

# Novell® eDirectory™ 8.8

[www.novell.com](http://www.novell.com)

---

TECHNICAL WHITE PAPER



**Novell®**

- 2 OVERVIEW
- 2 IDENTITY MANAGEMENT BASED ON NOVELL eDIRECTORY
- 3 WHAT NOVELL eDIRECTORY DOES
- 5 NEW IN eDIRECTORY 8.8
- 9 SUMMARY

# Overview



Novell eDirectory™, the world's leading directory service, just got better. With eDirectory version 8.8, multiple enhancements and improvements have been included which strengthen suitability for complex environments—whether centralized or distributed—and simplify installation, migration and management. Novell eDirectory 8.8 provides the most complete set of directory services available for a wide selection of operating systems, supported on Linux\*, UNIX\*, Windows\* and NetWare®.

New features and capabilities include the following:

- **Install & Upgrade Enhancements**—health checks, scriptable installs, patch management
- **Data Import Improvements**—bulk load import speed enhancements
- **Priority Sync**—modify critical data (e.g., passwords) immediately writing to all replicas at once
- **Multi-instance Support**—multiple instances of eDirectory on one server
- **Encryption**—more flexible encryption options
- **SASL GSSAPI Support**—authenticate to eDirectory through LDAP using Kerberos
- **Enhanced Universal Password Enforcement**—support special characters in passwords and enforce policies requiring case sensitivity

Novell eDirectory is the foundation for many of the world's largest and most complex identity management deployments—a high-end directory service that allows businesses to manage identities

and security access for employees, customers and partners. With eDirectory, businesses lay the groundwork for identity and access management solutions that span small-to-medium business, enterprise, business-to-business, business-to-consumer and Web services deployments.

Version 8.8 marks a major milestone for the Novell eDirectory product line with enhanced required for high-end deployments, as well as small and mid-sized organizations. Improvements in eDirectory 8.8 dramatically simplify installation and the process for updating support packs and patches, reducing the time and cost of administration as well as significantly simplifying an eDirectory rollout.

## IDENTITY MANAGEMENT BASED ON NOVELL eDIRECTORY

Novell eDirectory is a unique and powerful technology that simplifies the problem of controlling who has access to what. Novell eDirectory is particularly suited to enterprise organizations that are complex, distributed and require management at multiple levels. As a flexible

management framework, eDirectory can accommodate a vast range of resources including data, peripherals, connections and applications as well as users. No other identity management service has the flexibility to integrate such a broad collection of resources for precise and granular control. Nor is any other directory service architected to scale in size and across disparate systems and multiple locations like Novell eDirectory.

Novell eDirectory acts as a central repository for all identity information. Identity attributes include all standard variables such as user ID, password, location, department and more, plus can be extended to include customized attributes and multiple identities. eDirectory content can be centralized, distributed or replicated with automatic synchronization between data partitions, replicas and even other directory services or identity stores.

All eDirectory information is protected with the highest levels of security. Individual attributes can be encrypted and all connections or requests for information may be encrypted for secure access. Novell eDirectory is not tied to any particular physical machine and can be clustered or replicated to ensure fault tolerance.

Further, Novell eDirectory is platform agnostic running on multiple operating systems (Linux, UNIX, Windows or NetWare)—with interaction between instances of eDirectory on each platform—while providing identity management services for resources across all platforms simultaneously.

#### **WHAT NOVELL eDIRECTORY DOES**

To effectively and efficiently manage who has access to what requires a full-service directory.

Novell eDirectory is much more than a simple LDAP directory or a database of user names, passwords and access control lists. A full-service directory consists of specialized elements in an advanced architecture that provide a unique combination of identity and control services.

In a short, Novell eDirectory provides the single, centralized credential repository and common management platform required to control access to and effectively manage a company's applications, systems and services.

#### **Foundation for Identity Management**

At a high level, Novell eDirectory can become the authoritative source for an individual's identity. It is possible to precisely define all attributes associated with a specific individual that are required for any type of access, verification, authorization or permission. Novell eDirectory provides the ability to create an individual user object and then associate with this object all attributes or properties that accurately define it. This definition information is extensible, meaning new attributes can be designed for customization, and includes data (name, location, department, permissions, etc.) as well as relationships. Relationships include position in hierarchies, membership in groups, conditions, policies and more. The combination of identity definition and relationship information provides for unique and granular control as well as powerful organization-wide management.

