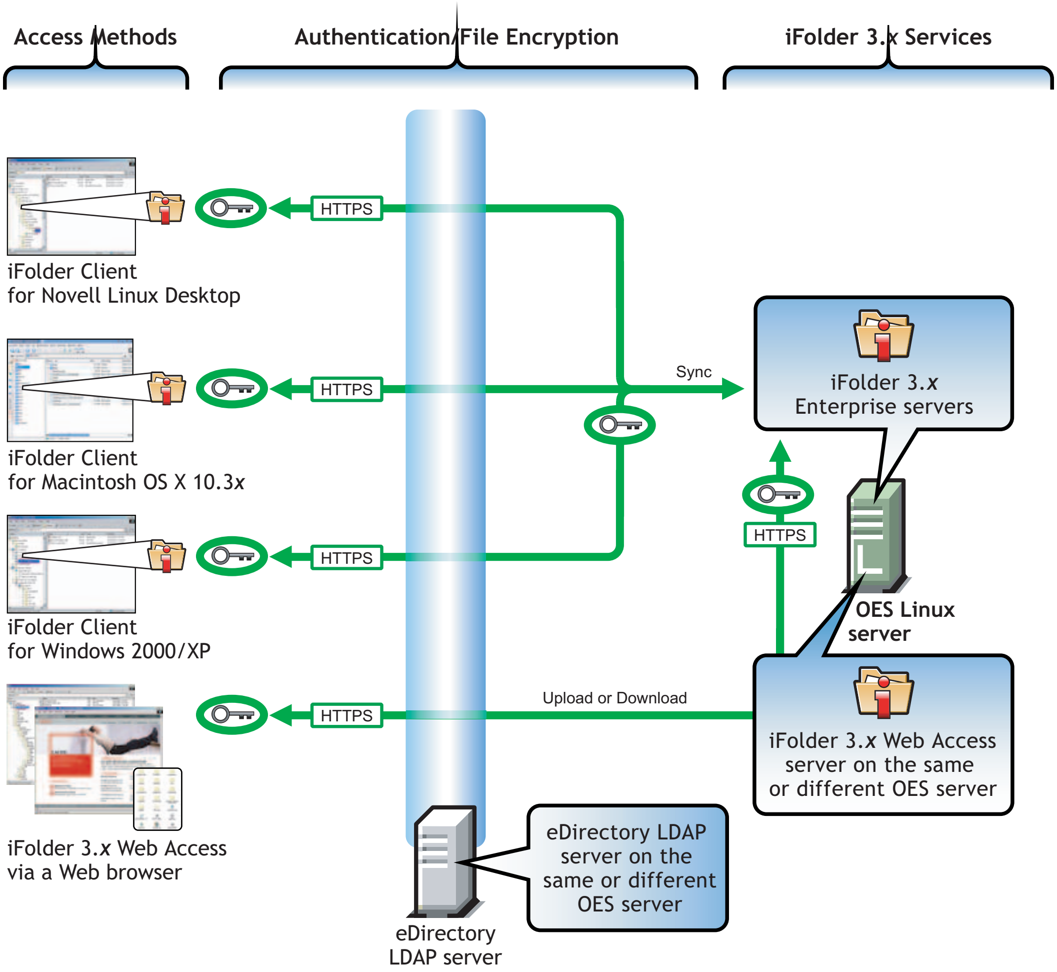
- "Seamless Data Access" on page 13
- "Data Safeguards and Data Recovery" on page 14
- "Reliable Data Security" on page 14
- "Productive Mobile Users" on page 14
- "Cross-Platform Client Support" on page 15
- "Simple Data and Account Management" on page 15
- "No Training Requirements" on page 15

1.1.1 Seamless Data Access

Novell iFolder greatly simplifies the IT department's ability to keep users productive. It empowers users by enabling their data to follow them wherever they go.

The days of users e-mailing themselves project files so they can work on them from home are gone, along with the frustration associated with sorting through different versions of the same file on different machines. iFolder stores and synchronizes users' work in such a way that no matter what client or what location they log in from, their files are available and in the condition that they expect them to be. Users can access the most up-to-date version of their documents from any computer using the iFolder client or Web access.

Figure 1-1 *Novell iFolder 3.x Access Methods*



1.1.2 Data Safeguards and Data Recovery

With Novell iFolder, data stored on the server can be easily safeguarded from system crashes and disasters that can result in data loss. When a user saves a file locally, the iFolder client can automatically update the data on the iFolder server, where it immediately becomes available for an organization's regular network backup operations. iFolder makes it easier for IT managers to ensure that all of an organization's critical data is protected.

1.1.3 Reliable Data Security

With Novell iFolder, LDAP-based authentication for access to stored data helps prevent unauthorized network access.

1.1.4 Productive Mobile Users

A Novell iFolder solution makes it significantly easier to support mobile users. VPN connections are no longer needed to deliver secure data access to mobile users. Authentication and data transfer use Secure Sockets Layer (SSL) technology to protect data on the wire.

Users do not need to learn or perform any special procedures to access their files when working from home or on the road. iFolder does away with version inconsistency, making it simple for users to access the most up-to-date version of their documents from any connected desktop, laptop, Web browser, or handheld device.

In preparation to travel or work from home, users no longer need to copy essential data to their laptops from various desktop and network locations. The iFolder client can automatically update a user's local computer with the most current file versions. Even when a personal computer is not available, users can access all their files via Web access with any computer connected to the Internet.

1.1.5 Cross-Platform Client Support

The iFolder client is available for Linux, Windows*, and Macintosh* desktops. The Novell iFolder 3.*x* Web Access server provides a Web interface that allows users to access their files on the enterprise server with a Web browser from any computer with an active network or Internet connection.

1.1.6 Scalable Deployment

iFolder easily scales from small to large environments. You can install iFolder on multiple servers, allowing your iFolder environment to grow with your business. A single iFolder enterprise server handles up to about 1,000 user accounts, depending on the amount of memory and storage available. Users in an LDAP context can be concurrently provisioned for iFolder services simply by assigning the context to an iFolder server.

1.1.7 Simple Data and Account Management

Management of all iFolder enterprise servers is centralized through the Novell iFolder 3 plug-in to Novell iManager 2.5. Novell iFolder allows management from any location, using a standard Web browser. iFolder also frees IT departments from routine maintenance tasks by providing secure, automatic synchronization of local files to the server.

1.1.8 No Training Requirements

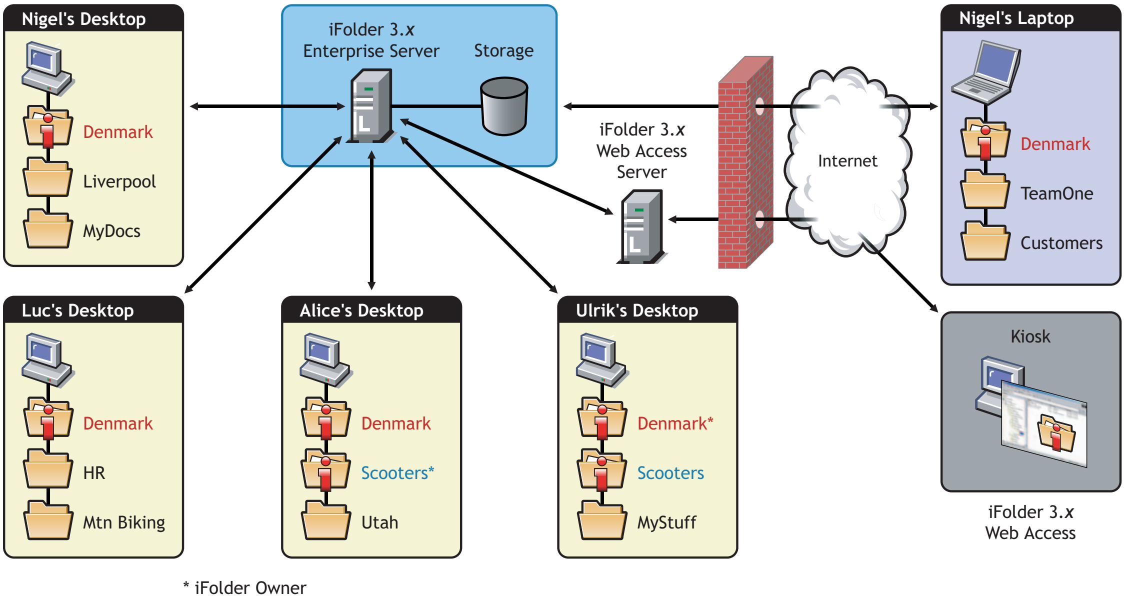
IT personnel no longer need to condition or train users to perform special tasks to ensure the consistency of data stored locally and on the network. With Novell iFolder, users simply store their files in the local iFolder directory. Their files are automatically updated to the iFolder server and any other workstations that share the iFolder. iFolder works seamlessly behind the scenes to ensure that data is protected and synchronized.

1.2 Benefits of iFolder for Users

Typically, when users work in multiple locations or in collaboration with others, they must conscientiously manage file versions. With iFolder, the most recent version of a user's files can follow the user to any computer where the iFolder client is installed and a shared iFolder is set up. iFolder also allows users to share multiple iFolders and their separate content with other users of the iFolder system. Users decide who participates in each shared iFolder and their level of access. Similarly, users can participate in shared iFolders that are owned by others in the collaboration environment.

In the following example, Ulrik owns an iFolder named Denmark and shares it via his iFolder enterprise account with Nigel, Luc, and Alice. Nigel travels frequently, so he also set up the iFolder on his laptop. Any iFolder member can upload and download files from the Denmark iFolder from anywhere, using the iFolder Web Access server. In addition, Alice shares a non-work iFolder named Scooters with her friend Ulrik.

Figure 1-2 *Collaboration and Sharing with iFolder*



With an enterprise server, the iFolders are stored centrally for all iFolder members. The iFolder server synchronizes the most recent version of documents to all authorized users of the shared iFolder. All that the iFolder owner and iFolder members need is an active network connection and the iFolder client.

Novell iFolder provides the following benefits:

- Guards against local data loss by automatically backing up local files to the iFolder server and multiple workstations
- Transparently updates a user's iFolder files to the iFolder enterprise server and multiple member workstations with the iFolder client
- Tracks and logs changes made to iFolder files while users work offline, and synchronizes those changes when they go online
- Provides access to user files on the iFolder server from any workstation without the iFolder client, using a Web browser and an active Internet or network connection
- With SSL encryption enabled, protects data as it travels across the wire
- Makes files on the iFolder server available for regularly scheduled data backup

For more information, see "Benefits of iFolder" in the *iFolder User Guide for Novell iFolder 3.x*.

1.3 Enterprise Server Sharing

The iFolder client included in this release supports synchronization across multiple computers through a central Novell iFolder 3.*x* enterprise server.

- Users can share files across computers.
- Users can share files with others.
- Each user can own multiple iFolders.
- Each user can participate in multiple iFolders owned by other users.
- Files can be synchronized via the central server at any time and with improved availability, reliability, and performance.
- Data is transferred securely over the wire using SSL connections.
- Users are autoprovisioned for iFolder services based on their assignment to administrator-specified LDAP containers and groups.
- A list of iFolder users is synchronized at regular intervals with the LDAP directory services.
- Local files are automatically backed up to the server at regular intervals and on demand.
- iFolder data on the server can be backed up to backup media and restored.
- Administrators can manage the iFolder system, user accounts, and user iFolders using the Novell iFolder 3 plug-in to iManager.

1.4 Key Components of iFolder

- Section 1.4.1, "iFolder Enterprise Server," on page 17
- Section 1.4.2, "Novell iFolder 3 Plug-in to Novell iManager 2.5," on page 17
- Section 1.4.3, "iFolder Web Access," on page 18
- Section 1.4.4, "The iFolder Client," on page 18
- Section 1.4.5, "Shared iFolders," on page 18
- Section 1.4.6, "iFolder Access Rights," on page 18
- Section 1.4.7, "Account Setup for Enterprise Servers," on page 19
- Section 1.4.8, "Access Authentication," on page 19
- Section 1.4.9, "File Synchronization and Data Management," on page 19
- Section 1.4.10, "Synchronization Log," on page 19
- Section 1.4.11, "iFolder Client APIs," on page 19

1.4.1 iFolder Enterprise Server

The iFolder enterprise server is a central repository for storing iFolders and synchronizing files for enterprise users.

1.4.2 Novell iFolder 3 Plug-in to Novell iManager 2.5

The Novell iFolder 3 plug-in to Novell iManager 2.5 is an administrative tool used to manage the iFolder system, user accounts, and user iFolders and data.

1.4.3 iFolder Web Access

The iFolder 3.*x* Web Access server provides an interface to allow users remote access to iFolders on the enterprise server.

For information about using Web Access, see "Using Novell iFolder 3.x Web Access" in the *iFolder User Guide for Novell iFolder 3.x*.

1.4.4 The iFolder Client

The iFolder client integrates with the user's operating system to provide iFolder services in a native desktop environment. It supports the following client operating systems:

- Novell Linux Desktop 9
- Windows 2000/XP
- Macintosh OS X v10.3 or later

An iFolder session begins when the user logs in to an iFolder services account and ends when the user logs out of the account or exits the iFolder client. The iFolders synchronize files with the enterprise server only when a session is active and the computer has an active connection to the network or Internet. Users can access data in their local iFolders at any time; it does not matter if they are logged in to their server accounts or if they are connected to the network or Internet.

The iFolder client allows users to create and manage their iFolders. For information, see the *iFolder User Guide for Novell iFolder 3.x*.

1.4.5 Shared iFolders

An iFolder is a local directory that the user selectively shares with other users in a collaboration environment. The iFolder files are accessible to all members of the iFolder and can be changed by those with the rights to do so. Users can share iFolders across multiple workstations and with others.

Because the iFolder client is integrated into the operating environment, users can work with iFolders directly in a file manager or in the My iFolders window. Within the iFolder, users can set up any subdirectory structure that suits their personal or corporate work habits. The subdirectory structure is constant across all member iFolders. Each workstation can specify a different parent directory for the shared iFolder.

1.4.6 iFolder Access Rights

The iFolder client provides four levels of access for members of an iFolder:

- **Owner:** Only one user serves as the owner. This is typically the user who created the iFolder. The owner or an iFolder administrator can transfer ownership status from the owner to another user.

  The owner of an iFolder has the Full Control right. This user has read/write access to the iFolder, manages membership and access rights for member users, and can remove the Full Control right for any member. With an enterprise server, the disk space used by the owner's iFolders count against the owner's user disk quotas on the enterprise server.

If a user is deleted as a user for the iFolder system, the iFolders owned by the user are orphaned. Orphaned iFolders are assigned temporarily to the iFolder Admin user, who becomes the owner of the iFolder. Membership and synchronization continues while the iFolder Admin user determines whether an orphaned iFolder should be deleted or assigned to a new owner.

- **Full Control:** A member of the shared iFolder, with the Full Control access right. The user with the Full Control right has read/write access to the iFolder and manages membership and access rights for all users except the owner.
- **Read/Write:** A member of the shared iFolder, with the Read/Write access right to directories and files in the iFolder.
- **Read Only:** A member of the shared iFolder, with the Read Only access right to directories and files in the iFolder. This member can copy an iFolder file to another location and modify it outside the iFolder.

When used with an enterprise server account, the server hosts every iFolder created for that account. Users create an iFolder and the enterprise server makes it available to the specified list of users. A user can have a separate account on each enterprise server. A user’s level of membership in each shared iFolder can differ.

1.4.7 Account Setup for Enterprise Servers

The iFolder client allows you to set up multiple accounts, with one each allowed per enterprise server. Users specify the server address, username, and password to uniquely identify an account. On his or her computer, a user sets up accounts while logged in as the local identity he or she plans to use to access that account and its iFolders. Under the local login, the user can set up multiple iFolder accounts, but each account must belong to a different iFolder enterprise server.

1.4.8 Access Authentication

Whenever iFolder connects to an enterprise server to synchronize files, it connects with HTTP BASIC and SSL connections to the server, and the server authenticates the user against the LDAP directory service.

1.4.9 File Synchronization and Data Management

When you set up an iFolder account, you can enable Remember Password so that iFolder can synchronize iFolder invitations and files in the background as you work. The iFolder client runs automatically each time you log in to your computer’s desktop environment. The session runs in the background as you work with files in your local iFolders, tracking and logging any changes you make. With an enterprise server, you can synchronize the files at specified intervals or on demand.

1.4.10 Synchronization Log

The log displays a log of your iFolder background activity.

1.4.11 iFolder Client APIs

As part of the iFolder project, APIs are available for the client. For iFolder Client developer documentation, see the *iFolder Software Developers Kit* (http://forge.novell.com/modules/xfmod/docman/?group_id=1372).

1.5 What’s Next

Before you install iFolder, review the following sections:

- “What’s New” on page 21
- “Planning iFolder Services” on page 31
- “Coexistence and Migration Issues” on page 41
- “Prerequisites and Guidelines” on page 45

When you are done, install and configure your iFolder enterprise server and Web Access server. For information, see “Installing and Configuring iFolder Services” on page 51.

What’s New 2

Novell® iFolder® 3.*x* and the iFolder™ client offer many new capabilities as compared to Novell Novell iFolder 2.1*x*. This section discusses the following:

- Section 2.1, “What’s New in Novell iFolder 3.2 (OES SP2 Linux),” on page 21
- Section 2.2, “What’s New in Novell iFolder 3.1 (OES SP1 Linux),” on page 21
- Section 2.3, “What’s New in Novell iFolder 3.0 (OES Linux),” on page 21
- Section 2.4, “Comparison of 2.1x and 3.x Server Features and Capabilities,” on page 22
- Section 2.5, “Comparison of 2.1x and 3.x Client Features and Capabilities,” on page 25
- Section 2.6, “Comparison of 2.1x and 3.x Web Access Features and Capabilities,” on page 28

2.1 What’s New in Novell iFolder 3.2 (OES SP2 Linux)

The following features are new in iFolder 3.2 for OES SP2 Linux:

- Localized user help for the iFolder client
- Support for users to log in to the iFolder server with their common name or e-mail address. The iFolder Admin User configures the option during installation and the setting applies to all users. For information, see Section 6.2, “Configuring the iFolder Enterprise Server,” on page 53.

2.2 What’s New in Novell iFolder 3.1 (OES SP1 Linux)

The following features are new in iFolder 3.1 for OES SP1 Linux:

- Support for the iFolder data store on Novell Storage Services™ (NSS) volumes on Linux
- Support for Novell Cluster Services™ for Linux
- Support for iFolder data store backup with the Target Service Agent for iFolder (TSAIF) with NBackup, a Novell Storage Management Services command line utility
- Support for Mono 1.1.7.7*x*
- Interoperability for Novell iChain, Novell BorderManager, and Novell Security Manager
- Support for the OES patch channel

2.3 What’s New in Novell iFolder 3.0 (OES Linux)

Novell iFolder 3.0 includes several important new features.

- **Multiple iFolders:** A user creates as many iFolders as desired and manages each one separately. Each iFolder functions independently to synchronize its own set of files. Users specify the local path for each iFolder.

- **Shared iFolders:** Each iFolder can be kept private or shared with a different group of users. For a shared iFolder, the owner or a member with the Full Control right controls who participates in the iFolder and the level of access granted to each member, such as Full Control, Read/Write, or Read Only.
- **Centralized iFolder Synchronization and Storage:** iFolder data is automatically synchronized by the iFolder client to the iFolder enterprise server over an IP network. The enterprise server stores files for each iFolder, then synchronizes them to other member computers. Encryption is supported for data transfers. Administrators control whether data is transported securely with HTTPS (SSL) connections during synchronization, or if data is transported with standard HTTP BASIC connections.
- **Multiple iFolder Accounts:** Users can concurrently access iFolder accounts on different servers.
- **Web Access to iFolders:** Users access their iFolder enterprise server accounts from any computer with Internet access. They create subdirectories, upload files, and download files to any of their iFolders. All iFolders for the account are available, whether the user is the owner or a member.
- **Remote and Policy-Based Administration:** Administrators manage iFolder services with the Novell iFolder 3 plug-in to Novell iManager, which is the central management console for Novell Open Enterprise Server. The tool supports policy-based management of the iFolder system, user accounts, and users' iFolders.
- **Client-Side APIs:** Almost every function an end user can accomplish through the UI is exposed as an API. This allows third-party developers to more easily integrate their applications with iFolder and gives organizations the tools they need to customize iFolder.

For information about key features of the iFolder client, see the *iFolder User Guide for Novell iFolder 3.x*.

2.4 Comparison of 2.1*x* and 3.x Server Features and Capabilities

Feature or Capability	Novell iFolder 2.1*x* Server	Novell iFolder 3.x Enterprise Server
Server management	iFolder Administration tool `http://serveraddress/iFolderServer/iFolder.html` You can also access the iFolder Administration tool from iManager by selecting iFolder 2.1*x* from Roles and Tasks.	Novell iFolder 3 plug-in to iManager For information, see Section 8.1, "Accessing the Novell iFolder 3 Plug-In for iManager," on page 79.

Feature or Capability	**Novell iFolder 2.1*x* Server**	**Novell iFolder 3.x Enterprise Server**
Automatic provisioning of iFolder services	No The administrator enables iFolder services for users, requires users to log in to activate the account, and then creates the iFolder on the server.	Yes iFolder automatically provisions iFolder users based on LDAP containers, groups, or users the administrator specifies. The server periodically polls your LDAP server for a list of authorized network users in those contexts and updates the iFolder users accordingly.
Maximum iFolders per username	One	Multiple. Virtually unlimited number of iFolders as an owner or member.
Allows administrators to create an iFolder for a user	No	Yes
Allows administrators to share an iFolder and specify its member users	No	Yes • For each iFolder, specify a list of users, which can be further modified by the iFolder owner. • For each member of an iFolder, specify the user's level of access with Full Control, Read/Write, and Read Only rights.
Allows administrators to transfer ownership of a shared iFolder to another user	No	Yes
Detects orphaned iFolders and allows the iFolder Admin user to manage them	No	Yes
Maximum file size	Software limits file size to 4 GB. Below 4 GB, the maximum file size depends on the server's and clients' local file systems. For example, on Windows clients, FAT32 limits file sizes to 4 GB. On Linux, EXT2 limits file sizes to 2 GB.	There are no software restrictions, but the administrator can specify the maximum file size that users can synchronize as a system-wide policy. Below the administrative maximum, the practical maximum file size depends on the server's and clients' local file systems.
Maximum number of directories	32,765	No software restrictions; depends on the server's and clients' local file systems

Feature or Capability	Novell iFolder 2.1*x* Server	Novell iFolder 3.x Enterprise Server
Disk quotas	The administrator can specify a default user quota that applies system-wide, and specify individual user quotas for iFolder accounts.	The administrator can specify a default account quota that applies system-wide, individual user account quotas, and individual iFolder quotas. An owner can also specify a quota for an individual iFolder, but the total combined quotas for all the iFolders the user owns cannot exceed the system-wide account quota or the user's individual account quota, whichever is less. An iFolder member can specify a quota for the iFolder on each client. The quota cannot exceed the iFolder's quota or that user's own quota for his or her account.
Minimum synchronization interval	The administrator can set minimum synchronization intervals to apply system-wide and for individual users.	The administrator can set minimum synchronization intervals to apply system-wide, for individual users, or for an individual iFolder.
Allows administrators to specify which file types to synchronize	No	Yes Administrator can specify file types to include or exclude by setting system-wide, individual account, or individual iFolder policies.
Allows administrators to enable or disable the iFolder synchronization	Yes, by temporarily disabling iFolder services for the user account.	Yes, by using the iFolder Enable/ Disable User function to temporarily disable login for the user to the user's iFolder account.
Authenticated access	Yes, using the Admin username and password for the iFolder Management tool	Yes. The Admin user logs in to iManager, then must use credentials equivalent to the iFolder Admin user to connect to the iFolder server.
Encrypted data transfer	Yes, with the encrypted iFolder option The Blowfish algorithm is applied with a user-specified passphrase. The admin user determines whether encryption services are available to users.	Yes, with automatic HTTPS (SSL) connections. The iFolder Admin user or equivalent determines whether secure or insecure connections are used.
iFolder data stored encrypted on server	Yes, with the encrypted iFolder option The user must specify a passphrase when first creating the iFolder account.	No. Data is stored unencrypted for all iFolders.

Feature or Capability	Novell iFolder 2.1*x* Server	Novell iFolder 3.x Enterprise Server
Backup of local files to a network server	Files in users' local iFolders are backed up on the iFolder server.	Files in users' local iFolders are backed up on the iFolder enterprise server.
Backup support to restore deleted files	Entire iFolder contents must be backed up and restored.	Individual files, directories, and iFolders can be backed up and restored.

2.5 Comparison of 2.1*x* and 3.x Client Features and Capabilities

Feature or Capability	Novell iFolder 2.1*x* Client	iFolder Client with a Novell iFolder 3.*x* Enterprise Server
Download location	The iFolder download page is `http://serveraddress/iFolder` Replace *serveraddress* with the IP address or DNS name of your iFolder server. For example, `192.168.1.1` or `nifsvr1.example.com`. The path is case sensitive.	The administrator provides a download site where users can download the iFolder client, such as the iFolder 3.*x* Welcome page on the OES Linux server.
Default location of the iFolder directory on a client	Windows: `C:\Documents and Settings\`*`username`*`\My Documents\iFolder\`*`username`*`\Home` Linux: `/home/userid/ifolder/userid` Macintosh: Not supported	Anywhere the user wants to create an iFolder on his or her Windows, Linux, or Macintosh computers.
Connect to server	Log in to one account at a time.	Set up accounts for multiple iFolder servers and log in to one or more as desired.
Authenticated access	Yes, with username and password authentication via your LDAP server.	Yes, with username and password authentication via your LDAP server.
Encrypted data transfer	Yes, with the encrypted iFolder option. The Blowfish algorithm is applied with a user-specified passphrase.	Yes, with automatic HTTPS (SSL) connections. Administrators control whether connections use HTTPS or HTTP.

