AUTHORIZED DOCUMENTATION

Administration Guide

Novell® iFolder®

3.6

October 2009

www.novell.com

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 Novell International Trade Services Web Page (http://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.

THIS DOCUMENT AND MODIFIED VERSIONS OF THIS DOCUMENT ARE PROVIDED UNDER THE TERMS OF THE GNU FREE DOCUMENTATION LICENSE WITH THE FURTHER UNDERSTANDING THAT:

1. THE DOCUMENT IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE, OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY, ACCURACY, AND PERFORMANCE OF THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS WITH YOU. SHOULD ANY DOCUMENT OR MODIFIED VERSION PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL WRITER, AUTHOR OR ANY CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER; AND

2. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE AUTHOR, INITIAL WRITER, ANY CONTRIBUTOR, OR ANY DISTRIBUTOR OF THE DOCUMENT OR MODIFIED VERSION OF THE DOCUMENT, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER DAMAGES OR LOSSES ARISING OUT OF OR RELATING TO USE OF THE DOCUMENT AND MODIFIED VERSIONS OF THE DOCUMENT, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

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 on Novell Legal Patents Web Page (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 The Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For a list of Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html)

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide 11

1 Overview of Novell iFolder 3.6 13

1.1 Benefits of iFolder for the Enterprise . . . 13
1.1.1 Seamless Data Access . . . 13
1.1.2 Data Safeguards and Data Recovery . . . 14
1.1.3 Reliable Data Security . . . 14
1.1.4 Encryption Support . . . 15
1.1.5 Productive Mobile Users . . . 15
1.1.6 Cross-Platform Client Support . . . 15
1.1.7 Scalable Deployment . . . 15
1.1.8 Multi Server Support . . . 16
1.1.9 Multi Volume Support . . . 16
1.1.10 Enhanced Web Administration . . . 16
1.1.11 No Training Requirements . . . 16
1.2 Benefits of iFolder for Users . . . 16
1.3 Enterprise Server Sharing . . . 18
1.4 Key Features of iFolder . . . 18
1.4.1 iFolder Enterprise Server . . . 18
1.4.2 Novell iFolder 3.6 Web Admin Console . . . 19
1.4.3 iFolder Web Access Console . . . 19
1.4.4 The iFolder Client . . . 19
1.4.5 Multi Server Support . . . 19
1.4.6 Encryption . . . 19
1.4.7 Shared iFolders . . . 19
1.4.8 iFolder Access Rights . . . 20
1.4.9 Account Setup for Enterprise Servers . . . 20
1.4.10 Access Authentication . . . 20
1.4.11 File Synchronization and Data Management . . . 21
1.4.12 Synchronization Log . . . 21
1.4.13 iFolder Client APIs . . . 21
1.5 What's Next . . . 21

2 What's New 23

2.1 What's New in Novell iFolder 3.6 (OES 2.0 Linux) . . . 23
2.2 What's New in Novell iFolder 3.2 (OES SP2 Linux) . . . 23
2.3 What's New in Novell iFolder 3.1 (OES SP1 Linux) . . . 24
2.4 What's New in Novell iFolder 3.0 (OES Linux) . . . 24
2.5 Comparison of 2.*x* and 3.6 Server Features and Capabilities . . . 25
2.6 Comparison of 2.*x* and 3.6 Client Features and Capabilities . . . 27
2.7 Comparison of 2.*x* and 3.6 Web Access Features and Capabilities . . . 31

3 Novell iFolder Upgrade, Migration, and Coexistence 33

3.1 Upgrading iFolder 2.*x* to iFolder 3.6 . . . 33
3.1.1 In-place Upgrade . . . 33
3.1.2 Parallel Upgrade . . . 33
3.1.3 Client Upgrade . . . 34
3.2 Upgrading iFolder 3.*x* to iFolder 3.6 . . . 34

3.2.1 In-place Upgrade . . . 34
3.2.2 Parallel Upgrade . . . 34
3.2.3 Client Upgrade . . . 35
3.3 Migration From iFolder 2.*x* to iFolder 3.6 . . . 36
3.3.1 Planning . . . 36
3.3.2 User Data Migration . . . 37
3.3.3 User Identity And Configuration Migration . . . 37
3.4 Coexistence of iFolder 3.6 and 2.*x* Servers . . . 37
3.5 Coexistence of the iFolder 3.6 Client with Novell iFolder 1.*x* and 2.*x* Clients . . . 37

4 Planning iFolder Services 39

4.1 Security Considerations . . . 39
4.2 Server Workload Considerations . . . 39
4.3 Naming Conventions for Usernames and Passwords . . . 40
4.4 Admin User Considerations . . . 41
4.5 iFolder User Account Considerations . . . 42
4.5.1 Preventing the Propagation of Viruses . . . 42
4.5.2 Provisioning User Accounts . . . 42
4.5.3 Setting Account Quotas . . . 43
4.6 iFolders Data and Synchronization Considerations . . . 43
4.6.1 Naming Conventions for an iFolder and Its Folders and Files . . . 43
4.6.2 Guidelines for File Types and Sizes to Be Synchronized . . . 44
4.7 Management Tools . . . 45
4.7.1 iFolder Configuration Plug-Ins for YaST . . . 45
4.7.2 Novell iFolder Web Admin for Novell iManager 2.7 . . . 46
4.7.3 Web Access Configuration File . . . 46

5 Running Novell iFolder in a Virtualized Environment 47

5.1 What's Next . . . 47

6 Prerequisites and Guidelines 49

6.1 File System . . . 49
6.2 Enterprise Server . . . 49
6.2.1 Prerequisites for the Operating System . . . 50
6.2.2 Install Guidelines When Using an NSS Volume to Store iFolder Data . . . 50
6.2.3 Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data . . . 51
6.2.4 Install Guidelines for Other Components . . . 51
6.2.5 Installing the OES 2.0 Linux Server . . . 52
6.3 Novell eDirectory 8.8 . . . 52
6.4 Novell iManager 2.7 . . . 52
6.5 Mono 1.2.2 . . . 52
6.6 Client Computers . . . 53
6.7 Web Browser . . . 53

7 Installing and Configuring iFolder Services 55

7.1 Installing iFolder on an Existing OES 2 Linux Server . . . 55
7.2 Deploying iFolder Server in a Multi-server Environment . . . 58
7.2.1 Configuring the iFolder Enterprise Server . . . 59
7.2.2 Configuring the iFolder Slave Server . . . 66
7.2.3 Loading Recovery Agent Certificates in The iFolder Server . . . 73
7.3 Configuring the iFolder Web Access Server . . . 73

7.3.1 Configuring iFolder Web Access for iChain or AccessGateway 74
7.4 Configuring the iFolder Web Admin Server 75
7.4.1 Configuring iFolder Web Admin for iChain or AccessGateway 76
7.5 Installing the Novell iFolder 3 Plug-In for iManager 77
7.5.1 Prerequisites 77
7.5.2 Installing a Plug-In When RBS Is Not Configured 78
7.5.3 Installing a Plug-In When RBS Is Configured 78
7.6 Recovery Agent Certificates 79
7.6.1 Understanding Digital Certification 80
7.6.2 Creating a YaST-based CA 81
7.6.3 Creating Self-Signed Recovery Certificates Using YaST 83
7.6.4 Exporting Self-Signed Certificates 85
7.6.5 Exporting Self-Signed Private Key Certificates For Key Recovery 86
7.6.6 Using KeyRecovery to Recover the Data 86
7.7 Accessing iManager and the Novell iFolder Web Admin 87
7.8 Provisioning Users and iFolder Services 89
7.8.1 Prerequisites 89
7.9 Distributing the iFolder Client to Users 89
7.9.1 Accessing the OES 2 Linux Welcome Page 90
7.9.2 Downloading the iFolder Client 90
7.9.3 Installing the iFolder Client 91
7.10 Updating Novell iFolder 3.6 91
7.11 Updating Mono for the Server and Client 91
7.12 Uninstalling the iFolder 3.6 Enterprise Server 91
7.13 What's Next 91

8 Managing an iFolder Enterprise Server 93

8.1 Starting iFolder Services 93
8.2 Stopping iFolder Services 93
8.3 Restarting iFolder Services 93
8.4 Managing the Simias Log and Simias Access Log 94
8.5 Backing Up the iFolder Server 95
8.6 Backing Up the iFolder Store with the TSAIF 96
8.6.1 Understanding TSAIF 96
8.6.2 Syntax 97
8.6.3 iFolder Path Options 97
8.6.4 iFolder Path Examples 99
8.6.5 SMSConfig Options 99
8.6.6 TSAIF and SMSConfig Examples 100
8.6.7 NBackup Options 100
8.6.8 TSAIF and NBackup Examples 101
8.6.9 Additional Information 102
8.7 Recovering from a Catastrophic Loss of the iFolder Server 102
8.8 Recovering Individual Files or Directories 103
8.9 Moving iFolder Data from One iFolder Server to Another 104
8.10 Changing The IP Address For iFolder Services 105
8.11 Securing Enterprise Server Communications 106
8.11.1 Using SSL for Secure Communications 106
8.11.2 Configuring the SSL Cipher Suites for the Apache Server 106
8.11.3 Configuring the Enterprise Server for SSL Communications with the LDAP Server 107
8.11.4 Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server 108
8.11.5 Configuring an SSL Certificate for the Enterprise Server 108

9 Managing iFolder Services via Web Admin 109

9.1 Accessing the Novell iFolder Web Admin . . . 109
9.2 Connecting to the iFolder Server . . . 110
9.3 Accessing iFolder Web Admin Via OES Welcome Page . . . 111
9.4 Managing Web Admin Console . . . 112
9.5 Managing the iFolder System . . . 113
9.5.1 Viewing and Modifying iFolder System Information . . . 113
9.5.2 Configuring iFolder Administrators . . . 114
9.5.3 Configuring System Policies . . . 115
9.6 Managing iFolder Server For a Multi-Server Setup . . . 118
9.6.1 Searching For Servers . . . 118

10 Managing iFolder Users 123

10.1 Provisioning Users for iFolder Services . . . 123
10.2 Searching for a User Account . . . 123
10.3 Accessing And Viewing General User Account Information . . . 124
10.3.1 Enabling or Disabling an iFolder For an User Account . . . 124
10.3.2 Deleting An iFolder . . . 125
10.4 Creating an iFolder . . . 125
10.5 Configuring User Account Policies . . . 125
10.5.1 Viewing the Current User Account Policies . . . 125
10.5.2 Modifying User Account Policies . . . 127
10.6 Enabling and Disabling iFolder User Accounts . . . 129

11 Managing iFolders 131

11.1 Creating an iFolder for a User's Account . . . 131
11.1.1 Creating an iFolder from the iFolders Page . . . 131
11.1.2 Creating an iFolder from the Users Page . . . 132
11.2 Viewing Details And Configuring Policies for An iFolder . . . 132
11.2.1 Accessing the iFolders Details Page . . . 132
11.2.2 Viewing The iFolder Details . . . 132
11.2.3 Searching for an iFolder . . . 133
11.2.4 Managing iFolder Members . . . 134
11.2.5 Managing an iFolder . . . 134
11.2.6 Managing iFolder Policies . . . 136
11.2.7 Enabling, Disabling and Deleting an iFolder . . . 138

12 Managing an iFolder Web Access Server 139

12.1 Starting iFolder Web Access Services . . . 139
12.2 Stopping iFolder Web Access Services . . . 139
12.3 Distributing the Web Access Server URL to Users . . . 139
12.4 Configuring the HTTP Runtime Parameters . . . 139
12.5 Securing Web Access Server Communications . . . 141
12.5.1 Using SSL for Secure Communications . . . 141
12.5.2 Configuring the SSL Cipher Suites for the Apache Server . . . 141
12.5.3 Configuring the Web Access Server for SSL Communications with the Enterprise Server . . . 142
12.5.4 Configuring the Web Access Server for SSL Communications with Web Browsers 143
12.5.5 Configuring an SSL Certificate for the Web Access Server . . . 143

A Configuration Files **145**

A.1 Simias.config File . . . 145
A.2 Web.config File for the Enterprise Server . . . 146
A.3 Web.config File for the Web Access Server . . . 148

B Managing SSL Certificates for Apache **153**

B.1 Generating an SSL Certificate for the Server . . . 153
B.2 Generating a Self-Signed SSL Certificate for Testing Purposes . . . 154
B.3 Configuring Apache to Point to an SSL Certificate on an iFolder Server . . . 155
B.4 Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster . . . 155

C Clustering iFolder 3.6 Servers with Novell Cluster Services for Linux **157**

C.1 Prerequisites for Clustering iFolder 3.6 Services . . . 157
C.2 Installing Novell Cluster Services for Linux . . . 157
C.3 Configuring iFolder 3.6 Servers on an NCS for Linux Cluster . . . 158
C.4 Creating the iFolder 3.6 Cluster Resource . . . 160
C.5 Managing the iFolder 3.6 Cluster Resource . . . 160
C.6 Sample Load Scripts for iFolder 3.6 Clusters . . . 160
C.6.1 Linux Traditional File System . . . 160
C.6.2 NSS File System . . . 161
C.7 Sample Unload Scripts for iFolder 3.6 Clusters . . . 161
C.7.1 Linux Traditional File System . . . 162
C.7.2 NSS File System . . . 162
C.7.3 Troubleshooting . . . 163

D Troubleshooting Tips For Novell iFolder 3.6 **165**

D.1 iFolder User Account Creation Delays with Timeout Error . . . 165
D.2 Web Admin Console Fails to Start Up . . . 166
D.3 Exception Error while Configuring iFolder on a Samba Volume . . . 166
D.4 Samba Connection to the Remote Windows Host Times out . . . 166
D.5 LDAP Users Are Not Reflected in iFolder . . . 166
D.6 Changing Permission to the Full Path Fails . . . 167
D.7 iManager Single Sign-on Fails . . . 167
D.8 List of Items Fail to Synchronize . . . 167
D.9 Access Permission Error While Logging in Through Web Access . . . 167
D.10 iFolder Upgrade From OES 1 SP2 to OES 2 Fails . . . 167
D.11 Web Admin and Web Access Show Blank Page . . . 168

E Frequently Asked Questions **169**

E.1 iFolder 3.6 Server . . . 169
E.1.1 Is iFolder 3.6 supported on a 64-bit OS? . . . 169
E.1.2 Is iFolder going to support non-eDirectory related platforms as an identity source? 169
E.1.3 Because iFolder is developed on Mono, can it be deployed in a Microstoft environment? . . . 169
E.2 iFolder 3.6 Client . . . 170
E.2.1 Is iFolder 3.6 supported on Windows Vista? . . . 170
E.2.2 Is iFolder 3.6 supported on the Macintosh platform? . . . 170
E.2.3 Can I use the iFolder 2.*x* client to connect to an iFolder 3.6 server? . . . 170

E.2.4 Can I use the iFolder 3.*x* client to connect to the iFolder 3.6 server? 170
E.2.5 Can I can use iFolder 3.6 on different operating systems on different workstations to access and share the files? 171
E.2.6 There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.6? 171
E.2.7 I deleted a file accidentally? Can I recover it? 171
E.2.8 What are the migration scenarios recommended and supported by iFolder 3.6? . . 171
E.3 iFolder 3.6 Administration 171
E.3.1 What is the management console for iFolder 3.6? 171
E.3.2 What are the new features in the Web Admin console? 172
E.3.3 Can the administrator control the ability to encrypt iFolder files? 172
E.3.4 Are there any enhancements for how bulk users are enabled for iFolder? 172
E.3.5 Can the administrator control the ability to share files? 172
E.3.6 How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain? 172

F Caveats for Implementing iFolder 3.6 Services 173

F.1 Loading Certificates to the Recovery Agent Path 173
F.2 Using Novell iFolder Server to Serve Large Files 173
F.3 Deployment in an Active Directory Environment 174
F.4 Using a Single Proxy User for a Multi-Server Setup 174
F.5 Slave Configuration 174
F.6 LDAP SSL Certificate 174
F.7 Novell iFolder Admin User 174
F.8 Novell iFolder with iChain and the Access Gateway 174

G Product History of iFolder 3 177

G.1 Version History 177
G.2 Network Operating Systems Support 178
G.3 Directory Services Support 178
G.4 Workstation Operating Systems Support for the iFolder Client 178
G.5 Web Server Support 179
G.6 iFolder User Access Support 179
G.7 Management Tools Support 179

About This Guide

This guide describes how to install, configure, and manage the Novell® iFolder® 3.6 enterprise server, the iFolder 3.6 Web Access server, the iFolder 3.6 Web Admin server, and the iFolder™ Client. This guide is divided into the following sections:

- Chapter 1, "Overview of Novell iFolder 3.6," on page 13
- Chapter 2, "What's New," on page 23
- Chapter 4, "Planning iFolder Services," on page 39
- Chapter 3, "Novell iFolder Upgrade, Migration, and Coexistence," on page 33
- Chapter 6, "Prerequisites and Guidelines," on page 49
- Chapter 7, "Installing and Configuring iFolder Services," on page 55
- Chapter 8, "Managing an iFolder Enterprise Server," on page 93
- Chapter 9, "Managing iFolder Services via Web Admin," on page 109
- Chapter 12, "Managing an iFolder Web Access Server," on page 139
- Chapter 10, "Managing iFolder Users," on page 123
- Appendix A, "Configuration Files," on page 145
- Appendix C, "Clustering iFolder 3.6 Servers with Novell Cluster Services for Linux," on page 157
- Appendix B, "Managing SSL Certificates for Apache," on page 153
- Appendix G, "Product History of iFolder 3," on page 177

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 3.6 Administration Guide*, visit the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/beta/ifolder3/index.html).

For emerging issues with Novell iFolder 3.6 and the iFolder client, see the *Novell iFolder 3.6 Readme* (http://www.novell.com/documentation/beta/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 3.6* (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™ 8.8 documentation (http://www.novell.com/documentation/edir873/treetitl.html)
- Novell iManager 2.7 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 3.6

1

Novell® iFolder® 3.6 is the next generation of iFolder, supporting multiple iFolders per user, user-controlled sharing, and a centralized network server for secured file storage and 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 16
- Section 1.3, "Enterprise Server Sharing," on page 18
- Section 1.4, "Key Features of iFolder," on page 18
- Section 1.5, "What's Next," on page 21

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
- "Encryption Support" on page 15
- "Productive Mobile Users" on page 15
- "Cross-Platform Client Support" on page 15
- "Scalable Deployment" on page 15
- "Multi Server Support" on page 16
- "Multi Volume Support" on page 16
- "Enhanced Web Administration" on page 16
- "No Training Requirements" on page 16

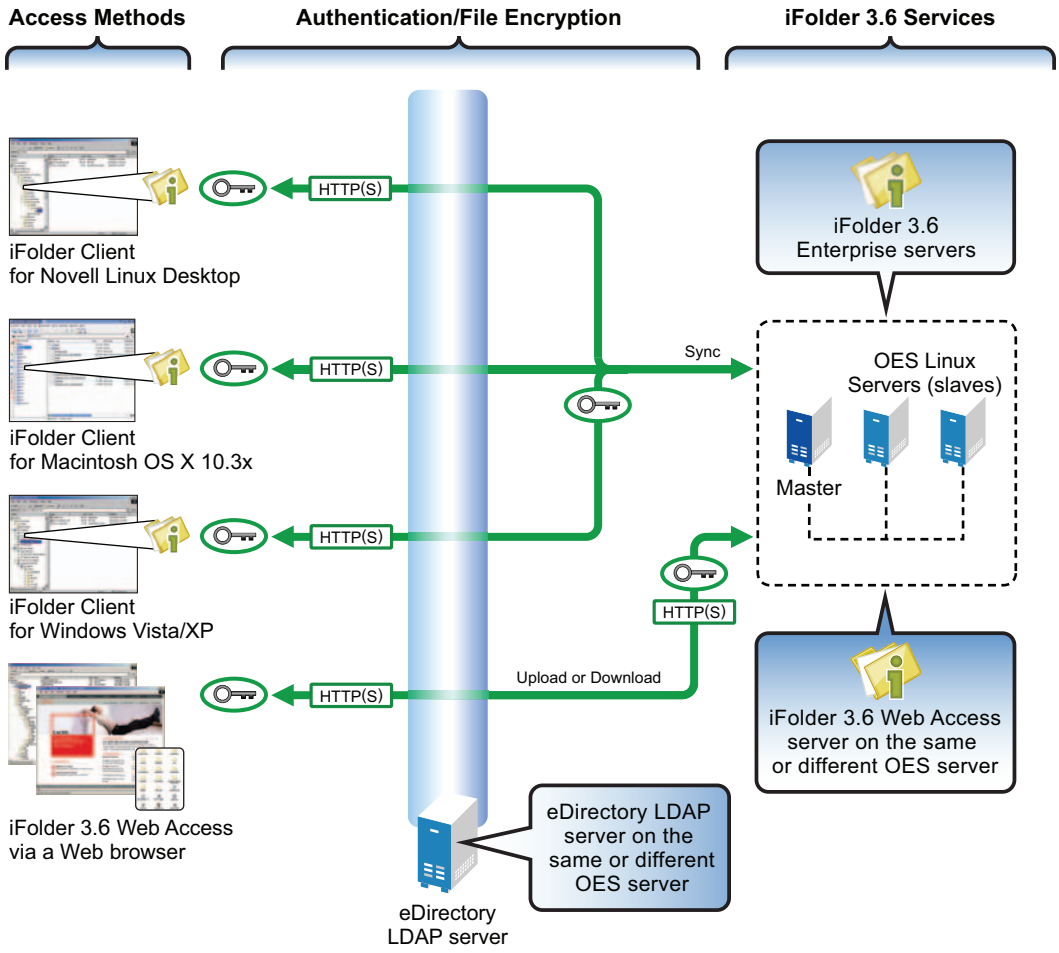
1.1.1 Seamless Data Access

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 3.6 Access Methods*



NOTE: Currently, iFolder 3.6 does not support Macintosh and Vista.

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 Encryption Support

In a corporate environment, Enterprise level data is generally accessible to it's IT department which in turn can lead to intentional or unintentional access by unauthorized personnel. In the past, executives fearing this unauthorized access to sensitive data have been hesitant to store some confidential documents on the network.

With encryption support, iFolder 3.6 ensure higher security for users' confidential documents by encrypting it at the client side before transferring it to the server. Data is thus stored encrypted on the server which can be retrievable only by the user who created that iFolder.

iFolder makes it easier for IT managers to ensure that all of an organization's critical data is protected on the iFolder servers without involving any significant risks. iFolder also gives Internet Service Providers (ISPs) the ability to offer a user-trusted backup solution for their customers' critical business or personal data.

1.1.5 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 laptop 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.

1.1.6 Cross-Platform Client Support

The iFolder client is available for Linux, and Windows* desktops. The Novell iFolder 3.6 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.

1.1.7 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 unlimited 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.

1.1.8 Multi Server Support

Handling enormous data and provisioning immense number of Enterprise users in a corporate environment is an herculean task for any administrator. iFolder 3.6 simplify these tasks with Multi-server configuration. Multi-server support is designed exclusively for meeting your enterprise requirements. It serves the purpose of provisioning higher number of users and hosting large amount of data on your iFolder domain. You can scale up the domain across servers to the needs of enterprise level user requirements by adding multiple servers to a single domain. This will allow you to leverage under-utilized servers in an iFolder domain. With multi-server deployment, thus, Enterprise level provisioning can be effectively managed and Enterprise level data can be scaled up.

1.1.9 Multi Volume Support

One of the key features of iFolder is it's storage scalability. With multi volume support, Internet Service Providers and Enterprise Data centers can manage huge amount of data beyond the file system restriction per volume. This facilitates to move data across the volumes based on file size and storage space availability.

1.1.10 Enhanced Web Administration

Management of all iFolder enterprise servers is centralized through the enhanced iFolder Web Admin Console. Administrators can perform server management and maintenance activities 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.

