Novell NetWare® 6.5

www.novell.com

SECURITY OVERVIEW

February 28, 2005

Novell®

Legal Notices

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

www.novell.com

NetWare 6.5 Security Overview
February 28, 2005

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.
DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
exteNd is a trademark of Novell, Inc.
exteNd Director is a trademark of Novell, Inc.
GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare is a registered trademark of Novell, Inc. in the United States and other countries.
NMAS is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.
Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.
Novell SecretStore is a registered trademark of Novell, Inc. in the United States and other countries.
Nsure is a trademark of Novell, Inc.
ZENworks is a registered trademark of Novell, Inc. in the United States and other countries.

Third-Party Materials

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

Contents

About This Guide

As a key component of the Novell® One Net vision, Novell Nsure™ places a robust identity and access management foundation at the heart of your IT infrastructure. This foundation unifies identity information and policies across all the different systems in your organization. NetWare® 6.5 includes several Nsure products and services that allow you to centrally manage access to your systems and resources. They allow you to safeguard your resources from intruders and to present your customers, partners, and employees with a dynamic combination of information, resources, and processes—all based on their relationship with your business.

Documentation Updates

For the most recent version of the *NetWare 6.5 Security Overview*, see the NetWare 6.5 Security Overview online documentation (http://www.novell.com/documentation/lg/nw65/security_overview/data/a20gkue.html).

Documentation Conventions

In this 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 UNIX*, should use forward slashes as required by your software.

User Comments

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.

1 Authentication

This section discusses authentication and the related products Novell® offers in NetWare® 6.5:

Extended Characters in Passwords

In the past, Novell has not supported international or extended characters in passwords. In some instances passwords with these extended characters would work, but it was only by chance. Extended characters were handled in different ways by different products and services.

All Novell products and services are being developed to work with extended character (UTF8-encoded) passwords. For a current list of products and services that work with extended characters, see Novell TID 10083884 (http://support.novell.com/servlet/tidfinder/10083884).

NetIdentity Agent

The NetIdentity agent works with Novell eDirectory™ authentication to provide background authentication to Windows* Web-based applications that require eDirectory authentication such as iPrint, Novell exteNd™ Director™, Novell eGuide, Novell Virtual Office, ZENworks®, NetStorage, and iManager. NetIdentity provides a secure identity "wallet" on the workstation so that applications that require eDirectory authentication can access these credentials and bypass asking users for their usernames and passwords.

NOTE: NetIdentity browser authentication is supported only by Windows Internet Explorer. It is not supported by Apple* or Netscape* Navigator*.

If the agent software is installed on the workstation and users authenticate to eDirectory through Novell Client™ login or through a Web-based application that uses the NetIdentity agent, users are not prompted to log in when opening another application that requires eDirectory authentication.

NOTE: The Novell Client provides authentication credentials to NetIdentity but does not obtain authentication credentials from NetIdentity because it is not a Web-based application

In order to use NetIdentity, you must have the Middle Tier (XTier) framework installed on NetWare 6.5 servers in the tree that is identified by the host used in the URL for the Web-based applications and the NetIdentity agent installed on the workstations.

For more information on using the Netdentity agent, see the *NetIdentity Agent Administration Guide for NetWare 6.5* (http://www.novell.com/documentation/lg/netidentity).

Novell Modular Authentication Services (NMAS)

Novell Modular Authentication Service (NMAS™) is designed to help you protect information on your network. NMAS provides additional ways of authenticating to Novell eDirectory on NetWare, Windows, and UNIX networks to help ensure that the people accessing your network resources are who they say they are.

In previous releases of NetWare and eDirectory, Novell bundled an evaluation version of NMAS (Standard Edition) that was a scaled-down version of NMAS Enterprise Edition. Novell no longer provides a standard edition and an enterprise edition. Starting with NetWare 6.5, Novell provides a fully functional version of NMAS to the products that bundle it.

The NMAS server components are installed as part of the NetWare 6.5 installation process. You must also install the NMAS client on each workstation that will be authenticating using NMAS.

