AUTHORIZED DOCUMENTATION

# Security Administration Guide

# Novell® iFolder

**3.8.4**

December 2010

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 the 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.

Copyright © 2007-2010 Novell, Inc. All rights reserved. Permission is granted to copy, distribute, and/or modify this document under the terms of the GNU Free Documentation License (GFDL), Version 1.2 or any later version, published by the Free Software Foundation with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the GFDL can be found at the GNU Free Documentation Licence (http://www.fsf.org/licenses/fdl.html).

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.
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).

# Contents

# About This Guide

This guide provides specific instructions on how to install, configure, and maintain Novell iFolder server and iFolder clients in the most secure way possible.



### Audience

This guide is intended for network security 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 Novell Documentation Feedback (http://www.novell.com/documentation/feedback.html) and enter your comments there.

### Documentation Updates

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

For emerging issues with Novell iFolder server and client, see the *Novell iFolder 3.8.4 Readme* (http://www.novell.com/documentation/ifolder3/index.html).

### Additional Documentation

- Novell iFolder 3.*x* documentation (http://www.novell.com/documentation/ifolder3/index.html)
- Novell Technical Support (http://www.novell.com/support/)

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.

# Security Best Practices Overview

1

This section summarizes the recommended configurations and settings required to run Novell iFolder server and the iFolder clients in a secure mode.



## 1.1 Security Recommendations for iFolder

The following table lists the iFolder server configuration settings that impact iFolder security.

***Table 1-1*** *Security Recommendations*

| Parameter | Possible Values | Default Value | Recommended Value for Best Security |
|---|---|---|---|
| iFolder Admin user | User-specified | User-specified administrator user | Special iFolder Admin user identity for managing iFolder services |
| Equivalent iFolder Admin users | User-specified | None | Users with limited administrator rights, such as for a specific iFolder server |
| iFolder Proxy user password | User-specified | Auto generated during initial configuration of the iFolder server | User-specified, using strong password practices |
| Server to client communications | SimiasRequireSSL (Yes/No) | SimiasRequireSSL = Yes | SimiasRequireSSL = Yes |
| Server to Server Communication | Select Yes during setup to enable SSL, or select No to disable SSL | Yes, SSL enabled<br>SimiasUrl https<br>SimiasCert <*RAW certificate*> | Yes, SSL enabled |
| `/usr/web/web.config` file | SimiasUrl (https/http) | SimiasRequireSSL https | SimiasRequireSSL https |
| | SimiasCert (RAW certificate/none) | SimiasCert <*RAW certificate*> | SimiasCert <*RAW certificate*> |

# Security Best Practices for Novell iFolder

# 2

This section provides specific instructions on how to install, configure, and maintain Novell iFolder in the most secure way possible.



## 2.1 Secure Communication with the LDAP Server



### 2.1.1 Using SSL for Server Communications

By default, the iFolder enterprise server is configured to communicate with the LDAP server via SSL. For most deployments, this setting should not be changed. If the LDAP server co-exists on the same server as the iFolder enterprise server, you can reconfigure to disable SSL, which increases the performance of LDAP authentications.

For information, see “Configuring the iFolder Enterprise Server” in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.2 Communication between the Web Admin Server and the Web Admin Browser

By default, the Novell iFolder Web Admin uses SSL for communications to the iFolder enterprise server being managed. For most deployments, this setting should not be changed. If the Web Admin service and the iFolder enterprise service are on the same server, SSL is not required. For HTTP connections, the password is passed in the clear.

## 2.3 Enterprise Client/Server Communications

By default, the iFolder enterprise server is configured for shared iFolder access. Client/Server communication is not through SSL. All data is sent to the server in the clear. For most deployments, this setting is used for high performance. This setting can be changed during the simias-server-setup configuration for iFolder.

If you disable SSL for client/server communications, you should use a VPN (virtual private network) for communications over wireless networks and outside the firewall. For information, see Section 4.3, “Securing Communications with a VPN If SSL Is Disabled,” on page 19.