1.1.11 No Training Requirements

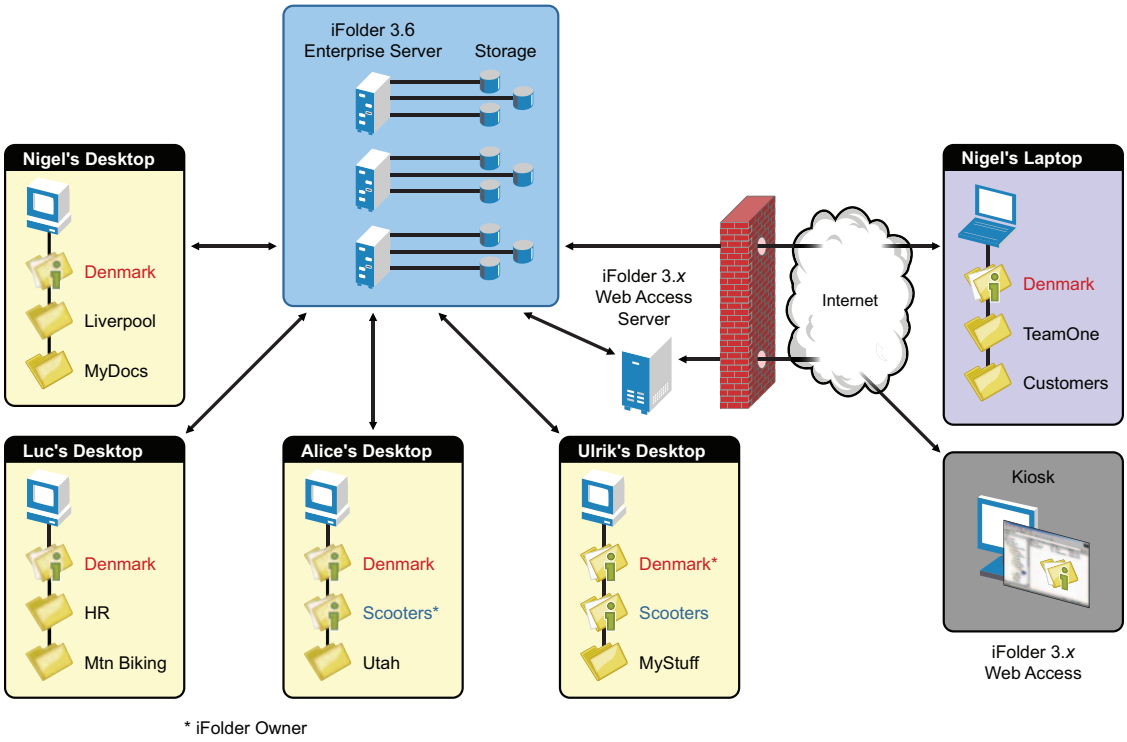
IT personnel no longer need to condition or train users to perform special tasks to ensure the consistency of data stored locally and on the network. With Novell iFolder, users simply store their files in the local iFolder directory. Their files are automatically updated to the iFolder server and any 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
- Prevent unauthorized network access to sensitive iFolder files.
- Allow multiple servers to participate in a single iFolder domain so as to allow scale up the number of users and data transfer bandwidth.
- 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.

1.3 Enterprise Server Sharing

The iFolder client included in this release supports synchronization across multiple computers through a central Novell iFolder 3.6 enterprise server.

- Users can share files across computers.
- Users can share files with others.
- Each user can own multiple iFolders.
- User can be assigned to set encryption policy for their individual iFolder files.
- 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 encrypted over the wire.
- Users are autoprovisioned for iFolder services based on their assignment to administrator-specified LDAP containers and groups. If there are multiple servers participating in a single domain, it's users are balanced across the servers.
- 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 Web Admin.

1.4 Key Features of iFolder

- Section 1.4.1, "iFolder Enterprise Server," on page 18
- Section 1.4.2, "Novell iFolder 3.6 Web Admin Console," on page 19
- Section 1.4.3, "iFolder Web Access Console," on page 19
- Section 1.4.4, "The iFolder Client," on page 19
- Section 1.4.5, "Multi Server Support," on page 19
- Section 1.4.6, "Encryption," on page 19
- Section 1.4.7, "Shared iFolders," on page 19
- Section 1.4.8, "iFolder Access Rights," on page 20
- Section 1.4.9, "Account Setup for Enterprise Servers," on page 20
- Section 1.4.10, "Access Authentication," on page 20
- Section 1.4.11, "File Synchronization and Data Management," on page 21
- Section 1.4.12, "Synchronization Log," on page 21
- Section 1.4.13, "iFolder Client APIs," on page 21

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 3.6 Web Admin Console

The Novell iFolder 3.6 Web Admin is an administrative tool used to manage the iFolder system, user accounts, and user iFolders and data.

1.4.3 iFolder Web Access Console

The iFolder 3.6 Web Access console provides the users an interface for remote access to iFolders on iFolder enterprise server.

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:

- SLED 10 SP1
- openSUSE
- Windows XP SP2/2000 Professional SP4

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 *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

1.4.5 Multi Server Support

Hosting huge amount of data as well as provisioning higher number of users is highly demanded in any Enterprise environment. iFolder domain was dedicated to a single server and this limits the number of users and the hosting bandwidth. With multi-server support, iFolder 3.6 overcame these major setbacks of single server per domain limitations.

Multi-server support expands iFolder domain across servers so that Enterprise level user provisioning can be effectively managed and Enterprise level data can be scaled up accordingly.

1.4.6 Encryption

Encryption support offers full security to iFolder 3.6 users for their sensitive iFolder documents. Users can back up their confidential files encrypted on the server without fear of it losing or exposing or falling into the wrong hands.

1.4.7 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.

1.4.8 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.

1.4.9 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.

1.4.10 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.

1.4.11 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.

1.4.12 Synchronization Log

The log displays a log of your iFolder background activity.

1.4.13 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 23
- "Planning iFolder Services" on page 39
- "Novell iFolder Upgrade, Migration, and Coexistence" on page 33
- "Prerequisites and Guidelines" on page 49

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 55.

What's New

2

Novell® iFolder® 3.6 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 3.6 (OES 2.0 Linux)," on page 23
- Section 2.2, "What's New in Novell iFolder 3.2 (OES SP2 Linux)," on page 23
- Section 2.3, "What's New in Novell iFolder 3.1 (OES SP1 Linux)," on page 24
- Section 2.4, "What's New in Novell iFolder 3.0 (OES Linux)," on page 24
- Section 2.5, "Comparison of 2.x and 3.6 Server Features and Capabilities," on page 25
- Section 2.6, "Comparison of 2.x and 3.6 Client Features and Capabilities," on page 27
- Section 2.7, "Comparison of 2.x and 3.6 Web Access Features and Capabilities," on page 31

2.1 What's New in Novell iFolder 3.6 (OES 2.0 Linux)

The following features are new in iFolder 3.6 for OES 2.0 Linux:

- Multi-sever support with no limit on the number of users and servers to allow expanding the iFolder domain across multiple servers
- Encryption support for users to store sensitive files secured on servers.
- Enhanced Web Admin console to manage,deploy and maintain iFolder system.
- Volume scalability support for iFolder servers to allow administrator to move data across multiple volume on a single server.
- With Multi-domain capability, iFolder 3.6 allows users to work with files belonging to two iFolders that reside on two different iFolder servers
- Enhanced web access for users to help them perform all the operations equivalent to that of iFolder client through web access. It allow mobile users access their iFolder and thus perform all the iFolder operations via mobile.
- Simplified iFolder sharing via Web Access.
- Enhanced reporting for better manageability.
- Support for multiple directories (eDirectory, OpenLDAP and SunOne)

2.2 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.

2.3 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.

2.4 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 section "Key Features of iFolder" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

2.5 Comparison of 2.*x* and 3.6 Server Features and Capabilities

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.6 Enterprise Server
Server management	iFolder Administration tool `http://serveraddress/iFolderServer/Admin.html` You can also access the iFolder Administration tool from iManager by selecting iFolder 2.1*x* from Roles and Tasks.	Novell iFolder 3.6 web admin. `http://serveraddress/admin`
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 Multiple servers participate in a single iFolder domain and iFolder users are automatically balanced across participant servers.
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.

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.6 Enterprise Server
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.
Multi Volume support	No	Administrator can move data across multiple volume available on a single server or across servers.
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.
Multi-volume support	No	With multi volume support, administrator can move the data across multiple volumes available on a single server. In effect, it ensure increased storage scalability.
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.

Feature or Capability	Novell iFolder 2.*x* Server	Novell iFolder 3.6 Enterprise Server
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.	Yes.
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 are backed up.

2.6 Comparison of 2.*x* and 3.6 Client Features and Capabilities

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.6 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 OES Welcome page on the OES Linux server.

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.6 Enterprise 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	`/home/username/`
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.
iFolder data stored encrypted on server	Yes, with encrypted iFolder option The user must specify a passphrase when first creating the iFolder account.	Yes Data is stored encrypted 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.

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.6 Enterprise Server
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.
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.

Feature or Capability	Novell iFolder 2.*x* Client	iFolder Client with a Novell iFolder 3.6 Enterprise Server
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.
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)
Passphrase Management	No	Automated passphrase management.
Remote access to iFolder data on the server	Yes, using NetStorage. Your administrator must configure NetStorage for iFolder services.	Yes, using iFolder 3.6 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.
Enhanced Web access	No	Management of all iFolder enterprise servers is centralized through the enhanced Web Admin. iFolder 3.6 allows management from any location, using a standard Web browser.

2.7 Comparison of 2.*x* and 3.6 Web Access Features and Capabilities

Feature or Capability	Novell iFolder 2.*x* Web Access	Novell iFolder 3.6 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 3.6 Web Access for Novell Open Enterprise Server for Linux.
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 the encrypted iFolder option. The Blowfish algorithm is applied with an auto-generated passphrase. An additional option is available to enable HTTPS(SSL) connection.
WebDAV protocol support	Yes, allows WebDAV clients, such as Microsoft Explorer, to seamlessly access folders and files on an iFolder 2.*x* server.	No

Novell iFolder Upgrade, Migration, and Coexistence

3

One of the top priorities in designing Novell® iFolder® 3.6 was to ensure that new iFolder services, running on Novell Open Enterprise Server 2.0 Linux can bridge the gap between the Novell iFolder 2.*x* services and the iFolder 3.2 services that are currently running on OES 1.0.

This section familiarizes you with the migration and upgrade capabilities of the iFolder 3.6. It also discusses introducing the iFolder 3.6 services into an existing network environment without disrupting existing Novell iFolder 2.*x* services.

This section discusses the following:

- Section 3.1, “Upgrading iFolder 2.x to iFolder 3.6,” on page 33
- Section 3.2, “Upgrading iFolder 3.x to iFolder 3.6,” on page 34
- Section 3.3, “Migration From iFolder 2.x to iFolder 3.6,” on page 36
- Section 3.4, “Coexistence of iFolder 3.6 and 2.x Servers,” on page 37
- Section 3.5, “Coexistence of the iFolder 3.6 Client with Novell iFolder 1.x and 2.x Clients,” on page 37

3.1 Upgrading iFolder 2.*x* to iFolder 3.6

This section helps you understand the types of upgrade, prerequisites for upgrading, and the upgrade process.

- Section 3.1.1, “In-place Upgrade,” on page 33
- Section 3.1.2, “Parallel Upgrade,” on page 33
- Section 3.1.3, “Client Upgrade,” on page 34

3.1.1 In-place Upgrade

An in-place upgrade is a one-way process that directly changes the server database of the previous version to the latest version.

IMPORTANT: Currently, there is no server-side upgrade available.

3.1.2 Parallel Upgrade

A parallel upgrade assumes that both versions run simultaneously on different servers, different databases exist for the two versions, and the database is upgraded in manageable chunks.

In a parallel upgrade, the binaries are upgraded, and the 2.*x* server data is not upgraded but is moved to the iFolder 3.6 server.

IMPORTANT: Currently, there is no server-side upgrade available.

3.1.3 Client Upgrade

The Novell iFolder 2.*x* client and the iFolder 3.6 client can run independently and concurrently on the same user system or desktop. They are separate applications and should not be installed in the same location.

After the installation of the iFolder 3.6 client, you must remove the iFolder 2.*x* client if the client-side migration is performed.

3.2 Upgrading iFolder 3.*x* to iFolder 3.6

This section helps you understand the following:

- Section 3.2.1, "In-place Upgrade," on page 34
- Section 3.2.2, "Parallel Upgrade," on page 34
- Section 3.2.3, "Client Upgrade," on page 35

3.2.1 In-place Upgrade

Ensure that the server-side data is backed up before you perform the upgrade.

You must run the YaST Novell iFolder configuration for the In-place upgrade. YaST upgrade of OES1 to OES2 upgrades configuration values of iFolder enterprise server format from 3.*x* server to the 3.6 server.

For more information on YaST-based configuration, see Section 7.2, "Deploying iFolder Server in a Multi-server Environment," on page 58.

3.2.2 Parallel Upgrade

- "Parallel Upgrade Using the Server Migration Tool" on page 34
- "Parallel Upgrade Using the File System Backup and Restore" on page 35

Parallel Upgrade Using the Server Migration Tool

The Server Migration tool is used to migrate the data in a parallel upgrade. For more information on migration, see the *OES2: Migration Tools Administration Guide* (http://www.novell.com/documentation/migtools/mig_tools_lx/index.html?page=/documentation/migtools/mig_tools_lx/data/bookinfo.html#bookinfo).

After migrating the data, you must follow the steps given below:

1. Open a terminal console and run `/opt/novell/ifolder3/bin/simias-server-setup --upgrade`.
2. Restart Apache server to accept the upgraded configuration.

   Server-side data is upgraded when the iFolder 3.6 server comes up for the first time.

Parallel Upgrade Using the File System Backup and Restore

If you need to migrate only the iFolder services, use the file system backup and restore for migration.

1. Make sure that the 3.*x* server and the target 3.6 server are in the same LDAP directory.
2. Back up the Simias store of the 3.*x* server using the file system backup. The default location of the Simias store is `/var/opt/novell/ifolder3/`
3. Back up `the Simias.config` file of the 3.*x* server. The location of `Simias.config` is `/var/lib/wwwrun/.local/share/simias/`.
4. On the target server, restore the backup of the Simias store and the `Simias.config` file to the original location.
5. Open a terminal console and run `/opt/novell/ifolder3/bin/simias-server-setup --upgrade`.
6. Restart the Apache server to accept the upgraded configuration.

   Server-side data is upgraded when the iFolder 3.6 server comes up for the first time.

3.2.3 Client Upgrade

- "Understanding the Upgrade Process" on page 35
- "Planning the Upgrade for the Administrator" on page 35
- "Upgrade Procedure for the User" on page 36

Understanding the Upgrade Process

With the client upgrade, binaries are upgraded with the new version of binaries and the client data is auto-upgraded.

Planning the Upgrade for the Administrator

Make sure that you perform the following server-side operations so that the user is notified of the new version of iFolder client and prompted for client upgrade.

IMPORTANT: You must ensure that the user backs up the Simias store before upgrading the client.

---

1. Enter `http:\\` *`IP address of iFolder server`* in the browser to go to the OES 2.0 home page.
2. Download the client RPMs or executables from the OES 2.0 home page.
3. Place the RPMs under respective platform directories in the path *`ifolder_installDirectory`*`/lib/simias/web/update/unix`

   The latest client RPMs are installed only if they are present in the given path. The automatic installation happens when the user attempts to connect the 3.*x* or 3.4.1 client to the iFolder 3.6 server. The names of the platform specific directories are in the `version.config` file in the same path. A script file named `install-ifolder.sh` in the `unix` directory contains the commands for upgrading the RPMs to the latest version.

   Examples for `install-ifolder3.sh` are as follows:

   ```
   rpm -Uvh <absolute path of simias rpm>
   ```

```
rpm -Uvh <absolute path of ifolder rpm>
rpm -Uvh <absolute path of nautilus-ifolder3 rpm>
```

4 Modify `version.config` to include the entries of the directory where in the RPMs or the .exe are placed.

Upgrade Procedure for the User

1 Connect the exisitng client to the server.

The client automatically prompts the user for upgrade when he or she attempts to connect an iFolder 3.*x* or 3.4 1 to a 3.6 server. For more information, refer to "Automatically Upgrading to iFolder 3.6" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

For manual upgrade, refer to "Manually Upgrading to iFolder 3.6" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

3.3 Migration From iFolder 2.*x* to iFolder 3.6

Migration refers to the process of migrating the iFolder and the user data from an iFolder 2.*x* domain to iFolder 3.6. For the migration process, a client-based migration tool is used.

This section discusses the following:

- Section 3.3.1, "Planning," on page 36
- Section 3.3.2, "User Data Migration," on page 37
- Section 3.3.3, "User Identity And Configuration Migration," on page 37

3.3.1 Planning

- The user must have both an iFolder 2.*x* account and a corresponding iFolder 3.6 account.
- The user must use only the Migration Wizard available in the iFolder client to convert an existing 2.*x* iFolder to a 3.6 iFolder. The user should not perform iFolder 2.*x* to 3.6 conversion by any other means such as using iFolder shell integration (Windows Explorer or Nautilus)or iFolder 3.6 client upload mechanism from the thick client.
- If the user selects to make a copy of the iFolder 2.*x* data and move it to the iFolder 3.6 domain, ensure that you allocate sufficient space (at least 10 MB larger than the size of the iFolder 2.*x* data) on the hard disk before performing migration. The additional space is used to store the iFolder database.

  In this case, the user must log out of the 2.*x* client before performing the migration to avoid synchronization issues and related possible data corruption.
- If the user selects to migrate the iFolder and disconnect it from 2.*x* domain, the folder is not accessible through the 2.*x* account after the migration, because it is completely moved to the 3.6 domain and 2.*x* registry entries are removed in the client. It is possible that the same 2.x iFolder is available on another user desktop. If so, make sure that it is manually removed to avoid data inconsistency, because it is not under the control of iFolder 3.6 domain.

3.3.2 User Data Migration

This section discusses the following:

- “Client-Based Migration” on page 37
- “Server-Based Migration” on page 37

Client-Based Migration

There is an automatic client-side migration from Novell iFolder 2.*x* to 3.6. The Migration Wizard provided for the user in the iFolder 3.6 client migrates the existing 2.*x* iFolder and user data to iFolder 3.6. The Migration Wizard appears soon after the installation of iFolder 3.6 client, and displays a message about the existence of previous version data and request for a migration.This Wizard is also available in the preferences page so that it can be invoked at any time after installation.

Server-Based Migration

Currently there is no server-side migration from Novell iFolder 2.*x* to Novell iFolder 3.6.

3.3.3 User Identity And Configuration Migration

User and configuration migration are not currently supported.

If the same LDAP tree is used in both iFolder 2.*x* and iFolder 3.6, a user is automatically provisioned in the 3.6 domain. You can also use the Novell Migration tool to migrate the iFolder users from 2.*x* to 3.6.

3.4 Coexistence of iFolder 3.6 and 2.*x* Servers

If you use both iFolder 2.*x* and Novell iFolder 3.6 services, we recommend that you install each version on its own dedicated server. The OES 2.0 Linux services do not support iFolder 2.*x* services.

3.5 Coexistence of the iFolder 3.6 Client with Novell iFolder 1.*x* and 2.*x* Clients

Do not install the iFolder 3.6 client in the same application folder as the Novell iFolder 1.*x* or 2.*x* client.

The iFolder 3.6 client can coexist on the same workstation as the Novell iFolder 1.*x* client or 2.*x* client, with the following caveats:

- The iFolder 3.6 client and its iFolders work only with the Novell iFolder 3.6 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 3.6 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 Novell iFolder 1.*x* or 2.*x* to an iFolder to be managed by Novell iFolder 3.6 by any other means other than using the migration tool. Similarly, you should not convert parent folders of that iFolder to a next-generation iFolder.

  For example, if *abc* is the parent directory of the *xyz* directory, you should not attempt to migrate *abc* to iFolder 3.6 while *xyz* still remains an iFolder of type 2.*x* or 1.*x*. In addition, you should not attempt to migrate *xyz* to iFolder 3.6 while *abc* still belongs to a 2.*x* or 1.*x* domain.

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

Planning iFolder Services

4

This section discusses the planning considerations for providing Novell® iFolder® 3.6 services on OES Linux.

- "Security Considerations" on page 39
- "Server Workload Considerations" on page 39
- "Naming Conventions for Usernames and Passwords" on page 40
- "iFolder User Account Considerations" on page 42
- "iFolder User Account Considerations" on page 42
- "iFolders Data and Synchronization Considerations" on page 43
- "Management Tools" on page 45

4.1 Security Considerations

For information about planning security for your iFolder 3.*x* system, see the *Novell iFolder 3.6 Security Administration Guide*.

4.2 Server Workload Considerations

The iFolder 3.6 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.

iFolder 3.6 provides you Multi-server and Multi-volume support to enhance the storage capability of it's servers. Multi-volume feature exempt from the single iFolder per volume restriction and thus enable you to move the data across multiple volume available on a single server. With Web Admin console, you can add multiple mount points to a single server and thus increase the effective space available. iFolder server will also have the capability to configure the volume on which a particular iFolder needs to be created using the Web Admin console.

Multi-server support is another key feature in iFolder 3.6 that makes server workload management significantly easier for administrators. In the past, iFolder domain was dedicated to a single server that limited the number of users and data transfer bandwidth. With Multi-server support, iFolder 3.6 will have the capability to add more than one server to a single iFolder domain, thus enterprise level provisioning is effectively managed and hosting enterprise data is scaled up.

You can even 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.
- The amount of 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 3.6 server with a workload similar to a typical iFolder 2.*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 4-1 *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 per server (Multi Server Configuration)
	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

4.3 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 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/treetitl.html).

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 2 Linux and SLED.

For information, see "Multilingual Considerations" (http://www.novell.com/documentation/edir88/edir88/data/a2iiidp.html#a2iiie7) in the *Novell eDirectory 8.8 Administration Guide.*

4.4 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 LDAP Search contexts.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the Web Admin console to add or remove the iFolder Admin right for users. Only users who are in one of the contexts specified in the LDAP Search contexts 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 LDAP 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 LDAP Search contexts, or move the user to a context that is not in the LDAP Search contexts.

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 container configured during iFolder enterprise server setup. The iFolder Proxy user is created during the iFolder install and appropriate access rights are provided. 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 4-2 *Encryption Method for the iFolder Proxy User Password*

iFolder Version	Encryption Method	iFolder Proxy User Password
iFolder 3.6	YaST encryption method	Generates an alphanumeric, 21-digit mixed-case 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 `/datapath/simias/.local.ppf` file. At the end of the configuration process, the system reboots Apache 2 and starts iFolder. When iFolder runs this for the first time after configuration, the iFolder process encrypts the password and stores it in the Simias database and remove the entry from the `.local.ppf` file.

IMPORTANT: Currently, the Proxy user password cannot be changed in the iFolder system. Ensure that you don't change the password in the LDAP directory as well. Changing the password in LDAP directory makes iFolder unfunctional.

4.5 iFolder User Account Considerations

This section describes iFolder user account considerations.

- "Preventing the Propagation of Viruses" on page 42
- "Provisioning User Accounts" on page 42
- "Setting Account Quotas" on page 43

4.5.1 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 *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

4.5.2 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.

4.5.3 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 level. Within a give account quota, you can also set a quota for any iFolder.

4.6 iFolders Data and Synchronization Considerations

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

- "Naming Conventions for an iFolder and Its Folders and Files" on page 43
- "Guidelines for File Types and Sizes to Be Synchronized" on page 44

4.6.1 Naming Conventions for an iFolder and Its Folders and Files

The iFolder client imposes naming conventions that consider the collective restrictions of the Linux, and Windows 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.

4.6.2 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.

4.7 Management Tools

Use the following tools to manage the Novell iFolder 3.6 enterprise server and Web Access server.

- "iFolder Configuration Plug-Ins for YaST" on page 45
- "Novell iFolder Web Admin for Novell iManager 2.7" on page 46
- "Web Access Configuration File" on page 46

4.7.1 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, *Open Enterprise Server > OES Install and Configuration> Novell iFolder* For information, see Section 7.2, "Deploying iFolder Server in a Multi-server Environment," on page 58.
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, *Open Enterprise Server > OES Install and Configuration> Novell iFolder > iFolder Web Access* For information, see Section 7.2, "Deploying iFolder Server in a Multi-server Environment," on page 58.

iFolder Plug-In for YaST	Purpose	Tasks
iFolder 3 Web Admin	Use this function to configure the following parameters for the iFolder Web Admin ◆ Web Admin alias ◆ iFolder server URL	In YaST, *Open Enterprise Server > OES Install and Configuration> Novell iFolder > iFolder Web Admin* For information, see Section 7.2, "Deploying iFolder Server in a Multi-server Environment," on page 58.

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.

4.7.2 Novell iFolder Web Admin for Novell iManager 2.7

The Novell iFolder Web Admin 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 2.6 Installation Guide* (http://www.novell.com/documentation/imanager26/imanager_install_26/data/hk42s9ot.html).

To access Novell iFolder 3, see Section 7.7, "Accessing iManager and the Novell iFolder Web Admin," on page 87.

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.

Additional Information

For additional information, see the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_26/data/hk42s9ot.html).

4.7.3 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 12.4, "Configuring the HTTP Runtime Parameters," on page 139.

Running Novell iFolder in a Virtualized Environment

5

Novell iFolder 3.6 runs in a virtualized environment just as it does on a physical server running OES 2 Linux, and requires no special configuration or other changes.

To get started with virtualization, see "Introduction to Xen Virtualization" in the *Getting Started with Virtualization* guide.

For information on setting up virtualized OES 2 Linux, see "Setting Up Virtual Machines" in the *Getting Started with Virtualization* guide and "OES Linux Virtual Machines"in the *Novell Virtualization Technology: Guest Operating System Guide*.

5.1 What's Next

"To get started with virtualization, see "Introduction to Xen Virtualization" in the *Getting Started with Virtualization* guide.

