Novell iFolder®

3.x

www.novell.com

SECURITY ADMINISTRATOR GUIDE

August 15, 2006

Novell®

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

This guide provides specific instructions on how to install, configure, and maintain Novell® iFolder® 3.*x* and the iFolder™ client for iFolder 3.*x* 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 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 3.x and the iFolder client, see the *Novell iFolder 3.x Readme* (http://www.novell.com/documentation/ifolder3/readme/data/readme.html).

Additional Documentation

For information, see the following:

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

Documentation Conventions

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

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

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

Security Best Practices Overview

1

This section summarizes the recommended configurations and settings required to run Novell® iFolder® 3.*x* and the iFolder™ client in a secure mode.

- Section 1.1, "Security Recommendations for iFolder 3.x," on page 9
- Section 1.2, "Security Recommendations for OES Linux," on page 10

1.1 Security Recommendations for iFolder 3.*x*

The following table lists the iFolder server configuration settings that are security related or that impact the security of iFolder resources.

Parameter	Possible Values	Default Value	Recommended Value for Best Security
Port for server to LDAP server communications *iManager > Novell iFolder 3 > System > LDAP Settings > Server Port*	Port 636 (secure) or port 389 (insecure)	636, secure	636, secure
SSL for server to LDAP server communications *iManager > Novell iFolder 3 > System > LDAP Settings > Port Is Secure*	Select *Yes* to enable SSL; deselect *Yes* (No) to disable SSL	Yes, SSL enabled	Yes, SSL enabled
iFolder Proxy user *iManager > Novell iFolder 3 > System > LDAP Settings > iFolder Proxy User*	Autogenerated during the iFolder enterprise server configuration; can be modified thereafter	Autogenerated	Keep the autogenerated iFolder Proxy username; if you change it, make sure the username is different than the iFolder Admin user, equivalent iFolder Admin users, and other system users; and update the Proxy User password.
iFolder Proxy user password *iManager > Novell iFolder 3 > System > LDAP Settings > Proxy User Password*	User-specified	Autogenerated during initial configuration of the iFolder server	User-specified, using strong password practices
Web browser to iManager Server communications	HTTPS and Novell eDirectory™ authentication	HTTPS and eDirectory authentication	HTTPS and eDirectory authentication

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
Port for iManager to server communications *iManager > Novell iFolder 3 > (select any task to go to the iFolder Login page) > Port*	Port 443 (secure) or port 80 (insecure)	443, secure	443, secure
SSL for iManager to server communications *iManager > Novell iFolder 3 > (select any task to go to the iFolder Login page) > Secure*	Select *Secure* (secure) to use SSL; deselect *Secure* (insecure) to use unencrypted connections	Select Secure, SSL enabled	Select Secure, SSL enabled
Server to client communications	SimiasRequireSSL (Yes/No)	SimiasRequireSSL = Yes	SimiasRequireSSL = Yes
`/opt/novell/ifolder3/web/web.config` file	SimiasSSLPort (443/80)	SimiasSSLPort = 443	SimiasSSLPort = 443

1.2 Security Recommendations for OES Linux

For information about security issues in Novell Open Enterprise Server, see the following in the *Novell OES Planning and Implementation Guide* (http://www.novell.com/documentation/oes/implgde/data/front.html):

- "Authentication" (http://www.novell.com/documentation/oes/implgde/data/authentication.html)
- "Security" (http://www.novell.com/documentation/oes/implgde/data/security.html)

Security Best Practices for Novell iFolder 3.*x*

2

This section provides specific instructions on how to install, configure, and maintain Novell® iFolder® 3.*x* in the most secure way possible.

2.1 Using SSL for Server - LDAP Server Communications

By default, the iFolder enterprise server and Web Access server are 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 machine as the iFolder enterprise server, an administrator can reconfigure to disable SSL, which increases the performance of LDAP authentications.

For information, see “Configuring the Enterprise Server for SSL Communications with the LDAP Server” in the *Novell iFolder 3.x Administration Guide*.

2.2 Using SSL for Enterprise Server - iManager Communications

By default, the Novell iFolder 3.*x* plug-in to iManager uses SSL for communications to the iFolder enterprise server being managed. For most deployments, this setting should not be changed. If the iManager server and the iFolder enterprise server are on the same computer, SSL is not required. For HTTP connections, the password is passed in the clear.

For information, see "Accessing the Novell iFolder 3 Plug-In for iManager" in the *Novell iFolder 3.x Administration Guide*.

2.3 Using SSL for Enterprise Server - Client Communications

By default, the iFolder enterprise server is configured to require SSL. All client communication to the server is encrypted using the SSL protocol. 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.