## 2.4 Web Access Server Communications

By default, the iFolder Web Access server is configured to require SSL. All Web-browser-based communication to the Web Access server is encrypted by using the SSL protocol. In most deployments, this setting should not be changed because iFolder uses Forms-based authentication for browser communications, which means passwords are sent to the server in the clear. For information, see “Configuring the Web Access Server for SSL Communications with Web Browsers” in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.5 Disabling the SSL 2.0 Protocol

The built-in protections of SSL 3.0 for version rollback attacks (where the session is rolled back to SSL 2.0 even when both client and server support SSL 3.0) are not effective against a version rollback attackers who can brute force the key and substitute a new `ENCRYPTED-KEY-DATA` message containing the same key (but with normal padding) before the application specified wait threshold has expired. You can disable SSL 2.0 on the server, so it is not possible to establish a session using SSL 2.0, and so version rollback attacks are not be possible.

For information about disabling the SSL 2.0 protocol for the Apache server, see “Configuring the SSL Cipher Suites for the Apache Server” in the *Novell iFolder 3.8.4 Administration Guide*.

For 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.

## 2.6 Configuring a Cipher Suite to Use for SSL/TLS

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.
- Disable the Low, Export, and Null cipher suites unless you need them for other applications.

  Do not disable the Low and Export cipher suites if they are required by your customer base. Individuals using older browsers (4-5 years old) and older versions of Windows, such as Windows 98 might still need those cipher suites for other services.

For information, see "Configuring the SSL Cipher Suites for the Apache Server" in the *Novell iFolder 3.8.4 Administration Guide*.

For 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.

## 2.7 Installing Trusted Roots and Certifications on the iFolder Server

You can manually install the trusted roots and the directory public key out-of-band. For information, see "Managing SSL Certificates for Apache" in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.8 Installing Server Certificates from a Known Certificate Authority

You should use valid certificates for both the Apache server and for communication between the Simias server and the Simias client daemon. Simias is the technology underpinning your iFolder server and client software. You should have the server public key signed by a known certificate authority (CA). For information, see "Generating an SSL Certificate for the Server" in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.9 Using a Shared Certificate in iFolder Clusters

For a cluster where all of the nodes are acting like the same machine when they are taking their turn hosting, the user should have a single certificate for the highly available IP address that all of the nodes in the cluster share. For information, see "Configuring Apache to Point to an SSL Certificate on an iFolder Server" in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.10 Ensuring Privilege Separation for the iFolder Proxy User

The iFolder Proxy user is a proxy user identity used to access the LDAP server to retrieve a list of authorized users. The proxy user is automatically created during the iFolder enterprise server configuration. The username is predetermined (hard-coded) on the system. For most deployments, this username should never change.

Make sure that the user account assigned as the iFolder Proxy user is different than the one used for the iFolder Admin user and other system users. Separating the proxy user from the administrator provides privilege separation.

The proxy user password is auto-generated and stored briefly in the `/<data path>/simias/.simias.ppf` file of the iFolder server. This file is created during the configuration of the iFolder enterprise server and is removed when the server starts for the first time. A restart of Apache is forced at the end of the configuration process, which in turn starts the iFolder service. During the initial startup, the iFolder process reads the file, stores and encrypts the password by using the public key of the iFolder server in the server's Simias database, and then removes the password from the file.

## 2.11 Using Synchronize Now to Remove Users

The iFolder user or group list is periodically updated based on the LDAP synchronization interval. Whenever you remove users or groups from a LDAP Search DN, or remove contexts from the Search DN list, you should synchronize the list immediately using the *Synchronize now* option in the server details page in the Web iFolder Admin to enforce your changes.

## 2.12 Controlling Access to the iFolder Data Store

By default, the iFolder server stores the database and user files under the `/<data path>/simias` directory. The Apache Server user *wwwrun* by default owns those files. You must use every precaution to avoid inadvertently assign rights to unauthorized users.

## 2.13 Controlling Access to the iFolder Server Configuration Files

The iFolder server stores the configuration files in the `/<data path>/simias` directory. The Apache Server user *wwwrun* owns the configuration file. You must use every precaution to avoid inadvertently assigning rights to unauthorized users.

## 2.14 Controlling Access to And Backing Up the iFolder Audit Logs

By default, the iFolder server stores the audit logs in the `/<data path>/simias/logs` directory. The iFolder server administrator should guarantee that rights are not inadvertently assigned to unauthorized users. Administrators should also periodically back up the rolled-over logs in case they are ever needed for forensic purposes. Audit logs should be monitored periodically.

