AUTHORIZED DOCUMENTATION

Installation Guide

Novell® Access Manager

3.1 SP1

April 08, 2010

www.novell.com

Legal Notices

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

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

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

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).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

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

For information about the J2EE* Agents and the SSL VPN server, see the following guides:

- *Novell Access Manager 3.1 SP1 Agent Guide*
- *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*

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).

Additional Documentation

- *Novell Access Manager 3.1 SP1 Setup Guide*
- *Novell Access Manager 3.1 SP1 Administration Console Guide*
- *Novell Access Manager 3.1 SP1 Identity Server Guide*
- *Novell Access Manager 3.1 SP1 Access Gateway Guide*
- *Novell Access Manager 3.1 SP1 Policy Management Guide*
- *Novell Access Manager 3.1 SP1 Agent Guide*
- *Novell Access Manager 3.1 SP1 SSL VPN Server 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.

What's New in Access Manager 3.1 SP1

1

Novell® Access Manager 3.1 SP1 provides a number of key enhancements to various components. These enhancements improve management, enhance security, and add cross-platform capabilities to major components. These key features include:

1.1 Identity Server Enhancements

- **Session Failover:** If you have a cluster of two or more Identity Servers, you can configure the Identity Servers so that the user experiences no interruption of services when the Identity Server that created the user's session goes offline. For configuration information, see "Configuring Session Failover" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.
- **Session-Based Logging:** This feature allows the administrator to enable file logging for an individual user. All of the user's interaction with the Identity Server and the embedded service provider are logged to a single file, which can be used to analyze the cause of the user's problem. For configuration information, see "Configuring Session-Based Logging" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*
- **ORing of Contacts:** You can now let the user select an authentication method from a list of methods. You do this by ORing two or three contracts together. You can OR the name/password, X.509, and RADIUS contracts together. For configuration information, see "Creating an ORed Credential Class" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.
- **Non-Redirected Login:** For applications that use basic authentication to reauthenticate users before they can access specific resources or for their own session timeouts, you can configure the Identity Server to verify this type of authentication without using a redirect (which is unsupported by these types of applications). This allows for better integration with Microsoft* SharePoint* and Microsoft Outlook* Web Access. For configuration information, see "Modifying Authentication Procedures" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- **Security Configuration for 128-bit Authentication:** You can now force all client communication to use 128-bit encryption when communicating with the Identity Server. For configuration information, see "Forcing 128-Bit Encryption" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.
- **Reusing Modified 3.0 Login JSP Pages:** Changes were made in Access Manager 3.1 to simplify the JSPs that need to be created by authentication class developers. These changes have made JSPs used in version 3.0 incompatible with version 3.1. Additional changes have been made so that modified 3.0 JSP pages can be manually converted so that they work with

Access Manager 3.1 SP1. For information about the modifications you need to make, see "Customizing the Identity Server Login Page" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

- **Active Directory Account Checks:** The Identity Server now checks for user account errors from Active Directory* user stores and can display appropriate messages for wrong username or password, expired passwords, intruder lockout, and account disabled.

1.2 Access Gateway Enhancements

- **Support for Novell Teaming and Conferencing:** Linux Access Gateway can now accelerate Novell Teaming and Conferencing servers. For more information, see "Configuring a Protected Resource for a Novell Teaming 2.0 Server" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- **Better Integration with Microsoft SharePoint Servers and Outlook Web Access:** Linux Access Gateway now comes with better integration with Microsoft* SharePoint Server and Outlook Web Access. For more information, see "Configuring the Access Gateway to Protect Web Resources" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- **Faster File Uploads:** The file uploads are two times faster than the previous releases of Linux Access Gateway.
- **Support for iChain Cookie:** Linux Access Gateway now provides support for iChain cookies with the help of a touch file. This touch file forwards a proxy session cookie to a back-end application. For more information, see "Useful Files for Troubleshooting the Access Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- **Disable Caching Option:** This option allows you to globally disable caching so that the Access Gateway also retrieves fresh content from the Web server. For configuration information, see "Configuring Caching Options" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- **Proxy Settings:** These options for secure cookies and the Via header, which were formerly available as touch files, can now be configured from the Administration Console for all Access Gateways. See "Creating a Reverse Proxy and Proxy Service" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.

1.3 SSL VPN Enhancements

- **Enable Full Tunneling:** With this release, SSL VPN supports full tunneling of traffic in both Enterprise as well as Kiosk mode running on Windows* and Linux* platforms. When you configure SSL VPN for full tunneling, all traffic to the protected network as well as the public network passes through the tunnel, thereby making the SSL VPN connection more secure. But any session management information between the client and the Identity Server or the Linux Access Gateway (in the case of traditional SSL VPN) and the SSL VPN server is exchanged outside the SSL VPN tunnel. You can configure full tunneling for both Kiosk mode and Enterprise mode SSL VPN. For more information, see, "Configuring Full Tunneling" in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.
- **Disconnecting Active SSL VPN Connections:** The Administration Console now contains options that allow you to disconnect SSL VPN users. You can either disconnect one user at a time or select and delete multiple users. For more information, see "Disconnecting Active SSL VPN Connections" in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.

- **UI Option to Configure SNAT Entry:** You can now configure the source NAT (SNAT) entries through the Administration Console to change the dynamically assigned client addresses to the address of the SSL VPN server before sending them to the application server. For more information, see "Configuring SNAT for Enterprise Mode" in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*
- **Configuration File to Add Additional Enterprise Mode Configurations:** SSL VPN has many extended configuration options for both the SSL VPN Enterprise client and the Enterprise server that can be saved and executed from a configuration file. For more information, see "Creating a Configuration File to Add Additional Configuration Changes" in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.

1.4 J2EE Agent Enhancements

- **Cluster Support on All Application Servers:** With this release, you can cluster the WebLogic* J2EE* agent, thus providing the ability to cluster J2EE agents on the JBoss*, WebSphere*, and WebLogic Application server. You can also cluster multiple instances of J2EE agents residing on a single WebSphere server.
- **Authentication Contract per Resource:** The Novell J2EE Agent now comes with the ability to configure different authentication contracts to protect different applications that reside on the same application server instance. You can also configure additional authentication contracts for applications that require them. For more information, see "Configuring Authentication Contract" in the *Novell Access Manager 3.1 SP1 Agent Guide*.

Novell Access Manager Product Overview

2

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:

2.1 How Access Manager Solves Business Challenges

As networks expand to connect people and businesses throughout the world, secure access to business resources becomes increasingly more important and more complex. Gone are the days when all employees worked from the same office; today's employees work from corporate, home, and mobile offices. Equally gone are the days when employees were the only ones who required access to resources on your network; today, customers and partners require access to resources on your network, and your employees require access to resources on partners' networks or at service providers.

Novell ®Access Manager lets you provide employees, customers, and partners with secure access to your network resources, whether those resources are Web applications, traditional server-based applications, or other content. If your business faces any of the following access-related challenges, Access Manager can help:

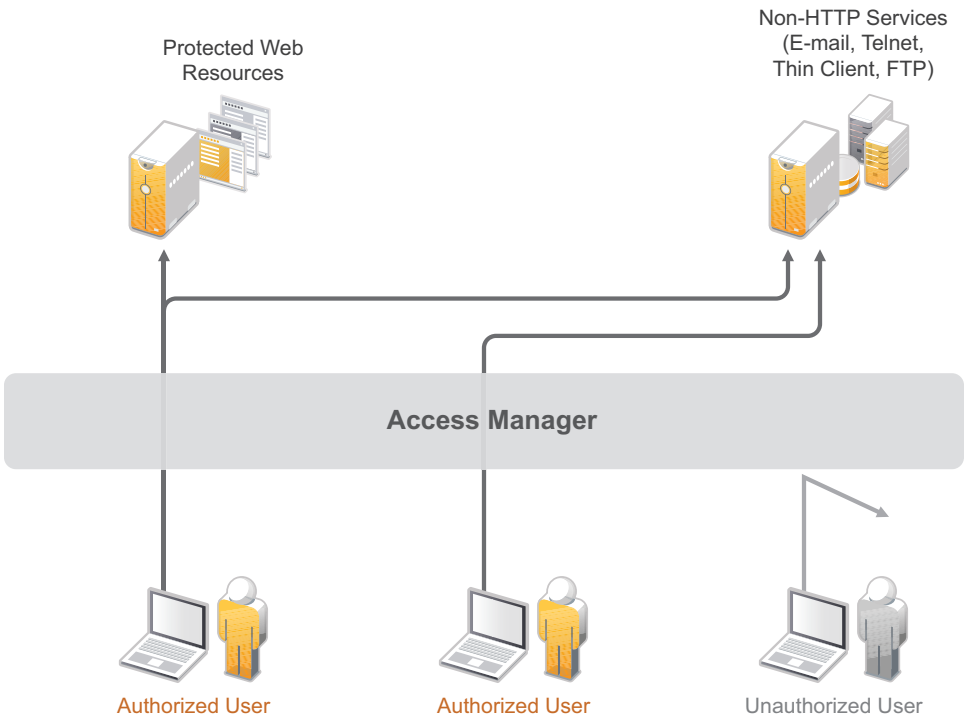
- Protecting resources so that only authorized users can access them, whether those users are employees, customers, or partners.
- Ensuring that the users who are authorized to use a resource can access that resource regardless of where the users are currently located.
- Requiring users to manage multiple passwords for authentication to Web applications.
- Making sure users have access only to the resources required for their jobs. In other words, ensuring that your authorization processes and practices match the business policies that define access privileges to your network resources.
- Revoking network access from users in minutes rather than days.

- Protecting users' privacy and confidential information as they access company resources or partners' resources.
- Proving compliance with your business policies, privacy laws such as Sarbanes-Oxley, HIPPA, or European Union, and other regulatory requirements.

The following sections expand on these challenges and introduce the solutions provided by Access Manager. If you are already aware of the business solutions provided by Access Manager, you might want to skip to the technical introduction provided in Section 2.2, "How Access Manager Works," on page 23.

2.1.1 Protecting Resources While Providing Access

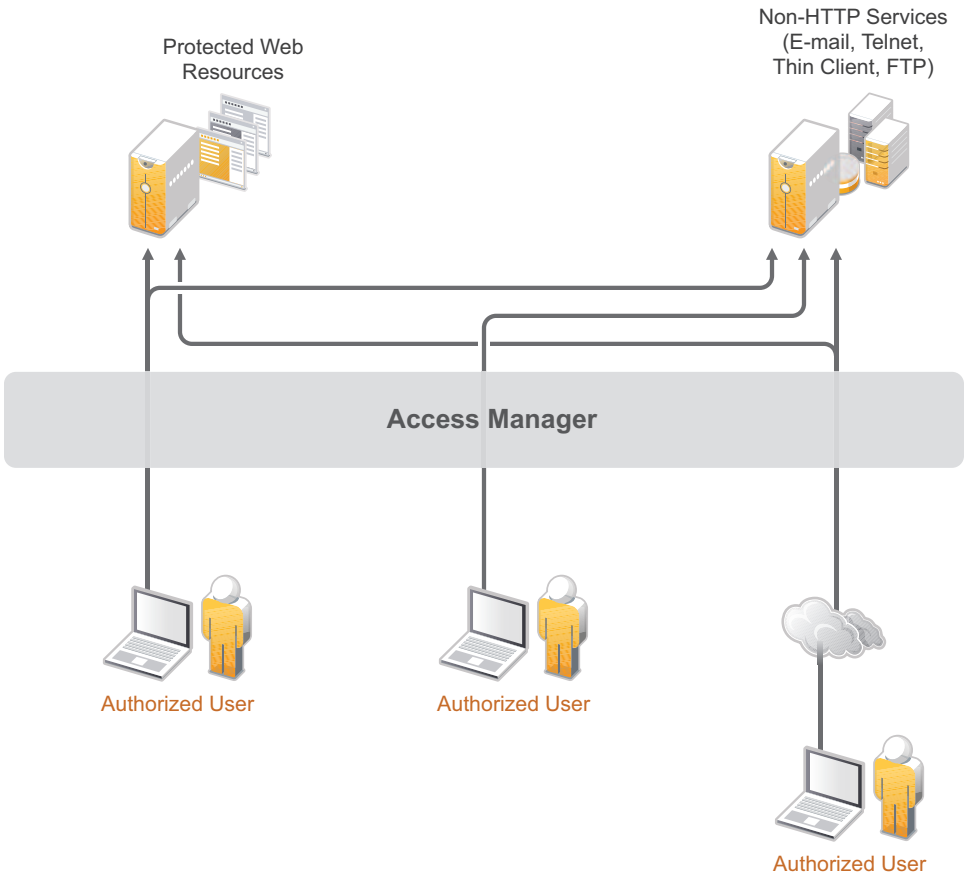
The primary purpose of Access Manager is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources as well as traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized to use the protected resources are allowed access, while unauthorized users are denied access.



Access Manager secures your protected Web resources from Internet hackers. The addresses of the servers that host the protected resources are hidden from both external and internal users. The only way to access the resources is by logging in to Access Manager with authorized credentials.

Access Manager protects only the resources you have set up as protected resources. It is not a firewall and should always be used in conjunction with a firewall product.

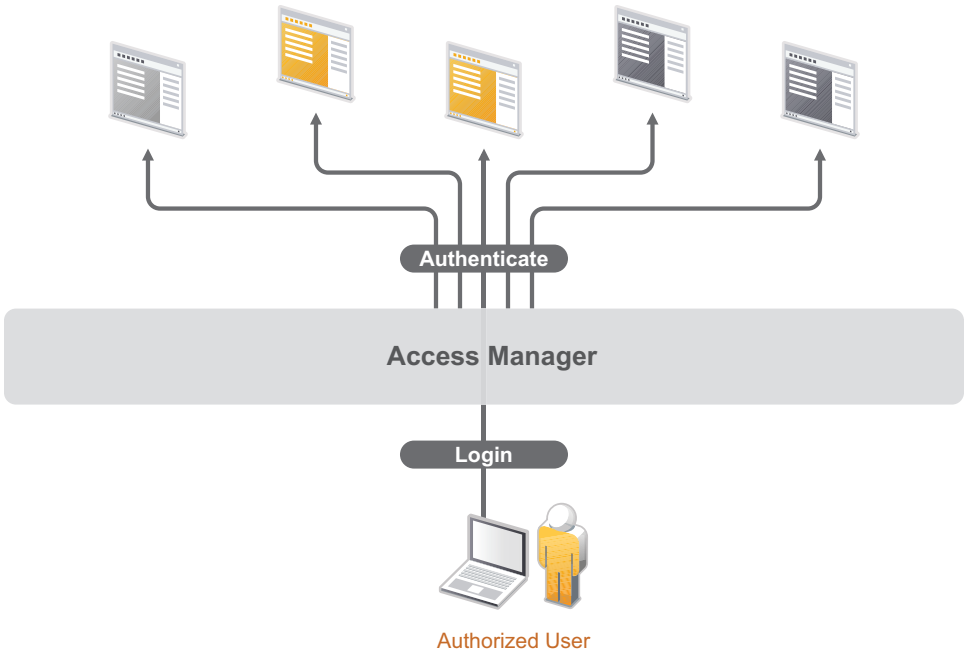
Because not all users work from within the confines of your local network, access to resources is independent of a user's location, as shown in the following illustration. Access Manager provides the same secure access and same experience whether the user is accessing resources from your local office, from home, or from an airport terminal.



2.1.2 Managing Passwords with Single Sign-On

If your organization is like most, you have multiple applications that require user login. Multiple logins typically equates to multiple passwords. And multiple passwords means forgotten passwords.

Authentication through Access Manager not only establishes authorization to applications (see Protecting Resources While Providing Access above), but it can also provide authentication to those same applications. With Access Manager serving as the front-end authentication, you can deploy standards-based Web single sign-on, which means your employees, partners, and customers only have to remember one password or login routine to access all the corporate and Web-based applications they are authorized to use. That means far fewer helpdesk calls—and the reduced likelihood of users resorting to vulnerable written reminders.