For information, see "Configuring the Enterprise Server for SSL Communications with the iFolder Client" in the *Novell iFolder 3.x Administration Guide*.

If you disable SSL for server-client 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 21.

2.4 Using SSL for Enterprise Server - Web Access Server Communications

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. If the Web Access server co-exists on the same machine as the iFolder enterprise server, an administrator can reconfigure to disable SSL, which increases the performance of local communications between the two servers.

For information, see "Configuring the Web Access Server for SSL Communications with the Enterprise Server" in the *Novell iFolder 3.x Administration Guide*.

2.5 Using SSL for Web Access Server - Users' Web Browser 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 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.x Administration Guide*.

If you disable SSL for server-client 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 21.

2.6 Disabling 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 secure against 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. If you disable SSL 2.0 on the server, it is not possible to establish a session using SSL 2.0, and version rollback attacks are not be possible.

For information about disabling SSL 2.0 protocol for the Apache server, see "Configuring the SSL Cipher Suites for the Apache Server" in the *Novell iFolder 3.x 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 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 Low and Export cipher suites if they are required by your customer base. Those 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.x 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.

2.8 Installing Trusted Roots and Certifications on the iFolder server

You should 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.x Administration Guide*.

2.9 Installing Server Certificates from a Known Certificate Authority

You should use valid certificates for both the Apache server and the 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 pubic key signed by a known Certificate

Authority (CA). For information, see "Generating an SSL Certificate for the Server" in the *Novell iFolder 3.x Administration Guide*.

2.10 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 a Shared Volume for an iFolder Cluster" in the *Novell iFolder 3.x Administration Guide*.

2.11 Ensuring Privilege Separation for the iFolder Proxy User

The iFolder Proxy user is a proxy user identity used to access the LDAP server with Read access to retrieve a list of authorized users. The proxy user is automatically created during the iFolder enterprise server configuration in YaST. The username is autogenerated to be unique on the system. For most deployments, this username should never change.

The iFolder Admin user or equivalent can use the iFolder 3.*x* iManager plug-in to change the iFolder Proxy user identity in the LDAP settings for the iFolder server. Make sure that the user account assigned as the iFolder Proxy user is different than the one used for the iFolder Admin user and other system users. Separating the proxy user from the administrator provides privilege separation.

The proxy user password is stored briefly in the `/opt/novell/ifolder3/etc/simias-server-bootstrap.config` on the iFolder server after configuring the iFolder enterprise server and before the iFolder service is started for the first time. The restart of Apache is forced at the end of the configuration process, which starts the iFolder service. During the initial startup, the iFolder process reads the `simias-server-bootstrap.config` file, stores the password in reversible encrypted format in the server's Simias database, and then removes the password from the file. For information, see "Admin User Considerations" in the *Novell iFolder 3.x Administration Guide*.

For information about modifying the password, see the iFolder Proxy User setting in "Modifying the iFolder LDAP Settings" in the *Novell iFolder 3.x Administration Guide*.

2.12 Securing the iFolder Proxy User Password

The iFolder Proxy user's password is used to authenticate the iFolder Proxy user to the LDAP server when iFolder synchronizes users for the iFolder user list.

When you initially configure the iFolder enterprise server in YaST, iFolder autogenerates a password for the iFolder proxy user, using the BASH random number generator for a number between 0 and 10,000. Initially, the password for the iFolder Proxy user is stored in clear text in the `/opt/novell/ifolder3/etc/simias-server-bootstrap.config` file. At the end of the configuration process, the system reboots Apache 2 and starts iFolder. When iFolder runs this first time after configuration, the iFolder process copies the simias-server-bootstrap.config file to the Simias.config file. The default location of the `Simias.config` file is `/var/lib/wwwrun/.local/share/simias` directory or the `/home/wwwrun/.local/share/simias` directory. The proxy user password is stored in a reversible encrypted form in the Simias database, then the value is removed from both configuration files.

The password stored on the system for the iFolder Proxy user must match the password stored in the iFolder Proxy user's eDirectory™ object. If you ever modify the iFolder Proxy user password in eDirectory, you must also change the password stored on the system. For example, if you change the iFolder Proxy user assignment, or if you want to set a longer password for the iFolder Proxy user, you must modify the values in iFolder's LDAP settings or iFolder cannot access the LDAP server to update the user list. For information, see "Modifying the iFolder Proxy User Password" in the *Novell iFolder 3.x Administration Guide*.

