

Novell Access Manager

3.0 SP2

www.novell.com

INSTALLATION GUIDE

February 22, 2008

Interim Release 1



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. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](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 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](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 latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	9
1 Introduction to Novell Access Manager	11
1.1 How Access Manager Works	11
1.1.1 Authentication	12
1.1.2 Identity Federation	12
1.1.3 Authorization	12
1.1.4 Identity Injection	13
1.2 Access Manager Features and Components	13
1.2.1 The Administration Console	13
1.2.2 Identity Servers	14
1.2.3 Access Gateways	15
1.2.4 SSL VPN	16
1.2.5 J2EE Agents	16
1.2.6 Policies	16
1.2.7 Certificate Management	17
1.2.8 Auditing and Logging	17
1.2.9 Embedded Service Provider	17
1.2.10 The User Portal Application	18
2 Installation Requirements	19
2.1 Recommended Installation Scenarios	19
2.1.1 Basic Setup	19
2.1.2 Advanced Network Configuration with a DMZ	21
2.2 Hardware Platform Requirements	21
2.3 Network Requirements	22
2.4 Access Manager 3 SP2 Administration Console Requirements	22
2.5 Access Manager 3 SP2 Identity Server Requirements	24
2.6 Access Manager 3 SP2 Access Gateway Requirements	25
2.7 Access Manager 3 SP2 SSL VPN Requirements	25
2.8 VMware ESX Requirements	26
3 Installing the Access Manager Administration Console	27
3.1 Installation Procedures	27
3.2 Logging In to the Administration Console	29
3.3 Enabling the Administration Console for Multiple Network Interface Cards	31
3.4 Administration Console Conventions	31
4 Installing the Novell Identity Server	33
5 Installing the Linux Access Gateway	35
5.1 Prerequisites for a Linux Access Gateway	35
5.2 Boot Screen Function Keys	36
5.3 Using a Standard Linux Installation with the Default Settings	36
5.4 Using the Advanced Installation Option	42

5.4.1	Planning Your Partition Strategy	42
5.4.2	Starting the Installation.	43
5.4.3	Customizing the Partitions	45
5.4.4	Configuring Date and Time Values	48
5.4.5	Customizing Optional Settings	49
5.4.6	Configuring Hardware and System Services	49
5.5	Viewing the Linux Installation Log	53
6	Installing the NetWare Access Gateway	55
6.1	Running the NetWare Installation Program	55
6.2	Configuring the Log Partition on the NetWare Access Gateway	57
6.3	Customizing Error Pages	58
7	Installing SSL VPN	59
7.1	Identifying the Installation You Should Use	59
7.1.1	Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server	60
7.1.2	Deployment Scenario 2: Access Gateway and SSL VPN on Different Servers	61
7.1.3	Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server .	62
7.2	SSL VPN and the Access Gateway	62
7.2.1	SSL VPN and the Linux Access Gateway	62
7.2.2	SSL VPN and the NetWare Access Gateway	62
7.3	Installing SSL VPN Services	63
7.3.1	Prerequisites	63
7.3.2	Deployment Scenario 1: Installing SSL VPN on the Linux Access Gateway	63
7.3.3	Deployment Scenario 2: Installing SSL VPN on a Separate Machine	64
7.3.4	Deployment Scenario 3: Installing Identity Server and SSL VPN on the same Machine	65
7.3.5	Verifying that Your SSL VPN Service Is Installed	66
7.4	Re-Installing SSL VPN on Linux Access Gateway	66
7.5	Installing the High Bandwidth Version of SSL VPN	67
7.6	Pre-Installing SSL VPN Client Components	68
7.6.1	Installing Client Components for Linux	68
7.6.2	Installing the Client Component for Macintosh	68
7.6.3	Installing the Client Component for Windows	69
8	Upgrading Access Manager Components	71
8.1	Upgrading the Administration Console	71
8.2	Upgrading the Identity Server	72
8.3	Upgrading the Linux Access Gateway	74
8.3.1	Prerequisites	74
8.3.2	Upgrading Linux Access Gateway by Using the Interactive Method	75
8.3.3	Upgrading Linux Access Gateway By Passing Parameters in the Command Line . .	75
8.3.4	Upgrading the Linux Access Gateway by Using the Administration Console	76
8.3.5	Installing the Latest Linux Patches	77
8.4	Upgrading the SSL VPN Server	79
8.4.1	Upgrading SSL VPN to IR1	79
8.4.2	Upgrading Low Bandwidth SSL VPN to High Bandwidth SSL VPN	80
8.4.3	Upgrading SSL VPN Installed with Linux Access Gateway	80
8.4.4	Upgrading SSL VPN Installed with Identity Server	80
8.5	Upgrading the NetWare Access Gateway	81
8.6	Verifying Version Compatibility	84

9	Removing Components	85
9.1	Uninstalling the Identity Server	85
9.1.1	Deleting NIDS References	85
9.1.2	Uninstalling NIDS	85
9.2	Reinstalling an Identity Server to a New Hard Drive	86
9.3	Uninstalling the Administration Console	86
9.4	Uninstalling the Access Gateway	87
9.5	Uninstalling the SSL VPN	87
10	Migrating from iChain to Access Manager	89
10.1	Understanding the Differences between iChain and Access Manager	89
10.1.1	Component Differences	89
10.1.2	Feature Comparison	90
10.2	Planning the Migration	91
10.2.1	Possible Migration Strategies	91
10.2.2	Outlining the Migration Requirements for Each Resource	97
10.3	Migrating Components	99
10.3.1	Setting Up the Hardware and Installing the Software	99
10.3.2	Using an L4 Switch	100
10.3.3	Configuring the Identity Server for Authentication	100
10.3.4	Configuring System and Network Settings	103
10.3.5	Migrating the First Accelerator	106
10.3.6	Enabling Single Sign-On between iChain and Access Manager	114
10.3.7	Migrating Resources with Special Configurations	117
10.3.8	Moving Staged Components	128
10.3.9	Removing iChain	129
A	Troubleshooting Installation	131
A.1	Troubleshooting the Access Gateway Import	131
A.1.1	Repairing an Import	131
A.1.2	Triggering an Import Retry	132
A.1.3	Troubleshooting the Import Process	133
A.1.4	Unlocking the NetWare Access Gateway Console	138
A.2	Troubleshooting Linux Access Gateway Installation	138
A.2.1	Some of the New Hardware Driver or Network Card are Not Detected During Manual or Advanced Installation	139
A.2.2	Manually Configuring a Network Interface	139
A.2.3	Manually Setting and Deleting the Default Gateway	140
A.2.4	Manually Configuring the Hostname, Domain Name and DNS Server	141
A.2.5	Troubleshooting Import Failure	142
A.3	Troubleshooting the SSL VPN Device Import	143
A.4	Troubleshooting the Administration Console Upgrade	143

About This Guide

The purpose of this guide is to provide an introduction to Novell® Access Manager and to describe the installation procedures.

- ♦ Chapter 1, “Introduction to Novell Access Manager,” on page 11
- ♦ Chapter 2, “Installation Requirements,” on page 19
- ♦ Chapter 3, “Installing the Access Manager Administration Console,” on page 27
- ♦ Chapter 4, “Installing the Novell Identity Server,” on page 33
- ♦ Chapter 5, “Installing the Linux Access Gateway,” on page 35
- ♦ Chapter 6, “Installing the NetWare Access Gateway,” on page 55
- ♦ Chapter 7, “Installing SSL VPN,” on page 59
- ♦ Chapter 8, “Upgrading Access Manager Components,” on page 71
- ♦ Chapter 9, “Removing Components,” on page 85
- ♦ Chapter 10, “Migrating from iChain to Access Manager,” on page 89
- ♦ Appendix A, “Troubleshooting Installation,” on page 131

Audience

This guide is intended for Access Manager administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

- ♦ Extensible Markup Language (XML)
- ♦ Simple Object Access Protocol (SOAP)
- ♦ Security Assertion Markup Language (SAML)
- ♦ Public Key Infrastructure (PKI) digital signature concepts and Internet security
- ♦ Secure Socket Layer/Transport Layer Security (SSL/TSL)
- ♦ Hypertext Transfer Protocol (HTTP and HTTPS)
- ♦ Uniform Resource Identifiers (URIs)
- ♦ Domain Name System (DNS)
- ♦ Web Services Description Language (WSDL)

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments 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 *Access Manager Installation Guide*, visit the [Novell Access Manager Documentation Web site](http://www.novell.com/documentation/novellaccessmanager) (<http://www.novell.com/documentation/novellaccessmanager>).

Additional Documentation

- ♦ *Novell Access Manager 3.0 SP2 Setup Guide*
- ♦ *Novell Access Manager 3.0 SP2 Administration Guide*
- ♦ *Novell Access Manager 3.0 SP2 J2EE Agent Guide*

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.

Introduction to Novell Access Manager

1

Novell® Access Manager is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager also provides seamless single sign-on across technical and organizational boundaries, and uses industry standards including SAML (Secure Assertions Markup Language) and Liberty Alliance protocols. Access Manager combines simplified deployment and administration with advanced capabilities, such as multi-factor authentication, role-based access control, Web single sign-on, data encryption, and SSL VPN, to provide secure access from any location.

This section discusses the following topics:

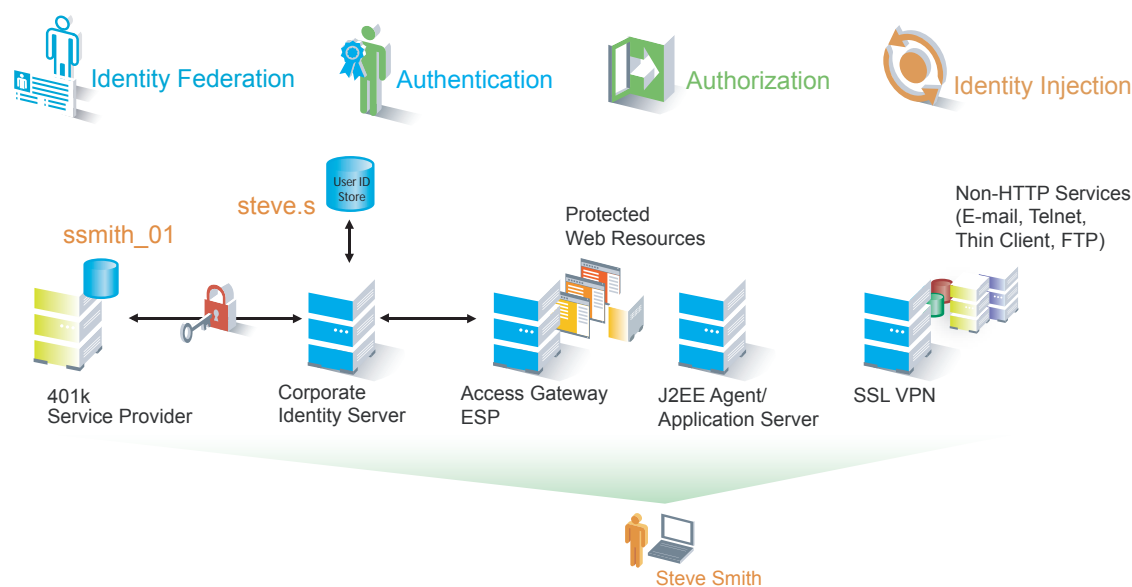
- Section 1.1, “How Access Manager Works,” on page 11
- Section 1.2, “Access Manager Features and Components,” on page 13

1.1 How Access Manager Works

Access Manager deployments typically use Identity Servers and Access Gateways to provide policy-driven access control for HTTP services. For non-HTTP services, Access Manager provides secure VPN and J2EE Agent components. You can use the Access Gateway on both NetWare® (soft appliance) or Linux.

Figure 1-1 illustrates the primary purposes of Access Manager: **authentication**, **identity federation**, **authorization**, and **identity injection**.

Figure 1-1 Access Manager



1.1.1 Authentication

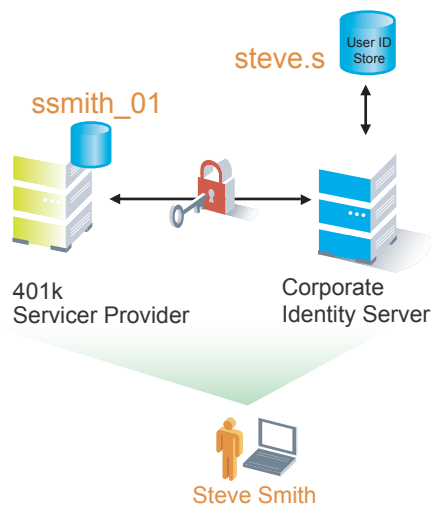
The **Identity Server** facilitates authentication for all Access Manager components. This authentication is shared with internal or external service providers on behalf of the user, by means of assertions. Access Manager supports a number of authentication methods, such as name/password, RADIUS token-based authentication, and X.509 digital certificates. You specify authentication methods in the contracts that you want to make available to the other components of Access Manager, such as the Access Gateway.

User data is stored in user stores. User stores are LDAP directory servers to which end users authenticate. You can configure a user store with more than one replica to provide load balancing and failover capability.

1.1.2 Identity Federation

Identity federation is the association of accounts between an identity provider and a service provider. As shown in **Figure 1-2**, an employee named Steve is known as `steve.s` at his corporate identity provider. He has an account at a work-related service provider called 401k, which has set up a trust relationship with his company. At 401k he is known as `ssmith_01`.

Figure 1-2 Identity Federation



As a service provider, 401k can be configured to trust the authentication from the corporate identity provider. Steve can enable single sign-on and single logout by federating, or linking, his two accounts.

From an administrative perspective, this type of sharing reduces identity management costs, because multiple organizations do not need to independently collect and maintain identity-related data, such as passwords. From the end user's perspective, this results in an enhanced experience by requiring fewer sign-ons.

1.1.3 Authorization

Authentication is the process of determining who a user is. Authorization is the process of determining what a user is allowed to do. Access Manager allows you to configure Identity Server roles and authorization policies, based on criteria other than authentication, to protect a resource.

Authorization policies are dynamically applied after authentication and are enforced when a user attempts to access a protected resource.

1.1.4 Identity Injection

An **Access Gateway** lets you retrieve information from your LDAP directory, use it to inject information into HTML headers, query strings, or basic authentication headers, and send this information to the back-end Web servers. Access Manager calls this technology *identity injection* (iChain® calls it object level access control). The Web server uses this information to personalize content, or can use it for additional authorization decisions. Where Web servers require additional authentication, Identity injection can also provide the necessary credentials to perform a single sign-on.

1.2 Access Manager Features and Components

This section describes the following Access Manager features:

- ♦ [Section 1.2.1, “The Administration Console,” on page 13](#)
- ♦ [Section 1.2.2, “Identity Servers,” on page 14](#)
- ♦ [Section 1.2.3, “Access Gateways,” on page 15](#)
- ♦ [Section 1.2.4, “SSL VPN,” on page 16](#)
- ♦ [Section 1.2.5, “J2EE Agents,” on page 16](#)
- ♦ [Section 1.2.6, “Policies,” on page 16](#)
- ♦ [Section 1.2.7, “Certificate Management,” on page 17](#)
- ♦ [Section 1.2.8, “Auditing and Logging,” on page 17](#)
- ♦ [Section 1.2.9, “Embedded Service Provider,” on page 17](#)
- ♦ [Section 1.2.10, “The User Portal Application,” on page 18](#)

1.2.1 The Administration Console

The Administration Console is the central configuration and management tool for the product. It is a modified version of iManager that can be used only to manage the Access Manager components. It contains an Overview option, which allows you to assess the health of all Access Manager components.

Figure 1-3 *Novell Access Manager Overview Page*



It also allows you to configure and manage each component, and allows you to centrally manage resources, such as policies, hardware, and certificates, which are used by multiple components.

1.2.2 Identity Servers

The Identity Server is the central authentication and identity access point for all other services. It is responsible for authenticating users and distributing role information to facilitate authorization decisions. It also provides the Liberty Alliance Web Service Framework to distribute identity information.

An Identity Server always operates as an identity provider and can optionally be configured to run as an identity consumer (also known as a service provider), using either Liberty, SAML 1.1, or SAML 2.0 protocols. As an identity provider, the Identity Server validates authentications against the supported identity user store, and is the heart of the user's identity federations or account linkage information.

In an Access Manager configuration, the Identity Server is responsible for managing:

- ♦ **Authentication:** Verifies user identities through various forms of authentication, both local (user supplied) and indirect (supplied by external providers). The identity information can be some characteristic attribute of the user, such as a role, e-mail address, name, or job description.
- ♦ **Identity Stores:** Links to user identities stored in eDirectory™, Microsoft* Active Directory*, or Sun ONE* Directory Server.
- ♦ **Identity Federation:** Enables user **identity federation** and provides access to Liberty-enabled services.
- ♦ **Account Provisioning:** Enables service provider account provisioning, which automatically creates user accounts during a federation request.
- ♦ **Custom Attribute Mapping:** Allows you to define custom attributes by mapping Liberty Alliance keywords to LDAP-accessible data, in addition to the available Liberty Alliance Employee and Person profiles.
- ♦ **SAML Assertions:** Processes and generates SAML assertions. Using SAML assertions in each Access Manager component protects confidential information by removing the need to pass user credentials between the components to handle session management.

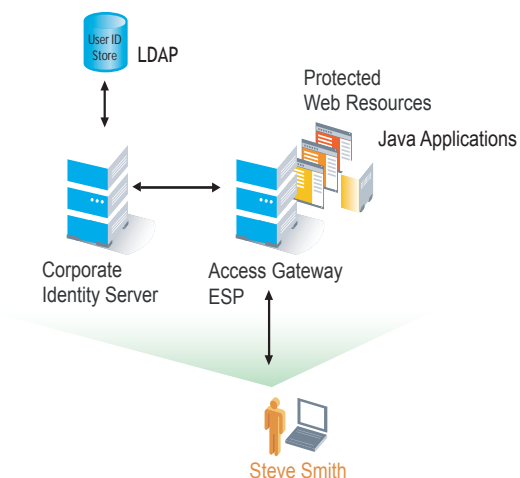
- ♦ **Single Sign-on and Logout:** Enables users to log in only once to gain access to multiple applications and platforms. Single sign-on and single logout are primary features of Access Manager and are achieved after the federation and trust model is configured among trusted providers and the components of Access Manager.
- ♦ **Access Gateway Integration:** Provides authentication and identity services to **Access Gateways** that are configured to protect Web servers, Java* applications, and SSL VPN. The Access Gateway and other Access Manager components include an embedded service provider that is trusted by Novell Access Manager Identity Servers.
- ♦ **Roles:** Provides RBAC (role-based access control) management. RBAC is used to provide a convenient way to assign a user to a particular job function or set of permissions within an enterprise, in order to control access. The identity provider service establishes the active set of roles for a user session each time the user is authenticated. Roles can be assigned to particular subsets of users based on constraints outlined in a role policy. The established roles can then be used in authorization **policies** and J2EE* permissions, to form the basis for granting and restricting access to particular Web resources.
- ♦ **Clustering:** Adds capacity and failover management. An Identity Server can be a member of a cluster of Identity Servers, and the cluster is configured to act as a single server. An Access Gateway can be a member of a group of Access Gateways, and the group is configured to act as a single server.

For an overview of Liberty, see “**About Liberty**” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

1.2.3 Access Gateways

An Access Gateway provides secure access to existing HTTP-based Web servers. It provides the typical security services (authorization, single sign-on, and data encryption) previously provided by Novell iChain, and is integrated with the new identity and policy services of Access Manager.

Figure 1-4 Access Gateway Component



The Access Gateway is designed to work with the Identity Server to enable existing Web services for Liberty and SAML. In addition to using **identity injection**, the Access Gateway can be configured so that it automatically fills in requested form information (called form fill). If your Web servers have not been configured to enforce authentication and authorization, you can configure the

Access Gateway to provide these services. Authentication contracts and authorization policies can be assigned so that they protect the entire Web server, a single page, or somewhere in between.

The Access Gateway can also be configured so that it caches requested pages. When the user meets the authentication and authorization requirements, the user is sent the page from cache rather than requesting it from the Web server, which can increase content delivery performance.

Access Manager provides both a NetWare and Linux version of the Access Gateway. Both the NetWare Access Gateway and Linux Access Gateway are soft appliances, which simplifies installation and configuration. For more information, see “[Access Gateway Configuration](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

1.2.4 SSL VPN

The SSL VPN component provides secure access to non-HTTP based applications, such as e-mail servers, FTP services, or Telnet services. SSL VPN is a Linux-based service, which is actually accelerated by (and shares session information with) the Access Gateway.

An ActiveX* plug-in or Java applet is delivered to the client on successful authentication. Roles and policies determine authorization decisions for back-end applications. Client integrity checking is available to ensure the existence of approved firewall and virus scanning software, before the SSL VPN session is established.

1.2.5 J2EE Agents

You install and configure the J2EE Agent components only when you need fine-grained access control to Java applications. Access Manager provides JBoss and IBM* WebSphere* server agents for Java 2 Enterprise Edition (J2EE) application servers.

These agents leverage the Java Authentication and Authorization Service* (JAAS) and Java Authorization Contract for Containers* (JACC) standards for Access Manager-controlled authentication and authorization to Java Web applications and Enterprise JavaBeans*. For more information about these Java authentication and authorization standards, see the [JAAS Authentication Tutorial \(http://java.sun.com/j2se/1.4.2/docs/guide/security/jaas/tutorials/GeneralAcnOnly.html\)](http://java.sun.com/j2se/1.4.2/docs/guide/security/jaas/tutorials/GeneralAcnOnly.html) and [Java Authorization Contract for Containers \(http://java.sun.com/j2ee/javaacc/index.html\)](http://java.sun.com/j2ee/javaacc/index.html).

Like the Access Gateway, J2EE Agents are federation-enabled and therefore operate as service provider agents. As such, they redirect all authentication requests to the Identity Server, which returns a SAML assertion to the component. This process has the added security benefit of removing the need to pass user credentials between the components to handle session management.

1.2.6 Policies

Policies provide the authorization component of Access Manager. Using policies, the administrator of the Identity Server defines how properties of a user’s authenticated identity map to the set of active roles for the user. This role definition serves as the starting point for role-based authorization policies of the Access Gateway and J2EE components. Additionally, authorization policies can be defined that control access to protected resources based on user and system attributes other than assigned roles.

The flexibility built into the policy component is nearly unlimited. You can, for example, set up a URL-based policy that permits or denies access to a protected Web site, depending on user roles, such as employee or manager.

Each Access Gateway and J2EE component includes an embedded service provider agent that interacts with the Identity Server to provide authentication, policy decision, and enforcement. For the Java application servers, the agent also provides role pass-through to allow integration with the Java Application server's authorization processes. For Web application servers, the Access Gateway provides the ability to inject the user's roles into HTTP headers to allow integration with the Web server's authorization processes.

1.2.7 Certificate Management

Access Manager includes a certificate management service, which allows you to manage centrally stored certificates used for digital signatures and data encryption. You can create locally signed certificates and import externally signed certificates and assign these certificates to the trust stores of the following components:

- ♦ **Identity Server:** Certificates allow you to provide secure authentication to the Identity Server and enable encrypted content from the Identity Server portal, via HTTPS. They also provide secure communications between trusted Identity Servers and user stores.
- ♦ **Access Gateway:** Uses server certificates and trusted roots to protect Web servers, provide single sign-on, and enable the product's data confidentiality features, such as encryption.
- ♦ **SSL VPN:** Uses server certificates and trusted roots to secure access to non-HTTP applications.
- ♦ **J2EE Agents:** The embedded service providers that Novell provides for the J2EE Agents use signing and SSL certificates. Access Manager's certificate management features can manage certificates for your J2EE application servers if the application server uses one of the supported key store types: Java Key Store (JKS) eDirectory, PKCS12 (or .pfx), DER (.cer).

You can install and distribute certificates to the Access Manager components and configure how the components use certificates. This includes central storage, distribution, and expired certificate renewal.

1.2.8 Auditing and Logging

Access Manager supports audit logging and file logging at the component level. A licensed version of Novell Audit is included to provide compliance assurance logging and to maintain audit log entries that can be subsequently included in reports. Each component creates assurance log entries to show the effect of each policy statement on each access control decision. Log entries include events such as notifications pertaining to the operational state of Access Manager components, the results of administrator and user requests, and policy actions invoked in determining request results.

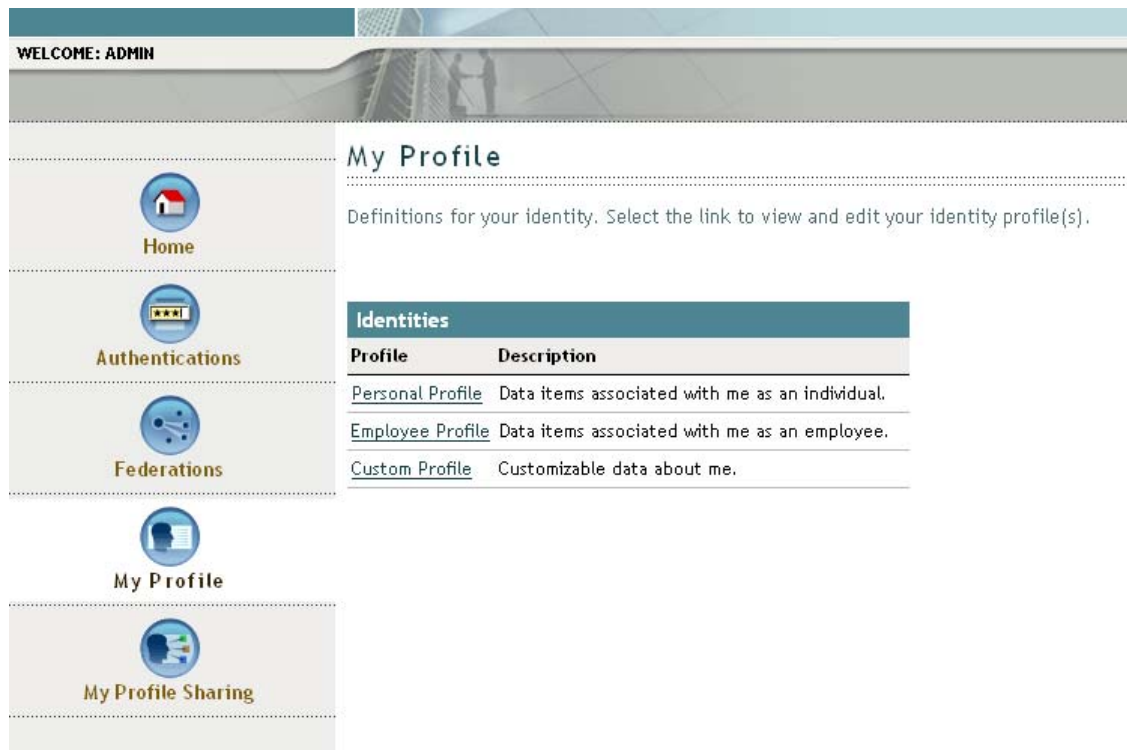
1.2.9 Embedded Service Provider

The Access Gateway and J2EE Agent use an embedded service provider to redirect authentication requests to the Identity Server. The Identity Server requires requests to be digitally signed and encrypted and allows only trusted devices to participate. To become trusted, devices must exchange metadata. The embedded service provider performs this task automatically for the Access Gateway and J2EE Agent.

1.2.10 The User Portal Application

The Access Manager User Portal is a customizable application where end users can access and manage their authentications, federations, and profile data. The authentication methods you create in the Administration Console are reflected in the Portal.

Figure 1-5 Access Manager User Portal



Help information for the end users is provided in the user interface. If you know how to customize JSP* pages, you can customize the portal for rebranding purposes and for creating custom login pages.

Installation Requirements

2

This section explains the requirements for installing the Novell® Access Manager 3 SP2. For a list of current filenames and for information about installing the latest release, please review the [Access Manager Readme \(http://www.novell.com/documentation/novellaccessmanager/readme/accessmanager_readme.html\)](http://www.novell.com/documentation/novellaccessmanager/readme/accessmanager_readme.html).

Because all of the components can be installed on separate machines, the following sections describe the software and hardware requirements of each component and suggest some possible installation scenarios:

- ♦ [Section 2.1, “Recommended Installation Scenarios,” on page 19](#)
- ♦ [Section 2.2, “Hardware Platform Requirements,” on page 21](#)
- ♦ [Section 2.3, “Network Requirements,” on page 22](#)
- ♦ [Section 2.4, “Access Manager 3 SP2 Administration Console Requirements,” on page 22](#)
- ♦ [Section 2.5, “Access Manager 3 SP2 Identity Server Requirements,” on page 24](#)
- ♦ [Section 2.6, “Access Manager 3 SP2 Access Gateway Requirements,” on page 25](#)
- ♦ [Section 2.7, “Access Manager 3 SP2 SSL VPN Requirements,” on page 25](#)
- ♦ [Section 2.8, “VMware ESX Requirements,” on page 26](#)

2.1 Recommended Installation Scenarios

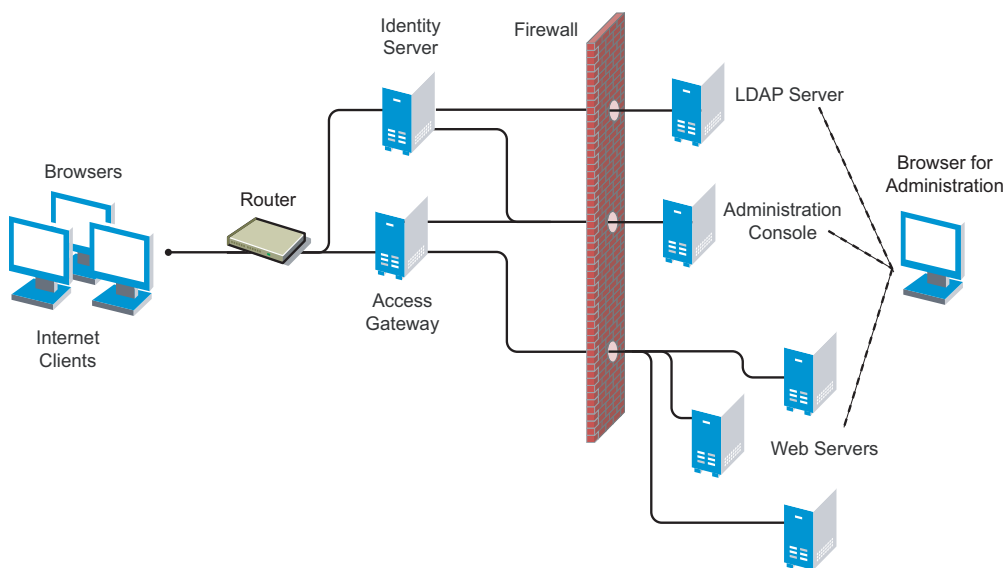
The following scenarios provide an overview of the flexibility built into Access Manager 3 SP2. Use them to design a deployment strategy that fits the needs of your company.

- ♦ [Section 2.1.1, “Basic Setup,” on page 19](#)
- ♦ [Section 2.1.2, “Advanced Network Configuration with a DMZ,” on page 21](#)

2.1.1 Basic Setup

For a basic Access Manager installation, you can install the Identity Server and the Access Gateway outside your firewall. [Figure 2-1](#) illustrates this scenario:

Figure 2-1 Basic Installation Configuration



1 Install the Administration Console.

The Administration Console and the Identity Server are bundled in the same download file or on CD 1.

2 If your firewall is set up, open the ports required for the Identity Server and the Access Gateway to communicate with the Administration Console: TCP 1443, TCP 8444, TCP 289, TCP 524, TCP 636.

For more information about these ports, see “[Setting Up Firewalls](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

3 Run the installation again and install the Identity Server on a separate server.

Log in to the Administration Console and verify that the Identity Server installation was successful.

4 Install the Access Gateway. You can install either the NetWare® (CD 2) or the Linux (CD 3 or download file).

Log in to the Administration Console and verify that the Access Gateway imported successfully.

5 Configure the Identity Server and the Access Gateway. See “[Setting Up a Basic Access Manager Configuration](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

In this configuration, the LDAP server is separated from the Identity Server by the firewall. Make sure you open the required ports. See “[Setting Up Firewalls](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

For information about setting up configurations for fault tolerance and clustering, see “[Clustering and Fault Tolerance](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*

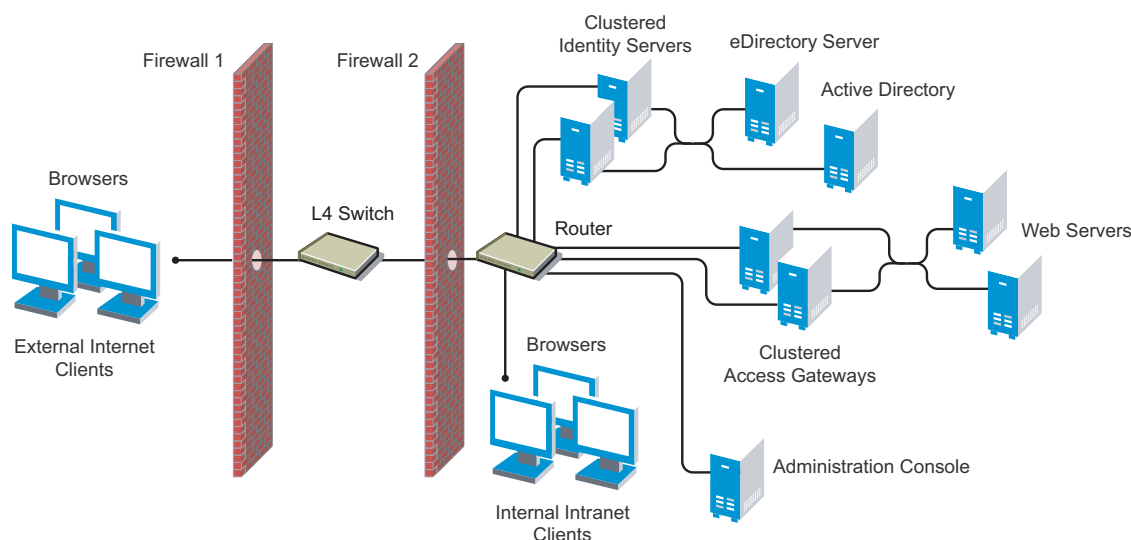
The firewall protects the LDAP server and the Administration Console, both of which contain a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. The Identity Server is not much of a security risk, because it does not permanently store any user data. This is a configuration that Novell has tested and can recommend. We have also tested

this configuration with an L4 switch in place of the router so that the configuration can support clusters of Identity Servers and Access Gateways.

2.1.2 Advanced Network Configuration with a DMZ

An advanced network configuration assumes that you want fault tolerance, so you will install clusters of Access Gateways and Identity Servers. It also assumes that your network has at least two firewalls, one that separates external clients from your network and one that separates internal clients from some components of your network. [Figure 2-2](#) illustrates this type of network.