Feature or Capability	**Novell iFolder 2.1*x* Client**	**iFolder Client with a Novell iFolder 3.*x* Enterprise Server**
iFolder data stored encrypted on server	Yes, with encrypted iFolder option The user must specify a passphrase when first creating the iFolder account.	No Data is stored unencrypted on the server.
iFolder data stored encrypted on clients	No iFolder data is stored unencrypted on the client. Use third-party local encryption options, if needed.	No iFolder data is stored unencrypted on the client. Use third-party local encryption options, if needed.
Create an iFolder	Yes, by logging in to the server for the first time after being provisioned for iFolder services.	Yes, by selecting any local directory and making it an iFolder. A user can create multiple iFolders in each iFolder account.
Maximum iFolders per username	One	Multiple. Virtually unlimited number of iFolders as an owner or member.
Share an iFolder across multiple computers	Yes, by logging in to an iFolder server from a computer with the iFolder client, or by accessing the iFolder via the Web with NetStorage.	Yes, by logging in to an iFolder account from another computer with an iFolder client and setting up the available iFolder. You can select which of the iFolders you own or participate in to set up on each computer, according to your needs at each location.
Share an iFolder with other users	Not as designed, but it is possible. The administrator can create a username for this purpose. Membership in the iFolder is determined by who has access to the password for that username and its iFolder account.	Yes, as the owner user or a member user with the Full Control right. • For each iFolder, specify a list of users. • For each member of an iFolder, specify different levels of access with the Full Control, Read/Write, or Read Only right.

Feature or Capability	Novell iFolder 2.1*x* Client	iFolder Client with a Novell iFolder 3.*x* Enterprise Server
Participate in a shared iFolder owned by another user	Not as designed, but it is possible if the iFolder's owner shares his or her username and password. **IMPORTANT:** Sharing a password is a security risk and is never recommended.	Yes, if the owner adds you as a member. After the owner makes you a member of the iFolder, the server notifies you by making the iFolder available in your My iFolders window. Use the iFolder Setup function to activate the iFolder on one or more computers where you want to participate.
Allows the owner of a shared iFolder to transfer ownership of a shared iFolder to another user	No	Yes
Allows the iFolder owner to transfer ownership the iFolder to another user	No	Yes
Maximum file size	Software limits file size to 4 GB. Below 4 GB, the maximum file size depends on the server's and clients' local file systems. For example, on Windows clients, FAT32 limits file sizes to 4 GB. On Linux, EXT2 limits file sizes to 2 GB.	There are no software restrictions, but the administrator can specify the maximum file size that users can synchronize as a system-wide policy. Below the administrative maximum, the practical maximum file size depends on the server's and clients' local file systems.
Restrict synchronization by including or excluding files by file type, such as `.mp3`	No	Yes, with policies set by the administrator that can apply system-wide, to individual user accounts, or to individual iFolders.
Maximum number of directories	32,765	No software restrictions; depends on the server's and clients' local file systems.
Disk quotas	No	An owner can specify a quota for each iFolder, but the total combined administrative quotas for all owned iFolders cannot exceed the user's quota, or the system-wide quota if there is no user quota. An iFolder member can specify a quota for the iFolder on each computer where the iFolder is set up.

Feature or Capability	Novell iFolder 2.1*x* Client	iFolder Client with a Novell iFolder 3.*x* Enterprise Server
Minimum synchronization interval	The user sets a synchronization interval for each workstation. The value cannot be less than the system-wide setting or individual user setting.	The user sets a synchronization interval for each computer that applies to all iFolders in all accounts on that computer.
Allows users to suspend synchronization for a given client computer	Yes, using any of the following methods: • Log out of the iFolder server • Disable Automatic Synchronization in the Preferences tab. You can remain logged in, and then synchronization when you want with the Synchronization Now option.	Yes, using any of the following methods: • Log out of the iFolder server account • Disable Automatic Sync • Disable the account in the Account window (deselect Enable Account)
Remote access to iFolder data on the server	Yes, using NetStorage. Your administrator must configure NetStorage for iFolder services.	Yes, using iFolder 3.*x* Web Access
Backup of local files to a network server	Files in users' local iFolders are backed up on the iFolder server.	Files in users' local iFolders are backed up on the iFolder enterprise server.
Backup support to restore deleted files	Administrators must back up and restore the entire iFolder contents.	Administrators can back up the entire iFolder data store. They can restore individual files, directories, or iFolders.

2.6 Comparison of 2.1*x* and 3.x Web Access Features and Capabilities

Feature or Capability	Novell iFolder 2.1*x* Web Access	Novell iFolder 3.x Web Access
Web access method	For iFolder 2.1.4 and earlier, the Java* applet or Novell NetStorage (for NetWare® servers only) For iFolder 2.1.5 and later, Novell NetStorage for Novell Open Enterprise Server (both Linux and NetWare servers)	iFolder 3.x Web Access for Novell Open Enterprise Server for Linux

Feature or Capability	**Novell iFolder 2.1*x* Web Access**	**Novell iFolder 3.x Web Access**

Web access location	http://serveraddress/iFolder
	Replace `serveraddress` with the IP address or DNS name of your iFolder server. For example, `192.168.1.1` or `nifsvr1.example.com`. The path is case sensitive.
		`http://serveraddress/webalias`
		Replace `serveraddress` with the IP address or DNS name of your iFolder server. For example, `10.10.1.1` or `nifsvr1.example.com`.
		Replace `webalias` with the administrator-specified path. The default path is `/ifolder.` The path is case sensitive. For example:
		`http://10.10.1.1/ifolder`

Connect to server	The user has only one iFolder per username. The user accesses the iFolder server where his or her files are located for that username.	Users separately access the different servers where you have accounts. All iFolders for the individual account are available.
Authenticated access	Yes, with username and password authentication via your LDAP server.	Yes, with username and password authentication via your LDAP server.
Encrypted data transfer	Yes, with the encrypted iFolder option. The Blowfish algorithm is applied with a user-specified passphrase.	Yes, with HTTPS (SSL) connections for data transfer.
WebDAV protocol support	Yes, allows WebDAV clients, such as Microsoft Explorer, to seamlessly access folders and files on an iFolder 2.1*x* server.	No

Planning iFolder Services

3

This section discusses the planning considerations for providing Novell® iFolder® 3.*x* services on OES Linux.

- Section 3.1, “Security Considerations,” on page 31
- Section 3.2, “Server Workload Considerations,” on page 31
- Section 3.3, “Naming Conventions for Usernames and Passwords,” on page 32
- Section 3.4, “Admin User Considerations,” on page 33
- Section 3.5, “iFolder User Account Considerations,” on page 35
- Section 3.6, “iFolders Data and Synchronization Considerations,” on page 36
- Section 3.7, “Management Tools,” on page 37

3.1 Security Considerations

For information about planning security for your iFolder 3.*x* system, see the *Novell iFolder 3.x Security Administrator Guide*.

3.2 Server Workload Considerations

The iFolder 3.*x* enterprise server supports a complex usage model where each user can own multiple iFolders and participate in iFolders owned by other users. Instead of a single user working from different workstations at different times, multiple users can be concurrently modifying files and synchronizing them. Whenever a user adds a new member to an iFolder, the workload on the server can increase almost as much as if you added another user to the system.

We recommend a maximum of 1000 users per iFolder server, depending on the performance characteristics of your hardware. You can set user account quotas to control the maximum storage space consumed by a user’s iFolders on the server. The actual bandwidth usage for each iFolder depends on the following:

- The number of members subscribed to the iFolder
- The number of computers actively sharing the iFolder
- How much data is stored in the iFolder
- The actual and average size of files in the iFolder
- The number of files in the iFolder
- How frequently files change in the file
- How much data actually changes
- How frequently files are synchronized
- The available bandwidth and throughput of network connections

We recommend that you set up a pilot program to assess your operational needs and performance based on your equipment and collaboration environment, then design your system accordingly.

The following is a suggested baseline configuration for an iFolder 3.*x* server with a workload similar to a typical iFolder 2.1*x* server. It is based on an example workload of about 12.5 GB of data throughput (up and down) each 24 hours, including all Ethernet traffic and protocol overhead. Your actual performance might differ.

Table 3-1 *Suggested Baseline Configuration for an iFolder Enterprise Server*

Component	Example System Configuration
Hardware	1.8 GHz Single processor
	1.2 GB RAM
	300 GB hard drive
iFolder Services	500 users
	500 MB user account quota per user
	1 iFolder per user that is not shared with other users
	5% change in each user's data per 24-hour period

3.3 Naming Conventions for Usernames and Passwords

LDAP Naming Requirement

Usernames and passwords must comply with the constraints set by your LDAP service. For information, see the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/treetitl.html).

E-Mail Address Naming Requirement

If you configure iFolder to authenticate users at login based on their e-mail addresses, make sure that each e-mail address in eDirectory satisfies the following naming requirements:

- Conforms to standard e-mail naming conventions
- Is unique in the directory

  For example, if two identical e-mail addresses exist in the directory, iFolder could synchronize both of them, but it attempts to authenticate only to the first matching e-mail address it finds. Authentication fails if the password does not match that address.

iFolder does not transform the address the user enters in any way and treats the names as case sensitive. Your users should be aware of the format and case used for their e-mail addresses that are stored in eDirectory.

For example, if user John Smith has an e-mail address based on a user ID of `js1234`, such as `js1234@example.com`, but is allowed to use an e-mail alias such as `john.smith@example.com`, which address should the user enter as the iFolder user name?

Length and Format Considerations for an LDAP Object

In iManager, the maximum number of characters for most LDAP objects is 64 characters. Some fields require common name format and others require fully distinguished name format for objects. View the iManager Help for the different plug-ins to make sure your entries comply with length and format restrictions for the individual plug-in.

Multilingual Considerations

If you have workstations running in different languages, you might want to limit User object names to characters that are viewable on all the workstations. For example, a name entered in Japanese cannot contain characters that are not viewable in Western languages.

IMPORTANT: eDirectory supports only English language characters for usernames and passwords on Linux and HP-UNIX. This applies to OES Linux and Novell Linux Desktop.

For information, see "Multilingual Considerations" (http://www.novell.com/documentation/edir873/edir873/data/a2iiidp.html#a2iiie7) in the *Novell eDirectory 8.7.3 Administration Guide.*

3.4 Admin User Considerations

During the iFolder install, iFolder creates two administrator users, the iFolder Admin user and the iFolder Proxy user. After the install, you can also configure other users with the iFolder Admin right to make them equivalent to the iFolder Admin user.

iFolder Admin User and Equivalent Users

The iFolder Admin user is the primary administrator of the iFolder enterprise server. Whenever iFolders are orphaned, ownership is transferred to the iFolder Admin user for reassignment to another user or for deletion. You initially specify the iFolder Admin user during the iFolder enterprise server configuration in YaST.

The iFolder Admin user must be provisioned to enable the iFolder Admin to perform management tasks. iFolder tracks this user by the LDAP object GUID, allowing it to belong to any LDAP container or group in the tree, even those that are not identified as Search DNs. The user's movement can be tracked anywhere in the tree because it is known by the GUID, not the user DN.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the Administrators page in the Novell iFolder 3 plug-in to add or remove the iFolder Admin right for users. Only users who are in one of the DNs specified in the LDAP Search DN are eligible to be equivalent to the iFolder Admin user.

If you assign the iFolder Admin right to other users, those users are governed by the roster and Search DN relationship. The user is removed from the roster and stripped of the iFolder Admin right if you delete the user, remove the user's DN from the list of Search DNs, or move the user to a DN that is not in the Search DNs.

iFolder Proxy User

The iFolder Proxy user is the identity used to access the LDAP server to retrieve lists of users in the specified containers, groups, or users that are defined in the iFolder LDAP settings. This identity must have the Read right to the LDAP directory. The iFolder Proxy user is created during the iFolder install. You probably never need to modify this value.

IMPORTANT: If you do modify the iFolder Proxy user, make sure that the identity you specify is different than the iFolder Admin user or other system users because the iFolder Proxy user password is stored in reversible encrypted form in the Simias database on the iFolder server.

When you initially configure the iFolder enterprise server in YaST, iFolder autogenerates a password for the iFolder proxy user.

Table 3-2 *Encryption Method for the iFolder Proxy User Password*

iFolder Version	Encryption Method	iFolder Proxy User Password
iFolder 3.2	YaST encryption method	Generates an alphanumeric, 13-digit, mixed-case password
iFolder 3.0 and 3.1	BASH random number generator	Generates a number between `0` and `10,000` and appends it to iFolderProxy. For example, `iFolderProxy1234`.

Initially, the password for the iFolder Proxy user is stored in clear text in the `/opt/novell/ifolder3/etc/simias-server-bootstrap.config` file. At the end of the configuration process, the system reboots Apache 2 and starts iFolder. When iFolder runs this first time after configuration, the iFolder process copies the `simias-server-bootstrap.config` file to the `Simias.config` file. The default location of the `Simias.config` file is `/var/lib/wwwrun/.local/share/simias` directory or the `/home/wwwrun/.local/share/simias` directory. The proxy user password is stored in a reversible encrypted form in the Simias database, then the value is removed from both configuration files.

The password stored on the system for the iFolder Proxy user must match the password stored in the iFolder Proxy user's eDirectory object. If you ever modify the iFolder Proxy user password in eDirectory, you must also change the password stored on the system. For example, if you change the iFolder Proxy user assignment, or if you want to set a longer password for the iFolder Proxy user, you must modify the values afterwards in iFolder's LDAP settings or iFolder cannot access the LDAP server to update the user list. For information, see Section 8.4.5, "Modifying the iFolder Proxy User Password," on page 86.

To secure access to the `Simias.config` file, administrators of the iFolder 3.*x* server computer must use every precaution to not inadvertently assign file system rights to the `/var/lib/wwwrun/.local/share/simias` directory or the `/home/wwwrun/.local/share/simias` directory to unauthorized users.

3.5 iFolder User Account Considerations

3.5.1 Preventing the Propagation of Viruses

Because iFolder is a cross platform, distributed solution there is a possibility of virus infection on Windows machines migrating across the iFolder server to other platforms, and vice versa. You should enforce server-based virus scanning to prevent viruses from entering the corporate network.

You should also enforce client-based virus scanning. For information, see “Configuring Local Virus Scanner Settings for iFolder Traffic” in the *iFolder User Guide for Novell iFolder 3.x*.

3.5.2 Provisioning User Accounts

You can specify any existing containers and groups in the Search DNs field of the iFolder LDAP settings to govern which users are automatically provisioned with accounts for iFolder services. The LDAP synchronization tracks a user object’s eDirectory™ GUID to identify the user in multiple contexts as you add, move, or relocate user objects, or as you add and remove contexts as Search DNs.

The following guidelines apply:

- If the user is added to an LDAP container, group, or user that is in the Search DN, the user is added automatically to the iFolder user list.
- If a user is moved to a different container, and the new container is also in the Search DN, the user remains in the iFolder user list.

  If you intend to keep the user as an iFolder user without interruption of service and loss of memberships and data, the new container must be added as a Search DN before the user is moved.

  If the user is moved to a different container that is not specified as a Search DN before the user is moved, the user is removed from the iFolder user list. The user’s iFolders are orphaned and the user is removed as a member of iFolders owned by others. If the new container is later added as a Search DN, the user is treated as a new user, with no association with previous iFolders and memberships.
- If the user appears in multiple defined Search DNs, if one or more DNs are removed from the LDAP settings, the user remains in the iFolder user list if at least one DN containing the user remains.
- If the user is deleted from LDAP or moved from all defined Search DNs, the user is removed as an iFolder user. The user’s iFolders are orphaned and the user is removed as a member of iFolders owned by others.
- The iFolder Admin user and iFolder Proxy user are tracked by their GUIDs, whether their user objects are in a context in the Search DN or not.

3.5.3 Setting Account Quotas

You can restrict the amount of space each user account is allowed to store on the server by setting an account quota. The account quota applies to the total space consumed by the iFolders the user owns. If the user participates in other iFolders, the space consumed on the server is billed to the owner of that iFolder. You can set quotas at the system or user. Within a give account quota, you can also set a quota for any iFolder.

3.6 iFolders Data and Synchronization Considerations

Consider the following when setting policies for iFolders data and synchronization:

- Section 3.6.1, "Naming Conventions for an iFolder and Its Folders and Files," on page 36
- Section 3.6.2, "Guidelines for File Types and Sizes to Be Synchronized," on page 36

3.6.1 Naming Conventions for an iFolder and Its Folders and Files

The iFolder client imposes naming conventions that consider the collective restrictions of the Linux, Windows, and Macintosh file systems. An iFolder, folder, or file must have a valid name that complies with the naming conventions before it can be synchronized.

Use the following naming conventions for your iFolders and the folders and files in them:

- iFolder supports the Unicode* (http://www.unicode.org) character set with UTF-8 encoding.
- Do not use the following invalid characters in the names of iFolders or in the names of folders and files in them:

  `\/:*?"<>|;`

  iFolder creates a name conflict if you use the invalid characters in a file or folder name. The conflict must be resolved before the file or folder can be synchronized.
- The maximum name length for a single path component is 255 bytes. For filenames, the maximum length includes the dot (`.`) and file extension.
- Names of iFolders, folders, and files are case insensitive; however, case is preserved. If filenames differ only by case, iFolder creates a name conflict. The conflict must be resolved before the file or folder can be synchronized.
- If users create iFolders on the FAT32 file system on Linux, they should avoid naming files in all uppercase characters. The VFAT or FAT32 file handling on Linux automatically changes the filenames that are all uppercase characters and meet the MS-DOS 8.3 file format from all uppercase characters to all lowercase characters. This creates synchronization problems for those files if the iFolder is set with the Read Only access right.

3.6.2 Guidelines for File Types and Sizes to Be Synchronized

You can set policies to govern which files are synchronized by specifying file type restrictions and the maximum file size allowed to be synchronized. You can set these policies at the system, user account, and iFolder level.

Some file types are not good candidates for synchronization, such as operating system files, hidden files created by a file manager, or databases that are implemented as a collection of linked files. You might include only key file types used for your business, or exclude files that are likely unrelated to business, such as `.mp3` files.

Operating System Files

You should not convert system directories to iFolders. Most system files change infrequently and it is better to keep an image file of your basic system and key software than to attempt to synchronize those files to the server.

Hidden Files

If your file system uses hidden files to track display preferences, you should determine the file types of these files and exclude them from being synchronized on your system. Usually, they are relevant only to the particular computer where they were created, and they change every time the file or directory is accessed. You do not need to keep these files, and synchronizing them results in repeated file conflict errors.

For example, iFolder automatically excludes two hidden file manager files called `thumbs.db` and `.DS_Store`.

Database Files

iFolder synchronizes the changed portions of a file; it does not synchronize files as a set. If you have a database file that is implemented as a collection of linked files, do not try to synchronize them in an iFolder.

Do not try to synchronize your GroupWise® data by making the GroupWise archive, cache, or remote directories into iFolders. If you do this, the GroupWise data files becomes corrupted after synchronizing the file a few times. GroupWise needs the files in the archive to be maintained as a set of files.

File Sizes

The maximum file size you allow for synchronization depends on your production environment. While some users work with hundreds of small files, other users work with very large files. You might set a system-wide policy to restrict sizes for most users, then set individual policies for power users.

3.7 Management Tools

Use the following tools to manage the Novell iFolder 3.*x* enterprise server and Web Access server.

- Section 3.7.1, "iFolder Configuration Plug-Ins for YaST," on page 38
- Section 3.7.2, "Novell iFolder 3 Plug-In for Novell iManager 2.5," on page 38
- Section 3.7.3, "Web Access Configuration File," on page 39

3.7.1 iFolder Configuration Plug-Ins for YaST

iFolder provides the following plug-ins to YaST for configuring basic parameters for your iFolder system:

iFolder Plug-In for YaST	Purpose	Tasks
iFolder 3	Use this function to configure the following parameters for the iFolder enterprise server. • LDAP server name, LDAP admin DN, and password • iFolder system name, store path, and description • iFolder proxy DN, password, and search context for retrieving user information from LDAP • iFolder admin DN and password	In YaST, click *Network Services*, then click *iFolder 3*. For information, see Section 6.2, "Configuring the iFolder Enterprise Server," on page 53.
iFolder 3 Web Access	Use this function to configure the following parameters for the iFolder Web Access server. • Web Access alias • iFolder server URL	In YaST, click *Network Services*, then click *iFolder 3 Web Access*. For information, see Section 6.3, "Configuring the iFolder Web Access Server," on page 55.

If both iFolder components are installed on the same computer, both plug-ins are available; otherwise, only the plug-in that is needed is available.

3.7.2 Novell iFolder 3 Plug-In for Novell iManager 2.5

The Novell iFolder 3 plug-in for Novell iManager 2.5 is an administrative tool used to manage the iFolder system, user iFolder accounts, and user iFolders and data. For information about installing iManager, see the *Novell iManager 2.5 Installation Guide* (http://www.novell.com/documentation/imanager25/imanager_install_25/data/hk42s9ot.html).

Before you can use Novell iFolder 3 for managing your iFolder system, you must install it in iManager. For information, see Section 6.4, "Installing the Novell iFolder 3 Plug-In for iManager," on page 57.

To access Novell iFolder 3, see Section 6.5, "Accessing iManager and the Novell iFolder 3 Plug-In," on page 59.

Web Browser Language Setting

An iManager plug-in might not operate properly if the highest priority Language setting for your Web browser is set to a language other than one of the supported languages. To avoid problems, in your Web browser's Languages setting, set the first language preference in the list to a supported language, such as English.

NOTE: In the initial release, iFolder supports only English. Localization in additional languages is planned for future releases.

Additional Information

For information about iManager, see the *Novell iManager 2.5 Administration Guide* (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/hk42s9ot.html).

3.7.3 Web Access Configuration File

Use the `/opt/novell/ifolder3/webaccess/Web.config` file to configure HTTP runtime parameters for your iFolder Web Access server. For information, see Section 9.4, "Configuring the HTTP Runtime Parameters," on page 98.

Coexistence and Migration Issues

4

One of the top priorities in designing Novell® iFolder® 3.*x* was to ensure that new iFolder services, running on Novell Open Enterprise Server, can be introduced into an existing network environment without disrupting existing Novell iFolder 2.1*x* services.

This section discusses the following the issues:

- Section 4.1, "Coexistence of iFolder 3.x and 2.1x Servers," on page 41
- Section 4.2, "Coexistence of the iFolder Client with Novell iFolder 1.x and 2.x Clients," on page 42
- Section 4.3, "Migrating from iFolder 2.1x to 3.x Server," on page 42
- Section 4.4, "Migrating User Files from an iFolder 2.1x to a 3.x Server," on page 42

4.1 Coexistence of iFolder 3.*x* and 2.1*x* Servers

If you use both Novell iFolder 3.*x* and iFolder 2.1*x* servers, we recommend that you install each version on its own dedicated server. However, iFolder 3.*x* enterprise and Web access servers can coexist with an iFolder 2.1*x* server on an OES Linux computer under the following conditions:

- Both iFolder 3.*x* and iFolder 2.1*x* run Apache 2 Worker. However, iFolder 2.1*x* runs a special configuration of Apache 2 Worker where the number of threads is limited. iFolder 3.*x* runs with the default Apache 2 Worker configuration that comes with OES. The separate instances of Apache run in parallel, with no interaction between them.
- You must use different IP addresses for the iFolder 3.*x* enterprise server and the iFolder 2.1*x* server running on the same computer. The iFolder 3.x enterprise server and iFolder 3.x Web access server share the same IP address when they are on the same server.
- The processor, memory, network adapter, and storage disks on the computer must be sized to support the combined workload and storage requirements for the iFolder servers.
- iFolder 3.*x* and 2.1*x* are not integrated in any way.
  - They are different software packages and share no files in common.
  - They use different methods and settings for management, security, policies, data storage, user provisioning, Web access, and backup.
  - They do not share or coordinate information about servers, LDAP, administrators, users, or iFolders.
  - There are no storage economies for or coordination of iFolder files and data.
  - Users must use each server's corresponding iFolder client to access their iFolder data on that server.
  - Users must use the corresponding access method to access their iFolder data via a Web browser. iFolder 3.*x* requires the iFolder 3.*x* Web access server, and iFolder 2.1*x* requires Novell NetStorage.

For more information, see Section 2.4, "Comparison of 2.1x and 3.x Server Features and Capabilities," on page 22.

4.2 Coexistence of the iFolder Client with Novell iFolder 1.*x* and 2.*x* Clients

Do not install the iFolder™ client in the same application folder as the Novell iFolder 1.x or 2.x client.

The iFolder client can coexist on the same workstation as the Novell iFolder 1.*x* client or 2.*x* client, with the following caveats:

- The iFolder client and its iFolders work only with the Novell iFolder 3.*x* enterprise server.
- The Novell iFolder 1.*x* or 2.*x* client and its iFolder on the workstation continue to work only with the assigned Novell iFolder server of the same release.
- The single iFolder created with the iFolder 1.*x* or 2.*x* client can coexist with the multiple iFolders created with the iFolder client. The iFolders function independently on the workstation; they do not exchange information or data. However, you can manually transfer local data between old and new iFolder folders.
- You should not attempt to convert the iFolder for Novell iFolder 1.*x* or 2.*x* to an iFolder to be managed by Novell iFolder 3.*x*. Similarly, you should not covert parent folders of that iFolder to a next-generation iFolder.

  If the folder is no longer used by a prior version of the Novell iFolder client, such as when you uninstall the old client from the workstation, you can convert the folder or its parent folders to a next-generation iFolder.

For more information, see Section 2.5, “Comparison of 2.1x and 3.x Client Features and Capabilities,” on page 25.

4.3 Migrating from iFolder 2.1*x* to 3.*x* Server

There is no migration path between Novell iFolder 2.1*x* and Novell iFolder 3.*x*. There is no migration of configuration, policies, user information, and iFolder data on the server.

4.4 Migrating User Files from an iFolder 2.1*x* to a 3.*x* Server

The Novell iFolder 2.1*x* client and the iFolder client for Novell iFolder 3.*x* can run independently and concurrently on the same user computer. They are separate applications and should not be installed in the same location.

There is no automatic upgrade or migration from Novell iFolder 2.1*x* to the iFolder client for Novell iFolder 3.*x*. Each user can manually copy some or all of the files in the iFolder 2.1*x* directory to one or more iFolders for synchronization by an iFolder 3.*x* enterprise server.

Make sure to review the Section 2.5, “Comparison of 2.1x and 3.x Client Features and Capabilities,” on page 25. Some features, such as encrypted data storage on the server, are not available in the new iFolder client. You might make both servers available to users if encrypted data storage is essential for some of their files. Work with users to determine what their needs are for encrypted data on the server.

For information about migrating files from iFolder 2.1*x* to iFolders for the iFolder 33.*x* enterprise server, see "Migrating Files from iFolder 2.1x to 3.x" in the *iFolder User Guide for Novell iFolder 3.x*. After users have successfully migrated their files to the new system, you can determine the need to maintain a 2.1*x* server in your environment.