"For information on setting up virtualized NetWare, see "Setting Up Virtual Machines" in the *Getting Started with Virtualization* guide and "NetWare Virtual Machines" in the *Novell Virtualization Technology: Guest Operating System Guide*.

"For information on setting up virtualized OES 2 Linux, see "Setting Up Virtual Machines" in the *Getting Started with Virtualization* guide and "OES Linux Virtual Machines" in the *Novell Virtualization Technology: Guest Operating System Guide*."

Prerequisites and Guidelines

6

This section discusses prerequisites and guidelines for this release of Novell® iFolder® 3.6 and the iFolder™ Client. Before installing and configuring iFolder, make sure that your system meets the requirements in each of the following:

- Section 6.1, “File System,” on page 49
- Section 6.2, “Enterprise Server,” on page 49
- Section 6.3, “Novell eDirectory 8.8,” on page 52
- Section 6.4, “Novell iManager 2.7,” on page 52
- Section 6.5, “Mono 1.2.2,” on page 52
- Section 6.6, “Client Computers,” on page 53
- Section 6.7, “Web Browser,” on page 53

6.1 File System

iFolder Application Files

iFolder 3.6 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

6.2 Enterprise Server

We recommend that you install iFolder 3.6 enterprise server, Web Admin server and Web Access server after your OES 2.0 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 6.2.1, “Prerequisites for the Operating System,” on page 50
- Section 6.2.2, “Install Guidelines When Using an NSS Volume to Store iFolder Data,” on page 50
- Section 6.2.3, “Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data,” on page 51

- Section 6.2.4, “Install Guidelines for Other Components,” on page 51
- Section 6.2.5, “Installing the OES 2.0 Linux Server,” on page 52

6.2.1 Prerequisites for the Operating System

Novell iFolder 3.6 is designed to work only on the Novell Open Enterprise Server for Linux (OES 2 Linux) platform, which is comprised of specific versions of the SUSE® Linux Enterprise Server platform and the basic OES applications and services.

IMPORTANT: iFolder 3.6 and earlier does not support SUSE Linux Enterprise Server without the basic OES applications and services. It also does not support OES NetWare.

iFolder 3.*x* requires the following versions of the OES Linux server:

iFolder Version	OES Linux Version
iFolder 3.6	Novell Open Enterprise Server 2 for SUSE Linux Enterprise Server 10 Support Pack 1
iFolder 3.2	Novell Open Enterprise Server Support Pack 2 for SUSE Linux Enterprise Server 9 Support Pack 3 (OES SP2 Linux)
iFolder 3.1	Novell Open Enterprise Server Support Pack 1 for SUSE Linux Enterprise Server 9 Support Pack 2 (OES SP1 Linux)
iFolder 3.0	Novell Open Enterprise Server for SUSE Linux Enterprise Server 9 Support Pack 1 (OES Linux)

Currently there is no upgrade or migration path from Novell iFolder 2.*x* and earlier versions of iFolder. It is supported for the future releases.

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

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

Modify the OES 2.0 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 (http://www.novell.com/documentation/oes2/inst_oes_lx/index.html?page=/documentation/oes2/inst_oes_lx/data/front.html#front) in the OES Linux Installation Guide (http://www.novell.com/documentation/oes2/inst_oes_lx/index.html?page=/documentation/oes2/inst_oes_lx/data/front.html#front) 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.

6.2.3 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 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 7.2, “Deploying iFolder Server in a Multi-server Environment,” on page 58

6.2.4 Install Guidelines for Other Components

We recommend that your iFolder enterprise server, Web Admin server and Web Access server run on separate dedicated servers. For small office use, both enterprise server, Web Admin 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 2.0 Linux (Minimum predefined server plus graphics support and NSS if desired)
- Novell eDirectory 8.8 (can be configured on a different OES 2.0 Linux server)
- Novell iManager 2.7 (can be configured on a different OES 2.0 Linux server)
- Novell iFolder 3.6 (typically post-installed on an OES 2.0 Linux server)
  - Enterprise server
  - Web Access server (can be installed and configured on a different OES 2.0 Linux server)
  - Web Admin server (can be installed and configured on a different OES 2.0 Linux server)
  - Mono 1.1.18 (The Mono package is required for iFolder 3.6 enterprise server, Web Admin server and Web Access server.)
  - Apache 2 Web Server (The apache2-worker package is required for iFolder 3.6 enterprise server, Web Admin server and for Web access server.)
  - Other iFolder dependencies as noted in YaST by the iFolder 3.6 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.

6.2.5 Installing the OES 2.0 Linux Server

For detailed information about prerequisites, installation, and configuration of your OES 2.0 Linux server, see the *OES for Linux Installation Guide* (http://www.novell.com/documentation/oes/install_linux/data/front.html).

6.3 Novell eDirectory 8.8

Novell eDirectory™ 8.8 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 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html):

- "Designing Your Novell eDirectory Network" (http://www.novell.com/documentation/edir88/edir88/data/a2iiido.html)
- "Managing User Accounts" (http://www.novell.com/documentation/edir88/edir88/data/afxkmdi.html)

Make sure your LDAP objects comply with the naming conventions for your LDAP services. For information, see Section 4.3, "Naming Conventions for Usernames and Passwords," on page 40.

6.4 Novell iManager 2.7

Novell iManager 2.7 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 Web Admin for iManager, iManager must be installed and configured.

For information, see the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_26/data/hk42s9ot.html).

6.5 Mono 1.2.2

Novell iFolder 3.6 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 also require Mono 1.2.x. The required version of Mono is packaged in the iFolder client installation files that you distribute to your users. For information, see Section 7.9, "Distributing the iFolder Client to Users," on page 89. Linux and Macintosh users must install both iFolder and Mono packages. For information, see "Getting Started" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

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 3.6 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).

6.6 Client Computers

The iFolder client supports the following workstation operating systems:

- SLED 10 SP1 (requires Mono 1.2.*x* for Linux)
- Windows 2000/XP with the latest .NET support patches

The Mono modules you need for this release are included on the `.iso` files for iFolder 3.6

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

6.7 Web Browser

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

- Mozilla* Firefox* 2.*x*
- Microsoft* Internet Explorer
- Safari*

Installing and Configuring iFolder Services

7

This section describes how to install and configure Novell® iFolder® 3.6 Enterprise and Web Access servers.

- Section 7.1, “Installing iFolder on an Existing OES 2 Linux Server,” on page 55
- Section 7.2, “Deploying iFolder Server in a Multi-server Environment,” on page 58
- Section 7.3, “Configuring the iFolder Web Access Server,” on page 73
- Section 7.4, “Configuring the iFolder Web Admin Server,” on page 75
- Section 7.5, “Installing the Novell iFolder 3 Plug-In for iManager,” on page 77
- Section 7.6, “Recovery Agent Certificates,” on page 79
- Section 7.7, “Accessing iManager and the Novell iFolder Web Admin,” on page 87
- Section 7.8, “Provisioning Users and iFolder Services,” on page 89
- Section 7.9, “Distributing the iFolder Client to Users,” on page 89
- Section 7.10, “Updating Novell iFolder 3.6,” on page 91
- Section 7.11, “Updating Mono for the Server and Client,” on page 91
- Section 7.12, “Uninstalling the iFolder 3.6 Enterprise Server,” on page 91
- Section 7.13, “What’s Next,” on page 91

7.1 Installing iFolder on an Existing OES 2 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 2 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.

NOTE: If you used the Minimum install option for your OES 2 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.

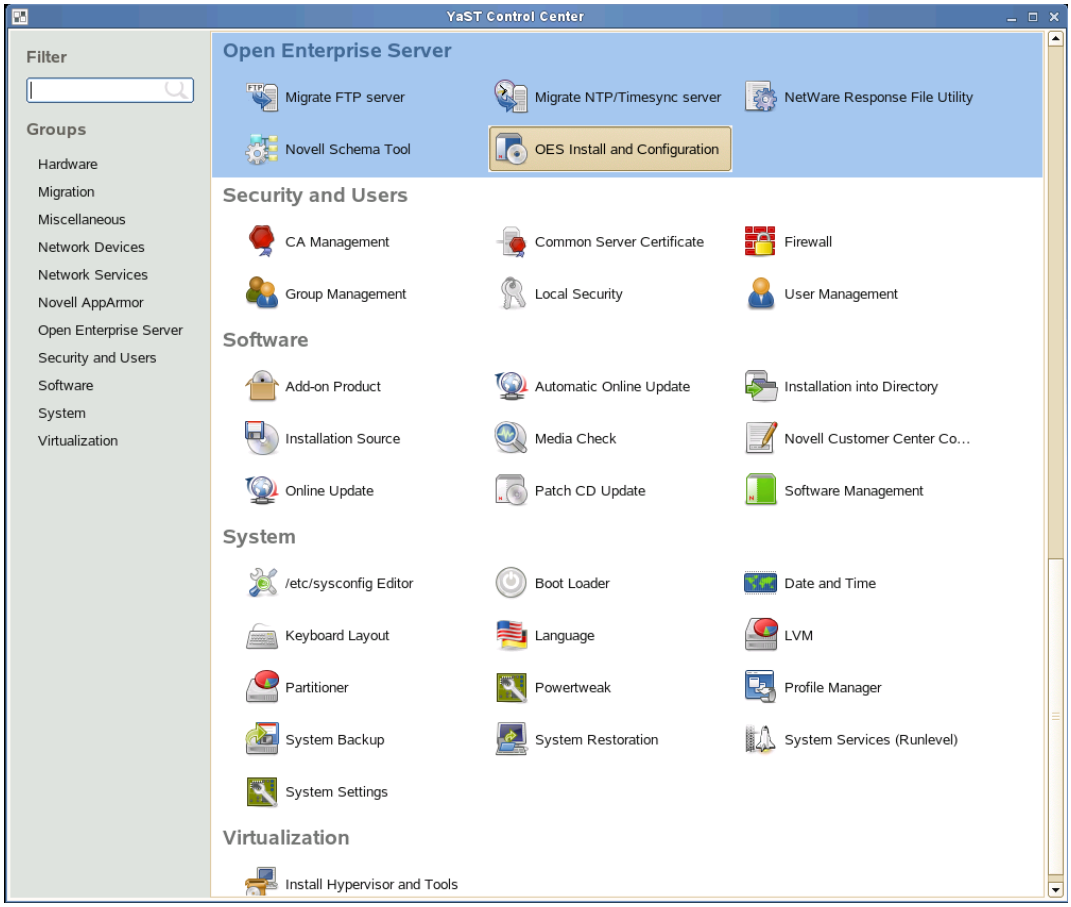
---

1. Before you begin, make sure your OES 2 Linux system setup meets the “Prerequisites and Guidelines” on page 49.
2. 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

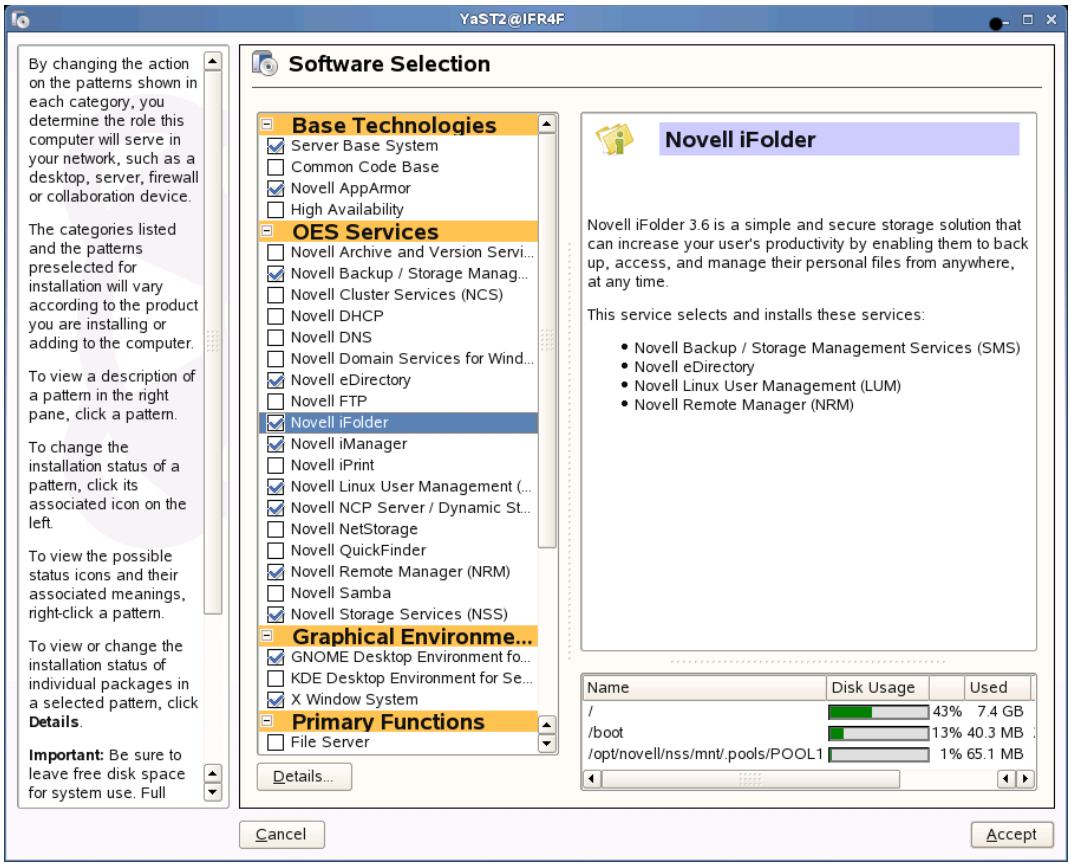
     ```
     yast2
     ```

IMPORTANT: Ensure that you are logged in as the `root` user before performing the installation and configuration procedure.

3 In the left menu, select `Open Enterprise Server > OES Install and Configuration`.



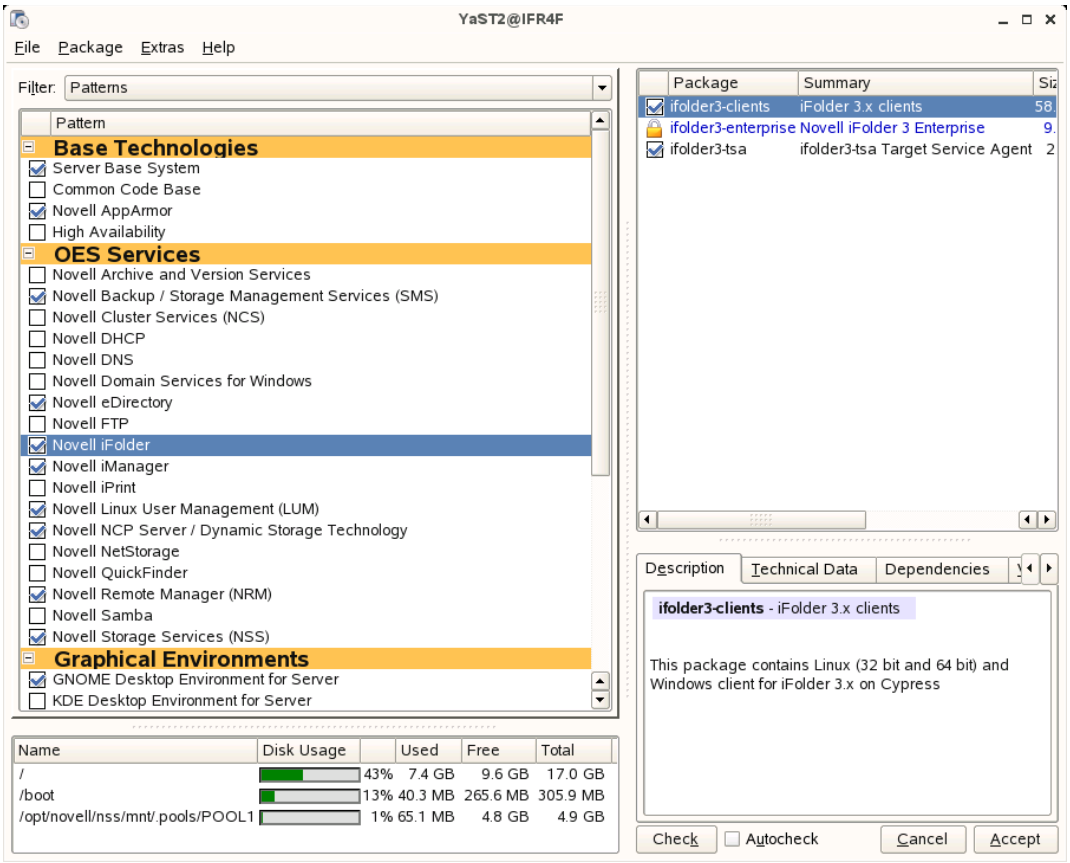
A window displays with the Open Enterprise Server Services and Server Role patterns under software selection.



4 Select the *Novell iFolder* option.

You can install the iFolder 3.6 Enterprise Server, Web Admin Server, and Web Access Server on the same computer or on different computers.

5 Click Details to resolve the dependency conflicts if you encounter any.



Resolve all the dependencies before continuing.

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

7 When the installation is complete, either close YaST or continue with one or all of the following as needed:

- Section 7.2, “Deploying iFolder Server in a Multi-server Environment,” on page 58
- Section 7.3, “Configuring the iFolder Web Access Server,” on page 73
- Section 7.4, “Configuring the iFolder Web Admin Server,” on page 75

7.2 Deploying iFolder Server in a Multi-server Environment

This section describes how to configure Novell® iFolder® 3.6 servers in a Multi-server environment.

- Section 7.2.1, “Configuring the iFolder Enterprise Server,” on page 59
- Section 7.2.2, “Configuring the iFolder Slave Server,” on page 66
- Section 7.2.3, “Loading Recovery Agent Certificates in The iFolder Server,” on page 73

7.2.1 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.

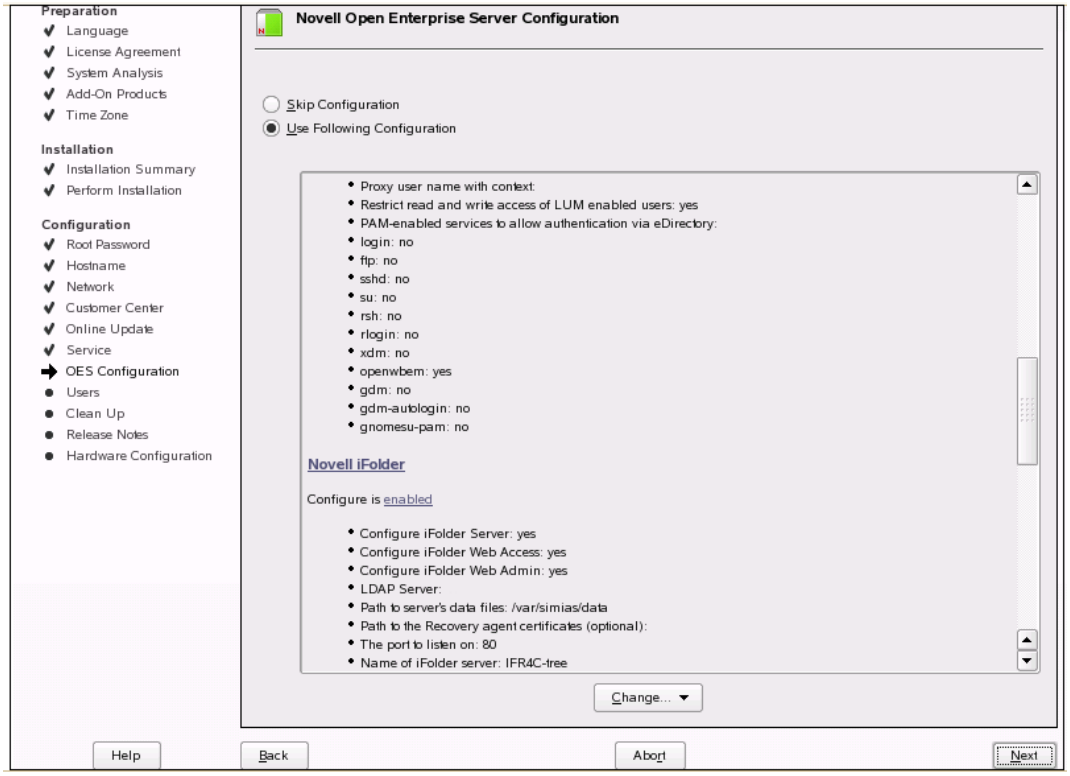
1. If you plan to use an NSS volume as the System Store Path for the users' iFolder data, use iManager to create the NSS volume, then create a directory on the volume.

   For information, see Managing NSS Volumes (http://www.novell.com/documentation/oes2/stor_nss_lx_nw/index.html?page=/documentation/oes2/stor_nss_lx_nw/data/front.html#front) in the Novell Storage Services File System Administration Guide (http://www.novell.com/documentation/oes2/stor_nss_lx_nw/index.html?page=/documentation/oes2/stor_nss_lx_nw/data/front.html#front).

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

3. Start YaST, follow the YaST on-screen instruction to finish the installation. For more information see Step 1 on page 55 through Step 7 on page 58 in the section Section 7.1, "Installing iFolder on an Existing OES 2 Linux Server," on page 55.

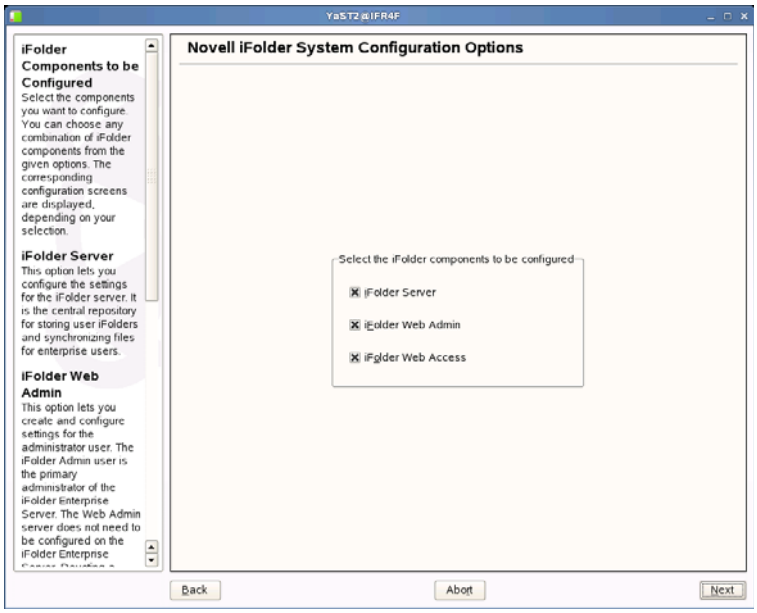
4. Select *Use Following Configuration* and click *Novell iFolder* to change the default configuration settings for iFolder.



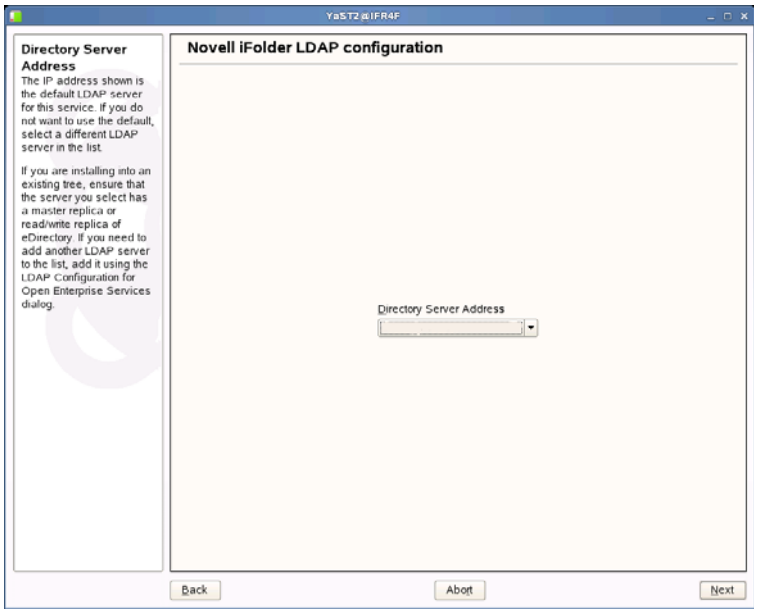
   If you decide to use default settings, click *Next* to start Novell iFolder 3 configuration.

   IMPORTANT: For security reasons, it is recommended that you always change the default iFolder configuration settings.