Figure 2-2 Advanced Network Configuration



In this configuration, you can install the Access Manager components and configure them. When you install the machines for clustering, you need to configure the L4 switch and the second firewall. The firewall and the router can be the same piece of hardware. When you are ready to have external customers access resources, you need to configure the first firewall. For firewall information, see “[Setting Up Firewalls](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

Novell uses this configuration for its internal Web site, and we can recommend it as a tested configuration.

For clustering information, see “[Clustering and Fault Tolerance](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

2.2 Hardware Platform Requirements

For the Linux components (Identity Server, Administration Console, SSL VPN), you should select a platform supported by Suse[®] Linux Enterprise Server (SLES) 9 SP3 or SLES 10. For the Linux Access Gateway, you should select a platform supported by SLES 9 SP3. For the NetWare Access Gateway, you should select a platform supported by NetWare 6.5.

For the hard disk, RAM, and CPU requirements, see the requirements for the individual components.

2.3 Network Requirements

In addition to the servers on which software is installed, your network environment needs to have the following:

- ❑ A server configured with an LDAP directory (eDirectory™ 8.7 or higher, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.

Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

- ❑ Web servers with content or applications that need protection.
- ❑ Clients with an Internet browser.
- ❑ An L4 switch if you are going to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- ❑ Static IP addresses for each machine used for an Access Manager component. If the IP address of the machine changes, the Access Manager component or components on that machine cannot start.
- ❑ Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse look ups to their user stores. If reverse lookups are not available, host table entries can be used.

- ❑ Network time protocol server, which provides accurate time to the machines on your network. Time must be synchronized within one minute among the components, or the security features of the product disrupt the communication processes. You can install your own or use a publicly available server such as pool.ntp.org.

WARNING: If time is not synchronized, users cannot authenticate and access resources.

- ❑ Novell Access Manager does not work in a NAT (Network Address Translation) environment unless all the Access Manager devices are on the same side of the NAT. Clients can be on the other side.

2.4 Access Manager 3 SP2 Administration Console Requirements

The Access Manager Administration Console, which you install on Linux, is a modified version of iManager. After you have installed the Administration Console, the installation scripts for the other components (Identity Server, Access Gateway, SSL VPN, and J2EE Agents) auto-import their configurations into the Administration Console.

IMPORTANT: The Administration Console is the first component you install. If you have iManager installed for other products, you still need to install this version on a separate machine. You also cannot add other iManager product plug-ins to this Administration Console.

Requirements

The Access Manager Administration Console has the same hardware requirements as the SLES operating system with one exception. It requires a minimum of 1 GB of RAM. Because the Administration Console is installed with an embedded version of eDirectory, which is used as the configuration store for Access Manager, the machine has the following software and hardware requirements:

- ❑ SLES 10 SP1 or SLES 9, either with 32-bit or 64-bit software on x86-32 and x86-64 hardware.

Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

You cannot install the Administration Console on a machine with a minimal SLES installation. The Administration Console requires a GUI (such as the X Windows system), and a minimal SLES installation does not install a GUI.

- ❑ 1 GB RAM minimum requirement.
- ❑ 100 GB hard disk (30 GB minimum).

This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote (which is a possible configuration with a blade server).

- ❑ Make sure the following packages are installed:
 - ♦ gettext: The required library and tools to create and maintain message catalogs.
 - ♦ python (interpreter): The basic Python object-oriented programming package.
 - ♦ compat: Libraries to address compatibility issues

Use the following command to verify:

```
rpm -qa | grep <package name>
```

Use YaST to install the packages.

- ❑ OpenLDAP must be uninstalled.
- ❑ ZIP and Unzip utilities for the backup and restore procedure.
- ❑ No LDAP software, such as eDirectory, can be installed.
- ❑ No other version of iManager can be installed.
- ❑ Static IP address (if the IP address changes after devices have been imported, these devices can no longer communicate with the Administration Console.)
- ❑ The tree for the configuration store is named after the server on which you install the Administration Console. Check the host name and rename the machine if the name is not appropriate for a configuration tree name.
- ❑ The Administration Console can be installed on the same machine as the Identity Server. If you are planning to install an L4 switch on a SLES machine, using the Linux Virtual Services software, you can also install the Administration Console on this machine.

SLES 10 Requirements: On a minimal install of SLES 10, make sure the following packages (with their dependent packages) are installed before installing the Administration Console:

- ♦ gtk (version 1.2.10): A graphical user interface library required for the installation of iManager.
- ♦ gtk2 (version 32bit-1.2.10 for a 64-bit installation, version 2.8.10 for a 32-bit installation): A graphical user interface library required for the installation of iManager.

Use the following command to verify:

```
rpm -qa | grep gtk
```

Use YaST to install the packages.

Browser Support

To access the Administration Console after it has been installed, you need a workstation with a browser. You can use one of the following:

- ♦ Internet Explorer 6 or higher on Windows* XP
- ♦ Firefox* 2.0 or higher

IMPORTANT: Browser pop-ups must be enabled to use the Administration Console.

For Administration Console installation instructions, see [“Installing the Access Manager Administration Console” on page 27](#).

2.5 Access Manager 3 SP2 Identity Server Requirements

The Identity Server is the second component you install. It requires the following hardware:

- ❑ 100 GB hard disk (30 GB minimum).

This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote (which is a possible configuration with a blade server).

- ❑ 2 GB RAM recommended with 1 GB as the minimum
- ❑ 2.0 GHz processor or better

The Identity Server must be installed on a Linux operating system and requires the following software:

- ❑ SLES 10 SP1 or SLES 9 SP3, either with 32-bit or 64-bit software on x86-32 and x86-64 hardware.

Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

- ❑ gettext
- ❑ python (interpreter)
- ❑ compat: Libraries to address compatibility issues

Also for SLES 9 or 10:

- ❑ Configure SLES for a static IP address.
- ❑ Uninstall OpenLDAP. (A default installation of SLES installs and enables OpenLDAP.)

For installation instructions, see [Chapter 4, “Installing the Novell Identity Server,” on page 33](#).

2.6 Access Manager 3 SP2 Access Gateway Requirements

The Access Gateway runs on any NetWare 6.5 supported platform. The Linux version runs on SLES 9 SP3. It has the same features on both platforms. Select one or the other based on your network preferences. You install the Access Gateway on a separate machine because it clears the hard drive and sets up a soft appliance environment.

The Access Gateway requires the following hardware:

- ❑ 100 GB of disk space recommended, with 20 GB as the minimum. This disk space must be local and not remote (which is a possible configuration with a blade server).
- ❑ 3 GB RAM recommended, with 2 GB as the minimum.
- ❑ 3.0 GHz processor or better recommended, with 2.0 GHz as the minimum.
- ❑ (NetWare Access Gateway) If your machine has hyper-threading (or logical processor) technology, you should use the computer's setup program to turn it off. The NetWare Access Gateway shows a significant increase in performance and stability when this feature is turned off.
- ❑ (Linux Access Gateway) supports x86-32 only.

The Access Gateway has no software requirements. The installation program for the Access Gateway re-images the hard drive, embeds the operating system (either NetWare or Linux), then configures the embedded operating system for optimal performance.

Before proceeding with the Access Gateway installation, make sure you have a static IP address for your Access Gateway server and an assigned DNS name (host name and domain name). You need to know the following about your network:

- ❑ The subnet mask that corresponds to the IP address of the Access Gateway.
- ❑ The IP address of the default gateway.
- ❑ The IP addresses of the DNS servers on your network. These DNS servers need to be configured to resolve the DNS name of the Access Gateway to the IP address that you assign to it.
- ❑ The IP address or DNS name of a NTP server, if you have one in your local environment.

You are prompted to enter this information during the install. For installation instructions, see

- ♦ [Chapter 5, “Installing the Linux Access Gateway,” on page 35](#)
- ♦ [Chapter 6, “Installing the NetWare Access Gateway,” on page 55](#)

2.7 Access Manager 3 SP2 SSL VPN Requirements

The SSL VPN server requires the following software and hardware:

- ❑ 100 MB of disk space
- ❑ Two or more network interface cards
- ❑ SLES 9 SP3 or higher

NOTE: If you want 64-bit client support you must use SLES 10

- ☐ gettext package
- ☐ Tomcat and Java installed and running
- ☐ Stunnel and OpenVPN port configured on the gateway should be opened

2.8 VMware ESX Requirements

The VMware* ESX Server version 2.5.3 and higher is a supported platform for Access Manager, but your VMware machine must have enough resources. You need to dedicate the minimum requirements that a physical machine would require for the Access Manager component. To have performance comparable to a physical machine, you need to increase the memory and CPU requirements.

For the hard disk, RAM, and CPU requirements, see the requirements for the individual components:

- ◆ [Section 2.4, “Access Manager 3 SP2 Administration Console Requirements,” on page 22](#)
- ◆ [Section 2.5, “Access Manager 3 SP2 Identity Server Requirements,” on page 24](#)
- ◆ [Section 2.6, “Access Manager 3 SP2 Access Gateway Requirements,” on page 25](#)
- ◆ [Section 2.7, “Access Manager 3 SP2 SSL VPN Requirements,” on page 25](#)

Installing the Access Manager Administration Console

3

For a functioning system, you need an Administration Console, an Identity Server, and an Access Gateway or a J2EE server and agent. The Administration Console must be installed before you install the Identity Server, Access Gateway, or J2EE Agent.

- ♦ [Section 3.1, “Installation Procedures,” on page 27](#)
- ♦ [Section 3.2, “Logging In to the Administration Console,” on page 29](#)
- ♦ [Section 3.3, “Enabling the Administration Console for Multiple Network Interface Cards,” on page 31](#)
- ♦ [Section 3.4, “Administration Console Conventions,” on page 31](#)

For information about installing a secondary Administration Console and fault tolerance, see [“Installing Secondary Versions of the Administration Console”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

3.1 Installation Procedures

Installation time: about 15 minutes.

You might want to have a pen handy to record the static IP address and login credentials in the spaces provided below.

- 1 If you have Red Carpet* or auto update running, stop these programs before you install Access Manager Administration Console.
- 2 Verify that the machine meets the minimum requirements. See [Section 2.4, “Access Manager 3 SP2 Administration Console Requirements,” on page 22](#).
- 3 Open a terminal window.
- 4 Log in as the `root` user.
- 5 Insert CD 1 into the drive, then navigate to the device. Enter the following:

```
cd /media
```

Change to your CD-ROM drive, which is usually `cdrom` but can be something else such as `cdrecorder` or `dvdrecorder`, depending on your hardware.

- 6 If you downloaded the `tar.gz` file, unpack the file using the following command:

```
tar -xzf <filename>
```

- 7 At the command prompt, enter the following:

```
./install.sh
```

- 8 When prompted to install a product, type 1 for *Install Novell Access Manager Administration*, then press the Enter key.
- 9 (Conditional) If the install does not detect a static IP address that Access Manager requires on your machine, you receive an advisory message asking whether or not you want to continue the

installation. At this point, stop the installation and configure your machine for a static IP address.

Record Static IP Address here: _____

- 10** (Conditional) If the install detects a version of LDAP on your machine, enter *Y* to continue the installation.

If requested during installation, make certain the uninstall option for Open LDAP is selected. Later in the installation, you are prompted to uninstall LDAP and replace it with the required Access Manager configuration store components.

- 11** Review and accept the License Agreement.

- 12** Specify whether this is the primary Access Manager Administration Console in a failover group. The first Administration Console installed becomes the primary console.

You can install up to three Administration Consoles for replication and failover purposes. If this is not the primary console, you must provide the IP address for the primary Administration Console.

- 13** Specify the administration username.

Press Enter to use *admin* as the default admin username, or change this to a username of your choice.

Record the admin username here: _____

- 14** Specify the administration password.

Use alphanumeric characters only. You must remember this password because it gives rights to the administrator, the configuration store, and subsequent logins to the Administration Console.

Record admin Password here: _____

- 15** Confirm the password, then wait as the system installs the components.

This can take several minutes, depending upon the speed of your hardware. The following components are installed:

- ♦ **Novell Audit Platform Agent:** Responsible for packaging and forwarding the audit log entries to the configured Novell® Audit Server. For more information, see “**Enabling Auditing**” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ♦ **Tomcat for Novell:** The Novell packaging of the Java-based Tomcat Web server used to run servlets and JavaServer Pages* (JSP*) associated with Novell Access Manager Web applications.
- ♦ **Novell Access Manager Configuration Store:** An embedded version of eDirectory™ used to store user-defined server configurations (user stores), LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored. For more information, see “**Configuration Store**” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ♦ **Novell iManager:** The Web-based administration console that provides customized, secure access to server administration utilities. It is a modified version and cannot be used to manage other eDirectory trees.
- ♦ **Novell Audit Server:** The server bundled as part of the Administration Console to monitor and log all enabled Access Manager components. For more information, see “**Enabling Auditing**” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

- ♦ **Novell Administration Console:** A modification of Novell iManager that enables management of all aspects of Access Manager. This component is not a standard iManager plug-in. It significantly modifies the tasks that iManager can perform.
- ♦ **Novell Identity Server Administration Plug-In:** Works in conjunction with the Novell Administration Console to specifically manage the Novell Identity Server.

16 Record the login URL.

When the installation completes, the login URL is displayed. It looks similar to the following:

`http://10.10.10.50:8080/nps`

Record your login URL here: _____

This is the URL you enter into a browser to configure the Access Manager components. If you log in now with the username and password you entered during the installation, you have an empty system with no components installed.

17 To verify that the console is running, log in to the console from a workstation (a machine other than where Administration Console is located).

SLES 10 comes with a firewall enabled by default. You need to either disable this firewall or open the ports that allow you to log in to the Administration Console. You also need to open the ports that allow Access Manager devices installed on other machines to auto-import into the Administration Console. See “[Setting Up Firewalls](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

Continue with [Section 3.2, “Logging In to the Administration Console,”](#) on page 29.

If the configuration store (eDirectory) does not install correctly and you are instructed to view the edir install log, you need to uninstall the Administration Console and start over. See [Section 9.3, “Uninstalling the Administration Console,”](#) on page 86 and use option 3.

3.2 Logging In to the Administration Console

The Administration Console supports the following Web browsers:

- ♦ Microsoft Internet Explorer 6 or higher
- ♦ Mozilla* Firefox 2.0 or higher

WARNING: The Administration Console is a combination of iManager and a device manager. It has been customized for Access Manager so that it can manage the Access Manager components.

You cannot use it to log into other eDirectory trees and manage them.

You should not download and add iManager plug-ins to this customized version. If you do, you can destroy the Access Manager schema, which can prevent you from managing the Access Manager components. This can also destroy communication among the modules.

You should not start multiple sessions of the Administration Console on the same machine using the same browser. Because the browser shares session information, this can cause unpredictable results in the Administration Console. You can, however, start different sessions with different brands of browsers.

To log in:

- 1** Enable browser pop-ups.

- 2 On the Administration Console, ensure that ports 8080 and 8443 are open.
SLES 10 comes with a firewall enabled by default, which closes these ports.
 - 3 From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

Use the IP address established when you installed the Administration Console. It should include the port 8080 and the application nps. If the IP address of your Administration Console is 10.10.10.50, you would enter the following:
`http://10.10.10.50:8080/nps`
-
- IMPORTANT:** If you enter `https` instead of `http`, you receive the following error message:
The connection was interrupted.
-
- 4 Click *OK* to accept the certificate. You can select either the permanent or temporary session certificate option.
 - 5 On the Login page, specify the administrator name and password that you defined during the Administration Console installation.

Login
?

Username:

(Ex: admin or admin.novell)

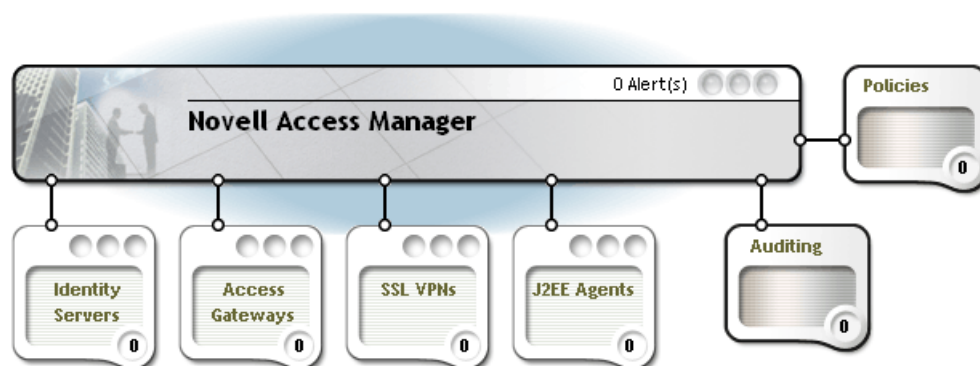
Password:

© Copyright 1999-2005 Novell, Inc. All rights reserved.

As you log in, your browser creates a secure connection with your Identity Server and the various installed Access Manager components, which are displayed in the left navigation panel of the Administration Console.

- 6 In the left navigation panel of the console, click *Access Manager*, then click *Overview*.

Access Manager Overview



Before you can configure the system, you need to install some of the other Access Manager components. You need to install at least one Identity Server and one Access Gateway or J2EE Agent. It is recommended that you next install the Identity Server. See [Chapter 4, “Installing the Novell Identity Server,”](#) on page 33.

IMPORTANT: All of the configuration and management tasks in the Access Manager documentation assume that you have logged in to the Administration Console.

3.3 Enabling the Administration Console for Multiple Network Interface Cards

Making the Administration Console available for all network interface cards (NICs) is a security risk. However, you might want to allow this situation if, for example, the Identity Server has multiple NICs and is also available on all ports. You must modify the `/var/opt/novell/tomcat4/conf/server.xml` file as follows:

- 1 Open the `/var/opt/novell/tomcat4/conf/server.xml` file in a text editor.
- 2 Locate the connector with the `NIDP_Name="connector"` set.
- 3 Delete the `address` attribute.
- 4 Save the file.

3.4 Administration Console Conventions

- ♦ The required fields on a configuration page contain an asterisk by the field name.
- ♦ All actions such as delete, stop, and purge require verification before they are executed.
- ♦ Changes are not applied to a server until you update the server.
- ♦ Sessions are monitored for activity. If your session becomes inactive, you are asked to log in again and unsaved changes are lost.

Installing the Novell Identity Server

4

Installation time: about 10 minutes.

IMPORTANT: Make sure to complete the following before you begin:

- ♦ If you are installing the Access Manager components on multiple machines, ensure that time and date are synchronized on all machines.
- ♦ Make sure that the Access Manager Administration Console is running. (See [“Installing the Access Manager Administration Console” on page 27.](#)) However, you must not perform any configuration tasks in the Administration Console during an Identity Server installation.
- ♦ If you are installing the Administration Console on a separate machine, ensure that the DNS names resolve between the Identity Server and the Administration Console.
- ♦ When you are installing the Identity Server on a separate machine (recommended for production environments), you need to ensure that ports 8080 and 8446 are open on the Administration Console machine.
- ♦ When you are installing the Identity Server on the same machine as the Administration Console (not recommended for production environments), do not run simultaneous external installations of the Identity Server, Access Gateway, J2EE Agent, or SSL VPN. These installations must communicate with the Administration Console. During installation, Tomcat is restarted, which can disrupt the component import process.

1 Verify that the machine meets the minimum requirements. See [Section 2.5, “Access Manager 3 SP2 Identity Server Requirements,” on page 24.](#)

2 Open a terminal window.

3 Log in to SUSE Linux Enterprise Server (SLES) as the `root` user.

4 If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be `/media/cdrom`, `/media/cdrecorder`, or `/media/dvdrrecorder`, depending on your hardware.

If you downloaded the `tar.gz` file, unpack the file using the following command:

```
tar -xzvf <filename>
```

5 At the command prompt, run the following install script:

```
./install.sh
```

6 When prompted to install a product, type `2`, *Install Novell Identity Server*, then press the Enter key.

This selection is also used for installing additional Identity Servers for clustering behind an L4 switch. You need to run this install for each Identity Server you add to the cluster.

7 If prompted, decide whether or not you want to continue the installation without a static IP address. Under most production environments, you must establish a static IP address for your Identity Server to reliably connect with other Access Manager components.

8 Review and accept the License Agreement.

- 9 Specify the IP address of the Administration Console, if you are not installing this Identity Server on the same machine where you installed the Administration Console.
- 10 Specify the name of the administrator for the Administration Console.
- 11 Specify the password of the administrator.
- 12 Confirm the password, then wait as the system installs the components. (This will take several minutes.)

The following components are installed:

- ♦ **Novell Access Manager Server Communications:** The components necessary to enable network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
- ♦ **Novell Identity Server:** The component of Novell Access Manager that provides authentication and identity services for the other Access Manager components and third-party service providers.
- ♦ **Novell Identity Server Configuration:** The configuration that allows the Identity Server to be securely configured by the Administration Console.

If the installation process terminates at this step, the probable cause is a failure to communicate with the Administration Console. Ensure that you entered the correct IP address.

- ♦ **Novell Access Manager Server Communications Configuration:** The communication configuration that enables the Identity Server to auto-import itself into the Administration Console.

This completes the Novell Identity Server installation. The install logs are located in `/tmp/novell_access_manager`. These logs are all dated and time-stamped.

- 13 (Optional) To verify that the Identity Server installation was successful, log in to the Administration Console (see [Section 3.2, “Logging In to the Administration Console,” on page 29](#)), then click *Access Manager > Identity Servers*.

After you log in to the Administration Console, click *Access Manager > Identity Servers*. The system displays the installed server, as shown in the following example:

Identity Servers ?

Servers

Shared Settings

New Cluster... | Start | Stop | Refresh | Actions

1 Item(s)

<input type="checkbox"/>	Name	Status	Health	Alerts	Commands	Statistics	Configuration
<input type="checkbox"/>	10.10.157.30	Not Configured	?	0		View	None

At this point the Identity Server is in an unconfigured state and is halted. It remains in this state and cannot function until you create an Identity Server configuration, which defines how an Identity Server or Identity Server cluster operates.

- 14 Continue with one of the following:
 - ♦ To install an Access Gateway, see [Chapter 5, “Installing the Linux Access Gateway,” on page 35](#) or [Chapter 6, “Installing the NetWare Access Gateway,” on page 55](#).
 - ♦ To configure the Identity Server, see [“Setting Up a Basic Access Manager Configuration”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

Installing the Linux Access Gateway

5

Installation time: 15 to 30 minutes, depending upon the hardware.

The Access Gateway runs on NetWare® 6.5 (included in the installation) or Linux (included in the installation). If you intend to install the NetWare Access Gateway, skip this section and go to [“Installing the NetWare Access Gateway” on page 55](#).

You have the following options for installing the Linux Access Gateway, depending on whether you want to do an advanced installation or accept the default settings:

- ♦ **Standard Installation:** A standard installation can be done with minimal user intervention. Use this method if you want to use the default installation settings. See [Section 5.3, “Using a Standard Linux Installation with the Default Settings,” on page 36](#).
- ♦ **Advanced Installation:** An advanced installation allows you to customize the machine. The default partition proposal for advanced installation creates a 4 GB swap partition and one-thirds each of the remaining space will be utilized to create the / partition, /var partition and COS partition. You can change the partition sizes according to your requirements. See [Section 5.4, “Using the Advanced Installation Option,” on page 42](#).
- ♦ **Manual Installation:** Manual installation is similar to the advanced installation in that you can customize the machine. If the automatic loading of drivers causes problems with the advanced installation, you can perform a manual installation and manually select the drivers.

The Linux Access Gateway can be installed on all SUSE Linux Enterprise Server (SLES) 9 SP 3 supported hardware platforms.

This section provides the following information on how to install the Linux Access Gateway:

- ♦ [Section 5.1, “Prerequisites for a Linux Access Gateway,” on page 35](#)
- ♦ [Section 5.2, “Boot Screen Function Keys,” on page 36](#)
- ♦ [Section 5.3, “Using a Standard Linux Installation with the Default Settings,” on page 36](#)
- ♦ [Section 5.4, “Using the Advanced Installation Option,” on page 42](#)
- ♦ [Section 5.5, “Viewing the Linux Installation Log,” on page 53](#)

5.1 Prerequisites for a Linux Access Gateway

- ❑ Ensure that you have backed up all data and software on the disk to another machine. The Linux Access Gateway installation completely erases all the data on your hard disk.
- ❑ An Administration Console must be installed before you can install the Access Gateway. See [“Installing the Access Manager Administration Console” on page 27](#).
- ❑ If a firewall separates the Linux Access Gateway and the Administration Console, make sure the required ports are opened. See [“When a Firewall Separates the Administration Console from a Component”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

5.2 Boot Screen Function Keys

You can use the function key options in the boot screen to change installation settings as desired.

- ♦ **F1:** Lets you access the context-sensitive help for the currently active screen element of the boot screen.
- ♦ **F2:** Lets you select different graphical display modes for the installation. Also included is an entry to select the text mode. This helps you if there are issues with installation in the graphical mode.
- ♦ **F3:** Lets you choose the installation media if you want to use a different source, for example, FTP or NFS, instead of the installation disk. The SLP (Service Location Protocol) entry allows you to access an SLP server on the network, which in turn gives access to a selection of installation media provided by that server.
- ♦ **F4:** Lets you select the display language for the installation.
- ♦ **F5:** Lets you access the diagnostic messages. By default, these messages from the Linux kernel are not displayed during system startup; only a progress bar is displayed. To display the messages, select *Native*. For information in verbose mode, select *Verbose*.
- ♦ **F6:** Lets you communicate to your system that you have an optional disk with a driver update. At the prompt, insert the update disk. A few seconds after starting the installation, a minimal Linux system is loaded to run the installation procedure.

5.3 Using a Standard Linux Installation with the Default Settings

This is the recommended installation method for a machine that meets but doesn't exceed the minimal hardware requirements. Use this method if you want to use the default installation settings, as described in the following table.

Table 5-1 *Default Installation Settings*

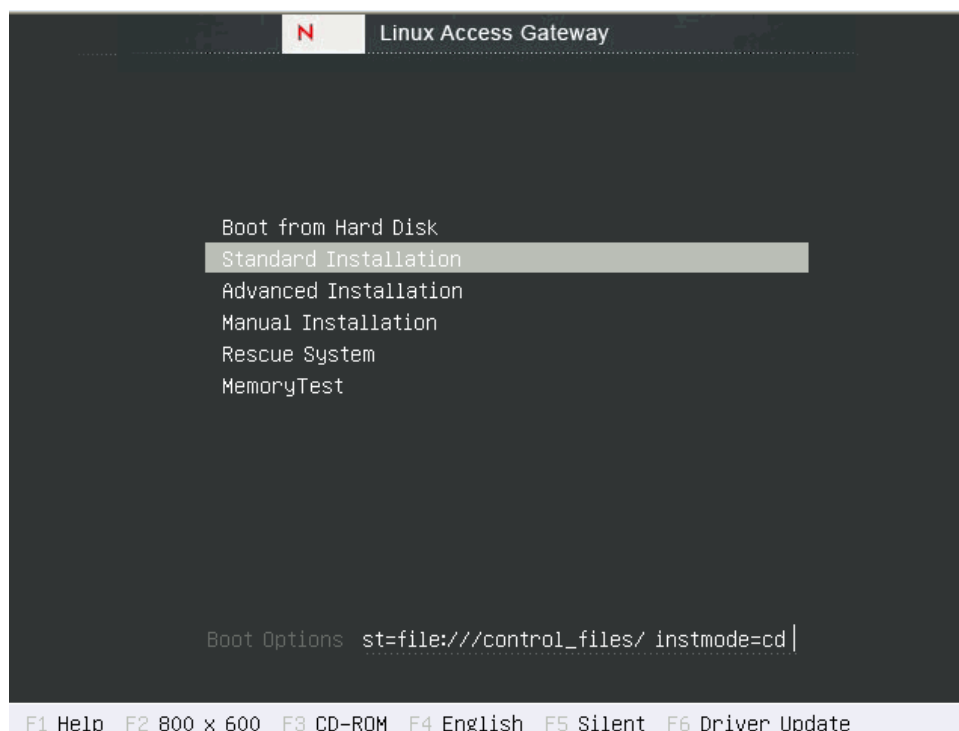
Default Settings	Description
Partitions	<p>Partitions are created with the following default specifications:</p> <ul style="list-style-type: none">♦ /boot: The size is automatically calculated and the mount point is <code>/boot</code>.♦ swap: Double the size of RAM and mount point is <code>swap</code>. <p>The remaining disk space after the creation of <code>/boot</code> and swap partition is allocated as the extended drive. The extended drive has the following partitions:</p> <ul style="list-style-type: none">♦ root: The default size is one-third the size of extended drive and the mount point is <code>/</code>.♦ var: The default size is one-third the size of the extended drive and the mount point is <code>/var</code>.♦ COS: This partition is created with the remaining free space on the extended drive.

Default Settings	Description
User/Password	<p>Two users are created:</p> <ul style="list-style-type: none"> ♦ <code>root</code> with password <code>novell</code> and login shell as <code>bash</code> ♦ <code>config</code> with password <code>novell</code> and login shell as <code>nash</code> <p>NOTE: Make sure you change the passwords after installation.</p>

A standard installation does not support configuring multiple network interfaces. Only the `eth0` interface can be configured during installation. However, you can configure multiple interfaces through the Administration Console after installation.

- 1 Insert the Linux Access Gateway CD into the CD drive.

The boot screen appears.



- 2 By default, the *Boot From Hard Disk* option is selected in the boot screen. Use the Down-arrow key to select *Standard Installation*.
- 3 Use the function key options to change installation settings as desired. For more information on these function keys, see [Section 5.2, “Boot Screen Function Keys,” on page 36](#).
- 4 After you have completed any changes to the installation options, press Enter.
- 5 Review the agreement on the License Agreement page, then click *I Agree* to accept the agreement.
- 6 Select *English (US)* on the Language Selection page, then click *Accept*.
The current version of the product is an English-only version.
- 7 Select a keyboard layout on the Keyboard Configuration page, then click *Accept*.

- 8 Configure values for region and time zone, change the date and time setting on the Clock and Time Zone Configuration page, then click *Next*.

The Network Configuration page appears.

Novell Linux Access Gateway

Network Configuration
Select the **Interface Alias** (In the current version only eth0 is supported).
Enter the **IP address** of Linux Access Gateway (e.g., 192.168.100.99).
Enter the **Subnet mask** (e.g., 255.255.255.0).
Enter the **Default Gateway** IP address.
Click **Next** to complete the Network configuration.

Novell Linux Access Gateway Configuration

Network Configuration

Interface Alias:
eth0

IP Address:

Subnet Mask:

Default Gateway:

Abort Next

Configure the following:

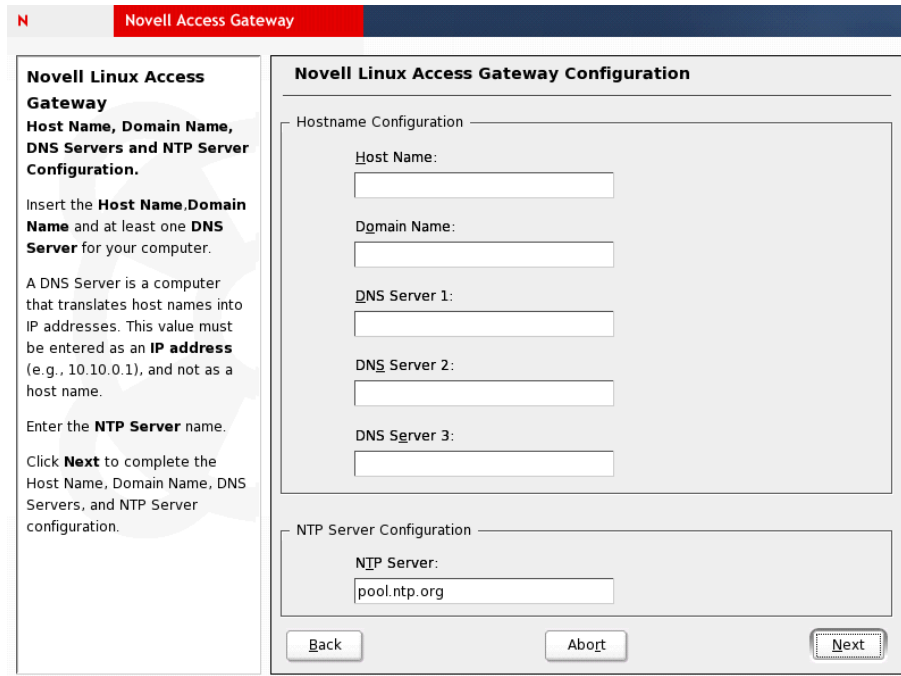
Interface Alias: This option displays the eth0 interface that is configured by default. The Standard Installation does not support configuring multiple interfaces. Only the eth0 interface can be configured during the install. You can configure multiple interfaces by using the Administration Console after installation. For more information, see [Section A.2.2, “Manually Configuring a Network Interface,” on page 139](#).

IP Address: Specify the IP address of the Access Gateway.

Subnet Mask: Specify the subnet mask of the Linux Access Gateway network.

Default Gateway: Specify the default gateway.

- 9 Click *Next*. The *Hostname Configuration* section appears.



The image shows a software configuration window titled "Novell Linux Access Gateway Configuration". The window has a red header bar with the text "Novell Access Gateway". On the left side, there is a sidebar with instructions: "Novell Linux Access Gateway", "Host Name, Domain Name, DNS Servers and NTP Server Configuration.", "Insert the **Host Name**, **Domain Name** and at least one **DNS Server** for your computer.", "A DNS Server is a computer that translates host names into IP addresses. This value must be entered as an **IP address** (e.g., 10.10.0.1), and not as a host name.", "Enter the **NTP Server** name.", "Click **Next** to complete the Host Name, Domain Name, DNS Servers, and NTP Server configuration." The main area of the window is divided into two sections: "Hostname Configuration" and "NTP Server Configuration". The "Hostname Configuration" section contains four input fields: "Host Name:", "Domain Name:", "DNS Server 1:", and "DNS Server 2:". The "NTP Server Configuration" section contains one input field: "NTP Server:". At the bottom of the window, there are three buttons: "Back", "Abort", and "Next".