The same identity capabilities (definition and relationship) are also applied to network resources such as peripherals, applications,

storage, connections, etc. Explicit definition of resources enables identification and location of resources and these relationships determine how resources are allowed to interact. Novell eDirectory controls how resources can access other resources with the same levels of security or based on the same types of policies as users. Identities are unique, well defined, protected from vulnerability and available for credentialed, controlled access to all types of resources.

### Repository

A Novell eDirectory competitive advantage is the unique architecture of the credential repository. Only a single identity is maintained but different credentials for different services are stored providing a “single source/all access” model. The concept of partitions and replicas makes it possible to widely distribute and scale a directory without creating bottlenecks or decreasing performance. eDirectory can be distributed across multiple servers, which eliminates dependencies or conditions that disable the service if a particular server becomes unavailable. Partitions provide the ability to scale across geography and in size without a decrease in performance, and synchronized replicas provide local rapid access to identity data.

Directory attribute data can also be pulled from eDirectory and made available for high-speed access in applications (such as white page directories) for internal or external use. APIs and standards-based access protocols like LDAP provide a high degree of flexibility in populating or extracting directory object and attribute information.

The fact that Novell eDirectory is platform agnostic provides great flexibility in mixed environments. Instances of eDirectory, partitions, replicas and associated services can reside on Linux, UNIX, Windows and NetWare—or any combination of these—and still seamlessly interoperate with the ability to create fault tolerant solutions, clusters and redundant systems. No other identity management repository is as flexible, secure or scalable.

### Management

A common management platform provides simplified control as well as directory content exposure. Novell eDirectory includes Novell iManager—a management interface that provides administrators a comprehensive and holistic view of all resources and relationships using a common Web browser—as well as a host of other monitoring, diagnostic and maintenance tools. Administration tasks can be delegated, providing the ability to more easily administer a globally distributed network. As appropriate, eDirectory also provides client and command-line management options.

As a result of its unique architecture and years of evolution in many of the world’s largest organizations, Novell eDirectory provides an unmatched selection of foundational identity services. Here is an overview of these service concepts.

### Storage

Content in Novell eDirectory is always safe because of the following characteristics:

- **Persistence**—impervious to hardware failure
- **Integrity**—ensures all synchronizations are validated

- **Segmentation**—able to split directory store into separate segments
- **Distribution**—segments or replicas can be distributed to other locations
- **Indexing**—content indexing enables high-speed access for various uses

### *Relationship*

Unique identity and powerful management is enabled through the following relationship characteristics:

- **Hierarchy**—provides identity based on location in tree hierarchy
- **Roles**—provides privileges based on roles, interests or behaviors
- **Reference**—maintains link integrity between multiple object/identity instances
- **Inference**—applies access privileges and policies based on context

### *Security*

Security ensures that resources are only available once identity is established. The following security characteristics apply:

- **Authentication**—process of proving identity to the system
- **Qualification**—multiple control elements applied to authentication process
- **Authority**—delegating, distributing or sharing authentication
- **Enforcement**—mechanisms for ensuring appropriate access
- **Audit**—tracking and historical logging of all transactions for audit

### *Discovery*

Discovery is the ability of a user or application to browse or consume the contents of a directory.

Discovery characteristics include:

- **Publication**—updating and sharing directory content
- **Notification**—alerting external systems that directory events have occurred
- **Search**—ad hoc retrieval of directory information
- **Retrieval**—allows information access in only a specified manner

These characteristics and others have been engineered into Novell eDirectory making it far more than a user database or simple LDAP directory. A full-service directory empowers administrators to safely and securely manage and control a network while experiencing dynamic organizational changes such as growth and integration and while accommodating new technology. The bottom line is that Novell eDirectory is the only full-service directory that simplifies, automates and protects information, while taking full advantage of emerging information and technologies.

### **NEW IN eDIRECTORY 8.8**

Novell eDirectory 8.8 includes enhancements for performance, security, consolidation and installation. The balance of this paper describes in detail the new features and enhancements available with eDirectory 8.8. For an in-depth description of all features, deployment scenarios and documentation, please visit the eDirectory Web site at: [www.novell.com/products/edirectory](http://www.novell.com/products/edirectory)

## Performance Enhancements

Several new enhancements in version 8.8 have enabled higher performance for specific functions. These include the following:

- **Priority Sync**—Priority Sync complements the existing eDirectory replication process by allowing administrators to designate particular identity attributes for priority synchronization when a change is made. With the normal replication process changes are synchronized in the order they are made. With Priority Sync, certain changes or operations can be given priority over the rest.