Prerequisites and Guidelines

5

This section discusses prerequisites and guidelines for this release of Novell® iFolder® 3.*x* and the iFolder™ Client. Before installing and configuring iFolder, make sure that your system meets the requirements in each of the following:

- Section 5.1, “File System,” on page 45
- Section 5.2, “Enterprise Server,” on page 45
- Section 5.3, “Novell eDirectory 8.7.3,” on page 48
- Section 5.4, “Novell iManager 2.5,” on page 48
- Section 5.5, “Mono,” on page 48
- Section 5.6, “Client Computers,” on page 49
- Section 5.7, “Web Browser,” on page 49

5.1 File System

iFolder Application Files

iFolder 3.*x* installs the iFolder files on the system volume. OES Linux requires the Reiser (default) or EXT3 file system for the system device.

iFolder Data Store

We recommend that you store the users’ iFolder data on a separate volume.

Version	Data File System Support
iFolder 3.1 and later	EXT3, ReiserFS, or NSS
iFolder 3.0	EXT3 or ReiserFS

5.2 Enterprise Server

We recommend that you install iFolder 3.*x* enterprise server and Web Access server after your OES Linux system is configured and running properly. You must post-install iFolder if you plan to use NSS volumes for your iFolder data because you cannot set up NSS volumes during an OES Linux install. However, if you plan to use a Linux traditional volume such as EXT3 or ReiserFS for your iFolder data, you can optionally install and configure iFolder when you install OES Linux.

- Section 5.2.1, “Prerequisites for the Operating System,” on page 46
- Section 5.2.2, “Install Guidelines When Using an NSS Volume to Store iFolder Data,” on page 46
- Section 5.2.3, “Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data,” on page 47
- Section 5.2.4, “Install Guidelines for Other Components,” on page 47

- Section 5.2.5, “Installing the OES Linux Server,” on page 47

5.2.1 Prerequisites for the Operating System

Novell iFolder 3.*x* supports a server platform with the following components of Novell Open Enterprise Server:

iFolder Version	Operating System and Applications
iFolder 3.2	Novell Open Enterprise Server Support Pack 2 for SUSE® Linux (OES Linux SP2)
	SUSE Linux Enterprise Server 9 Support Pack 3 (SLES 9 SP3)
iFolder 3.1	Novell Open Enterprise Server Support Pack 1 for SUSE® Linux (OES Linux SP1)
	SUSE Linux Enterprise Server 9 Support Pack 2 (SLES 9 SP2)
iFolder 3.0	Novell Open Enterprise Server for SUSE Linux (OES Linux)
	SUSE Linux Enterprise Server 9 Support Pack 1 (SLES 9 SP1)

There is no upgrade or migration path from Novell iFolder 2.1x and earlier versions of iFolder.

For information, see the Novell Open Enterprise Server product site (http://www.novell.com/products/openenterpriseserver).

5.2.2 Install Guidelines When Using an NSS Volume to Store iFolder Data

Modify the OES Linux install and configuration to comply with the following guidelines:

- In YaST, on the *Installation Settings* page, reconfigure the *Partitioning* settings as needed to support using NSS.
  - Specify a ReiserFS (default) or EXT3 partition as your system device.
  - NSS volumes are configured after the install is complete. If you plan to use NSS volumes, some deployment scenarios require that you modify the partitioning to use EVMS (Enterprise Volume Management System) as the device manager of the system device instead of LVM (Linux Volume Manager, default) or a third-party volume manager. Make sure to compare your storage deployment plan to those listed in “Installing Linux with EVMS as the Volume Manager of the System Device” in the *Open Enterprise Server* to determine if you need to do this.

    For example, if you have only a single device on the server (such as a single physical disk or a hardware RAID 1 or RAID 5 device) and you plan to configure an NSS volume to use as your iFolder data volume, you must modify your partitioning to use EVMS to manage the device.
- In YaST, on the Installation Settings page, modify the Software components to add the NSS package to the install. Plan to install iFolder after your OES Linux server is set up and you have created an NSS volume to use.
- In YaST, on the Installation Settings page, make sure you do not add the iFolder 3 or iFolder 3 Web Access components to the install. You will install them later.

- After the OES Linux system is up and running, use the Storage plug-in to iManager to create the NSS volume, create a directory at the volume root, then use YaST to install and configure iFolder. Make sure to specify the path to the directory as the iFolder data store during the iFolder configuration.

5.2.3 Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data

- In YaST, specify an EXT3 or ReiserFS partition as your system device.
- (Optional) Modify the Software components to add the iFolder 3 or iFolder 3 Web Access components to the install.

  If you install iFolder at this time, be prepared to configure iFolder as part of the install process. See the following:

  - Section 6.2, "Configuring the iFolder Enterprise Server," on page 53
  - Section 6.3, "Configuring the iFolder Web Access Server," on page 55

5.2.4 Install Guidelines for Other Components

We recommend that your iFolder enterprise server and Web Access server run on separate dedicated servers. For small office use, both enterprise server and Web access server can run on the same server without degraded performance. For best performance, configure your iFolder server as an independent system with, at most, the following services:

- OES Linux (Minimum predefined server plus graphics support and NSS if desired)
- Novell eDirectory 8.7.3 (can be configured on a different OES server)
- Novell iManager 2.5 (can be configured on a different OES server)
- Novell iFolder 3.*x* (typically post-installed on an OES Linux server)
  - Enterprise server
  - Web Access server (can be installed and configured on a different OES Linux server)
  - Mono (The Mono package is required for iFolder 3.*x* enterprise server and for Web Access server.)
  - Apache 2 Web Server (The apache2-worker package is required for iFolder 3.*x* enterprise server and for Web access server.)
  - Other iFolder dependencies as noted in YaST by the iFolder 3.x and iFolder 3.x Web Access install packages.

Installing other applications or services on the iFolder server affects iFolder performance and might introduce conflicts with the required versions of applications iFolder depends on, such as Apache 2 or Mono.

5.2.5 Installing the OES Linux Server

For detailed information about prerequisites, installation, and configuration of your OES Linux server, see the *OES for Linux Installation Guide* (http://www.novell.com/documentation/oes/install_linux/data/front.html).

5.3 Novell eDirectory 8.7.3

Novell eDirectory™ 8.7.3 is a secure identity management solution that provides centralized identity management, infrastructure, Net-wide security, and scalability to all types of applications running behind and beyond the firewall. It natively supports the directory standard Lightweight Directory Access Protocol (LDAP) 3 and provides support for TLS/SSL services based on the OpenSSL source code. eDirectory is available as a component of Novell Open Enterprise Server.

Before you configure iFolder, eDirectory must be configured and running. In iFolder, you specify LDAP containers and groups that contain User objects of users who you want to be iFolder users. You must create contexts and define users in eDirectory. For information, see the following topics in the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a2iii88.html):

- "Designing Your Novell eDirectory Network" (http://www.novell.com/documentation/edir873/edir873/data/a2iiido.html)
- "Managing User Accounts" (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html)

Make sure your LDAP objects comply with the naming conventions for your LDAP services. For information, see Section 3.3, "Naming Conventions for Usernames and Passwords," on page 32.

5.4 Novell iManager 2.5

Novell iManager 2.5 is a Web-based administration console that provides secure, customized access to network administration utilities and content. Before you can configure the Novell iFolder 3 plug-in for iManager, iManager must be installed and configured.

For information, see the *Novell iManager 2.5 Administration Guide* (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/hk42s9ot.html).

5.5 Mono

Novell iFolder 3.*x* requires the Mono® framework for Linux. Mono is a development platform for running and developing modern applications. Based on the ECMA/ISO Standards, Mono can run existing programs that target the .NET or Java frameworks. The Mono Project is an open source effort led by Novell and is the foundation for many new applications. For information about Mono, see the Mono Project Web site (http://www.mono-project.com/Main_Page).

The required version of Mono is included on the `.iso` files. Mono is installed automatically as a dependency of iFolder during the install of the iFolder enterprise server or the Web Access server.

The iFolder clients for Linux and Macintosh also require Mono 1.1.7. The required version of Mono is packaged in the iFolder client installation files that you distribute to your users. For information, see Section 6.7, "Distributing the iFolder Client to Users," on page 62. Linux and Macintosh users must install both iFolder and Mono packages. For information, see "Getting Started" in the *iFolder User Guide for Novell iFolder 3.x*

Make sure to use the required version of Mono. If you have a different version of Mono on your OES Linux server, uninstall it before you install iFolder.

Novell iFolder 3.*x* supports only the version of Mono included in its install software. If you need to upgrade Mono for another reason, please check our online documentation to see if we explicitly support that version and to learn any necessary steps to make the upgrade work correctly. For information, see the latest version of the online documentation on the Novell iFolder 3.*x* Documentation Web site (http://www.novell.com/documentation/ifolder3).

5.6 Client Computers

The iFolder client supports the following workstation operating systems:

- Novell Linux Desktop 9 and later (requires Mono 1.1.7.1.44342 for Linux)
- Windows 2000/XP/2003 with the latest .NET support patches
- Macintosh OS X v10.3 and later (requires Mono 1.1.7.2 for Macintosh).

The Mono modules you need for this release are included on the `.iso` files for iFolder 3.*x*.

Make sure you have installed the latest critical updates for your operating system or .NET.

5.7 Web Browser

You need one or more of the following supported Web browsers on the computer you use to access iManager and on the client computers:

- Mozilla* Firefox*
- Microsoft* Internet Explorer
- Safari* on Macintosh

Installing and Configuring iFolder Services

6

This section describes how to install and configure Novell® iFolder® 3.*x* enterprise and Web Access servers.

6.1 Installing iFolder on an Existing OES Linux Server

We recommend that you install iFolder after your server operating system is installed and all storage services are configured. The following procedure describes how to install iFolder enterprise server, iFolder Web access server, or both of the servers on an existing OES Linux platform. If you install only one of the iFolder servers, repeat the entire install process for the other on a second OES Linux server.

The Novell iFolder install modules are available on media for the Support Pack releases of OES Linux.

NOTE: If you used the Minimum install option for your OES Linux server, which has no GUI installed, the iFolder services configuration is done with the YaST 2 text-based interface. For example, there are no check boxes and clicking is not possible. Use the standard methods for navigating the text-based interface to achieve the tasks as described here.

1 Before you begin, make sure your OES Linux system setup meets the "Prerequisites and Guidelines" on page 45.

2 If you have previously installed Mono on your OES SP1 server, make sure the permissions on Mono directories are set correctly.

This should set the rights correctly for Mono, and enable iFolder 3.1 enterprise server to run.

2a On your Linux computer, open a shell window.

2b At the prompt, log in as the root user by entering `su`, then entering your root password.

2c At the prompt, enter

```
cd /usr/lib
```

2d Change the Mono permissions in the `/usr/lib` directory. At the prompt, enter

```
chmod 755 -R mono
```

2e At the prompt, enter

```
cd /etc
```

2f Change the Mono permissions in the `/etc` directory. At the prompt, enter

```
chmod 755 -R mono
```

3 Open YaST2 using one of the following methods:

- On your desktop, click the *YaST* shortcut icon to launch YaST, then enter the root password when prompted.
- At a terminal, log in as the root user, then enter

```
yast2
```

4 In the left menu, select *Software*, then select *Install and Remove Software*.

A window appears in the upper left with a *Filter* drop-down menu preselected to the *Search* option.

5 Use the *Filter* drop-down menu to specify the *Selections* option.

6 You can install the iFolder 3 Enterprise Server and Web Access Server on the same computer or on different computers. Do one or both of the following, depending on your deployment preferences:

- **iFolder 3:** In the left *Selections* menu, locate and select *Novell iFolder 3*, then select its check box to signify that you want to install the RPMs for Novell iFolder 3 and its dependencies.
- **iFolder 3 Web Access:** In the left *Selections* menu, locate and select *Novell iFolder 3 Web Access*, then select its check box to signify that you want to install the RPMs for Novell iFolder 3 Web Access and its dependencies.

IMPORTANT: If you install only one of the components, repeat the entire install process for the other on your second server.

You might need to scroll down to locate the entries. All of the RPMs in the Package list should be selected for install (check mark) or for upgrade (green and black arrow icon).

7 If you encounter any dependency conflicts, resolve them before continuing.

8 To begin the installation, click *Accept* at the bottom right of the screen.

9 When the installation is complete, close YaST.

10 Continue with one or both of the following as needed:

- Section 6.2, “Configuring the iFolder Enterprise Server,” on page 53
- Section 6.3, “Configuring the iFolder Web Access Server,” on page 55

IMPORTANT: If you have problems with Mono after the install, check the POSIX* permissions on Mono directories to make sure they comply with the settings in Step 2 of the iFolder installation.

6.2 Configuring the iFolder Enterprise Server

After you install the iFolder enterprise server, you must configure the iFolder services, including the LDAP, iFolder system, and iFolder administration settings.

IMPORTANT: If you install iFolder when you install OES Linux, the same parameters described in this procedure are available as an integrated part of the server install. However, you cannot choose an NSS volume as the iFolder *System Store Path* because NSS volumes cannot be created during the server platform install.

1 If you plan to use an NSS volume as the System Store Path for the users' iFolder data, use iManager to create the NSS volume, then create a directory on the volume.

   For information, see "Managing NSS Volumes" in the *Open Enterprise Server*.

2 Log in to the server as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.

3 Start YaST to refresh its list of installed configuration modules.

4 Start YaST, click *Network Services*, then click *iFolder 3*.

5 Follow the Yast on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

   IMPORTANT: If you ever need to run the configuration again, you can modify any field except the *System Store Path* and the *iFolder User Login Based on Which LDAP Attribute* options. These parameter settings cannot be modified after the initial configuration.

Install Settings	Description
LDAP Server Configuration	• **Local or Remote Directory Server:** Select *Local* if your LDAP directory services are running on the same server as the iFolder 3 enterprise server. Otherwise, select *Remote*. • **Directory Server Address:** If directory services are Remote, specify the IP address of the LDAP server to use for this iFolder enterprise server. • **LDAP Admin Name:** The fully distinguished name of the Admin user with administrative rights to LDAP. This information is needed during the configuration to create User objects for the administrative iFolder Proxy user. The LDAP schema is not extended. Specify an existing username and an existing context. If the user does not already exist, the username is created only if the context is valid. For example: `cn=admin.o=acme` • **LDAP Admin Password:** Specify the LDAP Admin user's password. • **iFolder User Login Based on Which LDAP Attribute:** Specify which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Options are Common Name (`cn`, default) and e-mail address (`mail`). This setting cannot be changed after the install. For example, if a user named John Smith has a common name of `jsmith` and e-mail of `john.smith@example.com`, this field determines whether the user enters `jsmith` or `john.smith@example.com` as the *Username* when logging in to the iFolder server.

Install Settings	Description

iFolder System Configuration	• **System Name:** A unique name to identify your iFolder 3 server.
	For example, `IF3EAST Server`.
	• **System Store Path:** The case-sensitive location where this iFolder enterprise server stores the iFolder 3.*x* application files and the users' iFolders and files. This location cannot be modified after the initial configuration.
	The store path should not be set at the root of a volume, such as the root (`/`) or the root of a mount point (for example, `/mnt/ifolder3`). Make sure to add a standard directory to the end of the path. For example:
	`/var/opt/novell/ifolder3/data`
	`/ifolder3/data`
	`/mnt/ifolder3/data`
	• **System Description:** A descriptive label for your iFolder 3 server.
	For example, `iFolder 3 Eastern Server`.

iFolder Admin Configuration	• **iFolder Admin DN:** The iFolder Admin user manages iFolder services with the iFolder 3 plug-in to iManager. If it does not already exist, this user is created and granted the necessary rights to manage all iFolder services. Specify the fully distinguished name of the iFolder Admin user.
	For example:
	`cn=ifolderadmin.o=acme`
	• **iFolder Admin User Password:** The password to use for the iFolder Admin user. Type the password again to verify the entry.
	• **Proxy Context:** The existing context where you want to create the iFolder Proxy user. A generated username and password are used to create the user in the specified context, then the user is granted the Read right to LDAP. The generated username is `iFolderProxy`*`xxxx`*, where *`xxxx`* is a four-digit random number.
	For example:
	`o=acme`
	You should never have to modify the user and password for the iFolder Proxy user, but it is possible. For information, see Section 8.4.2, "Modifying the iFolder LDAP Settings," on page 84.

6 When the system prompts you to restart the Apache server, accept the option by clicking *Yes*, then restart the Apache server and Tomcat Web application. This is necessary to use the new settings.

6a Open a terminal console, then log in as the root user.

6b Stop the Apache server by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 stop
```

```
rcapache2 stop
```

6c Stop Tomcat by entering either of the following commands at the prompt:

```
/etc/init.d/novell-tomcat4 stop
```

```
rcnovell-tomcat4 stop
```

6d Start Tomcat by entering either of the following commands at the prompt.

```
/etc/init.d/novell-tomcat4 restart
```

```
rcnovell-tomcat4 start
```

6e Start Apache by entering either of the following commands at the prompt:

```
/etc/init.d/apache2 start
```

```
rcapache2 start
```

7 Go to Novell iManager to install the Novell iFolder 3 plug-in or to manage iFolder services.

For information, see Installing the Novell iFolder 3 Plug-In for iManager. Use the plug-in to provision users for services and to manage iFolder services, user access, and iFolders.

6.3 Configuring the iFolder Web Access Server

After you install the iFolder Web Access server, you must specify which iFolder enterprise server it supports and the user-friendly URL that users enter in their Web browsers to access it.

IMPORTANT: If you install iFolder when you install OES Linux, the same parameters described in this procedure are available as an integrated part of the server install.

Configuring Web Access

1. Log in as the root user, or open a terminal console, enter `su`, then enter a password to log in as root.
2. Start YaST to refresh its list of installed configuration modules.
3. When YaST opens, click *Network Services*, then click *iFolder 3 Web Access*.
4. Follow the Yast on-screen instructions to proceed through the iFolder 3 Web Access configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Access Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`

Install Settings	Description
iFolder Server URL	The iFolder 3 Web Access server and the iFolder 3 enterprise server can reside on the same computer or on different computers. Specify the URL and port number of the iFolder 3 enterprise server served by this instance of Web Access. Make sure to specify secure HTTP (`https://`) in the URL for secure communications between the enterprise server and the Web Access server. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering. By default, the iFolder enterprise server is configured to communicate with the iFolder Web Access server via SSL (HTTPS). For most deployments, this setting should not be changed. If the iFolder deployment is small so that you can install both the Web Access server and the iFolder enterprise server on the same machine, you can optionally specify HTTP (`http://`) to use clear traffic, which would increase the performance of local communications between the two servers. For example, use `https://192.168.1.1:443` (different servers) or `http://localhost:80` (same server).

5 When the system prompts you to restart the Apache server, accept the option by clicking *Yes*.

Restarting Apache is necessary to use the new settings.

6 (Optional) Tune the performance of the Web Access server by configuring its HTTP runtime parameters.

For information, see Section 9.4, “Configuring the HTTP Runtime Parameters,” on page 98.

7 If it is not already installed, go to Novell iManager to install the Novell iFolder 3 plug-in or to manage iFolder services.

For information, see Installing the Novell iFolder 3 Plug-In for iManager. You use the plug-in to provision users for services and to manage iFolder services, user access, and iFolders. There are no specific Web Access settings to with the plug-in.

Reconfiguring Web Access

If you run the iFolder 3.*x* Web Access configure again, a new link is created on the Novell iFolder 3.*x* Welcome page to point to the new Web Access Alias. It does this whether you actually change the alias or not. It does not delete the old link when it adds the new one. Each Web Access link in the iFolder Links area of the Welcome page is indistinguishable by its link name alone.

After you finish reconfiguring Web Access, you must manually remove the old URL from the WebLink section in the `/var/opt/novell/tomcat4/webapps/welcome/WEB-INF/XMLData/ifolder3.xml` file.

For example, edit the file to remove a WebLink section like this one where the Web Access Alias value is *`ifolder`*:

```
<WebLinkType>0</WebLinkType>

  <URLDescriptor>Open iFolder 3.x Web Access</URLDescriptor>

  <Login>
```

```
    <URL>https://%*reqservername%/ifolder</URL>
  </Login>
</WebLink>
```

6.4 Installing the Novell iFolder 3 Plug-In for iManager

Before you can manage Novell iFolder 3 services, you must install the iFolder iManager Module for Novell iManager 2.5. After it is installed, this plug-in is named Novell iFolder 3 in the iManager Roles and Tasks list.

Make sure you meet prerequisites, then use one of the methods for installing the iFolder plug-in:

- Section 6.4.1, “Prerequisites,” on page 57
- Section 6.4.2, “Installing a Plug-In When RBS Is Not Configured,” on page 57
- Section 6.4.3, “Installing a Plug-In When RBS Is Configured,” on page 58

6.4.1 Prerequisites

Novell iManager 2.5

If you have not already done so, install Novell iManager 2.5 on the same or different server as your iFolder server. For information, see *Novell iManager 2.5 Installation Guide* (http://www.novell.com/documentation/imanager25/imanager_install_25/data/hk42s9ot.html)

Role-Based Services

The iFolder 3 plug-in supports the optional use of Role Based Services (RBS) in Novell iManager. RBS gives you the ability to assign specific tasks to iManager admin users and to present the admin user with only the tools necessary to perform a specified set of tasks or manage only objects as determined by their roles. What admin users see when they access iManager is based on their role assignments in Novell eDirectory™. Only the roles and tasks assigned to that user are displayed.

For information, see “Configuring Role-Based Services” (http://www.novell.com/documentation/edir873/edir873/data/a31aexm.html) in the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a2iii88.html)

6.4.2 Installing a Plug-In When RBS Is Not Configured

If you do not have Role-Based Services (RBS) configured for Novell eDirectory™, install the iFolder Manager Module as follows:

1 In a Web browser, log in to iManager on the iFolder server where you installed iManager.

   `https://ifolder.example.com/nps/iManager.html`

   Replace `ifolder.example.com` with the IP address (such as `192.168.1.1`) or the DNS name of the iFolder server.

   If you installed iManager on a different server in the same tree as your iFolder server, log in to iManager on that server.

2 In the toolbar, click the *Configure* icon (person seated behind a desk).

3 In Roles and Tasks, expand *Module Installation*, then click *Available Novell Plug-In Modules*.

4 Locate the *iFolder iManager Module* plug-in, select its plug-in check box, then click *Install*.

This install takes a few minutes. You should receive a message confirming a successful install.

5 Click *OK* to dismiss the message, then close iManager.

6 Stop and start the Tomcat servlet engine by entering the following command at the server console:

```
/etc/init.d/novell-tomcat4 restart
```

Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log in to iManager.

7 Verify that the plug-in is enabled by opening iManager in a Web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of Roles and Tasks.

For information, see Section 6.5, “Accessing iManager and the Novell iFolder 3 Plug-In,” on page 59.

8 Continue with Section 6.6, “Provisioning Users and iFolder Services,” on page 60.

6.4.3 Installing a Plug-In When RBS Is Configured

If you are running iManager in Assigned Mode and have RBS configured for eDirectory, complete the following steps to install the iFolder iManager Module.

IMPORTANT: To re-install an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory, using the *Module Configuration* > *Delete RBS Module* task.

1 In a Web browser, log in to iManager as an RBS Collection Owner on the system where you installed iFolder.