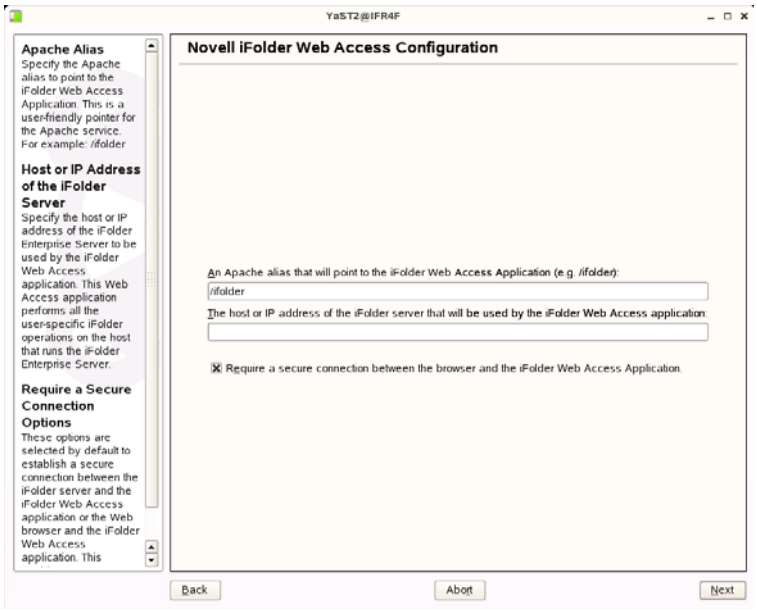
5. Follow the Yast on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

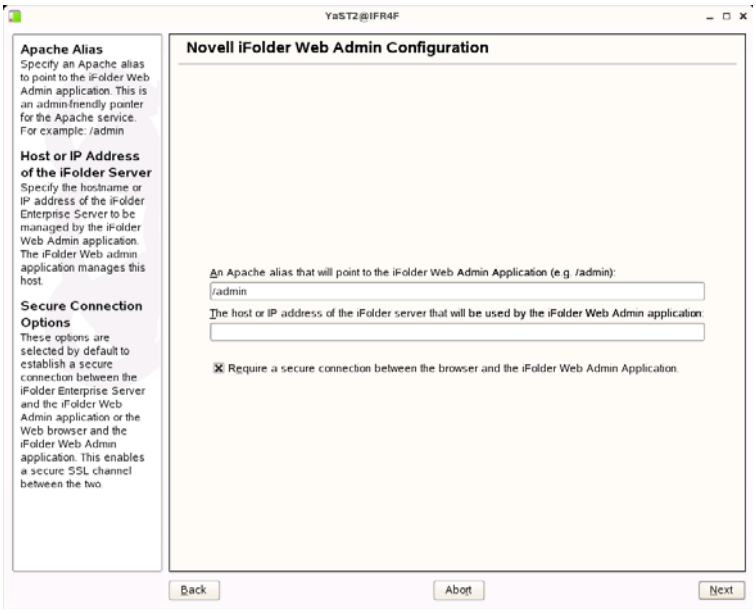
Install Settings	Description
iFolder components	 ◆ **Select the iFolder components to be configured:** Select the components you want to configure. You can choose any combination of iFolder components from the given options. The corresponding screens are displayed depending on your selection. ◆ **iFolder Server (optional):** Select the check box adjacent to the iFolder Server to configure iFolder server.This option lets you configure the settings for the iFolder server. It is the central repository for storing user iFolders and synchronizing files for enterprise users. ◆ **iFolder Web Admin (optional):** Select the check box adjacent to the iFolder Web Admin to configure iFolder Web Admin server. This option lets you create and configure settings for the Administrator user. The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic. ◆ **iFolder Web Access (optional):** Select the check box adjacent to the iFolder Web Access to configure iFolder Web Access server. This option lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server. The Web Access server lets users perform all the operations equivalent to those of the iFolder client through using a standard Web browser. The Web Access server does not need to be configured in the same iFolder Enterprise Server. Channeling the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.

Install Settings	Description
Novell iFolder System Configuration	• **Name Used to Identify the iFolder System to Users:** A unique name to identify your iFolder 3 server. For example, `iFolder Server`. • **System Description:** A descriptive label for your iFolder 3 server. For example, `iFolder3 Enterprise Server` • **Path to the Server Data File:** Specify the case-sensitive address of the location where the iFolder enterprise server stores iFolder application files as well as the users' iFolders and files. For example, `/var/simias/data/simias`. This location cannot be modified after install. • **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key. After you configure the path to the Recovery Agent, you must load the Agent certificates to this location. For more information, see Section 7.2.3, “Loading Recovery Agent Certificates in The iFolder Server,” on page 73. • **Name of iFolder Server:** Specify a unique name to identify your iFolder server. For example, `IF3EastS` • **iFolder Public URL:** Specify the public URL to reach the iFolder server. • **iFolder Private URL:** Specify the private URL corresponding to the iFolder server to allow communication between the servers within the iFolder domain. The Private URL and the Public URL can be the same. • **iFolder Port to Listen On:** Specify the port for the iFolder to Listen On. Port 80 is the default • **Install into Existing iFolder Domain:** If left unselected, this server becomes the Master iFolder server. Select this option when you want to use an existing iFolder domain and provide the Master server information. **IMPORTANT:** You must ensure that the server you install and the current iFolder domain are in the same LDAP tree. • **Private URL Host or IP address of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Server. For more information, see the Section 7.2.2, “Configuring the iFolder Slave Server,” on page 66

Install Settings	Description
Novell iFolder LDAP Configuration	 ◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it using the LDAP Configuration for Open Enterprise Services dialog.

Install Settings	Description
Novell iFolder System Configuration	◆ **The iFolder Default Administrator:** Specify the username for the default iFolder Admin user. Use the full distinguished name of the iFolder Admin user. For example:`cn=admin,o=acme`. ◆ **iFolder Admin Password:** Specify a password for the iFolder Admin user. ◆ **Verify iFolder Admin Password:** Type the password for the iFolder Admin user again. ◆ **LDAP Proxy User:** Specify the full distinguished name of the LDAP Proxy user. For example:`cn=iFolderproxy,o=acme.` This user must have the Read right to the LDAP service. The LDAP Proxy user is used for provisioning the users between the iFolder Enterprise Server and the LDAP server. If the Proxy user does not exist, it is created and granted the Read right to the root of the tree. If the Proxy user already exists, but the given credentials don't match, then a new Proxy user is automatically created. The Proxy user's domain name (dn) and password are stored by the iFolder. ◆ **LDAP Proxy User Password:** Specify a password for the LDAP Proxy user. By default, it is YaST-generated password. **IMPORTANT:** You are recommended not to use the YaST-generated default password. You must specify the password for the Proxy user. You cannot change the Proxy user password once it is set. ◆ **Verify LDAP Proxy User Password:** Type the password for the LDAP Proxy User again. ◆ **LDAP Search Context** Click *Add*, then specify an LDAP tree context to be searched for users and provisioning them in to iFolder. For example, `o=acme, o=acme2,` or`o=acme3`. If no context is specified, only the iFolder Admin user is provisioned for services during the install. ◆ **LDAP Naming Attribute:** Select which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Common Name (cn) is the default and an e-mail address (email) is the other option. 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. This setting cannot be changed after the install using the Web Admin console. ◆ **Require a Secure Connection between the LDAP server and the iFolder Server:** Select this option to require a secure connection between the LDAP server and the iFolder server. This option is selected by default. If the LDAP server co-exists on the same machine as the iFolder server, an administrator can disable SSL, which increases the performance of LDAP authentications.

Install Settings	Description
iFolder Web Access Configuration Help	 • **An Apache alias that will point to the iFolder Web Access Application:** Specify an Apache alias to point to the iFolder Web Admin application. This is an admin-friendly pointer for the Apache service. For example, /access • **The host or IP address of the iFolder server that will be used by the iFolder Web Access application:** Specify the hostname or IP address of the iFolder Enterprise Server to be managed by the iFolder Web Admin application. The iFolder Web Admin application manages this host. • **Require a secure connection between the browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

Install Settings	Description
iFolder Web Admin Configuration Help	 • **An Apache alias that will point to the iFolder Web Admin Application:** Specify the Apache alias to point to the iFolder Web Access Application. This is a user-friendly pointer for the Apache service. For example, /admin • **The host or IP address of the iFolder server that will be used by the iFolder Web Admin application:** Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server. • **Require a secure connection between the browser and the iFolder Web Admin application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.

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

To manually restart the Apache Web server,

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 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 plug-in or to manage iFolder services.

8 If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object `wwwrun` before restarting your web server. At a terminal console prompt, log in as the root user or equivalent, then enter

```
rights -f /media/nss/NSSVOL -r rwfcem trustee wwwrun.ou.o.treename
```

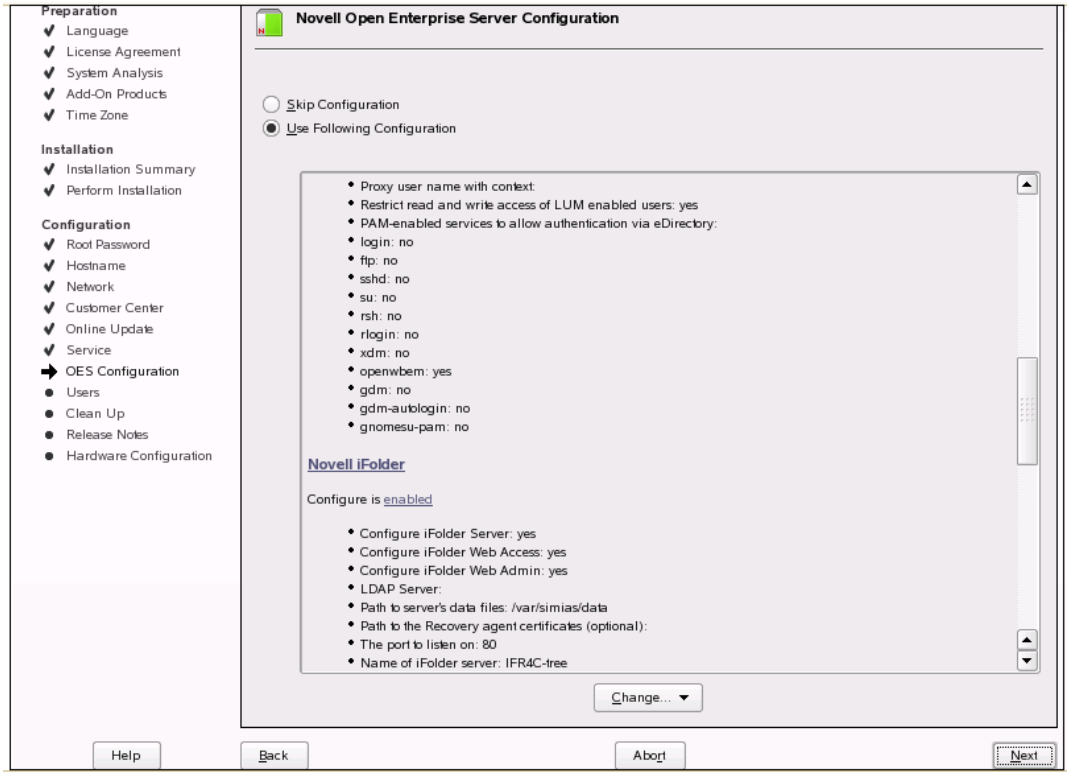
If you ever get `An Internal Error has occurred` error message within the iManager plug-in, this is a sure sign that you have not set up file system trustee rights within NSS properly.

7.2.2 Configuring the iFolder Slave Server

To deploy iFolder server in a Multi-server set up,

After you configure the iFolder enterprise master server, you must configure the iFolder slave servers.

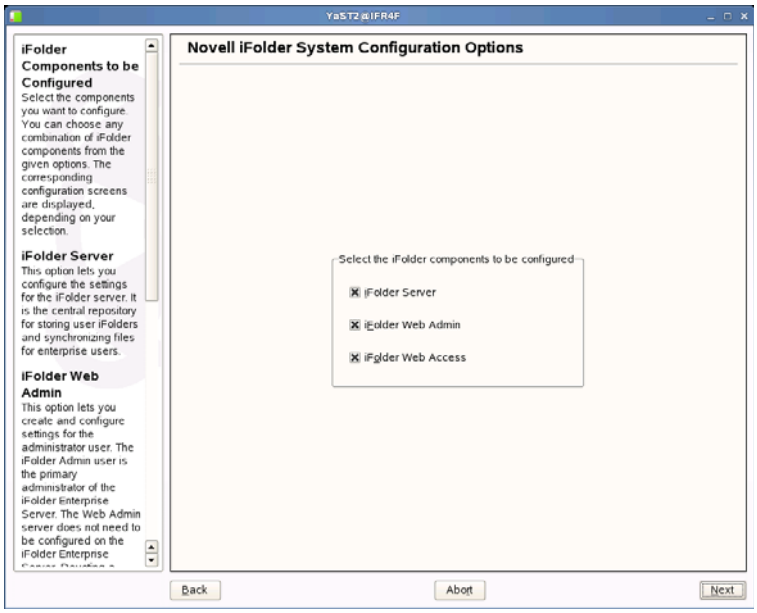
1 Select *Use Following Configuration* and click *Novell iFolder* in the window displayed.



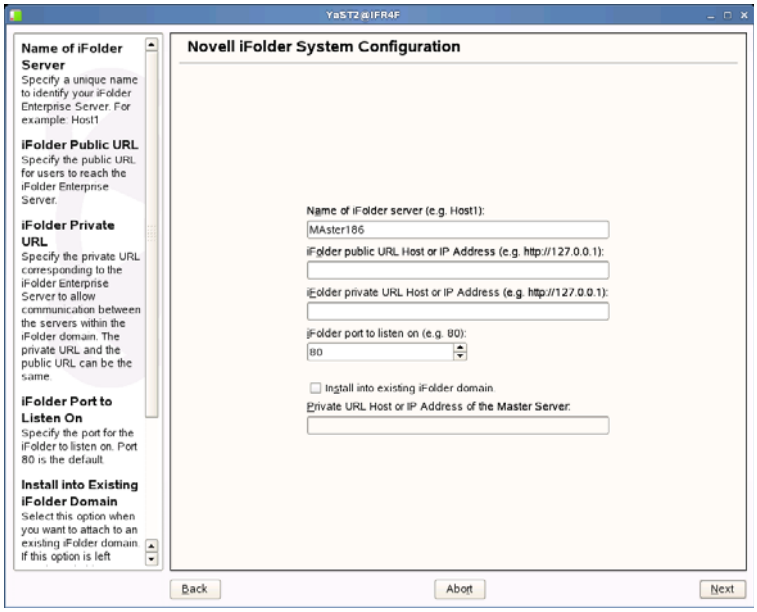
2 Click *Novell iFolder* and then *Next* to start configuring the slave server.

IMPORTANT: For security reasons, it is recommended that you always change the default iFolder configuration settings.

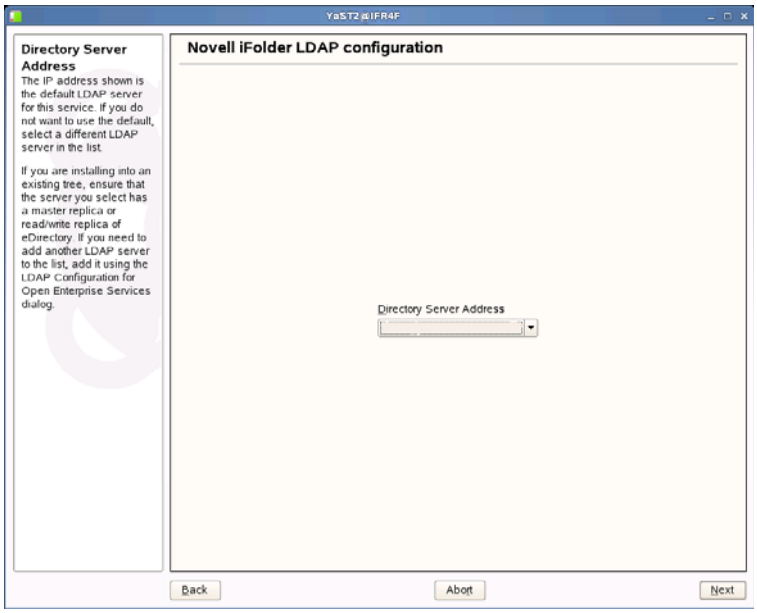
3 Follow the Yast on-screen instructions to proceed through the Novell iFolder 3 configuration. The following table summarizes the decisions you make.

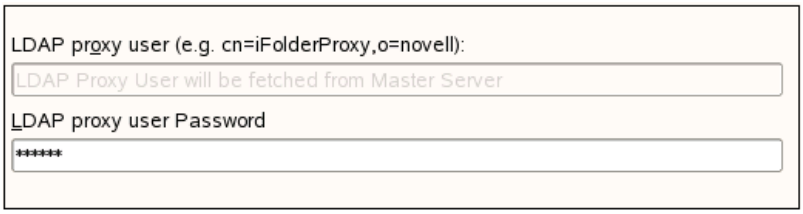
Install Settings	Description
iFolder components	 • **Select the iFolder components to be configured:** Select the components you want to configure. You can choose any combination of iFolder components from the given options. The corresponding screens are displayed depending on your selection. • **iFolder Server (optional):** Select the check box adjacent to the iFolder Server to configure iFolder server.This option lets you configure the settings for the iFolder server. It is the central repository for storing user iFolders and synchronizing files for enterprise users. • **iFolder Web Admin (optional):** Select the check box adjacent to the iFolder Web Admin to configure iFolder Web Admin server. This option lets you create and configure settings for the Administrator user. The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic. • **iFolder Web Access (optional):** Select the check box adjacent to the iFolder Web Access to configure iFolder Web Access server. This option lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server. The Web Access server lets users perform all the operations equivalent to those of the iFolder client through using a standard Web browser. The Web Access server does not need to be configured in the same iFolder Enterprise Server. Channeling the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.

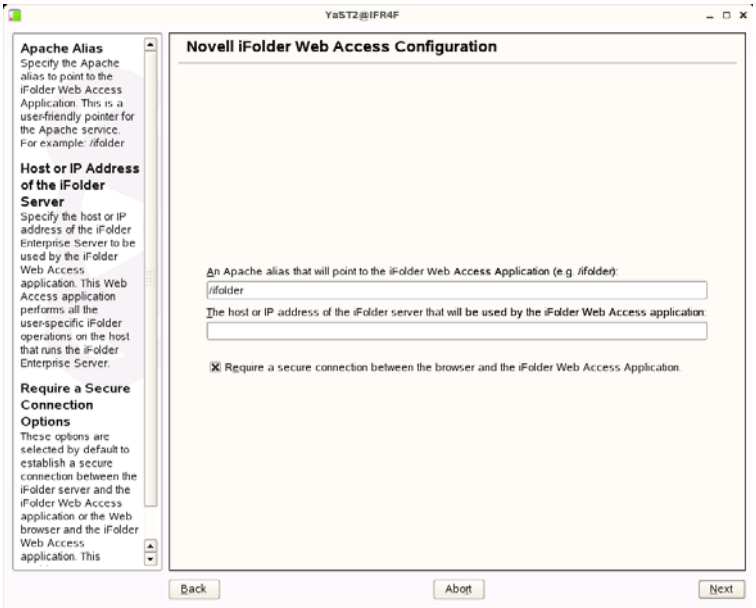
Install Settings	Description
Novell iFolder System Configuration	• **Name Used to Identify the iFolder System to Users:** A unique name to identify your iFolder 3 server. For example, `iFolder Server`. • **System Description:** A descriptive label for your iFolder 3 server. For example, `iFolder3 Enterprise Server` • **Path to the Server Data File:** Specify the case-sensitive address of the location where the iFolder enterprise server stores iFolder application files as well as the users' iFolders and files. For example, `/var/simias/data/simias`. This location cannot be modified after install. • **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key. If the path to the Recovery Agent is configured, you need to copy the Agent certificates to this location. For more information, see Section 7.2.3, “Loading Recovery Agent Certificates in The iFolder Server,” on page 73.



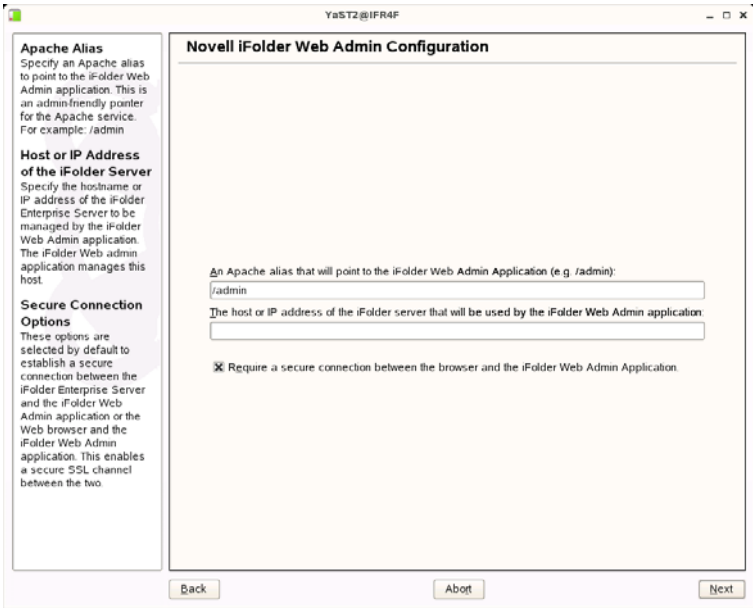
- **Name of iFolder Server:** Specify a unique name to identify your iFolder server. For example, `IF3EastS`
- **iFolder Public URL:** Specify the public URL to reach the iFolder server.
- **iFolder Private URL:** Specify the private URL corresponding to the iFolder server to allow communication between the servers within the iFolder domain. The Private URL and the Public URL can be the same.
- **iFolder Port to Listen On:** Specify the port for the iFolder to Listen On. Port 80 is the default
- **Install into Existing iFolder Domain:** If left unselected, this server becomes the Master iFolder server. For slave server configuration, select this option.
  - **Private URL Host or IP address of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Server.

Install Settings	Description
Novell iFolder LDAP Configuration	 ◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it using the LDAP Configuration for Open Enterprise Services dialog. **IMPORTANT:** iFolder Master server and slave servers must be in the same eDirectory tree.

Install Settings	Description
Novell iFolder System Configuration	• **The iFolder Default Administrator:** Specify the username for the default iFolder Admin user. Use the full distinguished name of the iFolder Admin user. For example:`cn=admin,o=acme` • **iFolder Admin Password:** Specify a password for the iFolder Admin user. • **Verify iFolder Admin Password:** Type the password for the iFolder Admin user again. • **LDAP Proxy User:** This option is disabled by default as the LDAP Proxy user is fetched from the Master server.  • **LDAP proxy user Password:** Specify a password for the LDAP Proxy user. The current credentials should match the Master server credentials. By default, it is the YaST-generated password, you must replace it with the Master server credentials. If the credentials does not match or you don't remember the current credentials of the Master server Proxy user, then a new Proxy user is automatically created with the editable password available in the *LDAP proxy user Password* field. **IMPORTANT:** You cannot change the Proxy user password once it is set. • **LDAP Search Context** Click *Add*, then specify an LDAP tree context to be searched for users and provisioning them in to iFolder. For example, `o=acme, o=acme2,` or`o=acme3`. If no context is specified, only the iFolder Admin user is provisioned for services during the install. The recommended settings must have a mutually exclusive LDAP search context list with other participating servers in the iFolder domain. • **LDAP Naming Attribute:** Select which LDAP attribute of the User account to apply when authenticating users. Each user enters a Username in this specified format at login time. Common Name (cn) is the default and an e-mail address (email) is the other option. 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. This setting cannot be changed after the install. • **Require a Secure Connection between the LDAP server and the iFolder Server:** Select this option to require a secure connection between the LDAP server and the iFolder server. This option is selected by default. If the LDAP server co-exists on the same machine as the iFolder server, an administrator can disable SSL, which increases the performance of LDAP authentications.

Install Settings	Description
iFolder Web Access Configuration Help	

- **An Apache alias that will point to the iFolder Web Access Application:** Specify an Apache alias to point to the iFolder Web Access application. This is an admin-friendly pointer for the Apache service. For example, /access
- **The host or IP address of the iFolder server that will be used by the iFolder Web Access application:** Specify the hostname or IP address of the iFolder Enterprise Server to be managed by the iFolder Web Access application. The iFolder Web Access application manages this host.
- **Require a secure connection between the browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

Install Settings	Description
iFolder Web Admin Configuration Help	 • **An Apache alias that will point to the iFolder Web Admin Application:** Specify the Apache alias to point to the iFolder Web Admin Application. This is a user-friendly pointer for the Apache service. For example, /admin • **The host or IP address of the iFolder server that will be used by the iFolder Web Admin application:** Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server. • **Require a secure connection between the browser and the iFolder Web Admin application:** Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.

4 Click *Accept* to complete the configuration.

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

To manually restart the Apache Web server,

5a Open a terminal console, then log in as the `root` user.

5b Stop the Apache server by entering either of the following commands at the prompt:

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

```
rcapache2 stop
```

5c Start Apache by entering either of the following commands at the prompt:

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

```
rcapache2 start
```

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

7 If you are using an NSS volume to store user data, you must set up NSS file system trustee rights for the Web server user object `wwwrun` before restarting your web server. At a terminal console prompt, log in as the root user or equivalent, then enter

```
rights -f /media/nss/NSSVOL -r rwfcem trustee wwwrun.ou.o.treename
```

If you ever get `An Internal Error has occurred` error message within the iManager plug-in, this is a sure sign that you have not set up file system trustee rights within NSS properly.