A common application of this feature is with passwords; a change to a user password can be made effective immediately throughout the system when the appropriate attributes are tagged for Priority Sync. With this feature, there is no lag time for access or vulnerability window where two passwords provide access to the same data.

- **Increased Import Performance**—Novell eDirectory has always allowed for mass updates using a variety of tools, including the OpenLDAP tools and the Novell Import Convert Export (ICE) utility. In eDirectory 8.8, Novell has continued to improve import performance in order to streamline the process of consolidating directory content.

## Installation Enhancements

The process of physically installing Novell eDirectory, on any of the available platforms, is standard and straightforward. In large enterprise organizations

with multiple IT centers in various locations, the process of configuring eDirectory components and ensuring that the entire directory is fault tolerant can require time and care when setting it up. Several new features of Novell eDirectory 8.8 simplify and streamline the install and configuration process.

- **Fully Scriptable**—The install process can be scripted with variables included or with prompts for input. This enables central administrators to automate and offload installation and configuration tasks. Scripts can accommodate different variables for configuration, including file and license locations as well as locations for application, data and configuration files.
- **DIB Location**—Administrators are free to specify the location of the directory information base (DIB) (previously restricted to a single location). This provides more flexibility in configuring clustered and fault tolerant solutions.
- **Pre-upgrade Health Check**—Since eDirectory can function as the “central nervous system” for an enterprise with identity information for every resource, location and user, it can become a complex configuration. The pre-upgrade health check process looks for abnormalities that would result in an improper upgrade and reports them. Administrators can ensure the upgrade installs cleanly, rather than perpetuating existing problems in the new environment. Pre-upgrade health checks are automatic when installing eDirectory 8.8 or can be initiated manually.
- **Configuration**—The time required to configure eDirectory has been considerably reduced and

administrators are allowed to decide which configuration options they wish to initiate. Schema checking, indexing and validity checking are all options that can be turned on or turned off as circumstances and time allow.

- **Patch Capabilities**—In many cases, a server or application can be upgraded without the need to reinstall the entire software package. Novell eDirectory 8.8 not only provides the ability to update a system via patches—adding new files and then restarting the process—but also the ability to roll back patch updates. This simplifies keeping directory applications current and up-to-date.
- **Deployment Using ZENworks® Linux Management (Ximian® Red Carpet®)**—Novell eDirectory 8.8 can be installed and updated remotely on Linux servers using Novell ZENworks Linux Management (formerly Ximian Red Carpet). ZENworks Linux Management enables administrators to install and manage Linux servers and workstations remotely. Using ZENworks Linux Management, eDirectory can easily be deployed, configured and controlled from any remote location.
- **Supervisor Rights**—Heretofore, installing eDirectory required supervisor rights to the tree root—sometimes a hindrance in a distributed enterprise. With eDirectory 8.8, supervisor rights to the tree root are no longer required.
- **Service Rights**—With version 8.8, eDirectory services can run as a non-root user. This again provides flexibility for configuration and helps accommodate multiple instances of eDirectory

on the same server while providing higher levels of security.

### Consolidation Enhancements

Features included with Novell eDirectory 8.8 that enable administrators to easily consolidate other directories and to standardize on a common directory platform include the following.

- **Bulk Load**—Bulk loading enables administrators to import directory and identity information from other sources. Schema checking and schema extension is possible and the entire process has been streamlined to make consolidation of directories or importing of information from other sources simple and easy. As mentioned above, bulk load performance for eDirectory 8.8 has been significantly enhanced.
- **Multi-instance Support**—Prior versions of eDirectory were only able to accommodate one instance of eDirectory per server. With Novell eDirectory 8.8, multiple instances of eDirectory can reside on the same server. This enables administrators to configure test trees, department- or project-specific trees, separate trees for internal and external use, and any of hundreds of other possible scenarios. Multiple instances of eDirectory can be consolidated to a single high-end server. Load balancing can be accomplished running multiple replicas on clustered servers. Training configurations can be used and tested without affecting production systems.
- **LDAP-based Backup**—LDAP-based backup allows third-party applications or developers

to backup eDirectory on all supported platforms. This allows for higher-performing backup options as well as object-centric backup and restore. Objects can optionally be backed up using incremental backups, allowing for backups that contain only objects that have been changed since the last full backup.