```
https://ifolder.example.com/nps/iManager.html
```

Replace *ifolder.example.com* with the IP address (such as 192.168.1.1) or the DNS name of the iFolder server.

2 In the toolbar, click the *Configure* icon (person seated behind a desk).

3 In Roles and Tasks, expand *Module Installation*, then click *Available Novell Plug-In Modules*.

4 Locate the iFolder iManager Module, select its plug-in check box, then click *Install*.

This install takes a few minutes. You should receive a message confirming a successful install.

5 Click *OK* to dismiss the message, then close iManager.

6 Stop and start the Tomcat servlet engine by entering the following command at the server console:

```
/etc/init.d/novell-tomcat4 restart
```

Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log in to iManager.

7 After Tomcat initializes, in a Web browser, log in to iManager as a Collection Owner again.

8 Click the *Configure* icon.

9 Under *Role-Based Services*, select *RBS Configuration*.

The table on the Collections tabbed page displays modules ready to update.

10. Locate the collection where you want to install the plug-in, then click its *Out-of-Date* number.

    The *iFolder iManager Module* plug-in should be displayed under *Modules Not Yet Installed* column.

11. Select the *iFolder iManager Module* plug-in.
12. Click *Update*.
13. Wait for the Completed message, then click *OK* to continue.
14. Verify that the plug-in is enabled by opening iManager in a Web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of *Roles and Tasks*.

    For information, see Section 6.5, “Accessing iManager and the Novell iFolder 3 Plug-In,” on page 59.

15. Continue with Section 6.6, “Provisioning Users and iFolder Services,” on page 60.

6.5 Accessing iManager and the Novell iFolder 3 Plug-In

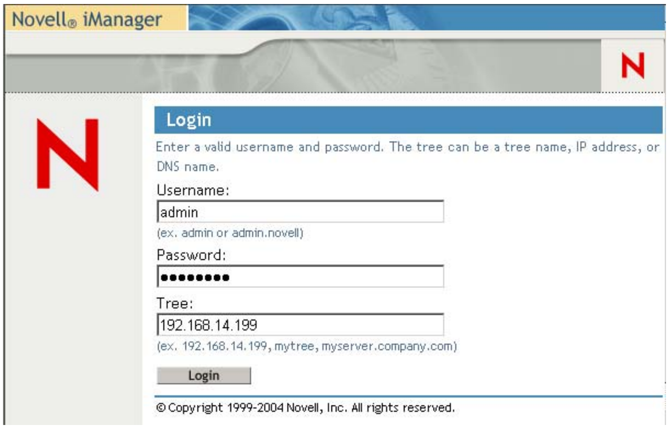
The Novell iFolder 3 plug-in to Novell iManager 2.5 is the tool used to manage your iFolder server. For information, see Section 6.4, “Installing the Novell iFolder 3 Plug-In for iManager,” on page 57.

1. Open a Web browser to the iManager Login page by entering the following location:

    ```
    http://servername.example.com/nps/iManager.html
    ```

    Replace `servername.example.com` with the DNS name or IP address (such as `192.168.1.1`) of the OES Linux server where you installed iManager. This might be the same or different computer where you installed iFolder 3.*x* or iFolder 3.*x* Web Access.

2. (Conditional) If prompted to accept the server’s certificate, review the certificate information, then click *OK* to accept it if it is valid.
3. On the iManager Login page, specify the Admin username and password you created during the OES Linux install, then click *Login*.



Login

Enter a valid username and password. The tree can be a tree name, IP address, or DNS name.

Username: admin

(ex. admin or admin.novell)

Password: ••••••••

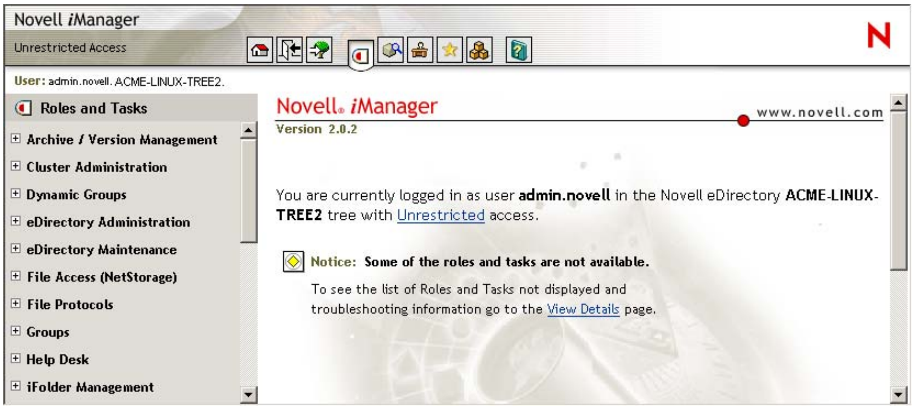
Tree: 192.168.14.199

(ex. 192.168.14.199, mytree, myserver.company.com)

© Copyright 1999-2004 Novell, Inc. All rights reserved.

The user name can be specified as contextless (such as *admin*) or with the context (such as `cn=admin.o=acme`). You must use a dot delimiter in fully distinguished names when working in iManager.

The iManager Web management interface opens with Roles and Tasks listed in the navigator on the left.



You are currently logged in as user **admin.novell** in the Novell eDirectory **ACME-LINUX-TREE2** tree with Unrestricted access.

Notice: Some of the roles and tasks are not available.

To see the list of Roles and Tasks not displayed and troubleshooting information go to the View Details page.

4 In Roles and Tasks, click *Novell iFolder 3 > System*.

The Connect Login page opens.

5 Log in to connect to the iFolder 3.*x* enterprise server you want to manage.

For information, see Section 8.2, “Connecting to the iFolder Server,” on page 80.

Novell iFolder 3.*x* opens to the System Management page, which consists of a tabbed list of the main administrative functions that can be performed on iFolder.

6.6 Provisioning Users and iFolder Services

After you configure your Novell iFolder 3.*x* enterprise server, you must specify containers and groups as Search DNs in the LDAP settings. iFolder uses these to provision user accounts.

- Section 6.6.1, “Prerequisites,” on page 60
- Section 6.6.2, “Configuring the Search DNs for Provisioning Users,” on page 61
- Section 6.6.3, “Synchronizing the List of Provisioned Users with the LDAP Directory,” on page 61

6.6.1 Prerequisites

iFolder Plug-Ins

The iFolder plug-in in Novell iManager 2.5 must be installed, and the iManager server must be running. For information, see Section 6.4, “Installing the Novell iFolder 3 Plug-In for iManager,” on page 57.

Users and LDAP Contexts

The contexts you plan to use as Search DNs in the LDAP settings must exist in the LDAP directory; they are not created and configured from within the iFolder plug-in.

For information about configuring user, group, and container objects, see the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/treetitl.html).

6.6.2 Configuring the Search DNs for Provisioning Users

All users in the containers and groups listed in the iFolder LDAP settings' Search DN field are automatically provisioned as iFolder users.

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

2 Select *LDAP* to open the System page to the LDAP tab, then click *Modify*.

3 Repeat the following for each context you want to add or modify:

3a Specify the context:

- **Add:** Type the DN of the LDAP context you want to add in the *Search DN* field.
- **Search:** To search, click the *Search* icon to open a browsable list of LDAP objects, then select the context to add.

  The LDAP object selector is not available if you logged into iManager in a different LDAP tree than the one where the Server Host (iFolder's LDAP server) resides.
- **Edit:** To edit a value, select it from the list of Search DNs, click the *Edit* icon (pen), then make your changes.

DNs are entered in LDAP format. For example:

```
o=acme
```

```
ou=group,o=acme
```

The iFolder Admin User is provisioned for services during the install. It is tracked by its GUID, so it is available even if the Search DN is empty, or if you specify Search DNs that do not contain the Folder Admin user. This identity must be provisioned to enable the iFolder Admin to perform management tasks.

3b Click *OK* to apply the change.

4 Continue with Section 6.6.3, "Synchronizing the List of Provisioned Users with the LDAP Directory," on page 61.

To modify LDAP settings at any time, see Section 8.4, "Configuring the LDAP Settings for an iFolder Server," on page 82.

6.6.3 Synchronizing the List of Provisioned Users with the LDAP Directory

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

2 Select *LDAP* to open the System page to the LDAP tab, then click *Modify*.

3 Click *Update and Synchronize Now*.

During LDAP synchronization, the iFolder server queries the LDAP server to retrieve a list of users in the DNs as specified in the Search DN field. This might take several minutes, depending on the size of your LDAP directory.

4 Continue with Section 6.7, "Distributing the iFolder Client to Users," on page 62.

The iFolder User list is updated periodically based on the LDAP synchronization interval. Whenever you remove users from a LDAP Search DN, or remove contexts from the Search DN list, you should synchronize the list immediately using Update and Synchronize now to enforce your changes. For information, see Section 8.4.6, "Synchronizing the iFolder User List with the LDAP Server," on page 87.

6.7 Distributing the iFolder Client to Users

After you configure iFolder services on the enterprise server, users can download the install files for the iFolder client from the iFolder 3.*x* Welcome page.

- Section 6.7.1, "Configuring the iFolder 3.x Welcome Page," on page 62
- Section 6.7.2, "Accessing the iFolder 3.x Welcome Page," on page 62
- Section 6.7.3, "Downloading the iFolder Client," on page 63
- Section 6.7.4, "Installing the iFolder Client," on page 63

6.7.1 Configuring the iFolder 3.*x* Welcome Page

The iFolder 3.*x* enterprise server installs the client install files in the `/var/opt/novell/tomcat4/webapps/ifolder3-client/` directory. The references to these files are in the `/var/opt/novell/tomcat4/webapps/welcome/WEB-INF/XMLData/ifolder3.xml` file.

After the iFolder 3.*x* enterprise server install, you must restart Tomcat 4 to install the iFolder 3.*x* link in the OES Welcome pages.

Stop and start the Tomcat servlet engine by entering the following commands at the server console:

```
/etc/init.d/novell-tomcat4 stop
```

```
/etc/init.d/novell-tomcat4 start
```

Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to access the OES Welcome pages.

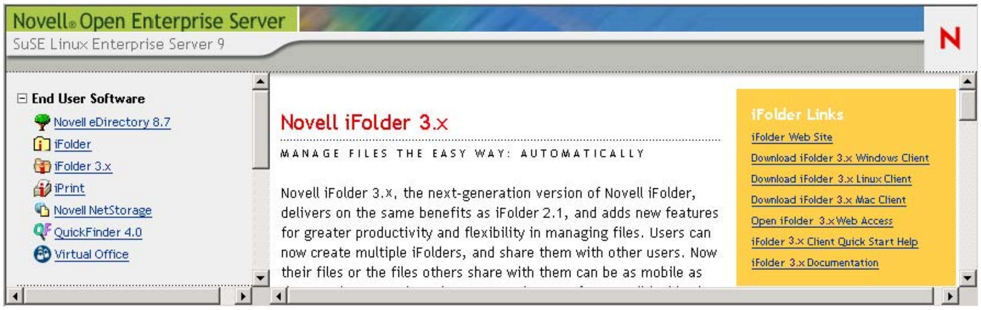
6.7.2 Accessing the iFolder 3.*x* Welcome Page

1 Open a Web browser to the following location to open the server's Welcome page:

`http://`*`ifolder3.example.com`*

Replace *`ifolder3.example.com`* with the DNS name or the IP address (such as *`192.168.1.1`*) of the Novell iFolder 3.*x* enterprise server.

2 In the left navigator, click *iFolder 3.x* to open the iFolder 3.*x* Welcome page.


Novell® Open Enterprise Server
SuSE Linux Enterprise Server 9
N
End User Software
Novell eDirectory 8.7
iFolder
iFolder 3.x
iPrint
Novell NetStorage
QuickFinder 4.0
Virtual Office
Novell iFolder 3.x
MANAGE FILES THE EASY WAY: AUTOMATICALLY
iFolder Links
iFolder Web Site
Download iFolder 3.x Windows Client
Download iFolder 3.x Linux Client
Download iFolder 3.x Mac Client
Open iFolder 3.x Web Access
iFolder 3.x Client Quick Start Help
iFolder 3.x Documentation

Novell iFolder 3.x, the next-generation version of Novell iFolder, delivers on the same benefits as iFolder 2.1, and adds new features for greater productivity and flexibility in managing files. Users can now create multiple iFolders, and share them with other users. Now their files or the files others share with them can be as mobile as

6.7.3 Downloading the iFolder Client

On the iFolder 3.*x* Welcome page, users can select one of the following client links to download the install files for the iFolder client for Novell iFolder 3.*x*:

Link Name	Operating System	Filename
iFolder 3.*x* Linux Client	Novell Linux Desktop 9 and later	`ifolder3-linux.tar.gz`
iFolder 3.*x* Windows Client	Windows 2000/XP/2003	`ifolder3-windows.exe`
iFolder 3.*x* Mac Client	Macintosh OS X v10.3 and later	`ifolder3-mac.tar.gz`

After expanding the `tar.gz` files, users are ready to install the iFolder client and its dependencies with the following files:

iFolder Client	Install Files

iFolder for Linux	`../linux/ifolder3` directory
	`ifolder3-3.x.`*`yyyymmdd`*`-1.i686.rpm`
	`nautilus-ifolder-3.x.`*`yyyymmdd`*`-1.i586.rpm`
	`simias-1.0.`*`yyyymmdd`*`-1.i686.rpm`
	`../linux/mono` directory
	`gtk-sharp-1.0.9-0.sles9.novell.i586.rpm`
	`libgdiplus-1.1.7-1.ximian.i586.rpm`
	`mono-core-1.1.7.`*`x-xxxxx-x`*`.novell.i586.rpm`
	`mono-data-1.1.7..`*`x-xxxxx-x`*`.novell.i586.rpm`
	`mono-web-1.1.7..`*`x-xxxxx-x`*`.novell.i586.rpm`
	`xsp-1.0.9-0.novell.noarch.rpm`

iFolder for Windows	`ifolder3-windows.exe`

iFolder for Mac	`ifolder3-3.x.`*`yyyymmdd`*`.dmg`
	`MonoFramework-1.1.7..`*`x-x`*`.dmg`

6.7.4 Installing the iFolder Client

For information about prerequisites and installation, see "Getting Started" in the *iFolder User Guide for Novell iFolder 3.x*.

6.8 Updating Novell iFolder 3.*x*

As patches become available for iFolder 3.*x* and the iFolder client, they are delivered to the OES Patch channel. Any iFolder server or client patches or updates are installable through the ZENworks® Linux Management (formerly Red Carpet®) channels.

- The iFolder client for Windows checks for updates on the server whenever a user logs in, and prompts the user to install a new update if it exists.
- Patches or updates to the iFolder client for Linux and Macintosh must be delivered through a customer-hosted channel, so that your users have access to them. For information on how to set

up a customer-hosted channel, please see documentation for ZENworks Linux Management or Red Carpet.

6.9 Updating Mono for the Server and Client

Novell iFolder 3.*x* supports only the version of Mono included in the install software. The iFolder client for Linux or Macintosh supports only the version of Mono included in the install software for those platforms. Whenever a Novell iFolder 3.*x* patch or upgrade includes updates for the iFolder client, the update software also includes any updates for Mono on Linux and Macintosh. You can update Mono concurrently with the iFolder updates on the server or client.

If you need to upgrade Mono for another reason, please check our online documentation to see if we explicitly support that version and to learn any necessary steps to make the upgrade work correctly. For information, see the latest version of the online documentation on the Novell iFolder 3.*x* Documentation Web site (http://www.novell.com/documentation/ifolder3).

6.10 Uninstalling the iFolder 3.*x* Enterprise Server

Use YaST to uninstall the iFolder 3.*x* enterprise server `.rpm` file. Uninstalling iFolder 3.*x* software also removes the Simias store, including all data in `/var/opt/novell/ifolder3/simias/SimiasFiles`, from the server.

IMPORTANT: During the uninstall, all user data and iFolder share information on the server is destroyed.

If you want to keep the iFolder data store and share information, make sure to make a backup of the data before you uninstall iFolder. The users still have a local copy of all their data, which might not be the most up-to-date version, depending on when they last synchronized their files.

When the server is re-installed, each of the iFolder clients must remove the old iFolder account and re-create it, even if the server IP address for the iFolder account has not changed. Users must also set up iFolders and share relationships again.

6.11 What's Next

You have now installed and configured your Novell iFolder 3.*x* enterprise server and provisioned iFolder services for users. To set up system policies for iFolder services, continue with Chapter 8, "Managing iFolder Services," on page 79.

Provisioned iFolder users can install the Novell iFolder 3.*x* client on their workstations, create iFolders, and share iFolders with other authorized Novell iFolder users. For information, see the *iFolder User Guide for Novell iFolder 3.x*.

Managing an iFolder Enterprise Server

7

This section describes how to manage your Novell® iFolder® 3.*x* enterprise server on Novell Open Enterprise Server platform.

7.1 Starting iFolder Services

iFolder services start whenever you reboot the system or whenever you start Apache services.

As a root user, enter the following command at the server console:

```
/etc/init.d/apache2 start
```

7.2 Stopping iFolder Services

iFolder services stop whenever you stop the system or whenever you stop Apache services.

As a root user, enter the following command at the server console:

```
/etc/init.d/apache2 stop
```

7.3 Restarting iFolder Services

If you need to restart iFolder services, you must stop and start Apache services:

As a root user, enter the following command at the server console:

```
/etc/init.d/apache2 stop

/etc/init.d/apache2 start
```

Avoid using the Apache Restart command. If any other modules using the Apache instance do not exit immediately in response to the Apache Restart command, iFolder might hang.

7.4 Configuring the iFolder Nightly Restart

The iFolder enterprise server restarts nightly to control the consumption of system resources. The restart stops both Apache and Mono, then starts them. It is implemented with the following linked scripts in the `/etc/cron.daily` directory:

```
/etc/cron.daily/a-simias-stop
```

```
/etc/cron.daily/z-simias-start
```

By default on OES, the `cron.daily` scripts run at 4:15 AM. You can modify the run time of cron.daily in the `/etc/crontab` file.

If iFolder ever becomes unresponsive, execute the above scripts in the order shown as the root user.

7.5 Managing the Simias Log and Simias Access Log

On the iFolder enterprise, there are two logs that track events:

- **Simias Log:** The `/simias/Simias.log` file contains status messages about the health of the Simias Service.
- **Simias Access Log:** The `/simias/Simias.access.log` file contains file access events for data and metadata about iFolders, users, membership in shared iFolders, and so on. It reports the success of the event and identifies who did what and when they did it. For example, if a file was deleted on the server, it identifies the user who initiated the deletion.

Review the logs whenever you need to troubleshoot problems with your iFolder system.

The Simias Log4net file (`/simias/Simias.log4net`) allows you specify output location of the log files and what events are recorded at run time. Its parameters are based on, but not compliant with, the Apache Logging Services (http://logging.apache.org/log4net). The following parameters are modifiable:

Parameters	Description	Examples

Location and name of the log
`<file value=”`*`pathname`*`” />`
	The location of the log file. Specify the full path where the file is located on the computer, including the volume, intermediate directories, and filename.	`<file value="c:/simias/Simias.log" />`
		`<file value=”c:/simias/Simias.access.log” />`

Parameters	Description	Examples
Maximum size of the log file `<maximumFileSize value=”*size*” />`	The maximum size of the log file. When the file grows to this size, the content is rolled over into a backup file and the recording continues in the now-empty file. A period and sequential number are appended to the filename of the backup log files, such as `Simias.log.1` and `Simias.log.2`. For *`size`*, specify the number and unit, such as `10MB` or `20MB`, with no space between them.	`<maximumFileSize value="10MB" />`
How much logged data to retain `<maxSizeRollBackups value=”*number*” />`	The maximum number of backup log files that are kept before they are overwritten. The log rolls over sequentially until the maximum number of backups are created, then overwrites the oldest log file.	`<maxSizeRollBackups value="10" />`

Level of Simias Services messages
`<level value=”*status*” />`
(Use only for the `Simias.log`.)
	The type of messages or level of detail you want to capture for the log. Valid levels include the following:
	`OFF`
	`FATAL`
	`ERROR`
	`WARN`
	`INFO`
	`DEBUG`
	`ALL`
		`<level value="ERROR" />`

Fields to report for file access events
`<header value=”*layout*” />`
(Use only for the `Simias.access.log`.)
	Specify which fields to report and the order you want them to appear for each entry. Valid fields include the following:
	`date`
	`time`
	`method` (program call or event)
	`status` (success or failure)
	`user`
	`uri` (relative path of the file in an iFolder)
	`id` (node key)
	The fields are tab delimited (`\t`) by default, but you can specify a space or tab character in front of the field name to serve as a delimiter.
		`<header value="#version: 1.0&#xD;&#xA;#Fields:\tdate\ttime\tmethod\tstatus\tuser\turi\tid\t&#xD;&#xA;" />`

In the Log4net terminology, each output destination is defined in an XML `appender` tag. If you do not want to log events for the Simias Service or for file access, comment out (`!--`) the related `appender` tag and its child elements for that log file.

7.6 Backing Up the iFolder Server

1. Stop the iFolder server by entering the following command as root user:

   ```
   /etc/init.d/apache2 stop
   ```

2. Use your normal file system backup procedures to back up the following data:

   - Simias store directory

     The default location is `/var/opt/novell/ifolder3/simias`.

   - Simias configuration file

     The default locations are `/var/lib/wwwrun/.local/share/simias/Simias.config` or `/home/wwwrun/.local/share/simias/Simias.config`.

3. Start the iFolder server by entering the following command as root user:

   ```
   /etc/init.d/apache2 start
   ```

7.7 Backing Up the iFolder Store with the TSAIF

The Target Service Agent (TSA) for Novell iFolder 3.*x* supports the back up of the iFolder store.

- Section 7.7.1, "Understanding TSAIF," on page 68
- Section 7.7.2, "Syntax," on page 70
- Section 7.7.3, "iFolder Path Options," on page 70
- Section 7.7.4, "iFolder Path Examples," on page 71
- Section 7.7.5, "SMSConfig Options," on page 71
- Section 7.7.6, "TSAIF and SMSConfig Examples," on page 72
- Section 7.7.7, "NBackup Options," on page 73
- Section 7.7.8, "TSAIF and NBackup Examples," on page 74
- Section 7.7.9, "Additional Information," on page 75

7.7.1 Understanding TSAIF

iFolder TSA

Novell Storage Management Services (SMS) is an API framework that backup applications consume to provide a complete backup solution. The SMS framework is implemented by two main components: The Storage Management Data Requester and the Target Service Agent.

The TSA provides an abstraction of a particular backup target. The TSA uses native interfaces to read target data and transforms it to a continuous stream of data objects. The data objects are formatted in the ECMA standard System Independent Data Format (SIDF).

The TSA for iFolder (TSAIF) provides an implementation of the SMS API for an iFolder store. Backup applications, such as nbackup(1), can make use of its features by writing to the SMS API.

iFolder and Simias

iFolder is built upon Simias technology. Simias is a general-purpose object repository that provides a foundation for building collaborative solutions. A Simias Collection store contains Collection objects. At a minimum, a Simias Collection store contains a Local Database Collection and one or more Domain Collections. The Local Database Collection controls access to the physical storage of the Collection store on the file system. A Domain Collection contains a list of members in a given domain. For example, a Domain might contain all the members from a given LDAP directory. Each Collection is owned by exactly one Domain member.

An iFolder is a type of Simias Collection that has a root directory on the file system. Each file or subdirectory in the iFolder's root directory has a corresponding FileNode or DirNode in the Collection. An iFolder store is a Simias Collection store that contains one or more iFolders and includes the directories and files associated with the iFolders.

For more information on the iFolder and Simias technologies, see the iFolder Project at www.ifolder.com (http://www.ifolder.com).

iFolder TSA Granularity

TSAIF supports creating archives that contain the following:

- The entire iFolder store
- All iFolders owned by a specified Domain member
- An individual iFolder

TSAIF supports restoring the following:

- The entire iFolder store
- All iFolders owned by a specified Domain member
- An individual iFolder
- An individual subdirectory in an iFolder
- An individual file in an iFolder

The entire iFolder store should be backed up regularly. In certain cases, a backup administrator might choose to back up an individual iFolder or to back up all iFolders owned by a specific owner. These special-case archives can be restored only to the same iFolder store from which they were backed up.

IMPORTANT: If you are restoring an entire iFolder and want to ensure that it is in the exact state it was in when it was backed up, you should first delete it from the server using a client or the iFolder 3 plug-in for iManager.

Deleting the iFolder is not necessary to restore any or all of the files in the iFolder; the difference is in what metadata is given preference during the restore. If you do not delete the iFolder before restoring, the attributes of the iFolder, such as the owner, members, file type or size restrictions, remain as they are in the current version.

7.7.2 Syntax

At an OES Linux server terminal console, enter

```
smsconfig -l tsaif [OPTION]...
```

The `-1` option registers the TSAIF with the Storage Management Data Requester (SMDR).

TSAIF uses the `libtsaif.so` file. The library implements all the necessary service functions to backup an iFolder target.

7.7.3 iFolder Path Options

The top-level resource for an iFolder store is `/` (a single forward slash) and represents the root of the iFolder store. The paths for iFolder data objects are specified relative to the root of the iFolder store, using the syntax of the Network File System (NFS) namespace. iFolder paths are logical paths into an iFolder store and do not correspond directly to file system paths.

Parameter	Description

`path`	iFolder path such as the following:
	`/`
	`/owner`
	`/owner/collection`
	`/owner/collection/relative-path`

`owner`	`owner-name.owner-id`
`owner-name`	Collection owner name (`Simias.Storage.Collection.Owner.Name`)
`owner-id`	Collection owner ID (`Simias.Storage.Collection.Owner.ID`)
`collection`	`collection-name.collection-id`
`collection-name`	Collection name (`Simias.Storage.Collection.Name`)
`collection-id`	Collection ID (`Simias.Storage.Collection.ID`)

`relative-path`	Relative path such as
	`file`
	`subdir`
	`subdir/relative-path`

`file`	name of file on file system
`subdir`	name of subdirectory on file system

The `\fIowner-id\fR` and `\fIcollection-id\fR` are required because `\fIowner-name\fR` and `\fIcollection-name\fR` are not guaranteed to be unique. Using both the name and ID properties to identify Collections and Collection owners provides a “friendly” name along with the required unique identifier.

In many configurations, the names of Collections and Collection owners are unique. For example, if Domain members are obtained from an LDAP directory, it is not likely that two members would have the same username. Likewise, it would be unusual for an owner to give two iFolders the same name.

Although a backup application must pass both the name and ID to TSAIF, it might display only the name to the backup administrator to simplify the user interface. The ID would need to be displayed to the backup administrator only when two Collections, or two Collection owners, have the same name and the backup administrator wants to perform an operation on only one of them.

The name of the Collection or Collection owner can be obtained by stripping off the pattern

```
".????????-????-????-????-????????????"
```

from the first two components of the path TSAIF returns to the backup application.

7.7.4 iFolder Path Examples

The following examples show how to use iFolder paths to backup and restore data at different levels in the iFolder store.

```
/
```

Back up or restore the entire iFolder store.

```
/myOwner.12345678-1234-1234-1234-123456789abc
```

Back up or restore all Collections owned by `myOwner`.

```
/myOwner.12345678-1234-1234-1234-123456789abc/myCollection.22345678-
1234-1234-1234-123456789abc
```

Back up or restore the Collection named myCollection. If the Collection is an iFolder, all files and directories in the iFolder will be backed up or restored along with the Simias data in the Collection store.

```
/myOwner.12345678-1234-1234-1234-123456789abc/myCollection.22345678-
1234-1234-1234-123456789abc/myFile
```

Back up or restore the file named myFile in the root directory of the iFolder along with its Simias data from the Collection store.

```
/myOwner.12345678-1234-1234-1234-123456789abc/myCollection.22345678-
1234-1234-1234-123456789abc/mySubdir
```

Back up or restore the subdirectory named `mySubdir` in the root directory of the iFolder along with its Simias data from the Collection store, and recursively backup or restore each file and subdirectory in `mySubdir` along with its respective Simias data.

7.7.5 SMSConfig Options

The TSAIF command is not a standalone shell command; it is exercised using smsconfig. All configuration options are managed via smsconfig. The TSAIF can be configured during registration and the configuration persists until TSAIF is unloaded.

All long options (options that have the format `--optionname`) are case insensitive.

Option	Command
`--help`	Displays the options supported by the TSA.
`--ReadBufferSize`	This is the amount of data (Bytes) read from the Simias store and/or file system by a single read operation. This switch is based on the buffer sizes used by the applications. For example, if the application requests 32 KB of data for each read operation, set the buffer size to 32 KB to allow the TSA to service the application better. This value works well with Simias store and/or file system reads if set in multiples of 512 Bytes. The default value is 64 KB.
`--ReadThreadsPerJob`	This enables the TSA to read data ahead of the application request during backup. This switch is based on the number of processors in the system. This switch can also be used to influence the disk activity based on system configuration. The default value is 4.
`--ReadThreadAllocation`	This sets the maximum number of read threads that process a data set at a given time. This determines the percentage of ReadThreadsPerJob that should be allocated to a data set before proceeding to cache another data set. This enables the TSA to store a cache of data sets in a non sequential manner. This sets all read threads to completely process a data set before proceeding to another data set. The default value is 100.
`--ReadAheadThrottle`	This sets the maximum number of data sets that the TSA caches simultaneously. This prevents the TSA from caching parts of data sets and enables complete caching of data sets instead. Use this switch along with the ReadThreadAllocation switch. The default value is 2.
`--CacheMemoryThreshold`	This is used to specify the percentage of available server memory that the TSA can utilize to store cached data sets. This represents a maximum percentage value of available server memory that the TSA uses to store cached data sets. The default value is 10% of the total server memory.

7.7.6 TSAIF and SMSConfig Examples

The following examples show how to perform typical TSAIF configuration for SMS.

```
smsconfig -l tsaif --help
```

Displays the options supported by the TSAIF.

```
smsconfig -l tsaif --readthreadsperjob=8
```

Sets the number of read threads that the TSAIF starts per job to 8.