Configure the following:

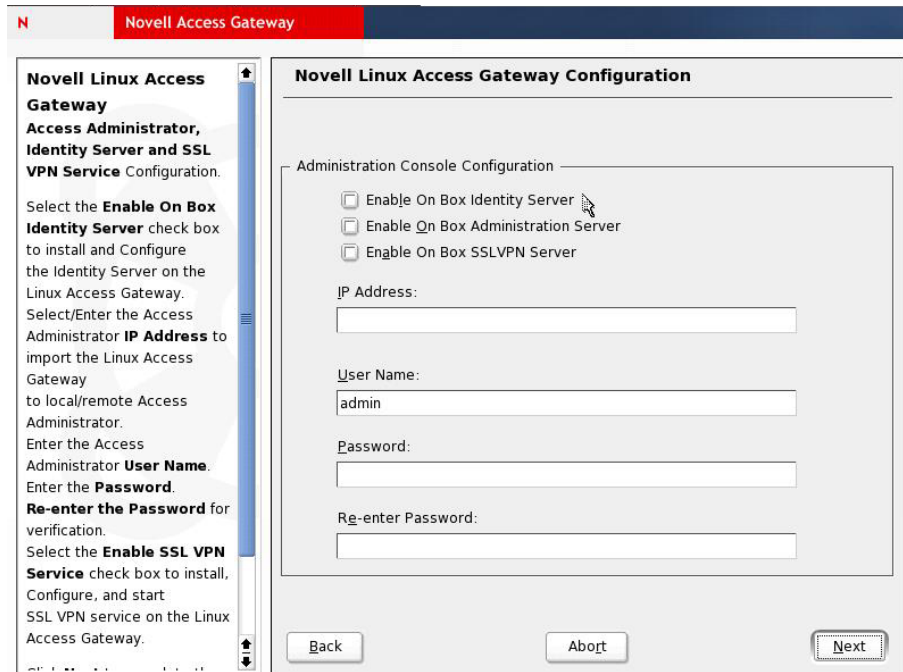
Host Name: Specify the hostname for the Linux Access Gateway machine.

Domain Name: Specify the domain name for your network.

DNS Server 1: Specify the IP address of your DNS server. You can configure a maximum of three DNS servers. It is mandatory to configure at least one DNS server.

NTP Server: Specify the name of the NTP server.

- 10 Click *Next*. The *Administration Console Configuration* section appears.



Configure the following:

Enable On Box Identity Server: Not currently available.

Enable On Box Administration Server: Not currently available.

Enable On Box SSL VPN Server: Select this check box to install and configure the SSL VPN service on the Linux Access Gateway.

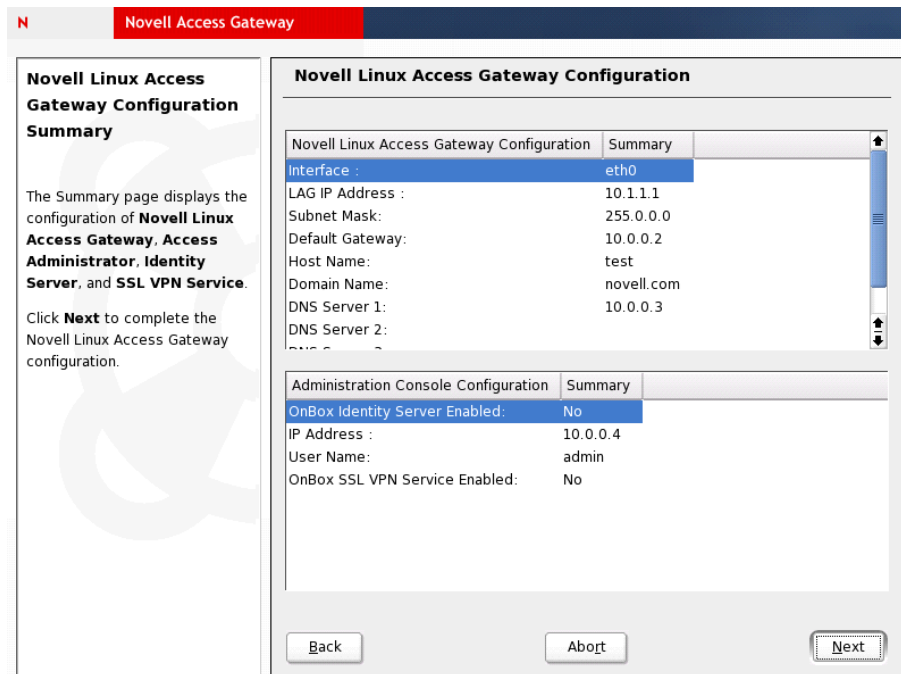
IP Address: Specify the IP address of the Administration Console. The Linux Access Gateway is imported into this Administration Console. If you have selected the *Enable on Box SSL VPN Server* option, the SSL VPN is imported into this Administration Console.

Username: Specify the name of the Administration Console user.

Password: Specify the password for the user.

Reenter Password: Re-enter the password for verification.

- 11 Click *Next*. The Novell Linux Access Gateway Configuration Summary page appears.



This page summarizes the configuration that you have selected. If you want to change any configuration, click *Back*.

- 12 Click *Next*, then click *Yes, install* to start the installation process.

This process might take 15 to 30 minutes, depending on the configuration and hardware.

The machine reboots after the installation is completed and the Linux Access Gateway is imported to the Administration console.

Ignore the warning about failed services in `runlevel3` for `novell-jcc`.

- 13 Log in as `root` and change the password.

13a At the login prompt, enter `root`.

13b At the password prompt, enter `novell`.

13c To change the password, enter `passwd`.

13d Enter a password.

13e Confirm the password by entering it again.

- 14 To change the password for the `config` user, enter the following commands:

14a Enter `passwd config`.


14b Enter a new password.

14c Confirm the password by entering it again.

- 15 (Optional) To verify the installation of the Access Gateway, log in to Administration Console (see [Section 3.2, “Logging In to the Administration Console,”](#) on page 29), then click *Access Manager* > *Access Gateways*.

If the installation was successful, the IP address of your Access Gateway appears in the Server list.

Access Gateways

Access Gateway Servers							
New Cluster... Shutdown Reboot Refresh Actions ▼							
<input type="checkbox"/> Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration
<input type="checkbox"/> 10.10.16.42	Current		0	Succeeded	View	Linux	Edit
<input type="checkbox"/> 10.10.16.64	Current		0	Succeeded	View	NetWare	Edit

The Health status indicator appears yellow after the Access Gateway is imported and registers with the Administration Console, which can take up to 5 minutes. You must configure the Access Gateway in order to change its health to green.

If an Access Gateway starts to import into the Administration Console but fails to complete the process, the following message appears:

Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

If you have waited at least ten minutes, but the message doesn't disappear and the Access Gateway doesn't appear in the list, click the *repair import* link. For additional help, see [Appendix A.1, "Troubleshooting the Access Gateway Import," on page 131](#).

- 16** This completes the installation of the Linux Access Gateway. Continue with the one of the following:

- ♦ ["Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.0 SP2 Setup Guide*](#)
- ♦ [Section 5.5, "Viewing the Linux Installation Log," on page 53](#)

5.4 Using the Advanced Installation Option

An advanced installation allows you to customize the default settings. This section describes how to run the advanced installation and customize the partitions.

- ♦ [Section 5.4.1, "Planning Your Partition Strategy," on page 42](#)
- ♦ [Section 5.4.2, "Starting the Installation," on page 43](#)
- ♦ [Section 5.4.3, "Customizing the Partitions," on page 45](#)
- ♦ [Section 5.4.4, "Configuring Date and Time Values," on page 48](#)
- ♦ [Section 5.4.5, "Customizing Optional Settings," on page 49](#)
- ♦ [Section 5.4.6, "Configuring Hardware and System Services," on page 49](#)

5.4.1 Planning Your Partition Strategy

Linux allows you to have four primary partitions per hard disk. The Linux Access Gateway requires a swap partition, a cache object store (COS) partition, and a root partition. For a machine with only one large hard disk (100 GB or larger), we recommend creating the following partitions:

Table 5-2 *Partitions for One Large Hard Disk*

Partition Type	Requirements
root	This partition contains the boot files, the system files, and the log files (if you don't create a var partition). You should assign 25% of available disk space to this partition.
swap	This is a mandatory partition. Because the advanced installation option assumes that you have a large hard disk, we recommend that you create a swap partition that is twice the size of the RAM installed on the machine.
var	This partition is optional, but highly recommended if you turn on logging. The var partition should take about 25% of available disk space.
COS	This is a mandatory partition. It should be as large as possible. This is the partition that holds the caching objects of the Access Gateway.

Other configurations are possible if you know Linux and the Access Gateway.

When the machine has an array of disks, we recommend that you configure the first hard disk with the following partitions:

Table 5-3 *Partitions for an Array of Disks*

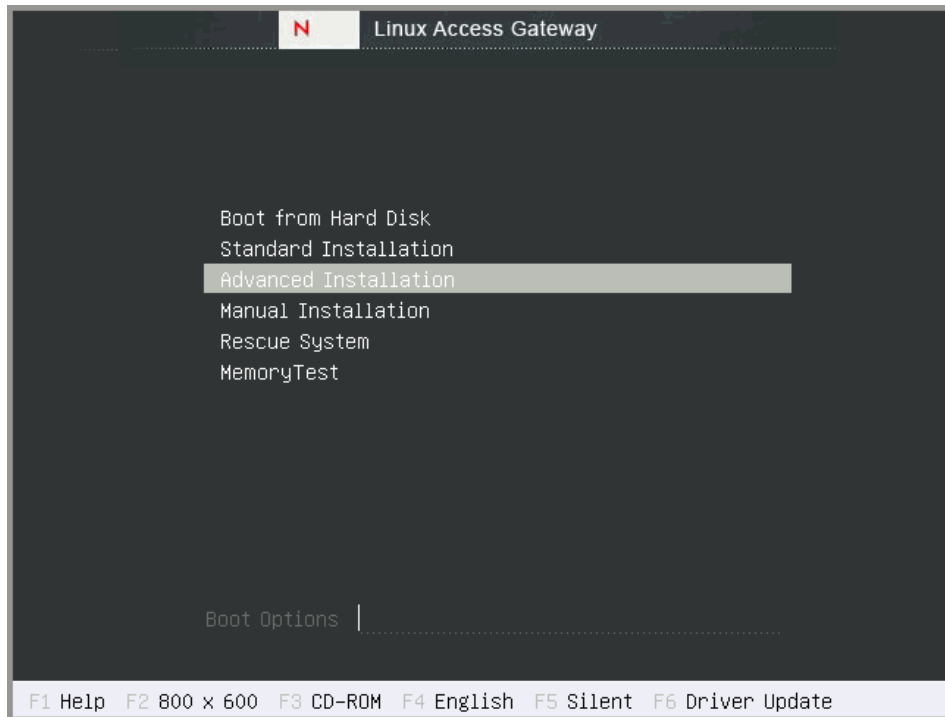
Partition Type	Requirements
boot	This partition contains the boot files. It should be 500 MB.
swap	This is a mandatory partition on the first hard disk. Because the advanced installation option assumes that you have a large hard disk, we recommend that you create a swap partition that is twice the size of the RAM installed on the machine.
var	The var partition should take about 40% of available disk space.
root	This partition contains the system and application files. It should take about 40% of available disk space.

These partitions can be imaged on a pair of disks so that disk failover is supported. The remaining disks in the array can have one large COS partition. You can also divide them into multiple COS partitions so you can configure multiple virtual machines. The COS partitions need to be the same size for all virtual machines.

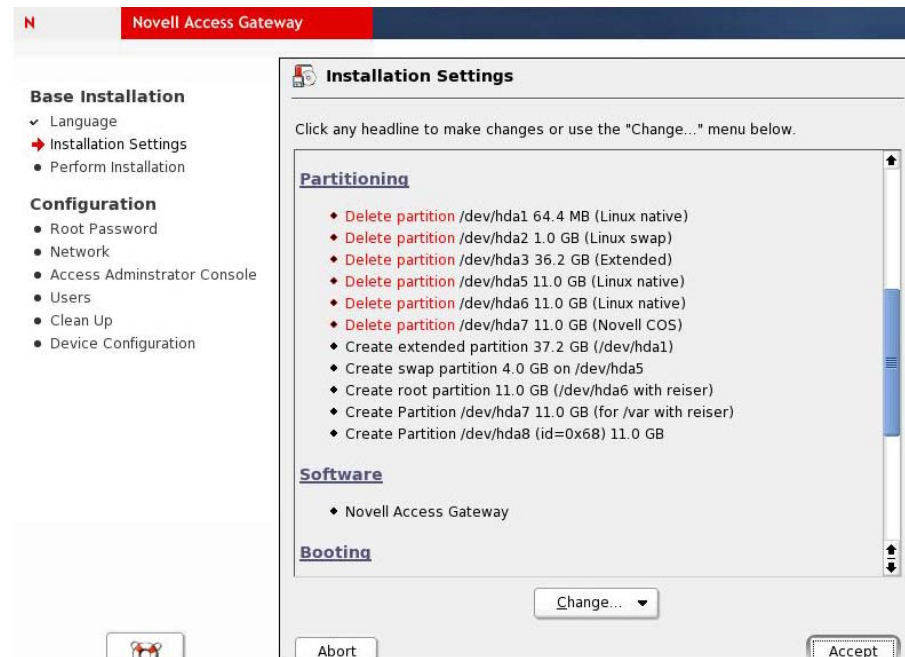
5.4.2 Starting the Installation

- 1 Insert the Linux Access Gateway CD into the CD drive.

The boot screen appears.



- 2 Use the Down-arrow key to select *Advanced Installation*.
- 3 Use the function key options to change installation settings as desired.
For more information on these function keys, see [Section 5.2, “Boot Screen Function Keys,” on page 36](#).
- 4 After you have completed any changes to the installation options, press Enter.
The Linux kernel loads, and the advanced installation starts and displays the Linux Access Gateway splash screen followed by the License Agreement section.
- 5 Read the agreement, then select *I Agree* to proceed.
- 6 Select *English (US)* on the Language selection page, then click *Accept*.
The current version is an English-only version.
- 7 (Conditional) If you are prompted to load the hardware drivers, follow the prompts.
- 8 (Conditional) If you have previously installed a version of Linux on the machine, make sure that *New installation* is selected, then click *OK*.
The other options are not supported for this release.
The Installation Settings page appears.



WARNING: The proposed partition overwrites the existing partitions, if any, in the disk.

Before you click *Accept* on the Installation Settings page, you must complete the following tasks:

- ♦ Create custom partitions. See [Section 5.4.3, “Customizing the Partitions,”](#) on page 45.
- ♦ Modify the time zone. See [Section 5.4.4, “Configuring Date and Time Values,”](#) on page 48.

Other modifications, explained in [Section 5.4.5, “Customizing Optional Settings,”](#) on page 49, are optional.

5.4.3 Customizing the Partitions

NOTE: You must format the partition after you have modified the partition size during installation.

- 1 To create a custom partition, click *Change*, then select *Partitioning*.

This page lists the partition settings as currently proposed.

- 2 Select *Create custom partition setup*, then click *Next*.

The other options are not recommended.

- 3 Select *Custom partitioning -- for experts*, then click *Next*.

- 4 (Conditional) If the installation program discovers any existing partitions, select the hard disk, click *Delete*, then confirm the deletion of the partitions.

- ♦ If your machine has one hard disk, continue with [Step 5](#).
- ♦ If your machine has two hard disks, continue with [Step 10](#).

- 5 For a machine with one hard disk, create a root partition that uses 25% of the disk space. The following values assume a machine with a 100 GB hard drive and 4 GB of RAM. If your machine has a different configuration, adjust the values as you create the partitions.
 - 5a Click *Create*, select *Primary partition*, then click *OK*.
 - 5b Fill in the following fields:
 - Format:** Make sure *Format* is selected.
 - File system:** Select either *Reiser* or *Ext3* for the type.
 - Size:** Specify +25GB for the *End cylinder* value.
 - Mount Point:** Select */*.
 - 5c Click *OK*.
- 6 Create a swap partition that is double the size of the RAM in the machine.
 - 6a Select the hard drive, click *Create*, select *Primary partition*, then click *OK*.
 - 6b Fill in the following fields:
 - Format:** Make sure *Format* is selected.
 - File system:** Select *Swap* for the type.
 - Size:** Specify +8GB for the *End cylinder* value.
 - Mount Point:** Leave the default value of *swap*.
 - 6c Click *OK*.
- 7 Create a var partition that uses 25% of the disk space on the hard disk.
 - 7a Select the hard drive, click *Create*, select *Primary partition*, then click *OK*.
 - 7b Fill in the following fields:
 - Format:** Make sure *Format* is selected.
 - File system:** Select either *Reiser* or *Ext3* for the type.
 - Size:** Specify +25GB for the *End cylinder* value.
 - Mount Point:** Select */var*.
 - 7c Click *OK*.
- 8 Create a COS partition that uses the remaining space on the hard disk:
 - 8a Select the hard drive, click *Create*, select *Primary partition*, then click *OK*.
 - 8b Fill in the following fields:
 - Format:** Select *Do not format*.
 - File system ID:** Select *0x68 Novell COS* for the ID.
 - Size:** Accept the default value for the *End cylinder* value.
 - Mount Point:** Make sure the *Mount Point* has no value.
 - 8c Click *OK*.
- 9 Click *Next*, then continue with [Section 5.4.4, “Configuring Date and Time Values,” on page 48](#).
- 10 For a machine with a disk array, create a boot partition on the first hard drive. The following values assume that the machine has 100 GB hard drives and 4 GB of RAM. If your machine has a different configuration, adjust the values as you create the partitions.
 - 10a Select the first hard drive, click *Create*, select *Primary partition*, then click *OK*.

- 10b** Fill in the following fields:
- Format:** Make sure *Format* is selected.
 - File system:** Select either *Reiser* or *Ext3* for the type.
 - Size:** Specify +500MB for the *End* cylinder value.
 - Mount Point:** Specify */boot*.
- 10c** Click *OK*.
- 11** Create a swap partition that is double the size of the RAM in the machine on the first hard disk.
- 11a** Select the first hard drive, click *Create*, select *Primary partition*, then click *OK*.
- 11b** Fill in the following fields:
- Format:** Make sure *Format* is selected.
 - File system:** Select *Swap* for the type.
 - Size:** Specify +8GB for the *End* cylinder value.
 - Mount Point:** Leave the default value of *swap*.
- 11c** Click *OK*.
- 12** Create a var partition that uses 25% of the disk space on the first hard disk.
- 12a** Select the first hard drive, click *Create*, select *Primary partition*, then click *OK*.
- 12b** Fill in the following fields:
- Format:** Make sure *Format* is selected.
 - File system:** Select either *Reiser* or *Ext3* for the type.
 - Size:** Specify +25GB for the *End* cylinder value.
 - Mount Point:** Select */var*.
- 12c** Click *OK*.
- 13** Create a root partition that uses the rest of the space on the first disk.
The installation program creates this partition into a COS partition.
- 13a** Click *Create*, select *Primary partition*, then click *OK*.
- 13b** Fill in the following fields:
- Format:** Make sure *Format* is selected.
 - File system:** Select either *Reiser* or *Ext3* for the type.
 - Size:** Accept the default value for the *End* cylinder value.
 - Mount Point:** Select */*.
- 13c** Click *OK*.
- 14** Create a COS partition. The partition can consume all or part of the space on the hard disk. The following values assume you are going to create two 50 GB partitions on a 100 GB hard disk.
- 14a** Select a hard drive from the array, click *Create*, select *Primary partition*, then click *OK*.
- 14b** Fill in the following fields:
- Format:** Select *Do not format*.
 - File system ID:** Select *0x68 Novell COS* for the ID.
 - Size:** Specify +50GB for the *End* cylinder value.

Mount Point: Make sure the *Mount Point* has no value.

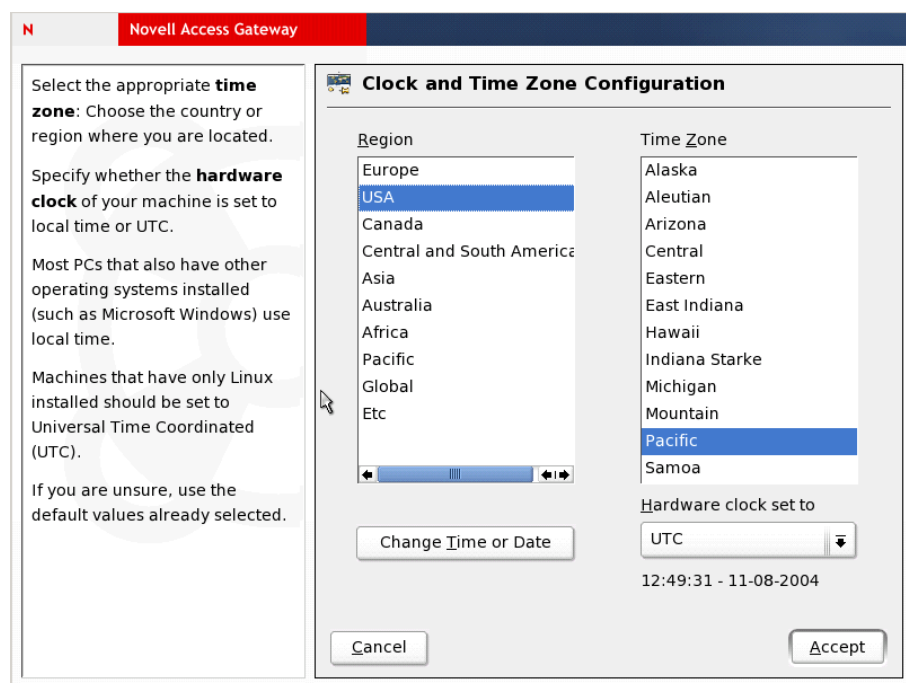
14c Click *OK*.

14d Repeat these steps to create additional COS partitions.

15 Click *Next*, then continue with [Section 5.4.4, “Configuring Date and Time Values,”](#) on page 48.

5.4.4 Configuring Date and Time Values

1 To change the time zone, click *Change*, then select *Time Zone*.



2 Configure values for the region and time zone.

3 Use the *Hardware clock set to* drop-down list to select between local time and UTC.

The selection depends on how the hardware (BIOS) clock is set on your machine. If it is set to GMT, which corresponds to UTC, your system can automatically switch from standard time to daylight saving time.

4 Click *Change Time or Date* to correct the current time or date.

IMPORTANT: Make sure that the time is synchronized on the Linux Access Gateway, Identity Server, and Administration Console.

5 Click *Accept*.

6 Continue with [Section 5.4.5, “Customizing Optional Settings,”](#) on page 49 or [Section 5.4.6, “Configuring Hardware and System Services,”](#) on page 49.

5.4.5 Customizing Optional Settings

Use the *Change* button on the Installation Settings page to change the following settings. These changes are optional. If you do not want to change the installation settings, continue with [Section 5.4.6, “Configuring Hardware and System Services,” on page 49](#).

- 1 Click *Software* to select software packages to be installed with the Linux Access Gateway installation.

During installation, YaST checks whether the disk space is sufficient for the software selection you made. If not, YaST automatically removes parts from the software selection as needed. The suggestion window then includes a notice to inform you about this. As long as there is sufficient disk space available, YaST accepts your settings and partitions the hard disk accordingly.

- 2 Click *System* to detect the hardware components on your system.

The components are detected and listed in the *Detected Hardware* section. You can save this information to a file or floppy disk.

- 3 Click *Mode* to see details of the installation mode.

- 4 Click *Run Level* to see the default run level.

- 5 Skip the *Mouse* configuration option.

The installation program disables the mouse.

- 6 If you have not yet selected a language for installation, click *Language*, then select *English (US)*.

- 7 During installation, YaST proposes a boot configuration for your system. Unless you require a custom setup, leave these settings unchanged.

For a custom setup, modify the proposal for your system by choosing either of the following options:

- ♦ Configure the boot mechanism to rely on a special boot floppy.

Although this has the disadvantage of requiring the floppy to be in the drive when booting, it leaves an existing boot mechanism untouched. However, in most cases this should not be necessary, because YaST can configure the boot loader to boot existing operating systems.

- ♦ Change the location of the boot mechanism on the hard disk.

To change the boot configuration proposed by YaST, select *Booting* to modify the boot mechanism details.

After you finish modifying the settings, click *Next* to return to the Installation Settings page.

- 8 At the prompt, click *Continue*. The changes you made to the installation settings are ignored.

IMPORTANT: Do not select the *Reset Defaults* option. It overwrites the changes you have configured for Date and Time and for partitions.

- 9 Continue with [Section 5.4.6, “Configuring Hardware and System Services,” on page 49](#).

5.4.6 Configuring Hardware and System Services

- 1 On the Installation Settings page, click *Accept* after you have finished customizing the settings.

You are prompted to start the installation.

- 2 Click *Yes, install* to start the installation.

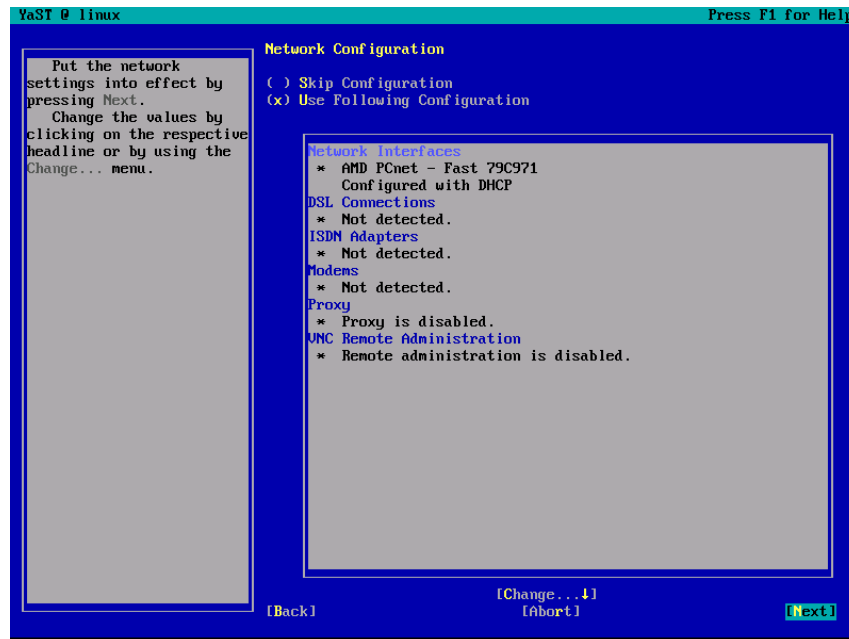
The hard disk is formatted, destroying all data, and the partitions are created. After all the packages are installed, the system reboots.

- 3 To clear the message about why the graphical interface cannot be started, press Enter.

The `root` user password screen appears.

- 4 Specify the password for `root`, re-type it, tab to *Next*, then press Enter.

The *Network Configuration* screen appears.



- 5 Tab to *Network Interfaces*, then press Enter.

You must complete the network interface configuration. If you do not configure the network interface, the Linux Access Gateway setup fails.

The Access Gateway must not use DHCP; it must be assigned a static IP address. To configure a static IP address:

- 5a Tab to *Change*, then press Enter.

- 5b Tab to *Edit*, press Enter, and fill in the following fields:

Static address setup: Select this option, which allows you to enter a static IP address.

IP address: Specify the IP address assigned to the Access Gateway.

Subnet mask: Specify the subnet mask for your network.

- 5c Tab to *Select Hostname and server*, press Enter, and fill in the following fields:

Host Name: Change the hostname to a unique name for the Access Gateway machine.

Domain Name: Change the domain name to the domain name for your network.

Name Server 1: Specify the IP address of your DNS server. If you have more than one DNS server, enter their IP addresses in the *Name Server 2* and *Name Server 3* fields. You do not need to configure a domain search.

- 5d** Tab to *OK*, then press Enter.
- 5e** Tab to *Routing*, then press Enter.
- 5f** Specify the gateway for your network, tab to *OK*, then press Enter.
- 5g** Tab to *Next*, then press Enter.
- 5h** Tab to *Finish*, then press Enter.

For more information on this process, refer to the relevant parts of “Network Devices” in the *Novell SUSE Linux Administration Guide* (http://www.novell.com/documentation/sles9/pdfdoc/sles_9_admin_guide/sles_9_admin_guide.pdf).

- 6** Tab to *Next*, then press Enter. The *Access Administrator Configuration* screen appears.

Novell Linux Access Gateway Administration Console, NTP Server and SSL VPN Configuration

Novell Linux Access Gateway
Access Administrator, Identity Server, NTP
Server and SSL VPN Service Configuration.

Enter the NTP Server name.
Check the Enable On Box Identity Server
to install and Configure the
Identity Server on the Linux Access
Gateway.
Select/Enter the Access Administrator IP
Address to import the Linux Access Gateway
to local/remote Access Administrator.
Enter the Access Administrator User Name.
Enter the Password.
Re-enter Password for verification.
Check the Enable SSL VPN Service to
configure and start SSL VPN service
on the Linux Access Gateway.
Click Next to complete the Access
Administrator, Identity Server
and SSL VPN Service configuration.

NTP Server Configuration

NTP Server
pool.ntp.org

Administration Console Configuration

☐ Enable On Box Device Manager.
☐ Enable On Box Identity Server.
☐ Enable On Box SSL Service.

Access Administrator IP Address

Access Gateway IP Address
192.168.1.1

User Name:

Password:

Re-enter Password:

[Back] [Abort] [Next]

Fill in the following fields:

NTP Server: Specify the name of the NTP server.

Enable On Box Identity Server: Not currently available.

Enable On Box Administration Server: Not currently available.

Enable On Box SSL VPN Server: Select this check box to install and configure the SSL VPN service on the Linux Access Gateway.

Access Administrator IP Address: Specify the address of the Administration Console.

Access Gateway IP Address: Specify the IP address of the Access Gateway.

Username: Specify the name of the Administration Console user.

Password: Specify the password for the user.

Reenter Password: Re-type the password for the user.

- 7** Tab to *Next*, then press Enter.

The Health status indicator appears yellow after the Access Gateway is imported and registers with the Administration Console, which can take up to 5 minutes. You must configure the Access Gateway in order to change its health to green.

If an Access Gateway starts to import into the Administration Console but fails to complete the process, the following message appears:

Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

If you have waited at least ten minutes, but the message doesn't disappear and the Access Gateway doesn't appear in the list, click the *repair import* link. For additional help, see [Appendix A.1, “Troubleshooting the Access Gateway Import,” on page 131](#).

- 14** This completes the installation of the Linux Access Gateway. Continue with the one of the following:

- ♦ “[Setting Up a Basic Access Manager Configuration](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*
- ♦ [Section 5.5, “Viewing the Linux Installation Log,” on page 53](#)

5.5 Viewing the Linux Installation Log

While installing, the Linux Access Gateway generates a log file detailing the installation progress. The install log is available at `/var/log/YaST2/y2logRPM`.

IMPORTANT: Log in as `root` to view the logs.

The log has the following format:

```
'date' 'time' 'versioned rpm-name' 'status'
```

The log also provides some additional information generated from the pre-script and the post-script of the RPM package.

Installing the NetWare Access Gateway

6

Installation time: about 15 minutes

The Access Gateway runs on NetWare® 6.5 (included in the installation) or Linux (included in the installation). If you intend to install the Linux Access Gateway, skip this section and go to [“Installing the Linux Access Gateway” on page 35](#).

6.1 Running the NetWare Installation Program

WARNING: This installation re-images your machine. Remember to remove the Installation CD when prompted to do so at the end of the Access Gateway installation, because the system reinstalls the product if the CD remains in the drive when you reboot.

You must install the NetWare Access Gateway on a separate machine because it re-images the hard drive and sets up a soft appliance environment.

- 1 Ensure that you have installed the Administration Console, and that it is running before you proceed. See [“Installing the Access Manager Administration Console” on page 27](#).
- 2 If a firewall separates the Access Gateway from the Administration Console, make sure the required ports are open. See [“When a Firewall Separates the Administration Console from a Component”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.
- 3 Verify that the machine meets the minimum requirements. See [Section 2.6, “Access Manager 3 SP2 Access Gateway Requirements,” on page 25](#).
- 4 Insert the NetWare Access Gateway CD into the CD drive of your Access Gateway machine.
- 5 Boot to the CD drive.
- 6 Select the language for the License Agreement.
- 7 Review the License Agreement, then press F10 to accept it and proceed with the installation.
- 8 Specify the following network configuration information for eth0, then select *Continue*:
 - IP Address:** Specify the static IP address for the Access Gateway machine.
 - Subnet Mask:** Specify the subnet mask for your network. The default value is 255.255.0.0.
 - Default Gateway:** Specify the IP address of the gateway (IP router) for your network.
- 9 Specify the following DNS information, then select *Continue*:
 - DNS Servers:** Specify the IP address of your DNS server. You can provide up to three addresses. You must specify the IP address of at least one DNS server.
 - Hostname:** Specify a unique host, or computer name, for the Access Gateway machine.
 - Domain:** Specify the domain name for your network. Your DNS server must be configured to resolve the combination of the hostname and the domain name to the Access Gateway machine.
- 10 Specify the following date and time information, then select *Continue*.
 - Timezone:** From the drop-down list, select the time zone for the machine.

Date: Inspect the date information and correct it if it is inaccurate.

Time: Inspect the time information and correct it if it is inaccurate.

IMPORTANT: This time must match the time on the Administration Console and the Identity Server machines. If the time is not synchronized within one minute of each other, they cannot communicate with each other.

Network Time Protocol (NTP): Specify a server for the network time synchronization protocol. The [pool.ntp.org](http://www.pool.ntp.org) (<http://www.pool.ntp.org/>) server is entered by default.

- 11** Specify the following Administration Console information, then select *Continue*.

Username: Specify the name of the administrator that you set up with Administration Console.

Password and Reenter Password: Specify the password for the Administration Console administrator.

IP Address: Specify the IP address of the Administration Console server.

- 12** Specify whether you have custom drivers that you need to load during the installation process.

- ♦ If your machine is using standard hardware, you can select *No*.
- ♦ If you are in doubt or you know you are using hardware components that are not popular items, select *Yes*. During the installation, you are prompted to accept the drivers for the various hardware devices in the machine. If the OS can find a driver for the device, you are prompted to accept it or load a custom driver. Custom drivers can be loaded from either a floppy drive or a flash drive.

- 13** Review the selected configuration. If it is accurate, select *Continue*. If it is inaccurate, select *Back* and fix the problem.

When you select *Continue*, all data currently on the machine is erased.

About 230 modules are installed, depending upon your hardware. The machine reboots, then the following message appears:



Importing into the Administration Console...Please wait.

- 14** Remove the CD.

- 15** (Optional) To verify the installation of the Access Gateway, log in to Administration Console (see [Section 3.2, “Logging In to the Administration Console,”](#) on page 29), then click *Access Manager > Access Gateways*.

If the installation was successful, the IP address of your Access Gateway appears in the Server list.

Access Gateways

Access Gateway Servers							
New Cluster... Shutdown Reboot Refresh Actions ▼							
<input type="checkbox"/> Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration
<input type="checkbox"/> 10.10.16.42	Current		0	Succeeded	View	Linux	Edit
<input type="checkbox"/> 10.10.16.64	Current		0	Succeeded	View	NetWare	Edit

The import into Administration Console can take a few minutes, so if your Access Gateway does not appear in the list, wait a few minutes and refresh the screen.