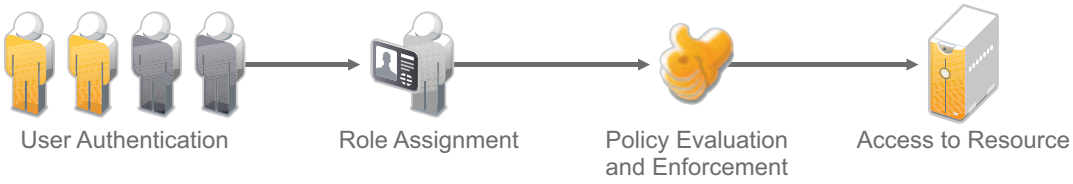


By simplifying the use and management of passwords, Access Manager helps you enhance the user's experience, increase security, streamline business processes, and reduce system administration and support costs.

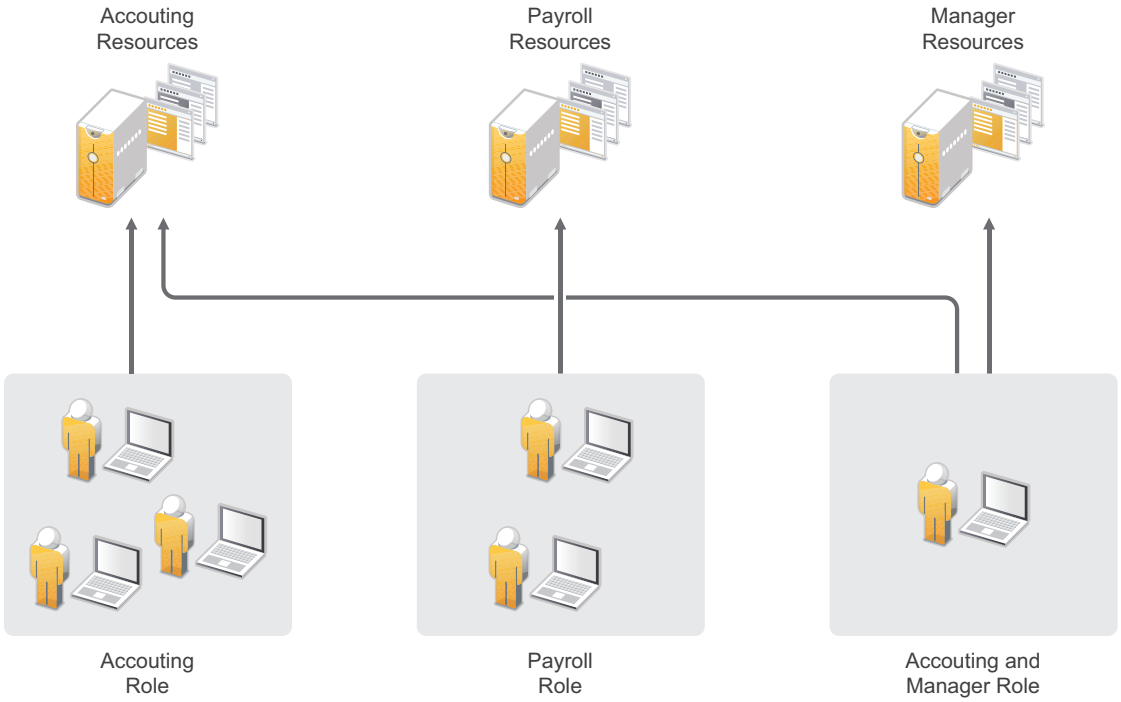
2.1.3 Enforcing Business Policies

Determining the access policies for an organization is often complicated and difficult, but the difficulty pales in comparison to enforcing the policies. Your IT personnel can spend hours attempting to give users the correct access to resources, and hours more retracing their steps to see why the users can't access what they should be able to. What's worse, you might never know about the situations where users are granted access to resources they shouldn't be accessing.

Access Manager automates the granting and removing of access through the use of roles and policies. As shown in the following illustration, users are assigned to roles that have access policies associated with them. Each time a user authenticates through Access Manager, the user's access is determined by the policies associated with the user's roles.



In the following example, users assigned to the Accounting role receive access to the Accounting resources, Payroll users receive access to the Payroll resources, and Accounting managers receive access to both the Accounting and Manager resources.



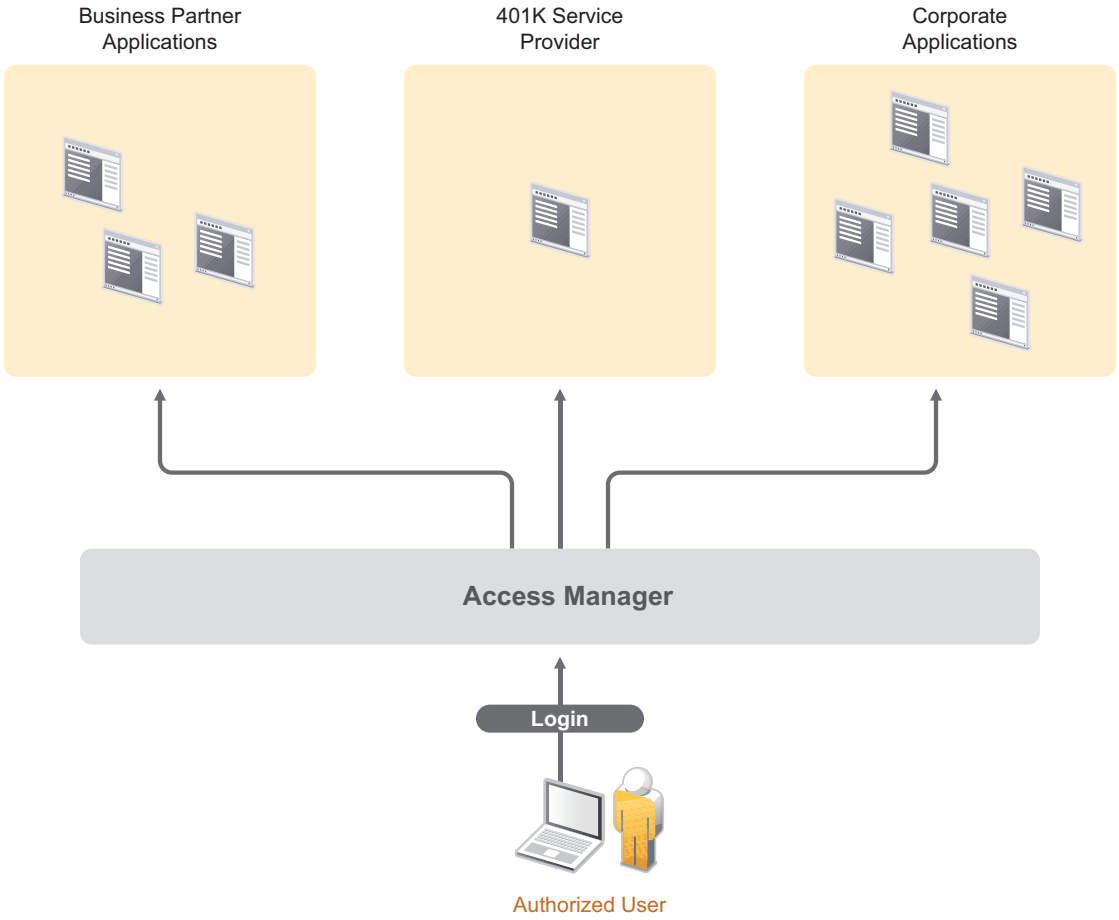
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

For security-minded organizations, it comes down to this simple fact: you set the policies by which users gain access, and Access Manager enforces them consistently and quickly. There are no surprises and no delays.

2.1.4 Sharing Identity Information

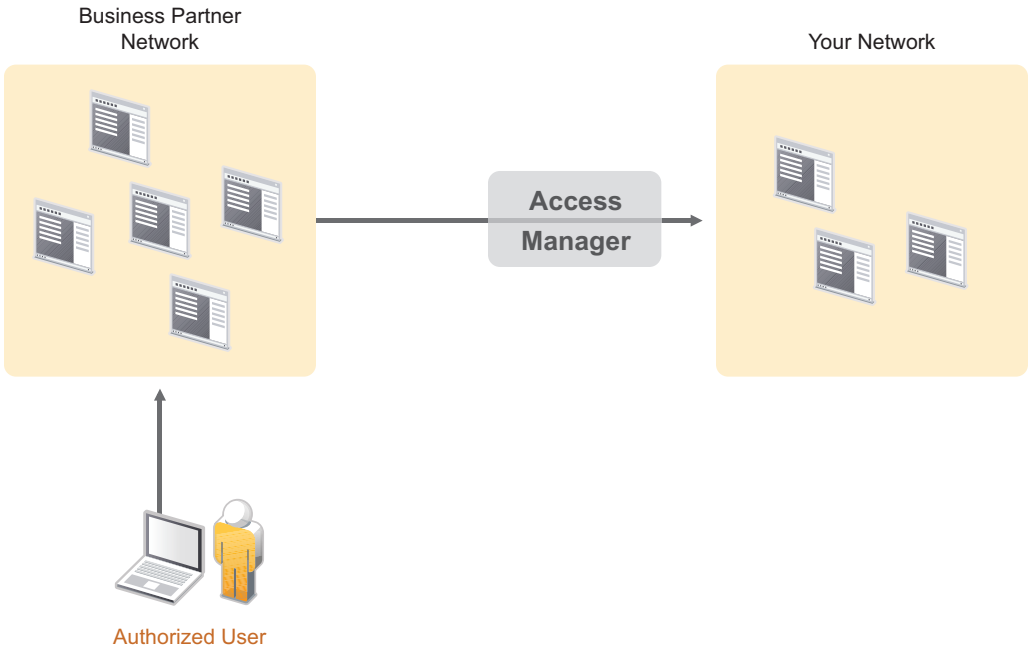
In today's business environment, few organizations stand alone. More than likely, you have trusted business partners with whom you need to shared resources in a secure manner. Or, you have business services, such as a 401k management system, to which you need to provide employee access. Or, maybe your organization is the one providing services to another business. Access Manager provides federated identity management to enable users to seamlessly and securely authenticate across autonomous identity domains.

For example, assume that you have employees who need access to your corporate applications, several business partner's applications, and their 401k service, as shown in the following figure.



Each identity domain (your organization, your partner's organization, and the 401k service) requires an account and authentication to that account in order to access the resources. However, because you've used Access Manager to establish a trust relationship with the business partner and the 401k service, your employees can log in through Access Manager to gain access to the authorized resources in all three identity domains.

But Access Manager not only enables your employees to access resources from business partners and service providers, it also lets business partners access authorized resources on your network as if the resources were part of their own network. Or, if you are a service provider, the same is true for your customers. The following figure illustrates this type of access.



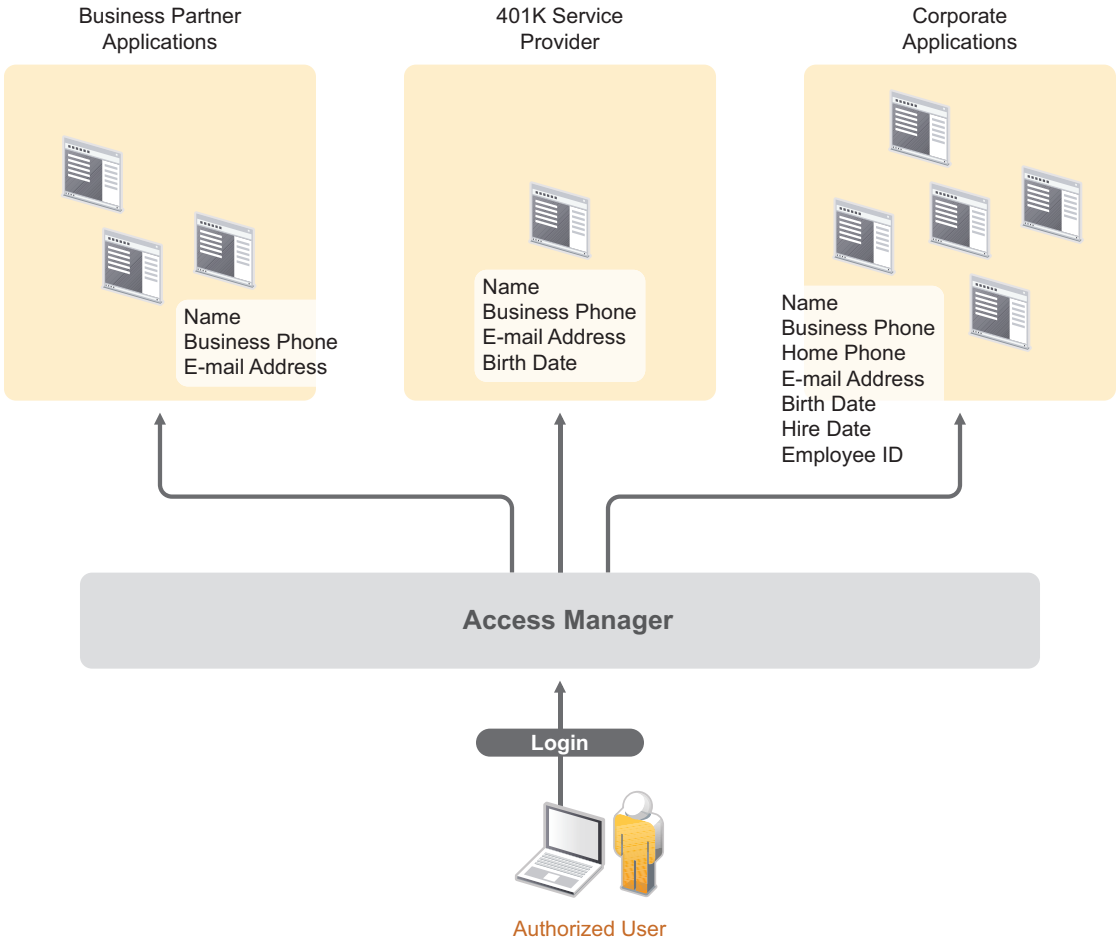
In addition to simply linking user accounts in different identity domains, Access Manager also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partners (or providers) systems. For example, a new employee in your organization can initiate the creation of an account in your business partner's system through Access Manager rather than relying on the business partner to provide the account. Or, customers or trusted business partners can automatically create accounts in your system.

Access Manager leverages identity federation standards, including Liberty Alliance, WS-Security and SAML. This foundation minimizes—or even eliminates—interoperability issues among external partners or internal workgroups. In fact, Access Manager features an identical configuration process for all federation partners, whether they are different departments within your organization or external business partners.

2.1.5 Protecting Identity Information

Whenever you exchange identity information with other businesses or service providers, you must be concerned with protecting the privacy of your employees, customers, and partners. In fact, it's an integral part of trusted business partnerships and regulatory compliance: the ability to establish policies on the exchange of identity information.

For example, Access Manager enables you to determine which business and personal information from your corporate directory is shared with others. As shown in the following illustration, you can choose to share only the information required to establish the account at the service provider or trusted partner.



Access Manager offers this built-in privacy protection for your employees, partners, and customers alike, wherever they are working. With Access Manager in place, your organization can guarantee user confidentiality. And for federated provisioning, Access Manager adheres to those same policies and protections.

2.1.6 Complying with Regulations

Regulations can be a hassle, but an agile, automated IT infrastructure substantially cuts costs and reduces the pain of compliance. By implementing access based on user identities, you can protect users' privacy and confidential information. At the same time, you can reduce the amount of paperwork needed to prove that proper access control measures are in place. Compliance assurance and documentation is an inherent benefit of Access Manager.