NMAS provides multiple login methods to choose from based on three login factors (password, physical device or token, and biometric authentication). For example, you can have users log in using a password, a fingerprint scan, a token, a smart card, a certificate, a proximity card, etc. Or you can have them log in using a combination of methods, which provides a higher level of security. Some login methods require additional hardware and software not included with the NMAS product. Make sure that you have all of the necessary hardware and software for the methods you will use.

NMAS includes several login methods on the Client CD (CD-10). The login methods are located in the nmas\nmasmethods folder. Other third-party methods are available for download. For information on the available third-party login methods, see the NMAS Partner's Web site (http://www.novell.com/products/nmas/partners). Each method has a readme.txt file or a readme.pdf file that will include specific installation and configuration instructions.

For more information on how to use NMAS, see the *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide* (http://www.novell.com/documentation/lg/nmas23).

Universal Password

Novell eDirectory includes some enhancements in the way passwords are handled and maintained. These changes provide several benefits.

In the past, administrators have had to manage multiple passwords (simple password, NDS® passwords) because of password limitations. Administrators have also had to deal with keeping the passwords synchronized.

- NDS Password: The older NDS password is stored in a hash form that is non-reversible in eDirectory. Only the NDS system can make use of this password, and it cannot be converted into any other form for use by any other system.
- Simple Password: The simple password provides a reversible value stored in an attribute on the user object in eDirectory. NMAS securely stores a clear-text value of the password so that it can use it against any type of authentication algorithm. To ensure that this value is secure, NMAS uses either a DES key or a triple DES (key depending upon the strength of the Secure Domain Key) to encrypt the data in the NMAS Secret and Configuration Store.

  The simple password was originally implemented to allow administrators to import users and hashed passwords from foreign LDAP directories such as Active Directory* and iPlanet*.

  The limitations of the simple password are that no password policy (minimum length, expiration, etc.) is enforced. Also, by default, users do not have rights to change their own simple passwords.

Universal Password enforces uniform password policy across multiple authentication systems (such as Native File Access). Universal password also manages multiple types of password authentication methods from disparate systems. This is done by creating a common password that can be used by all protocols to authenticate users.

Universal Password is managed by the Secure Password Manager (SPM), a component of the NMAS module (nmas.nlm on NetWare). SPM simplifies the management of password-based authentication schemes across a wide variety of Novell products as well as our partner's products. The managment tools only expose one password and do not expose all of the behind-the-scenes processing for backwards compatibility.

All of the password restrictions and policies (expiration, minimum length, etc.) are supported.

Secure Password Manager and the other components that manage or make use of Universal Password are installed in the NetWare 6.5 install; however, Universal Password is disabled by default. Because all APIs for authentication and setting passwords are moving to support Universal Password, all the existing management tools, when run on clients with these new libraries, automatically work with the Universal Password.

The Novell Client supports the Universal Password. It will also continue to support the NDS password for older systems in the network. The Novell Client has the capability of automatically upgrading to the new Password from the NDS password.

For a more details about deploying the Universal Password, see the *NetWare 6.5 Universal Password Deployment Guide* (http://www.novell.com/documentation/lg/nw65/universal_password/data/front.html).

2 Encryption

The Novell®International Cryptography Infrastructure (NICI) is the Novell solution to a cross-platform, policy-driven, independently certified, and extensible cryptography service. NICI is the cryptography module that provides keys, algorithms, various key storage and usage mechanisms, and a large-scale key management system.

Novell International Cryptography Infrastructure (NICI)

NICI controls the introduction of algorithms and the generation and use of keys. NICI allows production of a single commodity version of security products that support strong cryptography and multiple cryptographic technologies for worldwide consumption. Initial services built on this infrastructure are Directory Services (Novell eDirectory™), Novell Modular Authentication Services (NMAS™), Novell Certificate Server™, Novell SecretStore®, and TLS/SSL.