The Health status indicator appears yellow after the Access Gateway is imported and registers with the Administration Console, which can take up to 5 minutes. You must configure the Access Gateway in order to change its health to green.

If an Access Gateway starts to import into the Administration Console but fails to complete the process, the following message appears:

Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

If you have waited at least ten minutes, but the message doesn't disappear and the Access Gateway doesn't appear in the list, click the *repair import* link. For additional help, see [Appendix A.1, "Troubleshooting the Access Gateway Import," on page 131](#).

- 16** This completes the installation of the NetWare Access Gateway. Continue with one of the following:

- ♦ ["Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.0 SP2 Setup Guide*.](#)
- ♦ [Section 6.2, "Configuring the Log Partition on the NetWare Access Gateway," on page 57.](#)
This is highly recommended if you plan to enabling the logging of transactions. The installation program limits the log: volume to 2 GB.
- ♦ [Section 6.3, "Customizing Error Pages," on page 58.](#)

6.2 Configuring the Log Partition on the NetWare Access Gateway

When the NetWare Access Gateway is installed, the log: volume is configured to share a 4 GB partition with the sys: volume. The log: volume is limited to 2 GB. You can change these limits, if you have the disk space to create a larger log: volume, but the change must be made at the NetWare Access Gateway console and not from the Administration Console. It also requires a reboot of the NetWare Access Gateway to allow access to the NetWare operating system.

- 1** Boot the NetWare Access Gateway with the -NetWareOnly option. See ["Additional Options During the Boot Process" in the *Novell Access Manager 3.0 SP2 Administration Guide*.](#)
- 2** At the NetWare command prompt, unload `autovol`.
- 3** Load `nssmu`.

For more information about this console utility, see [NSSMU \(http://www.novell.com/documentation/nw65/nss_enu/data/boswz11.html\)](http://www.novell.com/documentation/nw65/nss_enu/data/boswz11.html).

- 4** In `nssmu`, delete the log: volume.
Note the drive (device) of the log: volume.
- 5** Delete the FastCache partition on same drive (device) as the log: volume you deleted.
- 6** Create a partition for the log: volume.

Make it as large as you want the log: volume, but no larger. This partition should not take all the space on the drive. On reboot, the FastCache partition for the log: volume is automatically created for you on the same device as the log: volume. You want to reserve as much space as possible for the FastCache partition.

- 7** Create a log: volume on the newly created partition.
Ignore the error on creation.
- 8** Reboot the NetWare Access Gateway.

6.3 Customizing Error Pages

The error messages are in the `sys:\etc\proxy\data\errpage\english\messages.cfg` file. To customize these messages for another language, create a language directory, such as `spanish` in the `errpage` directory and copy the `messages.cfg` file to this directory. Follow the instructions in the `message.cfg` file to localize the error page.

IMPORTANT: When customizing the messages, do not use a semicolon (;) in the message. If you do, the message truncates at the semicolon and only the portion of the message before the semicolon is displayed.

You need to enable FTP or SHH to copy this file, edit it, and return it to the NetWare Access Gateway. See “[Configuring Console Access](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

After you have created the file, you need to select the language. See “[Configuring Error Page Presentation](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Installing SSL VPN

7

You can deploy SSL VPN to interoperate with the Access Gateway in different ways. The default SSL VPN server is restricted to 250 simultaneous user connections and a transfer rate of 50Mbits per second due to some export restrictions. If the export law permits, you can install the high bandwidth version of SSL VPN, as that version does not have the connection and performance restrictions. You can order the high bandwidth version of SSL VPN at no extra cost. After the export controls have been satisfied, the order will be fulfilled.

This section describes deployment scenarios and then describes how to install them.

- ♦ [Section 7.1, “Identifying the Installation You Should Use,” on page 59](#)
- ♦ [Section 7.2, “SSL VPN and the Access Gateway,” on page 62](#)
- ♦ [Section 7.3, “Installing SSL VPN Services,” on page 63](#)
- ♦ [Section 7.4, “Re-Installing SSL VPN on Linux Access Gateway,” on page 66](#)
- ♦ [Section 7.5, “Installing the High Bandwidth Version of SSL VPN,” on page 67](#)
- ♦ [Section 7.6, “Pre-Installing SSL VPN Client Components,” on page 68](#)

7.1 Identifying the Installation You Should Use

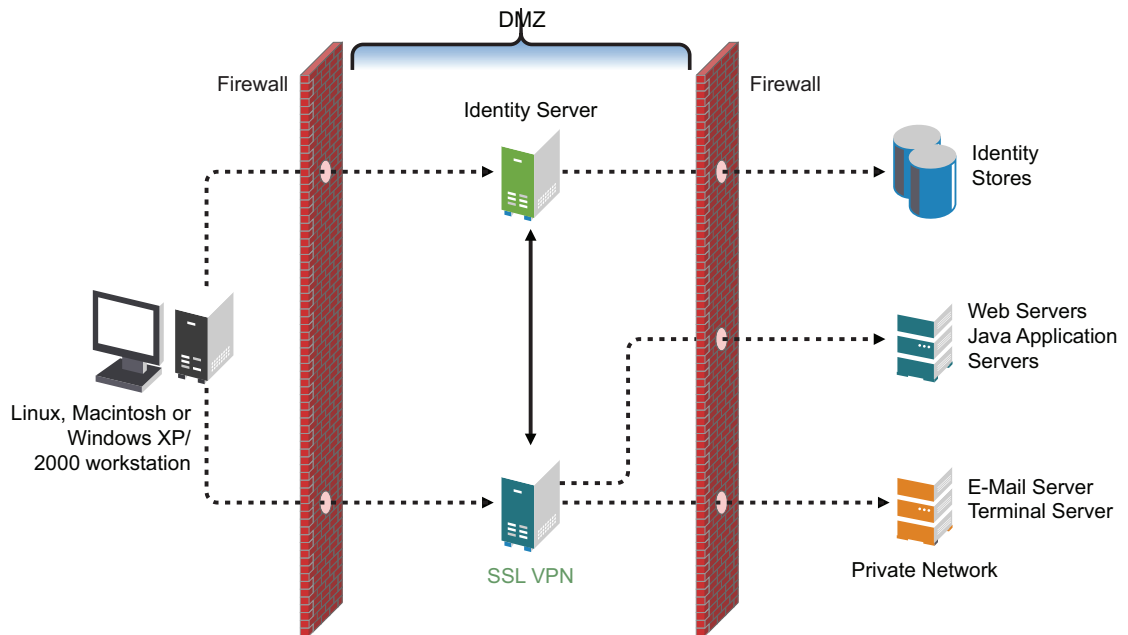
This section provides detailed information about three possible deployment scenarios for SSL VPN. After you determine the deployment scenario, refer to the relevant installation instructions.

This section includes the following topics:

- ♦ [Section 7.1.1, “Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server,” on page 60](#)
- ♦ [Section 7.1.2, “Deployment Scenario 2: Access Gateway and SSL VPN on Different Servers,” on page 61](#)
- ♦ [Section 7.1.3, “Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server,” on page 62](#)

7.1.1 Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server

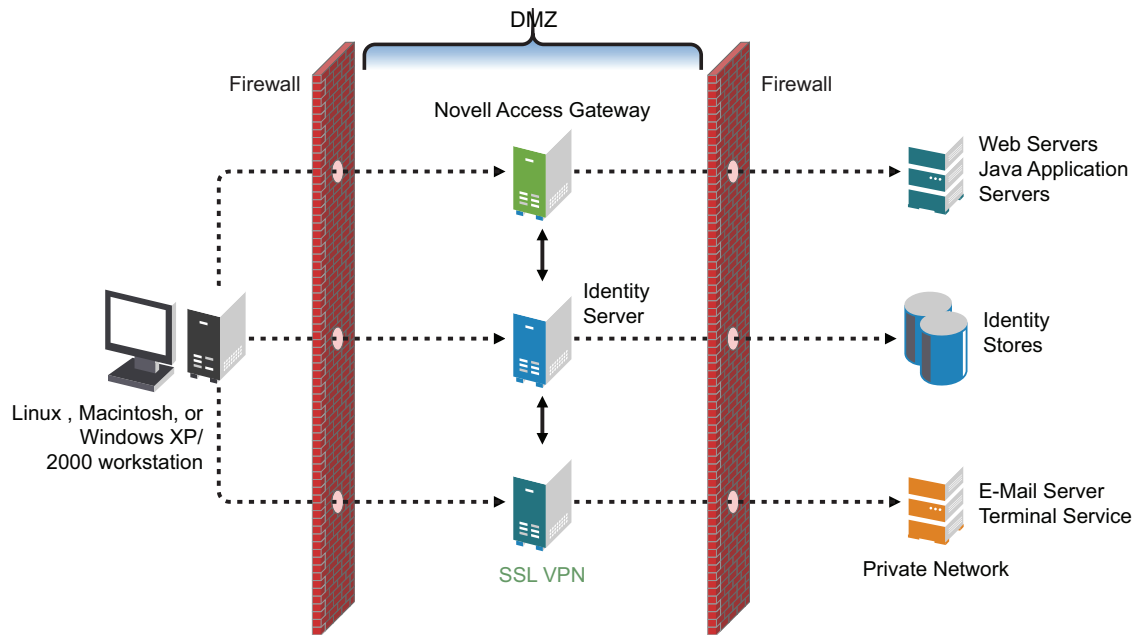
Figure 7-1 *Deployment Scenario 1*



This deployment scenario consists of a demilitarized zone, where the Linux Access Gateway and SSL VPN are on the same server and the Identity Server is deployed separately. For installation instructions for this scenario, see [Section 7.3.2, “Deployment Scenario 1: Installing SSL VPN on the Linux Access Gateway,”](#) on page 63.

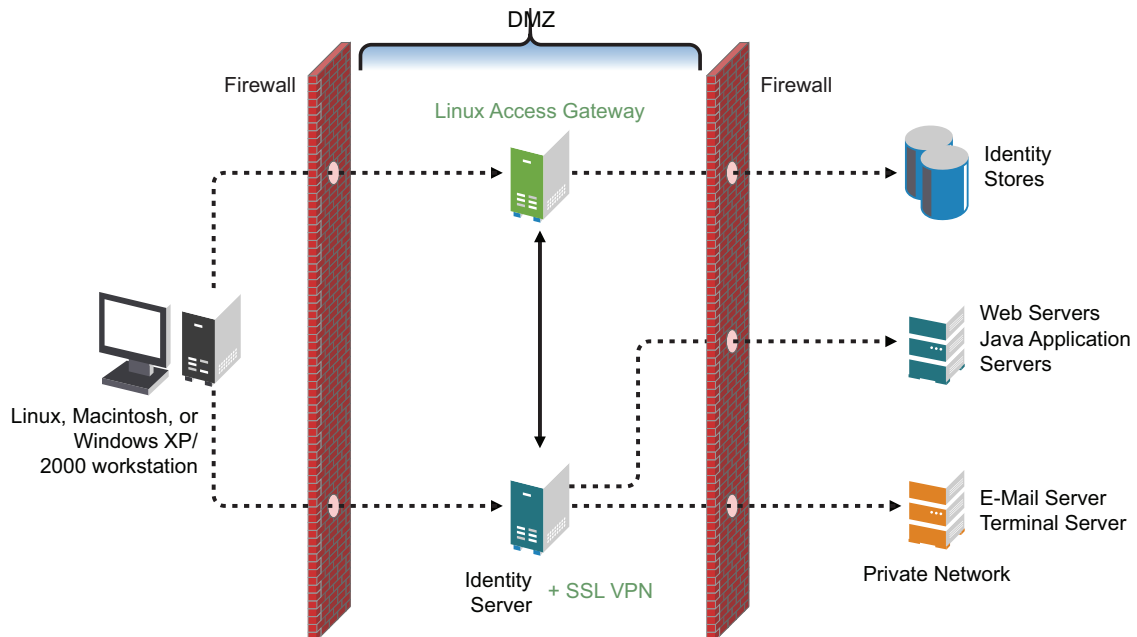
7.1.2 Deployment Scenario 2: Access Gateway and SSL VPN on Different Servers

Figure 7-2 *Deployment Scenario 2*



This deployment scenario consists of a demilitarized zone, where the Access Gateway, Identity Server, and SSL VPN are deployed separately. For installation instructions for this scenario, see [Section 7.3.3, “Deployment Scenario 2: Installing SSL VPN on a Separate Machine,”](#) on page 64.

7.1.3 Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server



This deployment scenario consists of a demilitarized zone, where the Identity Server and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see [Section 7.3.4, “Deployment Scenario 3: Installing Identity Server and SSL VPN on the same Machine,”](#) on page 65.

7.2 SSL VPN and the Access Gateway

When used in conjunction with the Novell® Access Gateway, the SSLVPN server provides access to non-Web resources. SSL VPN is deployed differently depending on which Access Gateway you are using.

- ♦ [Section 7.2.1, “SSL VPN and the Linux Access Gateway,”](#) on page 62
- ♦ [Section 7.2.2, “SSL VPN and the NetWare Access Gateway,”](#) on page 62

7.2.1 SSL VPN and the Linux Access Gateway

If you are using the Linux Access Gateway, you can use [Deployment Scenario 1: Linux Access Gateway and SSL VPN on the Same Server](#), [Deployment Scenario 2: Access Gateway and SSL VPN on Different Servers](#), or [Section 7.1.3, “Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server,”](#) on page 62.

7.2.2 SSL VPN and the NetWare Access Gateway

If you are using the NetWare® Access Gateway, you can use [Deployment Scenario 2: Access Gateway and SSL VPN on Different Servers](#), or [Section 7.1.3, “Deployment Scenario 3: Novell Identity Server and SSL VPN on the Same Server,”](#) on page 62. In other words, you cannot have a deployment scenario where SSL VPN and the NetWare Access Gateway are on the same server.

7.3 Installing SSL VPN Services

Your installation depends on the preferred deployment scenario explained in [Section 7.1, “Identifying the Installation You Should Use,”](#) on page 59. Decide which scenario to use, make sure you have filled the prerequisites, then install SSL VPN.

This section includes the following topics:

- ♦ [Section 7.3.1, “Prerequisites,”](#) on page 63
- ♦ [Section 7.3.2, “Deployment Scenario 1: Installing SSL VPN on the Linux Access Gateway,”](#) on page 63
- ♦ [Section 7.3.3, “Deployment Scenario 2: Installing SSL VPN on a Separate Machine,”](#) on page 64
- ♦ [Section 7.3.4, “Deployment Scenario 3: Installing Identity Server and SSL VPN on the same Machine,”](#) on page 65
- ♦ [Section 7.3.5, “Verifying that Your SSL VPN Service Is Installed,”](#) on page 66

7.3.1 Prerequisites

- ☐ You have root privileges.
- ☐ You have the following information:
 - ♦ IP address of the SSL VPN server
 - ♦ Name of the internal interface
 - ♦ IP address of Administration Console installed on the Identity Server

7.3.2 Deployment Scenario 1: Installing SSL VPN on the Linux Access Gateway

- ♦ [“Standard Installation”](#) on page 63
- ♦ [“Advanced Installation”](#) on page 64

Standard Installation

In a standard installation of the Linux Access Gateway, SSL VPN is installed automatically. This is the preferred method of installation.

For more information on a standard installation of the Linux Access Gateway, refer to [Section 5.3, “Using a Standard Linux Installation with the Default Settings,”](#) on page 36.

In the Access Administrator Configuration section in the Novell Linux Access Gateway Configuration page, select the *Enable SSL VPN Service* check box to install and configure SSL VPN on the Linux Access Gateway.

Figure 7-3 Novell Linux Access Gateway Configuration Page

Novell Linux Access Gateway

Access Administrator, Identity Server and SSL VPN Service Configuration.

Select the **Enable On Box Identity Server** check box to install and Configure the Identity Server on the Linux Access Gateway. Select/Enter the Access Administrator **IP Address** to import the Linux Access Gateway to local/remote Access Administrator. Enter the Access Administrator **User Name**. Enter the **Password**. **Re-enter the Password** for verification. Select the **Enable SSL VPN Service** check box to install, Configure, and start SSL VPN service on the Linux Access Gateway.

Novell Linux Access Gateway Configuration

Administration Console Configuration

☐ Enable On Box Identity Server

☐ Enable On Box Administration Server

☐ Enable On Box SSLVPN Server

IP Address:

User Name:

admin

Password:

Re-enter Password:

Back Abort Next

Advanced Installation

For an advanced installation of Linux Access Gateway, use the following steps to install SSL VPN:

- 1 Start the advanced installation of the Linux Access Gateway. For details, refer to [Chapter 5, “Installing the Linux Access Gateway,”](#) on page 35.
- 2 On the Access Administrator Configuration page, select *Enable SSL VPN Service*. This installs SSL VPN along with the Linux Access Gateway.
- 3 Click *Accept*.
The Installation Settings page is displayed. If the installation is successful, SSL VPN is displayed in the Software section.
- 4 Follow the on-screen instructions to continue with the Linux Access Gateway installation.

7.3.3 Deployment Scenario 2: Installing SSL VPN on a Separate Machine

- 1 Insert the CD into the CD drive, then locate `install.sh`.
- 2 At a command prompt, enter the following install script command:
`./install.sh`
You are prompted to select an installation.
- 3 Type 3 to install Novell SSL VPN Agent, then press Enter.
The license agreement is displayed.
- 4 Review and accept the License Agreement.
- 5 Specify the name of the administrator for the Administration Console.

- 6 Specify the administration password.
- 7 Confirm the password.
- 8 (Conditional) If you are installing the SSL VPN server on the same machine as the Administration Console, you are not prompted for the IP address of the Administration Console. If the Administration Console is on a different machine, you are prompted for its IP address.
- 9 (Conditional) If the SSL VPN machine has been configured with multiple IP address, you are prompted to select an IP address for the SSL VPN server.
- 10 Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.
The installation ends with the following message: `Installation complete.`
- 11 To verify the installation of the Access Gateway, continue with [Section 7.3.5, “Verifying that Your SSL VPN Service Is Installed,” on page 66.](#)

7.3.4 Deployment Scenario 3: Installing Identity Server and SSL VPN on the same Machine

- 1 Insert the CD into the CD drive, then locate `install.sh`.
- 2 At the command prompt, enter the following install script command:
`./install.sh`
You are prompted to select an installation.
- 3 When prompted to install a product, type 3 to install the Novell SSL VPN Agent, then press Enter key to begin.
The license agreement is displayed.
- 4 Review and accept the License Agreement.
- 5 Specify the name of the administrator for the Administration Console.
- 6 Specify the administration password.
- 7 Confirm the password.
- 8 (Conditional) If you are installing the SSL VPN server on the same machine as the Administration Console, you are not prompted for the IP address of the Administration Console. If the Administration Console is on a different machine, you are prompted for its IP address.
- 9 (Conditional) If the SSL VPN machine has been configured with multiple IP address, you are prompted to select an IP address for the SSL VPN server.
- 10 Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.
The installation ends with the following message: `Installation complete.`
- 11 To verify the installation of the Access Gateway, continue with [Section 7.3.5, “Verifying that Your SSL VPN Service Is Installed,” on page 66.](#)






7.3.5 Verifying that Your SSL VPN Service Is Installed

You can check the status of the SSL VPN server in the Administration Console:

- 1 In the Administration Console, click *Access Manager > SSL VPNs*.

A list of SSL VPN servers appears and displays their status under the Server Status icon.

- 2 Click the *Server Status* icon to display the health of the SSL VPN server.

General	Health	Alerts	Command Status	Statistics
Refresh Update from Server				
Status	Description			
	Server is operational (Passed)			
Services Detail				
Type	Status	Message		
Socks		(Passed) Socks Server is up and running.		
Stunnel		(Passed) Stunnel Server is running properly		
OpenVPN		(Passed) OpenVPN service is running properly		
Servlet		(Passed) Servlet is running and registered with Connection Manager		
Close				

The Socks and Stunnel server connections should display green and report Passed. The Servlet status might report Failed until the connection is configured later. This should not impact server functionality.

- 3 Continue with see “[Configuring SSL VPN to Protect an Application](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

For more information, see “[Configuring Basic Setup](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*

7.4 Re-Installing SSL VPN on Linux Access Gateway

If you had installed SSL VPN along with Linux Access Gateway and had to delete SSL VPN, follow the steps given below to re-install SSL VPN:

- 1 Copy the Novell Access Manager `tar.gz` files on to the Linux Access Gateway machine.

For the actual filename, see the “[Novell Access Manager 3.0 SP2 Readme](#)”.

- 2 After downloading the upgrade, unpack the `tar.gz` file using the following command:

```
tar -xzf <filename>
```

- 3 At the command prompt, enter the following install script command:

```
./install.sh
```

You are prompted to select an installation.

- 4 When prompted to install a product, type 1 to install the Novell SSL VPN Agent, then press Enter key to begin.
- 5 Review and accept the License Agreement.
- 6 Specify the IP address of the Administration Console when prompted.
- 7 Specify the name of the administrator for the Administration Console.
- 8 Specify the administration password.
- 9 Confirm the password.
- 10 (Conditional) If the SSL VPN machine has been configured with multiple IP address, you are prompted to select an IP address for the SSL VPN server.
- 11 Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.
The installation ends with the following message: `Installation complete.`
- 12 To verify the installation of the Access Gateway, continue with [Section 7.3.5, “Verifying that Your SSL VPN Service Is Installed,”](#) on page 66.

7.5 Installing the High Bandwidth Version of SSL VPN

The high bandwidth SSL VPN server does not ship with the product because of export laws and restrictions. The high bandwidth version does not have the connection and performance restrictions that are part of the version that ships with the product. Your regular Novell sales channel can determine if the export law allows you to order the high bandwidth version at no extra cost.

After you have ordered the high bandwidth version, log in to the [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) and you will see a link that allows you to download the high bandwidth version.

To check the version of SSL VPN that is currently installed on your system, enter the following command:

```
rpm -qa | grep novl-sslvpn
```

The RPM names for the high bandwidth version appear with an `_hb`.

To install the high bandwidth version of SSL VPN:

- 1 Download the high bandwidth RPMs.
- 2 Log in as `root`.
- 3 Enter the following command to save the backup information in the `config.xml` file:

```
cp /etc/opt/novell/sslvpn/config.xml /etc/opt/novell/sslvpn/config.xml.backup
```
- 4 Enter the following command to stop all services:

```
/etc/init.d/novell-sslvpn stop
```
- 5 Enter the following command to uninstall the RPMs for the low bandwidth version of SSL VPN:

```
rpm -ev novl-sslvpn novl-sslvpn-servlet
```
- 6 Enter the following command to install the RPMs for the high bandwidth version of SSL VPN:

```
rpm -ivh <rpm names>
```

- 7 Enter the following command to restore the configuration information:

```
cp /etc/opt/novell/sslvpn/config.xml.backup /etc/opt/novell/sslvpn/config.xml
```

- 8 Enter the following command to restart all SSL VPN services:

```
/etc/init.d/novell-sslvpn start
```

- 9 Enter the following command to check the status:

```
/etc/init.d/novell-sslvpn status
```

7.6 Pre-Installing SSL VPN Client Components

You can pre-install SSL VPN client components in the client machine, so that the users can access SSL VPN in the Enterprise mode. This section has the following information:

- ♦ [Section 7.6.1, “Installing Client Components for Linux,” on page 68](#)
- ♦ [Section 7.6.2, “Installing the Client Component for Macintosh,” on page 68](#)
- ♦ [Section 7.6.3, “Installing the Client Component for Windows,” on page 69](#)

7.6.1 Installing Client Components for Linux

To install client components for Linux:

- 1 Download the following RPM from the `/var/opt/novell/tomcat4/webapps/sslvpn/linux` directory:

```
novell-sslvpn-serv.tar.gz
```

- 2 Enter the following command to untar the file:

```
tar -zxvf <filename>
```

- 3 Enter the following command to install `novl-sslvpn-service-xxx-xx.i586.rpm`:

```
rpm -ivh <rpm_name>
```

7.6.2 Installing the Client Component for Macintosh

To install client components on Macintosh:

- 1 Download the following package from the `/var/opt/novell/tomcat4/webapps/sslvpn/MacOS` directory:

```
novell-sslvpn-serv.tar.gz
```

- 2 Enter the following command to untar the file:

```
tar -zxvf novell-sslvpn-serv.tar.gz
```

- 3 Enter the following command to install the `novl-sslvpn-service.pkg` package extracted from the tar ball:

```
installer -pkg novl-sslvpn-service.pkg -target “”
```

7.6.3 Installing the Client Component for Windows

To install the client components on Windows:

- 1 Download the following file from `/var/opt/novell/tomcat4/webapps/sslvpn/windows:`

`novel-sslvpn-service-install.exe`

- 2 Run the .exe file to install the client components.

Upgrading Access Manager Components

8

WARNING: Before upgrading, make a backup of your configuration. If the upgrade fails, you need a way to recover your configuration. Because a backup can only be restored to the version it was created on, you'll need to restore your Access Manager components to that version. You can then restore the configuration with the backup file and work with Novell® Support to solve the upgrade problem before attempting to upgrade again.

When upgrading Access Manager components, you need to start the process by first upgrading the Administration Console. You can then upgrade the various devices that you have imported into the Administration Console. We highly recommend that you upgrade all members of a cluster before moving to another type of device to upgrade.

This section discusses the procedures for upgrading the Novell Access Manager components.

- ♦ [Section 8.1, “Upgrading the Administration Console,” on page 71](#)
- ♦ [Section 8.2, “Upgrading the Identity Server,” on page 72](#)
- ♦ [Section 8.3, “Upgrading the Linux Access Gateway,” on page 74](#)
- ♦ [Section 8.4, “Upgrading the SSL VPN Server,” on page 79](#)
- ♦ [Section 8.5, “Upgrading the NetWare Access Gateway,” on page 81](#)
- ♦ [Section 8.6, “Verifying Version Compatibility,” on page 84](#)

For information on upgrading the J2EE Agents, see “[Upgrading the J2EE Agents](#)” in the *Novell Access Manager 3.0 SP2 J2EE Agent Guide*.

8.1 Upgrading the Administration Console

Upgrade running time: about three minutes.

To upgrade from 3.0 SP1 (version 3.0.1-255 or higher if you installed an IR release) to 3.0 SP2:

- 1 Make a backup of your current Access Manager configuration. For instructions, see “[Backing Up and Restoring Components](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

IMPORTANT: You cannot restore data from a previous version of Access Manager to a new version. It is recommended that you create a new configuration backup whenever you upgrade to a newer version of Access Manager.

- 2 If you have Red Carpet® or auto update running, stop these programs before you upgrade the Access Manager Administration Console.
- 3 Open a terminal window.
- 4 Log in as the `root` user.
- 5 Download the upgrade file from [Novell \(http://support.novell.com/patches.html\)](http://support.novell.com/patches.html) and extract the file.

One of the extracted files contains the Administration Console, the Identity Server, and SSL VPN. For the actual filename, see the [Readme \(http://www.novell.com/documentation/novellaccessmanager/index.html\)](http://www.novell.com/documentation/novellaccessmanager/index.html).

- 6 After downloading the upgrade, unpack the `tar.gz` file by using the following command:

```
tar -xzf <filename>
```

For this installation, you need to unpack the Identity Server `.tar.gz` file.

- 7 Open the unpacked Identity Server file, and enter the following at the terminal window:

```
./install.sh
```

- 8 When prompted to install a product, type 1 for *Install Novell Access Manager Administration*, then press the Enter key.

The system detects whether the Administration Console is installed, and prompts you whether to upgrade.

- 9 (Conditional) If the install does not detect a static IP address that Access Manager requires on your machine, you receive an advisory message asking whether or not you want to continue the installation.

Type *Y*, then press *Enter*.

- 10 Type *Y* when the system detects the previous version of the Administration Console, then press *Enter*.

- 11 Review and accept the License Agreement.

- 12 Specify the administration username.

Press Enter to use *admin* as the default admin username, or change this to a username of your choice.

- 13 Specify the administration password.

Use alphanumeric characters only. You must remember this password because it gives rights to the administrator, the configuration store, and subsequent logins to the Administration Console.

- 14 Confirm the password, then wait as the system upgrades the components.

- 15 To verify that the console is running, log in to the console from a workstation (a machine other than where Administration Console is located).

If you encounter an error, see [Section A.4, “Troubleshooting the Administration Console Upgrade,” on page 143](#).

8.2 Upgrading the Identity Server

Upgrade running time: about three minutes.

IMPORTANT: Make sure to complete the following before you begin:

- ♦ If you are upgrading the Access Manager components on multiple machines, ensure that time and date are synchronized on all machines.
 - ♦ Make sure that the Access Manager Administration Console is running. However, you must not perform any configuration tasks in the Administration Console during an Identity Server upgrade.
-

To upgrade from 3.0 SP1 (version 3.0.1.255 or higher if you installed an IR release) to 3.0 SP2:

- 1 Back up any customized JSP pages and related files. The upgrade process replaces all JSP pages in the `/opt/novell/nids/lib/webapp/jsp` directory.
- 2 Open a terminal window.
- 3 Log in as the `root` user.
- 4 Download the upgrade file from Novell (<http://support.novell.com/patches.html>) and extract the file.

One of the extracted files contains the Administration Console, the Identity Server, and SSL VPN. For the actual filename, see the [Readme \(http://www.novell.com/documentation/novellaccessmanager/index.html\)](http://www.novell.com/documentation/novellaccessmanager/index.html).

- 5 After downloading the upgrade, unpack the `tar.gz` file using the following command:

```
tar -xzf <filename>
```

For this installation, you need to unpack the Identity Server `.tar.gz` file.

- 6 Open the unpacked Identity Server file, and enter the following at the terminal window:

```
./install.sh
```

- 7 When prompted to install a product, type 2 to select *Install Novell Identity Server*, then press the Enter key.

The system detects whether an Identity Server is installed, and prompts you whether to upgrade.

- 8 Type *Y*, then press the Enter key.

- 9 If you have backed up your custom JSP pages or you haven't created any, answer *Y* to prompt to continue the upgrade. Otherwise, answer *N* and back up the custom JSP pages before upgrading.

- 10 Review and accept the License Agreement.

- 11 Press Enter to accept the current Administration Console IP address.

- 12 Specify the name of the administrator for the Administration Console.

- 13 Specify the administration password.

- 14 Confirm the password, then wait as the system installs the components. (This takes several minutes.)

The following components are installed:

- ♦ **Novell Access Manager Server Communications:** The components necessary to enable network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
- ♦ **Novell Identity Server:** The component of Novell Access Manager that provides authentication and identity services for the other Access Manager components and third-party service providers.
- ♦ **Novell Identity Server Configuration:** The configuration that allows the Identity Server to be securely configured by the Administration Console.

If the installation process terminates at this step, the probable cause is a failure to communicate with the Administration Console. Ensure that you entered the correct IP address.

- ♦ **Novell Access Manager Server Communications Configuration:** The communication configuration that enables the Identity Server to auto-import itself into the Administration Console.

This completes the Novell Identity Server upgrade. The install logs are located in `/tmp/novell_access_manager`. These logs are all dated and time-stamped.

8.3 Upgrading the Linux Access Gateway

Upgrade running time: about five minutes.

You can upgrade the Linux Access Gateway from 3.0 SP2 to the Novell Access Manager 3.0 SP2 IR1 without affecting the current configuration. This upgrade script downloads the Linux Access Gateway RPM package from the specified server address through either the HTTP or FTP protocol, and then upgrades the Access Gateway modules.

The Linux Access Gateway can be upgraded either in an interactive method, where you are prompted to enter the required parameters; or in a silent method, where all the required parameters are passed in the command line, or by using the administration console.

If you have installed SSL VPN along with the Linux Access Gateway, check for the version of SSL VPN that is currently installed on your machine. If you have the high bandwidth version of SSL VPN installed, log in to the [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) to download the high bandwidth version. The low bandwidth version of SSL VPN is packaged with the Linux Access Gateway upgrade file by default.

This section contains the following information:

- ♦ [Section 8.3.1, “Prerequisites,” on page 74](#)
- ♦ [Section 8.3.2, “Upgrading Linux Access Gateway by Using the Interactive Method,” on page 75](#)
- ♦ [Section 8.3.3, “Upgrading Linux Access Gateway By Passing Parameters in the Command Line,” on page 75](#)
- ♦ [Section 8.3.4, “Upgrading the Linux Access Gateway by Using the Administration Console,” on page 76](#)
- ♦ [Section 8.3.5, “Installing the Latest Linux Patches,” on page 77](#)

8.3.1 Prerequisites

Before you proceed to upgrade the Linux Access Gateway, make sure you do the following:

- ♦ Download the upgrade file from [Novell \(http://support.novell.com/patches.html\)](http://support.novell.com/patches.html) and extract it.
For the actual filename, see the [Readme \(http://www.novell.com/documentation/novellaccessmanager/index.html\)](http://www.novell.com/documentation/novellaccessmanager/index.html).
- ♦ Copy the Linux Access Gateway upgrade file to an HTTP or an FTP server accessible by the gateway.
- ♦ Rename the `.tar.gz` file to `lagrpms.tar.gz`.

The file posted for download needs a specific name that reflects the version of the upgrade. The upgrade script requires that the file have a generic name: `lagrpms.tar.gz`.

NOTE: By default, the Linux Access Gateway RPM package is named `lagrpms.tar.gz`. The RPMs are packaged with the directory name `lagrpms` for the `lagrpms.tar.gz` file. If you have downloaded and repackaged the RPMs with a different package name or directory name, make sure that the directory name matches the package name. For example, if the package name is `final.tar.gz`, make sure that the directory name is also `final`.

8.3.2 Upgrading Linux Access Gateway by Using the Interactive Method

You can interactively upgrade Linux Access Gateway by using the `lagupgrade.sh` script.

- 1 Log in as `root`.
- 2 Enter the following command to start the upgrade script:

```
/chroot/lag/opt/novell/bin/lagupgrade.sh
```
- 3 Specify the upgrade option to use. Enter 1 to upgrade only Linux Access Gateway, 2 to upgrade only SSLVPN, and 3 to upgrade Linux Access Gateway and SSL VPN installed on the same machine.

NOTE: If you have installed Linux Access Gateway and the high bandwidth version of SSL VPN, select option 1 to upgrade Linux Access Gateway only, and then follow the procedure in [“Upgrading High Bandwidth SSL VPN to IR1” on page 80](#) to upgrade SSL VPN. If you select option 3 to upgrade Linux Access Gateway and SSL VPN installed on the same machine, the upgrade process terminates after the Linux Access Gateway is upgraded. Follow the procedure in [“Upgrading High Bandwidth SSL VPN to IR1” on page 80](#) to upgrade SSL VPN.