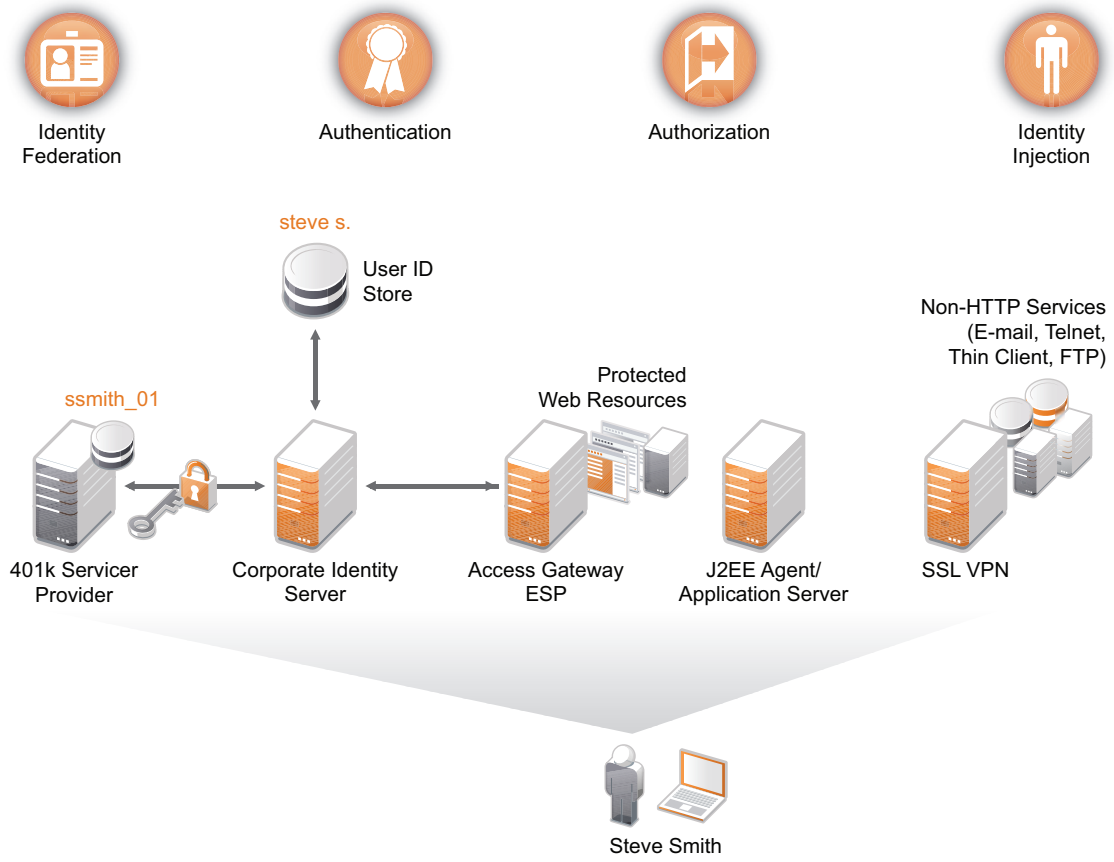
Specifically, Access Manager helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager can generate the reports you need, turning compliance requirements into opportunities to develop and implement processes that improve your business practices.

2.2 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.

Figure 2-1 illustrates the primary purposes of Access Manager: authentication, identity federation, authorization, and identity injection.

Figure 2-1 *Access Manager*



2.2.1 Authentication

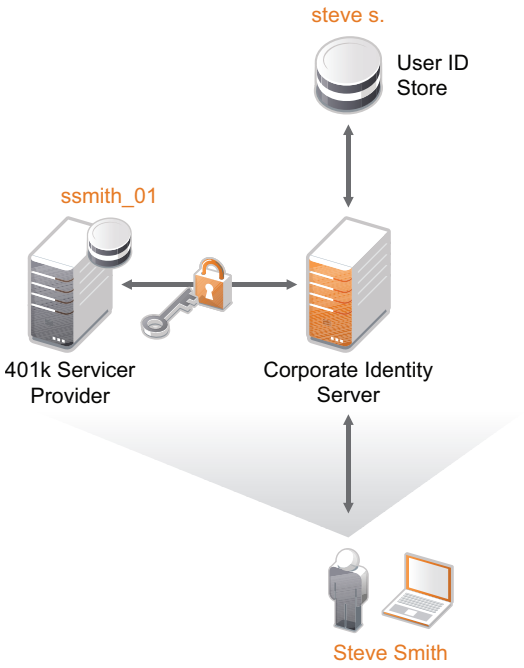
The Identity Server facilitates authentication for all Access Manager components. This authentication is shared with internal or external service providers on behalf of the user, by means of assertions. Access Manager supports a number of authentication methods, such as name/password, RADIUS token-based 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.

2.2.2 Identity Federation

Identity federation is the association of accounts between an identity provider and a service provider. As shown in Figure 2-2, 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 2-2 *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.

2.2.3 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.

2.2.4 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.

2.3 Access Manager Components and Their Features

This section describes the following Access Manager features:

2.3.1 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 2-3 *Novell Access Manager Dashboard 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.

2.3.2 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.

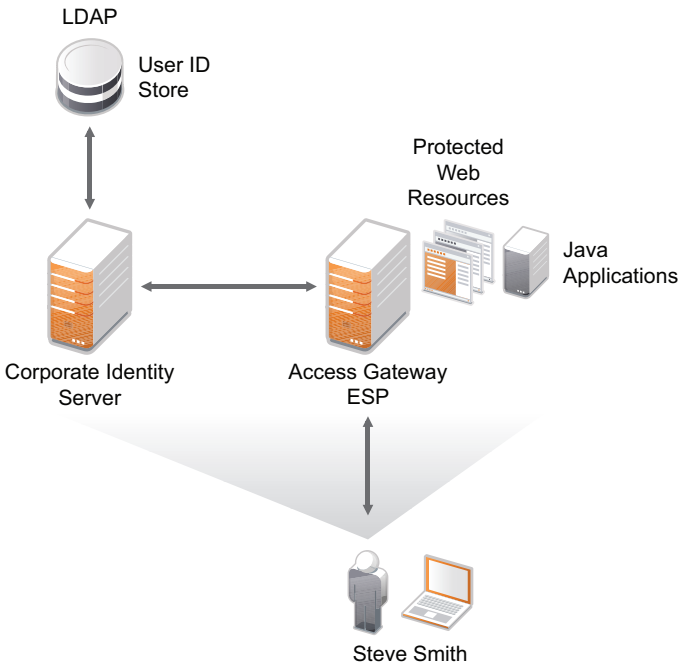
- **Custom Attribute Mapping:** Allows you to define custom attributes by mapping Liberty Alliance keywords to LDAP-accessible data, in addition to the available Liberty Alliance Employee and Person profiles.
- **SAML Assertions:** Processes and generates SAML assertions. Using SAML assertions in each 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 3.1 SP1 Identity Server Guide*.

2.3.3 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 2-4 *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.

The Access Gateway is a soft appliance, which simplifies installation and configuration. For more information, see the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.

2.3.4 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 accelerated by (and shares session information with) the Access Gateway if installed in the Access Gateway protected mode. Novell SSL VPN can also be installed in the standalone mode without 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.

2.3.5 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*, WebLogic*, 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) and Java Authorization Contract for Containers (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.

2.3.6 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.

2.3.7 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 (`.pfx`), or 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.

2.3.8 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.

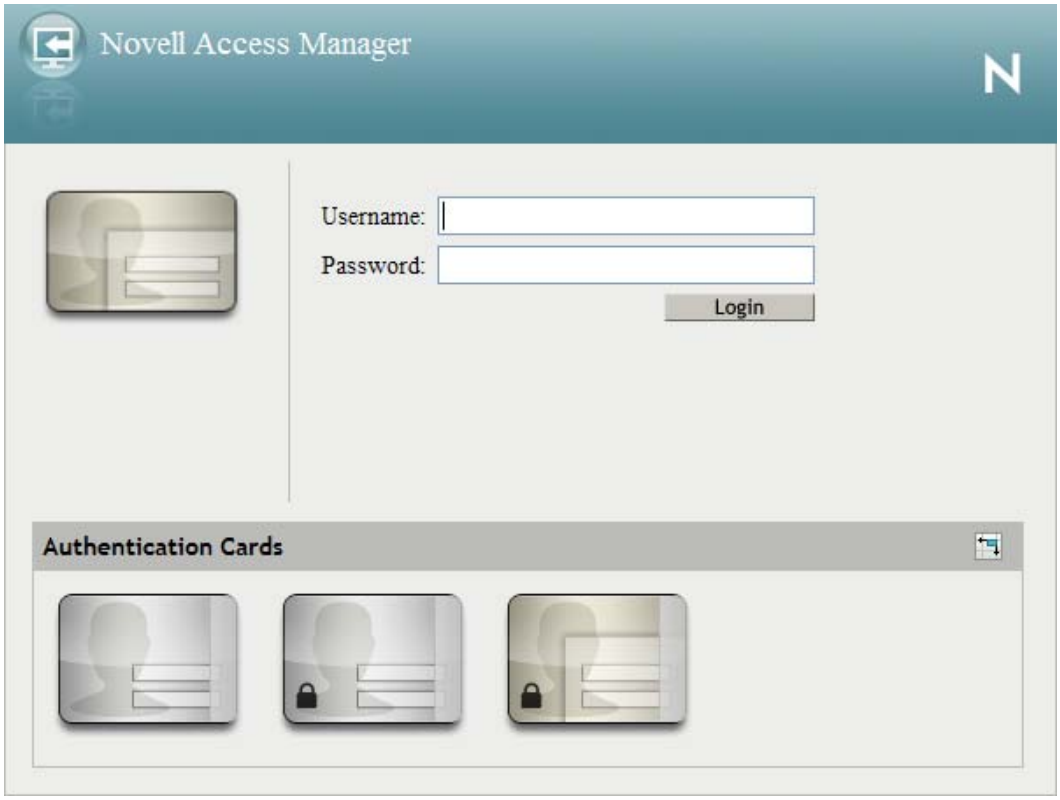
2.3.9 Embedded Service Provider

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.

2.3.10 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 2-5 *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.

2.3.11 Language Support

The Access Manager software for installation and administration uses English and is not localized. The Administration Console is also not localized and uses only English. However, the client pieces of Access Manager are either localized or allow you to create custom pages.

- The User Portal, which appears when the user logs directly into the Identity Server, is localized and so is its help file.
- The SSL VPN client, which displays when the user establishes an SSL VPN session, is also localized.

The User Portal and the SSL VPN client are localized for German, French, Spanish, Italian, Japanese, Portuguese, Dutch, Chinese (Simplified), and Chinese (Traditional). The language must be set in the client's browser to display a language other than English.

The Access Gateway and Identity Server, which can send messages to users when an error occurs, allow you to customize the error pages, but you are responsible for supplying the content of the customized pages. For information on customizing these pages, see the following:

- For the Linux Access Gateway Appliance, see "Customizing Error Pages on the Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- For the Identity Server, see "Customizing Identity Server Messages" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

Installation Requirements

3

This section explains the requirements for installing the Novell® Access Manager. 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).

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:

For information about the J2EE Agents and the SSL VPN server, see the following guides:

- *Novell Access Manager 3.1 SP1 Agent Guide*
- *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*

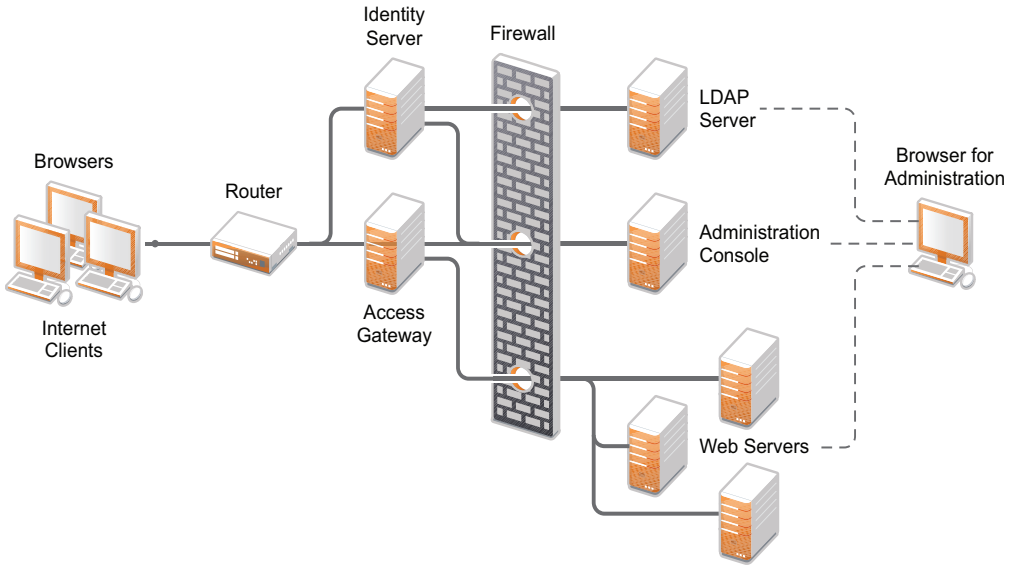
3.1 Recommended Installation Scenarios

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

3.1.1 Basic Setup

For a basic Access Manager installation, you can install the Identity Server and the Access Gateway outside your firewall. Figure 3-1 illustrates this scenario:

Figure 3-1 *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 3.1 SP1 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.

   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 3.1 SP1 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 3.1 SP1 Setup Guide*.

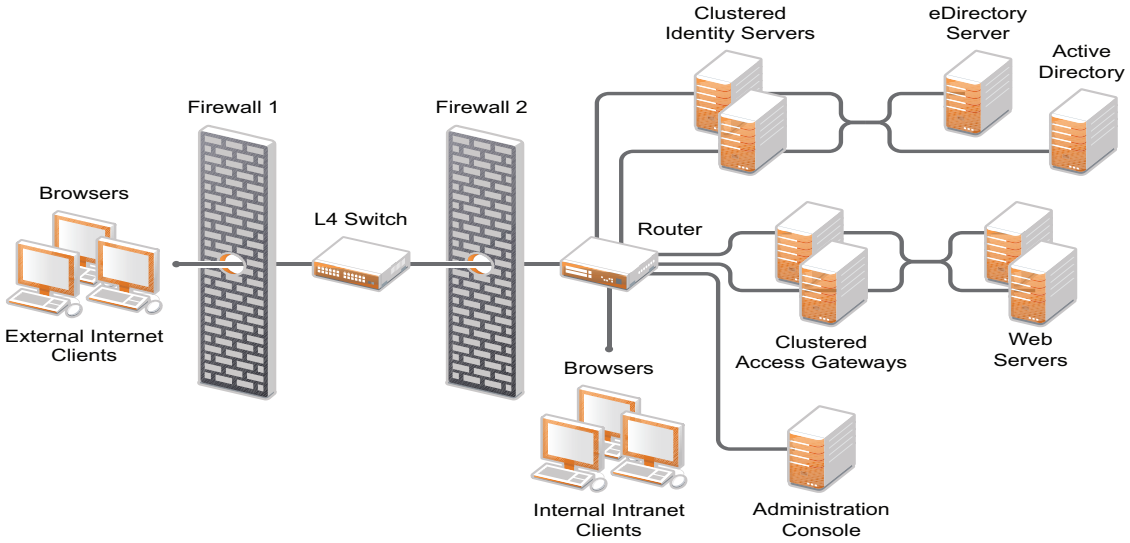
For information about setting up configurations for fault tolerance and clustering, see "Clustering and Fault Tolerance" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

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.

3.1.2 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 3-2 illustrates this type of network.

Figure 3-2 *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 3.1 SP1 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 3.1 SP1 Setup Guide*.

3.2 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) 10 or later. For the Linux Access Gateway, you should select a platform supported by SLES 9.

For the Windows components (Identity Server and Administration Console), you should select a platform supported by Windows Server 2003.

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

3.3 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 lookups 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.

  If you are using a load balancer to communicate with the Identity Servers and the Access Gateways, the load balancer can enable NATing to make sure that all requests continue to go back thru the load balancer and not directly between the devices.