NICI includes the following key features:

- Supports industry standards. NICI is implemented following recognized industry standards.
- Certified. NICI is FIPS-140-1 certified on selected platforms.
- Cross-platform support. NICI is available on a variety of operating systems and platforms.
- Complies with governmental export and import regulations. NICI has cryptographic interfaces that are exportable from the U.S. and importable into other countries with government-imposed constraints on the export, import, and use of products that contain embedded cryptographic mechanisms.
- Secure and tamper-resistant architecture. The NICI architecture uses digital signatures to implement a self-verification process so that consuming services are assured that NICI has not been modified or tampered with when it is initialized.

For more information on how to use NICI, see the *NICI 2.6x Administration Guide* (http://www.novell.com/documentation/lg/nici20).

3 Identity Management

Today's businesses are faced with the challenge of managing user accounts in many independent systems. The creation and management of separate user accounts is expensive and prone to data synchronization errors.

DirXML® is a data-sharing solution that leverages Novell® eDirectory™ to automatically synchronize, transform, and distribute information across applications, databases, and directories.

DirXML Starter Pack

The solution included with NetWare® 6.5 provides licensed synchronization of information held in NT Domains, Active Directory, and eDirectory. Additionally, evaluation drivers for several other systems including PeopleSoft*, GroupWise®, and Lotus* Notes*, are included to allow you to explore data synchronization for your other systems.

When data from one system changes, DirXML detects and propagates these changes to other connected systems based on the business policies you define. Using DirXML rules and style sheets, you can make any of these systems the authoritative source for all or some of the data, or you can make each of the systems equally responsible for updating any data changes.

This solution also offers you the ability to synchronize user passwords. With PasswordSync, a user is required to remember only a single password to log in to any of these systems. Administrators can manage passwords in the system of their choice. Any time a password is changed in one of these environments, it is updated in all of them.

For more information about DirXML Starter Pack, see the DirXML Starter Pack online documentation Web site (http://www.novell.com/documentation/lg/dirxmlstarterpack/treetitl.html).

4 Public Key Infrastructure (PKI)

Novell® Certificate Server™ provides public key cryptography services that are natively integrated into Novell eDirectory™ and that allow you to mint, issue, and manage both user and server certificates. These services allow you to protect confidential data transmissions over public communications channels such as the Internet.

Novell Certificate Server

Novell Certificate Server offers the following public key infrastructure services:

- Provides public key cryptography services on your network

  You can create an Organizational Certificate Authority (CA) within your eDirectory tree, allowing you to issue an unlimited number of user and server certificates. You can also use the services of an external certificate authority, or use a combination of both as your needs dictate.

- Controls the costs associated with obtaining and managing public key certificates

  You can create an Organizational CA and issue public key certificates through the Organizational CA.

- Allows public key certificates to be openly available while also protecting them against tampering

  Certificates are stored in eDirectory and can therefore leverage eDirectory replication and access control features.

- Allows private keys to be accessible to only the software routines that use them for signing and decrypting operations

  Private keys are encrypted by Novell International Crytography Infrastructure (NICI) and made available only to the software routines using them for signing and decrypting operations.

- Securely backs up private keys

  Private keys are encrypted by NICI, stored in eDirectory, and backed up using standard eDirectory backup utilities.

- Allows central administration of certificates using ConsoleOne®. You can also perform some administration tasks using Novell iManager.

  ConsoleOne snap-ins are provided, allowing you to manage certificates issued from your Organizational CA or from any other CA that supports a certificate signing request in PKCS #10 format. The Novell iManager plug-in also allows you to some administration tasks.

- Allows users to manage their own certificates

  Users can use ConsoleOne to export keys for use in cryptography-enabled applications without system administrator intervention.

- Supports popular e-mail clients and browsers

  Novell Certificate Server allows you to create and manage user certificates for securing e-mail. Novell Certificate Server supports GroupWise® 5.5, Microsoft* Outlook 98 and Outlook 2000, Netscape Messenger*, and other popular e-mail clients. It's also compatible with both Netscape Navigator and Microsoft Internet Explorer.

For more information on how to use Novell Certificate Server, see the *Novell Certificate Server 2.7 Administration Guide* (http://www.novell.com/documentation/lg/crt27).