- 4 Specify the protocol to use when downloading the RPM packages. Enter 1 to use HTTP, 2 to use FTP, and q to quit the upgrade process.
- 5 (Optional) If you selected FTP, you are prompted to specify following information:
 - 5a Specify the FTP username.
 - 5b Specify the FTP password.
- 6 Specify the address of the server where the RPM packages are located.
Use either the IP address or the DNS hostname of the server.
- 7 Specify the path and name of the RPM packages. For example:

```
/publish/upgrades/accessgateway/SP2/lagrpms.tar.gz
```


The RPM package is downloaded to your system and the upgrade begins.
- 8 View the `/var/log/lagupgrade.log` file to verify the results of the upgrade process.

8.3.3 Upgrading Linux Access Gateway By Passing Parameters in the Command Line

The `lagupgrade.sh` upgrade script allows you to enter the required parameters on the command line.

- 1 Log in as `root`.
- 2

```
/chroot/lag/opt/novell/bin/lagupgrade.sh --url <protocol>://  
<hostname>/<path>/<packageName> --upgrade-option <option>
```

<protocol> refers to the protocol to use when downloading the RPM packages. It can be HTTP or FTP.

<hostname> refers to the address of the server from where the RPM packages can be downloaded. Enter either the IP address or the DNS hostname of the server at the prompt.

<path> refers to the path to the RPM packages.

<packageName> refers to the RPM package name.

<option> refers to the upgrade option. By default, the script takes the *LAG only* option and upgrades only the Linux Access Gateway.

- ♦ If you want to upgrade only the Linux Access Gateway, enter the following command:

```
/chroot/lag/opt/novell/bin/lagupgrade.sh --url http://  
10.10.10.1/publish/upgrades/accessgateway/sp2/lagrpms.tar.gz
```

NOTE: If you have installed Linux Access Gateway and the high bandwidth version of SSL VPN, select option 1 to upgrade Linux Access Gateway only, and then follow the steps given in “**Upgrading High Bandwidth SSL VPN to IR1**” on page 80 to upgrade SSL VPN. If you select option 3 to upgrade Linux Access Gateway and SSL VPN installed on the same machine, the upgrade process terminates after the Linux Access Gateway is upgraded. Follow the procedure in “**Upgrading High Bandwidth SSL VPN to IR1**” on page 80 to upgrade SSL VPN.

- ♦ If you want to upgrade both the Linux Access Gateway and SSL VPN that is installed in the same machine, enter the following command:

```
/chroot/lag/opt/novell/bin/lagupgrade.sh --url http://  
10.10.10.1/publish/upgrades/accessgateway/sp2/lagrpms.tar.gz  
--upgrade-option LAG and SSLVPN
```

- ♦ If you want to upgrade only SSL VPN that is installed along with Linux Access Gateway, enter the following command:

```
For example, /chroot/lag/opt/novell/bin/lagupgrade.sh --url  
http://10.10.10.1/publish/upgrades/accessgateway/sp2/  
lagrpms.tar.gz --upgrade-option SSLVPN only
```

3 The RPM package is downloaded to your system and the upgrade begins.

4 View the `/var/log/lagupgrade.log` file to verify the results of the upgrade process.

8.3.4 Upgrading the Linux Access Gateway by Using the Administration Console

You can upgrade the Linux Access Gateway by using the Administration Console.

- 1** In the Administration Console, click *Access Manager > Access Gateways > <Name of Server> > Upgrade*.
- 2** In the *Upgrade URL* field, specify the URL from which to download the upgraded version of the server. The URL must begin with a scheme and end with the filename. For example:
`http://updates.company.com/lag/linux/lagrpms.tar.gz`
- 3** Select either *Upgrade Now* and continue with **Step 4**, or select *Schedule Upgrade* and skip to **Step 7**.
- 4** Click *OK* to start the upgrade.

5 Click *Command Status*, then select the command to view more information about the upgrade.
If the Administration Console successfully sent the upgrade command to the Access Gateway, the command displays *Succeeded*. This does not mean that the upgrade is done, only that the command has been received.

6 Continue with **Step 12**.

7 Click *OK*.

8 Fill in the following fields:

- ♦ **Name Scheduled Command:** Specify a name for the command. This name is used to identify the command on the Command Status page and in log files.
- ♦ **Description:** Specify additional information about the command, if any. This field is optional.
- ♦ **Date & Time:** Specify the date and time to execute the upgrade command. You can select the day, month, year, hour, and minute from the respective drop-down lists.

9 Click *OK*.

10 Click *Command Status* to view more information about the command.

11 The status of the scheduled command changes from *pending* to *executing* when the upgrade begins.

12 To check the status of upgrade, do one of the following:

- ♦ Click *Access Gateways* > <*Name of Server*> > *Upgrade* > *View Upgrade Log* to view the upgrade log.
- ♦ Check the health of the Access Gateway. When the upgrade command is successfully sent, the Access Gateway should be in a green state. As the upgrade proceeds, the health should turn red when the Access Gateway is stopped, white when the Access Gateway is disconnected and rebooting, then green.

13 The following details on the Upgrade page are not updated until the Administration Console performs its regularly scheduled health check:

- ♦ **Current Running Version:** The version that is currently running on the Access Gateway.
- ♦ **Upgrade State:** The current state of the upgrade process.

It can take up to twenty minutes before these fields are refreshed with the current values.

14 (Conditional) If the Health status does not turn green, click the *Health* icon.

If NTP is configured but not synchronized, click *Access Gateways* > *Edit* > *Date & Time*.

If you are using the default NTP server (pool.ntp.org), either you need to wait a few minutes (or longer) for time to synchronize, or you can configure the Access Gateway to use a different NTP server.

8.3.5 Installing the Latest Linux Patches

Novell Linux Access Gateway installs a customized version of SLES 9 SP 3. If you want to install the latest patches as they become available, you must have a Novell user account for receiving Linux updates.

This section describes these tasks:

- ♦ **“Installing the Security Patches” on page 78**

- ♦ “Performing Periodic Installation of Security Patches” on page 78

Installing the Security Patches

To install the latest available Linux patches:

- 1 Log in as `root`.
 - 2 Enter the following command to launch YaST:
`you`
 - 3 In the *Installation source* option, select *Novell Accounts Only*, then tab to *Next* and press Enter.
 - 4 When you are prompted to log in, specify the credentials of your registered Novell user account.
Enable the *Keep Authentication Data* check box, then tab to *Login* and press Enter.
 - 5 Select *Filter > Installable Patches*.
 - 6 Select the security patches of type *Security*, then press Enter.
-
- NOTE:** ♦Make sure that the selected security patches display the + sign.
♦Make sure you select only the *Security* patches.
-
- 7 Click *OK* to proceed with the installation, after you have selected all the security patches.
 - 8 If a Security update for Linux Kernel warning message is displayed, then select *Install Patch* to proceed.
 - 9 If a Security update for subdomain-parser warning message is displayed, then Select *Install Patch* to proceed.
 - 10 Click *OK* to finish the installation process.
 - 11 Restart the Linux Access Gateway for the Linux kernel update to take effect.
 - 12 Enter the following to check the logs:
`tailf /var/log/YaST2/y2log`

Performing Periodic Installation of Security Patches

After you have installed the security patches as explained in “Installing the Security Patches” on page 78, you can follow the procedure given below to update the security patches periodically:

- 1 Log in as `root`.
 - 2 Enter the following command to start the YaST online update:
`you`
 - 3 In the *Installation source* option, select *Novell Accounts Only*, then tab to *Next* and press Enter.
 - 4 Select *Filter > Installable Patches*.
If the installed version is current, then no security patches are listed.
 - 5 Select the security patches of type *Security*, then press Enter.
-
- NOTE:** ♦Make sure that the selected security patches display the + sign.
♦Make sure you select only the *Security* patches.
-
- 6 Click *OK* to proceed with the installation, after you have selected all the security patches.

- 7 Click *OK* to finish the installation process.

8.4 Upgrading the SSL VPN Server

Upgrade running time: about three minutes.

IMPORTANT: Make sure to complete the following before you begin:

- ♦ Make sure that the Access Manager Administration Console is running.
 - ♦ Do not perform any configuration tasks in the Administration Console during an SSL VPN Server upgrade.
-

This section has the following information:

- ♦ [Section 8.4.1, “Upgrading SSL VPN to IR1,” on page 79](#)
- ♦ [Section 8.4.2, “Upgrading Low Bandwidth SSL VPN to High Bandwidth SSL VPN,” on page 80](#)
- ♦ [Section 8.4.3, “Upgrading SSL VPN Installed with Linux Access Gateway,” on page 80](#)
- ♦ [Section 8.4.4, “Upgrading SSL VPN Installed with Identity Server,” on page 80](#)

8.4.1 Upgrading SSL VPN to IR1

Select the correct procedure to upgrade SSL VPN based on the version of SSL VPN you have installed. Use the following instructions for all installations of SSL VPN: installed as standalone component, installed with the Identity Server or the Administration Console, or installed with the Linux Access Gateway.

- ♦ [“Upgrading Low Bandwidth SSL VPN to IR1” on page 79](#)
- ♦ [“Upgrading High Bandwidth SSL VPN to IR1” on page 80](#)

Upgrading Low Bandwidth SSL VPN to IR1

To upgrade the low bandwidth version of SSL VPN, extract the `AM_302_SP2_IR1_sslvpnrpms.tar.gz` file from the patch file.

To install the patch file:

- 1 Untar the `tar.gz` file using the following command:

```
tar -xzf <filename>
```

Replace `<filename>` with `AM_302_SP2_IR1_sslvpnrpms.tar.gz`.

The tar file contains the SSL VPN low bandwidth RPMs and the upgrade script `sslvpn-upgrade-massmedia.sh`.

- 2 Log in as `root`.
- 3 Run the following upgrade script to upgrade low bandwidth SSL VPN:

```
./sslvpn-upgrade-massmedia.sh
```

The low bandwidth SSL VPN is upgraded to the IR1 version.

Upgrading High Bandwidth SSL VPN to IR1

To upgrade the high bandwidth version of SSL VPN, download the AM_302_SP2_IR1_HB_sslvpnrpms.tar.gz file from [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center).

To install the patch file:

- 1 Untar the tar.gz file using the following command:

```
tar -xzf <filename>
```

Replace <filename> with AM_302_SP2_IR1_HB_sslvpnrpms.tar.gz for the high bandwidth SSL VPN.

The tar file contains the SSL VPN high bandwidth RPMs and the upgrade script sslvpn-upgrade-highbandwidth.sh.

- 2 Log in as root.
- 3 Run the following upgrade script to upgrade high bandwidth SSL VPN:

```
./sslvpn-upgrade-highbandwidth.sh
```

The high bandwidth SSL VPN is upgraded to the IR1 version.

8.4.2 Upgrading Low Bandwidth SSL VPN to High Bandwidth SSL VPN

To upgrade from the SP2 low bandwidth version of SSL VPN to the high bandwidth version of SSL VPN, refer to [Installing the High Bandwidth Version of SSL VPN \(http://www.novell.com/documentation/novellaccessmanager/installation/data/bdfqket.html\)](http://www.novell.com/documentation/novellaccessmanager/installation/data/bdfqket.html). Perform this upgrade before installing the patch.

8.4.3 Upgrading SSL VPN Installed with Linux Access Gateway

To upgrade SSL VPN installed with Linux Access Gateway, refer to [Section 8.3.2, “Upgrading Linux Access Gateway by Using the Interactive Method,” on page 75](#) or [Section 8.3.3, “Upgrading Linux Access Gateway By Passing Parameters in the Command Line,” on page 75](#).

8.4.4 Upgrading SSL VPN Installed with Identity Server

WARNING: The following upgrade steps do not work if you want to upgrade the existing SSL VPN 3.0 version installed with Identity Server to SSL VPN 3.0 SP2 IR1 version. To upgrade SSL VPN installed with the Identity Server, follow steps given in either [Section , “Upgrading Low Bandwidth SSL VPN to IR1,” on page 79](#) or [Section , “Upgrading High Bandwidth SSL VPN to IR1,” on page 80](#), whichever is applicable to you.

To upgrade from 3.0 existing version to 3.0 SP2:

- 1 Download the upgrade file from [Novell \(http://support.novell.com/patches.html\)](http://support.novell.com/patches.html) and extract the file.

One of the extracted files is an upgrade file for the SSL VPN, Administration Console, and the Identity Server. For the actual filename, see the [Readme \(http://www.novell.com/documentation/novellaccessmanager/index.html\)](http://www.novell.com/documentation/novellaccessmanager/index.html).

- 2 After downloading the upgrade file, unpack the `tar.gz` file by using the following command:

```
tar -xzf <filename>
```

For this installation, you need to unpack the Identity Server `.tar.gz` file, which contains the SSL VPN files.

The tar file contains the RPMs for the restricted SSL VPN. If you want to upgrade to the high bandwidth SSL VPN, make sure you download the high bandwidth SSL VPN RPM.

- 3 Log in as the `root` user.
- 4 Open the unpacked Identity Server file, and enter the following at the terminal window:
`./install.sh`
- 5 When prompted to install a product, type 3 to select SSL VPN, then press the Enter key.
The system detects whether an SSL VPN Server is installed, and prompts you whether to upgrade.
- 6 Type `Y`, then press the Enter key.
- 7 Review and enter `Y` to accept the License Agreement.
- 8 Press Enter to accept the current Administration Console IP address.
- 9 Specify the name of the administrator for the Administration Console.
- 10 Specify the administration password.
- 11 Confirm the password, then wait as the system installs the components. (This will take several minutes.)
- 12 View the files in the `/tmp/novell_access_manager` directory to verify the results of the upgrade process.

These log files are all dated and time-stamped.

NOTE: Occasionally, the first SSL VPN user connection might fail after upgrading from the Iterative Release version to the Support Pack 2 version, especially if you have encountered any problems during the upgrade process. To work around this problem, we recommend you to initiate a couple of SSL VPN connections after upgrading to the Support Pack 2 version.

8.5 Upgrading the NetWare Access Gateway

Upgrade running time: about ten minutes.

To upgrade from 3.0 SP1 (version 3.0.345, or higher if you installed an IR patch) to 3.0 SP2, you only need to upgrade the NetWare Access Gateway Modules by applying an over-the-wire upgrade. It is a quick and easy method to install patches and fixes from Novell. This process has the following features:

- ♦ Preserves your current configuration.
- ♦ Saves your current software version so you can revert to it if there are any problems with the newest version you have upgraded to.
- ♦ Any connections to the Access Gateway are dropped and cannot be established again until the upgrade process has finished.

To upgrade your NetWare Access Gateway:

- 1 Download the upgrade files from [Novell \(http://support.novell.com/patches.html\)](http://support.novell.com/patches.html) and extract the file.

For the actual filenames for upgrade files of the NetWare Access Gateway, see the [Readme \(http://www.novell.com/documentation/novellaccessmanager/index.html\)](http://www.novell.com/documentation/novellaccessmanager/index.html).

- 2 Copy the NetWare Access Gateway text and the .zip file to a Web server.
- 3 Open the text file, edit the URL line to specify the URL to the .zip file on your Web server, then save the file. For example:
url=http://updates.company.com/accessgateway/otwug/
AM_30_NetWare_AccessGateway_SP2.zip
- 4 In the Administration Console, click *Access Manager > Access Gateways > <Name of Server> > Upgrade*.

The screenshot shows a web-based upgrade interface. At the top, there is a navigation bar with links: "Upgrade Now", "Schedule Upgrade", "Backout to Previous Version", and "View Upgrade Log". Below this, the interface displays the following information:

- Current Running Version: 3000311
- Last Installed Version: 3000309
- Upgrade State: VersionUpgradeComplete
- Upgrade URL: (Note that the 'Upgrade URL' is the URL used to download the upgraded version of the Server.)

At the bottom of the dialog, there is a "Cancel" button.

- 5 In the *Upgrade URL* field, specify the URL to the upgrade text file, starting with the scheme and ending with the text filename. For example:
http://updates.company.com/accessgateway/otwug/
AM_30_NetWare_AccessGateway_SP2.txt
- 6 Select either *Upgrade Now* and continue with **Step 7** or select *Schedule Upgrade* and skip to **Step 10**.
- 7 Confirm the action.
The upgrade starts.
- 8 Click *Command Status*, then select the command to view more information about the upgrade.
If the Administration Console successfully sent the upgrade command to the Access Gateway, the command displays Succeeded. This does not mean that the upgrade is done, only that the command has been received.
- 9 Continue with **Step 14**.
- 10 Confirm the action.

Server Details Edit: Schedule New Command

Note: Date and time entries are specified in local time.

Name Scheduled Command: *

Type: Device Upgrade

Description:

Date & Time: at

- 11 Fill in the following fields:

Name Scheduled Command: A descriptive name for the command. Specify a name that you can use to identify the command on the Command Status page and in log files.

Description: A place to enter additional information about the command. This field is optional.

Date & Time: The date and time the upgrade command executes. From the drop-down lists, select the day, month, year, and the hour and minute when the command executes.

- 12 Click *OK*.

- 13 Click the *Command Status* of the Access Gateway to view more information about the command.

When the status of your scheduled command changes from pending to executing, the upgrade starts.

- 14 To determine when the upgrade has finished, do one of the following:

- View the upgrade log. Click *Access Gateways* > <Name of Server> > *Upgrade* > *View Upgrade Log*.
- View the status of the upgrade on the NetWare Access Gateway console.
- View the health of the Access Gateway. When the upgrade command is successfully sent, the Access Gateway should be in a green state. As the upgrade proceeds, the health should turn red when the Access Gateway is stopped, white when the Access Gateway is disconnected and rebooting, then green.

The following fields on the Upgrade page will not show current information until the Administration Console performs its regularly scheduled health check:

Current Running Version: The version that is currently running on the Access Gateway.

Upgrade State: The current state of the upgrade process.

It can take up to twenty minutes before these fields are refreshed with the current values.

- 15 (Conditional) If the Health status does not turn green, click the *Health* icon.

If NTP is configured but not synchronized, click *Access Gateways* > *Edit* > *Date & Time*:

If you are using the default NTP server (pool.ntp.org), either you need to wait a few minutes (or longer) for time to synchronize, or you can configure the Access Gateway to use a different NTP server.

8.6 Verifying Version Compatibility

After upgrading your Access Manager components, you should verify that they have all been upgraded to the latest version.

- 1 In the Administration Console, click *Access Manager > Overview*.

All of the components should be in a health state. If any have problems, fix those problems before continuing.

- 2 Click *Auditing > Troubleshooting > Version*.

Most of the components should display the same version number. If they don't, click the *Readme* link and verify what versions are required in the current update.

- 3 If any component is displaying an incorrect version number, update that component.

For smooth performance, make sure that all clustered devices are running the same version.

Removing Components

9

This section discusses the following topics related to installation:

- ♦ [Section 9.1, “Uninstalling the Identity Server,” on page 85](#)
- ♦ [Section 9.2, “Reinstalling an Identity Server to a New Hard Drive,” on page 86](#)
- ♦ [Section 9.3, “Uninstalling the Administration Console,” on page 86](#)
- ♦ [Section 9.4, “Uninstalling the Access Gateway,” on page 87](#)
- ♦ [Section 9.5, “Uninstalling the SSL VPN,” on page 87](#)

9.1 Uninstalling the Identity Server

Uninstalling the Novell Identity Server (NIDS) on your Linux box is a two-step process:

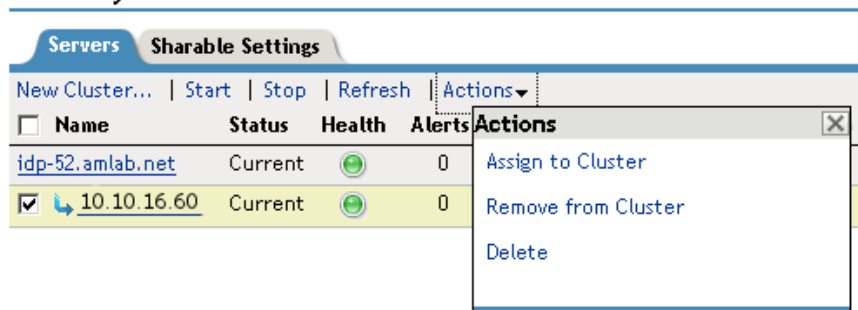
1. [Delete references to NIDS reporting on the Administration Console.](#)
2. [Uninstall NIDS from your host Linux machine.](#)

9.1.1 Deleting NIDS References

As part of the full NIDS uninstallation process, you must delete the Identity Server from the Administration Console. The Identity Server must first be removed from the cluster configuration, then it can be deleted from the Administration Console. You must do this before removing the software from the machine.

- 1 In the Administration Console, click *Identity Servers* > select the Identity Server that you want uninstalled > click the *Actions* drop-down menu under the Servers tab > click *Remove from Cluster*.

Identity Servers



- 2 Update the cluster configuration.
- 3 Select the Identity Server that you are going to uninstall, then click *Actions* > *Delete*.
- 4 Continue with [Section 9.1.2, “Uninstalling NIDS,” on page 85](#).

9.1.2 Uninstalling NIDS

- 1 On your NIDS machine, insert the Access Manager installation CD.

- 2 Navigate to the `novell-access-manager-3.x` directory.
- 3 Enter `./uninstall.sh` to initiate the uninstallation script.
- 4 Enter `1` to uninstall all Novell Access Manager components.

All Access Manager components are removed from the server.

9.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall the Identity Server (see [Chapter 4, “Installing the Novell Identity Server,” on page 33](#)) and leave the Identity Server configuration intact in the Administration Console. In order to preserve the existing keystores, perform the following steps before installing the Identity Server on the new hard drive.

- 1 Stop the server.

In the Administration Console, click *Access Manager > Identity Servers*. Select the server and click *Stop*. (Allow a few seconds for the server to stop.)

- 2 Select the server, then click *Actions > Remove from configuration*.
- 3 Select the server, then click *Actions > Delete*.
- 4 Reinstall the Identity Server. (See [Chapter 4, “Installing the Novell Identity Server,” on page 33](#).)
- 5 On the Identity Servers page, select the server, then click *Actions > Assign to Cluster*.
- 6 Select the Identity Server cluster configuration, then click *Assign*.
- 7 Click *OK*.

9.3 Uninstalling the Administration Console

Only the primary version of the Administration Console contains the Certificate Authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You will need to promote a secondary console to be the primary console. See [“Installing Secondary Versions of the Administration Console”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

To uninstall the Administration Console:

- 1 Insert CD 1 into the drive.
- 2 Log in as the `root` user or equivalent.
- 3 At the command prompt of the Novell Access Manager directory, enter the following:
`./uninstall.sh`
- 4 Select one of the following options:

Option	Description
1	All Access Manager components (including the config store and iManager)
2	Select specific components to uninstall

Option	Description
3	Forcefully uninstall all components (not recommended) Use this option after a failed installation; otherwise use 1 or 2 to uninstall Access Manager components.
4	Quit without uninstalling

9.4 Uninstalling the Access Gateway

- 1 In the Administration Console, click *Access Gateways*.
- 2 If the Access Gateway belongs to a cluster, you need to remove it from the cluster.
 - 2a Select the Access Gateway, then click *Actions > Remove from Cluster*.
 - 2b Confirm the action, then click *OK*.
 - 2c On the Identity Servers page, update the Identity Server status for the Identity Server cluster configuration that was using this Access Gateway. (See “[Updating an Identity Server Configuration](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.)
- 3 On the Access Gateways Servers page, select the IP address of the server, then click *Delete > OK*.

This removes the configuration object for the Access Gateway from the Administration Console.
- 4 On the Access Gateway machine, re-image the machine by booting to a CD containing the desired operating system software.

9.5 Uninstalling the SSL VPN

These instructions are valid for an SSL VPN that you installed with the Identity Server.

- 1 To uninstall, browse and locate the uninstall script.
- 2 At the command prompt, run the following command:
`./uninstall.sh`
- 3 Select the individual components or all the components.

NOTE: If you have installed the SSL VPN with Linux Access Gateway, you cannot uninstall it.

Migrating from iChain to Access Manager

10

One migration strategy cannot fit all iChain® deployments. The goal of this section is to describe several possible configurations, with the idea that you can pick and choose the elements that fit your deployment and design your own migration strategy.

- ♦ [Section 10.1, “Understanding the Differences between iChain and Access Manager,” on page 89](#)
- ♦ [Section 10.2, “Planning the Migration,” on page 91](#)
- ♦ [Section 10.3, “Migrating Components,” on page 99](#)

10.1 Understanding the Differences between iChain and Access Manager

The following sections describe some of the major differences between iChain and Access Manager:

- ♦ [Section 10.1.1, “Component Differences,” on page 89](#)
- ♦ [Section 10.1.2, “Feature Comparison,” on page 90](#)

10.1.1 Component Differences

With iChain, you have a single machine that provides authentication and authorization for single sign-on to protected resources. Administration is done through multiple applications: the Web application, ConsoleOne®, and sometimes an LDAP browser. The embedded operation system is NetWare®, and at the NetWare console, you use command line options to configure the system.

With Access Manager, you have multiple components. Each component can be installed on its own machine, some can be installed on the same machine, and some can be installed on different operations systems: Linux, Windows, and NetWare. Access Manager has the following components:

- ♦ **Administration Console:** Installed on Linux and provides a single point of administration. It stores the configuration for all Access Manager components and uses a modified iManager interface. It can be installed on the same machine as the Identity Server.
- ♦ **Identity Server:** Installed on Linux and provides single sign-on authentication, federation with other identity providers, and role and policy distribution. Roles are assigned at authentication time and filter through all components, thus simplifying the definition of authorization policies.
- ♦ **Access Gateway:** Installed on Linux or NetWare as a soft appliance and provides single sign-on to Web servers and access control through policies to the resources on the Web servers. You can require SSL connections between the browsers and the Access Gateway, but require only HTTP connections between the Access Gateway and the Web servers, thus reducing the need for certificates on the Web servers.
- ♦ **SSL VPN Server:** Installed on Linux and provides single sign-on to private networks with non-HTTP applications.

- ♦ **J2EE Agent:** Installed on a J2EE sever to proved fine-grained authorization for J2EE applications and single sign-on. Currently Access Manager has agents for WebSphere, WebLogic, and JBoss* servers installed on Linux or Windows.

One of the first decisions you'll need to make is which Access Manager components you need (an Administration Console, Identity Server, and Access Gateway are required, the others are optional) and which components you are going to install on separate machines, which ones you are going to combine on a single machine, and what operating systems you want to support.

For a more thorough description of these components, see [Chapter 1, "Introduction to Novell Access Manager,"](#) on page 11.

10.1.2 Feature Comparison

The following table lists some of the major features of Access Manager and indicates support levels for both iChain and Access Manager.

Table 10-1 *iChain and Access Manager Feature Comparison*

Feature	iChain	Access Manager
Web access management	iChain Proxy	Access Gateway
Access management of non-Web applications	Not supported	SSL VPN
Fine-grained access control of J2EE applications	Not supported	J2EE Agents
Identity Federation	SAML 1.0	SAML 1.1/2.0 Liberty Alliance
Management tools	ConsoleOne Web application	iManager (a product-specific version called the Administration Console)
Proxy configuration store	Local. Stored on each iChain appliance.	Global. Stored on the Administration Console and used by all devices.
Authorization configuration store	eDirectory ISO object for protected resources, trusted roots, Form Fill, and Session Broker. eDirectory™ Rule objects (static and dynamic)	Administration Console configuration store
User store and authentication sources	LDAP (eDirectory only), RADIUS, NMAS™, OCSP/CLR Server	LDAP (eDirectory, Active Directory, SunONE), RADIUS, NMAS, OCSP/CLR Server, Custom
Supported operation systems	NetWare	Linux, NetWare, Windows
Citrix* integration	Proxy ICA traffic	SSL VPN

10.2 Planning the Migration

Planning the migration is a three-step process.

- ♦ The first step is planning how you want to deploy the various Access Manager components. For some guidance, see [Section 2.1, “Recommended Installation Scenarios,” on page 19](#).
- ♦ The second step is identifying the type of iChain configuration you currently have deployed and then deciding the type of migrating strategy that fits the needs of your environment. For some ideas, see [Section 10.2.1, “Possible Migration Strategies,” on page 91](#).
- ♦ The third step is understanding how you are currently protecting each resource in your iChain deployment so you can identify the migration requirements of these resources. For some guidance in discovering these needs, see [Section 10.2.2, “Outlining the Migration Requirements for Each Resource,” on page 97](#).

10.2.1 Possible Migration Strategies

The following sections describe several types of iChain configurations and propose a migration strategy for each. These configurations build upon each other. They assume that you will first set up Access Manager independent of your iChain installation and then progressively configure Access Manager to assume responsibility for protecting iChain resources. Such a configuration requires the users to authenticate to both iChain and to Access Manager while the process takes place. If you need to preserve single sign-on while resources are migrated to Access Manager, you can use the phased migration strategy before migrating any important protected resources. If your iChain configuration includes L4 switches for fault tolerance and load balancing, you need to consider the third configuration, which describes how to cluster the various Access Manager components behind an L4 switch. You might also need to set up Access Manager in a staging environment, and when everything is working, transition the machines into your production environment. The staged migration describes some of the issues with this approach.

- ♦ [“A Simple Migration” on page 91](#)
- ♦ [“A Phased Migration” on page 93](#)
- ♦ [“A Phased Migration with an L4 Switch” on page 96](#)
- ♦ [“A Staged Migration” on page 97](#)

A Simple Migration

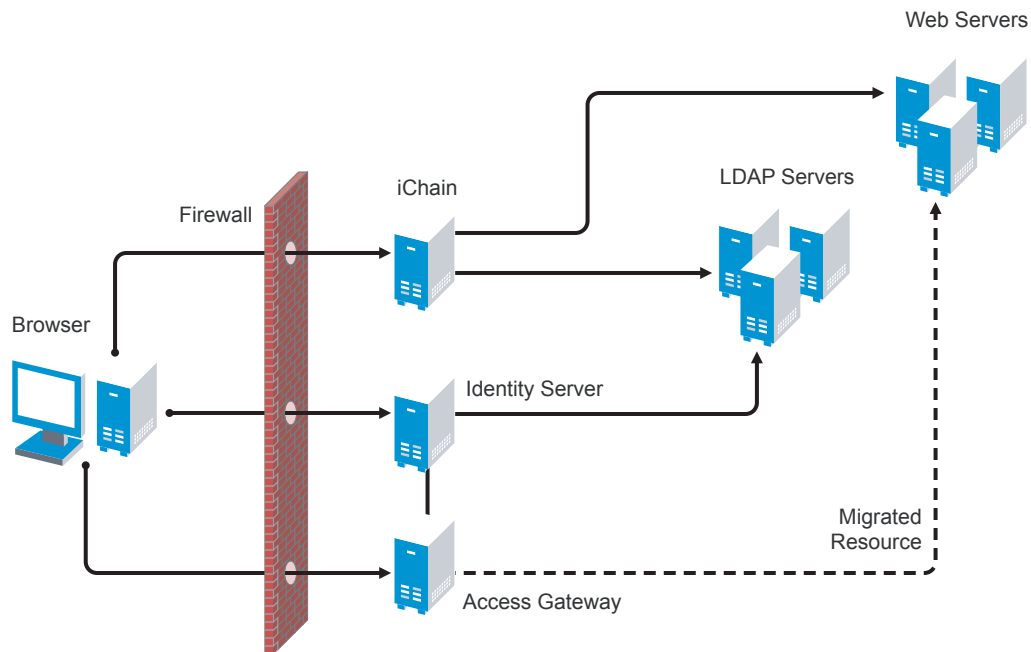
A simple migration works well in the following network environment:

- ♦ You use iChain to protect a few Web servers with only one or two applications each.
- ♦ The policies that control single sign-on and access are simple.
- ♦ If all resources cannot be moved at the same time, you have no problems with requiring your users to authenticate to both iChain and Access Manager:
 - ♦ They can log in to iChain for the resources you haven’t migrated.
 - ♦ They can log in to Access Manager for the resources you have migrated.

You might also use this type of migration when you want to use Access Manager to protect new resources and applications and to use iChain to protect already configured resources. Older resources can be migrated, as time permits, from iChain to Access Manager.

In this type of migration, you set up the Access Gateway independent of iChain. Your network configuration would look similar to the following:

Figure 10-1 Network Setup for a Simple Migration



In this scenario, when a user requests a resource that has not been migrated, the user is prompted to log in to iChain. When a user requests a resource that has been migrated to Access Gateway, the user is prompted to log in to the Identity Server. Both logins are required until all resources have been migrated and iChain has been removed.

Requirements

The following requirements assume that you have users outside your firewall that need access to the protected Web servers.

- ❑ The Access Gateway needs its own public IP address and DNS name, and the Access Gateway needs to be accessible through your firewall.
- ❑ The Identity Server needs its own public IP address and DNS name, and it needs to be accessible through your firewall.
- ❑ You need new hardware for the Access Gateway machine and the Identity Server. For more details, see [“Installation Requirements” on page 19](#).
- ❑ You need to configure your firewall to allow access to the Access Manager components. See [“Setting Up Firewalls”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

Major Tasks

- ❑ Install the software. You need an Administration Console (the Access Manager version of iManager), an Identity Server, and an Access Gateway.
- ❑ Set up a basic configuration. For instructions, see [“Setting Up a Basic Access Manager Configuration”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.

- ❑ Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See [Section 10.3.3, “Configuring the Identity Server for Authentication,”](#) on page 100.
- ❑ Configure the Access Gateway to have the same device settings as iChain. See [Section 10.3.4, “Configuring System and Network Settings,”](#) on page 103
- ❑ Migrate an accelerator with its resources from iChain to the Access Gateway. See [Section 10.3.5, “Migrating the First Accelerator,”](#) on page 106.
- ❑ Remove iChain. See [Section 10.3.9, “Removing iChain,”](#) on page 129.