3.4 Administration Console Requirements

The Access Manager Administration Console, which you install on Linux or Windows, 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.

3.4.1 Linux Requirements

The Access Manager Administration Console has the same hardware requirements as the SLES operating system with one exception. The Administration Console requires a minimum of 2 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 SP2 or 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 (LUM) machine.
- ❑ 2 GB RAM minimum requirement.
- ❑ 2.0 GHz processor or better
- ❑ 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.
- ❑ 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.
  - compat-libstdc++ (SLES 10) or compat-libstdc++-lsb (SLES 9): A required library for the configuration database.

  Use the following command to verify:

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

  Use YaST to install the packages.
- ❑ On a minimal install of SLES 10, make sure the following packages (with their dependent packages) are installed before installing the Administration Console. A graphical user interface library is required for the installation of iManager.
  - gtk (version 1.2.10).
  - gtk2 (version 2.8.10 or later).
  - gtk2-32bit (version 2.8.10 or later). Required for a 64-bit installation.

  Use the following command to verify:

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

  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.
- ❑ Ports 389 and 636 need to be free.
- ❑ 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.

3.4.2 Windows Requirements

- Windows 2003 Server 32-bit operating system, in either Standard or Enterprise Edition, with SP2
- 2.0 GHz processor or better
- 2.0 GB RAM minimum requirement
- 100 GB hard drive, dedicated

  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).
- Static IP address
- No LDAP software, such as eDirectory, can be installed.
- Ports 389 and 636 need to be free.
- No other version of iManager can be installed.
- Microsoft Internet Information Service cannot run on the same machine as the Administration Console without causing port conflicts.
- No JRE installed. If you have a version installed, remove it, install the Administration Console, then reinstall it.

3.4.3 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 on Windows* XP
- Internet Explorer 7 (latest version) on Windows XP and Vista
- Firefox* 2 and 3 (latest version) on Windows and Linux

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 43.

3.5 Identity Server Requirements

The Identity Server is the second component you install. It can be installed on Linux or Windows:

- Section 3.5.1, “Linux Requirements,” on page 39
- Section 3.5.2, “Windows Requirements,” on page 39

Clients, when authenticating directly to the Identity Server, can use any browser or operating system.

3.5.1 Linux Requirements

The Linux machine requires the following hardware and software:

- ❑ 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).
- ❑ 3 GB RAM recommended with 2 GB as the minimum
- ❑ 3.0 GHz processor or better
- ❑ SLES 10 SP2 or 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
- ❑ Configure SLES for a static IP address.
- ❑ No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP.)

For installation instructions, see Chapter 5, “Installing the Novell Identity Server,” on page 53.

3.5.2 Windows Requirements

The Windows machine requires the following software and hardware:

- ❑ Windows 2003 Server 32-bit operating system, in either Standard or Enterprise Edition, with SP2
- ❑ 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).
- ❑ 3 GB RAM recommended with 2 GB as the minimum
- ❑ 3.0 GHz processor or better

3.6 Access Gateway Requirements

The Access Gateway requires the following hardware:

- ❑ 100 GB of disk space recommended, with 30 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.
- ❑ Supports x86-32 and x86-64 hardware, but runs in 32-bit mode.

Clients, when accessing resources protected by the Access Gateway, can use any browser or operating system.

3.6.1 Linux Appliance Network Requirements

The Linux Appliance runs on SLES 9 SP3. You install it on a separate machine because it clears the hard drive and sets up a soft appliance environment.

The Linux Appliance has no software requirements. The installation program re-images the hard drive, embeds the Linux operating system, then configures the embedded operating system for optimal performance.

Before proceeding with the 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 6, “Installing the Linux Access Gateway Appliance,” on page 57.

3.7 Virtual Machine Requirements

The virtual 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 3.4, “Administration Console Requirements,” on page 36
- Section 3.5, “Identity Server Requirements,” on page 39
- Section 3.6, “Access Gateway Requirements,” on page 40

The following virtual machines are supported:

- VMware* ESX Server version 3.5 and higher
- "Xen Virtualization - SUSE Linux Enterprise Server 10 SP2 or later

The following sections contain some installation tips:

- Section 3.7.1, “Keeping Time Synchronized on the Access Manager Devices,” on page 41
- Section 3.7.2, “Graphical Install for the Linux Access Gateway Appliance,” on page 41

3.7.1 Keeping Time Synchronized on the Access Manager Devices

Even when the devices are configured to use a network time protocol server, time does not stay synchronized because the devices periodically lose their connection to the NTP server. The easiest solution is to configure the Administration Console to use an NTP server and have the other devices use a cron job to synchronize their time with the Administration Console.

Add the following command to the `/etc/crontab` file of the device:

```
*/5 * * * *     root  /usr/sbin/ntpdate -u 10.20.30.108 >/dev/null 2>&1
```

Replace 10.20.30.108 with the IP address of your Administration Console.

3.7.2 Graphical Install for the Linux Access Gateway Appliance

To perform a graphical install:

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

   The boot screen appears.

2 Add the following command to the *Boot Options* line:

```
x11i=fbdev
```

3 Select the type of install.

For installation instructions, see Chapter 6, “Installing the Linux Access Gateway Appliance,” on page 57.

Installing the Access Manager Administration Console

4

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.

For information about installing a secondary Administration Console and fault tolerance, see “Installing Secondary Versions of the Administration Console” in the *Novell Access Manager 3.1 SP1 Setup Guide*.

4.1 Installation Procedures

Installation time: about 20 minutes.

What you need to create	A username and password to use for the Access Manager administrator.

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

4.1.1 Installing on Linux

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 3.4, “Administration Console Requirements,” on page 36.
3. Open a terminal window.
4. Log in as the `root` user.
5. Access the install script. For software download instructions, see the “Novell Access Manager Readme” (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html).

   Select one of the following:

   - 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.

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

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

6 At the command prompt, enter the following:

```
./install.sh
```

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

8 (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 the static IP address here: _____

9 (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.

10 Review and accept the License Agreement.

11 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.

12 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: _____

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.

Record the admin password here: _____

14 Confirm the password, then wait as the system installs the components.

This can take several minutes, depending upon the speed of your hardware. Be patient.

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 3.1 SP1 Administration Console 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 "Configuring Identity User Stores" in the *Novell Access Manager 3.1 SP1 Identity Server 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 3.1 SP1 Administration Console 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.

15 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.

16 Continue with Section 4.2, "Configuring the Administration Console Firewall," on page 47.

4.1.2 Installing on Windows

1 Verify that the machine meets the minimum requirements. See Section 3.4, "Administration Console Requirements," on page 36.

2 Close any running applications and disable any virus scanning programs.

3 (Conditional) To use a remote desktop for installation, you must use VNC.

You cannot use MS Remote Desktop from a Windows machine or the rdesktop application from a Linux machine.

4 Download the file and execute it.

For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html).

5 Read the introduction, then click *Next*.

6 Accept the license agreement, then click *Next*.

7 Select *Novell Access Manager Administration Console*, then click *Next*.

If you are also installing the Identity Server on this machine, you can also select *Novell Identity Server*.

8 Specify whether this is the primary Administration Console in a failover group, then click *Next*.

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.

9 Specify the following information:

Administration user ID: Specify a name for the user account to use for logging into the Administration Console.

Password and Re-enter Password: Specify a password and re-enter the password for the administration user account.

Server IP Address: Specify the static IP address of the machine.

10 Click *Next*, then review the summary.

11 To start the install, click *Install*.

The configuration database takes awhile to install and configure. Be patient.

12 (Optional) View the install log file found in the following location:

```
C:\Program Files\Novell\log\AccessManagerServer_InstallLog.log
```

13 Reboot the machine.

IMPORTANT: You must restart the machine before installing any other Access Manager components.

14 In a terminal window, run the `auditext.exe` utility.

14a Change to the `C:\Program Files\Novell\NSure Audit` directory.

The `.lsc` file required when executing the `auditext.exe` utility is located in the `C:\Program Files\Novell\Nsure Audit\LogSchema\nids_en.lsc` directory.

14b Enter the following command:

```
auditext -lsc -u:<admin> -p:<novell> -a:Novell Access Manager -
f:c:\Program Files\Novell\Nsure Audit\LogSchema\\nids_en.lsc -l:en
```

Modify the following variables to match your system:

Variable	Description
-u:<*admin*>	This is the name of the administrator for the Administration Console. Replace <*admin*> with the name of your administrator
-p:<*novell*>	This is the password for the administrator. Replace <*novell*> with the password of your administrator.

For more information about this utility, see "AuditExt" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/all8rgt.html).

15 Continue with Section 4.2, "Configuring the Administration Console Firewall," on page 47.

4.2 Configuring the Administration Console Firewall

Before you can import the Access Manager components into the Administration Console, or before you can log in to the Administration Console from a client machine, you must first configure the firewall on the Administration Console.

4.2.1 Linux Administration Console

1. Click *Computer* > *YaST* > *Security and Users* > *Firewall*.

   This launches the Firewall Configuration screen.
2. Click *Allowed Services* > *Advanced*.
3. In the *TCP Ports* field, enter the following ports to open:
   - 8080
   - 8443
4. (Conditional) If you are importing the Access Gateway into the Administration Console, list the following additional ports in the *TCP Ports* field:
   - 1443
   - 8444
   - 289
   - 524
   - 636

   If you are importing a Linux Access Gateway, enter `icmp` in the *IP Protocols* field.

   For specific information about the ports listed in Step 3 and Step 4, see "When a Firewall Separates the Administration Console from a Component" in the *Novell Access Manager 3.1 SP1 Setup Guide*.
5. Click *OK*.
6. Click *Next* > *Accept*.
7. Restart Tomcat by entering `/etc/init.d/novell-tomcat5 restart` from the Administration Console command line.
8. Continue with Section 4.3, "Logging In to the Administration Console," on page 48.

4.2.2 Windows Administration Console

1. Click *Control Panel* > *Windows Firewall*.
2. Click *Advanced*, then for the Local Area Connection, click *Settings*.
3. For each port that needs to be opened, click *Add*, then fill in the following fields:

   Description of service: Specify a name, for example Admin Console Access for port 8080 or Secure Admin Console Access for port 8443.

   Name or IP address: Specify the IP address of the Administration Console

External Port number for this service: Specify the port in the box.

Open the following ports:

- 8080
- 8443

4 (Conditional) If you are importing the Access Gateway into the Administration Console, add the following ports:

- 1443
- 8444
- 289
- 524
- 636

For specific information about the ports listed in Step 3 and Step 4, see "When a Firewall Separates the Administration Console from a Component" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

5 (Conditional) If you are importing a Linux Access Gateway, click *ICMP*, select all options, then click *OK* twice.

6 Enter the following commands to restart Tomcat:

```
net stop Tomcat5
net start Tomcat5
```

7 Continue with Section 4.3, "Logging In to the Administration Console," on page 48:

4.3 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 through 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. For information on how to do this, see Section 4.2, “Configuring the Administration Console Firewall,” on page 47.

   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.

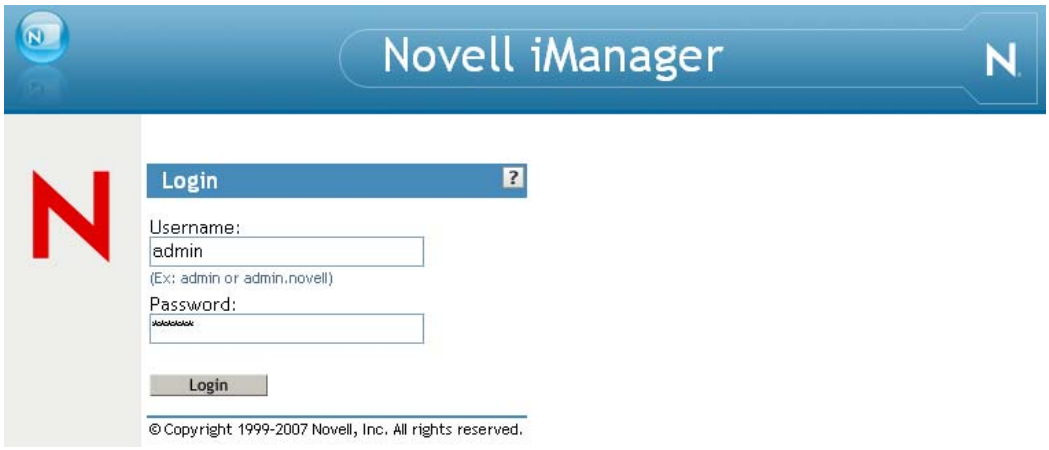
   Use the IP address established when you installed the Administration Console. It should include the port 8080 and the application nps. If the IP address of your Administration Console is 10.10.10.50, you would enter the following:

   ```
   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.



6 Click *Login*, and the following view appears.

This is the new view for Access Manager 3.1. For more information about this view or about configuring to the Administration Console for the 3.0 view, see "Configuring the Default View" in the *Novell Access Manager 3.1 SP1 Administration Console Guide*.

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 other Access Manager component: an Access Gateway, SSL VPN server, or a J2EE Agent. It is recommended that you next install the Identity Server. See Chapter 5, "Installing the Novell Identity Server," on page 53.

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

4.4 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 `server.xml` file:

1. Open the `server.xml` file found in the following directory.

   Linux: `/var/opt/novell/tomcat5/conf`

   Windows: `\Program Files\Novell\Tomcat\conf`
2. Locate the connector with the `NIDP_Name="connector"` set.
3. Delete the `address` attribute.
4. Save the file.

4.5 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

5

Installation time: about 10 minutes.

What you need to know	◆ Username and password of the Access Manager administrator. ◆ (Conditional) IP address of the Administration Console if it is installed on a separate machine.

5.1 Prerequisites

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 43.) However, you must not perform any configuration tasks in the Administration Console during an Identity Server installation.
- If you installed 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 the following ports are open on both the Administration Console and the Identity Server:

  8444
  1443
  289
  524
  636

  For information on how to open ports, see Section 4.2, “Configuring the Administration Console Firewall,” on page 47.
- 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.
- Verify that the machine meets the minimum requirements. See Section 3.5, “Identity Server Requirements,” on page 39.

5.2 Installing on Linux

1. Open a terminal window.
2. Log in as the `root` user.
3. Access the install script. For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html)

   Select one of the following:

   - 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/dvdrecorder`, depending on your hardware.
   - If you downloaded the `tar.gz` file, unpack the file using the following command:

     ```
     tar -xzvf <filename>
     ```
4. At the command prompt, run the following install script:

   ```
   ./install.sh
   ```
5. 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.
6. 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.
7. Review and accept the License Agreement.
8. 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.
9. Specify the name of the administrator for the Administration Console.
10. Specify the password of the administrator.
11. Confirm the password, then wait as the system installs the components. (This will take several minutes.)

    If the installation program rejects the credentials and IP address, ensure that the correct ports are open on both the Administration Console and the Identity Server, as described in Section 5.1, "Prerequisites," on page 53.

    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.

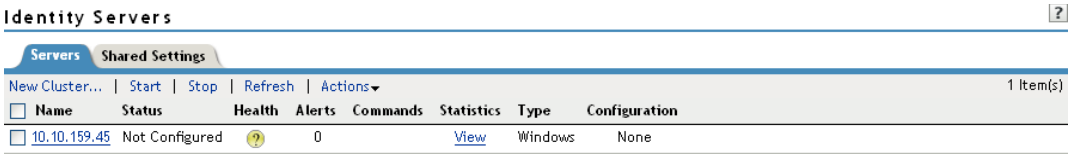
      If the installation process terminates at this step, the probable cause is a failure to communicate with the Administration Console. Ensure that you entered the correct IP address.

- **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.

12 (Optional) To verify that the Identity Server installation was successful, log in to the Administration Console (see Section 4.3, "Logging In to the Administration Console," on page 48), then click *Devices* > *Identity Server*s.

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:



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.

13 Continue with one of the following:

- To install an Access Gateway, see Chapter 6, "Installing the Linux Access Gateway Appliance," on page 57.
- To configure the Identity Server, see "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

5.3 Installing on Windows

1 Verify that the machine meets the minimum requirements. See Section 3.5, "Identity Server Requirements," on page 39.

2 Close any running applications and disable any virus scanning programs.

3 (Conditional) If you have installed the Administration Console on this machine, make sure you have rebooted the machine before installing the Identity Server.

4 Download the file and execute it.

For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html).

5 Read the introduction, then click *Next*.

6 Accept the license agreement, then click *Next*.

7 Select *Novell Identity Server*, then click *Next*.

8 Specify the following information:

Administration user ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.

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

9 Click *Next*, then review the summary.

10 To start the install, click *Install*.

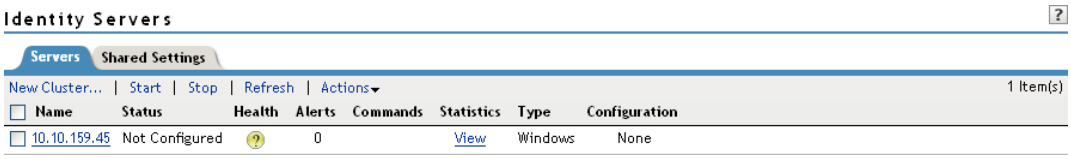
11 (Conditional) If you are installing the Identity Server on a machine that contains a previous installation of the Administration Console, you are asked whether the program should overwrite an existing file in the `\Program Files\Novell` directory. Answer yes to the prompt.

12 (Optional) View the install log file found in the following location:

```
C:\Program Files\Novell\log\AccessManagerServer_InstallLog.log
```

13 (Optional) To verify that the Identity Server installation was successful, log in to the Administration Console (see Section 4.3, "Logging In to the Administration Console," on page 48), then click *Devices* > *Identity Server*s.

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:



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 6, "Installing the Linux Access Gateway Appliance," on page 57.
- To configure the Identity Server, see "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

Installing the Linux Access Gateway Appliance

6

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

You have the following options for installing the Linux Appliance, 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 6.3, “Using a Standard Linux Installation with the Default Settings,” on page 58.
- **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 6.4, “Using the Advanced Installation Option,” on page 64.
- **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 Appliance can be installed on all SUSE® Linux Enterprise Server (SLES) 9 SP 3 supported hardware platforms.

IMPORTANT: After you have completed installing the Linux Access Gateway appliance, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities. For more information on upgrading the kernel, see Section 7.6.5, “Installing or Updating the Latest Linux Patches,” on page 99.

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

6.1 Prerequisites for the Linux Appliance

- ❑ Ensure that you have backed up all data and software on the disk to another machine. The Linux Appliance installation completely erases all the data on your hard disk.
- ❑ Make sure the machine meets the minimum hardware requirements. See Section 3.6, “Access Gateway Requirements,” on page 40.
- ❑ An Administration Console must be installed before you can install the Linux Appliance. See “Installing the Access Manager Administration Console” on page 43.

- ❑ If a firewall separates the Linux Appliance and the Administration Console:
  - Ensure that the required ports are opened. See "When a Firewall Separates the Administration Console from a Component" in the *Novell Access Manager 3.1 SP1 Setup Guide*.
  - To import the Linux Appliance into the Administration Console, you must open the ICMP protocol. For information on how to do this, see Section 4.2, "Configuring the Administration Console Firewall," on page 47.

6.2 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, such as 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.

6.3 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. Partitions are created with the following default specifications:

- **/boot:** The size is automatically calculated and the mount point is `/boot`.
- **swap:** Double the size of RAM and mount point is `swap`.

The remaining disk space after the creation of /boot and swap partition is allocated as the extended drive. The extended drive has the following partitions:

- **root:** The default size is one-third the size of extended drive and the mount point is `/`.
- **var:** The default size is one-third the size of the extended drive and the mount point is `/var`.
- **COS:** This partition is created with the remaining free space on the extended drive.

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 Appliance 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 6.2, “Boot Screen Function Keys,” on page 58.

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.

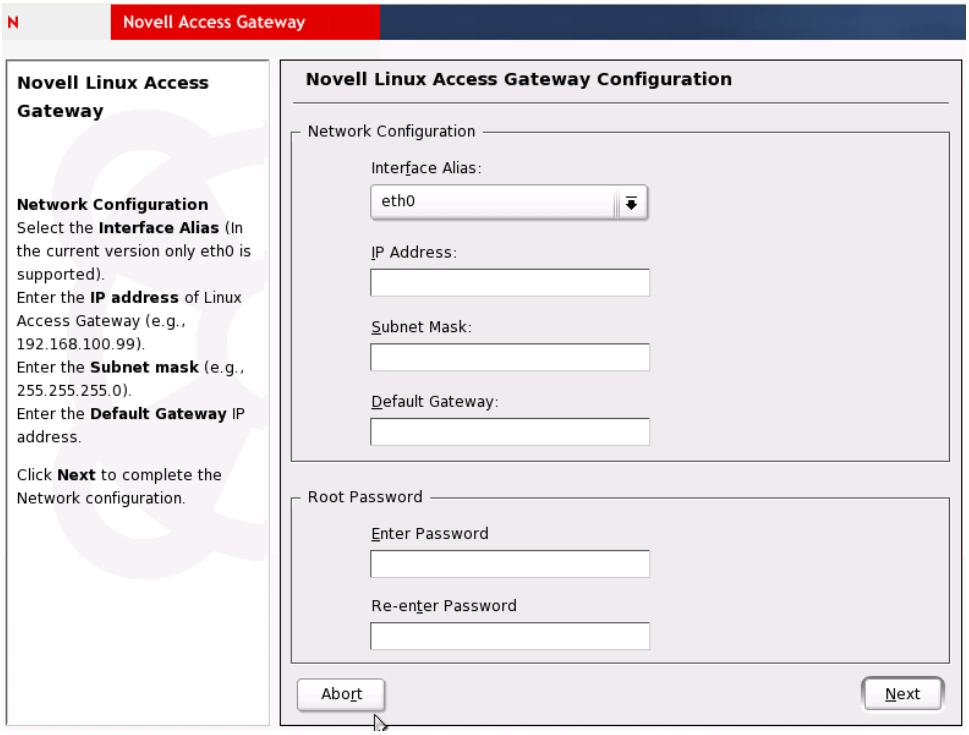
6 Select *English (US)* on the Language Selection page, then click *Accept*.

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.



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.2.3, “Manually Configuring a Network Interface,” on page 155.

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

Subnet Mask: Specify the subnet mask of the Linux Appliance network.

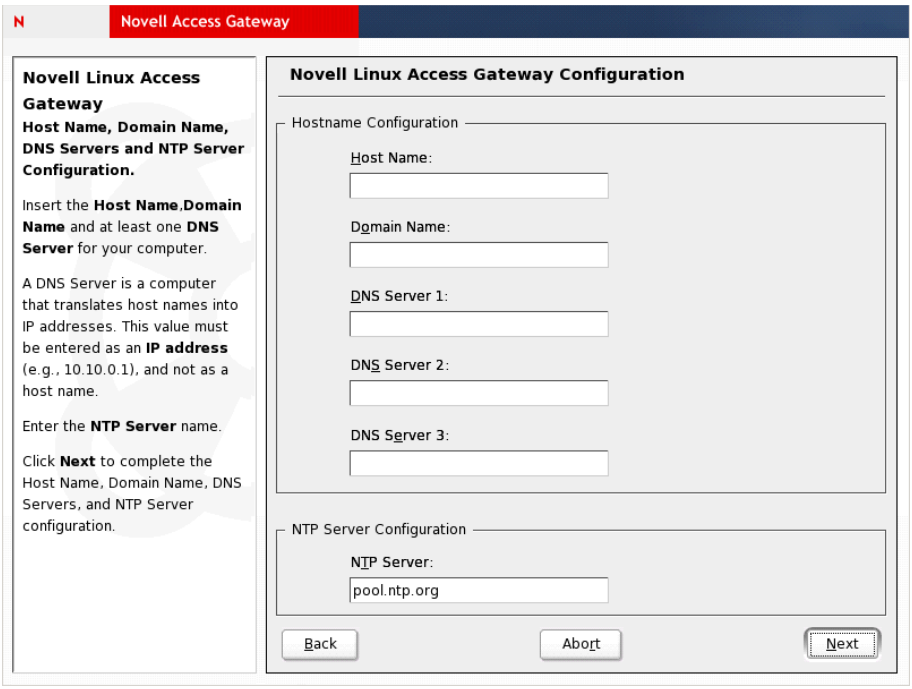
Default Gateway: Specify the default gateway.

9 Enter and re-enter a password for the root user. Make sure that the password contains more than 5 but fewer than 8 characters. The password must be a combination of alphanumeric characters and symbols.

NOTE: If you specify a password that is more than 8 characters, it is truncated to 8 characters only.

---

10 Click *Next*. The *Hostname Configuration* section appears.



Configure the following:

Host Name: Specify the hostname for the Linux Appliance machine.

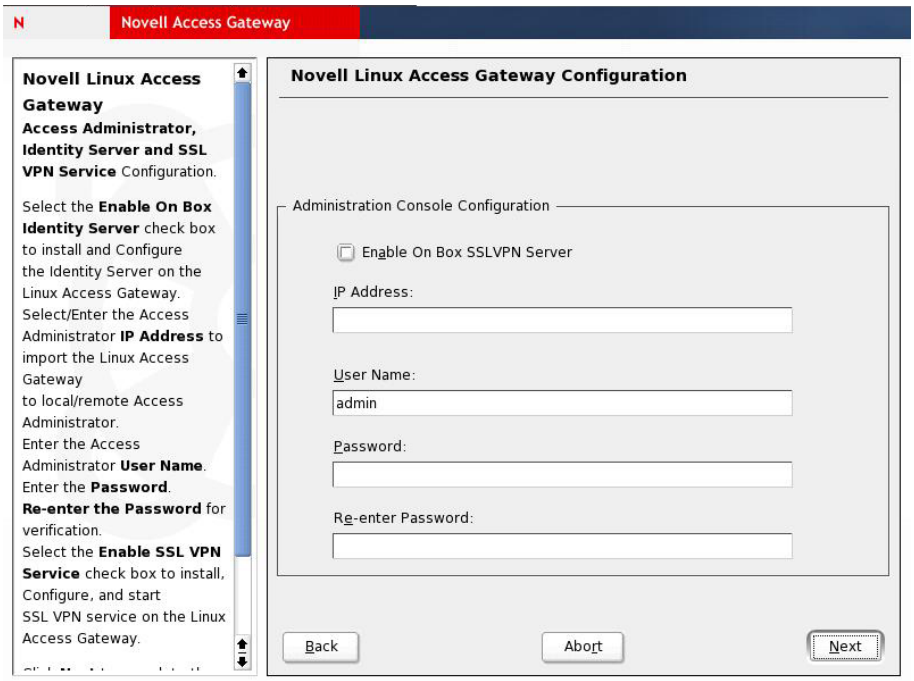
Do not use linux as the hostname. If you do, the Linux Access Gateway is not imported.

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.

11 Click *Next*. The *Administration Console Configuration* section appears.



Configure the following:

Enable On Box SSL VPN Server: Select this check box to install and configure the SSL VPN service on the Linux Appliance. When the SSL VPN server is installed on the same box as the Access Gateway, the SSL VPN server must be configured as a protected resource of the Access Gateway.

IMPORTANT: The SSL VPN Server cannot be uninstalled without uninstalling the Linux Appliance.

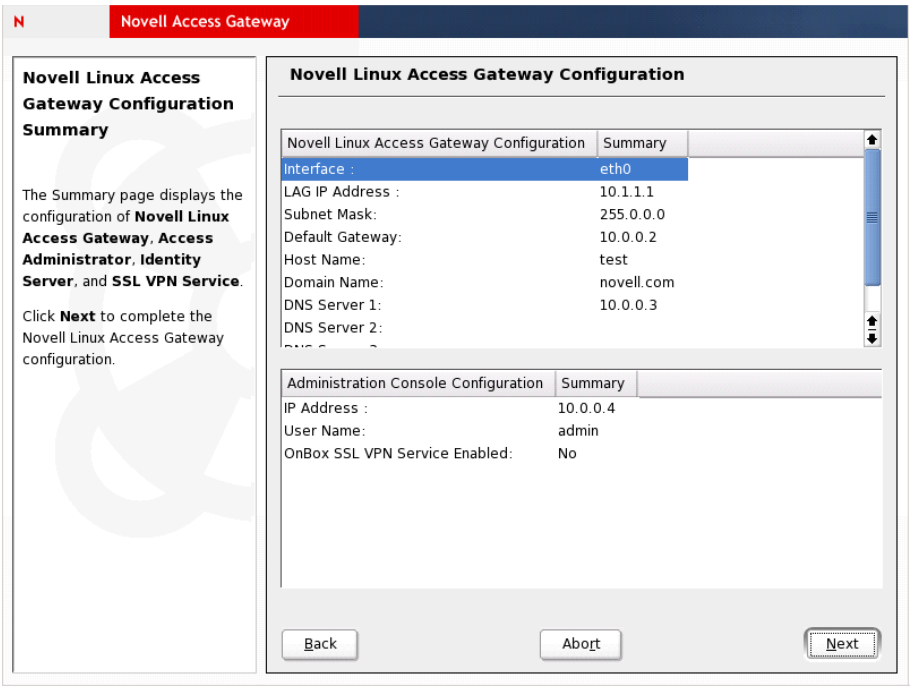
IP Address: Specify the IP address of the Administration Console. The Linux Appliance is imported into this Administration Console. If you have selected the *Enable on Box SSL VPN Server* option, the SSL VPN is imported into this Administration Console.

Username: Specify the name of the Administration Console user.

Password: Specify the password for the user.

Reenter Password: Re-enter the password for verification.

12 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*.

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

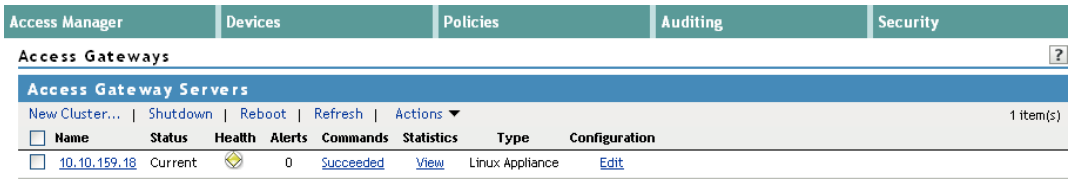
This process might take 15 to 30 minutes, depending on the configuration and hardware.

The machine reboots after the installation is completed. It runs an auto configuration script, and then the Linux Appliance is imported to the Administration Console.

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

14 (Optional) To verify the installation of the Access Gateway, log in to Administration Console (see Section 4.3, "Logging In to the Administration Console," on page 48), then click *Devices* > *Access Gateways*.

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



The Health status indicates the health state after the Access Gateway is imported and registers with the Administration Console. 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.3, "Troubleshooting the Access Gateway Import," on page 158.

15 This completes the installation of the Linux Appliance. Continue with the one of the following:

- "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP1 Setup Guide*
- Section 6.5, "Viewing the Linux Installation Log," on page 74

6.4 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.

6.4.1 Planning Your Partition Strategy

Linux allows you to have four primary partitions per hard disk. The Linux Appliance 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 6-1 *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 6-2 *Partitions for an Array of Disks*

Partition Type	Requirements
boot	This partition contains the boot files. It should be 80 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.

6.4.2 Starting the Installation

1. Insert the Linux Appliance 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 6.2, “Boot Screen Function Keys,” on page 58.

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.*

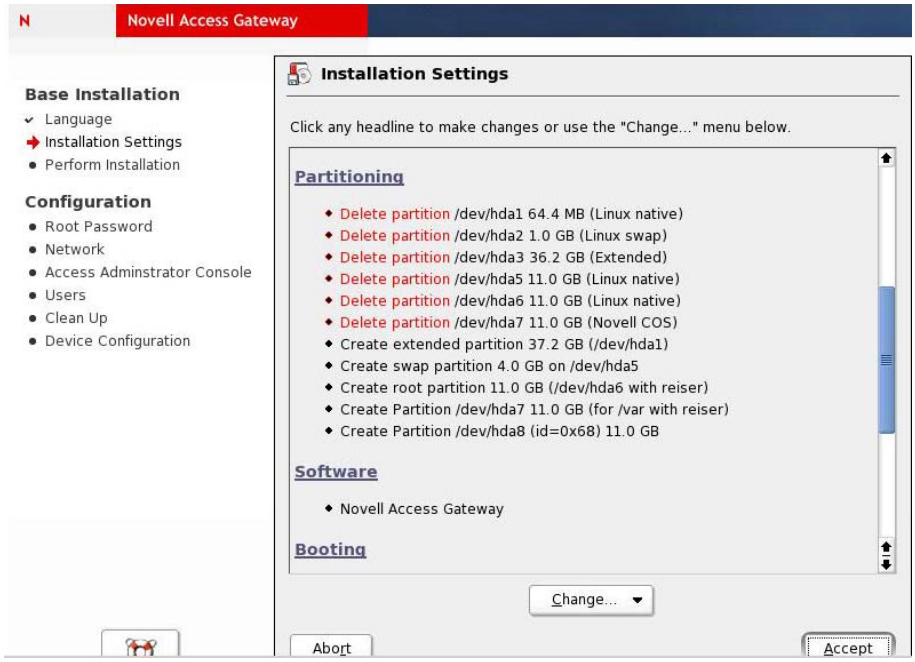
The current version is an English-only version.

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 6.4.3, “Customizing the Partitions,” on page 67.
- Modify the time zone. See Section 6.4.4, “Configuring Date and Time Values,” on page 69.

Other modifications, explained in Section 6.4.5, “Customizing Optional Settings,” on page 70, are optional.

6.4.3 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 6.4.4, "Configuring Date and Time Values," on page 69.

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.

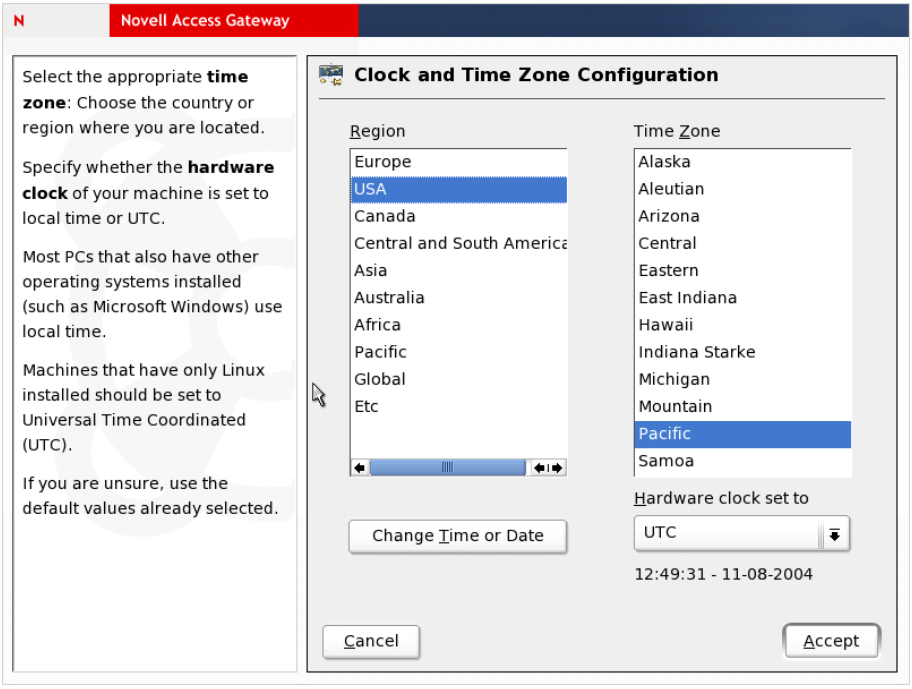
14c Click *OK*.

14d Repeat these steps to create additional COS partitions.

15 Click *Next*, then continue with Section 6.4.4, “Configuring Date and Time Values,” on page 69.

6.4.4 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 Appliance, Identity Server, and Administration Console.

---

5 Click *Accept.*

6 Continue with Section 6.4.5, "Customizing Optional Settings," on page 70 or Section 6.4.6, "Configuring Hardware and System Services," on page 71.

6.4.5 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 6.4.6, "Configuring Hardware and System Services," on page 71.

1 Click *Software* to select software packages to be installed with the Linux Appliance installation.

WARNING: The Linux Appliance is an appliance. Adding additional packages breaks your support agreement with Novell. If you encounter a problem, Novell Support can require you to remove the additional packages and to reproduce the problem before receiving any help with your problem.

---

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 6.4.6, “Configuring Hardware and System Services,” on page 71.

6.4.6 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.

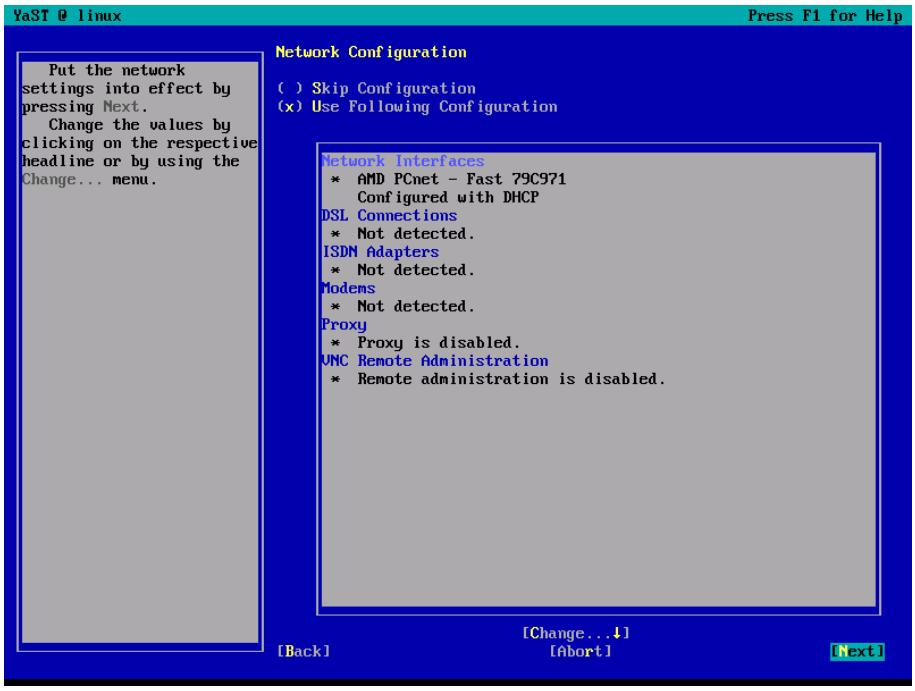
The hard disk is formatted, destroying all data, and the partitions are created. After all the packages are installed, the system reboots.

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 Appliance 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.

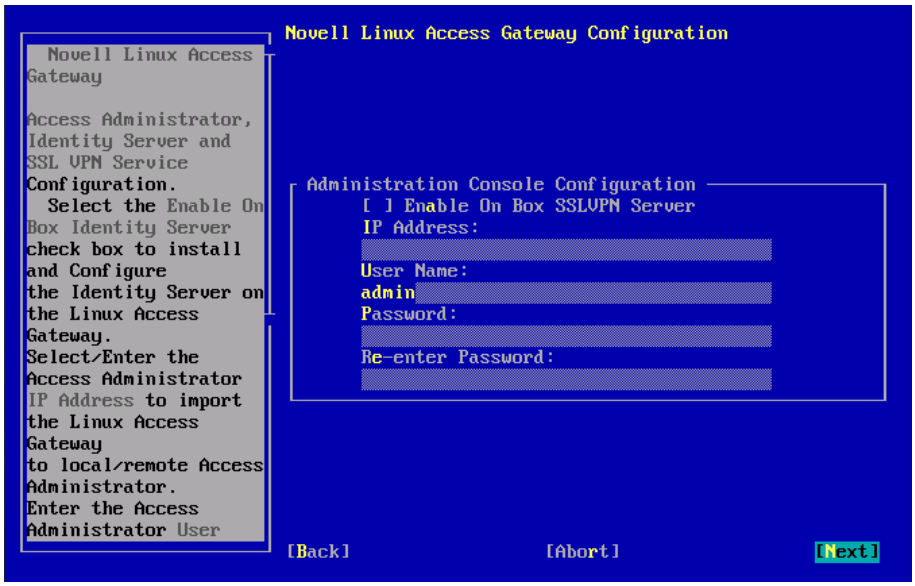
5f Specify the gateway for your network, tab to *OK*, then press Enter.

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 *Administrator Console Configuration* screen appears.



Fill in the following fields:

Enable On Box SSL VPN Server: Select this check box to install and configure the SSL VPN service on the Linux Appliance. When the SSL VPN server is installed on the same box as the Access Gateway, the SSL VPN server must be configured as a protected resource of the Access Gateway.

IMPORTANT: The SSL VPN Server cannot be uninstalled without uninstalling the Linux Appliance.

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

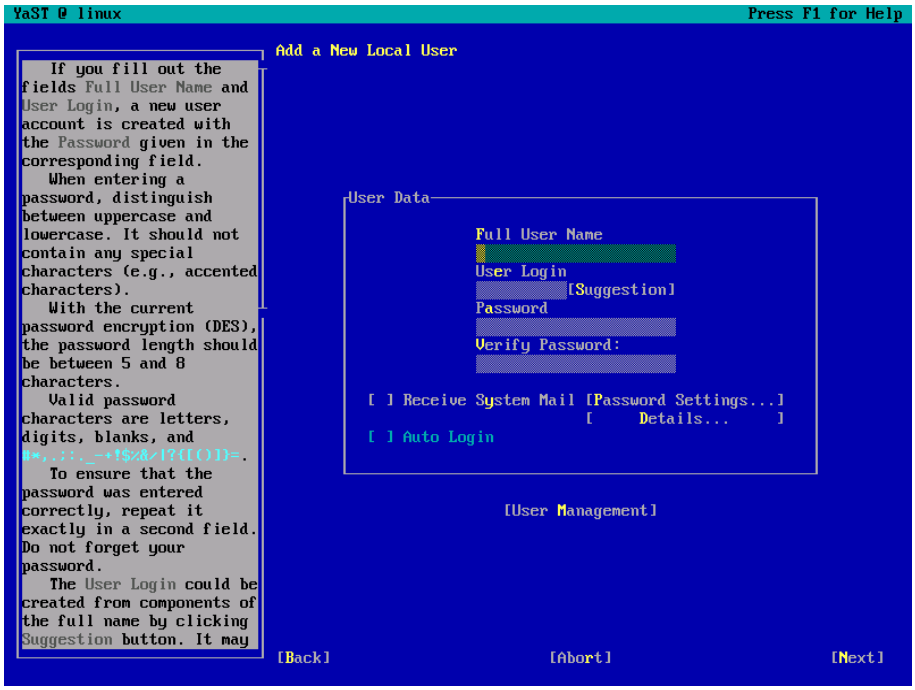
Access Gateway IP Address: Specify the IP address of the Access Gateway.

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.



8 To set a secure password for the `config` user, tab to *User Management*, then press Enter.

The `config` user should be highlighted.

9 Press Enter and change the following fields:

Password: Delete the displayed password and specify a new one.

Verify Password: Delete the displayed password and specify a new one.

10 Tab to *Next*, then press Enter.

11 Tab to *Next*, then press Enter.

The system configuration is written.

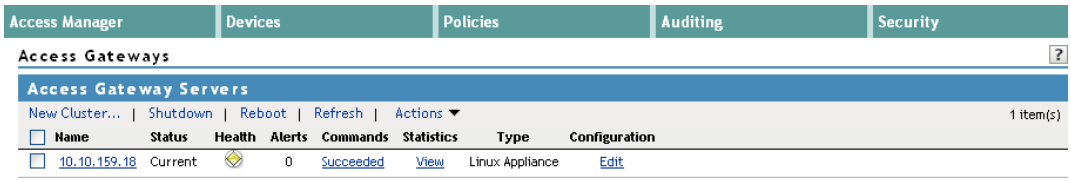
12 Tab to *Next*, then press Enter.

The final configuration and auto-import into the Administration Console is started. This might take 10 to 15 minutes, depending on the configuration and hardware.

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

13 (Optional) To verify the installation of the Access Gateway, log in to Administration Console (see Section 4.3, "Logging In to the Administration Console," on page 48), then click *Devices* > *Access Gateways*.

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



The Health status indicates the health state after the Access Gateway is imported and registers with the Administration Console. 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.3, "Troubleshooting the Access Gateway Import," on page 158.

14 This completes the installation of the Linux Appliance. Continue with the one of the following:

- "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP1 Setup Guide*
- Section 6.5, "Viewing the Linux Installation Log," on page 74

6.5 Viewing the Linux Installation Log

While installing, the Linux Appliance 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.

Upgrading Access Manager Components

7

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.

For information on upgrading the J2EE Agents, see the *Novell Access Manager 3.1 SP1 Agent Guide*. For information on upgrading the SSL VPN component, see the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.

7.1 Upgrading from the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the product.

7.2 Upgrading from Access Manager 3.0 SP4 to Access Manager 3.1 SP1

For the 3.0 support packs, we recommended that you upgrade all Access Manager components at the same time. The 3.1 SP1 upgrade process has been modified so that you can upgrade a cluster of components rather than all components. For example, you can upgrade your Administration Consoles, then wait a few days before upgrading the Identity Servers. You should not use the new 3.1 SP1 features until all components have been upgraded to 3.1 SP1.

IMPORTANT: Your Access Manager components must be running 3.0 SP4 to upgrade to 3.1 SP1. If they are running an earlier version, you must first upgrade them to 3.0 SP4.

The following steps outline the order in which you should upgrade the components. It is the only order that has been tested, and Novell strongly recommends that you take this approach. If you upgrade your components in a different order, you might experience problems and be requested by Novell Support to restore a backup on the previous version.

J2EE Agents cannot be upgraded from 3.0 SP4 to 3.1 SP1. To use the agents in 3.1 SP1, you need to perform a clean install.

We recommend that you use the following schedule as you upgrade to 3.1:

- Section 7.2.1, “Before Starting the Upgrade,” on page 76
- Section 7.2.2, “Upgrading the SP4 Administration Consoles,” on page 78
- Section 7.2.3, “Upgrading the SP4 Identity Servers,” on page 79
- Section 7.2.4, “Modifying 3.0 Login Pages for 3.1 SP1,” on page 81
- Section 7.2.5, “Upgrading the SP4 Linux Access Gateways,” on page 85
- Section 7.2.6, “Upgrading the SP4 SSL VPN Server,” on page 85
- Section 7.2.7, “Upgrading the Policies,” on page 86

If a component fails to upgrade successfully, see Section 7.2.8, “Troubleshooting a Failed Upgrade,” on page 87 for a solution.

7.2.1 Before Starting the Upgrade

1 Make sure all components are upgraded to at least 3.0 SP4:

1a In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.

1b Verify that your components are running the following versions:

Component	Access Manager 3.0 SP4 Version Number
Administration Console	3.0.4.38 through 3.0.4.69
Identity Server	3.0.4.38 through 3.0.4.69
Linux Access Gateway	3.0.4.38 through 3.0.4.69
NetWare® Access Gateway	3.0.503

Component	Access Manager 3.0 SP4 Version Number
J2EE Agents (all versions, all platforms)	3.0.4.38
SSL VPN	3.0.4

2 Back up your system.

For instructions, see "Backing Up the Administration Console" in the *Novell Access Manager 3.1 SP1 Administration Console Guide*.

3 Back up the custom configuration files that you have created for your Identity Server:

- Back up any customized JSP pages and related files. The upgrade process replaces all JSP pages on the Identity Server.

  Linux: `/var/opt/novell/tomcat5/webapps/nidp/jsp`

  Windows: `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp`

- If you are using Kerberos, back up the `bcsLogin.conf` and keytab files.

  Linux: `/opt/novell/java/jre/lib/security`

  Windows: `C:\Program Files\Novell\jre\lib\security`

4 (Conditional) If you have any Administration Consoles or Identity Servers running on SUSE® Linux Enterprise Server (SLES) 9, upgrade the operating system to SLES 10 with the latest support pack.

WARNING: When upgrading, select to view the update options on the Update Summary page. Deselect *Delete unmaintained packages*. If this option is enabled, all Access Manager software is removed.

For instructions, see "How to update to SLES/SLED 10 SP2" (http://www.novell.com/support/viewContent.do?externalId=7000387&sliceId=2).

5 (Conditional) If you have any Administration Consoles or Identity Servers running on SUSE® Linux Enterprise Server (SLES) 10 SP1, upgrade the operating system to SLES 10 SP2 or SP3.

6 If you have installed a previous version of the Administration Console or the Identity Server on a machine that does not have at least 1 GB (recommended minimum is 2 GB), the upgrade to SP1 fails. You need to install more memory before upgrading.

The installation script now checks for available memory and aborts the upgrade if the machine does not have at least 1 GB of memory.

7 If you have changed the password of the Tomcat keystore on an Administration Console that isn't installed with an Identity Server, you need to change the password back to the default password.

7a Change to the `/var/opt/novell/novlwww` directory.

7b Use the `keytool` utility to change the password in the `.keystore` file to `changeit`.

8 If you have installed the high bandwidth version of the SSL VPN server and the server is installed with another Access Manager component, install the SSL VPN High Bandwidth Key.

When you upgrade components on machines that have multiple Access Manager components installed, all components are automatically upgraded. If you have not installed this key, your SSL VPN server reverts to a low bandwidth version.

8a Log in to the Novell Customer Center (http://www.novell.com/center) and download the high bandwidth key.

8b Copy the RPM to your SSL VPN machines.

8c Use the following RPM command to install it:

```
rpm -ivh <rpm-name>
```

Replace <*rpm-name*> with the name of the SSL VPN High Bandwidth Key.

9 If you have any NetWare Access Gateways, export their configuration.

The NetWare Access Gateway is not supported in 3.1 SP1. As soon as you upgrade the Administration Console, the only option available for the NetWare Access Gateway is to export its configuration. For information on how to convert a NetWare Access Gateway to a Linux Access Gateway, see Section 7.7, "Converting a NetWare Access Gateway," on page 100.

10 Continue with Section 7.2.2, "Upgrading the SP4 Administration Consoles," on page 78.

7.2.2 Upgrading the SP4 Administration Consoles

The primary Administration Console must be the first device that is upgraded to 3.1 SP1.

If an Identity Server or an SSL VPN server is installed on the same machine as the Administration Console, these devices are automatically upgraded at the same time as the Administration Console.

1 (Conditional) If you have an Identity Server installed on the same machine as the primary Administration Console, modify the L4 switch so that no traffic is sent to this Identity Server.

When the Identity Server is taken off line for the upgrade, any users logged into this server are seamlessly transferred to another server.

2 Upgrade the primary Administration Console.

For upgrade information, see Section 7.4.1, "Upgrading the Linux Administration Console," on page 89.

3 Before logging into the 3.1 SP1 Administration Console, clear your browser cache.

4 (Conditional) If the machine contains a SSL VPN server, it was automatically upgraded with the Identity Server. To determine what needs to be done next, see Section 7.2.6, "Upgrading the SP4 SSL VPN Server," on page 85.

5 If the machine contains just an Administration Console or an Administration Console and an Identity Server, upgrade any secondary consoles.

6 Verify that the system is in a manageable state. All devices should display green as their health state.

You should be able to edit the configuration and policies for your Access Gateways and agents.

If you didn't need to upgrade an Identity Server with the Administration Console, your Identity Servers cluster should contain only 3.0 SP4 servers. In this condition, you should be able to edit their cluster configuration and the policies. If you needed to upgrade an Identity Server with an Administration Console, the Identity Servers cluster configuration should not be modified until you have upgraded all the Identity Servers in the cluster.

You should not try to use 3.1 or 3.1 SP1 features until all components have been upgraded. The new 3.1 policy features such as policy extensions, policy copy, and force data read appear on the policy configuration pages, but they won't be active until all components have been upgraded, including the policy engine.

7 If the upgrade is successful, continue with Section 7.2.3, “Upgrading the SP4 Identity Servers,” on page 79.

If the upgrade is unsuccessful, see Section 7.2.8, “Troubleshooting a Failed Upgrade,” on page 87.

7.2.3 Upgrading the SP4 Identity Servers

The Identity Servers can be upgraded one at time. This allows your site to remain up during the upgrade. However, they should all be upgraded as quickly as possible.

1 Modify the L4 switch so that no traffic is sent to the Identity Server you have selected to upgrade.

When the Identity Server is taken off line for the upgrade, any users logged into this server are seamlessly transferred to another server.

2 Upgrade the Identity Server.

For more information, see Section 7.5.1, “Upgrading the Linux Identity Server,” on page 92.

3 Decide whether a custom login page is required.

As soon as you have a 3.1 SP1 server in the cluster, be aware that the user experience is not the same for all users. Users who are attached to the 3.0 servers are prompted with the 3.0 login page. Users who are attached to the 3.1 SP1 servers are prompted with the 3.1 SP1 login page. One solution to this mixed environment is to upgrade all servers as quickly as possible. The other solution is to use a custom login page and enable it for both the 3.0 and 3.1 servers. This makes the login experience the same, but session failover when an Identity Server goes down is not seamless. The users who used the down server for authentication are prompted to log in again.

Custom 3.0 login pages cannot be used with 3.1 SP1 without modification. For information on how to modify 3.0 custom pages, see Section 7.2.4, “Modifying 3.0 Login Pages for 3.1 SP1,” on page 81.

4 (Conditional) If you have set up Kerberos authentication, restore the `bcsLogin.conf` and keytab files to the `/opt/novell/java/jre/lib/security` directory. In a text editor, modify the `bcsLogin.conf` file.

Replace `other` in the first line with the following:

```
com.sun.security.jgss.accept
```

This is required because Access Manager 3.1 SP1 uses a different version of Java.

5 (Conditional) If the Identity Server contained an SSL VPN server, the SSL VPN server was upgraded with the Identity Server. See Section 7.2.6, “Upgrading the SP4 SSL VPN Server,” on page 85 before upgrading another Identity Server.

6 (Conditional) If you are using Novell SecretStore®, verify that the 3.1 SP1 settings match your 3.0 configuration.

6a In the Administration Console, click *Devices* > *Identity Servers* > *Edit* > *Local* > *[Name of User Store]*.

6b If this eDirectory™ user store has SecretStore installed on it, select the *Install NMAS SAML method* option.

6c If you enabled secret store lock checking in 3.0, select the *Enable Secret Store lock checking* option.

6d Click *OK* twice, then update the Identity Server.

7 (Conditional) If you have set up trusted identity providers, you need to configure a card for them.

If you configured a link on the login page that allowed your users to select the identity provider they wanted to use for authentication, this link is removed when you upgrade to 3.1 SP1. To add the link to the 3.1 SP1 login page, you need to configure an authentication card for each identity provider.

7a In the Administration Console, click *Devices* > *Identity Servers* > *Edit* > *[Protocol]* > *[Identity Provider]* > *Authentication Card*.

7b In the *Text* box, specify a description for the identity provider.

If you used only a text link in 3.0, enter that text here.

7c In the Image list, click <*Select local image*> to upload a custom image.

If you used an image for the link in 3.0, upload the image file and use it for the authentication card. Images must fall within the size bounds of 60 pixels wide by 45 pixels high through 200 pixels wide by 150 pixels high.

For ease of use, each identity provider should have its own unique image.

7d Enable the *Show Card* option.

7e Repeat these steps for each configured identity provider.

7f Update the Identity Server.

8 Reconfigure the L4 switch so that the upgraded server receives traffic.

9 Upgrade another server in the cluster.

When you take the second server offline for an upgrade, users might not be seamlessly transferred. They might be prompted to log in again.

10 Restore any custom files before bringing the server back online. See Step 3 and Step 4.

11 Upgrade the remaining servers in the cluster.

You should not try to use any of the new 3.1 or 3.1 SP1 features such as CardSpace and WS Federation until all Access Manager components have been upgraded to 3.1 SP1.

12 (Conditional) If you are using the 3.1 login page, configure authentication cards for the contracts that you are using.Configure authentication cards for the contracts that you are using.

In 3.1 SP1, all contracts can have an associated authentication card. If you allow the cards to appear on the login page, users can select their authentication method by selecting the card.

The upgrade process does not try to assign cards to contracts because it cannot anticipate all the ways the contracts might have been customized. To assign a card to a contract:

12a In the Administration Console, click *Devices* > *Identity Servers* > *Edit* > *Local* > *Contracts*.

12b Click the name of a contract, then click *Authentication Card*.

12c In the Text box, specify a description of the contract. You might want to use the name of the contract for this description.

12d From the drop-down list, select an image.

For the default contracts and classes, Access Manager supplies some cards for you to use. You can use these images or use the <*Select local image*> option to upload your own custom images. Images must fall within the size bounds of 60 pixels wide by 45 pixels high through 200 pixels wide by 150 pixels high.

Default Contract or Class	Default Image Name
Name/Password - Basic	Basic Auth Username Password
Name/Password - Form	Form Auth Username Password
Secure Name/Password - Basic	Secure Basic Auth Username Password
Secure Name/Password - Form	Secure Form Auth Username Password
Kerberos	Kerberos
NMAS	NMAS Biometrics
X509	X509

12e Enable the Show Card option if you want the card to appear on the login page.

12f Repeat these steps for each contract.

If you have configured your protected resources on the Access Gateway to use *Any Contract* and you want the users to select how they authenticate, each configured contract needs to have a card.

12g Update the Identity Server.

13 If the upgrade is successful, continue with Section 7.2.5, "Upgrading the SP4 Linux Access Gateways," on page 85.

If the upgrade is unsuccessful, see Section 7.2.8, "Troubleshooting a Failed Upgrade," on page 87.

7.2.4 Modifying 3.0 Login Pages for 3.1 SP1

If you have created custom login pages for use with specific protected resources, you need to modify these login pages before installing them on the Identity Servers running Access Manager 3.1 SP1. If you want the login page to have the same look and feel as the 3.0 login page, you can modify the `login.jsp` file from 3.0 so that it works on 3.1 SP1. If you want your custom login pages to have the 3.1 look and feel, see "Customizing the Identity Server Login Page" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

For information on how to modify a 3.0 `login.jsp` page to compile and run on 3.1 SP1, see the following:

- "Modifying the Properties of the Authentication Class or Method" on page 82
- "Converting Custom Access Manager 3.0 JSPs to 3.1 JSPs" on page 82
- "Preserving the Target" on page 84
- "Modifying a Custom JSP for Federation Links" on page 84

Modifying the Properties of the Authentication Class or Method

In Access Manager 3.0, the login page for a particular authentication contract can be altered by setting an alternative JSP in the properties of an authentication class or method. In 3.1, setting the same JSP property causes the JSP to display in the credential frame of the login page. To create the same effect in 3.1 SP1, you must add the MainJSP property to the authentication method.

Property Name: MainJSP

Property Value: true

Property names and values are case sensitive.

Setting the MainJSP property causes the `login.jsp` page to be displayed in the main frame, not in the credential frame. For more information about setting property values, see "Specifying Common Class Properties" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

Converting Custom Access Manager 3.0 JSPs to 3.1 JSPs

Changes were made in Access Manager 3.1 to simplify the JSPs that need to be created by authentication class developers. The changes allow the developers of new authentication classes to focus on the collection of required credentials and not on other aspects of the user interface. These changes have made JSPs used in Access Manager 3.0 incompatible with 3.1 SP1.

The line numbers in the following steps refer to the lines in a unmodified 3.0 `login.jsp` file. To understand what the lines the numbers refer to, see Appendix B, "Modifications Required for a 3.0 Login Page," on page 169.

To convert a 3.0 JSP to a 3.1 SP1 JSP:

1. Remove the following import statement found in line 5:

   ```
   <%@ page import="java.net.*" %>
   ```

2. Add the following import statement:

   ```
   <%@ page import="com.novell.nidp.ui.*" %>
   ```

3. Find the following code in lines 12 through 18:

   ```
   response.setHeader("Pragma", "No-cache");
   response.setHeader("Cache-Control", "no-cache");

          Locale locale = request.getLocale();
          String strLanguageCode = locale.getLanguage();
          String strImageDirectory = NIDPResourceManager.getInstance().
   getImageDirectory(locale);
          NIDPResource resource = NIDPResourceManager.getInstance().
   get(JSPResDesc.getInstance(), locale);
   ```

4. Replace the code found in Step 3 with the following line:

   ```
   ContentHandler handler = new ContentHandler(request,response);
   ```

5. Remove all code and HTML associated with the following method:

   ```
   request.getAttribute("identify")
   ```

   Remove line 73 through line 79, and all of line 80 except for the ending Java code marker (%>). In 3.0, if user identification was necessary, this code handled it. In 3.1 SP1, the identity provider handles user identification when necessary.

6. .Remove all code and HTML associated with the following method:

`request.getAttribute("provision")`

Remove line 108 through line 120. In 3.0, if provisioning was available, this method handled provisioning. In 3.1 SP1, the identity provider handles provisioning.

7 Remove all code and HTML associated with `DisplayableProvider` objects. Remove line 126 through 159.

In 3.0, this code displayed the federated identity providers. In 3.1, this has been replaced with authentication cards and is handled by the identity provider. For information on how to add federation links to your login page, see "Modifying a Custom JSP for Federation Links" on page 84.

8 Remove all code and HTML associated with the following method:

`request.getAttribute("cancel")`

Remove line 165 through 176. In 3.0, if an option to cancel was available, this code handled it. In 3.1 SP1, the identity provider handles cancel.

9 Replace any references to `strLanguageCode` with `handler.getLanguageCode()`.

10 Replace all references to the `locale` variable with `request.getLocale()`.

11 Image references formerly included the `strImageDirectory` variable. This variable has been removed, and image references must use the following method:

`handler.getImage("btnlogin.gif",true)`

The first parameter specifies the filename of the image. The second parameter specifies the location of the file:

- Specify false if the image is not localized and always located in the `\images` directory.
- Specify true if the image is localized and is located in an appropriate language directory in the `\images` directory.

On line 104, replace the image src (`src="<%= request.getContextPath() %>/images/<%=strImageDirectory%>/btnlogin_<%=strImageDirectory%>.gif"`) with the following:

`src="<%=handler.getImage("btnlogin.gif",true)%>"`

12 Replace references to `resource.getString0(resource)` with `handler.getResource(resource)`.

13 Replace the following resources if they exist in your file:

`JSPResDesc.LOGIN_TITLE` with `JSPResDesc.TITLE`

`JSPResDesc. LOCAL_LOGIN` with `JSPResDesc.PRODUCT`

14 Some other resources might not be available. Replace any of these resources with the text that you need for your site.

15 Copy the file to the `jsp` directory of your Identity Server.

Linux: `/var/opt/novell/tomcat5/webapps/nidp/jsp`

Windows: `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp`

16 Test the page by logging in.

17 (Conditional) If you get a blank page instead of a login page:

17a Ensure that logging is turned on (click *Devices* > *Identity Servers* > *Edit* > *Logging*). Make sure that *File Logging* is enabled, that *Echo to Console* is enabled, and that *Application* logging is set to *Debug*.

17b Try logging in again.

17c Look for errors in the `catalina.out` (Linux) or `stdout.log` (Windows) file.

Search for the name of your custom login page. Each line in the file with an error generates an error message. For example, if you missed removing a reference to `locale`, the file contains a message similar to the following:

```
An error occurred at line: 129 in the jsp file: /jsp/login_custom.jsp
locale cannot be resolved
126:   {
127: %>
128:         <tr>
129:                <td colspan=4 width="100%"
align="center"><%=NIDPCripple.getCrippleAdvertisement(locale)%></td>
130:         </tr>
131: <%
132:   }
```

18 (Optional) To view a 3.0 `login.jsp` file that has been modified (but not customized) to compile on 3.1 SP1 IR1, see Appendix B, "Modifications Required for a 3.0 Login Page," on page 169.

Preserving the Target

With this custom login page setup, users accessing protected resources on the Linux Access Gateway sometimes get presented with the Identity Server user portal page and not the protected resource after submitting their credentials. This happens if the user, after getting redirected to the login page, waits for a timeout greater than the session timeout before submitting the credentials.

In this scenario, the Identity Server realizes that the original session is invalid and creates a new session to validate the credentials. With this new session, the original user's context is lost and that context contained the target, or the redirect URL, to be used after validating the credentials.

To get the hidden target or redirect field added to the form, the following code needs to be added somewhere within the form content of the JSP. With this code available, the new session can still reference the URL to redirect the user too even if the session has timed out.