### Security Enhancements

As a central point for controlling access to all resources, a directory service must be solidly secure. Novell eDirectory 8.8 extends a long tradition of premium security by adding several new features including the following:

- **Encrypted Attributes**—Previous versions of eDirectory protected data content through controlled access, encrypted key pairs for passwords and a variety of other functions. Version 8.8 adds yet another level of security with the option to encrypt attribute data in the directory information database, or DIB. This becomes more valuable as more information (such as credit card numbers) are included as part of identity profiles.
- **Encrypted Replication**—While directory replication typically occurs behind the firewall or over a virtual private network (VPN), some organizations would also like to use the

public Internet—minus any additional security infrastructure—as their replication vehicle.

To address that need, and to provide yet another layer of directory security, Novell eDirectory 8.8 provides the ability to encrypt replication sessions for entire directories and selected partitions, inside or outside of the organization.

- **Enhanced Universal Password Enforcement**—Novell continues to provide additional password policy options via Universal Password. With Novell eDirectory 8.8, administrators have support for localization of passwords as well as the use of special characters in passwords. Policies requiring the use of case sensitive passwords can also be enforced.
- **Kerberos Authentication**—For organizations that use a Kerberos trusted third-party security model, Novell eDirectory 8.8 accommodates login through LDAP using Kerberos. The SASL—GSSAPI (Simple and Authentic Security Layer—Generic Security Services API) mechanism for Novell eDirectory 8.8 enables authentication to eDirectory through LDAP using a Kerberos ticket and without the need to enter the eDirectory user password. This feature is primarily useful for LDAP application users in environments that already have a Kerberos infrastructure in place.

## Feature Availability

Some of the features mentioned above are specific to Linux or UNIX. Below is a summary features chart that indicates which of the Novell eDirectory 8.8 functions are available on what platforms:

FEATURE	NETWARE	LINUX	UNIX	WINDOWS
<b>PERFORMANCE</b>				
Priority Sync	X	X	X	X
Health checks	X	X	X	X
<b>INSTALL</b>				
Package formats		X	X	
Deployment with ZENworks Linux Management		X		
Custom location for application files		X	X	X
Custom location for data files		X	X	X
Custom location for configuration files		X	X	
Non-root install		X	X	
License file location		X	X	
Server health checks	X	X	X	X
<b>CONSOLIDATION</b>				
Multiple instances		X	X	
Bulk load improvements	X	X	X	X
LDAP-based backup	X	X	X	X
<b>SECURITY</b>				
Enhanced Universal Password enforcement	X	X	X	X
Encrypted attributes	X	X	X	X
Encrypted replication		X	X	X

## SUMMARY

Novell eDirectory 8.8 provides expanded and enhanced identity management capabilities. As the next release of the world's premier directory service, eDirectory 8.8 continues in the tradition of powerful user/resource management with added security, manageability and increased performance.

Organizations with existing Novell directory services deployments will benefit from multi-instance support, new backup options, more flexible and powerful security features and a host of other enhancements in eDirectory 8.8. Those customers, as well as organizations newly adopting eDirectory, will also enjoy dramatically streamlined and

improved installation and upgrade processes

thanks to pre-upgrade health checks, support for ZENworks Linux Management, and improved performance with faster bulk load speeds and the new Priority Sync feature.

Novell eDirectory 8.8 enhances the world's leading identity and resource management solution, providing secure and scalable directory services for small, medium and enterprise organizations. eDirectory is a cross-platform, high performance, flexible directory service suitable for any organization seriously considering simplifying the critical task of managing who has access to what resources from inside or outside of the enterprise.

© 2005 Novell, Inc. All rights reserved.  
Novell, the Novell logo, the N logo,  
NetWare, Red Carpet, Ximian and  
ZENworks are registered trademarks,  
and eDirectory is a trademark of  
Novell, Inc. in the United States and  
other countries.

\*Linux is a registered trademark of  
Linus Torvalds. UNIX is a registered  
trademark of X/Open Company, Ltd.  
Windows is a registered trademark  
of Microsoft Corporation. All other  
third-party trademarks are the property  
of their respective owners.

### **Novell Product Training and Support Services**

For more information about  
Novell worldwide product  
training, certification programs,  
consulting and technical support  
services, please visit:

**[www.novell.com/services](http://www.novell.com/services)**

### **For More Information**

Contact your local  
Novell Solutions Provider,  
or visit the Novell Web site at:  
**[www.novell.com](http://www.novell.com)**

You may also call Novell at:

1 888 321 4272 U.S./Canada  
1 801 861 4272 Worldwide  
1 801 861 8473 Facsimile

**Novell, Inc.**  
404 Wyman Street  
Waltham, MA 02451 USA

**[www.novell.com](http://www.novell.com)**

**Novell**