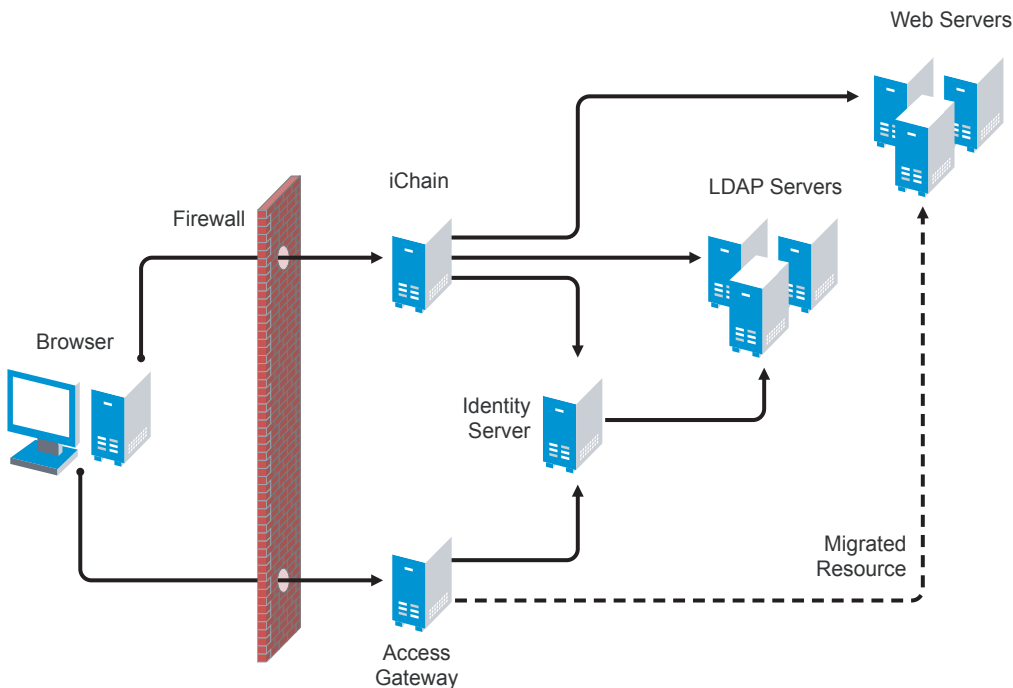
A Phased Migration

You can use a phased migration if iChain is protecting multiple resources that require Form Fill policies, SSL methods, and access control methods. While migrating these more complex resources, we recommend that you set up both iChain and Access Manager on your network. This allows an incremental migration of your resources. When your users access a migrated resource, they are directed to the Access Gateway, and they shouldn’t notice any difference.

Your users will have the same iChain experience with your resources until you have successfully migrated all of them to Access Manager. You can then disable the iChain system. The only differences users should experience are Access Manager login and error pages rather than iChain login and error pages.

Figure 10-2 illustrates the network layout for this type of migration.

Figure 10-2 Network Setup for a Phased Migration

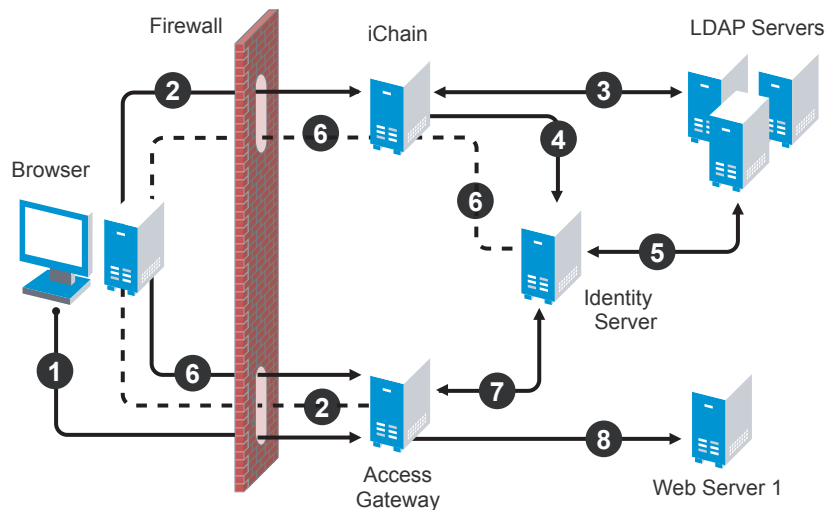


The phased migration uses iChain for authentication and single sign-on to the Identity Server. To do this, you configure the Identity Server to be a restricted resource of iChain, and you configure the Access Gateway to trust the Identity Server as its identity provider. The Access Gateway communicates with the Identity Server to obtain authentication credentials before allowing access to any resources it is protecting.

For resources that haven't been migrated, the browsers are directed to iChain to fulfill the Web resource requests. iChain prompts the user for login credentials, validates them, and if valid, grants access to the requested resource.

As you migrate resources, the Access Gateway is configured to use the same DNS names as you used for the iChain accelerators. As long as your DNS server is configured to resolve these DNS names to the iChain machine, your users access the resources through iChain. When you have completed the migration for one DNS name and have tested the results, you modify the record on the DNS server to resolve the DNS name to the IP address of the Access Gateway, rather than iChain. Your users are redirected to Access Gateway, and they shouldn't notice any differences. **Figure 10-3** illustrates this flow. The dotted lines represent redirected requests.

Figure 10-3 The Flow of a Client Request to a Migrated Resource



Requirements and Restrictions

Hardware: This migration strategy has the following minimum hardware requirements:

- ☐ Identity Server machine
- ☐ Access Gateway machine
- ☐ Administration Console machine (unless the Administration Console is installed with the Identity Server)

The Identity Server and the Access Gateway should be installed on separate machines.

IP Addresses: This migration strategy has the following IP address requirements:

- ☐ A new public DNS name and IP address for the iChain accelerator that is protecting the Identity Server.
- ☐ A DNS name and IP address for the Identity Server. During migration, the IP address and DNS name could be an internal address and name, accessible only behind your firewall.
- ☐ One new public IP address for the Access Gateway.

With this type of configuration, you can test your migrated resources, change the DNS name of the migrated resources to resolve to the Access Gateway, and not modify your iChain configuration. As soon as the DNS name change is propagated, users start accessing the resource through the Access Gateway. If you encounter problems, you can change the record on the DNS server to resolve to the iChain machine while you fix the problems.

Restrictions: This migration strategy has the following restrictions:

- ☐ If you are using path-based multi-homing, you must migrate all accelerators (parent and child) for a specified DNS name at the same time. If you have multiple accelerators that use different DNS names, the migration can be done one accelerator at a time.
- ☐ You cannot use any external identity providers for authentication until iChain is removed from the configuration.

If you need fault tolerance, you can set up clustering any time during the migration process. You can wait until you have migrated a few resources, or you can set up fault tolerance before migrating any resources. See [“A Phased Migration with an L4 Switch” on page 96](#).

Major Tasks

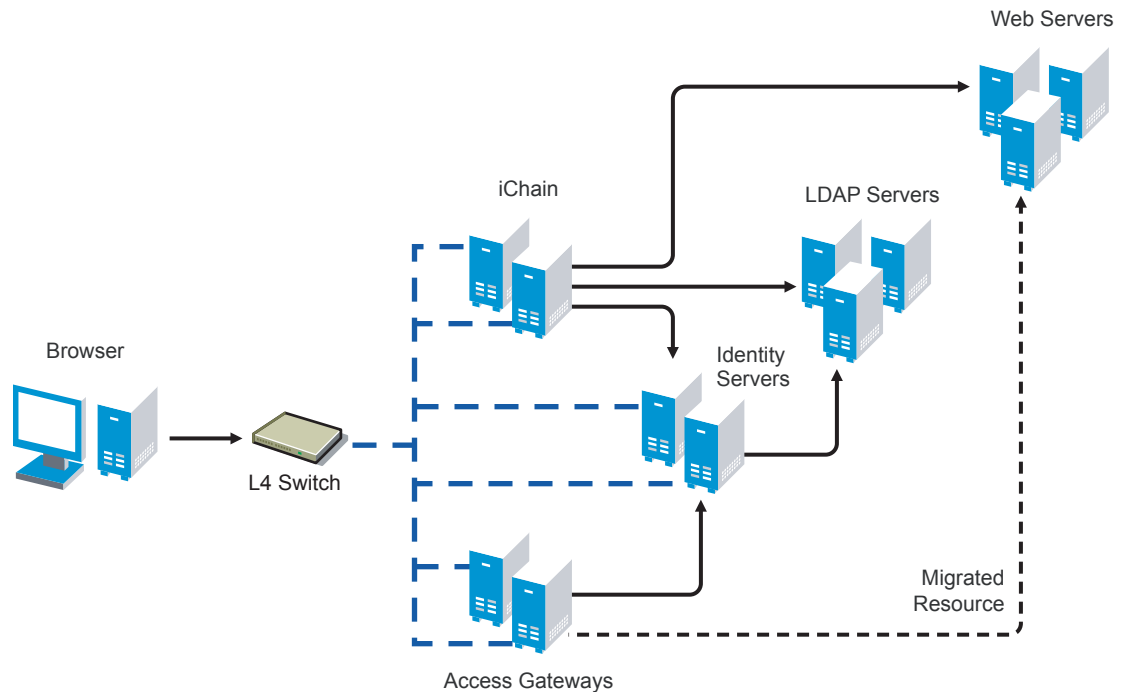
- ☐ Install the software. You need an Administration Console (the Access Manager version of iManager), an Identity Server, and an Access Gateway.
- ☐ Set up a basic configuration. For instructions, see [“Setting Up a Basic Access Manager Configuration”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.
- ☐ Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See [Section 10.3.3, “Configuring the Identity Server for Authentication,” on page 100](#).
- ☐ Configure the Access Gateway to have the same device settings as iChain. See [Section 10.3.4, “Configuring System and Network Settings,” on page 103](#).
- ☐ Migrate an accelerator with its resources from iChain to the Access Gateway. See [Section 10.3.5, “Migrating the First Accelerator,” on page 106](#).

- ❑ Configure iChain and the Identity Server so that the user can log in to iChain and access both iChain resources and Access Gateway resources. See [Section 10.3.6, “Enabling Single Sign-On between iChain and Access Manager,”](#) on page 114.

A Phased Migration with an L4 Switch

If you have configured iChain behind an L4 switch, you need to set up a similar configuration for your Identity Server and Access Gateway machines. This can be done before you migrate any resources from iChain to the Access Gateway or after you have migrated some.

Figure 10-4 Network Setup for a Migration with an L4 Switch



The L4 switch determines which iChain, Identity Server, or Access Gateway machine the user accesses. After you have set up this type of configuration, you then migrate your resources using the same processes as you would use if the servers were not grouped or clustered.

Major Tasks

- ❑ Set up a cluster of Identity Servers. See “[Clustering Identity Servers](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ❑ Set up a group of Access Gateways. See “[Clustering Access Gateways](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.
- ❑ Configure the L4 switch for the servers in the Identity Server cluster and the Access Gateway group. See your L4 switch documentation.
- ❑ Migrate a resource. See [Section 10.2.2, “Outlining the Migration Requirements for Each Resource,”](#) on page 97

A Staged Migration

Many companies have a staging area for deploying new products. The new products are configured and tested in this controlled environment. When the configuration meets the required needs, the machines are moved into the production environment and assigned new IP addresses. You can create such an environment for all components of the Access Manager except for the Access Manager Administration Console. It must be installed where it is going to be used; its IP address cannot change, because that is what all the other components use to trigger auto import and to establish communications with the Administration Console.

If staging is a requirement, you should not install the Administration Console and the Identity Server on the same machine. The Identity Server can be set up in a staged environment and then moved to a production environment and assigned a new IP address. For these same reasons, the Administration Console and the Linux Access Gateway should not be installed on the same machine.

NOTE: By adding a second Administration Console with the IP address you want to use in a production environment, making it the primary Administration Console, then removing the first Administration Console, you can overcome the IP address limitation. You can then perform a reinstall on the first Administration Console and change its IP address. Rather than performing these steps, we highly recommend that you install your Administration Console using the IP address that it needs in a production environment.

10.2.2 Outlining the Migration Requirements for Each Resource

Before you migrate your resources from iChain to Access Gateway, you need to know exactly how iChain was configured to protect your resources. You should export and have available the following iChain files:

- ♦ .nas file
- ♦ Any custom rewriter files
- ♦ XML files for Form Fill policies and the source code of the associated HTML pages
- ♦ Certificates used for SSL

With the aid of these files, determine how you have configured the following:

- ♦ “Proxy Server” on page 97
- ♦ “Accelerator” on page 98
- ♦ “Protected Resources” on page 98
- ♦ “Applications” on page 99

Proxy Server

List how you have configured the proxy server for the following features:

- ♦ Time zone
- ♦ Caching (pin lists and purge lists)
- ♦ Log pushing
- ♦ Alerts (system and Novell® auditing)

- ♦ Tunneling
- ♦ FTP
- ♦ Telnet
- ♦ Custom login, logout, and error pages
- ♦ Network settings: IP addresses of DNS servers and the gateway (router)

Accelerator

For each accelerator, list how you have configured it for the following features:

- ♦ SSL or mutual SSL and the certificates used
- ♦ DNS name and IP address
- ♦ Logging
- ♦ If you use path-base multi-homing in iChain, list the child accelerators for each parent.

Protected Resources

Make a list of the resources the accelerator protects, and by each resource, list how the resource is being protected and how communication between the accelerator and the resource is enabled.

- ♦ DNS name. All protected resources that share the same DNS name must be migrated at the same time.
- ♦ Whether the hostname was forwarded
- ♦ Login required (authentication) or public
- ♦ URLs
- ♦ OLAC
- ♦ ACLCheck
- ♦ Access Control Rules

Access Manager currently caches policy data for the lifetime of that user's session. iChain allows you to exempt a policy from caching, by defining a dynamic rule with a time to live (TTL) in seconds, which causes the policy to be re-evaluated when the TTL associated with that rule expires. This feature is often used to grant users entitlements when they purchase a product, and these new rights are granted without forcing the user to log out and then log in. Access Manager does not currently support this feature.

- ♦ Form Fill
- ♦ SSL or mutual SSL (and the certificates used)
- ♦ Custom HTML rewriter
- ♦ `rewriter.cfg` entries

You might want to use an LDAP browser to view the ACL objects in your directory. If you do not have an LDAP browser, free ones are available for download from the Internet.

Applications

For each protected application, determine the following:

- ♦ For applications residing on J2EE servers, investigate the J2EE Agent and determine if you want to use the J2EE Agent to protect these applications. See the *Novell Access Manager 3.0 SP2 J2EE Agent Guide*.
- ♦ For non-HTTP applications, investigate SSL VPN and determine if you want to use the SSL VPN server to protect these applications. See “[SSL VPN Gateway Configuration](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ♦ HTTP 1.0 applications must support HTTP 1.1 redirects to enable user login to the Identity Server.
- ♦ Citrix integration requires the use of the SSL VPN.

IMPORTANT: Support for NetIdentity authentication has been removed from Access Gateway. If your iChain environment uses NetIdentity authentication to support ZENworks® for Desktops or simple background authentication for proxy login, you’ll need to remove the NetIdentity dependencies before migrating to Access Gateway. If you are using NetIdentity only for background authentication to a back-end NetStorage server, this functionality will continue to work.

10.3 Migrating Components

This section describes the tasks you must complete to migrate iChain resources to Access Manager:

- ♦ [Section 10.3.1, “Setting Up the Hardware and Installing the Software,” on page 99](#)
- ♦ [Section 10.3.2, “Using an L4 Switch,” on page 100](#)
- ♦ [Section 10.3.3, “Configuring the Identity Server for Authentication,” on page 100](#)
- ♦ [Section 10.3.4, “Configuring System and Network Settings,” on page 103](#)
- ♦ [Section 10.3.5, “Migrating the First Accelerator,” on page 106](#)
- ♦ [Section 10.3.6, “Enabling Single Sign-On between iChain and Access Manager,” on page 114](#)
- ♦ [Section 10.3.7, “Migrating Resources with Special Configurations,” on page 117](#)
- ♦ [Section 10.3.8, “Moving Staged Components,” on page 128](#)
- ♦ [Section 10.3.9, “Removing iChain,” on page 129](#)

10.3.1 Setting Up the Hardware and Installing the Software

For details on hardware requirements and possible software configurations, see “[Installation Requirements](#)” on page 19.

For installation instructions, see the following:

- ♦ [“Installing the Access Manager Administration Console” on page 27](#)
- ♦ [“Installing the Novell Identity Server” on page 33](#)
- ♦ [“Installing the NetWare Access Gateway” on page 55](#)
- ♦ [“Installing the Linux Access Gateway” on page 35](#)

If you have firewalls installed that separate any of the Access Manager components from each other, you need to open the required ports so that the components can communicate with each other. If you have a firewall between a component and the Administration Console, the component cannot auto import into the console unless you have opened the ports that allow this communication. For firewall information, see “[Setting Up Firewalls](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

If you are new to Access Manager, we suggest you set up a basic configuration before starting your migration strategy. See “[Setting Up a Basic Access Manager Configuration](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.

If you are going to use SSL, these steps also assume that you have either created the required certificates or imported your third-party certificates.

- ♦ For information on how to configure Access Manager for SSL using certificates created by the the Access Manager CA, see “[Enabling SSL Communication](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.
- ♦ For information on how to use certificates generated by external CAs, see “[Replacing Identity Server SSL Certificates](#)” and “[Configuring the Access Gateway for SSL](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

10.3.2 Using an L4 Switch

When you use an L4 switch to cluster Identity Servers or Access Gateways or both, you need to configure it for each cluster. The base URL of the Identity Server configuration should be the DNS name you have configured the L4 switch to use for the Identity Server cluster. The Access Gateway should be configured to use the DNS name you have configured the L4 switch to use for the Access Gateway cluster. If you configure the Access Gateway to use multiple published DNS names, these DNS names must also resolve to the L4 switch, and the L4 switch must be configured to use them for the Access Gateway cluster.

In addition to this basic setup, see the following sections for configuration tips:

- ♦ “[Clustering with a Non-SSL-Enabled L4 Switch](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*
- ♦ “[Configuration Tips for the L4 Switch](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*

10.3.3 Configuring the Identity Server for Authentication

Before migrating resources, you need to configure the Identity Server to use the same LDAP user stores that iChain is using and configure the authentication profiles that you use for your iChain accelerators. The following sections describe these procedures:

- ♦ “[Migrating Your Authentication Profiles](#)” on page 100
- ♦ “[Migrating the User Store Configuration](#)” on page 101
- ♦ “[Enabling the User Stores for Authentication Methods](#)” on page 102
- ♦ “[Migrating Custom Login Pages](#)” on page 102

Migrating Your Authentication Profiles

You need to migrate authentication profiles that you set up in iChain. If you only set up one LDAP profile for secure name and password, this method is set up by default and you can continue with

“Migrating the User Store Configuration” on page 101. If you set up multiple LDAP profiles, Radius (tokens), mutual SSL (X509 certificates), or NMAS, you need to migrate these profiles.

iChain supports the ORing of profiles; a user can authenticate using one of two methods. The Identity Server does not support ORing of profiles. When you examine your iChain profiles, you need to decide whether to change the ORing to ANDing or to use just one method.

LDAP Authentication Profiles

Examine your iChain LDAP profiles (*Web App > Configure > Authentication > [Name of LDAP Profile] > Modify*). If you created multiple iChain authentication profiles for the same LDAP store by using a different LDAP context or LDAP search base, you need to decide how you are going to migrate these profiles. Select one of the following methods:

- ◆ You can create multiple Identity Server user stores, one for each LDAP context or search base. To create multiple user stores, repeat the procedure described in **“Migrating the User Store Configuration” on page 101**. In **Step 3**, specify a different LDAP context or search base for each user store.
- ◆ You can create authorization policies that restrict access according to the context of the user. To create this type of policy, see **“LDAP Context Policies”** in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ◆ You can create Identity Server roles that match an LDAP context, then create authorization policies that restrict access based on the user’s current roles. For information on creating such a role, see **“Managing Policies”** in the *Novell Access Manager 3.0 SP2 Administration Guide*.

SSL Mutual Authentication

If you used SSL mutual authentication in iChain, you need to configure the Identity Server for this method. Examine your SSL authentication profiles in iChain (*Web App > Configure > Authentication > [Name of SSL Profile] > Modify*).

To migrate this configuration to the Identity Server, see **“Setting Up Mutual SSL Authentication”** in the *Novell Access Manager 3.0 SP2 Administration Guide*.

RADIUS (Token) Authentication

If you used RADIUS authentication in iChain, you need to configure a contract for this method. Examine your RADIUS authentication profile in iChain (*Web App > Configure > Authentication > [Name of Radius Profile] > Modify*).

For Identity Server configuration information, see **“Creating a RADIUS Authentication Class”** in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Migrating the User Store Configuration

- 1** In the Administration Console, create an Identity Server User Store for each unique iChain LDAP Store.
 - 1a** Click *Identity Servers > Edit > Local > New*.
 - 1b** Specify the DN of the user and the user’s password that you want the Identity Server to use when logging into the LDAP server.
 - 1c** Select the type of directory that matches your LDAP server.

- 2 Add a replica to the user store for each LDAP server address in the iChain LDAP store configuration. In the *Server replicas* section, click *New* and specify the required information. You must enter at least one IP address for your LDAP server. If the LDAP directory has been replicated to other servers, enter their IP address information.
- 3 Add a search context.
 - ♦ Use a scope of *Subtree* for an iChain LDAP search base.
 - ♦ Use a scope of *One Level* for an iChain LDAP context.
- 4 To save the configuration, click *Finish*.
- 5 If you used more than one LDAP directory in iChain, repeat these steps and create a user store for each LDAP directory.
- 6 Continue with [“Enabling the User Stores for Authentication Methods” on page 102](#).

Enabling the User Stores for Authentication Methods

- 1 Click *Identity Servers > Edit > Local > Methods*.
- 2 Select the *Identifies User* option.
- 3 Click the name of the method you want to enable.
- 4 Select the user stores in the list of available stores and use the left-arrow to move them to the list of user stores.
- 5 In the list of *User stores*, use the up-arrow and the down-arrow to arrange the order in which the user stores are searched.
- 6 Click *Apply*.
- 7 Repeat [Step 3](#) through [Step 6](#) for any other authentication methods you want to enable for login.
- 8 If you used custom login pages in iChain, continue with [“Migrating Custom Login Pages” on page 102](#). Otherwise, continue with [Section 10.3.4, “Configuring System and Network Settings,” on page 103](#).

Migrating Custom Login Pages

If you used custom login pages in iChain, you need to convert the HTML login page to a JSP page, then associate the JSP page with a class or method that is used to create a contract. You then select this contract for a protected resource, and on first access to that resource, the custom login page is displayed to the user.

Custom Login Page: iChain uses HTML for its login page. Access Manager uses JSP. The default login page for Access Manager is the `login.jsp` file, located in the `/var/opt/novell/tomcat/webapps/nidp` directory. The easiest way to create a new login page is to copy this default page, rename it, then modify it to match your requirements. This page has been designed for the Basic and Protected classes.

Class or Method Properties: The authentication classes and methods support properties. The Radius and Protected classes support a JSP property. You can use other classes, but if you want to create a custom login page, you must select a class that supports the JSP property.

You add this property to either the class or to the method derived from the class. For its value you use the filename of the custom login page you created. If you set the property on the class, you need to create a method that uses the class, then a contract that uses the method.

Contract: In iChain, the custom login page was associated with an accelerator and its location was specified in the *Custom login page location* option on the Web Server Accelerator page. In Access Gateway, the login page is associated with a protected resource, which opens the possibility of having a different login page for each protected resource. You select the login page for the resource by selecting the contract.

For more information, see “[Creating Custom Login Pages](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

10.3.4 Configuring System and Network Settings

To configure the Access Gateway to match the system and network settings you have set up in iChain, you can either manually look at your iChain settings or export and print the `.nas` file and use it as a guide.

We suggest that you set up the Access Gateway to behave in a manner similar to iChain before you begin to migrate resources. However, this is optional. If the default system and network settings in Access Gateway are acceptable, you can skip these steps until later in your migration process except for **Date & Time**. If you have installed the Identity Server and the Access Gateway on separate machines, authentication requests fail if time is not configured accurately and synchronized.

- ♦ To configure the time for the Access Gateway, see **Date & Time**.
- ♦ To configure the time for the Identity Server, use the YAST utility.

Network Settings

This section describes the differences between network settings for iChain and Access Gateway and the paths to access the following settings:

- ♦ “**DNS Servers**” on page 103
- ♦ “**Gateways**” on page 103
- ♦ “**Telnet**” on page 104
- ♦ “**IP Addresses**” on page 104

DNS Servers

iChain Path	Access Gateway Path
Web App > Network > DNS	Access Gateways > Edit > DNS

Both products have the same options. You can add up to three DNS servers that the machine can use to resolve names. You can also configure the same advanced options that control the caching of DNS names.

Gateways

iChain Path	Access Gateway Path
Web App > Network > Gateways / Firewalls	Access Gateways > Edit > Gateways

Both products have the same gateway options. The NetWare Access Gateway does not support SOCKS clients. The Linux Access Gateway does.

Telnet

iChain Path	Access Gateway Path
Must be enabled from the command line: <code>set listener telnet enable=yes</code>	Access Gateways > Edit > Console Access

Telnet is inherently non-secure because everything is transmitted in clear text. If you have enabled Telnet in iChain, we recommend that you disable it in Access Gateway and use SSH instead, which supports data encryption. You enable SSH on the Console Access page of the NetWare Access Gateway. The Linux Access Gateway does not support the Telnet and SSH options.

IP Addresses

iChain Path	Access Gateway Path
Web App > Network > IP Addresses	Access Gateways > Edit > Adapter List

Both products allow you to add IP addresses to existing adapters and configure their subnet masks and options for speed and duplexing. The biggest difference is in how the TCP™ options are configured.

- ♦ In iChain, the TCP options are associated with an adapter.
- ♦ In Access Gateway, TCP Options are associated with a reverse proxy. See *Access Gateways > Edit > [Name of Reverse Proxy] > Listen Options*.

System Settings

In iChain, you could configure the following settings from system settings: Timezone, Date/Time, Actions, SNMP, Import/Export, Upgrade, Alerts, and Admin ACL. The Access Gateway does not support the Import/Export option or the Admin ACL option. Access Manager does allow you to back up the complete configuration and restore it. See “**Backing Up and Restoring Components**” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Both products allow you to configure the following system settings:

- ♦ **Date & Time** (includes time zone)
- ♦ **Upgrade**
- ♦ **Actions**
- ♦ **Alerts**
- ♦ **SNMP**

Date & Time

iChain Path	Access Gateway Path
Web App > System > Date / Time	Access Gateways > Edit > Date & Time
Web App > System > Timezone	

Both products allow you to set the date and time, set up an NTP server, and configure the time zone. Time synchronization is critical if you have installed the Identity Server and the Access Gateway on separate machines. The authentication process, which relies on the exchange of credentials and authentication assertions, fails when the two have a time discrepancy of more than one minute. We recommend that you set up both machines to use NTP and that you verify the time zone of each.

Upgrade

iChain Path	Access Gateway Path
Web App > System > Upgrade	Access Gateways > [Server Name] > Actions > Upgrade

Both iChain and the NetWare Access Gateway have the same options. You can enter the URL where the upgrade files are located and then select to upgrade immediately or schedule the upgrade for a later date. You can also back up to the previous version.

The Linux Access Gateway uses a script to download the upgrade RPMs from a server and upgrade the gateway. See [Section 8.3, “Upgrading the Linux Access Gateway,” on page 74](#).

Actions

iChain Path	Access Gateway Path
Web App > System > Actions	Access Gateways > [Server Name] > Actions

Both products support actions that purge the cache and restart or shut down the machine. Most of these options are not configurable; you need to learn the new location and the new names.

Alerts

iChain Path	Access Gateway Path
Web App > System > Alerts	Access Gateways > Edit > Legacy Alerts or Alerts

Both products have the same options. You can configure Access Gateway to use a Syslog server, send e-mail notifications to a specified list of users, and select the same types of alerts.

SNMP

iChain Path	Access Gateway Path
<i>Web App</i> > System > SNMP	Access Gateways > Edit > SNMP

Both products have the same options. You can allow the community Read access to monitor the state of the Access Gateway, allow the community Write access to the control states of the Access Gateway, and allow traps to be sent.

10.3.5 Migrating the First Accelerator

For your first accelerator, we suggest that you select the one with the fewest configuration requirements. If possible, select one that has only a few child accelerators (path-based or domain-based multi-homing accelerators) and does not require Form Fill or have complex access control policies.

IMPORTANT: All accelerators that use the same DNS name must be migrated at the same time.

The first migration task is to create a reverse proxy on your Access Gateway machine that mirrors the accelerator on your iChain machine. In the beginning, you can set it up to require only authentication because only you will know the URL of this migrated resource. When you know that this works, you can configure its protected resources to use the more advanced access control policies.

As you are configuring the reverse proxy, one of the big differences you'll notice between Access Gateway and iChain is the number of components. In iChain, you have a Web accelerator with protected resources. In Access Gateway, you have a reverse proxy with proxy services that have protected resources. [Figure 10-5](#) illustrates the configuration differences between iChain and Access Gateway.

Figure 10-5 Configuration Options for iChain and Access Gateway

iChain Modules	Configuration Options	Access Gateway Modules
Network / System	<ul style="list-style-type: none"> Gateways DNS Servers Alerts Date & Time 	Access Gateway
Web Server Accelerator	<ul style="list-style-type: none"> Tunnel DNS Name Authentication Accelerator IP Address Accelerator Proxy Port SSL Requirements 	Reverse Proxy
	<ul style="list-style-type: none"> Web Servers Multi-Homing Logging Alternate Host Name 	Proxy Service
ConsoleOne	<ul style="list-style-type: none"> URLs Authentication Procedures Authorization Identity Injection Form Fill 	Protected Resource

Because of these differences, migrating your iChain configuration can involve modifying the Access Gateway, reverse proxy, proxy services, and protected resource configurations. The following sections describe the required tasks:

- ♦ “Setting Up Certificates” on page 107
- ♦ “Migrating the Parent Accelerator” on page 108
- ♦ “Migrating the Path-Based Multi-Homing Accelerators” on page 110
- ♦ “Migrating the Protected Resources” on page 111
- ♦ “Testing the Migrated Resources” on page 113
- ♦ “Enabling User Access to the Migrated Resources” on page 113

Setting Up Certificates

To enable SSL for Access Gateway connections (from the browser to Access Gateway and from Access Gateway to the Web servers), you need to provide certificates:

- ♦ If you are using third-party certificates in iChain, you can import these certificates into Access Gateway. You can import all the certificates at once or you can import a certificate as you migrate a specific accelerator and its children. For information on importing certificates into Access Gateway, see “Importing a Private/Public Key Pair” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- ♦ You can use the certificate authority in Access Gateway to create the certificates. For instructions, see “Creating Certificates” in the *Novell Access Manager 3.0 SP2 Administration Guide*. When you are done with the migration process, you can upgrade these certificates to a higher-grade certificate.

Migrating the Parent Accelerator

A parent accelerator is an accelerator in iChain that has a unique DNS name:

- ♦ If you used domain-based multi-homing in iChain, the parent accelerator is the first accelerator that you created with a host name prepended to the common domain name (for example, test prepended to mycompany.com to create test.mycompany.com for the DNS name of the accelerator). The child accelerators are those that use the common domain name and prepended other host names such as sales.mycompany.com and dev.mycompany.com.
- ♦ If you used path-based multi-homing in iChain, the parent accelerator is the accelerator that defines the DNS name (for example, www.acme.com), and the child accelerators are those that use the DNS name with an appended path (for example, www.acme.com/sales and www.acme.com/products).

To migrate a parent accelerator:

- 1 In the Administration Console, click *Access Gateways > Edit > Reverse Proxy / Authentication*.
- 2 For the Trusted Identity Configuration, select the configuration you set up in [Section 10.3.3, “Configuring the Identity Server for Authentication,” on page 100](#).
The *Logout URL* is empty until you create a reverse proxy. If you have multiple reverse proxies, the URL corresponds to the reverse proxy that you have selected for authentication.
- 3 Click *New*, specify a display name for the reverse proxy, then click *OK*. There is no equivalent field in iChain.
- 4 To configure the reverse proxy communications between the browsers and the Access Gateway, fill in the following fields. (For iChain values, in the Web App click *Configure > Web Server Accelerator > [Name of Accelerator] > Modify*).

iChain Accelerator Parameter	Reverse Proxy Parameter
<i>Accelerator IP addresses</i>	<i>Listening Address(es)</i> : If the Access Gateway is a member of a group, you need to select each group member and configure a listening address. <i>Use SSL for Authentication</i> : This option is available only for the first reverse proxy created for an Access Gateway.
<i>Enable Secure Exchange</i>	<i>Enable SSL between Browser and Access Gateway</i> <i>Auto-generated key</i> : This option is not available in iChain. You can use this option to automatically generate a certificate.
<i>Certificate</i>	<i>Key with the Select Certificate icon</i> : Click the icon and select the certificate that you have set up for the proxy service.
<i>SSL listening port</i>	<i>Secure Port</i>
<i>Accelerator proxy port</i>	<i>Non-Secure Port</i>

The TCP Listen Options cannot be configured until after you have created a proxy service.

- 5 To create a proxy service with the accelerator values, click *New* and fill in the following fields:

iChain Accelerator Parameter	Reverse Proxy Parameter
<i>Name</i>	<i>Proxy Service Name</i> : In iChain, the accelerator name can only be 8 characters. In Access Gateway, the name can be up to 32 characters.
<i>DNS Name</i>	<i>Published DNS Name</i> : These instructions assume that you specify the same name as the value in iChain.
<i>Web server addresses</i>	<i>Web Server IP Address</i>
<i>Alternate host name</i> : selected	<i>Host Header</i> : <i>Web Server Host Name</i>
<i>Alternate host name</i> : deselected	<i>Host Header</i> : <i>Forward Received Host Name</i>
<i>Alternate host name</i> text box	<i>Web Server Host Name</i>

- 6 Click *OK* and configure the proxy service.

iChain Accelerator Parameter	Proxy Service Parameter
<i>DNS Name</i>	<i>Published DNS Name</i> <i>Description</i>
<i>Cookie domain</i>	<i>Cookie Domain</i>

- 7 Click *HTTP Options* and configure the following fields:

iChain Accelerator Parameter	HTTP Options Parameter
<i>Allow Pages to Be Cached at the Browser</i>	<i>Allow Pages to Be Cached by the Browser</i>
<i>Forward Browser IP address in Request Header [X-Forwarded-For]</i>	<i>Enable X-Forwarded-For</i>
<i>N/A</i>	<i>Enable Custom Cache Control Header</i> : iChain does not support this feature, which allows you to add custom headers to your HTML pages and specify a caching policy.

- 8 Click *Global Cache Options* and configure the following fields. (For iChain values, click *Configure > Tuning* or *Configure > Management* in the Web App.)

iChain Accelerator Parameter	Web Servers Parameter
<i>Do not cache objects with ? in the URL</i>	<i>Enable Caching of Objects with a Question Mark</i>
<i>Do not cache objects with /cgi in the path</i>	<i>Enable Caching of Objects with CGI in The Path</i>
<i>Ignore Refresh Requests from Browser</i>	<i>Refresh Request from Browser</i> <i>Enable Filter Cookies</i>
<i>Enable Initial Splash Screen</i>	<i>Enable Initial Splash Screen</i>

iChain Accelerator Parameter	Web Servers Parameter
<i>Act as a Single User (Private) Cache</i>	<i>Act as Single User (private) Cache</i>
<i>Enable Read-Ahead Images Embedded in the Page</i>	<i>Enable Read-Ahead Images Embedded in the Page</i>
	<i>Maximum Number of Concurrent Read-Ahead Requests</i>
<i>Configure > Tuning > Cache Freshness</i>	<i>Cache Freshness:</i> The options are identical except that for iChain they apply to all accelerators and for the Access Gateway they can be set for each proxy service.