7.2.3 Loading Recovery Agent Certificates in The iFolder Server

Recovery Agent certificates are the public key certificates that is used for encrypting the data encryption key. The user selects one of these certificates to perform the data key encryption for later key recovery. Note that he private key is either held by the Recovery agent or the user himself. The supported certificate formats are `*.cer` and `*.der(X.509).`

You can also use the self-signed certificates in the case that the iFolder is deployed in a trusted environment.This certificates is generated using YaST CA Management plug-in or OpenSSL tools. For more information on Certificate generation, see YaST Modules for CA Management (http://www.novell.com/documentation/sles10/sles_admin/index.html?page=/documentation/sles10/sles_admin/data/part_security.html) or OpenSSL Manpage (http://www.openssl.org/docs/apps/openssl.html).

After you configure the path to the Recovery Agent, copy the Agent certificates to this location. If the certificate is expired, you need to load the new certificates again to this location. You must restart the iFolder server after loading the new Recovery Agent certificates.

For information on encryption, see "Managing Passphrase for Encrypted iFolders" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide* and "Using the Recovery Agent" in the *Novell iFolder 3.6 Security Administration Guide*.

7.3 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 2.0 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 Click *Novell iFolder* in the window displays with Novell Open Enterprise Server Configuration.

4 Select *iFolder Web Access*.

5 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`
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.

6 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.

7.3.1 Configuring iFolder Web Access for iChain or AccessGateway

iFolder 3.6 is interoperable with iChain and AccessGateway*. iChain and AccessGateway requires it's own session (user authentication data) logout which is provided by a specified URL. You must configure this URL for the Web Access console for proper logout of iChain/AccessGateway sessions along with iFolder.

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

2 Change the directory by typing `cd /opt/novell/ifolder3/bin` at the command prompt.

3 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`
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Access application. This enables a secure SSL channel between the two.
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Access application. This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL	Specify the redirect URL for iChain or AccessGateway. This URL is used for the proper logout of iFolder Web Access console and iChain or AccessGateway sessions.
Require Server SSL	Skip this option to apply the default value.

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

7.4 Configuring the iFolder Web Admin Server

After you install the iFolder Web Admin 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 with OES 2.0 Linux, the same parameters described in this procedure are available as an integrated part of the server install.

Configuring Web Admin

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 Click *Novell iFolder* in the window displays with Novell Open Enterprise Server Configuration.

4 Select *iFolder Web Admin*.

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

Install Settings	Description
Web Admin Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server
Require Server SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two. **IMPORTANT:** If this option is not enabled, you cannot login to Web Admin via iManager.

6 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.

7.4.1 Configuring iFolder Web Admin for iChain or AccessGateway

iFolder 3.6 is interoperable with iChain and AccessGateway*. iChain and AccessGateway requires it's own session (user authentication data) logout which is provided by a specified URL. You must configure this URL for the Web Admin console for proper logout of iChain/AccessGateway sessions along with iFolder.

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

2 Change the directory by typing `cd /opt/novell/ifolder3/bin` at the command prompt.

3 Follow the on-screen instructions to proceed through the iFolder 3 Web Admin configuration. The table summarizes the decisions you make.

Install Settings	Description
Web Admin Alias	The user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server. For example: `/ifolder`
Require SSL	Select the check box to establish a secure connection between the Web browser and the iFolder Web Admin application. This enables a secure SSL channel between the two.
iFolder Server URL	Specify the host or IP address of the iFolder Enterprise Server to be used by the iFolder Web Admin application. This Web Admin application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server.
Redirect URL	Specify the redirect URL for iChain or AccessGateway. This URL is used for the proper logout of iFolder Web Admin console and iChain or AccessGateway sessions.
Require Server SSL	Skip this option to apply the default value.

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

7.5 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 2.7. 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 7.5.1, “Prerequisites,” on page 77
- Section 7.5.2, “Installing a Plug-In When RBS Is Not Configured,” on page 78
- Section 7.5.3, “Installing a Plug-In When RBS Is Configured,” on page 78

7.5.1 Prerequisites

Novell iManager 2.7

If you have not already done so, install Novell iManager 2.7 on the same or different server as your iFolder server. For information, see *Novell iManager 2.7 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)

7.5.2 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 *Plug-in 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 Apache server by entering the following command at the terminal console:

   ```
   /etc/init.d/apache2 restart
   ```
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 7.7, "Accessing iManager and the Novell iFolder Web Admin," on page 87.
8. Continue with Section 7.8, "Provisioning Users and iFolder Services," on page 89.

7.5.3 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 *Plug-in 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 Apache server by entering the following command at the terminal console:

   ```
   /etc/init.d/apache2 restart
   ```
7. Click the *Configure* icon.
8. Under *Role-Based Services*, select *RBS Configuration*.

   The table on the Collections tabbed page displays modules ready to update.
9. 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.
10. Select the *iFolder iManager Module* plug-in.
11. Click *Update*.
12. Wait for the Completed message, then click *OK* to continue.
13. 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 7.7, “Accessing iManager and the Novell iFolder Web Admin,” on page 87.

7.6 Recovery Agent Certificates

The Recovery agent is a trustworthy organizations that issue and sign public key certificates. This organization should be an entity independent of entities owning the iFolder server's infrastructure, or, independent of the IT department if deployed in a corporate environment.

Recovery agent certificates are the public key certificates used for encrypting the data encryption key. The user selects one of these certificates to perform the data key encryption for later key recovery. The supported certificate formats are `*.cer` and `*.der(X.509).`

You can use the self-signed certificates if the iFolder is deployed in a trusted environment.The certificates are generated by using the YaST CA Management plug-in or OpenSSL tools.

- Section 7.6.1, “Understanding Digital Certification,” on page 80
- Section 7.6.2, “Creating a YaST-based CA,” on page 81
- Section 7.6.3, “Creating Self-Signed Recovery Certificates Using YaST,” on page 83
- Section 7.6.4, “Exporting Self-Signed Certificates,” on page 85
- Section 7.6.5, “Exporting Self-Signed Private Key Certificates For Key Recovery,” on page 86
- Section 7.6.6, “Using KeyRecovery to Recover the Data,” on page 86

7.6.1 Understanding Digital Certification

To protect user data from access by unauthorized people, the user data is encrypted by using keys that always occur in private and public key pairs. The keys are applied to the user data in a mathematical process, producing an altered data record in which the original content can no longer be identified.

Private Key: The private key must be kept safely by the key owner. Accidental publication of the private key compromises the key pair and can also be a security threat. The private key is either held by the Recovery agent or the user.

Public Key: The key owner circulates the public key for use by third parties.

Certified Authority (CA): The public key process is popular and there are many public keys in circulation. Certified Authorities are the trustworthy organizations that issue and sign public key certificates. The CA ensures that a public key actually belongs to the assumed owner. The certificates that a CA holds contain the name of the key owner, the corresponding public key, and the electronic signature of the person or entity issuing the certificate. The iFolder Recovery Agents are examples of one kind of CA.

Public Key Infrastructure (PKI): Certificate authorities are usually part of a certification infrastructure that is also responsible for the other aspects of certificate management, such as publication, withdrawal, and renewal of certificates. An infrastructure of this kind is generally referred to as a Public Key Infrastructure or PKI. One familiar PKI is the X.509 Public Key Infrastructure (PKIX). The security of such a PKI depends on the trustworthiness of the CA certificates. To make certification practices clear to PKI customers, the PKI operator defines a certification practice statement (CPS) that defines the procedures for certificate management. This should ensure that the PKI issues only trustworthy certificates.

X.509 Public Key Infrastructure: The X.509 Public Key Infrastructure is defined by the IETF (Internet Engineering Task Force) that serves as a model for almost all publicly-used PKIs today. In this model, authentication is made by certificate authorities (CA) in a hierarchical tree structure. The root of the tree is the root CA, which certifies all sub-CAs. The lowest level of sub-CAs issue user certificates. The user certificates are trustworthy by certification that can be traced to the root CA.

X.509 Certificate: An X.509 certificate is a data structure with several fixed fields and, optionally, additional extensions. The fixed fields mainly contain the name of the key owner, the public key, and the data such as name and signature relating to the issuing CA. For security reasons, a certificate should only have a limited period of validity, so a field is also provided for this date. The CA guarantees the validity of the certificate in the specified period. The CPS usually requires the issuing CA to create and distribute a new certificate before expiration. The extensions can contain any additional information. An application is only required to be able to evaluate an extension if it is identified as critical. If an application does not recognize a critical extension, it must reject the certificate. Some extensions are only useful for a specific application, such as signature or encryption.

Table 7-1 *X.509v3 Certificate*

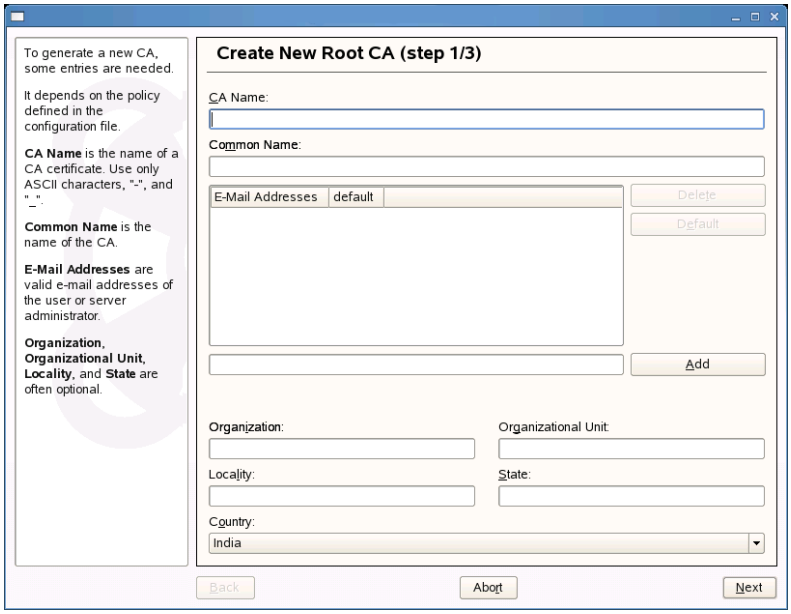
Field	Content
Version	The version of the certificate, for example, v3
Serial Number	Unique certificate ID (an integer)

Field	Content
Signature	The ID of the algorithm used to sign the certificate
Issuer	Unique name (DN) of the issuing authority (CA)
Validity	Period of validity
Subjectr	Unique name (DN) of the owner
Subject Public Key Info	InfoPublic key of the owner and the ID of the algorithm
Issuer Unique ID	Unique ID of the issuing CA (optional)
Subject Unique ID	Unique ID of the owner (optional)
Extensions	Optional additional information, such as KeyUsage or BasicConstraints

YaST-Based PKI: YaST contains modules for the basic management of X.509 certificates. This mainly involves the creation of CAs and their certificate. YaST provides tools for creating and distributing CAs and certificates, but cannot currently offer the background infrastructure that allow continuous update of certificates and CRLs. To set up a small PKI, you can use the available YaST modules. However, you should use commercial products to set up an official or commercial PKI.

7.6.2 Creating a YaST-based CA

1. Start YaST and go to *Security and Users* > *CA Management*.
2. Click *Create Root CA*.



3. Enter the information for creating the CA in the dialog boxes. The following table summarizes the decisions you make.

CA Settings	Description
CA Name	Enter the technical name of the CA. Because the Directory names, among other things, are derived from this name, you must use only the characters listed in the help. The technical name is also displayed in the overview when the module is started.
Common Name	Enter the name of the CA.
E-Mail Address	You can enter several e-mail addresses that a CA user can see. This is helpful for inquiries.
Country	Select the country where the CA is operated.
Organization, Organizational Unit, Locality, State	Optional Values.

4 Click *Next*.

5 Enter a password in the second dialog. This password is always required when using the CA for generating certificates. The following table summarizes the decisions you make.

CA Settings	Descriptions
Password	Specify a password with a minimum length of five characters. To confirm, re-enter it in the next field.
Key Length (bit)	Select the key length of minimum value of 512 and a maximum value of 2048.
Valid Period (days)	The Valid Period in the case of a CA defaults to 3650 days (roughly ten years). This long period makes sense because the replacement of a deleted CA involves an enormous administrative effort.
Advanced Options	Advanced Options are very special options.
	WARNING: If you change these options, iFolder cannot guarantee that the generated certificate works correctly. Clicking Advanced Options opens a dialog for setting different attributes from the X.509 extensions. These values have rational default settings and should only be changed if you are really sure of what you are doing.

YaST displays the current settings for confirmation.

6 Click *Create*.

The root CA is created then appears in the overview.

7.6.3 Creating Self-Signed Recovery Certificates Using YaST

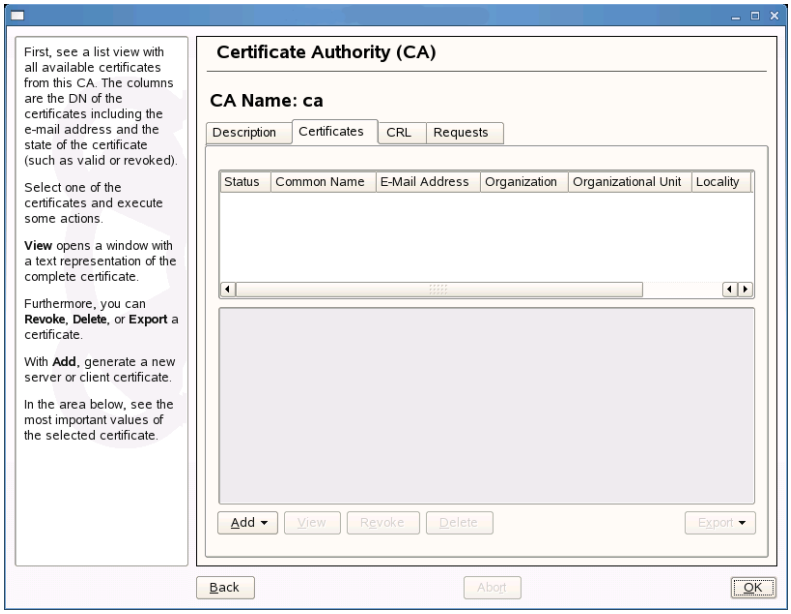
iFolder key recovery mechanism uses the X509 certificates to manage the keys. You can either get a certificate from an external Certified Authority, for instance Verisign* or generate a self-signed certificate if deployed in a trusted environment, where a trusted user-admin relationship exists.

NOTE: In certificates intended for e-mail signature, the e-mail address of the sender (the private key owner) should be contained in the certificate to enable the e-mail program to assign the correct certificate. For certificate assignment during encryption, it is necessary for the e-mail address of the recipient (the public key owner) to be included in the certificate. In the case of server and client certificates, the hostname of the server must be entered in the Common Name field. The default validity period for certificates is 365 days.

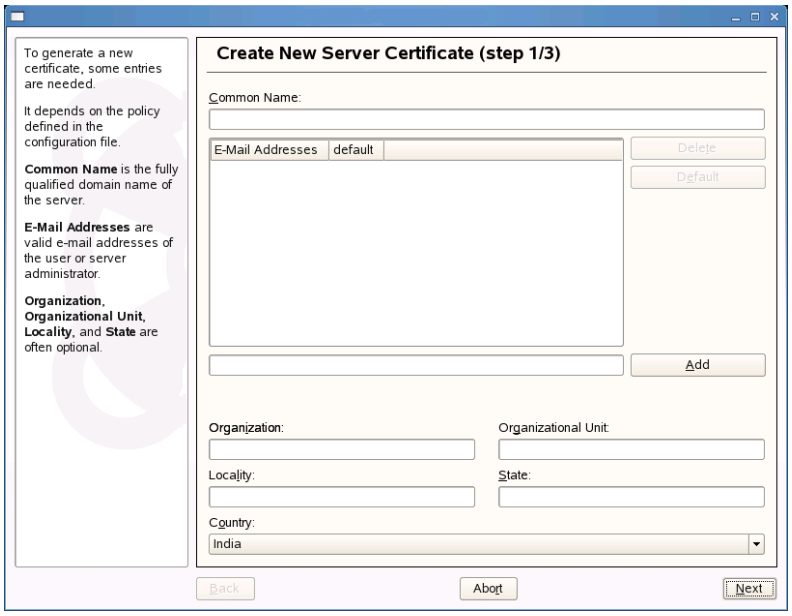
This section discusses creating self-signed certificates for encryption and self-signed key certificate for key recovery using YaST.

1. Start YaST and go to *Security and Users* > *CA Management*.
2. Select the required CA and click *Enter CA*.
3. Enter the password for the CA if asked for.

   YaST displays the CA key information in the Description tab.
4. Click Certificates tab.



5. Click *Add* > *Add Server Certificate*.



6 Enter the information for creating the certificates in the dialog boxes. The following table summarizes the decisions you make.

CA Settings	Description
Common Name	Enter the name of the CA.
E-Mail Address	You can enter several e-mail addresses that a CA user can see. This is helpful for inquiries.
Country	Select the country where the CA is operated.
Organisation, Organisational Unit, Locality, State	Optional Values.

7 Enter a password in the second dialog.The following table summarizes the decisions you make.

CA Settings	Descriptions
Password	Specify a password with a minimum length of five characters. To confirm, re-enter it in the next field.
Key Length (bit)	Select the key length of minimum value of 512 and a maximum value of 2048. iFolder supports only 512, 1024 and 2048 as the key length.
Valid Period (days)	The Valid Period in the case of a CA defaults to 3650 days (roughly ten years). This long period makes sense because the replacement of a deleted CA involves an enormous administrative effort.

CA Settings	Descriptions
Advanced Options	Advanced Options are very special options. **WARNING:** If you change these options, iFolder cannot guarentee that the generated certificate works correctly. Clicking Advanced Options opens a dialog for setting different attributes from the X.509 extensions. These values have rational default settings and should only be changed if you are really sure of what you are doing.

YaST displays the current settings for confirmation.

7.6.4 Exporting Self-Signed Certificates

1 Click Export drop-down and select *Export to File*.

2 Select *Only the Certificate in PEM format*.

3 Specify a password of minimum length of five characters.

4 Specify a filename for the certificate you have created and click Browse to find a loacation to save the file.

5 Click *OK* to save the certificate.

6 Convert the certificate in PEM format to DER format using OpenSSL command as given below:

```
openssl x509 -in <certificate>.pem -inform PEM -out
<certificate>.der -outform DER
```

7 Copy the certificate in DER format to the location you have configured for loading Recovery Agent Certificate during iFolder configuration.

If the certificate is expired, you need to load the new certificates again to this location.

For more information on this, see “Path to the Recovery Agent Certificates (optional):” on page 61.

8 Restart the iFolder server to load the Recovery agent certificates.

7.6.5 Exporting Self-Signed Private Key Certificates For Key Recovery

1 Click Export drop-down and select *Export to File*.

2 Select *Certificate and the Key in PKCS12 Format*.

3 Specify a new password and re-enter that for confirmation.

This password is used with the certificate and the keys exported to a file in XML format.

IMPORTANT: You must use a password different from the one you have used for certificate creation.

---

4 Specify a filename for the certificate you have created and click Browse to find a location to save the file.

5 Click *OK* to save the certificate.

7.6.6 Using KeyRecovery to Recover the Data

Each iFolder has a unique data encryption key which is auto-generated during iFolder creation. The key is encrypted by using a passphrase provided by individual user and also by using the public key with the Recovery agent. If the user forget the secret passphrase, he or she cannot access either the iFolder data or the encrypted key used for recovering it unless the passphrase is saved locally (enabling Remember passphrase). To avoid this problem, user export the keys using the *Security > Export Keys* option in the client and send it manually to the Recovery agent using the e-mail address provided in the Export dialog box in the client GUI. The Recovery agent retrieves the keys and sends back to the user through e-mail or any other communication channel. User can then import the keys and use them to reset the passphrase.

NOTE: The keys are exported to a file in XML format. It is recommended to save the file as `<filename>.xml`

This section help you understand the process followed by a Recovery agent to retrieve the key.

1 Go to the location where iFolder is installed.

Platorm	Default Location of the Utility
Linux	`/opt/novell/ifolder3/KeyRecovery`
Windows	`C:/Program Files/iFolder/KeyRecovery.exe`

2 Run `KeyRecovery` or `KeyReovery.exe` based on the platform you use and follow the on-screen instructions.

The following table summarizes the decisions you make.

Parameters	Description
Encrypted Key file path	Specify the path (including the file name of the encrypted key) for reading the encrypted keys.
Private Key	Specify the path to the private key file (PKCS12 file format, *.p12).
Decrypted Key file path	Specify the path to store the decrypted key file. Ensure that the filename also included in the path you specify.
Private Key password	Specify the password to decrypt the private key.
Encrypt Result key	Specify whether you want to encrypt the decrypted key with one time passphrase. Default value: Yes
One time passphrase	Specify a one time passphrase to encrypt the decrypted keys.

3 Send the decrypted key usually by replying to the mail attached with the encrypted keys and the one-time passphrase (if the key is encrypted using the one-time passphrase) to the user.

4 Send the one-time passphrase (if the key is encrypted using the one-time passphrase) to the user through any other communication channel other than the one you used to exchange the key files.

7.7 Accessing iManager and the Novell iFolder Web Admin

The Novell iFolder Web Admin is the tool used to manage your iFolder server.

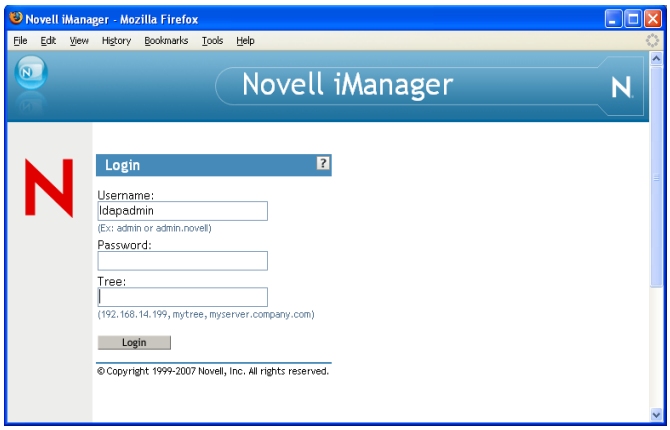
1 Open a Web browser to the iManager Login page by entering the following location:

`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 3.6 or iFolder 3.6 Web Access.

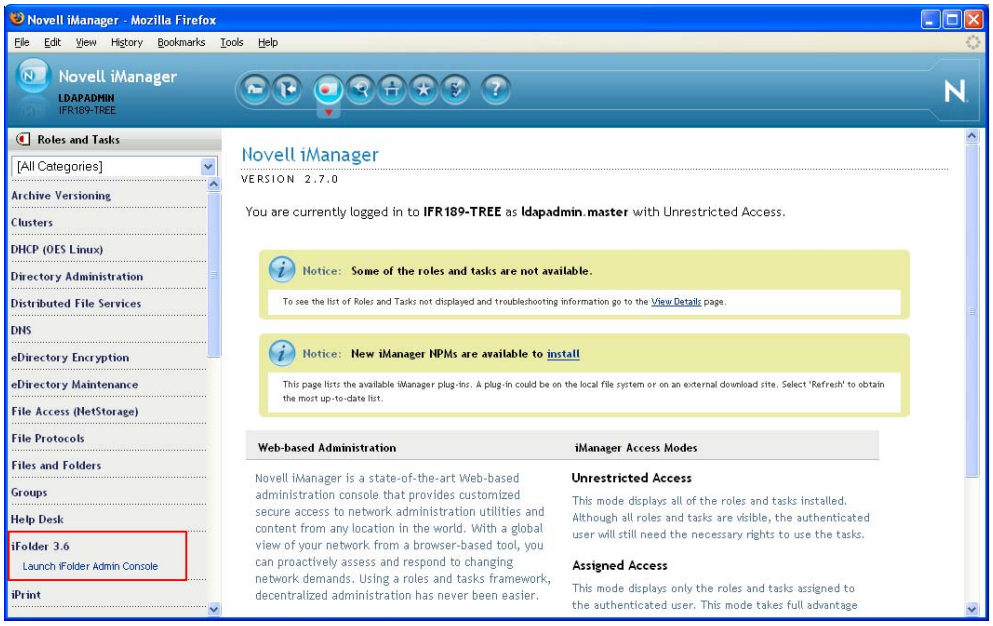
2 (Conditional) If prompted to accept the server's certificate, review the certificate information, then click *OK* to accept it if it is valid.

3 On the iManager Login page, specify the Admin username and password you created during the OES 2 Linux install, then click *Login*.



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.



4 In Roles and Tasks, click *iFolder 3.6* > *Launch Admin Console*.

5 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`.

6 Do one of the following:

6a If you logged in to iManager with the same username as the iFolder Admin user of the Web Admin, select Authenticate Using Current iManager Credentials.

6b If you logged in to iManager with a different username than the iFolder Admin user of the Web Admin, leave the check box Authenticate Using Current iManager Credentials unselected, then specify the iFolder Admin username and password.