```
smsconfig -l tsaif --readbuffersize=32768 --cachememorythreshold=15
```

Sets the read buffer size to 32KB and the maximum amount of cache memory that the TSAIF should use to 15%.

7.7.7 NBackup Options

TSAIF supports the following typical `nbackup(1)` options:

Option	Command
`--exclude-file=pattern`	Excludes all files matching the name (owner, folder, or file) or pattern for back up or restore. Use this option multiple times to exclude more than one pattern.
`-F, --full-paths`	Stores the full paths for both directories and files in the created archive.
`-k, --keep-old-files`	Does not overwrite existing files while extracting files from the archive. Files are overwritten if this option is not present.
`-N, --after-date=date`	Backs up files newer than date.
`-P, --password=password`	The password to connect to the TSA. The password can be supplied at runtime.
`-R, --remote-target=hostname`	Connects to the file system TSA of the host specified in hostname for backup. Use with the `--target-type` option.
`--target-type=target_name`	Connects to the TSA specified by `target_name`, where the target name is Linux, NetWare, or iFolder.
`-T, --input-file=file`	Takes file containing fully qualified paths as input for creating archive. This file should contain one path per line.
`-U, --user=username`	Username to use while connecting to the TSA.

TSAIF does not support the following nbackup(1) options:

Option	Command
`-m, --move-to=path`	Extracts the archive to the given path. This does not work with TSAIF because iFolder puts files in a `SimiasFiles` directory.
`-r, --restore-to="backup_path new_path"`	Restores by replacing `backup_path` with `new_path`. This does not work with TSAIF because iFolder puts files in a `SimiasFiles` directory.

If TSAIF cannot back up or restore a file, it skips the file and returns a warning. This can occur for various reasons. When this occurs, `nbackup(1)` creates a file with a `.warn` extension that contains a list of each file that was skipped along with the date and time it was skipped and the error code that was returned.

If files are skipped, try to resolve the issue, then run the operation again.

If you are unable to identify why the file was skipped, try running the operation again when the server is less busy.

If files are skipped during a restore, and if relatively few files are skipped, try individually restoring each skipped file.

7.7.8 TSAIF and NBackup Examples

The following examples show how to perform typical TSAIF backup and restore operations using NBackup.

Backup or Restore Task	Command
Full backup	`nbackup -cvf full.sidf -U root -P password --target-type=ifolder /`
Full restore	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder`
Owner backup	`nbackup -cvf owner.sidf -U root -P password --target-type=ifolder /owner`

Owner restore	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder`
	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder --extract-dir=/owner`

iFolder backup	`nbackup -cvf ifolder.sidf -U root -P password --target-type=ifolder /owner/collection`

iFolder restore	`nbackup -xvf ifolder.sidf -U root -P password --target-type=ifolder`
	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection`
	`nbackup -xvf full.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection`
	If you are restoring an entire iFolder and want to ensure that it is in the exact state it was in when it was backed up, you should first delete the current iFolder from the server using a client or the iFolder 3 plug-in for iManager.
	Deleting the iFolder is not necessary to restore any or all of the files in the iFolder; the difference is in what metadata is given preference during the restore. If you do not delete the iFolder before restoring, the attributes of the iFolder, such as the owner, members, file type or size restrictions, remain as they are in the current version.

Backup or Restore Task	Command

Subdirectory restore	`nbackup -xvf ifolder.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection/relative-path`
	`nbackup -xvf owner.sidf -U root -P password --target-type=ifolder --extract-dir=/owner/collection/relative-path`
	`nbackup -xvf full.sidf -U root -P`

7.7.9 Additional Information

For more information about backup, see the following man pages on your iFolder enterprise server: `nbackup(1)`, `sms(7)`, `smdrd(8)`, `smsconfig(1)`, `tsaif.conf(5)`.

7.8 Recovering from a Catastrophic Loss of the iFolder Server

If the iFolder server configuration or data store becomes corrupted, use your iFolder backup files to restore the database to its last good backup. Restoring the iFolder server to the state it was in at the time of the backup also reverts the iFolders on any connected iFolder clients to that same state.

IMPORTANT: All changes made since the time of the backup will be lost on all connected clients.

Consider the following implications of restoring iFolder data:

- Any new file or directory is deleted if it was added to an iFolder since the time of the backup.
- Any file that was modified is reverted to its state at the time of the backup.
- Any file or directory is restored if it was deleted since the time of the backup.

Before restoring the iFolder server, consider notifying all users to save copies of any files or directories they might have modified in their iFolders since the time of the last backup. After the iFolder server is restored, they can copy these files or directories back into their respective iFolders

1. Notify users to save copies of iFolders or files that have changed since the time of the backup you plan to use for the restore.
2. Stop the iFolder server by entering the following command as root user:

   ```
   /etc/init.d/apache2 stop
   ```
3. Remove the following corrupted data:

   - Simias store directory

     The default location is `/var/opt/novell/ifolder3/simias`.
   - Simias configuration file

     The default locations are `/var/lib/wwwrun/.local/share/simias/Simias.config` or `/home/wwwrun/.local/share/simias/Simias.config`.

4 Use your normal file system restore procedures to restore the following data to its original locations:

- Simias store directory

  The default location is `/var/opt/novell/ifolder3/simias`.
- Simias configuration file

  The default locations are `/var/lib/wwwrun/.local/share/simias/Simias.config` or `/home/wwwrun/.local/share/simias/Simias.config`.

5 Delete all files in the Simias log directory.

The default location is `/var/opt/novell/ifolder3/simias/log/*`.

IMPORTANT: Be careful not to modify anything else under the Simias store directory.

6 Start the iFolder server by entering the following command as root user:

```
/etc/init.d/apache2 start
```

7 Notify users that they can return their saved files to their iFolders for upload to the server. Users should coordinate this with other members of the iFolder to avoid competing updates.

7.9 Recovering Individual Files or Directories

1 Collect information that uniquely identifies the file or directory to be recovered, such as a combination of the following:

- iFolder name, such as MyiFolder
- iFolder owner
- iFolder member list
- Relative path of the file or directory, such as `/MyDir1/MyDir2/myfile.txt`
- Time stamp or approximate time of the version desired
- Other files or directories in the iFolder

2 Open a Web browser to iManager, then log in with your Admin username and password.

3 Under Roles and Tasks, expand *Novell iFolder 3*, select *iFolders*, then wait for the page to refresh.

4 If prompted, connect to the iFolder server where the iFolder is stored by entering the name of the iFolder server and iFolder Admin user credentials as needed.

5 On the Search for iFolders page, search for the target iFolder, such as *MyiFolder*.

6 Under Search Results, click the *Name* link of the target iFolder, then note the path to its root directory. For example:

```
/var/opt/novell/ifolder3/simias/SimiasFiles/62ba1844-6987-47fc-83ab-84bbd5d6130b/MyiFolder
```

7 On the iFolder server, use your normal file system restore procedures to restore the target file or directory from backup to a temporary location.

For example, restore `/var/opt/novell/ifolder3/simias/SimiasFiles/62ba1844-6987-47fc-83ab-84bbd5d6130b/MyiFolder/MyDir1/MyDir2/MyFile` to `/tmp/MyFile`.

IMPORTANT: Do not restore the file to its original location, or to any location under the Simias store directory.

8. Use one of the following methods to restore the recovered file to the target iFolder:

   - **Via E-Mail:** Send the restored files or directory to the iFolder owner or to any member who has the Write right to the iFolder.

     For example, e-mail the recovered file, such as `/tmp/MyFile`, to the user. A user with the Write right can restore the file to an iFolder simply by copying it back to the appropriate location on an iFolder client. For example, copy `MyFile` to `/home/`*`username`*`/MyiFolder/MyDir1/MyDir2/MyFile`.

   - **Via Web Access:** In iManager, expand the *Novell iFolder 3* role, select *Folders*, search for the iFolder you want to manage, and then click the *Name* link for the iFolder. On the iFolder page, click *Members*, then add yourself as a member of the target iFolder.

     In a Web browser, log in to iFolder 3.*x* Web Access, browse to locate and open the iFolder, then navigate to the directory where the files were originally located. Upload the file to the iFolder. For example, upload `MyFile` to `MyiFolder/MyDir1/MyDir2/MyFile`. If necessary, create the directory you want to restore, then upload the files in it.

     You can only upload one file at a time, so this option might be viable when only a few files need to be restored.

7.10 Moving iFolder Data from One iFolder Server to Another

You can relocate iFolder services and the iFolder data in the Simias Store from one iFolder server to another, such as if you want to migrate to a more powerful computer.

1. Notify users that the iFolder server is going down.
2. Stop iFolder services. As a root user, enter the following command at the server console:

   ```
   /etc/init.d/apache2 stop
   ```

3. Use your normal file system backup procedures to back up the following data:

   - Simias store directory

     The default location is `/var/opt/novell/ifolder3/simias`.

   - Simias configuration file

     The default locations are `/var/lib/wwwrun/.local/share/simias/Simias.config` or `/home/wwwrun/.local/share/simias/Simias.config`.

4. Install and configure iFolder on the target server, using the same configuration information and location as on the old computer, including the IP address.
5. On the target server, use your normal file system restore procedures to restore the following data to its original locations:

   - Simias store directory

     The default location is `/var/opt/novell/ifolder3/simias`.

   - Simias configuration file

The default locations are `/var/lib/wwwrun/.local/share/simias/Simias.config` or `/home/wwwrun/.local/share/simias/Simias.config`.

6. Start iFolder services. As a root user, enter the following command at the server console:

   ```
   /etc/init.d/apache2 start
   ```

7. Notify users that the server is back up.
8. Disconnect the original server from the network, then uninstall iFolder to remove iFolder software and the iFolder data. Make sure to reconfigure its IP address before using it on the network again.

Managing iFolder Services

8

This section discusses how to manage services for the Novell® iFolder® 3.*x* enterprise server with Novell iManager.

8.1 Accessing the Novell iFolder 3 Plug-In for iManager

Use the Novell iFolder 3 plug-in for Novell iManager 2.5 to manage the iFolder system, user accounts, and iFolders. For information about iManager, see the *Novell iManager 2.5 Administration Guide* (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/hk42s9ot.html#bktitle).

1 Open a Web browser to the following URL:

```
https://svrname.example.com/nps/iManager.html
```

Replace *svrname.example.com* with the actual DNS name or IP address (such as `192.168.1.1`) of the server where iManager is running. This might be the same server as your iFolder server.

IMPORTANT: The URL is case sensitive.

2 If prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.

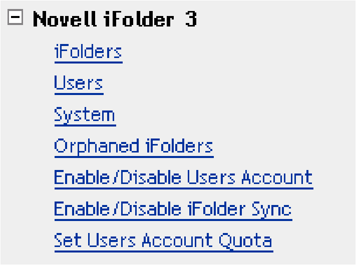
3 On the iManager Login page, log in as an admin user or equivalent.

The admin user can be the same or different user than the iFolder Admin user or equivalent.If the usernames do not have the effective iFolder Admin right needed to manage the iFolder server, you must specify the iFolder Admin user credentials whenever you log in to the iFolder server you want to manage.

If you log in to the Novell eDirectory™ tree where the server you want to manage resides, if you are modifying LDAP settings, you can browse the tree to specify containers or groups as Search DNs.

However, if you log in to a different tree, you are unable to browse the tree; you must explicitly specify Search DNs to use for provisioning iFolder users.

4 In Roles and Tasks, expand the *Novell iFolder 3* role to show its tasks.



⊟ **Novell iFolder 3**

- iFolders
- Users
- System
- Orphaned iFolders
- Enable/Disable Users Account
- Enable/Disable iFolder Sync
- Set Users Account Quota

5 Select any of the tasks to go to the Connection page where you log in to the iFolder server you want to manage.

When you first log in to iManager or if you have disconnected from an iFolder server management session, any task you select takes you to the Connection page.

6 Continue with Section 8.2, "Connecting to the iFolder Server," on page 80.

8.2 Connecting to the iFolder Server

Although you are logged in to iManager, you must provide the iFolder administrator credentials to authenticate to the specific iFolder server you want to manage. The iFolder Admin username can be the same LDAP identity as your iManager Admin username, depending on how you configure your iFolder system.

If you are not logged in to an iFolder server, whenever you click a task under the *Novell iFolder 3* role, the Connection page opens to allow you to log in to the iFolder enterprise server you want to manage. Log in with the iFolder Admin username and password for the target server.

NOTE: You cannot manage Novell iFolder 2.1*x* servers with the Novell iFolder 3 plug-in to iManager.

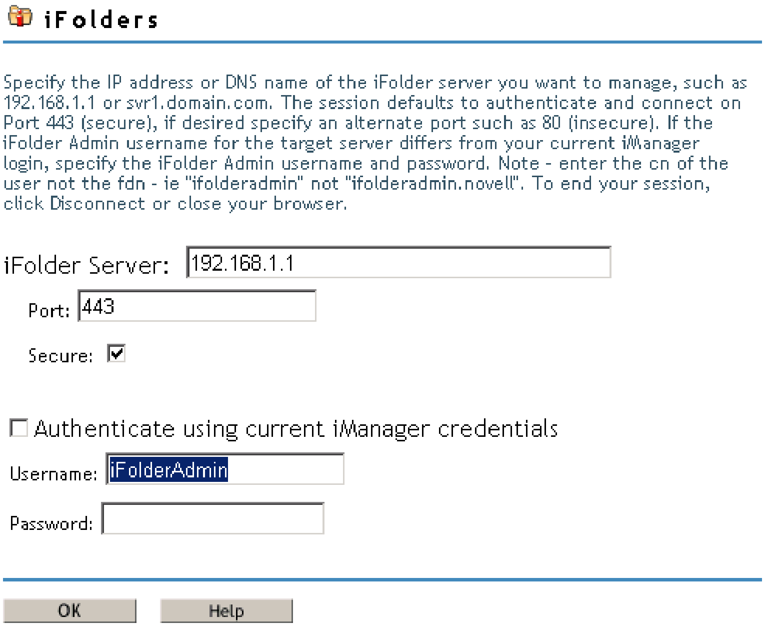
To connect to the iFolder server you want manage:

1 In a Web browser, log in to iManager.

For information, see Section 8.1, "Accessing the Novell iFolder 3 Plug-In for iManager," on page 79.

2 In Roles and Tasks, expand the *Novell iFolder 3* role, then select the task you want to perform.

You can click any of the Novell iFolder 3 tasks to open the Connection page.


iFolders

Specify the IP address or DNS name of the iFolder server you want to manage, such as 192.168.1.1 or svr1.domain.com. The session defaults to authenticate and connect on Port 443 (secure), if desired specify an alternate port such as 80 (insecure). If the iFolder Admin username for the target server differs from your current iManager login, specify the iFolder Admin username and password. Note - enter the cn of the user not the fdn - ie "ifolderadmin" not "ifolderadmin.novell". To end your session, click Disconnect or close your browser.

iFolder Server: 192.168.1.1

Port: 443

Secure: ☑

□ Authenticate using current iManager credentials

Username: iFolderAdmin

Password:

3 Specify the DNS name or IP address of the iFolder enterprise server you want to manager.

For example, type `svr1.example.com or 192.168.1.1`.

4 Specify the port to use for your management session and indicate whether the port traffic is secure (select *Secure*) or insecure (deselect *Secure*).

The default setting is `Port 443` for secure traffic.

5 Do one of the following:

- If you logged in to iManager with the same username as the iFolder Admin user of the target server, select *Authenticate Using Current iManager Credentials*.
- If you logged in to iManager with a different username than the iFolder Admin user of the target server, deselect *Authenticate Using Current iManager Credentials,* then specify the iFolder Admin username and password.

6 Click *OK* to connect to the iFolder server.

7 (Conditional) If prompted to accept the server's certificate, review the certificate information, then click *OK* to accept it if it is valid.

When you are done managing the iFolder server, click *Disconnect* (located in the upper right corner) or close your Web browser to disconnect from the iFolder server you are managing. If you do not log out, the connection to the iFolder enterprise server remains open until your session times out, which can be a security risk.

8.3 Viewing General System Information

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

By default, the System option opens to the General tab on the Systems page.

2 View the following information:

Parameter	Description
Domain	Descriptive name of the iFolder enterprise server. Each server is an iFolder domain.
Host Name	The host portion of the DNS name of the server. For example, in *`if3svr.example.com`*, *`if3svr`* is the host name.
Machine Name	The local name of the server
OS	The operating system as reported by Mono®. Mono might report Linux as UNIX.
User Name	The username of the session that spawned the iFolder services process. For example, *`wwwrun`*.
Total Disk Space Used	The total combined physical size (in MB) of all iFolders on the system
Total User Quotas	The total combined administrative size (in MB) of space allocated for use by iFolder users on this system. The administrative total can exceed the actual physical size of the system disks. Space is assigned as needed; it is not reserved. If no space restrictions are set for iFolder user accounts, the system reports `No Limit`. If space restrictions are set only for a subset of users, the reported size can be less than the current reported physical size.

8.4 Configuring the LDAP Settings for an iFolder Server

Use the LDAP Settings page to manage LDAP Settings for your iFolder server. In iManager, expand the *Novell iFolder 3* role, then select *System > LDAP* to open the System page to the LDAP tab.

- Section 8.4.1, “Viewing the Current LDAP Settings,” on page 83
- Section 8.4.2, “Modifying the iFolder LDAP Settings,” on page 84
- Section 8.4.3, “What to Do If the iFolder Admin User Is Deleted from LDAP,” on page 86
- Section 8.4.4, “Securing Access to the iFolder Proxy User Password,” on page 86
- Section 8.4.5, “Modifying the iFolder Proxy User Password,” on page 86
- Section 8.4.6, “Synchronizing the iFolder User List with the LDAP Server,” on page 87

8.4.1 Viewing the Current LDAP Settings

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

2 Select *LDAP* to open the System page to the LDAP tab.

3 View the following information:

Parameter	Description
Server Host	The DNS name or IP address of the LDAP server. This might be the same or a different server as your iFolder enterprise server or iFolder Web Access server.
Server Port	The port used for exchanging information between LDAP server and the iFolder enterprise server or Web Access server. Use port 636 (secure) or port 389 (insecure).
Port Is Secure (SSL)	Indicates whether the iFolder server is configured for SSL exchanges. If SSL is enabled on the server, the value is Yes; otherwise, the value is No.
Proxy User DN	The fully distinguished name of the iFolder Proxy user. For example: `cn=ifolderproxy,o=acme` This identity must have the Read right to the LDAP service. The Read right for the LDAP service is the default.
Proxy User Password	The password is used to authenticate the iFolder Proxy user to the LDAP server when iFolder synchronizes users for the iFolder user list. This password must match the password stored in the iFolder Proxy user's eDirectory object. For information, see Section 8.4.5, "Modifying the iFolder Proxy User Password," on page 86.
Search DNs	The LDAP containers and groups where iFolder searches to compile a list of authorized users to provision for iFolder services on this enterprise server.
Minimum Synchronization Interval	The interval of time (in seconds) between synchronization sessions with the LDAP server. For example, 86400 seconds (24 hours). During an LDAP synchronization session, the iFolder server queries the LDAP server to retrieve a list of users in the contexts that are specified in the Search DN field, then synchronizes that list with its list of iFolder users. The interval timer is reset to the Synchronization Interval value at the end of a session. When the time elapses, another session is started.
Synchronization on Start	If this option is enabled, the server synchronizes the LDAP information immediately upon server startup. If this option is disabled, the synchronization of LDAP data is not performed until the specified Synchronization Interval has elapsed. Values are Yes or No.
Last Synchronization Attempt	The date and time of the most recent attempt to connect to the LDAP server to retrieve data.
Last Successful Synchronization Time	The date and time that LDAP data was successfully retrieved from the LDAP server and the iFolder user list was updated.

8.4.2 Modifying the iFolder LDAP Settings

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

2 Select *LDAP* to open the System page to the LDAP tab, then click *Modify*.

3 Modify any of the following fields, then click *OK* to apply your changes.

Parameter	Description
Server Host	Specify the DNS name or IP address of the LDAP server. This might be the same or a different server as your iFolder enterprise server or iFolder Web Access server. Make sure this new LDAP server is in the same LDAP tree as the original LDAP server that you specified as Server Host when you configured the iFolder enterprise server in YaST.
Server Port	Specify port 636 (secure) or port 389 (insecure). If the LDAP server is on the same machine as the iFolder servers, a secure port is unnecessary. Default Value: 636
Port Is Secure (SSL)	Specify whether the iFolder server is configured for SSL exchanges. If SSL is enabled on the server, the value is Yes; otherwise, the value is No. Default Value: Yes
Proxy User DN	The iFolder Proxy user is an existing proxy user identity used to access the LDAP server with Read access to retrieve a list of authorized users. The proxy user is automatically created during the iFolder enterprise server configuration in YaST. The username is autogenerated to be unique on the system. For most deployments, this username should never change. Keep the autogenerated iFolder Proxy username. The iFolder Admin user or equivalent can use the iFolder 3 plug-in for iManager to change the iFolder Proxy user identity in the LDAP settings for the iFolder server. Make sure that the user account assigned as the iFolder Proxy user is different than the one used for the iFolder Admin user and other system users. Separating the proxy user from the administrator provides privilege separation and is also important because the proxy user password is stored in the file system on the iFolder server. Specify the fully distinguished name of an existing user that you want to make the iFolder Proxy user. This identity must have the Read right to the LDAP directory. For example: `cn=iFolderProxy1234,o=acme` Make sure to also enter the new user's password in the Proxy Password field. After you modify the Proxy user, you might want to immediately synchronize the LDAP user lists, using the new iFolder proxy information; otherwise, it is not tested until the next scheduled synchronization of the user list. Use the *Update and Synchronize* option on the LDAP Settings page to synchronize the iFolder user list on demand and verify your new Proxy user settings. (In iManager, expand the *Novell iFolder 3* role, select *Systems*, select the *LDAP* tab, then click *Update and Synchronize Now*.)

Parameter	Description
Proxy User Password	Specify the password twice, then click *OK* to update the password stored in the *LDAP Settings*. Whenever you modify the Proxy User DN, you must also specify the password associated with the new iFolder Proxy user. The password is used to authenticate the iFolder Proxy user to the LDAP server when iFolder synchronizes users for the iFolder user list. This password must match the password stored in the iFolder Proxy user's eDirectory object. For information, see Section 8.4.5, "Modifying the iFolder Proxy User Password," on page 86.

Search DNs	Specify the LDAP containers and groups where iFolder 3.*x* searches for a list of authorized users to provision for iFolder services on this enterprise server. DNs are entered in LDAP format. For example:
	`o=acme`
	`ou=group,o=acme`
	To add a DN, type it in the Search DN field, then click *OK*.
	To edit a DN in the list, select it, then click the *Edit* icon (pen) to bring it to the *Search DN* field. Make your changes, then click *OK* to accept the changes.
	To search, click the *Search* icon to open a browsable list of LDAP objects, select the container or group you want to add, then click *OK*. The LDAP Object selector is not available if you logged into iManager in a different LDAP tree than the one where the Server Host (iFolder's LDAP server) resides.
	To delete a DN from the list, select it, click the *Delete* icon (red X), then click *OK*. When you delete a DN from the Search DNs, users in that DN are removed from the iFolder user list the next time the iFolder server synchronizes LDAP information.
	During LDAP synchronization, the iFolder server queries the LDAP server to retrieve a list of users in the DNs (as specified in the Search DN field). The usernames in the iFolder user list are matched against this official LDAP list. Any new user in the specified Search DNs are added to the iFolder user list. If a user is no longer in the specified DNs, the username is removed from the user list, any iFolders the user owns are orphaned and reassigned to the iFolder Admin user, and the user is removed as a member of other iFolders.
	The iFolder Admin User is provisioned for services during the install. It is tracked by its GUID, so it is available even if the Search DN is empty, or if you specify Search DNs that do not contain the Folder Admin user. This identity must be provisioned to enable the iFolder Admin to perform management tasks.

Minimum Synchronization Interval	Specify the synchronization interval (in seconds) for the elapsed time to wait between attempts to retrieve an updated list of system users from the LDAP server. Default Value: 86400 seconds (elapsed time of 24 hours from whenever the timer is reset)
Synchronization on Start	Specify Yes to immediately synchronize the list of users with the LDAP server when you start the iFolder server, or specify No to wait until the specified Synchronization Interval has elapsed after startup to begin synchronizing. Default Value: Yes

8.4.3 What to Do If the iFolder Admin User Is Deleted from LDAP

If the iFolder Admin user is accidentally deleted from LDAP, the iFolder enterprise server cannot be managed from iManager, but the iFolder server is still usable. All services continue to run under the existing settings.

1 In iManager, select the *Users* role, then re-create the iFolder Admin username with the same GUID as the original iFolder Admin user.

2 Stop the iFolder server.

3 Edit the `Simias.config` file to add the new iFolder Admin user.

The default locations of the `Simias.config` file are the `/var/lib/wwwrun/.local/share/simias`/ directory and the `/home/wwwrun/.local/share/simias/` directory.

In the Domain section, modify the AdminDN value by entering the username of the iFolder Admin user in LDAP format. For example:

```
<section name="Domain">
    <setting name="AdminDN" value="cn=iFolderAdmin,o=acme" />
</section>
```

4 Start the iFolder server.

8.4.4 Securing Access to the iFolder Proxy User Password

The password for the iFolder Proxy user is stored in clear text in the `/var/lib/wwwrun/.local/share/simias/Simias.config` file on the iFolder enterprise server. To secure access to the Simias.config file, administrators of the iFolder 3.*x* server computer must use every precaution to not inadvertently assign file system rights to the `/var/lib/wwwrun/.local/share/simias` directory to unauthorized users.

To protect the password when authenticating to the LDAP server, make sure to configure the LDAP Server Port and Port Is Secure options in the iFolder LDAP settings for secure (default) communications between the servers and the LDAP server. For information, see Section 8.4.2, "Modifying the iFolder LDAP Settings," on page 84.

8.4.5 Modifying the iFolder Proxy User Password

Manage the iFolder Proxy user and password with the Users role in iManager, as you would for any network user. If you need to modify the iFolder Proxy User password, change it for the iFolder Proxy user object in eDirectory, then update the value stored in the iFolder enterprise server's LDAP Settings for every server that uses that iFolder Proxy user. The Folder server cannot synchronize its list of users with the LDAP server until the passwords match in the LDAP User object and the eDirectory LDAP settings.

1 Log in to iManager in the tree where the LDAP server and iFolder enterprise server reside.

2 Modify the iFolder Proxy user password in its eDirectory object.

2a In Roles and Tasks, expand the eDirectory *Users* role, then click *Modify User*.

2b Specify the iFolder Proxy user in DN format or browse to locate the user object, then click *OK*.

For example, type `SimiasProxy.acme`. The *Modify User* page opens to the General tab.

2c Click the *Restrictions* tab, then click *Set Password* (at the bottom of the page) to open the Set Password dialog box.

2d Specify the password twice, then click *OK*.

2e Click *OK* to dismiss the confirmation message.

3 Update the iFolder Proxy user password stored in the iFolder server's LDAP settings. Repeat this process for every iFolder server that uses the same iFolder Proxy user.

3a In Roles and Tasks, expand the *Novell iFolder 3* role, then click *System*.

3b If you are not connected to the iFolder server, specify the iFolder Admin credentials, then click *OK* to open the Systems page.

3c Click the *LDAP* tab, then click *Modify* (at the bottom of the page) to open the Modify LDAP Settings page.

3d Specify the Proxy User Password twice, then click *OK*.

Make sure you type the same password you entered for the LDAP user object. When the password updates, the LDAP Settings page opens.

4 Verify that the password in LDAP settings matches the password in eDirectory. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, select *Systems*, select the *LDAP* tab, then click *Update and Synchronize Now*.

If the user list synchronization is successful, the passwords match and scheduled synchronizations of the user list should succeed.

8.4.6 Synchronizing the iFolder User List with the LDAP Server

The iFolder user list includes enterprise users that are provisioned for iFolder services. The list is based on users found in the LDAP containers and groups that you specify as Search DNs in the LDAP settings for the iFolder enterprise server. The list comprises information about each user, such as a user's username, full name, and LDAP GUID. The LDAP GUID matches the Simias GUID, which is used to uniquely identify the iFolder user in the iFolder system.

The user list is updated periodically and on-demand by retrieving a list of current LDAP users in the Search DNs. iFolder compares its user list with this master list and takes none, one, or both of the following actions to synchronize the user list.

- If there are new users in the retrieved list, those users are provisioned for iFolder services and added to the user list.
- If users were deleted from the LDAP containers and groups or if contexts were removed, the deleted users that were formerly in the iFolder user list are no longer eligible for iFolder accounts. Deleted users are removed from the list. The iFolders owned by the deleted users are marked as orphaned. If the deleted user was a member in other iFolders, the user is removed from the list of members.

  For information, see Section 11.9, "Managing Orphaned iFolders," on page 115.

Synchronizing at Regular Intervals

The LDAP Synchronization Interval determines the elapsed time between sessions with the LDAP server. During the synchronization session, iFolder retrieves and compiles a list of users in the LDAP containers and groups that are specified as Search DNs, and then synchronizes the iFolder user list with this master list. The timer is reset when the synchronization session ends, whether the synchronization was successful or not. When the specified interval time elapses, a new session with the LDAP server is initiated.

IMPORTANT: Whenever you synchronize on demand, the interval timer is reset.

To change how often the user list is updated, modify the LDAP Synchronization Interval field on the Modify LDAP page. For information, see Section 8.4.2, "Modifying the iFolder LDAP Settings," on page 84.

Synchronizing On Demand

To force an immediate synchronization of user information:

1 In iManager, expand the *Novell iFolder 3* role.

2 Select *System*, then wait for the page to refresh.

3 Select *LDAP* to open the System page to the LDAP tab.

4 Click *Update and Synchronize Now*.

   iFolder immediately connects to the LDAP server, retrieves and compiles a list of users in the specified Search DNs, synchronizes the iFolder user list with it, and automatically resets the interval timer for the LDAP Synchronization Interval.

5 Verify the successful update by confirming the time noted in the *Last Successful Synchronization Time* field on the LDAP Settings tab.

   The time should be after the time that you initiated the *Updated and Synchronize Now* command.

8.5 Configuring System Policies

Use the System Policies page to manage system-wide policies. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *System* > *Policy* to open the System page to the Policy tab.

- Section 8.5.1, "Viewing the Current System Policies," on page 88
- Section 8.5.2, "Modifying iFolder System Policies," on page 89

8.5.1 Viewing the Current System Policies

1 In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.

2 Select *Policy* to open the System page to the Policy tab.

3 View the following information:

Parameter	Description
User Disk Space Limit	Specifies the maximum total space that each user's iFolder data is allowed to use, across all iFolders the user owns.
Maximum File Size Limit	Specifies the maximum file size (in MB) that iFolder is allowed to synchronize. If a quota is specified, the effective maximum file size limit is the same as the quota.
File Type Restriction	Specifies a list of file types to include or to exclude from synchronization for all iFolders on the system.
Minimum Synchronization Interval	If this option is enabled, specifies the minimum interval (in seconds) for synchronizing iFolder data for each user account. Larger values are more restrictive. If the option is disabled, the value is No Limit. The interval timer is reset to the Synchronization Interval value at the end of a synchronization session. When the time elapses, another session is started.

8.5.2 Modifying iFolder System Policies

1. In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.
2. Select *Policy* to open the System page to the Policy tab, then click *Modify*.
3. Select a *Policy* check box to enable the policy, specify values for the policy, then click *OK* to apply it:

Parameter	Description
Enable User Disk Space Limit	Deselect the check box to disable a system-wide quota. Select the check box to enable a system-wide quota, then specify the total space quota (in MB) for a user's account. If you enable a system-wide quota that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed. Enabling or modifying the system-wide quota does not affect existing individual user quotas. Any existing user quota always overrides system-wide quota, whether the user quota is lower or higher than the system-wide quota. Default Value: 100 MB

Parameter	Description
Enable Maximum File Size Limit	Deselect the check box to disable the Maximum File Size Limit policy. If the policy is disabled, the value is reported as No Limit. Select the check box to enable the Maximum File Size Limit policy, then specify the maximum allowed file size in MB. If a quota is specified, the default maximum file size limit is the same as the quota. Consider the following demands on your system to determine an appropriate file size limit for iFolders in your environment: • Intended use • How often the largest files are modified • How the applications that use the largest files actually save changes to the file (whole file or deltas) • How frequently the files are synchronized by each member • How many users share an iFolder • Whether users access iFolder on the local network or across WAN or Internet connections • The average and peak available bandwidth Even if you set a very large value as a file size limit and if there is no quota to limit file sizes, the practical limit is governed by the file system on the user's computer. For example, FAT32 volumes have a maximum file size of 4 GB minus 1 byte. Default Value: Disabled, No Limit
Enable File Type Restriction	Specify whether to restrict file types that are synchronized by inclusion or exclusion filters. You cannot set both. Type a file extension, then click *OK* to add it to the list. To edit an extension, select the value, click *Edit* (the pen icon), modify the entry, then click *OK*.
Minimum Synchronization Interval	To enable a policy, select the check box, then specify the minimum synchronization interval in seconds. For example, a practical value is 600 seconds (10 minutes). Larger values are more restrictive. To disable the policy, deselect the check box. The value is reported as No Limit. Default Value: Enabled, value=0 seconds. The effective minimum synchronization interval is always the largest value of the following settings: • The system policy (default of zero), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether the user policy is larger or smaller in value. • The local machine policy, or the setting on the client machine synchronizing with the server. • The iFolder (collection) policy.

8.6 Configuring iFolder Administrators

In iManager, expand the *Novell iFolder 3* role, select *System* > *Administrators* to open the System page to the Administrators tab.

- Section 8.6.1, "Understanding the iFolder Admin User," on page 91
- Section 8.6.2, "Adding the iFolder Admin Right for a User," on page 91
- Section 8.6.3, "Removing the iFolder Admin Right for a User," on page 92

8.6.1 Understanding the iFolder Admin User

The iFolder Admin user is the primary administrator of the iFolder enterprise server. Whenever iFolders are orphaned, ownership is transferred to the iFolder Admin user for re-assignment to another user or for deletion. You initially specify the iFolder Admin user during the iFolder enterprise server configuration in YaST. For information, see Section 6.2, "Configuring the iFolder Enterprise Server," on page 53.

The iFolder Admin user must be provisioned to enable the iFolder Admin to perform management tasks. iFolder tracks this user by the LDAP object GUID, allowing it to belong to any LDAP context in the tree, even those that are not identified as search contexts. The user's movement can be tracked anywhere in the tree because it is known by the GUID, not the user DN.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the Administrators page in the Novell iFolder 3 plug-in to iManager to add or remove the iFolder Admin right for users. Only users who are in one of the contexts specified in the LDAP Search DN are eligible to be equivalent to the iFolder Admin user. For information, see Section 8.4, "Configuring the LDAP Settings for an iFolder Server," on page 82.

If you assign the iFolder Admin right to other users, those users are governed by the iFolder user list and Search DN relationship. The user is removed from the user list and stripped of the iFolder Admin right if you delete the user, remove the user's context from the list of Search DNs, or move the user to a context that is not in the Search DNs.

8.6.2 Adding the iFolder Admin Right for a User

You add the iFolder Admin right to one user at a time, but you can assign it to multiple users.

Repeat the following process for each user who you want to become an iFolder Admin user:

1. In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.
2. Select *Administrators* to view a list of users with the iFolder Admin right.
3. Click *Add* to open the User Search page.
4. Search for the user who you want to give the iFolder Admin right.
5. Select the *User* check box next to the user, then select *OK*.

   The username is added in the list of users with the iFolder Admin right.

8.6.3 Removing the iFolder Admin Right for a User

You can delete the iFolder Admin right from all users in the list except the original iFolder Admin user.

If you delete the iFolder Admin right from the username you used to log in to the server, you are immediately disconnected. You must log in to the iFolder server under a different username with the iFolder Admin right to continue managing the server.

You remove the iFolder Admin right for one user at a time. Repeat the following process for each user who you want to remove as an iFolder Admin user:

1. In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.
2. Select *Administrators* to view a list of users with the iFolder Admin right.
3. Select the *User* check box next to the user who you want to remove as an iFolder Admin user.
4. Click *Remove*.
5. Click *OK* to confirm, or click *Cancel* to back out of the action.

   The username is removed from the list of users with the iFolder Admin right.

8.7 Securing Enterprise Server Communications

This section describes how to configure SSL traffic between the iFolder enterprise server and other components. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

- Section 8.7.1, "Using SSL for Secure Communications," on page 92
- Section 8.7.2, "Configuring the SSL Cipher Suites for the Apache Server," on page 93
- Section 8.7.3, "Configuring the Enterprise Server for SSL Communications with the LDAP Server," on page 94
- Section 8.7.4, "Configuring the Enterprise Server for SSL Communications with the iFolder Client," on page 94
- Section 8.7.5, "Configuring the Enterprise Server for SSL Communications with the Web Access Server," on page 95
- Section 8.7.6, "Configuring an SSL Certificate for the Enterprise Server," on page 95

For information about configuring SSL traffic for the iFolder Web access server, see Section 9.5, "Securing Web Access Server Communications," on page 99.

8.7.1 Using SSL for Secure Communications

In a default deployment, the iFolder 3 enterprise server uses SSL 3.0 for secure communications between components as shown in the following table.

iFolder Component	Web Access Server	LDAP Server	Client	Web Browser
Enterprise Server	X	X	X	

iFolder uses the SSL 3.0 protocol instead of SSL 2.0 because it provides authentication, encryption, integrity, and non-repudiation services for network communications. During the SSL handshake, the server negotiates the cipher suite to use, establishes and shares a session key between client and server, authenticates the server to the user, and authenticates the user to the server.

The key exchange method defines how the shared secret symmetric cryptography key used for application data transfer will be agreed upon by client and server. SSL 2.0 uses only RSA key exchange, while SSL 3.0 supports a choice of key exchange algorithms, including the RC4 and RSA key exchange, when certificates are used, and Diffie-Hellman key exchange for exchanging keys without certificates and without prior communication between client and server. SSL 3.0 also supports certificate chains, which allows certificate messages to contain multiple certificates and support certificate hierarchies.

8.7.2 Configuring the SSL Cipher Suites for the Apache Server

To restrict connections to SSL 3.0 and to ensure strong encryption, we strongly recommend the following configuration for the Apache server's SSL cipher suite settings.

- Use only High and Medium security cipher suites, such as RC4 and RSA.
- Remove from consideration any ciphers that do not authenticate, such as Anonymous Diffie-Hellman (ADH) ciphers.
- Use SSL 3.0, and disable SSL 2.0.
- Disable the Low, Export, and Null cipher suites.

To set these parameters, modify the aliases in the OpenSSL* ciphers command (the SSLCipherSuite directive) in the `/etc/httpd/conf/httpd.conf` file.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2. Open the `/etc/httpd/conf/httpd.conf` file in a text editor, then locate the SSLCipherSuite directive in the Virtual Hosts section:

   ```
   SSLCipherSuite
   ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
   ```

3. Modify the plus (`+`) to a minus (`-`) in front of the ciphers you want to disable and make sure there is a `!` (not) before ADH:

   ```
   SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:-
   eNULL
   ```

4. Save your changes.
5. Start the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 start
   ```

For more information about configuring strong SSL/TLS security solutions, see SSL/TLS Strong Encryption: How-To (http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html) on the Apache.org Web site.

8.7.3 Configuring the Enterprise Server for SSL Communications with the LDAP Server

By default, the iFolder enterprise server is configured to communicate via SSL with the LDAP Server. For most deployments, this setting should not be changed. If the LDAP server is on the same machine as the enterprise server, communications do not need to be secured with SSL.

1. In iManager, expand the *Novell iFolder 3* role, select *System*, then wait for the page to refresh.
2. Select *LDAP* to open the System page to the LDAP tab, then click *Modify*.
3. In the *Port Is Secure* field, specify *Yes* to configure for SSL exchanges, or specify *No* for insecure exchanges.
4. Click *OK* to apply your changes.

8.7.4 Configuring the Enterprise Server for SSL Communications with the iFolder Client

By default, the iFolder enterprise server is configured to require SSL. All iFolder client communication to the server is encrypted using the SSL protocol. In most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. Without SSL encryption, the iFolder data is also sent in the clear.

To modify the setting, edit the SSL parameters in the `appSettings` section of the `/opt/novell/ifolder3/web/web.config` file on the enterprise server.

To configure secure Web traffic with SSL, modify the value of SimiasRequireSSL to Yes and the SimiasSSLPort to 443. For example:

```
<appSettings>

   <add key="SimiasRequireSSL" value="yes" />

   <add key="SimiasSSLPort" value="443" />

</appSettings>
```

To configure insecure Web traffice with HTTP BASIC, modify the value of SimiasRequireSSL to No and the SimiasSSLPort to 80. For example:

```
<appSettings>

   <add key="SimiasRequireSSL" value="no" />

   <add key="SimiasSSLPort" value="80" />

</appSettings>
```

8.7.5 Configuring the Enterprise Server for SSL Communications with the Web Access Server

By default, the iFolder enterprise server is configured to communicate via SSL with the iFolder Web Access server. For most deployments, this setting should not be changed. If the iFolder deployment is small and the Web Access server co-exists on the same machine as the iFolder enterprise server, an Administrator could reconfigure to disable SSL, which would increase the performance of local communications between the two servers.

Communications between the two servers are governed by the Web access server’s settings for SSL traffic. For information, see Section 9.5.3, “Configuring the Web Access Server for SSL Communications with the Enterprise Server,” on page 100.

8.7.6 Configuring an SSL Certificate for the Enterprise Server

For information, see “Managing SSL Certificates for Apache” on page 133.

Managing an iFolder Web Access Server

9

This section describes how to manage your Novell® iFolder® 3.*x* Web Access server on Novell Open Enterprise Server.

9.1 Starting iFolder Web Access Services

iFolder Web Access services start whenever you reboot the system or whenever you start Apache services.

As a root user, enter the following command at the server console:

```
/etc/init.d/apache2 start
```

9.2 Stopping iFolder Web Access Services

iFolder services stop whenever you stop the system or whenever you stop Apache services.

As a root user, enter the following command at the server console:

```
/etc/init.d/apache2 stop
```

9.3 Distributing the Web Access Server URL to Users

After you install and configure the iFolder Web Access server, distribute the URL of the server Login page to users.

For information about configuring the URL, see Section 6.3, "Configuring the iFolder Web Access Server," on page 55.

9.4 Configuring the HTTP Runtime Parameters

Two HTTP runtime parameters—Execution Time-Out (`executionTimeout`) and Maximum Request Length (`maxRequestLength`)—can affect the successful upload of a file to the Web Access server. The following table defines these run time parameters and their default values:

Parameter	Description
`executionTimeout`	The interval of time in seconds to wait between the command to upload a file and the successful execution where the file is stored on the iFolder enterprise server. The default time out is 3 minutes. Default Value: 180 (in seconds)
`maxRequestLength`	The maximum file size in bytes that a user is allowed to upload to the server via the Web Access server. The default maximum size is 10 MB for Web access. This maximum is a software hard limit. You can modify the maximum length for any value up to 10 MB. Default Value: 10240 (in KB)

Using Web Access, a user can upload a local file to the user's iFolder on the enterprise server. If the file does not upload successfully before the interval times out or if the file size exceeds the allowed maximum, the upload is stopped and reported as a failure. Because the Web browser is controlling the errors, a problem of timing out or exceeding the maximum size might result in a Bad Request or other generic error.

The Execution Time-Out and Maximum Request Length parameters must be configured with compatible settings in the `/opt/novell/ifolder3/web/web.config file` for the iFolder enterprise server and in the `/opt/novell/ifolder3/webaccess/Web.config` file for the Web Access server. The settings in `Web.config` for the enterprise server must be the same size or larger than the settings in `../webaccess/Web.config` for the Web Access server.

For example, the following code is the httpRuntime element with the default settings in the `../webaccess/Web.config` file for Web Access:

```
<httpRuntime

     executionTimeout="180"

     maxRequestLength="10240"

/>
```

To modify the httpRuntime parameters:

1. Stop iFolder.
2. Set the httpRuntime parameters on the iFolder Web Access server by editing the values in the `/opt/novell/ifolder3/webaccess/Web.config` file.
3. If necessary, set the httpRuntime parameters on the iFolder enterprise server by editing the values in the `/opt/novell/ifolder3/web/web.config` file.

   IMPORTANT: Make sure the values are the same size or larger than those set for the Web Access server.
4. Start iFolder.

For example, to set the time-out to 5 minutes (300 seconds) and the maximum file size to 5 megabytes (5120 KB) for the Web Access server, modify its httpRuntime parameter values in the `../webaccess/Web.config` file:

```
<httpRuntime

     executionTimeout="300"

     maxRequestLength="5120"

/>
```

If the `../webaccess/Web.config` values exceed the values in `../web/web.config` for the enterprise server, you must also increase the sizes of runtime parameters in that file.

9.5 Securing Web Access Server Communications

This section describes how to configure SSL traffic between the iFolder Web Access server and other components. HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

- Section 9.5.1, "Using SSL for Secure Communications," on page 99
- Section 9.5.2, "Configuring the SSL Cipher Suites for the Apache Server," on page 100
- Section 9.5.3, "Configuring the Web Access Server for SSL Communications with the Enterprise Server," on page 100
- Section 9.5.4, "Configuring the Web Access Server for SSL Communications with Web Browsers," on page 101
- Section 9.5.5, "Configuring an SSL Certificate for the Web Access Server," on page 102

For information on how to configure SSL traffic on the iFolder enterprise server, see Section 8.7, "Securing Enterprise Server Communications," on page 92.

9.5.1 Using SSL for Secure Communications

In a default deployment, the iFolder 3.*x* Web Access server uses SSL 3.0 for secure communications between components as shown in the following table.

iFolder Component	Enterprise Server	LDAP Server	Client	Web Browser
Web Access Server	X			X

For more information about SSL 3.0, see Section 8.7.1, "Using SSL for Secure Communications," on page 92.

9.5.2 Configuring the SSL Cipher Suites for the Apache Server

To restrict connections to SSL 3.0 and to ensure strong encryption, we strongly recommend the following configuration for the Apache server's SSL cipher suite settings.

- Use only High and Medium security cipher suites, such as RC4 and RSA.
- Remove from consideration any ciphers that do not authenticate, such as Anonymous Diffie-Hellman (ADH) ciphers.
- Use SSL 3.0, and disable SSL 2.0.
- Disable the Low, Export, and Null cipher suites.

To set these parameters, modify the aliases in the OpenSSL* ciphers command (the SSLCipherSuite directive) in the `/etc/httpd/conf/httpd.conf` file.

1. Stop the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 stop
   ```

2. Open the `/etc/httpd/conf/httpd.conf` file in a text editor, then locate the SSLCipherSuite directive in the Virtual Hosts section:

   ```
   SSLCipherSuite
   ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
   ```

3. Modify the plus (`+`) to a minus (`-`) in front of the ciphers you want to disable and make sure there is a `!` (not) before ADH:

   ```
   SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP:-
   eNULL
   ```

4. Save your changes.
5. Start the Apache server: At a terminal console, enter

   ```
   /etc/init.d/apache2 start
   ```

For more information about configuring strong SSL/TLS security solutions, see SSL/TLS Strong Encryption: How-To (http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html) on the Apache.org Web site.

9.5.3 Configuring the Web Access Server for SSL Communications with the Enterprise Server

By default, the iFolder enterprise server is configured to communicate with the iFolder Web Access server via SSL. For most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. If the iFolder deployment is small and the Web Access server co-exists on the same machine as the iFolder enterprise server, an Administrator could reconfigure to disable SSL, which would increase the performance of local communications between the two servers.

The communication between the Web Access server and the iFolder enterprise server is determined during the YaST configuration of the Web Access server. Specify an https:// in the URL for the enterprise server for SSL (HTTPS) communications between the servers. Traffic between the two servers is secure. If you specify an http:// in the URL, HTTP is used for communications between the servers and traffic is insecure.

The setting is stored in the /opt/novell/ifolder3/webaccess/Web.config file under the following tag:

```
<add  key="SimiasUrl" value="https://localhost" />
```

If you disable SSL between Web Access server and the enterprise server and if the two servers are on different machines, you must also disable the iFolder server SSL requirement. Because the enterprise SSL setting also controls the traffic between the enterprise server and the client, all Web traffic between servers and between the clients and the enterprise server would be insecure.

IMPORTANT: Do not disable SSL on the Web Access server if the two servers are on different machines.

If the two servers are running on the same machine and you want to disable SSL, rerun the YaST configuration, and specify http://localhost as the URL for the enterprise server. For information, see Section 6.3, "Configuring the iFolder Web Access Server," on page 55.

9.5.4 Configuring the Web Access Server for SSL Communications with Web Browsers

The iFolder 3.*x* Web Access server requires a secure connection between the user's Web browser and the Web Access server. The SSL connection supports the secure exchange of data. For most deployments, this setting should not be changed because iFolder uses HTTP BASIC for authentication, which means passwords are sent to the server in the clear. Without SSL encryption, the iFolder data is also sent in the clear.

The following Rewrite parameters control this behavior and are located in the /etc/apache2/conf.d/ifolder_web.conf file:

```
LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so

RewriteEngine On

RewriteCond %{HTTPS} !=on

RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1 [R,L]
```

To disable the requirement for SSL connections, you can comment out these Rewrite command lines in the ifolder_web.conf file. Placing a pound sign (#) at the beginning of each line renders it as a comment.

WARNING: Without an SSL connection, traffic between a user's Web browser and the Web Access server is not secure.

To disable the SSL requirement:

1 Stop the iFolder Web Access services.

2 Edit the /etc/apache2/conf.d/ifolder_web.conf file to comment out the Rewrite command lines.

   For example:

```
#LoadModule rewrite_module /usr/lib/apache2/mod_rewrite.so
#RewriteEngine On
```