- 9 Click *OK > Web Servers*, and configure the following fields:

iChain Accelerator Parameter	Web Servers Parameter
<i>Return Error if Host Name Sent by Browser Does Not Match above DNS Name</i>	<i>Error on DNS Mismatch</i>
<i>Insert button for Web server addresses</i>	<i>New in the Web Server List table</i>
<i>Secure Exchange Options > Enable secure access between the iChain Proxy and the Origin Web Server</i>	<i>Connect Using SSL</i>
<i>Secure Exchange Options > Port (field between the iChain proxy and the Origin Web Server)</i>	<i>Connect Port</i>
	<i>Web Server Trusted Root</i>
<i>Authentication Options > [Name of Profile] > Modify</i>	<i>SSL Mutual Certificate:</i> In iChain, the certificate is part of the authentication profile.

- 10 Click *TCP Listen Options* and configure the fields.
iChain supports these same options. To view how you configured them in iChain, click *Network > IP Addresses > TCP Options* in the Web App.
- 11 To apply your changes, click the *Access Gateways* link, then click *Update > OK*.
- 12 If this accelerator has child accelerators, continue with “**Migrating the Path-Based Multi-Homing Accelerators**” on page 110. If doesn’t have any child accelerators, continue with “**Migrating the Protected Resources**” on page 111.

Migrating the Path-Based Multi-Homing Accelerators

Path-based multi-homing accelerators are migrated as proxy services of the reverse proxy that specifies the DNS name.

- 1 In the Administration Console, click *Access Gateways > Edit > [Name of Reverse Proxy]*.
The Proxy Service List should display the name of the parent accelerator as its first proxy service.
- 2 Click *New* and fill in the following fields. (For iChain values, click *Configure > Web Server Accelerator > [Name of Accelerator] > Modify* in the Web App.)

iChain Accelerator Parameter	Reverse Proxy Parameter
<i>Name</i>	<i>Proxy Service Name</i> : In iChain, the accelerator name can only be 8 characters. In Access Gateway, the name can be up to 32 characters.
<i>Multi-homing Options > Path-based multi-homing</i>	<i>Multi-Homing Type > Path-Based</i>
<i>Multi-homing Options > Sub-path match string</i>	<i>Path</i>
<i>Web server addresses</i>	<i>Web Server IP Address</i>
<i>Alternate host name</i> : checked	<i>Host Header</i> : <i>Web Server Host Name</i>
<i>Alternate host name</i> : unchecked	<i>Host Header</i> : <i>Forward Received Host Name</i>
<i>Alternate host name</i> text box	<i>Web Server Host Name</i>

3 Click OK and fill in the following fields:

iChain Accelerator Parameter	Reverse Proxy Parameter
<i>Multi-homing Options > Remove sub-path from URL</i>	<i>Remove Path on Fill</i>
	<i>Reinsert Path in "set-cookie" Header</i>

4 Click *OK*.

5 To apply your changes, click the *Access Gateways* link, then click *Update > OK*.

6 Continue with **“Migrating the Protected Resources” on page 111**.

Migrating the Protected Resources

In iChain, the ISO object holds the protected resources. You use ConsoleOne to manage the ISO object. You can configure each protected resource to be public, restricted, or secure. iChain could additionally use LDAP information to authorize access.

In Access Gateway, protected resources are not global like iChain; they are assigned to a specific proxy service (which is like an iChain accelerator). Novell Access Manager centralizes the authorization policies and authentication procedures, which can then be assigned to specific protected resources. These policies are greatly expanded and can do much more than the iChain policies. In addition, you do not need to change tools. You configure everything in Novell Access Manager with the Administration Console. In particular, you configure both the protected resources and the policies in the Administration Console.

Because iChain protected resources are global and associated with a DNS name, you need to migrate all the protected resources associated with a DNS name at the same time. The following sections describe how to migrate the protected resources:

- ♦ **“Migrating a Public Resource” on page 112**
- ♦ **“Migrating a Restricted Resource” on page 112**
- ♦ **“Migrating a Secure Resource” on page 113**

Examine your iChain protected resources, and then select the appropriate migration strategy for that resource. If possible, we suggest you migrate a public resource, then a restricted resource. After you have seen the process work for these types of resources, you can migrate your secure resources. The policies that make these resources secure must be re-created in the Administration Console.

Migrating a Public Resource

A public resource is a resource that requires no login procedures or authorization policies.

To migrate these protected resources:

- 1 In the Administration Console, select the Access Gateway, then click *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources* > *New*.
- 2 Specify a display name for the resource. This can be the same name you used for the resource in iChain.
- 3 (Optional) Specify a description for the protected resource.
- 4 In the Contract field, select *None*.
The *Contact* field must be set to *None*. This is what makes this resource a public resource.
- 5 Configure the URL Path List.
The default path is */ **, which allows access to everything on the Web server. Modify this to match your iChain value.
- 6 Click *OK* twice.
- 7 In the *Protected Resource List*, verify that the resource you created is enabled.
- 8 At the bottom of the page, select *Configuration Panel*, then click *OK*.
- 9 On the Server Configuration page, click *OK*.
- 10 On the Access Gateways page, click *Update* > *OK*.
- 11 Continue with **“Migrating a Restricted Resource” on page 112**, or to test the resource you have migrated, continue with **“Testing the Migrated Resources” on page 113**.

Migrating a Restricted Resource

A restricted resource is a resource that requires a login procedure but not an authorization policy. In iChain, these are the resources you configured with ConsoleOne.

To migrate these protected resources:

- 1 In the Administration Console, select the Access Gateway, then click *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources* > *New*.
- 2 Specify a display name for the resource. This can be the same name you used for the resource in iChain.
- 3 (Optional) Specify a description for the protected resource.
- 4 Select the type of contract, which determines the information a user must supply for authentication. During installation, the following contracts and options are set up:
 - ♦ **None:** If you want to allow public access to the resource and not require authentication, select *None* as the contract.

- ♦ **Any Contract:** If the user has authenticated, this option allows any contract defined for the Identity Server to be valid, or if the user has not authenticated, it prompts the user to authenticate using the default contract assigned to the Identity Server configuration.
- ♦ **Name/Password - Basic:** Specifies basic authentication over HTTP using a standard login pop-up screen provided by the Web browser.
- ♦ **Name/Password - Form:** Specifies a form-based authentication over HTTP using the Access Manager login form.
- ♦ **Secure Name/Password - Basic:** Specifies basic authentication over HTTPS using a standard login pop-up screen provided by the Web browser.
- ♦ **Secure Name/Password - Form:** Specifies a form-based authentication over HTTPS using the Access Manager login form.

If you have created other contracts, they appear in the list. If the type of contract you require is not displayed in the list, see [“Migrating Your Authentication Profiles” on page 100](#).

- 5** Configure the *URL Path List*. Add the path or the paths you want protected by this contract.
- 6** Click *OK* twice.
- 7** In the *Protected Resource List*, verify that the resource you created is enabled.
- 8** At the bottom of the page, select *Configuration Panel*, then click *OK*.
- 9** On the Server Configuration page, click *OK*.
- 10** On the Access Gateways page, click *Update > OK*.
- 11** Continue with [“Migrating a Secure Resource” on page 113](#), or to test the resource you have migrated, continue with [“Testing the Migrated Resources” on page 113](#).

Migrating a Secure Resource

A secure resource is a resource that requires a login procedure and an authorization policy. The authorization policy can specify Form Fill parameters, information to be injected into the HTML header (called OLAC in iChain), or additional criteria the user must match to access the resource (called ACLCheck in iChain). See [Section 10.3.7, “Migrating Resources with Special Configurations,” on page 117](#).

Testing the Migrated Resources

- 1** On the workstation where you are going to test the migrated resources, edit the `hosts` file so that the DNS name you have migrated resolves to the IP address of the Access Gateway:
 - ♦ If you are using a Windows workstation, the `hosts` file is located in `C:\Windows\System32\drivers\etc\hosts`.
 - ♦ If you are using a Linux workstation, the `hosts` file is located in `/etc/hosts`.
- 2** From this workstation, request access to all the resources you have migrated.

If you have various login profiles for your users, log in with each profile to ensure that you have access to the correct resources.

Enabling User Access to the Migrated Resources

If you want to create a single sign-on environment, you need to create an accelerator in iChain that protects the Identity Server. See [Section 10.3.6, “Enabling Single Sign-On between iChain and Access Manager,” on page 114](#).

If you are going to install an L4 switch so you can create a cluster of Access Gateways, you might want to install it before allowing public access to the migrated resource. You can use the L4 switch to determine which IP address the DNS name resolves to. The public DNS server resolves the DNS name of the migrated resource to the L4 switch, and the L4 switch determines whether that DNS name is sent to iChain or to the Access Gateway.

If it is acceptable for your users to authenticate to iChain for iChain resources and to use a separate authentication to access the resources migrated to the Access Gateway, complete the following steps:

- 1 Change how the migrated resources are resolved:
 - ♦ If you are using an L4 switch, change the VIP for the migrated resource so that it points to the Access Gateway.
 - ♦ If you aren't using an L4 switch, change the entry on your DNS server so that the DNS name you have migrated points to the IP address of the Access Gateway.
- 2 Monitor your users and see if they have any problems.
 - ♦ If they experience problems that you can't fix immediately, you can change the entry on the DNS server to again point to iChain and do more testing before enabling Access Gateway authentication.
 - ♦ If your users do not experience problems, use the Web application for iChain to disable the accelerator and child accelerators that you have migrated.

10.3.6 Enabling Single Sign-On between iChain and Access Manager

To enable single sign-on between iChain and Access Manager, you need to create an accelerator in iChain that protects the Identity Server. You also need to create a policy that supplies the authentication information. The following steps use OLAC, which is sufficient if your back-end Web servers are using basic authentication. You can also use Form Fill. If you prefer to use Form Fill, skip [Step 7](#) and see [“Using Form Fill instead of OLAC for Single Sign-On” on page 116](#).

- 1 In the iChain Web application, click *Configure > Web Server Accelerator > New*.
- 2 Configure the following fields:

DNS name: Set this to the DNS name specified for the domain name in the Base URL configuration for the Identity Server.

IMPORTANT: The Base URL for the Identity Server must be configured to use a domain name. If you used an IP address for the domain name when you configured the Identity Server, you must modify the Base URL configuration to use a domain name.

Alternate host name: Set this to the DNS name specified for the domain name in the Base URL configuration for the Identity Server.

Return error if host name sent by browser does not match above DNS name: Select this option.

Web server addresses: Set this to the IP address of your Identity Server.

Accelerator proxy port: Set this to the HTTP or HTTPS port value you specified in the Base URL configuration for the Identity Server. The default value is 8080 for HTTP and 8443 for HTTPS.

Enable authentication: Select this option to enable authentication between iChain and the Identity Server.

Enable Secure Exchange: Select this option to enable SSL between the browsers and iChain.

SSL listening port: Set this to the HTTPS port value you are going to use for this accelerator. The default value is 443.

- 3 Click *Secure Exchange Options* and make sure the protocol (HTTP or HTTPS) and port match the Base URL protocol specified in the Base URL configuration for the Identity Server.

- 4 Click *Authentication Options* and set the *Maximum idle time before requiring a new login*.

Set this idle time to the same value you set the Session timeout for the Identity Server.

To verify the Identity Server value, in the Administration Console, click *Access Manager > Identity Servers > Servers > Edit* and view the value for the *Session timeout* field.

- 5 Enable *Forward authentication information to web server*, and add the LDAP profile to the *Service profiles* list.

If you want to AND any other profiles with LDAP, add them to the *Service profiles* list, then click *OK*.

This enables the Identity Server to use the iChain authentication credentials for Identity Server authentication. This only works if you are using an LDAP profile or an LDAP profile ANDed with another profile. For more information, see [“Limitations of the Forward Authentication Method” on page 117](#).

- 6 To save the configuration, click *OK*.

- 7 In iChain ConsoleOne, create a protected resource for the Identity Server accelerator.

- 7a Select the ISO object and access the *Protected Resources* page.

- 7b Add a protected resource. For the URL, use the domain name that you specified for the Base URL of the Identity Server followed by a */**. For example if your domain name for the Identity Server is *users.acme.com*, you would enter

`users.acme.com/*`

- 7c Mark the protected resource as restricted.

- 7d Add an OLAC parameter with the following values:

Name: ICHAIN_UID

Data Source: ldap

Value: cn

This enables basic authentication for single sign-on.

- 7e Save the configuration.

- 8 In the iChain Web application, enable OLAC. Click *Configure > Access Control*, then select *Enable Object Level Access Control (OLAC)*.

- 9 On your DNS server, add an entry so that the domain name specified in the Base URL for the Identity Server resolves to the iChain accelerator IP address.

The domain name in the Base URL for the Identity Server needs to resolve to the iChain accelerator IP address until the migration is completed and iChain is removed. When iChain is removed, the domain name of the Base URL for the Identity Server needs to resolve to the IP address of the Identity Server.

- 10** On your Access Gateway machine, modify the `hosts` file (found in the `etc` directory). Add an entry so that the Access Gateway can directly resolve to the DNS name of the Identity Server.

This allows the Access Gateway to resolve the DNS name of the Base URL of the Identity Server.

Using Form Fill instead of OLAC for Single Sign-On

You can use Form Fill instead of OLAC to provide the authentication information. Your Form Fill policy should look similar to the following:

```
<urlPolicy>
  <name>Identity Provider login</name>
  <url>ncsles9.suse.de/nidp/idff/sso</url>
  <formCriteria>
    <title>Access Manager 3.0 Login</title>
  </formCriteria>
  <javascript></javascript>
  <scriptForPost></scriptForPost>
  <actions>
    <fill>
      <input name="Ecom_User_ID" value="~cn">
      <input name="Ecom_Password" value="~password">
    </fill>
    <post/>
  </actions>
</urlPolicy>
```

You need to modify the domain name (`ncsles9.suse.de`) of the `<url>` element to match the domain name of your Identity Server.

In addition to the Form Fill policy, you need a Login Failure policy. The Login Failure policy should precede the Form Fill policy in the XML file.

```
<urlPolicy>
  <name>IDP Failure</name>
  <url>ncsles9.suse.de/nidp/idff/sso</url>
  <formCriteria>Login failed, please try again. If you continue
    to be unable to login, please contact your system
    administrator.</formCriteria>
  <actions>
    <deleteRemembered>Identity Provider login</deleteRemembered>
    <redirect>ncsles9.suse.de/nidp/idff/sso</redirect>
  </actions>
</urlPolicy>
```

The `<deleteRemembered>` element should only be used if you are using shared secrets. The value of this element is the name of the Form Fill policy (in this example, Identity Provider login). If you are using some other mechanism such as LDAP attributes instead of shared secrets, the `<redirect>` element should be used to redirect your users to your password management URL.

The domain name of the Identity Server (`ncsles9.suse.de`) needs to be replaced and match the domain name of your Identity Server in the `<url>` and `<redirect>` elements.

Limitations of the Forward Authentication Method

Enabling the *Forward authentication information to web server* option has the following limitations:

- ♦ All authentication to the iChain accelerator for the Identity Server must be the same.
- ♦ Single sign-on to the Identity Server is done through the Name/Password - Basic contract and no other credentials if you are using OLAC. If you are using Form Fill, other options are available.

These limitations, if your iChain resources use other authentication methods, impose the following restrictions on your migration plans.

- ♦ Single sign-on is not possible with Token (RADIUS) authentication unless you AND it with LDAP authentication.
- ♦ Single sign-on is not possible with X509 (SSL Mutual) authentication unless you AND it with LDAP authentication.
- ♦ Single sign-on is not possible with multiple accelerators using dissimilar authentication configurations.

The workaround is to choose the most common authentication configuration and migrate all accelerators using that configuration. All other accelerators must be migrated at the same time that iChain is removed from the environment, or if you select to move them one at a time, there is no single sign-on for those accelerators until iChain is removed.

10.3.7 Migrating Resources with Special Configurations

The following sections describe how to configure resources that require such features as Form Fill and ACLCheck.

- ♦ “URLs Requiring Form Fill” on page 117
- ♦ “URLs Requiring OLAC” on page 120
- ♦ “URLs Requiring ACLCheck” on page 123
- ♦ “URLs Requiring HTML Rewriting” on page 126
- ♦ “Migrating Citrix Clients” on page 127
- ♦ “Migrating Protected Resources for J2EE Servers” on page 127
- ♦ “Migrating Protected Non-HTTP Applications” on page 127
- ♦ “Migrating Custom OLAC Drivers” on page 128

URLs Requiring Form Fill

There is no tool to convert the XML files for iChain Form Fill policies to Access Gateway policies. The tables below explain where the information in the iChain policy should be entered in the Access Gateway policy.

Table 10-2 *Form Fill Policy Tags*

Tag or Tag/Attribute	Access Gateway Field
<formName>	In the <i>Form Selection</i> section, select <i>Form Name</i> and specify the value in the text box.
<formNum>	In the <i>Form Selection</i> section, select <i>Form Number</i> and specify the number in the text box
<cgiCriteria>	In the <i>Form Selection</i> section, select the <i>CGI Matching Criteria</i> field. Copy the text between the <cgiCriteria> and the </cgiCriteria> tags into the text box.
<formCriteria>	In the <i>Form Selection</i> section, select the <i>Form Matching Criteria</i> field. Copy the text between the <formCriteria> and the </formCriteria> tags into the text box.
<input name="">	Specify the value in the <i>Input Field Name</i> of the <i>Fill Options</i> section.
<select name="">	Specify the value in the <i>Input Field Name</i> of the <i>Fill Options</i> section.
<input type="">	Select the type in the <i>Input Field Type</i> field of the <i>Fill Options</i> section. For an <input> tag, select <i>Text</i> , <i>Password</i> , <i>Checkbox</i> , or <i>Radio Button</i> .
<select type="">	Select the type in the <i>Input Field Type</i> field of the <i>Fill Options</i> section. For a <select> tag, select <i>Select</i> .
<input value=""> or <select value="">	To specify a value, use the <i>Input Field Value</i> field of the <i>Fill Options</i> section. You can select one of the following value types: <ul style="list-style-type: none"> ♦ Credential Profile: If you select this type, you must select either LDAP or X509 credentials, then select the credential. ♦ LDAP Attribute: If you select this type, you must specify the attribute that contains the value. ♦ Liberty User Profile: If you select this type, you must specify the Liberty attribute that contains the value. ♦ Shared Secret: If you select this type, you must also specify a shared secret store that is used to store the name/value pair. If you haven't created a shared secret store, you can create one. The user is prompt to supply the value on first access; thereafter the shared secret supplies the value.
<input ff_lower_upper=""> <select ff_lower_upper="">	To modify the case of an entered value, use the <i>Data Conversion</i> field of the <i>Fill Options</i> section. Select the appropriate value from the drop-down list.
<injectStaticValue>	To inject a static value, select <i>Insert Text in Header</i> in the <i>Submit Options</i> section.
<debugPost/>	To enabled a debug post, select the <i>Debug Mode</i> field in the <i>Submit Options</i> section.
<maskedPost/>	To mask the post data, select the <i>Mask Data</i> field in the <i>Submit Options</i> section.

Tag or Tag/Attribute	Access Gateway Field
<javaScript>	<p>To retain JavaScript* from the original page, select the <i>Functions to Keep</i> field in the <i>Submit Options</i> section. The <i>Enable JavaScript Handling</i> field must be enabled to modify the <i>Functions to Keep</i> field.</p> <p>Copy the text between the <javaScript> and the </javaScript> tags into the text box of the <i>Functions to Keep</i> field.</p>
<scriptForPost>	<p>To specify additional functions to be executed prior to posting the form, select the <i>Statements to Execute on Submit</i> field of the <i>Submit Options</i> section. The <i>Enable JavaScript Handling</i> option must be enabled to modify the <i>Statements to Execute on Submit</i> field.</p> <p>Copy the text between the <scriptForPost> and the </scriptForPost> tags into the text box.</p>
<errorRedirect>	<p>To redirect the user when an LDAP or NSSS error occurs, select the <i>Redirect to URL</i> field of the <i>Error Handling</i> section.</p> <p>Copy the text between the <errorRedirect> and </errorRedirect> tags to the text box of the <i>Redirect to URL</i> field.</p>
<urlPolicy>	This is the Form Fill policy.
<url>	You assign the Form Fill policy to a protected resource. The protected resource page has a <i>URL Path List</i> where you specify the URL.

Table 10-3 Form Login Failure Policy Tags

Tag or Tag/Attribute	Access Gateway Field
<formName>	In the <i>Form Selection</i> section, select <i>Form Name</i> and specify the value in the text box.
<formNum>	In the <i>Form Selection</i> section, select <i>Form Number</i> and specify the number in the text box
<cgiCriteria>	In the <i>Form Selection</i> section, select the <i>CGI Matching Criteria</i> field. Copy the text between the <cgiCriteria> and the </cgiCriteria> tags into the text box.
<formCriteria>	In the <i>Form Selection</i> section, select the <i>Form Matching Criteria</i> field. Copy the text between the <formCriteria> and the </formCriteria> tags into the text box.
<redirect>	<p>To redirect the user on login failure, select the <i>Redirect to URL</i> field in the <i>Login Failure Processing</i> section.</p> <p>Copy the URL between the <redirect> and </redirect> tags to the text box of the <i>Redirect to URL</i> field.</p>
<deleteRemembered>	To delete the user's stored data for a Form Fill policy, select the <i>Clear Shared Secret Data Values from Policy</i> in the <i>Login Failure Processing</i> section.

Tag or Tag/Attribute	Access Gateway Field
<urlPolicy>	This is the Form Fill policy.
<url>	You assign the Form Fill policy to a protected resource. The protected resource page has a URL Path List where you specify the URL of the page containing the form.

For more information, see “[Creating Form Fill Policies](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

NOTE: Do not migrate your Form Fill policy for Citrix clients. The Access Gateway uses a different process for enabling single sign-on for Citrix clients. For more information, see “[Migrating Citrix Clients](#)” on page 127.

URLs Requiring OLAC

OLAC is called *identity injection* in Novell Access Manager. Information can be injected in one of several ways: authorization header, custom header (name/value pairs), custom headers with tags (tag name-value pairs), or query strings. iChain has the ability to inject constants and authentication profiles from the authenticated directory user. Access Gateway has the ability to inject these and other new types of data.

Identity injection allows you to add information to the HTML header or to the query string of the URL before the request is sent to the Web server. The Web server can use this information to create dynamic pages customized to the user or to determine whether the user should have access to the resource. The Web server determines the information that you need to inject. The following sections provide the information you need to migrate your OLAC policies to Access Manager.

- ♦ “[Policy Comparison between iChain and Access Gateway](#)” on page 120
- ♦ “[Migrating a Policy for the Authorization Header](#)” on page 121
- ♦ “[Migrating a Policy for Custom Header Variables](#)” on page 122
- ♦ “[Migrating a Policy for a Query String](#)” on page 122
- ♦ “[Configuring a Resource to Use an Identity Injection Policy](#)” on page 123

Policy Comparison between iChain and Access Gateway

The following table lists the iChain feature and the equivalent Access Gateway feature.

Table 10-4 Policy Comparison

iChain Feature	Access Gateway Feature
Forward Authentication Information (accelerator properties)	Inject into Authorization Header
OLAC HTTP Header	Inject into Custom Header
OLAC Query String	Inject into Query String
N/A	Inject into Custom Header with Tags

As you can see from the table, Access Gateway supports all the iChain OLAC policies. However, the table doesn't show you all of the new types of data you can inject into the authentication header, the HTTP header, or the URL query string. You can also inject the following types of information:

- ♦ Authentication Contract
- ♦ Client IP
- ♦ Credential Profile (includes both LDAP and X509 credentials)
- ♦ LDAP Attribute
- ♦ Liberty User Profile
- ♦ Proxy Session Cookie
- ♦ Roles for Current User
- ♦ Shared Secret
- ♦ String Constant
- ♦ Java Data Injection Module

For more information, see “[Creating Identity Injection Policies](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Migrating a Policy for the Authorization Header

- 1 In the Administration Console, click *Policies > New*.
- 2 Specify a name for the policy, select *Access Gateway: Identity Injection* as the type, then click OK.
- 3 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple authorization policies to be used for multiple resources.
- 4 In the Actions section, click *New*, then select *Inject into Authentication Header*.
- 5 Configure the *User Name* and *Password* fields.

The following table lists the possible iChain values and indicates the Access Gateway values you need to select.

iChain Value	Access Gateway Value
Default authorization policy	User Name: Credential Profile > LDAP Credentials: LDAP User DN Password: Credential Profile > LDAP Credentials: LDAP Password
ICHAIN_UID=CN	User Name: Credential Profile > LDAP Credentials: LDAP User Name
ICHAIN_PWD=SSN	Password: LDAP Attribute > SSN

- 6 Click *OK* twice, then click *Apply Changes*.
- 7 (Optional) To create other types of OLAC policies, see
 - ♦ “[Migrating a Policy for Custom Header Variables](#)” on page 122
 - ♦ “[Migrating a Policy for a Query String](#)” on page 122

- 8 To assign this policy to a protected resource, see [“Configuring a Resource to Use an Identity Injection Policy” on page 123](#).

Migrating a Policy for Custom Header Variables

In iChain, an automatic X- prefix was added to all custom header variables. Some Web servers do not require the X- prefix to identify custom header variables. To accommodate these servers, Access Gateway does not add a X- prefix to the custom names. If your Web server requires the prefix, you need to add the prefix when you define the name in the Access Gateway policy.

- 1 In the Administration Console, click *Policies > New*.
- 2 Specify a name for the policy, select *Access Gateway: Identity Injection* as the type, then click *OK*.
- 3 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple custom header policies to be used for multiple resources.
- 4 In the *Actions* section, click *New*, then select *Inject into Custom Header*.
- 5 Fill in the following fields:
 - Custom Header Name:** Specifies the name to be inserted into the custom header. If your Web server requires the X- prefix, make sure you include the prefix in this field.
 - Value:** Specifies the value required by the custom header name.
- 6 Repeat [Step 4](#) and [Step 5](#) to add other name/value pairs.
- 7 Click *OK* twice, then click *Apply Changes*.
- 8 To assign this policy to a protected resource, see [“Configuring a Resource to Use an Identity Injection Policy” on page 123](#).

Migrating a Policy for a Query String

Some Web servers require custom information in a query string of the URL. The *Inject into Query String* option allows you to inject this information without prompting the user for it.

- 1 In the Administration Console, click *Policies > New*.
- 2 Specify a name for the policy, select *Access Gateway: Identity Injection* as the type, then click *OK*.
- 3 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple custom header policies to be used for multiple resources.
- 4 In the *Actions* section, click *New*, then select *Inject into Query String*.
- 5 Fill in the following fields:
 - Tag Name:** Specify the name to be inserted into the query string of the URL.
 - Tag Value:** Specify the value required by the tag name.
- 6 Repeat [Step 4](#) and [Step 5](#) to add other name/value pairs.
- 7 Click *OK* twice, then click *Apply Changes*.
- 8 To assign this policy to a protected resource, see [“Configuring a Resource to Use an Identity Injection Policy” on page 123](#).

Configuring a Resource to Use an Identity Injection Policy

Policies are independent of resources. After a policy is created, it can be assigned to multiple protected resources.

- 1 In the Administration Console, select the Access Gateway, then click *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources* > *New*.
- 2 Specify a display name for the resource. This can be the same name you used for the resource in iChain.
- 3 In the *Contract* field, select the type of contract you want the user to use for authentication.
- 4 In the *URL Path List*, click the default path (*/**) and modify it so that it references the resource you want to protect.
- 5 Click *Identity Injection*.
- 6 From the list of policies, select the policies you want to processed for this protected resource, then click *Enable*.
- 7 To save your changes, click *Configuration Panel* > *OK*.
- 8 On the Sever Configuration page, click *OK*.
- 9 On the Access Gateways page, click *Update* > *OK*.

URLs Requiring ACLCheck

In iChain, you set up an ACLCheck rule based on the user's LDAP attributes, objects in the user's dn, and group memberships, and you then assigned the rule to a protected resource. The Access Manager policies are more flexible, and each rule can be implemented in multiple ways. The following migration instructions explain how to use role policies to implement the same functionality you had with ACLCheck. Creating a role policy adds another configuration task, but it also exposes some of the power available in the Access Manager policy engine. After you have created a role and enabled it on the Identity Server, you can use the role in multiple authorization and identity injection policies.

Another option is to create an authorization policy using the LDAP attributes that you specified in the ACLCheck rule as the conditions of the authorization policy. See "[LDAP Context Policies](#)" in the *Novell Access Manager 3.0 SP2 Administration Guide*. For other methods, see "[Creating Access Gateway Authorization Policies](#)" in the *Novell Access Manager 3.0 SP2 Administration Guide*.

To migrate an ACLCheck rule using Access Manager roles, you first create a role policy based on the LDAP attributes you specified in the ACLCheck rule. This role policy is then used to create an authorization policy, which specifies the credentials the user requires to gain access to the resource. This authorization policy is then assigned to the protected resource.

This process is described in the following sections:

- ♦ "[Migrating an ACLCheck Rule to a Role Policy](#)" on page 124
- ♦ "[Creating an Authorization Policy with an Allow and a Deny Rule](#)" on page 124
- ♦ "[Protecting the Resource with the Authorization Policy](#)" on page 126

Migrating an ACLCheck Rule to a Role Policy

To use roles in migrating existing ACLCheck rules:

- 1 In the Administration Console, click *Policies > New*.
- 2 Specify a name for the role, select *Identity Server: Roles* as the type, then click *OK*.
- 3 (Optional) Specify a description for the role.
- 4 In Condition Group 1, click *New*, then select a condition.
 - ♦ For a container rule, select *LDAP OU*, then select *Current*.
 - ♦ For a group rule, select *LDAP Group*, then select *Current*.
 - ♦ For an LDAP attribute rule, select *LDAP Attribute*, then select the name of the attribute.
- 5 For the *Value* field, select the value the user must match to be granted the role.

For example, to create a role for all the users whose DN contained the following objects (ou=provo,ou=sales,o=novell), you would select LDAP OU, the user store, then the DN of the OU.

For an LDAP group, select *LDAP Group*, the user store, then the DN of the group.

For an LDAP attribute, select the value type that matches the attribute's value. To specify a value, select *Data Entry Field*.
- 6 In the Actions section, select *New > Add Role*.
- 7 In the text box, specify the name for the role.

When users log in to Access Manager and if they match the conditions for the role, they are assigned the role. You can then use these role assignments for authorization. See [“Creating an Authorization Policy with an Allow and a Deny Rule” on page 124](#).
- 8 To save the role, click *OK* twice, then click *Apply Changes*.
- 9 Repeat these steps to add other roles for ACLCheck rules.
- 10 Enable the role or roles you have created. Click *Identity Servers > Edit > Roles*. Select the roles you have created, click *Enable*, then click *Apply*.
- 11 Update the Identity Server configuration. Click *Identity Servers > Servers > Update Servers*.

Creating an Authorization Policy with an Allow and a Deny Rule

If you want to allow access to a resource when users meet a certain condition, and deny access to all users who do not meet that condition, one method is to create a policy with an Allow rule and a Deny rule. The policy engine in Access Gateway is flexible enough to allow many designs for a policy. The instructions in this section describe how to create a policy with an Allow rule and a Deny rule. For other ideas see [“Creating Access Gateway Authorization Policies”](#) in the *Novell Access Manager 3.0 SP2 Administration Guide*.

In iChain, the default behavior for secure resources was to deny access unless an ACLCheck rule allowed access. The behavior is different in Access Gateway. After a user has authenticated, the default behavior is to allow access to resources. Therefore, to restrict access to a resource, you need to create a policy that allows access to the users who meet the conditions and denies access to everyone else.

The following instructions explain how to create a rule that grants access to a URL when the user matches the sales role condition and denies access when the user doesn't match the condition.

- 1 In the Administration Console, click *Policies > New*.
- 2 Specify a name for the policy, such as *deny_all_but_sales*.
- 3 Select *Access Gateway: Authorization* from the menu, then click *OK*.

Type: Access Gateway: Authorization

Description:

Priority: 1

Conditions

Condition structure: AND Conditions, OR group:

☒ **Condition Group 1**

New

☒ **If**

Comparison: String : Equals

Mode: Case Sensitive

Value: Roles sales

Result on Condition Error: False

☒ **And If**

Comparison: URL : Equals

Value: Data Entry Field : https://www.novell.com/sales/*

Result on Condition Error: False

Actions

Do Permit

- 4 (Optional) Specify a description for the rule.
- 5 Select the Condition structure.
Select *AND Conditions, OR Groups*, which is the default value.
- 6 In *Condition Group 1*, select *New*, then *Roles for Current User*.
This sets up a condition where the roles that are assigned to the user making the request are compared to the content of the *Value* field.
- 7 Fill in the following fields:
If/If Not: Select *If*. This selection allows you to include or exclude certain roles. In this example, the rule is being configured to allow users with the sales role to access the resource.
Comparison: Select *String*, then select *Equals*.
Mode: Select *Case Sensitive*.
Value: Select *Roles*, then select *sales*.
Result on Condition Error: Select *False*. Because this condition evaluates to False when the user doesn't have the sales role, you want the result to be False when an error occurs during the evaluation of the condition.
- 8 To add a second condition to *Condition Group 1*, click *New*, then select *URL*.
- 9 Fill in the following fields:

If/If Not: Select *If*. This rule is being configured to allow users with the sales role to access the requested URL. The first rule for roles is ANDed with this rule for URLs.

Comparison: Select *URL: Equals*.

Value: Select *Data Entry Field*, then specify the URL in the text box. To allow access to all pages at a location, end the URL with a */**. For example:

`https://www.novell.com/sales/*`

Result on Condition Error: Select *False*. Because this condition evaluates to False when the requested URL doesn't match, you want the result to be False when an error occurs during the evaluation of the condition.

10 Under *Actions*, select *Permit*.

11 Click *OK*.

12 In the *Rule List*, click *New*.

Rule 2 is for denying access to everyone who does not match the conditions in Rule 1.

13 Set the *Priority* to be 2 or greater.

You want the Allow rule to be processed first, so it should have a priority of 1. The Deny rule needs to be processed last, so it needs a lower priority than the Allow rule.