For information, see "Managing the Simias Log and Simias Access Log" in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.15 Encrypting Data on the Server

iFolder uses Blowfish to encrypt the data on the wire. The data is then encrypted and stored on the enterprise server. This is same as in iFolder 2.*x*, which provides passphrase-based encryption. To enable encryption for the users, set the encryption policy to *On* under the *System policy* in the Web Admin console.

For more information, see "Configuring System Policies" in the *Novell iFolder 3.8.4 Administration Guide*.

## 2.16 Preventing the Propagation of Viruses

Because iFolder is a cross-platform distributed solution, there is a possibility of a virus infection on one platform 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.

## 2.17 Backing Up the iFolder Server

Backing up the iFolder user data and configuration data should be done regularly. The backup media should be stored in a secure offsite facility.

During backup and restore, the iFolder data itself is not encrypted. If the iFolder store and the backup media are on different computers, use SSL to transfer data between the computers. It is not necessary to use SSL if the iFolder store and backup media are on the same computer.

For information, see the following in the *Novell iFolder 3.8.4 Administration Guide*:

- "Backing Up the iFolder Server"
- "Recovering from a Catastrophic Loss of the iFolder Server"
- "Recovering iFolder Data from File System Backup"

For sensitive data, use one of the following methods to encrypt the data backup:

- Encrypt the data itself if the application that creates the data supports encryption. For example, database products and third-party tools support data encryption.
- Use backup software that is able to encrypt data as you back it up. This method has performance and manageability challenges, especially for managing encryption keys.
- Use an encryption appliance that encrypts sensitive backup media as data is backed up.

If you transport and store media offsite, use a company that specializes in media shipment and storage. This way, your tapes are tracked via bar codes, stored in environmentally friendly conditions, and are handled by a company whose reputation rests on its ability to handle your media properly.

## 2.18 Loading the Recovery Agent Certificates

The Novell iFolder service by default is not configured for the Recovery agent. During server configuration, ensure that the Recovery agent path is configured. This path should contain the list of certificates that the service can load for the users to select from. For more information on loading the Recovery agent certificates, see "Recovery Agent Certificates " in the *Novell iFolder 3.8.4 Administration Guide*.

# Security Best Practices for the iFolder Client

3

This section provides specific instructions on how to install, configure, and maintain the iFolder client in the most secure way possible.



## 3.1 Configuring Client-Side Firewalls for iFolder Communications

If users deploy a client-side firewall, they must set the firewall to allow the iFolder client to communicate locally (on the same computer) with Mono XSP Server. iFolder communicates to Mono XSP Web services, which communicates, in turn, with the iFolder enterprise server via HTTP BASIC or SSL, as governed by the system settings for the iFolder enterprise server. The user can allow iFolder to choose a local dynamic port for local iFolder traffic, or configure a local static port for iFolder to use for that purpose.

## 3.2 Configuring Client-Side Virus Scanners for iFolder Communications

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

Scanning the `..\simias\WorkArea\` directory for viruses causes problems with synchronization if a virus is detected on download. The `..\simias\WorkArea\` directory is where iFolder stages files for download from the server. Users should set their virus scanners to avoid scanning the `..\simias\WorkArea` directory. Scanners can detect the virus when iFolder moves the infected file from the staging area to the target iFolder.

## 3.3 Configuring a Web Browser to Use SSL 3.0

Novell iFolder servers expect users to connect to the enterprise server account and the Web access server with SSL 3.0 connections. Both the client and browser connections use the browser’s settings for SSL. If Microsoft IE is installed on your system, the iFolder client uses those settings over any other browser configuration for the client. Make sure the IE browser settings and other browsers you use to connect to iFolder servers are configured to use SSL 3.0.

## 3.4 Creating an Encrypted iFolder

Novell iFolder supports encrypted iFolder storage. To store the files encrypted, users must ensure that the iFolder they are uploading to is created as encrypted. For that, they must ensure that the option for Encryption is selected. They also must specify a passphrase and select a Recovery agent when creating an encrypted iFolder by using the iFolder thick client. However, this option is available only when you set the Encryption policy to *On*. In this case, users are free to choose between the two options: *Regular* and *Encrypted*. However, if you set the encryption policy to *Enforced*, users can create only encrypted iFolders and they cannot change this encryption settings for their iFolders.

---

**NOTE:** Even if the encryption policy is set to *Enforced*, you can create a regular iFolder by using the *Create* button on the iFolder page of the iFolder Web Admin console.