7 Click *OK*.

IMPORTANT: If you are logged in to iManager with iManager admin credential, iFolder Web Admin does not ask the credentials again for logging into Web Admin console.

For information, see Section 9.2, “Connecting to the iFolder Server,” on page 110.

Novell iFolder 3.6 opens to the User page, which consists of a tabbed list of the main administrative functions that can be performed on iFolder domain.

7.8 Provisioning Users and iFolder Services

After you configure your Novell iFolder 3.6 enterprise server, you must specify containers and groups as Search DNs in the LDAP settings. iFolder uses these to provision user accounts. You can provision users and iFolders through iFolder Web Admin console. For more information, see the following:

- Chapter 9, “Managing iFolder Services via Web Admin,” on page 109
- Chapter 10, “Managing iFolder Users,” on page 123
- Chapter 11, “Managing iFolders,” on page 131

7.8.1 Prerequisites

Users and LDAP Contexts

The contexts you plan to use as LDAP 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 8.8 Administration Guide* (http://www.novell.com/documentation/edir88/treetitl.html).

7.9 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 3.6 Welcome page.

NOTE: iFolder 3.6 does not support a silent install (that is, a scriptable non-interactive install) on any platform. A silent install is possible the Linux client using its `.rpm` files, but it is not supported.

- Section 7.9.1, “Accessing the OES 2 Linux Welcome Page,” on page 90
- Section 7.9.2, “Downloading the iFolder Client,” on page 90
- Section 7.9.3, “Installing the iFolder Client,” on page 91

7.9.1 Accessing the OES 2 Linux Welcome Page

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

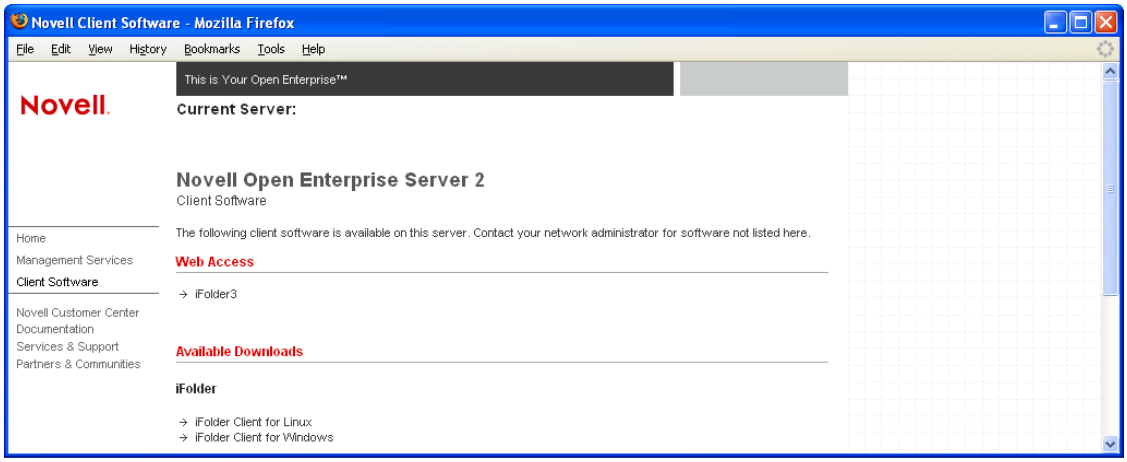
`http://ifolder3.example.com`

Replace *`ifolder3.example.com`* with the DNS name or the IP address (such as *`192.168.1.1`*) of the OES 2 Linux server.

7.9.2 Downloading the iFolder Client

On the OES 2.0 Welcome page, users can select one of the following client links from the *Client Software* page under *Available Downloads* to download the install files for the iFolder client for Novell iFolder 3.6:

Figure 7-1 *Client Download*



Users can download the following install files:

Link Name	Operating System	Filename
iFolder Client for Linux	Suse Linux Enterprise Desktop 10 and later	`ifolder3-linux.tar.gz`
iFolder Client for Windows	Windows XP	`ifolder3-windows.exe`

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	ifolder3-3.6.0.xxxx-1-2.1.i586.rpm nautilus-ifolder-3.6.0.xxxx-1-2.1.i586.rpm simias-1.6.0.xxxx-1-2.1.i586.rpm xsp-1.2.1-13.8.noarch.rpm
iFolder for Windows	`ifolder3-windows.exe`

7.9.3 Installing the iFolder Client

For information about prerequisites and installation, see "Getting Started" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

7.10 Updating Novell iFolder 3.6

As patches become available for iFolder 3.6 and the iFolder client, they are delivered to the OES Patch channel. Any iFolder server or client patches or updates can be installed through 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 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.

7.11 Updating Mono for the Server and Client

You can upgrade the Mono packages available in the SUSE distribution through Mono upgrade channel unless otherwise the iFolder Administrator guide specifies a particular version. For both server and client XSP RPMs must be atleast 1.1.18 or later.

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 3.6 Documentation Web site (http://www.novell.com/documentation/ifolder3).

7.12 Uninstalling the iFolder 3.6 Enterprise Server

Use YaST to uninstall the iFolder 3.6 enterprise server `.rpm` file. Uninstalling iFolder 3.6 software does not remove the Simias store, including the config files available in the `/etc/apache2/conf.d`.

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.

7.13 What's Next

You have now installed and configured your Novell iFolder 3.6 enterprise server and provisioned iFolder services for users. To set up system policies for iFolder services, continue with Chapter 9, "Managing iFolder Services via Web Admin," on page 109.

Provisioned iFolder users can install the Novell iFolder 3.*6* client on their workstations, create iFolders, and share iFolders with other authorized Novell iFolder users. For information, see the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

Managing an iFolder Enterprise Server

8

This section describes how to manage your Novell® iFolder® 3.6 enterprise server on Novell Open Enterprise Server platform.

- Section 8.1, “Starting iFolder Services,” on page 93
- Section 8.2, “Stopping iFolder Services,” on page 93
- Section 8.3, “Restarting iFolder Services,” on page 93
- Section 8.4, “Managing the Simias Log and Simias Access Log,” on page 94
- Section 8.5, “Backing Up the iFolder Server,” on page 95
- Section 8.6, “Backing Up the iFolder Store with the TSAIF,” on page 96
- Section 8.7, “Recovering from a Catastrophic Loss of the iFolder Server,” on page 102
- Section 8.8, “Recovering Individual Files or Directories,” on page 103
- Section 8.9, “Moving iFolder Data from One iFolder Server to Another,” on page 104
- Section 8.10, “Changing The IP Address For iFolder Services,” on page 105
- Section 8.11, “Securing Enterprise Server Communications,” on page 106

8.1 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 terminal console:

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

8.2 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 terminal console:

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

8.3 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 terminal console:

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

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

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

8.4 Managing the Simias Log and Simias Access Log

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

- **Simias Log:** The `/simias/log/Simias.log` file contains status messages about the health of the Simias Service.
- **Simias Access Log:** The `simias/log/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="<iFolder Data>/simias/log/Simias.log">` `<file value="<iFolder Data>/simias/log/Simias.access.log" />`
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" />`

Parameters	Description	Examples
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 pattern delimited (`**`) by default. Use this pattern to add additional fields.	`<header value="#version: 1.0
#Fields:**date* *time**method**status**user* *uri**id**
" />`

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.

8.5 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

     You can find the default location of the Simias store directory under *Data Store* section in the *Server Details* page of the Web Admin console.

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

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

8.6 Backing Up the iFolder Store with the TSAIF

The Target Service Agent (TSA) for Novell iFolder 3.6 supports the back up of the iFolder store.

- Section 8.6.1, “Understanding TSAIF,” on page 96
- Section 8.6.2, “Syntax,” on page 97
- Section 8.6.3, “iFolder Path Options,” on page 97
- Section 8.6.4, “iFolder Path Examples,” on page 99
- Section 8.6.5, “SMSConfig Options,” on page 99
- Section 8.6.6, “TSAIF and SMSConfig Examples,” on page 100
- Section 8.6.7, “NBackup Options,” on page 100
- Section 8.6.8, “TSAIF and NBackup Examples,” on page 101
- Section 8.6.9, “Additional Information,” on page 102

8.6.1 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 Web Admin console or Web Access console.

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.

8.6.2 Syntax

At an OES Linux server terminal console, enter

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

The `-l` 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.

8.6.3 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.

8.6.4 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.

To backup and restore individual or group of files or subdirectories, use the backup engine-supported file filters. These file filters perform the include or exclude operations for selective backup and restore.

8.6.5 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.

Option	Command
`--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.

8.6.6 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%.

8.6.7 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.

Option	Command
`--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.

The back-up administrator should use root or root-equivalent system user for bothe back-up and restore.

8.6.8 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`

Backup or Restore Task	Command
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`
Owner restore from the full backup file `full.sidf`	`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.
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`

8.6.9 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)`.

8.7 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/simias/data/simias`.
4. Use your normal iFolder system restore procedures to restore the following data to its original locations:
   - Simias store directory

     The default location is `/var/simias/data/simias`.

     IMPORTANT: Be careful not to modify anything else under the Simias store directory.
5. Start the iFolder server by entering the following command as root user:

   ```
   /etc/init.d/apache2 start
   ```
6. Notify users that they can return their saved files to their iFolders for upload to the server. Users should coordinate this with other shared members of the iFolder to avoid competing updates.

8.8 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, select *iFolder 3.6 > Launch iFolder Admin Console*, then wait for the page to refresh.

4 If prompted, connect to the iFolder domain by entering iFolder Admin user credentials as needed to launch the Web Admin console.

5 On the 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/simias/data/simias/SimiasFiles/06/62ba1844-6987-47fc-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 web admin, select *iFolders*, search for the iFolder you want to manage, and then click the 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 3.6 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.

8.9 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 system.

1 Notify users that the iFolder server is going down.

2 Stop iFolder services. As a root user, enter the following command at the terminal 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/simias/data/simias`.

- Apache config files for iFolder

The default location is `/etc/apache2/conf.d` and contain the following files:

- `simias.conf`
- `ifolder_admin.conf` (if available)
- `ifolder_web.conf` (if available)

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/simias/data/simias`.

6 On the target server, copy the apache config files for iFolder to `/etc/apache2/conf.d` if it is not already available.

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

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

8 Notify users that the server is back up.

9 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.

NOTE: This procedure is not applicable for the iFolder 2.*x* servers.

8.10 Changing The IP Address For iFolder Services

When you change the Novell OES 2 server IP address either through YaST or through command line, it does not automatically change the iFolder Service IP address. You can change the iFolder service IP address only by reconfiguring the iFolder service either through YaST or command line. When you reconfigure the iFolder services, you must ensure that the current data Store path is not changed. Changing the IP address of the Novell iFolder service also needs the Apache service to be restarted. Follow the steps given below to change the IP address through CLI.

1 Open a terminal console and enter `rcapache2 stop`.

2 Run `/opt/novell/ifolder3/bin/simias-server-setup.`

3 Specify the `Store path`.

  The default Store path is `/var/simias/data/simias`.

4 Specify the new Private IP address and Public IP address.

IMPORTANT: Ensure that the users are notified about the new IP address for connection.

---

5 For the rest of the options, accept the default values because these values are from the existing configuration.

6 Start Apache service by executing `rcapache2 start`.

8.11 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 8.11.1, “Using SSL for Secure Communications,” on page 106
- Section 8.11.2, “Configuring the SSL Cipher Suites for the Apache Server,” on page 106
- Section 8.11.3, “Configuring the Enterprise Server for SSL Communications with the LDAP Server,” on page 107
- Section 8.11.4, “Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server,” on page 108
- Section 8.11.5, “Configuring an SSL Certificate for the Enterprise Server,” on page 108

For information about configuring SSL traffic for the iFolder Web access server, see Section 12.5, “Securing Web Access Server Communications,” on page 141.

8.11.1 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	No	Yes	No	yes

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.

8.11.2 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.

8.11.3 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. Login to Web Admin.

   For more information, see Section 9.1, “Accessing the Novell iFolder Web Admin,” on page 109
2. Click Server in the Web Admin to open Server page.
3. On the Server page, use the search tool to locate the server.
4. Click the Server's name link to open the Server Details page to the Servers page.
5. Select *Yes* from LDAP SSL drop-down to enable LDAP SSL communication.

8.11.4 Configuring the Enterprise Server for SSL Communications with the Web Access Server and Web Admin Server

By default, the iFolder enterprise server is configured to communicate via SSL with the iFolder Web Access server/ Web Admin server. For most deployments, this setting should not be changed. If the iFolder deployment is small and the Web Access server/ Web Admin 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 or Web Admin server's settings for SSL traffic. For information, see Section 12.5.3, "Configuring the Web Access Server for SSL Communications with the Enterprise Server," on page 142.

8.11.5 Configuring an SSL Certificate for the Enterprise Server

For information, see "Managing SSL Certificates for Apache" on page 153.

Managing iFolder Services via Web Admin

9

This section discusses how to manage services for the Novell® iFolder® 3.6 enterprise server by using iFolder Web Admin Console.

- Section 9.1, “Accessing the Novell iFolder Web Admin,” on page 109
- Section 9.2, “Connecting to the iFolder Server,” on page 110
- Section 9.3, “Accessing iFolder Web Admin Via OES Welcome Page,” on page 111
- Section 9.4, “Managing Web Admin Console,” on page 112
- Section 9.5, “Managing the iFolder System,” on page 113
- Section 9.6, “Managing iFolder Server For a Multi-Server Setup,” on page 118

9.1 Accessing the Novell iFolder Web Admin

Use the Novell iFolder Web Admin to manage the iFolder system, user accounts, and iFolders.

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 LDAP Search DNs.

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

4 Continue with Section 9.2, “Connecting to the iFolder Server,” on page 110.

9.2 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 servers 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. Log in with the iFolder Admin username and password for the target server.

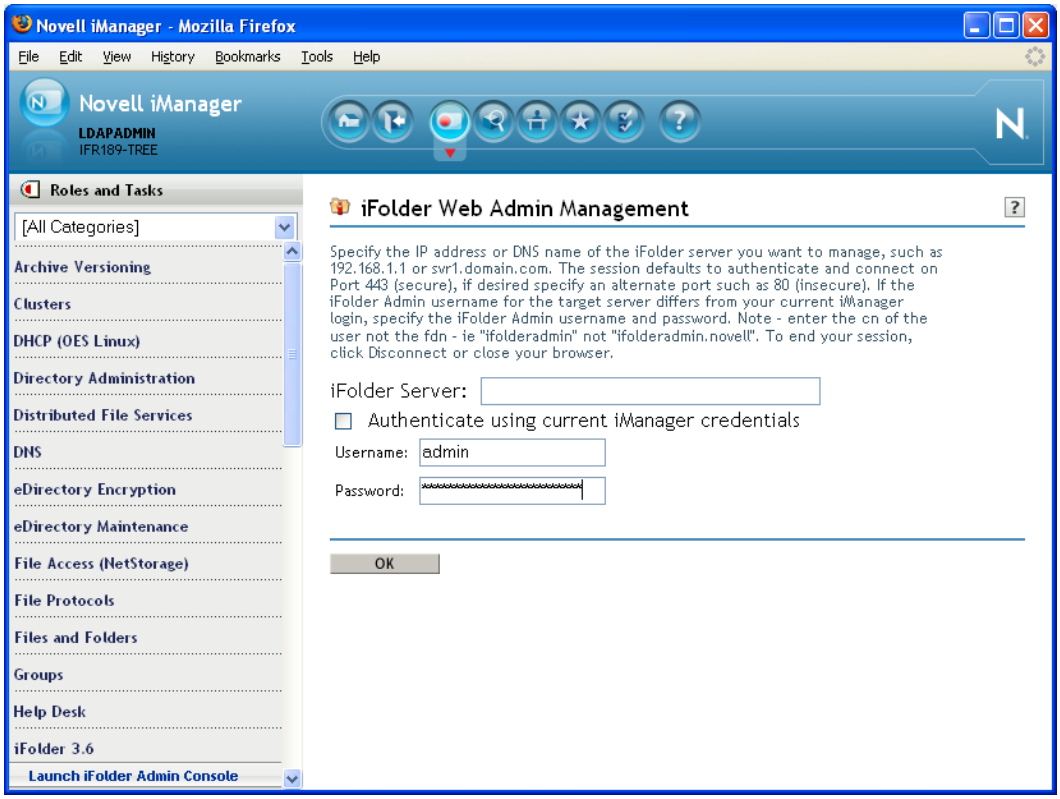
NOTE: You cannot manage Novell iFolder 2.*x* servers with the Novell iFolder 3 Web Admin.

To connect to the iFolder server you want manage:

1. If you are not logged in to iManager, log in to iManager in a Web browser.

   For information, see Section 9.1, "Accessing the Novell iFolder Web Admin," on page 109.

2. In *Roles and Tasks*, expand the *iFolder 3.6* role and click *Launch iFolder Admin Console* to launch iFolder Web Admin Management page.



IMPORTANT: Web Admin console does not appear unless you disable the pop up blocker.

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 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.

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

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

Based on the above selection, you are directed to the Web Admin users page.

7 Continue with Section 9.4, "Managing Web Admin Console," on page 112.

When you are done managing the iFolder server, click *logout* (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.

9.3 Accessing iFolder Web Admin Via OES Welcome Page

You can access the iFolder Web Admin through the OES 2.0 Welcome page.

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

`https://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 3.6 enterprise server where you have an account. Ask your iFolder Administrator for this information.

2 In the left navigator, click *Management Services*.

3 Click *iFolder 3* to open the Web Admin login page.

4 Specify the iFolder Admin username and password and continue with Step 5.

9.4 Managing Web Admin Console

With Web Admin console you can manage iFolder users, the iFolder system, servers, iFolders, and the iFolder statistics report. In Web Admin console by default the *Users* page opens to the *Users* tab.

Users Page

1 The *Users* tab displays the user's type (Admin user or user), username, user's full name (if available), the server to which the user is provisioned, and the user status (Enabled or Disabled).

2 Use the search tool to locate the user whose iFolder account you want to manage.

3 Click the user's name link to open the User Details page.

The User page opens to the Users tab, which displays the user details, iFolders owned, and shared and policy settings for this particular user account. For more information, see Chapter 10, "Managing iFolder Users," on page 123.

Accessing the iFolders Page

1 In the Web Admin console, click the *iFolders* tab.

iFolders tab displays the iFolder type (Admin user or user), iFolder name, iFolder owner, members, the date the iFolder was last modified.

2 Use the search tool to locate the iFolder you want to manage.

3 Click the iFolder's link to open the iFolder Details page to the iFolder tab.

The iFolder Details page displays the iFolder details, list of members who own or share the iFolders and policy settings for this particular iFolder.

Accessing Systems Page

1. In the Web Admin console, click the *Systems* tab.

   The Systems page displays the system settings and list of iFolder Administrators.

2. Locate the iFolder Administrator you want to manage. You can add or delete iFolder Administrator.

   You can also manage the policy settings for the Admin user.

3. Click the Admin user's Name link to open the User Details page.

   The User Details page opens to the Users tab, which displays the user details, iFolders owned, and shared and policy settings for this particular user account. For more information, see Section 9.5.1, “Viewing and Modifying iFolder System Information,” on page 113.

Accessing Servers Page

1. In the Web Admin console, click the *Servers* tab.
2. Use the search tool to locate the Server you want to manage.
3. Click the Server name link to open the Servers Details page.

   The Server Details page opens to the Servers tab, which displays server details, server status, server logs, and server reports, and to set the log level.

Accessing Reports Page

1. In the Web Admin console, click *Reports* tab.
2. Configure reporting according to the frequency and time schedule you want, then generate the output as desired.

9.5 Managing the iFolder System

This section discuss how to manage the iFolder 3.6 services for a selected server.

- Section 9.5.1, “Viewing and Modifying iFolder System Information,” on page 113
- Section 9.5.2, “Configuring iFolder Administrators,” on page 114
- Section 9.5.3, “Configuring System Policies,” on page 115

9.5.1 Viewing and Modifying iFolder System Information

1. In Web Admin Console, System page opens to the System tab to view and modify the following information:

Parameter	Description
Name	The name assigned to the iFolder domain. To edit the name of the iFolder domain, enter the new name and click Save. To cancel the changes made, click Cancel.
Description	A short description about the iFolder Domain. To edit the system description, enter the new description and click Save. To cancel the changes made, click Cancel.
Total Users (view only)	Reports the total number of users in the iFolder domain.
Total iFolders (view only)	Reports total number of iFolders that belongs to the iFolder domain.

9.5.2 Configuring iFolder Administrators

This section discusses the following:

- “Understanding the iFolder Admin User” on page 114
- “Viewing the Admin User Details” on page 115
- “Granting iFolder Admin Right to a User” on page 115
- “Removing the iFolder Admin Right for a User” on page 115

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 7.2, “Deploying iFolder Server in a Multi-server Environment,” on page 58.

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 User page in the Web Admin console 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.

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.

Viewing the Admin User Details

The System page displays the following iFolder Admin details for the iFolder domain.

Parameter	Description
Type	Displays the Admin user icon.
User Name	The username assigned to the Admin user account, such as jsmith or john.smith@example.com.
Full Name	The first and last name of the Admin user account.

To view or edit Admin user details, click the Admin user link to open the User Details page. The User Details page displays the iFolders owned or shared by the user. Click the *All* tab to list all the iFolders, both owned and shared. To view the iFolder owned by the user, click the *Owned* tab. *Shared* tab lists all the shared iFolders for this particular user account. You can also change the policy settings for the selected Admin user.

Granting iFolder Admin Right to 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 the System page, click *Add* to open a list of iFolder Admin users.
2. Search for the user you want to grant Admin rights.
3. Select the *User* check box next to the user, then click *Add*.

   The username is added in the list of users with the iFolder Admin right. You can assign the iFolder Admin right to multiple users.

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 System page, locate the Admin user you want to delete.
2. Click Delete to remove iFolder Admin right from the selected user.

9.5.3 Configuring System Policies

Use the System Policies page to manage system-wide policies.

Viewing the Current System Policies

The following table lists the system policies you can manage for any given iFolder System. Click *Save* to apply the modifications.

Parameter	Description
Disk Quotas	The total combined administrative size (in MB) of space allocated for use by all 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.
File Size	Specifies the maximum file size (in MB) that iFolder system is allowed to synchronize.
Excluded Files	Specifies a list of file types to include or to exclude from synchronization for all iFolders on the system. For example, to block all `.mp3` files you need to specify `*.mp3`.
Synchronization	If this option is enabled, specifies the minimum interval (in minutes) for synchronizing iFolder data for the system. 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.
Encryption	Specifies the encryption policy for the iFolder system. System-wide settings supersede user policies.

Modifying iFolder System Policies

1 Select the policy, specify values for the policy, then click *Save* to apply it:

Click *Cancel* to cancel the changes.

Parameter	Description
Disk Quota	Select the check box to enable a system-wide quota, then specify the total space quota (in MB) for the current iFolder domain. Deselect the check box to disable a system-wide quota. 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
File Size	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. 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
Excluded Files	Specify whether to restrict file types that are synchronized by exclusion filters. Type a file extension, then click *Add* to add it to the list. You can only add or delete file extensions; subsequent editing is not allowed on the entries.
Synchronization	To enable a policy, select the check box, then specify the minimum synchronization interval in minutes. 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: Disabled 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.
Encryption	Select *On* to enable the encryption feature for the iFolder system. This permits a user to set an encryption policy for his or her iFolders. Select *Enforced* to enable the encryption feature for all users. When it is set to Enforced, a user cannot change the encryption settings for his or her iFolders.

9.6 Managing iFolder Server For a Multi-Server Setup

This section describes how to manage a iFolder server for a multi-server setup.

IMPORTANT: You cannot change the settings of any server from the Web Admin page of a different server.

9.6.1 Searching For Servers

The search tool help you locate the server you want to manage.

1. In Web Admin, ensure that you are on Servers page.

   If you are not, click the Servers tab to open the Servers page.
2. Select a filter criterion (Contains, Begins With, Ends With, Equals).
3. Use one or more of the following search methods, then click Search:
   - Type the name of the server in the Search Servers field.
   - Type one or more letters in the Search Servers field.
   - Type an asterisk (*) in the Search Servers field to return a list of all Servers on the system.
   - Leave the Search Servers field empty to return a list of all Servers on the system.

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

Scroll up and down to browse the search results and locate the Server you want to manage.

Accessing and Viewing the Server Details Page

Follow the steps given below:

1. On the Server page, use the search tool to locate the server.
2. Click the Server's name link to open the Server Details page to the Servers page.
3. View the following server informations:

Parameter	Description
Name	The name assigned to the iFolder enterprise server.
Type	The host portion of the DNS name of the server. For example, in *`if3svr.example.com`*, *`if3svr`* is the host name.
DNS Name	For example: *192.168.1.1* or *svr1.domain.com*
Public URL	The public IP address corresponding to the iFolder server.
Private URL	The private URL corresponding to the iFolder server. This allows communication between the servers within the iFolder domain. The private URL and the public URL can be the same.