14 Leave the *Condition Group 1* empty.

15 In the *Actions* section, select *Deny* and either accept the default action or select one of the other actions.

16 Click *OK* twice.

17 Click *Apply Changes* on the Policies page.

18 Repeat this process for any other authorization policies you need to create for roles.

Protecting the Resource with the Authorization Policy

To apply the authorization policy to a protected resource:

1 In the Administration Console, click *Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > Protected Resources > [Name of Protected Resource] > Authorization*.

2 Select the authorization policy from the list, then click *Enable*.

3 Click *OK*.

4 To apply your changes, click the *Access Gateways* link, then click *Update > OK*.

URLs Requiring HTML Rewriting

If you created custom rewriter files for iChain or modified the configuration for the internal rewriter (the `sys:/etc/proxy/rewriter.cfg` file), you must enter the data from these files into an Access Gateway rewriter profile. You can create such a profile for each proxy service you configure.

To access the HTML rewriting policy page in the Administration Console, click *Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > HTML Rewriting*.

Table 10-5 shows where to place the information from the iChain file in the Access Gateway profile.

Table 10-5 Converting an iChain Rewriter File to an Access Gateway Profile

iChain File Section	Access Gateway Profile Location
[Name]	Name specified for the HTML rewriter profile
[Extension]	N/A
[Alias Host Names]—internal rewriter only	<i>Additional URL List</i> An additional section, <i>Exclude URL List</i> , allows you to list the URLs that you do not want rewritten.
[URL]	<i>[Profile Name] > If Requested URL Is</i>
[Exclude]	<i>[Profile Name] > And Requested URL Is Not</i>
[Mime Content-type]	<i>[Profile Name] > And Document Content-Type Header Is</i>
[Javascript Variables]	<i>[Profile Name] > Then Variable or Attribute Name to Search for Is</i> This option is available only for a Word profile.
[Javascript Calls]	<i>[Profile Name] > And JavaScript Method to Search for Is</i> This option is available only for a Word profile.
[Replace]	<i>[Profile Name] > Additional Strings to Replace</i>

Migrating Citrix Clients

The Access Gateway can be configured to provide single sign-on for Citrix clients. The iChain configuration for accommodating the Citrix clients cannot be migrated, because the Access Gateway uses an entirely different process and requires a different type of Form Fill policy. See “[Configuring SSL VPN for Citrix Clients](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Migrating Protected Resources for J2EE Servers

If you have created protected resources in iChain for J2EE servers, you should use the J2EE Agent, which hooks into JACC and JAAS rather than migrating these resources to the Access Gateway as protected Web servers. The J2EE Agent allows you to protect specific Web application pages and Java Enterprise Bean interfaces and methods, and you can create a customized authorization policy for each resource.

The J2EE Agent uses the Identity Server for authentication, so single sign-on is enabled between the Access Gateway protected resources and the J2EE Agent protected resources.

For more information, see the *Novell Access Manager 3.0 SP2 J2EE Agent Guide*.

Migrating Protected Non-HTTP Applications

If you have created protected resources in iChain for non-HTTP applications, you should use the SSL VPN server rather than migrating these resources to the Access Gateway as protected resources.

The SSL VPN server uses the Identity Server for authentication, so single sign-on is enabled between the Access Gateway protected resources and the SSL VPN protected resources.

For more information, see “[SSL VPN Gateway Configuration](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

Migrating Custom OLAC Drivers

Instead of migrating custom OLAC drivers, you can create the functionality of these drivers with Access Manager policies. For example, the LDAP OLAC driver could retrieve an LDAP attribute, such as employeeID, from eDirectory and inject the attribute and its value into the HTTP header or query string for the Web server requiring it. In Access Manager, you can accomplish all of this with an identity injection policy. For more information, see “[Creating Identity Injection Policies](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

If the user values you need to inject are not stored in an LDAP directory, you can create a secret store, prompt the users to enter the required values the first time they access the Web server requiring the values, store them in the secret store, and then inject the values when the user accesses the page requiring them. For more information, see “[Creating and Managing Shared Secrets](#)”, “[Creating Form Fill Policies](#)”, and “[Creating Identity Injection Policies](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

10.3.8 Moving Staged Components

The IP address of the Administration Console cannot be changed unless you reinstall all components that were auto-imported into the Administration Console or install a second Administration Console.

NOTE: By adding a second Administration Console with the IP address you want to use in a production environment, making it the primary Administration Console, then removing the first Administration Console, you can overcome the IP address limitation. You can then perform a reinstall on the first Administration Console and change its IP address. Rather than performing these steps, we highly recommend that you install your Administration Console using the IP address that it needs in a production environment.

The other Access Manager components, the Access Gateway, the Identity Server, J2EE Agent, and the SSL VPN server, can change the IP addresses.

- ♦ “[Changing the Address of an Identity Server, J2EE Agent, or SSL VPN Server](#)” on page 128
- ♦ “[Changing the IP Address of an Access Gateway](#)” on page 129

Changing the Address of an Identity Server, J2EE Agent, or SSL VPN Server

- 1 At the console of the machine, start the YaST utility.
- 2 Change the static IP address. If you are physically moving the machine, shut down the machine, move the machine to its new location, and start it.
- 3 In the Administration Console, change the IP address of the Management IP address to match this new IP address. Select one of the following:
 - ♦ For an Identity Server, click *Identity Servers* > *[Name of Server]*, then click the *Management IP Address* link.

- ♦ For an SSL VPN, click *SSL VPNs > [Name of Server]*, then click the *Management IP Address* link.
- ♦ For a J2EE Agent, click *J2EE Agents > [Name of Server]*, then click the *Management IP Address* link.

4 Specify the new address, then click *OK* to save your changes.

Changing the IP Address of an Access Gateway

If the new IP address is in the same subnet, see “[Changing the IP Address of the Access Gateway](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide* for instructions.

If the new IP address is in a different subnet:

- 1 In the Administration Console, click *Access Gateways > Edit > Adapter List*.
- 2 If the machine belongs to a group, select the Access Gateway from the *Group Member* list.
- 3 In the *Adapter eth0* section, select the subnet mask that contains the old IP address.
- 4 Set the Subnet Mask to 0.0.0.0, then click *OK*.
- 5 Select the 0.0.0.0 subnet mask.
- 6 Select the old IP address, click *Change IP Address*, specify the new IP address, then click *OK*.

This option changes all configuration instances of the old IP address to the new IP address. For example, any reverse proxies that have been assigned the old IP address as a listening address are modified to use the new IP address as the listening address.

- 7 To apply your changes, click the *Access Gateways* link, then click *Update > OK*.

The configuration changes are applied to the Access Gateway machine.

- 8 If you are physically moving the machine, move it before completing the rest of these steps.
- 9 Check the IP address that the Administration Console uses for managing the Access Gateway. Click *Access Gateways > [Name of Access Gateway] > Edit*.
- 10 If the old IP address is listed as the *Management IP Address*, select the new IP address. If your Access Gateway has multiple IP addresses, select the one that you want the Administration Console to use for communication with the Access Gateway.

The port should only be modified if there is another device on the Access Gateway that is using the default port of 1443.

- 11 If the name of the Access Gateway is the old IP address, modify the *Name* option.
- 12 Click *OK*.

The Administration Console uses the configured IP address to find the Access Gateway.

If your Access Gateway stops reporting to the Administration Console after completing these steps, you need to trigger an auto-import. See [Section A.1.2, “Triggering an Import Retry,” on page 132](#).

10.3.9 Removing iChain

When you have migrated all your resources to the Access Gateway and the only DNS name that resolves to the iChain machine is the DNS name for the Identity Server accelerator, you are ready to remove the iChain machine from your production environment.

- 1 Reconfigure your DNS server (or L4 switch) so that the DNS name of Identity Server accelerator resolves to the IP address of the Identity Server rather than to the iChain machine.

- 2** The Identity Server uses ports 8080 and 8443. If you have not opened these ports in your firewall, you need to configure iptables on your Identity Server. See “[Translating the Identity Server Configuration Port](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
- 3** When the new configuration has had time to propagate through out your network, remove the network cables from the iChain machine.
- 4** Continue testing the configuration.
- 5** If everything is working as expected, physically remove the iChain machine from your network.

Troubleshooting Installation

A

- ♦ [Section A.1, “Troubleshooting the Access Gateway Import,” on page 131](#)
- ♦ [Section A.2, “Troubleshooting Linux Access Gateway Installation,” on page 138](#)
- ♦ [Section A.3, “Troubleshooting the SSL VPN Device Import,” on page 143](#)
- ♦ [Section A.4, “Troubleshooting the Administration Console Upgrade,” on page 143](#)

A.1 Troubleshooting the Access Gateway Import

When you install the NetWare[®] Access Gateway or the Linux Access Gateway, it should automatically be imported into the Administration Console you specified during installation. If the Access Gateway does not appear in the server list, you need to repair the import.

If the repair option does not correct the problem, the following section explains what should happen and how you can discover what went wrong. This information can be used to accurately report the problem to Novell[®] Support.

- ♦ [Section A.1.1, “Repairing an Import,” on page 131](#)
- ♦ [Section A.1.2, “Triggering an Import Retry,” on page 132](#)
- ♦ [Section A.1.3, “Troubleshooting the Import Process,” on page 133](#)
- ♦ [Section A.1.4, “Unlocking the NetWare Access Gateway Console,” on page 138](#)

A.1.1 Repairing an Import

If the Access Gateway does not appear in the Administration Console within ten minutes of installing an Access Gateway, complete the following steps:

- 1 If a firewall separates the Administration Console and the Access Gateway, make sure the correct ports are opened. See [“When a Firewall Separates the Administration Console from a Component”](#) in the *Novell Access Manager 3.0 SP2 Setup Guide*.
- 2 In the Administration Console, click *Access Gateways*.
- 3 Wait a few minutes, then click *Refresh*.
- 4 Look for a failed import message.

If the device starts an import but fails to finish, a message similar to the following appears at the bottom of the table:

```
Server gateway-<name> is currently importing. If it has been  
several minutes after installation, click repair import to fix it.
```

- 5 Click *repair import*.
- 6 If the device still does not appear or you do not receive a repair import message, continue with [Section A.1.2, “Triggering an Import Retry,” on page 132](#).
- 7 If triggering an import retry does not solve the problem, reinstall the device.
- 8 If reinstalling the device does not correct the problem, continue with [“Understanding the Import Process” on page 133](#) and report the problem to Novell Support.

A.1.2 Triggering an Import Retry

If the import process failed to start (see [Step 3 on page 135](#)), you can manually trigger the import process. These steps explain how to set the IP address of the Administration Console to an incorrect address and then back to the correct address, which triggers the import process. Select the procedure that matches your Access Gateway platform.

- [“For the NetWare Access Gateway” on page 132](#)
- [“For the Linux Access Gateway” on page 132](#)

For the NetWare Access Gateway

- 1 Unlock the console (see [“Unlocking the NetWare Access Gateway Console” on page 138](#)).
- 2 Press Ctrl+Escape and select the Novell Access Gateway Console screen.
If you are in debug mode, first enter 0 to go to the next page and then enter 4.
- 3 Verify that the Access Gateway can communicate with the Administration Console. From the Novell Access Gateway Console screen, enter a ping command with the IP address of the Administration Console.
If the ping command successfully returns, continue with the following steps. If it is unsuccessful, fix the network communication problem before continuing.
- 4 From the Novell Access Gateway Console screen, enter the following two commands:

```
clear devicemanager serveraddress  
apply
```


These commands return you to the system console screen.
- 5 Press Ctrl+Escape and select the Novell Access Gateway Console screen.
- 6 To set the IP address, enter the following command:

```
set devicemanager serveraddress=<AC_address>
```


Replace <AC_address> with the address of the Administration Console.
- 7 When prompted, enter the name of the admin user.
- 8 Enter the password for the admin user and verify it.
- 9 To trigger the import process, enter

```
Apply
```


The system retries to import the device.
- 10 Wait 30 seconds, then log in to the Administration Console.
- 11 If these steps do not work, reinstall the device.

For the Linux Access Gateway

If the Administration Console is up and the ping command successfully returns, continue with the following steps. If it is unsuccessful, fix the network communication problem before continuing.

- 1 Verify if the Administration Console is up by logging into the Administration Console from a Web browser.
- 2 Verify that you can communicate with the Administration Console. From the command line of the Access Gateway machine, enter a ping command with the IP address of the Administration Console.

- 3 Log in as `root`.
- 4 Enter the following command:
`/chroot/lag/opt/novell/bin/lagconfigure.sh`
- 5 Specify the IP address of the Administration server.
- 6 Specify the username of the Access Manager administrator.
- 7 Specify the password of the Access Manager administrator.
- 8 Specify the password of the Access Manager again to reconfirm.
- 9 You are prompted to specify if you want to retain the current configuration or return to the initial configuration.
 - 9a Press *I* if you want to restore the initial values configured during the installation.
 - 9b Press *C* if you want to restore the current configuration of Access Gateway.
- 10 Wait 30 seconds, then log in to the Administration Console.
- 11 If these steps do not work, reinstall the device.

NOTE: If you are re-importing the Access Gateway, you must also do the following:

- ♦ Re-establish the trust between the embedded service provider and the Identity Server. For more information, see “[Configuring a Reverse Proxy](#)”, in the *Novell Access Manager 3.0 SP2 Administration Guide*.
 - ♦ If the Linux Access Gateway was part of a cluster, add it to the cluster. For more information, see “[Configuring a Cluster](#)” in the *Novell Access Manager 3.0 SP2 Setup Guide*.
 - ♦ Configure the certificate for SSL listener. For more information, see “[Configuring the Access Gateway for SSL](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.
-

A.1.3 Troubleshooting the Import Process

If a step in the import process does not complete successfully, the device does not show up in the Access Gateway list. The sections below describe the import process, where to find the log files, and how to use them to determine where the failure occurred so you can accurately report the problem.

- ♦ “[Understanding the Import Process](#)” on page 133
- ♦ “[Locating the Log Files](#)” on page 134
- ♦ “[Determining Where the Error Occurred](#)” on page 134

Understanding the Import Process

The following operations are performed during the import process:

1. A user specifies the IP address for the Administration Console during installation.
2. A Java process called “JCC” (Java Communication Channel) detects that the Administration Console IP address/port has changed between its own configuration in `SYS:\jcc\conf\settings.properties` and the CLI-updated settings in `SYS:\etc\proxy\ecc.cfg` on NetWare or `/opt/novell/devman/jcc/conf/settings.properties` and `/var/novell/cfgdb/.current/config.xml` on Linux.

3. An import message is sent to Administration Console notifying it of the IP, port, and ID of the Access Gateway device.
4. The Administration Console then connects to the Access Gateway device, asking for its configuration and version information. The Access Gateway portion of the import process is now complete.
5. As a separate asynchronous operation, the Access Gateway embedded service provider (ESP), running in Tomcat, connects and registers itself with the JCC.
6. When the ESP connects to the JCC, a similar import message is sent to the Administration Console notifying it to import into the system.
7. The Administration Console connects to the JCC, asking for the ESP configuration and version information. On the Administration Console, an LDIF (Lightweight Directory Interchange Format) file containing the default configuration for the ESP is applied on the local eDirectory™ configuration store.
8. The Administration Console then makes a link between the ESP and its configuration.
9. If the entire process completed properly, the Access Gateway device appears in the list of Access Gateways in the UI.

Locating the Log Files

Various Access Manager components produce log files. You use the following logs on either the Administration Console or the Access Gateway.

- ♦ **Administration Console Log:** /opt/novell/devman/share/logs/app_sc.0.log
- ♦ **Tomcat Log on the Administration Console:** /var/opt/novell/tomcat4/logs/catalina.out
- ♦ **JCC Log on the Access Gateway:** For the NetWare Access Gateway, the JCC events are logged to the SYS:\jcc\logs\jcc-0.log.0 file. They are also logged to the NetWare Logger Screen (screen #3).

For the Linux Access Gateway, the messages are logged in the /opt/novell/devman/jcc/logs/jcc-0.log.0 file.

Determining Where the Error Occurred

If the device does not show up in the list of Access Gateways in the UI after about 30 seconds, you can look for the following entries, determine which ones are not successful, and put the unsuccessful event messages in any bugs submitted.

- 1 From the Access Gateway console, verify the IP addresses.
 - ♦ On NetWare, unlock the console (see [Section A.1.4, “Unlocking the NetWare Access Gateway Console,” on page 138](#)). Enter `get devicemanager`. Verify that the *bindaddress* field is set to a bound address on the server. Verify that the *serveraddress* field is set to the correct address of the Administration Console.
 - ♦ On Linux, log in as `root`, start `nash`, and enter `show deviceManager`. Verify that the *bind-address* field is set to a bound address on the server. Verify that the *server-address* field is set to the correct address of the Administration Console.

2 Verify that the configuration file contains the correct information:

- ♦ On NetWare, verify that the `SYS:\etc\proxy\ecc.cfg` file contains the correct information set from the CLI. Open the `SYS:\jcc\conf\settings.properties` file and verify that the information matches that in `ecc.cfg` file:
- ♦ On Linux, verify that the `/var/novell/cfgdb/.current/config.xml` file contains the correct information set from the CLI. Open the `/opt/novell/devman/jcc/conf/lag-settings.properties` file and verify that the information matches that in the `config.xml` file.

3 In the JCC log, an entry for a successful Access Gateway import should look similar to the following:

```
Jan 30, 2006 3:19:34 PM com.novell.jcc.server.JCCServerImpl
register
INFO: Registering Proxy client "ag-AEF62A32"
com.novell.jcc.proxy.AGProxy$AGJCCClient@19113f8
Jan 30, 2006 3:19:34 PM com.novell.jcc.server.ClientRegistry
register
INFO: registering ag-AEF62A32 in client registry
Jan 30, 2006 3:19:34 PM com.novell.jcc.server.JCCServerImpl
processRegisterAlerts
INFO: Sending new device alert to Device Manager for ag-AEF62A32
Jan 30, 2006 3:19:34 PM com.novell.jcc.client.AlertDispatcher
sendAlert
INFO: alerts in send queue: 1
INFO: alert sent successfully
```

Look for an error message such as `sendAlert: IOException connection timed out`. This means the Access Gateway device could not connect to the Admin server. The operation will retry until it is successful. To trigger a retry, see [Section A.1.2, "Triggering an Import Retry," on page 132](#).

4 In the JCC log, an entry for a successful Access Gateway configuration import should look similar to the following:

```
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
handleRequest
INFO: This is a request from Device Manager.
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
proxyHttpURLConnection
INFO: Setting request method: GET for http://127.0.0.1:101
/Ex?Config:/appliance?Config:/appliance
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
proxyHttpURLConnection
INFO: Adding request headers:
X-Roma-Username: config.ics.ics_tree
X-Roma-Password:
X-Roma-Frequency: 0
X-Roma-Schedule-Id: 248237e8e9bc131da1bf7b23a1091ce91d43aa7c4a
X-Roma-Appliance-Id: ag-AEF62A32
Host: 10.155.164.14
X-Roma-Xml-Length: 0
Content-Length: 0
Pragma: no-cache
Cache-Control: max-age=0
X-Roma-Version: 1.0
```

```

User-Agent: Java1.3.0
Accept: text/html, text/plain, image/*, */*
Content-Type: text/plain
Connection: close
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
    proxyURLConnection
INFO: Connecting to http://127.0.0.1:101/Ex?Config:/appliance
    method GET
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
    proxyURLConnection
INFO: Response code: 200 OK
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
    proxyURLConnection
INFO: response body size: 5958 bytes
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
    proxyURLConnection
INFO: disconnecting client.

```

- 5** In the JCC log, a log entry for a successful ESP connection to the ESP should look similar to the following:

```

Jan 30, 2006 1:54:46 PM com.novell.jcc.client.JCCClientImpl <init>
INFO: Starting client esp-AEF62A32 of type idp
Jan 30, 2006 1:54:46 PM com.novell.jcc.sockets.CipherSocketUtils
    getKey
INFO: loading the secret key from /jcc/conf/jcc.keystore
Jan 30, 2006 1:54:47 PM com.novell.jcc.client.JCCClientImpl$
    ServerConnectionThread run
INFO: server connection thread started
Jan 30, 2006 1:54:47 PM com.novell.jcc.client.JCCClientImpl$
    ServerConnectionThread establishServerConnection
INFO: attempting to contact RMI server on 127.0.0.1:1197
INFO: Registering RMI client "idp-esp-AEF62A32" com.novell.jcc.
    client.JCCClientImpl$JCCRMIClient_Stub[RemoteStub [ref:
    [endpoint:[10.155.164.14:1029,com.novell.jcc.sockets.
    CipherSocketFactory@6a3960]remote),objID:[134ce4a:1091d189f37
    :-8000, 1]]]]
Jan 30, 2006 3:19:37 PM com.novell.jcc.server.ClientRegistry
    register
INFO: registering idp-esp-AEF62A32 in client registry
Jan 30, 2006 3:19:37 PM com.novell.jcc.server.JCCServerImpl
    processRegisterAlerts
INFO: Sending new device alert to Device Manager for
    idp-esp-AEF62A32
Jan 30, 2006 3:21:34 PM com.novell.jcc.client.AlertDispatcher$
    AlertQueueThreads
endAlert
INFO: alert sent successfully

```

- 6** In the JCC log, a successful logging of events for the ESP import should look similar to the following:

```

INFO: Sending new device alert to Device Manager for
    idp-esp-AEF62A32
Jan 30, 2006 3:21:34 PM com.novell.jcc.client.AlertDispatcher
    $AlertQueueThread sendAlert

```



```

INFO: alert sent successfully
Jan 30, 2006 3:21:34 PM com.novell.jcc.client.AlertDispatcher
    showAlert
INFO: alerts in send queue: 2INFO: Received GET: /Ex?Config:
    /appliance from 10.155.165.108:33812
Jan 30, 2006 3:21:34 PM com.novell.jcc.servlet.DispatchServlet
    dispatchHandler
INFO: looking up handler: Config
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.HandlerUtils
    verifyCredentials
INFO: login successful
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ConfigHandler
    handleRequest
INFO: <romaIDPConfiguration/>
Jan 30, 2006 3:21:34 PM com.novell.jcc.server.ClientRegistry
    setClientImported
INFO: setting client idp-esp-AEF62A32 as imported: true

```

- 7** When the LDIF file is successfully imported, the `app_sc.0.log` file contains an entry similar to the following. The example below contains an add entry for one schema definition; the ellipsis (...) indicates that the other definitions have not been included.

```

528(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
    (C)com.volera.vcdn.application.sc.alert.AlertCommandHandler$
    CommandThread(M)importDevice(Msg)Creating matching IDP server
    object for idp-esp-AEF62A32
529(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
    (C)com.volera.vcdn.application.sc.alert.AlertCommandHandler$
    CommandThread(M)importDevice(Msg)Successfully created
    cn=idp-esp-AEF62A32,cn=server,cn=nids,
    ou=accessManagerContainer,o=novell
530(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
    (C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
    $CommandThread(M)importDevice(Msg)
    dn: cn=SCCAEF62A32, cn=cluster, cn=nids,
    ou=accessManagerContainer,o=novell
    changetype: add
    nidsSignAuthnRequests: TRUE
    nidsIsConsumer: TRUE
    nidsSessionTimeout: 900
    nidsServerType: 3
    objectClass: nidsServerClusterConfiguration
    objectClass: Top
    nidsDisplayName: 10.155.164.14
    nidsServerConfigModified: FALSE
    nidsBaseURL: http://10.155.164.14/nidp
    nidsAssertionTimeToLive: 0
    cn: SCCAEF62A32
    nidsIsProvider: TRUE

```

[...]

```

531(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
    (C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
    (M)execute(Msg)Executing opt/novell/eDirectory/bin/ice

```

```

532(D)Mon Jan 30 15:21:37 MST 2006(L)System Controller(T)33
(C)com.volera.vcdn.application.sc.core.DeviceManager
(M)setHealthCheck(Msg)Setting the health attributes for nids
to: 1
533(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
(C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
(M)execute(Msg)Success, return code: 0

```

- 8** In the `app_sc.0.log` file, the record of a successful linking of the LDIF configuration to the ESP looks similar to the following:

```

534(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
(C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
$CommandThread(M)importDevice(Msg)S Searching for AEF62A32 in
cn=cluster,cn=nids,ou=accessManagerContainer,o=novell
535(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43(
C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
$CommandThread(M)importDevice(Msg)Checking configuration:
cn=SCCAEF62A32,cn=cluster,cn=nids,
ou=accessManagerContainer,o=novell with AEF62A32
536(D)Mon Jan 30 15:21:37 MST 2006(L)application.sc.alert(T)43
(C)com.volera.vcdn.application.sc.alert.AlertCommandHandler
$CommandThread(M)importDevice(Msg)Linking esp config to
cn=SCCAEF62A32,cn=cluster,cn=nids,
ou=accessManagerContainer,o=novell

```

A.1.4 Unlocking the NetWare Access Gateway Console

Before you can enter NetWare commands or view the logger screen, you must unlock the Novell Access Gateway Console.

- 1** To unlock the console, enter
unlock
- 2** When prompted for a password, press Enter.
The console is now unlocked and the active screen is the Access Gateway screen. From this screen you can enter device manager commands.
- 3** To switch to the logger screen or other NetWare screens, enter
debug
- 4** When prompted for a password, enter
proxydebug
- 5** To switch from the device manager screen, press Ctrl+Escape and enter the screen number.

A.2 Troubleshooting Linux Access Gateway Installation

This section contains the following troubleshooting scenarios for Linux Access Gateway:

- ♦ [Section A.2.1, “Some of the New Hardware Driver or Network Card are Not Detected During Manual or Advanced Installation,” on page 139](#)
- ♦ [Section A.2.2, “Manually Configuring a Network Interface,” on page 139](#)
- ♦ [Section A.2.3, “Manually Setting and Deleting the Default Gateway,” on page 140](#)

- ♦ [Section A.2.4, “Manually Configuring the Hostname, Domain Name and DNS Server,” on page 141](#)
- ♦ [Section A.2.5, “Troubleshooting Import Failure,” on page 142](#)

A.2.1 Some of the New Hardware Driver or Network Card are Not Detected During Manual or Advanced Installation

Sometimes, the advanced or manual installation of the Linux Access Gateway might fail if some of the hardware drivers or network cards are not detected. If this happens, you must upgrade the hardware drivers manually as follows:

- 1 Start the Manual installation of the Linux Access Gateway. See [Chapter 5, “Installing the Linux Access Gateway,” on page 35](#).
- 2 Select *Kernel Module (Hardware Driver)* in the Main Menu, then click *OK*.
- 3 Select *Add Driver Update*, then click *OK*.
- 4 Select the Driver Update Medium. The driver update medium can be CD-ROM or floppy disk. Click *OK*. The hardware driver is updated.
- 5 Continue with the Linux Access Gateway installation.

A.2.2 Manually Configuring a Network Interface

If you have configured a network interface during installation and it is not showing up, you can configure it manually through the command line interface (CLI) interface.

NOTE: If Linux Access Gateway is not imported, modifications to the Linux Access Gateway configuration should be done using `nash`. If the Linux Access Gateway is already imported, any modifications to the configuration should be done using the Administration Console.

Before you begin, make sure you have done the following:

- ♦ You have rebooted the system after installation.
- ♦ You have logged in as `root`.

- 1 At the command prompt, enter the following command:

```
nash
```

- 2 At the nash shell prompt, run the following command to enter the configuration mode:

```
configure .current
```

- 3 To display the current IP address for the `eth0` network card, enter the following:

```
show interface eth0
```

- 4 To change the IP address of `eth0`, enter the following:

```
interface eth0
```

- 5 To replace the IP address of `eth0`, enter the following command:

```
replace <current IP address> with <IP address/netmask>
```

Replace `<IP address/netmask>` with the IP address of the network interface card and the subnet mask. For example:

```
replace 10.0.0.1 with 12.1.1.1/23
```

IMPORTANT: Do not use the `interface eth0 no <ip_address>` command to remove the IP address. Always use the above command.

- 6** To return to the configuration mode, enter the following command:

```
exit
```

- 7** To save the configuration, enter the following command:

```
save .current
```

- 8** For the configuration to take effect, enter the following command:

```
apply
```

- 9** To exit from the configuration mode, enter the following command:

```
exit
```

- 10** To exit from the nash shell, enter the following command:

```
exit
```

A.2.3 Manually Setting and Deleting the Default Gateway

NOTE: If Linux Access Gateway is not imported, modifications to the Linux Access Gateway configuration should be done using nash. If the Linux Access Gateway is already imported, any modifications to the configuration should be done using the Administration Console.

- 1** Log in as `root`.

- 2** At the command prompt, enter the following shell command:

```
nash
```

- 3** At the nash shell prompt, run the following command to enter the configuration mode:

```
configure .current
```

- 4** To set up the default gateway IP address, enter the following command:

```
ip route 0.0.0.0/0 <gateway_IP_address> 1
```

Replace `<gateway_IP_address>`s with the IP address of your gateway server.

- 5** To delete the default gateway IP address, enter the following command:

```
no ip route 0.0.0.0/0 <gateway_IP_address> 1
```

Replace `<gateway_IP_address>` with the IP address of your gateway server.

- 6** To save the configuration, enter the following command:

```
save .current
```

- 7** For the configuration to take effect, enter the following command:

```
apply
```

- 8** To exit from the configuration mode, enter the following command:

```
exit
```

- 9** To exit from the nash shell, enter the following command:

```
exit
```

A.2.4 Manually Configuring the Hostname, Domain Name and DNS Server

- 1 At the command prompt, enter the following shell command:

```
nash
```

- 2 At the nash shell prompt, run the following command to enter the configuration mode:

```
configure .current
```

- 3 Configure the domain name and hostname.

- 3a To set up the domain name, enter the following command:

```
ip domain-name <domain_name>
```

Replace *<domain_name>* with the domain name for this network interface card.

- 3b To set up the hostname, enter the following command:

```
hostname <host_name>
```

Replace *<host_name>* with the hostname of the Linux Access Gateway machine.

- 3c If the hostname is not resolvable using an external DNS server, do the following to add the hostname and IP address mapping:

```
hosts <ip-address> <host_name>
```

```
hosts ip-address host-name.domainname
```

Replace *<ip_address>* with the IP address of this Access Gateway machine. Replace *<host_name>* with the computer name for this Access Gateway machine.

- 3d To set up the DNS server, enter the following command:

```
ip name-server <DNS_IP_address>
```

Replace *<DNS_IP_address>* with the IP address of your DNS server.

- 4 To save the configuration, enter the following command:

```
save .current
```

- 5 For the configuration to take effect, enter the following command:

```
apply
```

- 6 To exit from the configuration mode, enter the following command:

```
exit
```

- 7 To exit from the nash shell, enter the following command:

```
exit
```

- 8 You must exit from the bash shell for configuration changes to hostname, domain name and DNS server to take effect. To exit from the bash shell, enter the following command:

```
exit
```

- 9 Enter the following command to log in again:

```
root
```

- 10 To manually import the Linux Access Gateway to the Administration Console, enter the following command from the bash prompt:

```
/chroot/lag/opt/novell/bin/lagconfigure.sh
```

A.2.5 Troubleshooting Import Failure

There are several reasons for auto-import failure. The following sections list the causes and workarounds:

- ♦ “Manually Importing the Device to Administration Console” on page 142
- ♦ “Hostname Is Not Configured Properly” on page 142
- ♦ “Hostname Is Not Resolvable” on page 142
- ♦ “Some of the Components Failed to Install” on page 143

Manually Importing the Device to Administration Console

If the Linux Access Gateway failed to import during installation, follow the steps given below:

- 1 Log in as `root`.
- 2 Configure the network interface. For information on configuring the network interface, see [Section A.2.2, “Manually Configuring a Network Interface,” on page 139](#).
- 3 Configure the domain name and hostname. For information on configuring the hostname and domain name, see [Section A.2.4, “Manually Configuring the Hostname, Domain Name and DNS Server,” on page 141](#).
- 4 Configure the default gateway. For information on configuring the default gateway, see [Section A.2.3, “Manually Setting and Deleting the Default Gateway,” on page 140](#).

Hostname Is Not Configured Properly

If you have not configured the hostname properly, the following error messages are displayed:

- ♦ Hostname is not set. Please set the hostname in nash and run `/chroot/lag/opt/novell/bin/lagconfigure.sh` to trigger the configuration steps again.
- ♦ Default Hostname set. Please set the hostname in nash and run `/chroot/lag/opt/novell/bin/lagconfigure.sh` to trigger the configuration steps again.

To resolve the problem, manually configure the hostname. For information on how to manually configure hostname, see [Section A.2.4, “Manually Configuring the Hostname, Domain Name and DNS Server,” on page 141](#).

Hostname Is Not Resolvable

When hostname is not resolvable, the following error message is displayed:

```
Hostname cannot be resolved. Please set host entry in nash and run
/chroot/lag/opt/novell/bin/lagconfigure.sh to trigger the
configuration steps again.
```

To resolve the problem, manually configure the hostname. For information on how to manually configure hostname, see [Section A.2.4, “Manually Configuring the Hostname, Domain Name and DNS Server,” on page 141](#).

Some of the Components Failed to Install

- 1 Check the install logs at the following location:

```
/tmp/novell_access_manager
```

This directory has the install logs in the following format:

```
inst_component-name_date_time.log
```

For more information on collecting logs, see “[Linux Access Gateway Logs](#)” in the *Novell Access Manager 3.0 SP2 Administration Guide*.

- 2 Send the log to Novell Support.

A.3 Troubleshooting the SSL VPN Device Import

If you do not see the SSL VPN device after installation, follow the steps given below:

- 1 At command prompt, enter the following command:

```
sslvpc --configure
```

- 2 Enter the following configuration details:

- ♦ SSL VPN server IP address
- ♦ Administration Console IP address
- ♦ SSL VPN server internal interface name, such as eth0

- 3 At the command prompt, enter the following command:

```
/etc/init.d/novell-sslvpc start
```

The SSL VPN server is auto-imported into the Administration Console.

A.4 Troubleshooting the Administration Console Upgrade

If you see the following error message during the Administration Console upgrade:

```
Failed to load any MDB driver - Error: Could not load driver /usr/lib/mdb/mdbfile.so, error 9 - /usr/lib/mdb/mdbfile.so: cannot open shared object file: No such file or directory
```

The error is defined as: Running Novell Audit on Servers with More Than One IP Address. It occurs when the system attempts to upgrade the audit server. Systems with more than one IP address have problems running Novell Audit because multiple directory database (MDB) does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address using an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

Table A-1 *MDB Configuration File*

Platform	Directory
NetWare	sys:\etc\mdb.cfg
Linux	/etc/mdb.conf

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameter: `driver=mdbds referral=eDirectory_IP_Address`. For example, `driver=mdbds referral=10.10.123.45`.

You might only have one IP address, but your server might have two network adapters. If you create the `/etc/mdb.conf` file and specify your IP address and then the upgrade, you do not encounter this error message.