```
#RewriteCond %{HTTPS} !=on

#RewriteRule ^/ifolder/(.*) https://%{SERVER_NAME}/ifolder/$1
[R,L]
```

3 Start the iFolder Web Access services.

9.5.5 Configuring an SSL Certificate for the Web Access Server

For information, see "Managing SSL Certificates for Apache" on page 133.

Managing iFolder Users 10

This section discusses how to manage Novell® iFolder® 3.*x* enterprise server with iManager.

10.1 Provisioning Users for iFolder Services

Provisioning a user for iFolder occurs automatically based on the containers and groups you specify as Search DNs in the LDAP settings. You can specify any existing context. For information, see Section 3.5, "iFolder User Account Considerations," on page 35.

The list of iFolder users is updated periodically when the LDAP synchronization occurs. New users are added to the list of iFolder users. Deleted users are removed from the list of iFolder users. (This might create orphaned iFolders if the deleted user owned any iFolders.)

IMPORTANT: Whenever you move a user between contexts and you want to provide continuous service for the user, make sure to add the target context to the list of Search DNs before you move the User object in eDirectory.

For information about configuring Search DNs, see Section 8.4, "Configuring the LDAP Settings for an iFolder Server," on page 82.

10.2 Searching for a User Account

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Users* to go to the User Search page.
2. Select a name criterion (*User Name*, *First Name*, *Last Name*).
3. Select a filter criterion (*Contains*, *Begins With*, *Ends With*, *Equals*).
4. Use one or more of the following search methods, then click *Search*:
    - Type the name of the user in the *Search Users* field.
    - Type one or more letters in the *Search Users* field.
    - Type an asterisk (*) in the *Search Users* field to return a list of all Users on the system.
    - Leave the *Search Users* field empty to return a list of all Users on the system.

   Do not click anywhere in the page until the page completely refreshes.
5. Browse or sort the list of users to locate the one you want to manage.
6. Click the *User Name* link to view the view or set policies and manage its iFolders.

Browsing the Users in the Search Results

Scroll up and down to browse the search results and locate the User you want to manage. The combination of the username, first name, and last name should help you locate the user.

Sorting the Users in the Search Results

Your search results are initially displayed by username in alphabetical order. Click the column heading link to initiate the sort with that column as the primary key. Click the same heading link again to initiate a sort in the reverse sort order.

- **Type:** An icon indicating whether the user has the iFolder Admin right (user wearing a referee-striped uniform) or is a normal user (user icon).
- **Name:** The username assigned to the user account, such as `jsmith`.
- **Full Name:** The first and last name of the user account.

Click the user's name to manage User policies and iFolders for the user.

10.3 Viewing General User Account Information

In iManager, click *Novell iFolder 3.x* > *Users*, search for the user whose iFolder account you want to manage, then click the *Name* link for the User. The User page opens to the General tab, which displays the user's full name, username, and the last time the user logged in. If the user has not yet set up an account on a client machine, the *Last Login Time* reports `Not Set`.

10.4 Configuring User Account Policies

- Section 10.4.1, "Viewing the Current User Account Policies," on page 104
- Section 10.4.2, "Modifying User Account Policies," on page 106

10.4.1 Viewing the Current User Account Policies

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, select *Users*, then wait for the page to refresh to view a list of current iFolder users.
2. Click the link for the user's name to open the User page for that user account.
3. You can view the following information on the *User* > *Policy* page:

Parameter	Description
Account Enabled	Specifies whether the user is currently allowed to log in to synchronize iFolders.
Space Used	Specifies the total space currently in use on the server for all iFolders owned by this selected user.
Space Available	Specifies the difference between any space restrictions on the account and the space currently in use. If no quota is in effect, the value is No Limit.

Parameter	Description
Space Limit	Specifies the maximum total space (in MB) that a user's iFolder data is allowed to use, across all iFolders the user owns. A user quota supersedes a system-wide quota, whether the user quota is larger or smaller than the system-wide quota. The user quota can then be limited, but not increased by a policy on an iFolder. **IMPORTANT:** Users cannot successfully synchronize files of a size that would cause a quota to be exceeded. If they try to do so, only part of the file is synchronized, resulting in data corruption. If the total space consumed by iFolder data is nearing an effective quota (system, user, or iFolder), the user should stop synchronizing files until one or more of the following tasks results in enough space to safely synchronize the user's files in the iFolder where the file resides: • The system-wide quota, user quota for the iFolder owner, and the iFolder quota are modified as needed. • Files are moved from any of the iFolders owned by the user to another location where they no longer affect the effective quota, or files are deleted to clear space. • Files are moved from the iFolder to another location where they no longer affect the effective quota, or its files are deleted to clear space.
File Type Restriction	Specifies to allow all file types or lists the file types to include or to exclude from synchronization for the selected user's account. The file manager files called `thumbs.db` and `.DS_Store` are never synchronized. You do not need to keep these files, and synchronizing them results in repeated file conflict errors. If you have not set any individual restrictions for this user, this field reports `thumbs.db` and `.DS_Store` as part of the system-wide file-type restrictions. After you set individual file-type restrictions for the user, the user's settings are displayed instead. Even if the `thumbs.db` and `.DS_Store` restrictions are not displayed, they always apply; you cannot override them.
Minimum Synchronization Interval	Specifies the minimum interval (in seconds) that a user's client can check iFolder data on the server and iFolder data on local iFolders to identify files that need to be downloaded or uploaded. Longer interval limits are more restrictive than shorter ones. If a user policy is set, it overrides the system policy, whether the user's interval is shorter or longer in value.
Effective Synchronization Interval	Specifies the effective minimum synchronization interval for the selected user. The effective minimum synchronization interval is always the largest value from the following settings: • The system policy (default of zero (`0`)), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether the user policy is larger or smaller in value. • The local machine policy, or the setting on the client machine synchronizing with the server. • The iFolder (collection) policy.

10.4.2 Modifying User Account Policies

1 In iManager Roles and Tasks, expand the *Novell iFolder 3* role, select *Users*, then wait for the page to refresh to view a list of current iFolder users.

2 Click the link for the user's name to open the User page for that user account.

3 On the User page, click *Modify*.

4 Select the *Policy* check box to enable it, set its values, then click *OK* to apply the policies:

Parameter	Description
Account Enabled	Select the value to enable the account for login. Deselect the value to disable the account for login. If the user is logged in when you make this change, the user's session continues until the user logs out. The policy takes effect the next time the user attempts to log in to the account. To have the lockout take effect immediately, you must restart the Apache services for the iFolder server, which disconnects all active sessions, including the user's session. Default Value: Enabled, Yes
Enable Space Limit	Specifies the maximum total space (in MB) that a user's iFolder data is allowed to use, across all iFolders the user owns for the selected user account. Deselect this option if there is no individual user quota, or to accept the system-wide quota for the selected user account. Select this option to enforce a user quota, then specify the total space quota (in MB) for the selected user account. If you enable a user space limit that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed. Default Value: Disabled or the system-wide quota if it is set
Enable File Type Restriction	Deselect this option to allow all file types to be synchronized or to apply the system-wide file type restrictions for the user account. Select this option to restrict some file types for this user, then specify the inclusion or exclusion filters that determine the file types that can be synchronized for the user account. To add a file extension to an inclusion or exclusion filter, type the extension (such as `.mpg`), then click *OK* to apply the filter. To edit an extension, select the value, click *Edit* (the pen icon), modify the entry, then click *OK* to apply the change. Default Value: Disabled, Allow all file types or the System-wide settings

Parameter	Description
Minimum Synchronization Interval	Deselect the check box to set no synchronization interval or to accept the system-wide setting for the user account. If no value is set for system-wide or user policies, the value reported is `No Limit`. Select the check box to enable a minimum synchronization interval, then specify the minimum interval (in seconds). For example, a practical value is 600 seconds (10 minutes). Default Value: Disabled, or the system-wide policy

10.5 Enabling and Disabling iFolder User Accounts

Disabling a user's account temporarily, as opposed to deleting the user account, turns off the ability of that user to log in to the iFolder server. The user remains a valid iFolder user, can be shared with, and his or her iFolders are not orphans. The user cannot log in and, therefore, cannot synchronize (up or down) any data until the account is again enabled.

1 In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Enable/Disable Users Account*.

2 Search for the user whose account you want to enable or disable for login.

3 Select the *User* check box next to the user, then click *OK*.

4 Do one of the following:

- Enable login for the user account by selecting *Account Enabled*, then click *OK*.
- Disable login for the user account by deselecting *Account Enabled*, then click *OK*.

10.6 Setting a User Account Quota

1 In iManager, expand the *Novell iFolder 3* role, then select *Set Users Account Quota*.

2 Search for the user whose account you want to manage.

3 Select the *User* check box next to the user, then click *OK*.

4 Do one of the following:

- Enable a space quota for the selected user by selecting *Enable Space Limit*, specify how much space the user can consume for all iFolders owned by the user, then click *OK*.
- Disable a space quota for the selected user by deselecting *Enable Space Limit*, then click *OK*.

Managing iFolders

11

This section discusses how and administrator can manage iFolders on the Novell® iFolder® 3.*x* enterprise server, using the Novell iFolder 3 plug-in for Novell iManager 2.5.

11.1 Creating an iFolder in iManager

Creating an iFolder from the iFolders Page

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *iFolders*.
2. Click *New* to open the Create an iFolder dialog box.
3. Next to *Owner*, click *Select* to open the Select iFolder Owner page.
4. Search for the user who you want to make the owner of the iFolder, select the *User* check box, then click *OK*.

   On the New iFolder page, the Owner field shows the user's first and last name.
5. Specify a name for the iFolder.
6. Click *OK* to create the iFolder.

   On successful creation, a subscription notification is sent to the iFolder Owner. The new iFolder is listed alone in the Search Results area.
7. Click the iFolder's *Name* link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Creating an iFolder from the User Page

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Users*.
2. Search for and select the *Name* of the user you want to manage, then click *OK*.

   The User page opens to the user's information.
3. On the User page, select the *iFolders* tab, then click *New* to open the Create an iFolder dialog box.

   The user appears in the Owner field.
4. Specify a name for the iFolder.

5 Click *OK* to create the iFolder.

On successful creation, a subscription notification is sent to the iFolder Owner. The new iFolder is listed alone in the Search Results area.

6 Click the iFolder's *Name* link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

11.2 Searching for an iFolder

1 In iManager, expand the *Novell iFolder 3* role.

2 Use one of the following methods to get a list of iFolders:

- Click the *iFolders* role to open the Search iFolders page, specify your search criteria, then click OK.
- Click *Orphaned iFolders* on the iFolders page or click the *Orphaned iFolders* role to retrieve a list of orphaned iFolders.

3 Use one or more of the following search methods, then click Search:

- Select *Equals* as the filter criterion, then type the name of the iFolder you want to locate in the Search iFolders field.
- Select a filter criterion (*Contains*, *Begins With*, *Ends With*, *Equals*) for the name of the iFolder, then type one or more letters in the *Search iFolder*s field.
- Type an asterisk (*) in the *Search iFolders* field to return a list of all iFolders on the system.
- Leave the *Search iFolders* field empty to return a list of all iFolders on the system.

Do not click anywhere in the page until the page completely refreshes, then you can browse, sort, or manage the iFolders listed in the Search Results report.

4 Browse or sort the list of iFolders to locate the iFolder you want to manage.

5 Click the iFolder's *Name* link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Browsing the iFolders in the Search Results

Scroll up and down to browse the search results and locate the iFolder you want to manage. The combination of the iFolder's name and owner help to identify the iFolder you seek.

Sorting the iFolders in the Search Results

You can sort the list of iFolders by *Type*, *Name*, or *Owner*. Click the column heading link to initiate the sort with that column as the primary key. Click the same heading link again to initiate a sort in the reverse sort order.

11.3 Viewing Information about an iFolder

In iManager, select the *Novell iFolder* role, then select *iFolders* or *Orphaned iFolders*, locate the iFolder you want to manage, then click the iFolder's *Name* link to open the iFolder management page to the General tab.

Parameter	Description
Owner	The username of the owner of the selected iFolder. For orphaned iFolders, the iFolder Admin user is made the custodian owner until the iFolder can be reassigned or deleted. The iFolder owner has the Full Control right to the iFolder. The owner manages membership and access rights for users, and can remove the Full Control right for any member. With an enterprise server, the disk space used by the owner's iFolders counts against the owner's user account quotas on the enterprise server.
Path	The actual location of the iFolder and its data on the server. For example: `/var/opt/novell/ifolder3/simias/SimiasFiles/`*`e84fdc6e-3d51-49df-ae3f-8c9213c76994/iFolder_Name`* In this example, *`e84fdc6e-3d51-49df-ae3f-8c9213c76994`* is the unique ID of the iFolder share.

11.4 Configuring Policies for an iFolder

Use the iFolder Policy tab to view and manage the policies for an iFolder.

1. In iManager, expand the *Novell iFolder 3* role, then select *iFolders* or *Orphaned iFolders*.
2. Locate the iFolder you want to manage, then click the iFolder's *Name* link to open the iFolder management page to the General tab.
3. Click the *Policy* tab, then click *Modify*.
4. Configure one or more of the following values, then click *OK* to apply the new settings:

Parameter	Description
Synchronization Enabled	Select *Synchronization Enabled* to allow the synchronization of data in the iFolder. Deselect *Synchronization Enabled* to turn off synchronization, usually temporarily. Default Value: Enabled, Yes
Enable Space Limit	Select the *Enable Space Limit* check box, then specify the maximum size (in MB) for the selected iFolder. If you enable a system-wide iFolder quota, a user's account quota overrides it, whether the user quota is lower or higher than the system quota. Default Value: Disabled, No Limit
Space Used (View only)	Reports how much space the iFolder data currently consumes.

Parameter	Description
Enable File Type Restriction	To enable filtering, select *Enable File Type Restriction*. Specify one of the following methods to filter files that are synchronized: • Select *Allow All File Types Except*, then specify the list of file types to exclude when iFolder synchronizes files in the iFolder. • Select *Only Allow the Following File Types*, then specify the list of file types to include when iFolder synchronizes files in the iFolder. Type a file extension, then click *OK* to add it to the list. To edit an extension, select the value, click *Edit* (the Pen icon), modify the entry, then click *OK* to apply the change. Default Value: Disabled, No restriction
Minimum Synchronization Interval	Select the *Synchronization Interval* check box to enable a minimum interval setting for the selected iFolder, then specify the minimum value in seconds that users are allowed to set on their clients. To disable the setting, deselect the *Synchronization Interval* check box. If the option is disabled, the value reported is `No Limit`. If this option is enabled, the minimum synchronization interval specifies the minimum interval in seconds that a user's client can check iFolder data on the server and local iFolders to identify files that need to be downloaded or uploaded. The effective minimum synchronization interval is always the largest value from the following settings: • The system policy (default of zero (`0`)), unless there is a user policy set. If a user policy is set, the user policy overrides the system policy, whether it is larger or smaller in value. • The local machine policy, or the setting on the client machine synchronizing with the server • The iFolder (collection) policy Default Value: Enabled, 0 seconds

11.5 Sharing an iFolder

Use the *iFolder* > *Members* tab to manage membership in an iFolder.

- Section 11.5.1, "Adding a Member," on page 112
- Section 11.5.2, "Setting the iFolder Access Right for a Member," on page 113
- Section 11.5.3, "Removing a Member," on page 114

11.5.1 Adding a Member

1. In iManager, expand the *Novell iFolder 3* role, then select *iFolders* or *Orphaned iFolders*.
2. Locate the iFolder you want to manage, then click the iFolder's *Name* link to open the iFolder management page to the General tab.
3. Select the *Members* tab, then click *Add*.

4. Search for the user you want to make a member, select the check box next to the user's name, then click *OK*.

   The user is given Read Only access to the iFolder.

5. (Optional) Select the *User* check box, then click *Rights* and specify the Access right as *Full Control*, *Read/Write*, or *Read Only* right.

   Wait for the page to refresh. The user's icon should reflect the new access right. A notification message inviting the user to participate is sent to the user's account.

11.5.2 Setting the iFolder Access Right for a Member

For an overview of access rights, see Section 1.4.6, "iFolder Access Rights," on page 18.

The following table describes the capabilities associated with each level of access for users.

Capabilities	Owner	Full Control	Read/Write	Read Only
With an enterprise server, the space consumed by the iFolder on the server is charged against the user's quota	Yes	No	No	No
Reassign ownership to another user	Yes	No	No	No
Set a quota for the iFolder	Yes	No	No	No
Make the iFolder available to other users (sharing)	Yes	Yes	No	No
Make the iFolder unavailable to other users (stop sharing)	Yes	Yes, except the owner	No	No
Assign access rights for other users	Yes	Yes, except the owner	No	No
Read directories and files in the iFolder	Yes	Yes	Yes	Yes
Add, modify, or delete directories and files in the iFolder	Yes	Yes	Yes	No
Rename directories and files in an iFolder	Yes	Yes	Yes	Yes
Rename the iFolder	No	No	No	No
Set up an iFolder on multiple computers	Yes	Yes	Yes	Yes
Revert an iFolder (do not participate on a local computer)	Yes	Yes	Yes	Yes
Delete an available iFolder to decline participating	Yes	Yes	Yes	Yes
Delete the iFolder and delete the iFolder and its files from the server (make it a normal folder again and no longer share it with others)	Yes	No	No	No

1 In iManager, expand the *Novell iFolder 3* role, then select *iFolders* or *Orphaned iFolders*.

2 Locate the iFolder you want to manage, then click the iFolder's *Name* link to open the iFolder management page to the General tab.

3 Select the *Members* tab, then select the check box next to the member whose access right you want to manage.

4 Select the *Rights* drop-down menu, then select the *Full Control*, *Read/Write*, or *Read Only* right.

Wait for the page to refresh. The user's icon should reflect the new access right.

11.5.3 Removing a Member

1 In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *iFolders* or *Orphaned iFolders*.

2 Locate the iFolder you want to manage, then click the iFolder's *Name* link to open the iFolder management page to the General tab.

3 Select the *Members* tab, then select the check box next to the member user's name.

4 Click *Remove*.

The user's local copy of the data remains on the user's computer, but the user no longer has access to the server copy of the iFolder data.

11.6 Deleting an iFolder

1 In iManager Roles and tasks, expand the *Novell iFolder 3* role, then select *Users*.

2 Search for and select the user you want to manage, then click *OK*.

The User page opens to the user's information.

3 Select the check box next to the iFolder you want to delete, then click *Delete*.

4 Click *OK* to confirm the deletion.

The iFolder is removed from the list of iFolders. The local copies of the iFolder contents remain on all member users' computers.

11.7 Transferring Ownership of an iFolder

When you change the owner of an iFolder, the existing owner becomes a member of the iFolder and is assigned the Read/Write right. For orphaned iFolders, the iFolder Admin user becomes the owner. If the new owner is not currently a member of the iFolder, a subscription notification is sent to the user's iFolder account.

Changing the iFolder Owner from the iFolders Page

1 In iManager Roles and Tasks, expand the *Novell iFolder 3* role.

2 Use one of the following methods to get a list of iFolders:

- Select *iFolders* to open the Search iFolders page.
- Select *Orphaned iFolders* to retrieve a list of orphaned iFolders.

3 Search for the iFolder you want to manage.

4. Select the check box next to the iFolder, then click *Change Owner*.
5. Search for the user you want to assign as the new owner of the iFolder, select the check box next to the user's name, then click *OK*.

Changing the iFolder Owner from the User's Page

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Users*.
2. Search for and select the user you want to manage, then click *OK*.

   The User page opens to the user's information.
3. On the *User* > *iFolders* tab, select the check box next to the iFolder you want to manage, the click *Change Owner*.

   The Users Search page opens.
4. Search for the user who you want to make the new owner of the iFolder, select the check box next to the user's name, then click *OK*.

11.8 Enabling and Disabling Synchronization for an iFolder

Disabling synchronization temporarily, as opposed to deleting or disabling the entire user account, turns off the ability of the selected iFolder to synchronize.

If the iFolder is locked by an active system process (such as backup), you receive an Already Locked Exception (`AlreadyLockedException`) error. You cannot enable or disable synchronization for the iFolder until that process ends; try again later.

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Enable/Disable iFolder Sync*.
2. Search for the iFolder that you want to enable or disable for synchronization.
3. Select the *iFolder* check box, then click *OK*.
4. Do one of the following:
   - Enable synchronization for the iFolder by selecting *Synchronization Enabled*, then click *OK*.
   - Disable synchronization for the iFolder by deselecting *Synchronization Enabled*, then click *OK*.

11.9 Managing Orphaned iFolders

An iFolder becomes orphaned when its owner is no longer provisioned for iFolder services. Orphaned iFolders are automatically assigned to the iFolder Admin user, who serves as a temporary owner until the iFolder can be assigned or deleted. Meanwhile, the members of the iFolder can continue to use it under the policies and access controls that were in place at the time the iFolder became orphaned.

1. In iManager Roles and Tasks, expand the *Novell iFolder 3* role, then select *Orphaned iFolders*.
2. Browse to locate the orphaned iFolder you want to manage, then select the check box next to the iFolder.
3. Do one of the following:

- **Change Owner:** Click *Change Owner*, search for and select the user you want to make the owner, then click *OK*.

  The specified user becomes the iFolder's owner and has the Full Control right to the iFolder. If the user was not previously a member of the iFolder, the iFolder is made available for setup when the user next logs in, synchronizes invitations, or manually refreshes invitations. The previous owner's username is removed from the list of iFolder members. Any policies set for the new owner's account are imposed on the iFolder. The share relationship and access rights for current members are unchanged.
- **Delete iFolder:** Click *Delete*, then click *OK* to confirm the deletion. The iFolder share relationship is deleted and the iFolder and its files are removed from the iFolder server. The local copy of the iFolder on each member's computer is reverted to a normal folder.

Configuration Files

A

A.1 Simias.config File

The default locations of the `Simias.config` file are the `/var/lib/wwwrun/.local/share/simias/` directory and the `/home/wwwrun/.local/share/simias/` directory.

```
<configuration>

  <section name="Domain">

    <setting name="EnterpriseName" value="ifoldersvr1" />

    <setting name="EnterpriseDescription" value="20050525 Build 1" />

    <setting name="AdminDN" value="cn=iFolderAdmin,o=acme" />

    <setting name="Encoding" value="iso-8859-1" />

    <setting name="EnterpriseID"
        value="76c8cfd1-f876-4bc5-b7fd-beb5119c870d" />

  </section>

  <section name="StoreProvider">

    <setting name="Path" value="/var/opt/novell/ifolder3" />

    <setting name="Assembly" value="Simias.dll" />

    <setting name="Type"
       value="Simias.Storage.Provider.Flaim.FlaimProvider" />

    <setting name="Version" value="0.2" />

  </section>

  <section name="LdapAuthentication">

    <setting name="LdapUri" value="ldaps://10.10.10.1:636/" />

    <setting name="ProxyDN" value="cn=iFolderProxy1234,o=acme" />

    <setting name="ProxyPassword" value="" />

  </section>

  <section name="LdapSystemBook">

    <setting name="SyncInterval" value="86400" />

    <setting name="SyncOnStart" value="True" />
    <setting name="Search">

      <Context dn="o=acme" />

    </setting>

  </section>

  <section name="ServiceManager">

    <setting name="Services">

      <Service name="Enterprise Authentication Service"
         assembly="Novell.Simias.Enterprise.dll"
         enabled="True" type="Thread"
         class="Novell.iFolder.Ldap.EnterpriseAuthentication" />

      <Service name="Simias Local Domain Provider" assembly="Simias"
         enabled="True"
         type="Thread" class="Simias.LocalProvider" />

      <Service name="Simias Change Log Service" assembly="Simias"
         enabled="True" type="Thread"
         class="Simias.Storage.ChangeLog" />

      <Service
         name="LDAP to System Address Book Synchronization Service"
         assembly="Novell.Simias.Enterprise.dll" enabled="True"
         type="Thread"
         class="Novell.AddressBook.LdapSync.LdapSystemBookService" />

    </setting>

  </section>

  <section name="NodeCache">

    <setting name="TimeToLive" value="60" />

  </section>

  <section name="SyncService">

    <setting name="ConcurrentClients" value="64" />

  </section>

</configuration>
```

A.2 Web.config File for the Enterprise Server

By default, the `web.config` file for the enterprise server is in the `/opt/novell/ifolder3/web` directory. The following is an example of a configured file.

```
<?xml version="1.0" encoding="utf-8"?>

<configuration>

<!-- Enable this if you want gzip compression. Also uncomment the
<mono.aspnet> section below

  <configSections>

     <sectionGroup name="mono.aspnet">

     <section name="acceptEncoding"
        type="Mono.Http.Configuration.AcceptEncodingSectionHandler,
              Mono.Http, Version=1.0.5000.0,
              PublicKeyToken=0738eb9f132ed756" />

     </sectionGroup>

  </configSections>

-->

<system.web>

   <customErrors mode="Off"/>

   <httpRuntime

       executionTimeout="180"

       maxRequestLength="1048576"

   />

<!-- take this out until we need it

  <webServices>

    <soapExtensionTypes>

      <add type="DumpExtension, extensions" priority="0" group="0" />

      <add type="EncryptExtension, extensions" priority="1"
           group="0" />

    </soapExtensionTypes>

  </webServices>

-->

  <authentication mode="None">

  </authentication>

  <httpModules>
```

```
    <add name="AuthenticationModule"

       type="Simias.Security.Web.AuthenticationModule, Simias"/>

  </httpModules>

</system.web>

<!--

<mono.aspnet>

   <acceptEncoding>

   <add encoding="gzip"
       type="Mono.Http.GZipWriteFilter, Mono.Http, Version=1.0.5000.0,
            PublicKeyToken=0738eb9f132ed756" disabled="no" />

   </acceptEncoding>

</mono.aspnet>

-->

<appSettings>

    <add key="MonoServerDefaultIndexFiles" value="index.aspx,
              Default.aspx,default.aspx, index.html, index.htm" />

    <add key="SimiasAuthNotRequired" value="Login.ashx,
PingSimias:Simias.Web.SimiasService:Simias.Web,
GetDomainID:Simias.DomainService.DomainService:Novell.Simias.Enterpris
e" />

    <add key="SimiasRequireSSL" value="yes" />

    <add key="SimiasSSLPort" value="443" />

    <add key="Enterprise" value="True" />

</appSettings>

</configuration>
```

A.3 Web.config File for the Web Access Server

By default, the `Web.config` file for the Web Access server is in the `/opt/novell/ifolder3/webaccess/` directory. The following is an example of a configured file.

```
<?xml version="1.0" encoding="utf-8"?>

<configuration>

  <system.web>

    <httpRuntime executionTimeout="180" maxRequestLength="10240" />

    <!--  DYNAMIC DEBUG COMPILATION

          Set compilation debug="true" to enable ASPX debugging.

          Otherwise, setting this value to false will improve runtime

          performance of this application. Set compilation

          debug="true" to insert debugging symbols (.pdb information)

          into the compiled page. Because this creates a larger file

          that executes more slowly, you should set this value to true

          only when debugging and to false at all other times. For more

          information, refer to the documentation about debugging

          ASP.NET files.

    -->

    <compilation defaultLanguage="C#" debug="true" />

    <!--  CUSTOM ERROR MESSAGES

          Set customErrors mode="On" or "RemoteOnly" to enable custom

          error messages, "Off" to disable.

          Add <error> tags for each of the errors you want to handle.

          "On" Always display custom (friendly) messages.

          "Off" Always display detailed ASP.NET error information.

          "RemoteOnly" Display custom (friendly) messages only to users

          not running on the local Web server. This setting is

          recommended for security purposes, so that you do not display

         application detail information to remote clients.