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

To protect the password when authenticating to the LDAP server, make sure to configure the LDAP Server Port and Port Is Secure options in the iFolder LDAP settings for secure (default) communications between the servers and the LDAP server. For information, see "Modifying the iFolder LDAP Settings" in the *Novell iFolder 3.x Administration Guide*.

2.13 Using Synchronize Now to Remove Users Effective Immediately

The iFolder User list is periodically updated based on the LDAP synchronization interval. Whenever you remove users from a LDAP Search DN, or remove contexts from the Search DN list, you should synchronize the list immediately using Update and Synchronize now to enforce your changes. For information, see "Synchronizing the iFolder User List with the LDAP Server" in the *Novell iFolder 3.x Administration Guide*.

2.14 Controlling Access to the iFolder Data Store

The iFolder server stores the database and user files under the `/var/opt/novell/ifolder3/simias` directory. By default, the Apache Server user "wwwrun" owns those files. Administrators of the iFolder 3.*x* server machine must use every precaution to not inadvertently assign rights to unauthorized users.

2.15 Controlling Access to the iFolder Server Configuration Files

The iFolder server stores the configuration files in the `/var/lib/wwwrun/.local/share/simias` directory (or in the `/home/wwwrun/.local/share/simias` directory if NSS is post-installed on the server). The Apache Server user "wwwrun" owns the configuration file. Administrators of the iFolder 3.*x* server machine must use every precaution to not inadvertently assign rights to unauthorized users.

2.16 Controlling Access to and Backing Up the iFolder Audit Logs

By default, the iFolder server stores the audit logs in the `/var/opt/novell/simias` 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.x Administration Guide*.

2.17 Storing iFolder 3.*x* Data Nonencrypted on the Server

iFolder 3.*x* uses SSL to encrypt data exchanges between the client and enterprise server and the user Web browser and the Web Access server. The client and server do not store iFolder data in encrypted format. This is different than iFolder 2.1*x*, which provides passphrase-based encryption. Users and administrators need to be aware of this to determine which users have data that is eligible to an iFolder 3.*x* system. Some users might need to continue to use the iFolder 2.1*x* services.

For information, see "Migrating User Files from an iFolder 2.1x to a 3.x Server" in the *Novell iFolder 3.x Administration Guide*.

2.18 Preventing the Propagation of Viruses

Because iFolder is a cross-platform distributed solution, there is a possibility of a virus infection on on 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. For information, see "Configuring Local Virus Scanner Settings for iFolder Traffic" in the *iFolder User Guide for Novell iFolder 3.x*.

2.19 Backing Up the iFolder Server

Backup of iFolder user data and configuration data should be performed regularly. 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.x Administration Guide*:

- "Backing Up the iFolder Server"
- "Backing Up the iFolder Store with the TSAIF"
- "Recovering from a Catastrophic Loss of the iFolder Server"
- "Recovering Individual Files or Directories"

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

- 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 barcodes, stored in environmentally friendly

conditions, and are handled by a company whose reputation rests on its ability to handle your media properly.

Security Best Practices for the iFolder Client

3

This section provides specific instructions on how to install, configure, and maintain the iFolder™ client for Novell® iFolder® 3.*x* 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. For information, see "Configuring Local Firewall Settings for iFolder Traffic" in the *iFolder User Guide for Novell iFolder 3.x*.

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. For information, see "Configuring Local Virus Scanner Settings for iFolder Traffic" in the *iFolder User Guide for Novell iFolder 3.x*.

3.3 Configuring a Web Browser to Use SSL 3.0

Novell iFolder 3.*x* 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.

Other Security Best Practices

4

This section discusses other security best practices for your Novell® iFolder® 3.*x* 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 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® 3.*x* to use SSL (HTTPS) connections for all data exchanges between its different components because the iFolder authentication and iFolder data are not encrypted. If you configure iFolder to use insecure connections for communications 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, “Using SSL for Enterprise Server - Client Communications,” on page 12
- Section 2.5, “Using SSL for Web Access Server - Users’ Web Browser 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 21.
- 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 Passwords

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 mix of letters and numbers. It should contain both uppercase and lowercase letters and at least one numeric character. Adding numbers to passwords, especially when 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. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

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

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

This document was updated on the following dates:

A.1 August 15, 2006

Updates were made to the following sections. Changes are explained below.

A.1.1 Security Best Practices for iFolder 3.x

The following change was made to this section:

Location	Change
Section 2.7, "Configuring a Cipher Suite to Use for SSL/TLS," on page 13	Do not disable Low and Export cipher suites if they are required by your customer base. Those 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.2 November 1, 2005

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