---

An existing iFolder cannot be converted to be an encrypted iFolder, and an encrypted iFolder cannot be converted to be a regular iFolder.

During the creation of an encrypted iFolder, the user is prompted to enter a passphrase and select a Recovery agent. iFolder uses the passphrase to dynamically generate a unique encryption key for encrypting and decrypting the key used for data encryption. The encrypted iFolders are not processed without the passphrase. If the user forgets the secret passphrase, he or she cannot access either the iFolder data or the encrypted key used for recovering it. In this case, the Recovery agent that is selected when the passphrase is set helps in recovering the encryption key. For more information on the Recovery agent, see the Section 3.5, “Using the Recovery Agent,” on page 18.

## 3.5 Using the Recovery Agent

The Novell iFolder enterprise server uses a Recovery agent, which is an X.509 certificate-based entity used to recover a lost or otherwise unavailable key for encrypted iFolders.

iFolder prompts a user to select a Recovery agent from a list when the user specifies the passphrase for an encrypted iFolder. However, this option is available only if you set encryption policy to *On* by using the Web Admin console. When the user has lost or forgotten the passphrase, the Recovery agent helps the user to recover the data.The user exports the encrypted key and sends it to the Recovery agent by using the *Key Recovery* option available under the *Security* menu in the client. After receiving the encrypted key, the Recovery agent decrypts it by using its private key, and sends it back to the iFolder user. The user then imports the decrypted key and then resets the passphrase by using the *Security* menu in the client.

## 3.6 Transferring the Encryption Key

The Recovery agent can encrypt the decrypted keys using a one time passphrase (OTP), then it sends both the encrypted passphrase and the key to the user. For secure OTP transfer, make sure that the Recovery agent uses an out-of-band communication or a separate e-mail communication to send the passphrase and the key to the user.

All the keys are Base 4 encoded for easier data exchange. The key is highly vulnerable during transfer if it is not encrypted with the OTP.

# Other Security Best Practices

# 4

This section discusses other security best practices for your Novell iFolder servers and resources.



## 4.1 Controlling Physical Access to the iFolder Servers and Resources

- Servers must be kept in a physically secure location with access by authorized personnel only.
- The corporate network must be physically secured against eavesdropping or packet sniffing.

## 4.2 Securing Access to the Servers with a Firewall

If the iFolder enterprise server, Web Admin server or Web Access server is accessible from outside the corporate network, a firewall should be employed to prevent direct access by a would-be intruder.

## 4.3 Securing Communications with a VPN If SSL Is Disabled

We recommend configuring Novell iFolder to use encryption for all data exchanges between its different components because iFolder data is not encrypted by default. If you configure iFolder not to use encryption between the enterprise server and client or between the Web access server and the user’s Web browser, the user data is susceptible to eavesdropping or packet sniffing by third parties outside the corporate firewall.

Even if you consider the corporate environment to be a trusted environment, a VPN (virtual private network) should be employed for server-client and server-browser connections in the following situations:

- When the users access the servers from outside of the corporate firewall
- When the users access the servers across a wireless network. Wireless access points and adapters broadcast data into space, where the signals can be intercepted by anyone with the ability to listen in at the appropriate frequency.

For accessing the Web Access server over a VPN, make sure to disable split tunneling so that the traffic goes through the VPN connection to the corporate network, not over the public Internet.

For information about configuring SSL features for these communications, see the following:

- Section 2.3, “Enterprise Client/Server Communications,” on page 12
- Section 2.4, “Web Access Server Communications,” on page 12

## 4.4 Securing Wireless LAN Connections If SSL Is Disabled

Protecting a wireless network requires forethought and planning, just as protecting a wired network does. Among the key protective measures to be undertaken are:

- Enable WEP (Wired Equivalent Privacy) encryption, but do not rely on WEP alone to provide security for the wireless network. Use other typical LAN security mechanisms such as VPNs, firewalls, and authentication to ensure privacy. For information, see Section 4.3, “Securing Communications with a VPN If SSL Is Disabled,” on page 19.
- Survey the interference and jamming likelihood for a planned wireless LAN before it is installed.
- Change the default manufacturer’s password for your wireless access points, gateways, or routers.
- Limit, as much as is possible, who can attach to a wireless network. For example, using MAC address filtering is practical for small networks, but it is a time-consuming administrative effort for large networks.
- Use an anonymous Service Set Identifier (SSID) by turning off the SSID broadcast for access points.