4 Select the report from the drop down list to view the detailed statistics about the user activities.

This option is disabled if the Enable Reporting option on the Report page is left unselected.

5 View the following server log information:

Parameter	Description
System	Select System to view the `simias.log` that tracks all the system activities.
User Access	Select User Access to view `simias.access.log` that tracks the user activities on the selected server.

6 Set the log level information for the *System* or for each *User access*.

6a Select the option from the drop-down list for which you want to set the log level information.

System is selected by default.

6b Click View to view the log level information.

Either you can save it to the machine or open with a desired file format.

Parameter	Description
All	Shows all the server activities that help Novell support resolve the issues.
Debug	Shows the server activities that help Novell support debug the issues. .
Info	Shows the basic server activities that help Novell support resolve the issues. This option is selected by default.
Warn	Shows all the potential system errors.
Error	Shows all the system errors that halt system functioning.
Fatal	Shows the fatal system errors.
Off	Logging is turned off.

7 Set the LDAP Details:

Parameter	Description
LDAP Server	Shows LDAP Server address.
Up since	Shows the date and time of the very first synchronization.
LDAP SSL	Allow you to enable or disable LDAP SSL connection.
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.
Cycles	Shows the number of times the synchronization take place.
Identity Sync	Updates iFolder users in the selected iFolder domain from the LDAP information at the interval you select. Specify the time interval in minutes in the Identity Sync field and click Sync Now to start synchronizing iFolder users with the LDAP users.
Delete member grace interval	Specifies the time interval for the iFolder to remove the user information completely from the iFolder server after the user is deleted from LDAP. For example, if you specify 10 minutes as *Delete member grace interval*, iFolder removes all the user information 10 minutes after the deletion of the user from the LDAP. In case the user is removed accidentally from LDAP, you can recover all the user data within the specified period.
LDAP Context	Lists all the LDAP contexts. iFolder searches users only from the listed LDAP contexts.

8 Configure the Data store.

Data Store represents the iFolder storage that can span across multiple volumes (mount points) in a given server. By default every iFolder server has a default store which cannot be disabled. With web interface, you can add and configure multiple Data Store across which iFolder data is load balanced. When the user uploads an iFolder, it check for the Data Store with maximum free space, and stores the iFolder data in that particular Data Store thereby balancing the load. You can add as many Data Store as you want. Having multiple Data Store thus makes it possible to scale the data storage capacity in a large deployment to meet the enterprise-level requirements.

You can view the following data store information:

Parameter	Description
Name	Shows the unique name you have specified for the Data Store.
Full Path	Shows the path to the Data Store, where the volume is mounted on. This is the data path that you have specified while adding the data store using the web interface.
Free Space	Shows the space available in the volume.

Parameter	Description
Enabled	Shows the given Data Store is enabled or not. Default Data Store cannot be disabled.

Enable or Disable DataStore: Select the Data Store you want to disable or enable and click Disable or Enable respectively. When the user uploads an iFolder, disabled Data Stores are always skipped while checking for the maximum free space availability for storing the iFolder data.

To add a new Data Store,

8a Specify the following information:

Name: Assign a unique name to the Data Store, such as ifolder-store.

Path: Enter the path where the new volume is mounted. If it is a remote volume (CIFS, NFS, AFP), then ensure that the volume is mounted on every restart for proper functioning and load balancing. You need to check the permissions of the path specified, and change the ownership to Apache-user (wwwrun).

Accessing and Viewing the Report Page

Use this interface to enable reporting and generate reports for iFolder and Directories.

It generate reports based on the frequency you select.

1. Select Enable Reporting to enable reporting.
2. Select the frequency from the given options (Daily, Weekly, Monthly).
3. Select the time when you want to generate the report.
4. Select the output option from the given options (Report iFolder, Report Directories)
5. Select the format for generating the report.
6. Click *Save* to save the settings.

   Click *Cancel* to cancel the settings.

Managing iFolder Users

10

This section discusses how to manage iFolder users with Novell® iFolder® 3.6 enterprise server.

- Section 10.1, “Provisioning Users for iFolder Services,” on page 123
- Section 10.2, “Searching for a User Account,” on page 123
- Section 10.3, “Accessing And Viewing General User Account Information,” on page 124
- Section 10.4, “Creating an iFolder,” on page 125
- Section 10.5, “Configuring User Account Policies,” on page 125
- Section 10.6, “Enabling and Disabling iFolder User Accounts,” on page 129

10.1 Provisioning Users for iFolder Services

Provisioning a user for iFolder occurs automatically based on the containers and groups you specify as LDAP Search DNs in the LDAP settings. You can specify any existing context. For information, see Section 4.5, “iFolder User Account Considerations,” on page 42.

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). If by mistake user is deleted from the LDAP, you can create that user again with the same FDN within the *Delete member grace interval* so that you can recover the user’s iFolders. For more information on this, see Step 7 on page 119 in the “Accessing and Viewing the Server Details Page” on page 118.

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 LDAP Search DNs before you move the User object in eDirectory.

10.2 Searching for a User Account

1. In Web Admin console, enable the *Users* tab.
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 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.

- **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 Accessing And Viewing General User Account Information

The Web Admin console opens to the User Page which displays the user's type (Admin user or user), username, user's full name (if available), the server to which the user is provisioned and the user status (Enabled or Disabled).

Follow the steps given below to access the Users Details Page:

1. On the iFolder user page, use the search tool to locate the user whose iFolder account you want to manage.
2. Click the user's name link to open the User Details page to the Users tab.

The User Details page will display the following user details for the selected user's iFolder account.

Parameter	Description
User Name	The username assigned to the user account, such as jsmith or john.smith@example.com.
Full Name	The first and last name of the user account.
LDAP Context	The LDAP tree context is used for provisioning users in to iFolder.
Last Login Time	The last time the user logging in to the iFolder system.

The User Details page displays the iFolders owned or shared by the user. Click the *All tab* to list all the iFolders both owned and shared. To view the iFolder owned by the user, click the *Owned* tab. The *Shared* tab lists all the shared iFolders for this particular user account.

10.3.1 Enabling or Disabling an iFolder For an User Account

Follow the steps given below to enable or disable an iFolder for a given user account:

1. Locate the iFolder you want to manage, then select the check box next to the iFolder.
2. Click Enable to enable the iFolder.

   This allows the user to log in and synchronize iFolders.

3 Click Disable to disable the iFolder.

4 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.

10.3.2 Deleting An iFolder

To delete an iFolder:

1 Locate the iFolder you want to delete, then select the check box next to the iFolder.

2 Click *Delete*.

10.4 Creating an iFolder

To create a new iFolder:

1 On the iFolder Users page, click *New*.

The iFolder creation page opens to the iFolders page.

2 Specify the following information and then click *Create*.

Name: Assign a name to the iFolder such as ifolder 1.

Description: A short description about the iFolder.

3 Click *Next* to select additional member for the iFolder.

4 On the Additional member selection page, use the search tool to locate the desired users.

5 Select the users from the search result.

6 Click *Back* to make any changes.

7 Click *Create* to complete the iFolder creation.

10.5 Configuring User Account Policies

- Section 10.5.1, "Viewing the Current User Account Policies," on page 125
- Section 10.5.2, "Modifying User Account Policies," on page 127

10.5.1 Viewing the Current User Account Policies

1 In Web Admin console, select *Users* tab, 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 below Policies:

Parameter	Description
Account	Specifies whether the user is currently allowed to log in to synchronize iFolders. You can select the check box to disable the User login.

Parameter	Description
Disk Quota	**Limit:** Specifies the maximum space allotted on the server for this selected user. **Used:** Specifies the total space currently in use on the server for all iFolders owned by this selected user. **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. **Effective:** Effective space allocated on the server.
File size	Specifies the maximum total space (in MB) that a user's iFolder file 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 file 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.
Excluded files	Specifies to allow all file types or lists the file types 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.

Parameter	Description
Synchronization	Specifies the minimum interval (in minutes) 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. **Interval:** If a user policy is set, it overrides the system policy, whether the user's interval is shorter or longer in value. **Effective:** Specifies the current synchronization interval. For example, if the user sets a synchronization interval that is less than (more frequent) than the system minimum, the system setting applies. 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.
Encryption	You have two options for encryption to select from: **On** and **Enforced** Select **On** to enable Encryption. With this, user is allowed to set encryption policy for his or her iFolder files. User will have the control over the sharing of his iFolder data. Select **Enforced** to enable encryption for the iFolder files of the selected user account.

10.5.2 Modifying User Account Policies

1 In Web Admin console click the user name link listed under User's tab to open the user page

2 On the User page opened for that user account, you can select or deselect the following:

Parameter	Description
Account	Select the *Disable User Login* check box to disable the account for login. Deselect the value to enable 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

Parameter	Description
File size	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 *Limit* if there is no individual user quota, or to accept the system-wide quota for the selected user account. Select *Limit* 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.
Excluded Files	You can restrict some file types for this user, then specify the exclusion filters that determine the file types that can be synchronized for the user account. To add a file extension to exclusion filter, type the extension (such as `.mpg`), then click *Add* to apply the filter. To exclude a file type from the restricted file types, select the check box adjacent to the file type, then click *Allow*. Default Value: The System-wide settings.
Synchronization	**Interval:** Select the check box to enable a minimum synchronization interval, then specify the minimum interval (in minutes). For example, a practical value is 600 seconds (10 minutes). 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`. Default Value: Disabled, System-wide policy.
Encryption	You have two options for encryption to select from: **On** and **Enforced** Select **On** to enable Encryption. With this, user is allowed to set encryption policy for his or her iFolder files. User will have the control over the sharing of his iFolder data. Select **Enforced** to enable encryption for the iFolder files of the selected user account. **IMPORTANT:** This options is enabled only If the system level encryption policy is set to *On*.

10.6 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 Web Admin console, select *Users* tab
2. Search for the user whose account you want to enable or disable for login.
3. Do one of the following:
   - Enable login for the user account by selecting *Enable*.
   - Disable login for the user account by selecting *Disable*.

Managing iFolders

11

This section discusses how and administrator can manage iFolders on the Novell® iFolder® 3.6 enterprise server, using the Novell iFolder 3 Web Admin.

- Section 11.1, “Creating an iFolder for a User’s Account,” on page 131
- Section 11.2, “Viewing Details And Configuring Policies for An iFolder,” on page 132

11.1 Creating an iFolder for a User’s Account

You can create iFolders for a user’s account. A notification message advises the user that a new iFolder is available to download from the server.

You cannot specify where on the individual computers that the iFolder is to be stored. Each user decides where to set up the iFolder on his or her own computer. If you want users to each store iFolders in the same relative location on their computers, you must coordinate that behavior outside of iFolder. There is no way to enforce it using iFolder tools, of course.

- Section 11.1.1, “Creating an iFolder from the iFolders Page,” on page 131
- Section 11.1.2, “Creating an iFolder from the Users Page,” on page 132

11.1.1 Creating an iFolder from the iFolders Page

1. In Web Admin console, click *iFolders* tab to open the iFolder page.
2. Click *Create* to open the Create New iFolder page.
3. Specify the following information and then click *Create*.

   Name: Assign a name to the iFolder such as ifolder1.

   Description: A short description about the iFolder.
4. Click *Next* to open the Select iFolder Owner page.
5. Search for the user who you want to make the owner of the iFolder, then click the name of the user.

   On the New iFolder page, the Owner field shows the user’s first and last name.
6. Click *Next* to select additional members to the new iFolder.
7. Click *Cancel* to cancel the changes that you made and click *Back* to make any changes.
8. Select the members of your choice and click *Create* to add the selected members to the iFolder.

   For more information to select additional members, see Step 4 on page 132 through Step 6 on page 132 in the Section 11.1.2, “Creating an iFolder from the Users Page,” on page 132.
9. On successful creation, the new iFolder details page opens up.

   You can view its details, change the owner, configure its policies, share the iFolder, or modify members’ access rights.

11.1.2 Creating an iFolder from the Users Page

1. In Web Admin console, click *Users* tab.
2. Search for and click the name of the user you want to create a new iFolder for.

   The Users page opens to the user's information.
3. Click *create* to open the Add Additional Members page for the created iFolder.
4. Search for the users who you want to share the iFolder with, then click the check box next to the name of the user.
5. Click *Cancel* to cancel the changes that you made and click *Back* to make any changes.
6. Click *OK* to complete the operation.

   On successful creation, the new iFolder details page opens up.

   You can view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

11.2 Viewing Details And Configuring Policies for An iFolder

This section discusses the following:

- Section 11.2.1, "Accessing the iFolders Details Page," on page 132
- Section 11.2.2, "Viewing The iFolder Details," on page 132
- Section 11.2.3, "Searching for an iFolder," on page 133
- Section 11.2.4, "Managing iFolder Members," on page 134
- Section 11.2.5, "Managing an iFolder," on page 134
- Section 11.2.6, "Managing iFolder Policies," on page 136
- Section 11.2.7, "Enabling, Disabling and Deleting an iFolder," on page 138

11.2.1 Accessing the iFolders Details Page

1. Use the search tool to locate the iFolder you want to manage.
2. Click the name of the iFolder to open the iFolder Details page.

   For more details on search, see "Browsing the iFolders in the Search Results" on page 134.

   The iFolder Details page will display the iFolder details, a list of members who own or share the iFolders, and policy settings for this particular iFolder.

11.2.2 Viewing The iFolder Details

You can view the following information:

Parameter	Description
Type	Normal iFolder  Encrypted iFolder  Shared iFolder 
Name	The name assigned to the iFolder.
Description	A short description about the iFolder. You can edit this information. Click *Save* to save the changes.
Owner	The username of the owner of the selected iFolder. For orphaned iFolders, the iFolder Admin user is made the 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. Click the username link to view the details of the iFolder owner.
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.
Modified	The last modified time and date of the iFolder.
Size	Size of the iFolder.
Directories	Total number of directories in the iFolder.
Files	Total number of files in the iFolder.

11.2.3 Searching for an iFolder

1. Use one of the following methods to get a list of iFolders:
   - Click the *All* tab on the iFolders page.
   - Click the *Orphan* tab on the iFolders page to retrieve a list of orphaned iFolders.
2. 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 (*Begins With*, *Ends With*, *Contains, 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* 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 or manage the iFolders listed in the Search Results report.

3 Browse the list of iFolders to locate the iFolder you want to manage.

4 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.

11.2.4 Managing iFolder Members

You can view the members' name, type and access rights assigned to them. You are allowed to add or delete an owner, assign ownership, and set access rights to a selected member. For more information, see Section 11.2.5, "Managing an iFolder," on page 134.

11.2.5 Managing an iFolder

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

- "Adding a Member" on page 134
- "Understanding iFolder Access Rights" on page 135
- "Setting the iFolder Access Right for a Member" on page 135
- "Removing a Member" on page 136
- "Transferring Ownership of an iFolder" on page 136
- "Managing Orphaned iFolders" on page 136

In iFolder 3.2 and earlier, when an owner adds a user to an iFolder, the user does not become a member until he or she accepts the iFolder on at least one computer. After the user accepts the invitation and sets up the iFolder, the user shows up in the member list. But with iFolder 3.6, if you add the user as a member of an iFolder from the web access console, then the user is automatically a member. The user and the iFolder will show up in the Web access interface without the user setting up a local iFolder on his or her computer.

Adding a Member

1 On the iFolder Details page, click *Add*.

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.

Understanding iFolder Access Rights

For an overview of access rights, see Section 1.4.8, "iFolder Access Rights," on page 20.

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

Capabilities	Owner	Full Control	Read/Write	Read Only
Transfer ownership of an iFolder to another iFolder 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

Setting the iFolder Access Right for a Member

1. On the iFolder Details page, locate the iFolder user you want to manage.
2. Select the check box next to that iFolder user.
3. Select the Rights drop-down menu, then select the desired right (*Admin*, *Read/Write*, or *Read Only* right).

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

Removing a Member

1. Locate the iFolder you want to manage, then click the iFolder's name link to open the iFolder Details page to the iFolder tab.
2. On the *iFolder Details* page, select the check box next to the member user's name.
3. Select the *Members* tab, then select the check box next to the member user's name.
4. Click *Delete*.

   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.

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.

1. On the iFolder Details page, search for the user you want to assign as the new owner of the iFolder.
2. Select the check box next to the user's name, then click *Owner*.

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. On the iFolder details page, click *Orphan* tab to open the list of orphaned iFolders.
2. Browse to locate the orphaned iFolder you want to manage.
3. Click the iFolder name link to open the iFolder Details page.

   Under the title *iFolder details*, the iFolder details page display the property *Orphan:Yes*.
4. Click *Adopt* to select the owner for the Orphaned iFolder.
5. Select an owner for the owner from the list of iFolder members

   When you click Adopt, the iFolder details page lists all the members of that domain. The default owner for the orphaned iFolder is the Admin, who can assign himself or herself as the owner of the iFolder.

   The name of the orphaned owner also is listed, if he or she is present in the domain, and you can be re-assign the orphaned owner as the owner.

   The ownership is removed from you (default owner) after a member is selected as the owner of the orphaned iFolder. The specified user becomes the iFolder's owner and has the Full Control right to the iFolder. The Admin user, then will have only read permissions on that iFolder.

   The orphaned property is deleted for that iFolder and it becomes a normal iFolder.

11.2.6 Managing iFolder Policies

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

1. 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 *Save* to apply the new settings:

Parameter	Description
Disable Synchronization	Select this to disable the synchronization of data in the iFolder. Deselect this to turn on synchronization, usually temporarily. Default Value: Enabled, Yes
Disk Quota	Select the 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, 100MB
Used (View only)	Reports how much space the iFolder data currently consumes.
Available (View only)	Reports how much space is available on the server for the iFolder data.
Effective (View only)	Reports effective space available on the server for the iFolder data.
File Size	**Limit:** Specifies the maximum total file size (in MB) that an iFolder user is allowed to use, across all iFolders the user owns for the selected user account. **Effective:** Effective file size allocated for the user. **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.
Excluded Files	Specifies a list of file types to include or to exclude from synchronization for the selected iFolder. The file manager files called `thumbs.db` and `.DS_Store` are never synchronized. To add a file extension to an inclusion or exclusion filter, type the extension (such as *.mpg), then click *Add* to apply the filter. To exclude a file type from the restricted file types, select the check box adjacent to the file type, then click *Delete*. Default Value: Disabled, Allow all file types or the System-wide settings.

Parameter	Description
Synchronization	Select the *Synchronization Interval* check box to enable a minimum interval setting for the selected iFolder, then specify the minimum value in minutes 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 minutes 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. 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. 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 system synchronizing with the server ◆ The iFolder (collection) policy Default Value: Disabled

11.2.7 Enabling, Disabling and Deleting an iFolder

1. Click iFolders tab to open iFolders page.
2. Locate the iFolder you want to manage, then select the check box next to the iFolder name.
3. Select an action to perform on the iFolder:
   - Click Delete to delete the iFolder.
   - Click Enable to enable the iFolder.

     This allows the user to access the iFolder and synchronize the files in it. By default, all iFolders are enabled.
   - Click Disable to disable the iFolder.

     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.

     NOTE: Disabling synchronization temporarily, as opposed to deleting or disabling the entire user account, turns off the ability of the selected iFolder to synchronize.

Managing an iFolder Web Access Server

12

This section describes how to manage your Novell® iFolder® 3.6 Web Access server on Novell Open Enterprise Server.

- Section 12.1, “Starting iFolder Web Access Services,” on page 139
- Section 12.2, “Stopping iFolder Web Access Services,” on page 139
- Section 12.3, “Distributing the Web Access Server URL to Users,” on page 139
- Section 12.4, “Configuring the HTTP Runtime Parameters,” on page 139
- Section 12.5, “Securing Web Access Server Communications,” on page 141

12.1 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 terminal console:

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

12.2 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 terminal console:

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

12.3 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.

12.4 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. Default Value: 720 (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 1 GB for Web access. Default Value: 1048576 (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/lib/simias/web/web.config file` for the iFolder enterprise server and in the `/opt/novell/ifolder3/lib/simias/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="720"

     maxRequestLength="1048576"

/>
```

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/lib/simias/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/lib/simias/web/web.config` file.
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="720"

     maxRequestLength="1048576"
```

/>

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.

12.5 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 12.5.1, "Using SSL for Secure Communications," on page 141
- Section 12.5.2, "Configuring the SSL Cipher Suites for the Apache Server," on page 141
- Section 12.5.3, "Configuring the Web Access Server for SSL Communications with the Enterprise Server," on page 142
- Section 12.5.4, "Configuring the Web Access Server for SSL Communications with Web Browsers," on page 143
- Section 12.5.5, "Configuring an SSL Certificate for the Web Access Server," on page 143

For information on how to configure SSL traffic on the iFolder enterprise server, see Section 8.11, "Securing Enterprise Server Communications," on page 106.

12.5.1 Using SSL for Secure Communications

In a default deployment, the iFolder 3.6 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	Yes	No	No	Yes

For more information about SSL 3.0, see Section 8.11.1, "Using SSL for Secure Communications," on page 106.

12.5.2 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.

12.5.3 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/lib/simias/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.

12.5.4 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.

12.5.5 Configuring an SSL Certificate for the Web Access Server

For information, see "Managing SSL Certificates for Apache" on page 153.

Configuration Files

A

- Section A.1, “Simias.config File,” on page 145
- Section A.2, “Web.config File for the Enterprise Server,” on page 146
- Section A.3, “Web.config File for the Web Access Server,” on page 148

A.1 Simias.config File

The default locations of the `Simias.config` file is `<datapath>/simias/Simias.config`.

```
<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.Enterprise" />

    <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>
```

Managing SSL Certificates for Apache

B

This section discusses how to acquire and manage SSL certificates for your Novell® iFolder® 3.*x* servers.

- Section B.1, "Generating an SSL Certificate for the Server," on page 153
- Section B.2, "Generating a Self-Signed SSL Certificate for Testing Purposes," on page 154
- Section B.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 155
- Section B.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 155

B.1 Generating an SSL Certificate for the Server

Using SSL requires that you install an SSL certificate from on each iFolder enterprise server and Web Access server in your domain. Users accept the certificates to enable communications with the servers.

The certificate can be a self-signed certificate or a certificate from a trusted certificate authority. A self-signed certificate is usually used only for internal iFolder services, where the server's identity is not likely to be spoofed. 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 of the following methods, depending on your network needs:

- Use the self-signed certificate that is created and enabled for the server by default during the server install.
- Use the services of a third-party certificate authority to get trusted certificate, then use it instead of accepting the default certificate during the sever install.

Whichever method you use, the certificate is automatically used for the Apache Web Server configuration. If it does not automaticially configure the certificate for the Apache Web Server, see the following:

- Section B.3, "Configuring Apache to Point to an SSL Certificate on an iFolder Server," on page 155
- Section B.4, "Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster," on page 155

YaST contains modules for the basic management of X.509 certificates. This mainly involves the creation of CAs, sub-CAs, and their certificates. For more information about how to manage and update certificates, see Managing X.509 Certification (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) in the *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html).

B.2 Generating a Self-Signed SSL Certificate for Testing Purposes

If desired, you can use OpenSSL to create a self-signed SSL certificate to test your configuration. 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 B.3, “Configuring Apache to Point to an SSL Certificate on an iFolder Server,” on page 155
- Section B.4, “Configuring Apache to Point to an SSL Certificate on a Shared Volume for an iFolder Cluster,” on page 155

B.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.