    -->

    <customErrors defaultRedirect="Error.aspx" mode="On" />
```

```
 <!--  AUTHENTICATION
       This section sets the authentication policies of the
       application. Possible modes are
       "Windows", "Forms", "Passport" and "None".
       "None" No authentication is performed.
       "Windows" IIS performs authentication (Basic, Digest, or
       Integrated Windows) according to its settings for the
       application. Anonymous access must be disabled in IIS.
       "Forms" You provide a custom form (Web page) for users to
       enter their credentials, and then you authenticate them in
       your application. A user credential token is stored
       in a cookie.
       "Passport" Authentication is performed via a centralized
       authentication service provided by Microsoft that offers a
       single logon and core profile services for member sites.
 -->
 <authentication mode="Forms">
   <forms name="iFolderWebAuth" loginUrl="Login.aspx" timeout="20"
          slidingExpiration="true"  />
 </authentication>
<!--  AUTHORIZATION
       This section sets the authorization policies of the
       application. You can allow or deny access to application
       resources by user or role.
       Wildcards:
         "*" mean everyone,
         "?" means anonymous (unauthenticated) users.
 -->
 <authorization>
   <deny users="?" />
 </authorization>
```

```
  <!--  APPLICATION-LEVEL TRACE LOGGING
        Application-level tracing enables trace log output for every
        page within an application.
       Set trace enabled="true" to enable application trace logging.
       If pageOutput="true", the trace information will be displayed
        at the bottom of each page.  Otherwise, you can view the
        application trace log by browsing the "trace.axd" page from
        your web application root.
  -->
  <trace enabled="false" requestLimit="10" pageOutput="false"
         traceMode="SortByTime" localOnly="true" />
  <!--  SESSION STATE SETTINGS
        By default ASP.NET uses cookies to identify which requests
       belong to a particular session. If cookies are not available,
        a session can be tracked by adding a session
        identifier to the URL. To disable cookies, set
        sessionState cookieless="true".
  -->
  <sessionState mode="InProc" cookieless="false" timeout="30" />
  <!--  GLOBALIZATION
        This section sets the globalization settings of the
        application.
  -->
  <globalization requestEncoding="utf-8" responseEncoding="utf-8" />
</system.web>
<appSettings>
  <add key="SimiasUrl" value="https://localhost" />
  <add key="SimiasCert" value="a_certification_key_goes_here" />
</appSettings>
<location path="Default.aspx">
  <system.web>
    <authorization>
```

```
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
  <location path="Error.aspx">
    <system.web>
      <authorization>
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
</configuration>
```

Clustering iFolder 3.*x* with Novell Cluster Services for Linux

B

This section discusses how to configure a Novell® iFolder® 3.*x* server cluster, using Novell Cluster Services™ (NCS) for Linux.

- Section B.1, "Prerequisites for Clustering iFolder 3.x Services," on page 125
- Section B.2, "Installing Novell Cluster Services for Linux," on page 125
- Section B.3, "Configuring iFolder 3.x Services on an NCS for Linux Cluster," on page 126
- Section B.4, "Creating the iFolder 3.x Cluster Resource," on page 129
- Section B.5, "Managing the iFolder 3.x Cluster Resource," on page 129
- Section B.6, "Sample Load Scripts for iFolder 3.x Clusters," on page 129
- Section B.7, "Sample Unload Scripts for iFolder 3.x Clusters," on page 131

For information about NCS, see the *OES Novell Cluster Services 1.8 Administration Guide for Linux* (http://www.novell.com/documentation/oes/cluster_admin_lx/data/h4hgu4hs.html).

B.1 Prerequisites for Clustering iFolder 3.*x* Services

Your cluster must contain at least two OES Linux servers. Each node in your iFolder 3.*x* cluster must satisfy the following:

- "Prerequisites and Guidelines" on page 45 for iFolder 3.*x*
- Prerequisites and requirements for Novell Cluster Services for Linux. For information, see "Installation and Setup" (http://www.novell.com/documentation/oes/cluster_admin_lx/data/hc8jxt45.html) in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.

B.2 Installing Novell Cluster Services for Linux

For each node in the planned cluster:

1. Make sure each node in the cluster satisfies the Section B.1, "Prerequisites for Clustering iFolder 3.x Services," on page 125.
2. Install and configure Novell Cluster Services (NCS) on the OES Linux servers you plan to use in the iFolder 3.*x* cluster.

   IMPORTANT: Do not create a Cluster Resource at this time; it is configured after you set up iFolder services on the cluster.

   For information, see "Installing Novell Cluster Services" (http://www.novell.com/documentation/oes/cluster_admin_lx/data/ht05s5vv.html) in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.
3. Continue with Section B.3, "Configuring iFolder 3.x Services on an NCS for Linux Cluster," on page 126.

B.3 Configuring iFolder 3.*x* Services on an NCS for Linux Cluster

The following procedure describes how to configure Novell iFolder 3.*x* services on an NCS for Linux cluster. You can optionally add iFolder 3.*x* Web Access services to the cluster.

1 On one of the nodes (Node 1), set up a shared volume to use for storing iFolder data.

This can either be a SAN or iSCSI volume. For information, see "Setting Up Novell Cluster Services" (http://www.novell.com/documentation/oes/cluster_admin_lx/data/h2mdblj1.html) in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.

IMPORTANT: Do not create a Cluster Resource at this time; it is configured after you finish setting up iFolder services on the cluster.

2 Share the same Apache SSL certificate between all of the nodes.

For information, see Section C.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 135.

2a Get key and certificate for the cluster's highly available DNS name.

For information, see "Managing SSL Certificates for Apache" on page 133.

2b On Node 1: Mount the shared volume, then copy the key and certificate files to the cluster's shared volume.

2c On each node: Modify the node's Apache SSL configuration file to point to the key and certificate files on the shared volume.

3 For each node in the cluster, install iFolder services:

3a In YaST, install iFolder 3 and iFolder 3 Web Access (optional), but do not configure services at this time.

For information, see Section 6.1, "Installing iFolder on an Existing OES Linux Server," on page 51.

3b Repeat the install on each node in the cluster, then continue with Step 4.

4 Configure iFolder services Node 1 by doing the following:

In the following commands, replace */mnt/ifolder3* with the mount point of the shared volume you created in Step 1.

4a Mount the shared volume. At a server console, enter

```
mnt /dev/sda1 /mnt/ifolder3
```

Replace */dev/sda1* with the disk or partition containing the file system.

4b Create the `.local` directory structure on the shared volume. At a server console, enter

```
cd /mnt/ifolder3
mkdir -p .local/share/simias
```

4c Change ownership on the mounted shared volume to user `wwwrun` and group `www`. At a server console, enter

```
chown -R wwwrun:www /mnt/ifolder3
```

4d Create a symbolic link from the shared volume to your wwwrun users home directory. At a server console, enter

```
ln -s /mnt/ifolder3/.local /var/lib/wwwrun/
```

Verify that the symbolic link is valid. At a terminal console, enter

```
ll /var/lib/wwwrun/
```

If the link appears blue, it is valid. If the link appears red, the link is invalid.

4e Change ownership of the .local symbolic link to user `wwwrun` and group `www`. At a server console, enter

```
chown -R wwwrun:www /var/lib/wwwrun/.local
```

4f In YaSt, configure iFolder 3.*x*. For information, see Section 6.2, "Configuring the iFolder Enterprise Server," on page 53.

For the System Store Path, specify the mounted shared volume:

```
/mnt/ifolder3
```

At the end of the configuration, allow YaST to start Apache.

After the configuration has completed, open your Web browser to the iFolder server to make sure it is running.

```
http://192.168.1.1/simias10/Simias.asmx
```

Replace *192.168.1.1* with the IP address of the server node you are configuring. If everything is working properly, you should get an authentication prompt.

4g If you installed iFolder 3.*x* Web Access server, in YaST, configure Web Access. For information, see Section 6.3, "Configuring the iFolder Web Access Server," on page 55.

For the Web Access Alias, specify an alias such as /ifolder. Use the same alias on all nodes when you configure them later.

For the iFolder Server URL, specify SSL (by using https in the URL) and specify `localhost` as the location. For example:

```
https://localhost
```

4h Stop Apache on Node 1, then unmount the shared volume. At the server console, enter

```
/etc/init.d/apache2 stop
umount /mnt/ifolder3
```

4i Modify the server settings so that Apache does not load at boot and Apache starts and stops are controlled with the cluster's load and unload scripts.

At the server console, enter

```
chkconfig apache2 off
```

5 Configure iFolder services on each of the remaining nodes in the cluster by doing the following:

In the following commands, replace */mnt/ifolder3* with the mount point of the shared volume you created in Step 1.

5a Mount the shared volume. At a terminal console, enter

```
mnt /dev/sda1 /mnt/ifolder3
```

Replace `/dev/sda1` with the disk or partition containing the file system.

The shared volume needs to be available at this time so that the shared SSL certificate on the shared volume is accessible when YaST tries to restart Apache.

5b In YaSt, configure iFolder 3.*x*. For information, see Section 6.2, "Configuring the iFolder Enterprise Server," on page 53.

For the *System Store Path*, specify the some temporary location; this value is replaced later.

```
/tmp/ifolder3
```

At the end of the configuration, allow YaST to start Apache.

After the configuration has completed, open your Web browser to the iFolder server to make sure it is running.

```
http://192.168.1.1/simias10/Simias.asmx
```

Replace *192.168.1.1* with the IP address of the server node you are configuring. If everything is working properly, you should get an authentication prompt.

5c If you installed iFolder 3.*x* Web Access server, in YaST, configure Web Access. For information, see Section 6.3, "Configuring the iFolder Web Access Server," on page 55.

For the *Web Access Alias*, specify the same alias you used on Node 1 in Step 4g.

For the *iFolder Server URL*, specify SSL (by using https in the URL) and specify `localhost` as the location. For example:

```
https://localhost
```

5d Stop Apache on the node you are configuring. At a terminal console, enter

```
/etc/init.d/apache2 stop
```

5e Replace the `/opt/novell/ifolder3/etc/simias-server-bootstrap.config` file with the simias-server-bootstrap.config file from the first node you configured.

5f Delete the `.local` directory under `wwwrun`. At a terminal console, enter

```
rm -rf /var/lib/wwwrun/.local
```

Deleting the node's .local file is necessary so that the node can use the copy of the `/var/lib/wwwrun/.local` directory on the shared volume after you create a symbolic link to it in Step 5g. This also means that nodes share the `/var/lib/wwwrun/.local/share/simias/Simias.config` file on the shared volume.

5g Create a symbolic link from the shared volume's .local file to your wwwrun users home directory. At a terminal console, enter

```
ln -s /mnt/ifolder3/.local /var/lib/wwwrun/
```

Verify that the symbolic link is valid. At a terminal console, enter

```
ll /var/lib/wwwrun/
```

If the link appears blue, it is valid. If the link appears red, the link is invalid.

5h Change ownership of the .local symbolic link to user `wwwrun` and group `www`. At a server console, enter

```
chown -R wwwrun:www /var/lib/wwwrun/.local
```

5i Unmount the shared volume. At the server console, enter

```
umount /mnt/ifolder3
```

5j Modify the server settings so that Apache does not load at boot and Apache starts and stops are controlled with the cluster's load and unload scripts. At the server console, enter

```
chkconfig apache2 off
```

5k Repeat the preceding steps to configure any additional nodes in your iFolder cluster.

6 Continue with Section B.4, "Creating the iFolder 3.x Cluster Resource," on page 129.

B.4 Creating the iFolder 3.x Cluster Resource

1. In iManager Roles and Tasks, expand the *Clusters* role, then select *Cluster Options*.
2. Specify the cluster name, or browse and select the *Cluster* object.
3. Click *New*.
4. Specify Resource as the resource type you want to create by clicking the *Resource* radio button, then click *Next*.
5. Enter the name of the resource you want to create, such as `iFolder3`.

   Do not use periods in cluster resource names. Novell clients interpret periods as delimiters. If you use a space in a cluster resource name, that space is converted to an underscore.
6. Browse for the *Generic_IP_Service to Inherit From*.
7. Select *Define Additional Properties*, then click *Next*.
8. For the cluster *Load Script*, use one of the sample load scripts as a guide, then click *Next*.

   For information, see Section B.6, "Sample Load Scripts for iFolder 3.x Clusters," on page 129.
9. For the cluster *Unload Script*, use one of the sample unload scripts as a guide, then click *Next*.

   For information, see Section B.7, "Sample Unload Scripts for iFolder 3.x Clusters," on page 131.
10. Complete the remaining screens, then click *Finish*.
11. Continue with Section B.5, "Managing the iFolder 3.x Cluster Resource," on page 129.

B.5 Managing the iFolder 3.*x* Cluster Resource

In iManager Roles and Tasks, expand the *Clusters* role, then click *Cluster Manager* to manage the iFolder 3.*x* resource and bring it online.

For information, see "Managing Novell Cluster Services" (http://www.novell.com/documentation/oes/cluster_admin_lx/data/aj7bq8o.html) in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.

B.6 Sample Load Scripts for iFolder 3.*x* Clusters

- Section B.6.1, "Linux Traditional File System," on page 129
- Section B.6.2, "NSS File System," on page 130

B.6.1 Linux Traditional File System

If your shared volume uses a Linux traditional file system, use the following load script as a guide:

```
##### Linux Traditional File System Sample Load Script #####

#!/bin/bash

. /opt/novell/ncs/lib/ncsfuncs

#mount the file system

exit_on_error mnt /dev/sda1 /mnt/ifolder3
```

```
#add the IP address
##xx.xx.xx.xx is your ’highly available’ IP address
exit_on_error add_secondary_ipaddress xx.xx.xx.xx
# start the service
exit_on_error /etc/init.d/apache2 start
#return status
exit 0
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
##################################################
```

B.6.2 NSS File System

If your shared volume uses the NSS file system, use the following load script as a guide:

```
##### NSS File System Sample Load Script #########
#mount the file system
##MYPOOL is the name of your NSS pool
##MYVOL is the name of your NSS volume
nss /poolactivate=MYPOOL
exit_on_error nssmount -n MYVOL
#add the IP address
##xx.xx.xx.xx is your ’highly available’ IP address
exit_on_error add_secondary_ipaddress xx.xx.xx.xx
# start the service
exit_on_error /etc/init.d/apache2 start
#return status
exit 0
###################################################
```

B.7 Sample Unload Scripts for iFolder 3.*x* Clusters

B.7.1 Linux Traditional File System

If your shared volume uses a Linux traditional file system, use the following unload script as a guide:

```
##### Linux Traditional File System Sample Unload Script #####

#!/bin/bash

. /opt/novell/ncs/lib/ncsfuncs

#request service stop

ignore_error /etc/init.d/apache2 stop

#del the IP address

##xx.xx.xx.xx is your 'highly available' IP address

ignore_error del_secondary_ipaddress xx.xx.xx.xx

#umount the file system

exit_on_error umount /mnt/ifolder3

#return status

exit 0

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

B.7.2 NSS File System

If your shared volume uses the NSS file system, use the following unload script as a guide:

```
##### NSS File System Sample Unload Script ####################

#!/bin/bash

. /opt/novell/ncs/lib/ncsfuncs

#request service stop

ignore_error /etc/init.d/apache2 stop

#del the IP address

##xx.xx.xx.xx is your 'highly available' IP address

ignore_error del_secondary_ipaddress xx.xx.xx.xx

#umount the file system
```

```
##MYPOOL is the name of your NSS pool

##MYVOL is the name of your NSS volume

umount /media/nss/MYVOL

nss /pooldeactivate=MYVOL

#return status

exit 0

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

Managing SSL Certificates for Apache

C

This section discusses how to acquire and manage SSL certificates for your Novell® iFolder® 3.*x* servers.

- Section C.1, "Getting an SSL Certificate from a Trusted Certificate Authority," on page 133
- Section C.2, "Generating a Self-Signed SSL Certificate for Testing Purposes," on page 134
- Section C.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 135
- Section C.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 135

C.1 Getting an SSL Certificate from a Trusted Certificate Authority

Using SSL requires that you install an SSL certificate from a trusted Certificate Authority (CA) on each iFolder enterprise server and Web Access server in your domain. Users accept the certificates to enable communications with the servers.

The trusted CA signature on the certificate attests that the public key contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate. It assures users that they are accessing a valid, non-spoofed resource. If the information does not match or the certificate has expired, an error message warns the user.

Browsers are typically preconfigured to trust well-known certificate authorities. If you use a Certificate Authority that is not configured into browsers by default, it is necessary to load the Certificate Authority certificate into the browser, enabling the browser to validate server certificates signed by that Certificate Authority.

To acquire SSL certificates for use in an operational public-key infrastructure (PKI), use one or more of the following methods, depending on your network needs:

- Use Novell Certificate Server™, which is bundled with Novell Open Enterprise Server. Novell Certificate Server provides public key cryptography services that are natively integrated into Novell eDirectory™ to allow you to mint, issue, and manage both user and server certificates. Creating your own Certificate Authority might be useful within an intranet where the organization can easily verify the identities of servers and individuals.

  For information, see the *Novell Certificate Server 2.7.x Administration Guide* (http://www.novell.com/documentation/crt27/crtadmin/data/a2ebomw.html).
- Use the services of a third-party certificate authority.

For information about configuring Apache to point to the certificate, see the following:

- Section C.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 135

- Section C.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 135

C.2 Generating a Self-Signed SSL Certificate for Testing Purposes

If desired, create a self-signed SSL certificate to test your configuration, using OpenSSL. Because the certificate is not from a trusted certificate authority, users receive a warning when connecting to the server that the originator of the certificate cannot be verified. However, the traffic between the server and the client is encrypted at the same level of security that an official certificate generates.

WARNING: The self-signed certificate works correctly for testing purposes but should not be used in an operational deployment, especially when connections cross public communications networks such as the Internet.

1 Make sure you have a valid DNS name registered to a valid IP address on your network.

For a cluster solution, this should be the highly available DNS name and IP address of the cluster.

2 Create a private key (`.key` file). At a terminal console, enter

```
openssl genrsa -out filename.key 1024
```

Replace *filename* with the name you want to use for the key.

3 Create a certificate-signing request (`.csr` file), using the private key (`filename.key`) you created in Step 2.

3a At a terminal console, enter

```
openssl req -new -key filename.key -out filename.csr
```

3b When prompted, enter the following information:

- Locality
- Common name (domain name)

  iFolder 3.*x* requires accurate information for the common name of your Apache 2 server. For example, if you enter ifolder3.example.com, this common name should be a valid DNS name that is registered to a valid IP address on your network.
- Organization
- Other information

4 Generate the self-signed certificate (`.cert` file), using the private key (*filename*.key) you created in Step 2 and the certificate-signing request (*filename*.csr) you created in Step 3. At a terminal console, enter

```
openssl x509 -req -days 30 -in filename.csr -signkey filename.key
-out filename.cert
```

For information about configuring Apache to point to the self-signed certificate, see the following:

- Section C.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 135
- Section C.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 135

C.3 Configuring Apache to Point to an SSL Certificate on an iFolder Server

1 Get an SSL certificate from a trusted certificate authority.

2 Mount the volume where you manage certificates: At a terminal console, enter

```
mnt /dev/sda1 /mnt/ifolder3
```

Replace `/dev/sda1` with the actual disk or partition containing the file system. Replace `/mnt/ifolder3` with the mount point (directory path) where you are managing certificates.

3 Copy the private key (`.key` file) and the certificate (`.cert` file) to a location on the mounted volume. At a terminal console, enter

```
cp ./filename.key /mnt/ifolder3/key/
```

```
cp ./filename.cert /mnt/ifolder3/key/
```

Replace `filename` with the actual file name of your `.key` and `.cert` files. Replace the destination path with the location on the mounted volume where you want to store the `.key` and `.cert` files.

4 For each node in the cluster, edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.key` file and `.cert` file on the volume by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/mnt/ifolder3/key/filename.key
```

```
SSLCertificateFile=/mnt/ifolder3/key/filename.cert
```

Replace the path to the files with the actual location and filenames.

C.4 Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster

1 Mount the shared volume. At a terminal console, enter

```
mnt /dev/sda1 /mnt/ifolder3
```

Replace `/dev/sda1` with the actual disk or partition containing the file system. Replace `/mnt/ifolder3` with the mount point (directory path) of the shared volume.

2 Copy the private key (`.key` file) and the certificate (`.cert` file) to a location on the mounted shared volume. At a terminal console, enter

```
cp ./filename.key /mnt/ifolder3/sharedkey/
```

```
cp ./filename.cert /mnt/ifolder3/sharedkey/
```

Replace `filename` with the actual file name of your `.key` and `.cert` files. Replace the destination path with the location where you want to store the shared key and certificate files.

3 Edit the Apache SSL configuration file (`/etc/apache2/vhosts.d/vhost-ssl.conf`) to point to the `.key` file and `.cert` file on the shared volume by modifying the values for the following parameters:

```
SSLCertificateKeyFile=/mnt/ifolder3/sharedkey/filename.key
```

```
SSLCertificateFile=/mnt/ifolder3/sharedkey/filename.cert
```

Replace the path to the files with the actual location and filename on the shared volume.

4 Unmount the shared volume. At a terminal console, enter

```
umount /mnt/ifolder3
```

Product History of iFolder 3.*x*

D

This section compares the different versions of Novell® iFolder® 3.*x* to clarify which operating systems, directories, and other components are supported in each.

- Section D.1, "Version History," on page 137
- Section D.2, "Network Operating Systems Support," on page 137
- Section D.3, "Directory Services Support," on page 138
- Section D.4, "Workstation Operating Systems Support for the iFolder Client," on page 138
- Section D.5, "Web Server Support," on page 138
- Section D.6, "iFolder User Access Support," on page 138
- Section D.7, "Management Tools Support," on page 139

For a comparison of features in 2.1*x* and 3.*x*, see "What's New" on page 21.

D.1 Version History

Version	Type	Description
3.0	Bundled	A new code-base in this next-generation version supports multiple iFolders and member-based sharing. For information, see Section 2.3, "What's New in Novell iFolder 3.0 (OES Linux)," on page 21. Server is supported for Novell Open Enterprise Server on Linux servers. The client supports Linux, Windows, and Macintosh desktops.
3.1	Bundled	Adds support for OES SP1 Linux servers and repairs known defects. For information, see Section 2.2, "What's New in Novell iFolder 3.1 (OES SP1 Linux)," on page 21.
3.2	Bundled	Adds support for OES SP2 Linux servers and repairs known defects. For information, see Section 2.1, "What's New in Novell iFolder 3.2 (OES SP2 Linux)," on page 21.

D.2 Network Operating Systems Support

Network Operating System	3.0	3.1	3.2
OES Linux	Yes	Yes, but it does not support NSS volumes because of a kernel defect. Requires a Mono® update.	Yes, but it does not support NSS volumes because of a kernel defect. Requires a Mono update.

Network Operating System	3.0	3.1	3.2
OES SP1 Linux	No	Yes	Yes Requires a Mono update.
OES SP2 Linux	No	No	Yes

D.3 Directory Services Support

LDAP Directory Service	3.0	3.1	3.2
Novell eDirectory™	8.7.3	8.7.3	8.7.3

D.4 Workstation Operating Systems Support for the iFolder Client

Workstation Operating System	3.0	3.1	3.2
Novell Linux Desktop	v9	v9	v9 and later
Windows 2000/XP/2003	Yes	Yes	Yes
Macintosh OS X v10.3 and later	Yes	Yes	Yes

D.5 Web Server Support

Web Server	3.0	3.1	3.2
Apache	2 (worker mode)	2 (worker mode)	2 (worker mode)

D.6 iFolder User Access Support

iFolder User Access Method	3.0	3.1	3.2
iFolder client	Yes	Yes	Yes
iFolder client, using a proxy	No	Yes	Yes

iFolder User Access Method	3.0	3.1	3.2
Novell iFolder 3.x Web Access	IE 6.0 Firefox Safari (Macintosh)	IE 6.0 Firefox Safari (Macintosh)	IE 6.0 Firefox Safari (Macintosh)

D.7 Management Tools Support

iFolder Management Interfaces	3.0	3.1	3.2
iFolder 3 plug-in to iManager 2.5	Yes	Yes	Yes
iFolder 3 plug-in to YaST	Yes	Yes	Yes
iFolder 3 Web Access plug-in to YaST	Yes	Yes	Yes
RPM packages available in the OES install	No	Yes	Yes
Simias Log	Yes	Yes	Yes
Simias Access Log	No	Yes	Yes

Documentation Updates

E

This section contains information about documentation content changes made to the *Novell iFolder 3.x Administration Guide* since the initial release of Novell® iFolder 3.0 for OES Linux. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the front cover and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *Novell iFolder 3.x Administration Guide*, see the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/ifolder3).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

- Section E.1, "December 23, 2005 (Novell iFolder 3.2 for OES SP2 Linux)," on page 141
- Section E.2, "August 19, 2005 (Novell iFolder 3.1 for OES SP1 Linux)," on page 143

E.1 December 23, 2005 (Novell iFolder 3.2 for OES SP2 Linux)

Minor changes were made throughout for clarification. Updates were made to the following sections. The changes are explained below.

- Section E.1.1, "What's New," on page 141
- Section E.1.2, "Planning iFolder Services," on page 142
- Section E.1.3, "Installing and Configuring iFolder Services," on page 142
- Section E.1.4, "Managing iFolder Services," on page 142
- Section E.1.5, "Managing iFolder Users," on page 143
- Section E.1.6, "Managing iFolders," on page 143
- Section E.1.7, "Product History of iFolder 3.x," on page 143

E.1.1 What's New

The following change was made to this section:

Location	Change
What's New in Novell iFolder 3.2 (OES SP2 Linux)	This section is new.

E.1.2 Planning iFolder Services

The following change was made to this section:

Location	Change
Naming Conventions for Usernames and Passwords	The following configuration option is new. **E-Mail Address Naming Requirement:** If you configure iFolder to authenticate using the user's e-mail address as the user name for login, make sure the e-mail address conforms to standard e-mail naming conventions. For example, `john.smith@example.com` or `js1234@email.example.com`.

E.1.3 Installing and Configuring iFolder Services

The following changes were made to this section:

Location	Change
Installing iFolder 3.0	This section was removed. It is obsoleted by more recent releases.
Installing iFolder on an Existing OES Linux Server	This procedure has been updated to include instructions for restarting Apache and Tomcat.
Configuring the iFolder Enterprise Server	The following configuration option is new. **iFolder User Login Based on Which LDAP Attribute:** Specify which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Options are Common Name (cn, default) and e-mail address (mail). This setting cannot be changed after the install. For example, if a user named John Smith has a common name of jsmith and e-mail of `john.smith@example.com`, this field determines whether the user enters `jsmith` or `john.smith@example.com` as the Username when logging in to the iFolder server.

E.1.4 Managing iFolder Services

The following changes were made to this section:

Location	Change
Configuring the LDAP Settings for an iFolder Server	Information was modified for the LDAP Synchronization Interval.
Configuring System Policies	Information was added for the system-wide Minimum Synchronization Interval policy for synchronizing data.

E.1.5 Managing iFolder Users

The following change was made to this section:

Location	Change
Configuring System Policies	Information was added for the user's Minimum Synchronization Interval policy for synchronizing data.

E.1.6 Managing iFolders

The following change was made to this section:

Location	Change
Configuring Policies for an iFolder	Information was added for the iFolder's Minimum Synchronization Interval policy for synchronizing data.

E.1.7 Product History of iFolder 3.*x*

Changes were made in all sections to add information for iFolder 3.2 for OES SP2 Linux. In addition, the following change was made to this section:

Location	Change
Management Tools Support	This section is new.

E.2 August 19, 2005 (Novell iFolder 3.1 for OES SP1 Linux)

Updates were made to the following sections. The changes are explained below.

E.2.1 What's New

The following changes were made to this section:

Location	Change
What's New in Novell iFolder 3.1 (OES SP1 Linux)	This section is new.
What's New in Novell iFolder 3.0 (OES Linux)	This section was retitled.

E.2.2 Coexistence and Migration Issues for Novell iFolder 3.*x*

The following change was made to this section:

Location	Change
Coexistence of iFolder 3.x and 2.1x Servers	This section is new.

E.2.3 Planning iFolder Services

The following change was made to this section:

Location	Change
Security Considerations	This section is was moved to the *Novell iFolder 3.x Security Administrator Guide*.

E.2.4 Prerequisites and Guidelines

The following changes were made to this section:

Location	Change
Enterprise Server	Requirements were adjusted for OES SP1 Linux to use the Minimal install pattern.
File System	For OES SP1, iFolder supports storing iFolder data on NSS volumes on Linux.
Mono	The version of Mono® was updated for OES SP1.
Web Browser	Safari for Macintosh was added to the supported browsers list.

E.2.5 Installing and Configuring iFolder Services

The following change was made to this section:

Location	Change
Installing iFolder on an Existing OES Linux Server	This section is new.

E.2.6 Managing an iFolder Enterprise Server

The following change was made to this section:

Location	Change
Backing Up the iFolder Store with the TSAIF	This section is new.

E.2.7 Managing iFolder Services

The following change was made to this section:

Location	Change
Securing Access to the iFolder Proxy User Password	This section is new.
Multiple locations	Edits were made for clarity.

E.2.8 Clustering iFolder 3.*x* with Novell Cluster Services for Linux

This section is new.

E.2.9 Managing SSL Certificates for Apache

This section is new.

E.2.10 Product History of iFolder 3.*x*

This section is new.