## 4.5 Creating Strong Password And Passphrase

Make sure to employ security best practices for passwords, such as the following:

- **Length:** The minimum recommended length is 6 characters. A secure password is at least 8 characters; longer passwords are better.
- **Complexity:** A secure password contains a mixture of letters and numbers. It should contain both uppercase and lowercase letters and at least one numeric character. Adding numbers to passwords, especially when they are added to the middle and not just at the beginning or the end, can enhance password strength. Special characters such as &, $, and > can greatly improve the strength of a password.

  Do not use recognizable words, such as proper names or words from a dictionary, even if they are bookended with numbers. Do not use personal information, such as phone numbers, birth dates, anniversary dates, addresses, or ZIP codes. Do not invert recognizable information; inverting bad passwords does not make them more secure.
- **Uniqueness:** Do not use the same passwords for all servers. Make sure to use separate passwords for each server so that if one server is compromised, all of your servers are not immediately at risk.

# Documentation Updates

A

This section contains information about documentation content changes made to the *Novell iFolder 3.x Security Administrator Guide* since the initial release of Novell iFolder 3.*x*. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the title page and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *Novell iFolder 3.x Security Administrator Guide*, see the Novell iFolder 3.*x* documentation Web site (http://www.novell.com/documentation/ifolder3/index.html).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:



## A.1 December 2008

The following sections were added or changed:

| Location | Change |
|---|---|
| Section 1.1, “Security Recommendations for iFolder,” on page 9 | Updated Table 1-1 on page 9 with new entries for server-to-server communication and Web config file. |
| Section 2.10, “Ensuring Privilege Separation for the iFolder Proxy User,” on page 14 | Updated the default path to the iFolder proxy user password. |
| Section 2.11, “Using Synchronize Now to Remove Users,” on page 14 | Updated to include the details about iFolder Groups. |
| Section 3.5, “Using the Recovery Agent,” on page 18 | Modified the GUI reference for all shared or normal iFolder to Regular iFolder. |

## A.2 December 2007

Made editorial changes and revisions. The content is unchanged.

## A.3 October 2007

The following sections were added or changed:

| Location | Change |
|---|---|
| Section 2.3, “Enterprise Client/Server Communications,” on page 12 | All data are also sent to the server in the clear. For most deployments, this setting is maintained for performance. Currently, this setting cannot be changed. |
| Section 2.12, “Controlling Access to the iFolder Data Store,” on page 14 | Updated the section to include the new path to the simias directory, where the iFolder server stores the database and user files. |
| Section 2.13, “Controlling Access to the iFolder Server Configuration Files,” on page 14 | Updated the default path to the iFolder configuration files. |
| Section 2.14, “Controlling Access to And Backing Up the iFolder Audit Logs,” on page 14 | Updated the default path to the iFolder audit logs. |
| Section 2.18, “Loading the Recovery Agent Certificates,” on page 16 | The Novell iFolder service by default is not configured for the Recovery agent. During server configuration, ensure that the Recovery agent path is configured. |
| Section 3.4, “Creating an Encrypted iFolder,” on page 18 | The Novell iFolder 3.6 server supports encrypted iFolder storage. To store the files encrypted, the user must ensure that the iFolder is created encrypted before uploading the files. |
| Section 3.5, “Using the Recovery Agent,” on page 18 | The Novell iFolder 3.6 enterprise server uses a Recovery agent, which is an X.509 certificate-based entity used to recover a lost or otherwise unavailable key. |
| Section 3.6, “Transferring the Encryption Key,” on page 18 | For secure OTP transfer, make sure that the Recovery agent uses an out-of-band communication or a separate e-mail communication to send the passphrase and the key to the user. |

## A.4 August 15, 2006

The following change was made to this section:

| Location | Change |
|---|---|
| Section 2.6, “Configuring a Cipher Suite to Use for SSL/TLS,” on page 13 | Do not disable the Low and Export cipher suites if they are required by your customer base. Individuals using older browsers (4-5 years old) and older versions of Windows, such as Windows 98, might still need those cipher suites for other services. |

## A.5 November 1, 2005

The entire guide was reformatted to comply with revised Novell documentation standards. The content is unchanged.