B.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
   ```

Clustering iFolder 3.6 Servers with Novell Cluster Services for Linux

C

This section discusses how to configure a Novell® iFolder® 3.6 server cluster, using Novell Cluster Services™ (NCS) for Linux.

- Section C.1, "Prerequisites for Clustering iFolder 3.6 Services," on page 157
- Section C.2, "Installing Novell Cluster Services for Linux," on page 157
- Section C.3, "Configuring iFolder 3.6 Servers on an NCS for Linux Cluster," on page 158
- Section C.4, "Creating the iFolder 3.6 Cluster Resource," on page 160
- Section C.5, "Managing the iFolder 3.6 Cluster Resource," on page 160
- Section C.6, "Sample Load Scripts for iFolder 3.6 Clusters," on page 160
- Section C.7, "Sample Unload Scripts for iFolder 3.6 Clusters," on page 161

For information about NCS, see the *OES 2: Novell Cluster Services 1.8.4 for Linux Administration Guide*.

C.1 Prerequisites for Clustering iFolder 3.6 Services

Each node in your iFolder 3.6 cluster must satisfy the following:

- "Prerequisites and Guidelines" on page 49 for iFolder 3.6.
- Prerequisites and requirements for Novell Cluster Services for Linux. For information, see "Requirements for Novell Cluster Services" in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.

C.2 Installing Novell Cluster Services for Linux

For each node in the planned cluster:

IMPORTANT: If you are using iSCSI for shared disk system access, ensure that you have configured iSCSI initiators and targets prior to installing Novell Cluster Services.

---

1. Make sure each node in the cluster satisfies the Section C.1, "Prerequisites for Clustering iFolder 3.6 Services," on page 157.
2. Install and configure Novell Cluster Services (NCS) on the OES Linux 2 servers you plan to use in the iFolder 3.6 cluster.

   For information on installing NCS, see the section "Installing Novell Cluster Services" in the *OES Novell Cluster Services 1.8 Administration Guide for Linux*.
3. Continue with Section C.3, "Configuring iFolder 3.6 Servers on an NCS for Linux Cluster," on page 158.

C.3 Configuring iFolder 3.6 Servers on an NCS for Linux Cluster

The following procedure describes how to configure Novell iFolder 3.6 services on an NCS for Linux cluster. You can optionally add iFolder 3.6 Web Access and iFolder 3.6 Web Admin servers to the cluster.

1 On one of the nodes (Node 1), set up a shared volume to store iFolder data.

This can either be a SAN or iSCSI volume. For information, see "Configuring Cluster Resources for Shared NSS Pools and Volumes" and "Configuring Cluster Resources for Shared Traditional Linux Volumes"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 For each node in the cluster, install iFolder services:

2a In YaST, install iFolder 3.6, iFolder 3.6 Web Admin (optional) and iFolder 3.6 Web Access (optional), but do not configure services at this time.

For information, see Section 7.1, "Installing iFolder on an Existing OES 2 Linux Server," on page 55.

2b Repeat the install on each node in the cluster, then continue with Step 3.

3 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.

3a Mount the shared volume that you created in Step 1. At a server console, enter

```
mount /dev/sda1 /mnt/ifolder3
```

Replace `/dev/sda1` with the disk or partition containing the file system.

Ensure that you use NSSMU for NSS files systems. For more information on creating NSS pool, see the section "Creating NSS Volumes on a Shared Pool".

3b In YaST, configure the iFolder 3.6 enterprise server.

For information, see Section 7.2, "Deploying iFolder Server in a Multi-server Environment," on page 58.

For the System Store Path, specify the mount point of the shared volume that you created in Step 3a.

At the end of the configuration, allow YaST to start Apache, then 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 cluster node you are configuring. If everything is working properly, you should get an authentication prompt.

3c To configure Web Access in YaST,

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
```

3d To configure Web Admin in YaST,

For the Web Admin Alias, specify an alias such as `/admin`. 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
```

4 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 3a.

4a Mount the shared volume. At a terminal console, enter

```
mount /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.

4b In YaST, configure iFolder 3.6. For information, see Section 7.2, “Deploying iFolder Server in a Multi-server Environment,” on page 58.

For the *System Store Path*, specify the some temporary location or accept the default 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.

4c Stop Apache on the node you are configuring. At a terminal console, enter

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

4d Skip iFolder configuration and copy the following configuration files from the first node.

- `/etc/apache2/conf.d/ifolder-admin.conf`
- `/etc/apache2/conf.d/ifolder-web.conf`
- `/etc/apache2/conf.d/simias.conf`

Ensure that you configure Web Admin and Web Access by using YaST after copying these files.

4e Start Apache on this node.

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

4f Repeat Step 4 to configure any additional nodes in your iFolder cluster.

C.4 Creating the iFolder 3.6 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 C.6, “Sample Load Scripts for iFolder 3.6 Clusters,” on page 160.
9. For the cluster *Unload Script*, use one of the sample unload scripts as a guide, then click *Next*.

   For information, see Section C.7, “Sample Unload Scripts for iFolder 3.6 Clusters,” on page 161.
10. Complete the remaining screens, then click *Finish*.
11. Continue with Section C.5, “Managing the iFolder 3.6 Cluster Resource,” on page 160.

C.5 Managing the iFolder 3.6 Cluster Resource

In iManager Roles and Tasks, expand the *Clusters* role, then click *Cluster Manager* to manage the iFolder 3.6 resource and bring it online.

For information, see “Managing Novell Cluster Services Clusters” and “Configuring and Managing Cluster Resources” in the *OES Novell Cluster Services 1.8.4 Administration Guide for Linux*.

C.6 Sample Load Scripts for iFolder 3.6 Clusters

- Section C.6.1, “Linux Traditional File System,” on page 160
- Section C.6.2, “NSS File System,” on page 161

C.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
################################################
```

C.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
################################################
```

C.7 Sample Unload Scripts for iFolder 3.6 Clusters

- Section C.7.1, "Linux Traditional File System," on page 162
- Section C.7.2, "NSS File System," on page 162
- Section C.7.3, "Troubleshooting," on page 163

C.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

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

C.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

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

C.7.3 Troubleshooting

Linux does not allow you to umount a volume if any file is currently open. If your system is going comatose when you try to unload the cluster, it is probably because you have open user connections and files on the volume. You need to allow enough time for the connections to be closed before the umount is executed.

Add the following lines between the request to stop service and deleting the IP address:

```
#stop service otherwise

sleep 10

ignore_error fuser -k /$MOUNT-POINT

sleep 5
```

Replace */$MOUNT-POINT* with the actual path of the mount point of your iFolder data store. For example, if the mount point is `/var/opt/novell/ifolder3/data`, add:

```
#stop service otherwise

sleep 10

ignore_error fuser -k /var/opt/novell/ifolder3/data

sleep 5
```

Tune the script until the cluster no longer goes comatose under an operational load when the unload script is called. If the system goes comatose under a full load, increase the sleept time until the cluster is able to successfully execute the unload instead of going comatose.

Troubleshooting Tips For Novell iFolder 3.6

D

This section gives you a list of troubleshooting suggestions that can help you resolve some of the iFolder issues.

- Section D.1, “iFolder User Account Creation Delays with Timeout Error,” on page 165
- Section D.2, “Web Admin Console Fails to Start Up,” on page 166
- Section D.3, “Exception Error while Configuring iFolder on a Samba Volume,” on page 166
- Section D.4, “Samba Connection to the Remote Windows Host Times out,” on page 166
- Section D.5, “LDAP Users Are Not Reflected in iFolder,” on page 166
- Section D.6, “Changing Permission to the Full Path Fails,” on page 167
- Section D.7, “iManager Single Sign-on Fails,” on page 167
- Section D.8, “List of Items Fail to Synchronize,” on page 167
- Section D.9, “Access Permission Error While Logging in Through Web Access,” on page 167
- Section D.10, “iFolder Upgrade From OES 1 SP2 to OES 2 Fails,” on page 167
- Section D.11, “Web Admin and Web Access Show Blank Page,” on page 168

D.1 iFolder User Account Creation Delays with Timeout Error

When you attempt to configure an iFolder user account, either it takes a longer time (90 to 200 seconds) than expected or it throws a Timeout error. In the latter case, further iFolder operations fail and you cannot create a new account until the old one is removed. Due to this partial account creation, user account details have incorrect information and certain operations throw exception error.

As a workaround, you must first quit the iFolder client and then do the following:

For iFolder clients on Linux:

1. Open a terminal console and run `ps -eaf` command to verify if any instance of simias or iFolder is running.
2. Run the command `kill -9 <process id>` to kill any running instances of simias or iFolder.
3. Run `rm -rf <home directory>/.local/share/simias` to remove the simias directory.

For iFolder clients on Windows:

1. In the Windows Task Manager, ensure that no process named Simias or iFolderApp is running. If any of these processes is running, then select the process and terminate them by clicking *End Process*.
2. Remove the simias directory `%USERPROFILE%\Local Settings\Application Data\simias`.

After performing the operations described above, any data related to the previous iFolder setup is removed. You must then configure iFolder again.

NOTE: If multiple accounts were configured, then data related to all accounts is removed and you must configure that domain again. However, any data that is synced with the iFolder server will not be removed. After accounts are configured again, the previously configured iFolders are displayed under *iFolders on server* list in the iFolder client interface. You must then download or merge the iFolders and synchronize them to bring them back to the original state.

D.2 Web Admin Console Fails to Start Up

If the iFolder Web Admin console does not start on your first attempt, consider the following actions:

1. Run `apache2 --stop` to stop the Apache process.
2. Run `ps -ef|grep mono` to check if any Mono® process for iFolder is still running on the server side.
3. Run `kill <process id of the process>` to end the Mono process for iFolder.
4. Restart Apache.

Now you can successfully connect to the server.

D.3 Exception Error while Configuring iFolder on a Samba Volume

If iFolder server throws an exception when you configure the iFolder 3.6 server on Samba volume, check the properties of the folder in Windows. You must provide the read-write permission to the network users. In other words, you must ensure that the Read Only check box is deselected

D.4 Samba Connection to the Remote Windows Host Times out

If Samba connection to the remote Windows host times out when you execute `samba mount` command, you must check whether the Windows firewall is enabled or not. If it is enabled, add the Samba port to the list of permitted ports in the firewall configuration.

D.5 LDAP Users Are Not Reflected in iFolder

If the LDAP users are not synchronized immediately in iFolder, check to see if the default interval to synchronize the LDAP server with iFolder servers is 24 hours.

To reflect the changes immediately, you can use the *Sync now* option in the *Server details* page of the Web Admin console.

D.6 Changing Permission to the Full Path Fails

If you cannot change the permission to the full path specified while configuring Multi-volume, consider the following actions:

1. Run `chown -R <apache user>:<apache group> <Data/store/path/simias>`.
2. Change the permission that has already been set.

D.7 iManager Single Sign-on Fails

If you cannot log in to iManager by enabling single sign-on, consider the following actions:

- You must enable the SSL for iFolder Web Admin server.

  For more informations, see "Require Server SSL" on page 76.
- You must also provide the correct IP address instead of specifying *localhost* in the *iFolder server* field in the iFolder launch console of the iManager.

D.8 List of Items Fail to Synchronize

If a list of items fail to synchronize, consider the following causes:

- You excluded the non-synchronized file types in the Web Admin console policy.
- The disk space restriction has been exceeded for the specified user or the specified iFolder.
- User has the file or files open in an application. In this case, users must close the application and re-sync the iFolder.

D.9 Access Permission Error While Logging in Through Web Access

If the user cannot log in to iFolder Web Access, consider the following actions:

- Check the permission for the Apache user to the data store path of iFolder, and change permissions as necessary.
- Run `chown -R <apache user>:<apache group> <Data/store/path/simias>`.

D.10 iFolder Upgrade From OES 1 SP2 to OES 2 Fails

If the iFolder 3.6 server does not function after the upgrade from OES SP2 to OES 2, consider the following cause.

- The `Simias.config` file created during the upgrade is missing

The workaround is:

1. Take the file system backup of iFolder 3.2 data store and Simias.config file.

   Default location is `/var/lib/wwwrun/.local/share/Simias.config`.

   Ensure that you know the iFolder Proxy user password.
2. Open a terminal console and enter `/opt/novell/ifolder3/bin/simias-server-setup --upgrade`.
3. Follow the on-screen instruction to manually upgrade the server.

NOTE: This workaround works for all the iFolder 3.6 upgrade failures.

D.11 Web Admin and Web Access Show Blank Page

If the Web Admin console and Web Access console show blank pages, ensure that the Simias server and Web Access server are up and running.

Frequently Asked Questions

E

This section answers typical questions asked by the administrators of iFolder 3.6 server software, including the following:

- Section E.1, “iFolder 3.6 Server,” on page 169
- Section E.2, “iFolder 3.6 Client,” on page 170
- Section E.3, “iFolder 3.6 Administration,” on page 171

Additional Questions

For an additional listing of questions and answers that have been submitted by administrators and iFolder users, see the following:

- Appendix D, “Troubleshooting Tips For Novell iFolder 3.6,” on page 165

- *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*
- iFolder 3 Web site (http://www.ifolder.com/index.php/FAQ)

E.1 iFolder 3.6 Server

This section addresses the following issues:

- Section E.1.1, “Is iFolder 3.6 supported on a 64-bit OS?,” on page 169
- Section E.1.2, “Is iFolder going to support non-eDirectory related platforms as an identity source?,” on page 169
- Section E.1.3, “Because iFolder is developed on Mono, can it be deployed in a Microstoft environment?,” on page 169

E.1.1 Is iFolder 3.6 supported on a 64-bit OS?

Yes. Both the server and iFolder client for Linux work on 64-bit systems.

E.1.2 Is iFolder going to support non-eDirectory related platforms as an identity source?

Yes, it already does. Any open LDAP-based directory works seamlessly with iFolder 3.6.

E.1.3 Because iFolder is developed on Mono, can it be deployed in a Microstoft environment?

Yes. You can successfully deploy iFolder 3.6 on Microsoft’s .NET environment.

E.2 iFolder 3.6 Client

This section addresses the following issues:

- Section E.2.1, “Is iFolder 3.6 supported on Windows Vista?,” on page 170
- Section E.2.2, “Is iFolder 3.6 supported on the Macintosh platform?,” on page 170
- Section E.2.3, “Can I use the iFolder 2.x client to connect to an iFolder 3.6 server?,” on page 170
- Section E.2.4, “Can I use the iFolder 3.x client to connect to the iFolder 3.6 server?,” on page 170
- Section E.2.5, “Can I can use iFolder 3.6 on different operating systems on different workstations to access and share the files?,” on page 171
- Section E.2.6, “There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.6?,” on page 171
- Section E.2.7, “I deleted a file accidentally? Can I recover it?,” on page 171
- Section E.2.8, “What are the migration scenarios recommended and supported by iFolder 3.6?,” on page 171

E.2.1 Is iFolder 3.6 supported on Windows Vista?

iFolder 3.6 will have a Web release patch shortly after Open Enterprise Server 2 ships. This release will have Windows Vista support. For more information on supported platforms, see Section 7.9.2, “Downloading the iFolder Client,” on page 90.

E.2.2 Is iFolder 3.6 supported on the Macintosh platform?

iFolder 3.6 will have a Web release patch shortly after Open Enterprise Server 2 ships. This release will have Macintosh support.

E.2.3 Can I use the iFolder 2.*x* client to connect to an iFolder 3.6 server?

No. However, iFolder 3.6 supports client-side migration that helps the user to convert the 2.x iFolder data to iFolder 3.6 data. For more information on migration, see Chapter 3, “Novell iFolder Upgrade, Migration, and Coexistence,” on page 33 and “Migrating from iFolder 2.x to iFolder 3.6” in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

E.2.4 Can I use the iFolder 3.*x* client to connect to the iFolder 3.6 server?

No. When you install the iFolder 3.6 client, it overwrites the iFolder 3.*x* client if it is already installed and performs an in-place upgrade of the local store. For more information, see Section 3.2, “Upgrading iFolder 3.x to iFolder 3.6,” on page 34.

E.2.5 Can I can use iFolder 3.6 on different operating systems on different workstations to access and share the files?

Yes. You can use iFolder for different operating systems on different workstations to access and share the files. For example, you can use an iFolder client on a Windows workstation at home and on a Linux workstation at office to share the same files.

E.2.6 There was a 10 MB file limitation using Web Access? Is it still applicable for iFolder 3.6?

No. iFolder 3.6 Web Access no longer has this file size limitation. For more information on the Web Access console, see "Using Novell iFolder 3.6 Web Access" in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

E.2.7 I deleted a file accidentally? Can I recover it?

Currently iFolder does not support this functionality.

E.2.8 What are the migration scenarios recommended and supported by iFolder 3.6?

iFolder 2.*x* customers must first install a separate iFolder 3.6 server and deploy the iFolder 3.6 clients, then they must use the client-side migration tool to migrate the data from each of the iFolder clients. When migration is completed, the iFolder 2.*x* server and corresponding clients can be removed. For more information see Chapter 3, "Novell iFolder Upgrade, Migration, and Coexistence," on page 33 and "Novell iFolder Migration and Upgrade " in the *OES 2: Novell iFolder 3.6 Cross-Platform User Guide*.

E.3 iFolder 3.6 Administration

This section addresses the following issues:

- Section E.3.1, "What is the management console for iFolder 3.6?," on page 171
- Section E.3.2, "What are the new features in the Web Admin console?," on page 172
- Section E.3.3, "Can the administrator control the ability to encrypt iFolder files?," on page 172
- Section E.3.4, "Are there any enhancements for how bulk users are enabled for iFolder?," on page 172
- Section E.3.5, "Can the administrator control the ability to share files?," on page 172
- Section E.3.6, "How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain?," on page 172

E.3.1 What is the management console for iFolder 3.6?

There is a new Web-based console for managing iFolder 3.6. Novell iManager provides single sign-on authentication to the Web Admin console. For more information on the Web Admin console, see Chapter 9, "Managing iFolder Services via Web Admin," on page 109.

E.3.2 What are the new features in the Web Admin console?

You can manage the Multi-server and Multi-volume features from the Web Admin console. You can generate reports at a granular level and export them to a text file for later viewing or offline management. You can manage policy settings for the iFolder system, users, and for iFolders. For more information on the Web Admin console, see Chapter 9, "Managing iFolder Services via Web Admin," on page 109

E.3.3 Can the administrator control the ability to encrypt iFolder files?

Yes, the administrator can manage the encryption policy settings through the Web Admin console. For more information, see Section 9.5.3, "Configuring System Policies," on page 115.

E.3.4 Are there any enhancements for how bulk users are enabled for iFolder?

iFolder users can be provisioned based on LDAP groups and containers. The users are provisioned during their first login. The client transparently redirects to the appropriate server in a Multi-server environment. For more information, see Section 4.5, "iFolder User Account Considerations," on page 42.

E.3.5 Can the administrator control the ability to share files?

No. A future version of iFolder will support this feature.

E.3.6 How can the iFolder administrator manage the data owned by an iFolder user who has been removed from the iFolder domain?

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. These iFolders later can be assigned to other users by using the Web administration console. Membership and synchronization continue while the iFolder Admin user determines whether an orphaned iFolder should be deleted or assigned to a new owner. For more information, see "Managing Orphaned iFolders" on page 136.

Caveats for Implementing iFolder 3.6 Services

F

This section presents a few pointers for avoiding common iFolder 3.6 implementation problems.

The list that follows is not comprehensive. Rather, it simply outlines some of the more common problems reported by network administrators. To ensure successful service implementations, you should always follow the instructions in the documentation for the services you are implementing.

This section discusses the caveats to consider after installing and before implementing the iFolder 3.6 services.

- Section F.1, “Loading Certificates to the Recovery Agent Path,” on page 173
- Section F.2, “Using Novell iFolder Server to Serve Large Files,” on page 173
- Section F.3, “Deployment in an Active Directory Environment,” on page 174
- Section F.4, “Using a Single Proxy User for a Multi-Server Setup,” on page 174
- Section F.5, “Slave Configuration,” on page 174
- Section F.6, “LDAP SSL Certificate,” on page 174
- Section F.7, “Novell iFolder Admin User,” on page 174
- Section F.8, “Novell iFolder with iChain and the Access Gateway,” on page 174

F.1 Loading Certificates to the Recovery Agent Path

If the path to the Key Recovery Agent certificates is set during iFolder configuration, you must ensure that the certificates are copied to this location. The location is *datapath*`/simias/Simias.config` under the `RAPath` section.

For more information on the Recovery Agent, refer to the Section 7.2.3, “Loading Recovery Agent Certificates in The iFolder Server,” on page 73.

F.2 Using Novell iFolder Server to Serve Large Files

Novell iFolder is capable of serving large files, subject to the system or file system limits. However, Mono® has a race condition in the Mono version that ships with OES 2 that prevents large file uploads.The Mono team has fixed this issue in 1.2.5 release and the patch that contains all the Mono components, including XSP is available through the Novell Customer center. Ensure that you apply the patch before you start using iFolder for serving large file uploads.

To apply the patch, ensure that,

- You complete the *Novell Customer Center System Registration* Procedure.
- You resolve the dependencies and apply the Software updates available on your machine.

Follow the steps given below to apply the Mono patch:

1. Install iFolder with OES 2.
2. During OES 2 configuration, select *Customer Center Configuration*.
3. Complete the *Novell Customer Center System Registration* procedure.
4. Continue with the remaining steps for configuration.
5. Once you complete the configuration, open *YaST2 > Online Update* to resolve the dependencies and apply the Software patches available on your machine.

F.3 Deployment in an Active Directory Environment

If you are using a tree that does not depend on eDirectory, ensure that you create an iFolder Admin user and an iFolder Proxy user if they are not already present. You must also update this information during theYaST configuration.

F.4 Using a Single Proxy User for a Multi-Server Setup

By default each server creates its own Proxy user for role separation. However, you can use single Proxy user for both master and slave servers. You can provide the Proxy DN and Proxy password for the master server configuration and for the slave configurations. You must not use the default configuration for the Proxy user.

F.5 Slave Configuration

Selecting *Install into existing Domain* during YaST configuration is considered to be a slave configuration. If the option is not selected, the server you are configuring is considered to be a master.

F.6 LDAP SSL Certificate

The LDAP certificate is accepted without verification if you enable the *Require a Secure Connection between the LDAP server and the iFolder Server* option during YaST configuration.

F.7 Novell iFolder Admin User

By default, the LDAP admin assumes the iFolder Administrator position. You must change this default setting during the master server configuration to have a better role separation.

F.8 Novell iFolder with iChain and the Access Gateway

Novell iFolder can work with iChain® and the Access Gateway. However, the logout URLs for both of these products are not configured by default. You must use CLI to update the logout URL for both iFolder 3.6 Web Admin and iFolder 3.6 Web Access configuration work successfully with iChain or

the Access Gateway. For more information, refer to Section 7.3.1, “Configuring iFolder Web Access for iChain or AccessGateway,” on page 74 and Section 7.4.1, “Configuring iFolder Web Admin for iChain or AccessGateway,” on page 76.

Product History of iFolder 3

G

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 G.1, "Version History," on page 177
- Section G.2, "Network Operating Systems Support," on page 178
- Section G.3, "Directory Services Support," on page 178
- Section G.4, "Workstation Operating Systems Support for the iFolder Client," on page 178
- Section G.5, "Web Server Support," on page 179
- Section G.6, "iFolder User Access Support," on page 179
- Section G.7, "Management Tools Support," on page 179

For a comparison of features in 2.1*x* and 3.*x*, see "What's New" on page 23.

G.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 2.4, "What's New in Novell iFolder 3.0 (OES Linux)," on page 24. 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 2.3, "What's New in Novell iFolder 3.1 (OES SP1 Linux)," on page 24.
3.2	Bundled	Adds support for OES SP2 Linux servers and repairs known defects. For information, see Section 2.2, "What's New in Novell iFolder 3.2 (OES SP2 Linux)," on page 23.
3.6	Bundled	Adds support for OES 2 Linux servers. For more information, see Adds support to upgrade from previous iFolder 3.x clients to an iFolder 3.6 client and migrate from iFolder 2.x clients to an iFolder 3.6 client.

G.2 Network Operating Systems Support

Network Operating System	3.0	3.1	3.2	3.6
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.	No
OES SP1 Linux	No	Yes	Yes Requires a Mono update.	No
OES SP2 Linux	No	No	Yes	No
0ES 2.0 Linux	No	No	No	Yes

G.3 Directory Services Support

LDAP Directory Service	3.0	3.1	3.2	3.6
Novell eDirectory™	8.7.3	8.7.3	8.7.3	8.8

G.4 Workstation Operating Systems Support for the iFolder Client

Workstation Operating System	iFolder 3.0	iFolder 3.1	iFolder 3.2	iFolder 3.4	iFolder 3.6
Novell Linux Desktop	v9	v9	v9 and later	No	No
SUSE Linux Enterprise Desktop 10	No	No	No	Yes	No
SUSE Linux Enterprise Desktop 10 SP1	No	No	No	No	Yes
Windows 2000/XP/ 2003	Yes	Yes	Yes	No	Windows XP SP2/2000 Professional SP4
Macintosh OS X v10.3 and later	Yes	Yes	Yes	No	No

G.5 Web Server Support

Web Server	3.0	3.1	3.2	3.6
Apache	2 (worker mode)	2 (worker mode)	2 (worker mode)	2 (worker mode)

G.6 iFolder User Access Support

iFolder User Access Method	3.0	3.1	3.2	3.6
iFolder client	Yes	Yes	Yes	Yes
iFolder client, using a proxy	No	Yes	Yes	yes
Novell iFolder 3.x Web Access	IE 6.0	IE 6.0	IE 6.0	IE 6.0/7.0
	Firefox	Firefox	Firefox	Firefox
	Safari (Macintosh)	Safari (Macintosh)	Safari (Macintosh)	Safari
Novell iFolder 3.6 Web Admin	No	No	No	IE 6.0/7.0
				Firefox
				Safari

G.7 Management Tools Support

iFolder Management Interfaces	3.0	3.1	3.2	3.6
iFolder 3 plug-in to iManager 2.5	Yes	Yes	Yes	Yes, to iManager 2.7
iFolder 3 plug-in to YaST	Yes	Yes	Yes	Yes
iFolder 3 Web Access plug-in to YaST	Yes	Yes	Yes	Yes
iFolder 3 Web Admin plug-in to YaST	No	No	No	Yes
RPM packages available in the OES install	No	Yes	Yes	Yes
Simias Log	Yes	Yes	Yes	Yes
Simias Access Log	No	Yes	Yes	Yes