```
<%
 String target = (String) request.getAttribute("target");
 if (target != null)
   {
     %>
          <input type="hidden" name="target" value="<%=target%>">
    <%
   }
%>
```

Modifying a Custom JSP for Federation Links

The 3.1 login page uses cards for federation. To make your 3.0 federation links compatible with 3.1, make the following modifications to your custom login pages that contain federation links:

1. Near the top of the JSP file, add the following import statements:

   ```
   <%@ page import="com.novell.nidp.authentication.card.*" %>
   <%@ page import="com.novell.nidp.common.util.*" %>
   ```

2. Add the following include statement for the stylesheet:

```
<link rel="stylesheet" href="<%= handler.getImage("cards.css",false)%>"
type="text/css">
```

3 Add the following lines to include the `cards31.jsp` file:

```
<tr>
   <td width="50%"> </td>
   <td style="background-color: #efeee9; padding: 10px" colspan=2>

      <%@ include file="cards31.jsp" %>

   </td>
   <td width="100%"> </td>
</tr>
```

7.2.5 Upgrading the SP4 Linux Access Gateways

When the servers in the cluster have been upgraded, you can modify the 3.0 features, but you should not try to use any of the new 3.1 or 3.1 SP1 features until all Access Manager components have been upgraded to 3.1 SP1.

NetWare Access Gateways must be converted to Linux Access Gateways. For more information, see Section 7.7, “Converting a NetWare Access Gateway,” on page 100.

1 Upgrade a secondary server in the cluster. The primary server needs to be the last server upgraded.

   The Linux Access Gateway supports multiple upgrade methods. For information about these methods, see Section 7.6, “Upgrading the Linux Access Gateway Appliance,” on page 95.

   If the Access Gateway server contains an SSL VPN server, it is automatically upgraded with the Access Gateway.

2 (Conditional) If the Access Gateway server contains an SSL VPN server, continue with Section 7.2.6, “Upgrading the SP4 SSL VPN Server,” on page 85.

3 Upgrade the other secondary servers in the cluster.

4 Upgrade the primary server in the cluster.

5 If the upgrade is successful, continue with Section 7.2.6, “Upgrading the SP4 SSL VPN Server,” on page 85.

   If the upgrade is unsuccessful, see Section 7.2.8, “Troubleshooting a Failed Upgrade,” on page 87.

7.2.6 Upgrading the SP4 SSL VPN Server

Your configuration determines when you upgrade the SSL VPN servers:

- If the SSL VPN servers are installed on separate machines, upgrade them after the Administration Console, Identity Server, and Linux Access Gateways have been upgraded.

  For upgrade information, see “Upgrading SSL VPN Installed on a Separate Machine” in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.

- If they were installed with another Access Manager component (the Administration Console, the Identity Servers or a Linux Access Gateway), they are upgraded along with the respective components. What you upgrade next, depends upon your configuration. See “Multiple SSL VPN Servers per Protected Resource” on page 86 and “Servlet Load Balancing” on page 86.

After you have upgraded the SSL VPN servers, continue with the next required component. After all devices have been successfully upgrade, continue with Section 7.2.7, "Upgrading the Policies," on page 86.

If the upgrade is unsuccessful, see Section 7.2.8, "Troubleshooting a Failed Upgrade," on page 87.

Multiple SSL VPN Servers per Protected Resource

If you have configured a protected resource to be serviced by multiple SSL VPN servers, these servers can be a mixture of 3.1 SP1 and 3.0 until you have finished upgrading any secondary Administration Consoles, Identity Servers, and Linux Access Gateways. You need to be aware that as long as there is a mixture, the user experience varies. When the user sets up a connection to the 3.0 server, the user accesses the 3.0 client and uses its interface. When the user is directed to the 3.1 SP1 server and sets up a connection, the user accesses the 3.1 SP1 client and uses its interface.

Continue with the next required component:

- If the SSL VPN server was installed on the Administration Console, continue upgrading the secondary consoles.
- If the SSL VPN server was installed on the Identity Server, continue upgrading the other Identity Servers in the cluster.
- If the SSL VPN server was installed on the Linux Access Gateway, continue upgrading the other Access Gateways in the cluster.

Servlet Load Balancing

If you have configured the SSL VPN server to use servlet load balancing, you need to immediately upgrade all SSL VPN servers. If the servers are installed with other Access Manager components, upgrade that component. For instructions, see the following:

- Section 7.2.2, "Upgrading the SP4 Administration Consoles," on page 78
- Section 7.2.3, "Upgrading the SP4 Identity Servers," on page 79
- Section 7.2.5, "Upgrading the SP4 Linux Access Gateways," on page 85

If the SSL VPN servers are installed on separate machines, see "Upgrading SSL VPN Installed on a Separate Machine" in the *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*.

7.2.7 Upgrading the Policies

The following procedures cause some down time for your system. Perform them when the fewest users are accessing your system.

1. Make sure all devices are in a Current state.

   All configuration changes to the devices need to be applied before upgrading the policies.

2. Back up your system.

   For instructions, see "Backing Up the Administration Console" in the *Novell Access Manager 3.1 SP1 Administration Console Guide*.

3. After you have upgraded all the Access Manager components, upgrade the policies.

   3a In the Administration Console, click *Policies* > *Policies*.

3b To view the devices that need to have their policies upgraded, click *Details*.

3c Review the list, then click *Upgrade Policies*.

4 Update the policies on all the Identity Servers.

Existing authenticated sessions continue to work. New authentications fail until all the Identity Servers and Access Gateways have been updated.

If the update to an Identity Server fails, perform an amrestore. If you modified the Tomcat password, you need to back up the Tomcat `server.xml` file before running the restore. See "Restoring an Administration Console Configuration"in the *Novell Access Manager 3.1 SP1 Administration Console Guide* Then restart the Identity Server.

Solve the problem before attempting to upgrade the policies again.

5 Update the Access Gateways.

If the update to an Access Gateway fails, perform an amrestore. If you modified the Tomcat password, you need to back up the Tomcat `server.xml` file before running the restore. See "Restoring an Administration Console Configuration"in the *Novell Access Manager 3.1 SP1 Administration Console Guide*

Restart the Identity Servers, then re-push the configuration to the Access Gateway. Click *Auditing* > *Troubleshooting*, scroll to the *Current Access Gateway Configurations* section, select the Access Gateway, then click *Re-push Current Configuration*.

Solve the problem before attempting to upgrade the policies again.

6 Start using the new 3.1 and 3.1 SP1 features.

For a description of the new features, see Chapter 1, "What's New in Access Manager 3.1 SP1," on page 11.

7.2.8 Troubleshooting a Failed Upgrade

If the upgrade fails when upgrading the Administration Console, reinstall a 3.0 SP4 version of the Administration Console and restore the backup. Fix the problems encountered in the failed upgrade before trying again.

If the upgrade fails when upgrading an Identity Server, an Access Gateway, or an SSL VPN server but the Administration Console has been successfully upgraded to 3.1 SP1, try installing a 3.1 SP1 version of the component with the same IP address as the failed component. When the device imports into the Administration Console, the component's configuration information should be pushed to it.

- To push the configuration to an Identity Server, restart the Identity Server.
- To push the configuration to an Access Gateway, use the Re-push option. Click *Auditing* > *Troubleshooting*, scroll to the *Current Access Gateway Configurations* section, select the Access Gateway, then click *Re-push Current Configuration*.

If this does not work, you need to reinstall the 3.0 SP4 version of the component and fix the problems encountered in the failed upgrade before trying again. To return all components to 3.0 SP4, use the backup you took before upgrading and perform an amrestore. If you have modified the Tomcat password, you need to back up the Tomcat `server.xml` file before running the restore. See "Restoring an Administration Console Configuration"in the *Novell Access Manager 3.1 SP1 Administration Console Guide*

7.3 Upgrading from Access Manager 3.1 to 3.1 SP1

The upgrade from 3.1 to 3.1 SP1 uses the standard processes used in the other Access Manager support pack releases.

- Section 7.4, “Upgrading the Administration Console,” on page 89.
- Section 7.5, “Upgrading the Identity Server,” on page 92
- Section 7.6, “Upgrading the Linux Access Gateway Appliance,” on page 95

Your Access Manager components have 3.1 installed if they display a version number between 3.1.0.420 and 3.1.0.431.

There are some new processes you need to be aware of and some additional configuration steps.

- ❑ The installation script for the Administration Console and the Identity Server now checks to ensure that you have the at least 1 GB (Linux) or 1.2 GB (Windows) of memory on the machine, and the upgrade fails if you have less. This upgrade check is below the recommended minimum of 2 GB.
- ❑ When upgrading the Administration Console, answer Yes to the prompt to make a backup of your configuration.

  A recent backup is usually the quickest solution for restoring a system when an upgrade encounters a problem that requires an engineering fix. If you don’t have a recent backup, you might be forced to re-create your configuration.
- ❑ SP1 adds some new features. Do not try using any of the new features until after you have upgraded all components to 3.1 SP1.

  For information about these new features, see “What’s New in Access Manager 3.1 SP1” on page 11.
- ❑ Do not make modifications to your user stores until you have upgraded both the Administration Console and the Identity Server.

  If you make modifications, you break communication between the Identity Server and the user store until you upgrade the Identity Server.
- ❑ If you have customized the login pages, make sure you make a backup before you begin the upgrade process.

  Even though the program automatically backs up the JSP directory and stores a zip of these files in a `nambkup` directory (under $HOME on Linux and at the root of the operating system drive on Windows), you should have your own backup.
- ❑ If you have customized login pages and you answer Yes to the prompt to preserve your 3.1 login pages, the following modifications happen automatically:
  - The `main.jsp` file from the backup of the 3.1 system is renamed `nidp.jsp` and installed in the JSP directory.
  - The `menus.jsp`, `content.jsp`, and `login.jsp` files from the backup of the 3.1 system are copied to the JSP directory.
  - The Tomcat working directory is cleared.
  - If you have given any other of your custom login pages or custom images the same name as the files that come with the product, these files are overwritten. You need to manually restore them.

- ❑ If you have customized login pages and you answered No to the prompt to preserve your 3.1 login pages, they are backed up to the `nambkup` directory (under $HOME on Linux and at the root of the operating system drive on Windows). You can manually restore them by following the description in above or you can use the 3.1 SP1 process to customize the login experience (see "Customizing the Identity Server Login Page" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*).

  If you manually restore your files, remember to clear the Tomcat working directory.

  Linux: `/var/opt/novell/tomcat5/work/Catalina/localhosts/nidp`

  Windows: `C:\Program Files\Novell\Tomcat\work\Catalina\localhosts\nidp`

  Then restart Tomcat on the Identity Server.

- ❑ (Conditional) If you have configured your Identity Server for trace logging (*Identity Servers* > *Edit* > *Logging*), you need modify the logging page after you finish the upgrade.

  The trace logging option on the Logging page has been removed. You can obtain the same level of event messages when you set the *Component File Logger Levels* to *Debug*.

  The trace logging options are viewable in the Administration Console as long as one Identity Server in the cluster is still running version 3.1 or 3.0.4, but they can't be set.

- ❑ (Conditional) If you have configured the Identity Server for Kerberos authentication, you need to copy the `keytab` file and the `bcsLogin.conf` file from the `/opt/novell/jdk1.6.0_7/jre/lib/security` directory to the `/opt/novell/java/jre/lib/security` directory. (In 3.1 SP1, `java` is a symbolic link to the `jdk1.6.0_11` directory.) After copying the files, restart Tomcat, then check the log file and make sure the commit succeeded. See "Verifying the Kerberos Configuration" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

- ❑ (Conditional) If you have configured the Identity Server for Card Space, you need to download high encryption files and copy them to the `/opt/novell/java/jre/lib/security` directory. For instructions, see "Enabling High Encryption" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

- ❑ The touch files `.noCache` and `.EnableHttpOnlyCookie` are no longer valid in SP1. You can use the UI options instead to configure. For more information, see "Configuring Caching Options" and "Creating a Reverse Proxy and Proxy Service" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.

7.4 Upgrading the Administration Console

7.4.1 Upgrading the Linux Administration Console

Upgrade running time: about three minutes.

If the Identity Server is installed on the same machine as the Administration Console, the Identity Server is automatically upgraded with the Administration Console. If you are upgrading this configuration and you have custom JSP pages, you can either create your own backup of these files or allow the upgrade program to back them up for you.

To upgrade:

1. (Conditional) If the Identity Server is installed on the same machine, back up any customized JSP pages and related files.
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) 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/novellaccessmanager31/index.html).
6. After downloading the upgrade, unpack the `tar.gz` file by using the following command:

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

   For this installation, you need to unpack the Identity Server `.tar.gz` file.
7. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./install.sh
   ```
8. When prompted to install a product, type 1 for *Install Novell Access Manager Administration*, then press Enter.

   The system detects whether the Administration Console is installed, and prompts you whether to upgrade.
9. (Conditional) If you have installed the Identity Server with the Administration Console, you are asked whether you have backed up your custom login pages:
   - If you have, answer `Y` to the prompt.
   - If you haven't, we recommend that you answer `N` to the prompt, which cancels the upgrade. Even though the upgrade script automatically backs up the JSP directory, we recommend that you have your own backup of your customized files.
10. (Conditional) If you have installed the Identity Server with the Administration Console, you are upgrading from 3.1 to 3.1 SP1, and you have customized the 3.1 login pages, answer `Y` to the prompt to restore your custom login pages.

    For more information on what happens during this process, see Section 7.3, "Upgrading from Access Manager 3.1 to 3.1 SP1," on page 88.
11. Decide whether you want the upgrade program to create a backup of your current configuration:
    - If you have a recent backup, type *N*, then press Enter.

      If you select to not create a backup when you do not have a recent backup and you encounter a problem during the upgrade, you might be forced to recreate your configuration.
    - If you do not have a recent backup, type *Y*, press Enter, then complete the following:

    11a Specify the administration password, then press Enter.

    11b Confirm the password.

11c Specify a location for the backup files, then press Enter.

11d Specify a password for the encryption key.

When you use the backup files to restore this configuration, you must specify this password.

11e Confirm the password.

12 When prompted to upgrade, type *Y*, then press *Enter*.

13 Review and accept the License Agreement.

14 Specify the administration username.

15 Specify the administration password.

16 Confirm the password.

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

18 (Optional) To view the upgrade log file, see the files in y.

- To view the upgrade log files, see the files in the `/tmp/novell_access_manager` directory.
- If you selected to back up your configuration and used the default directory, see the zip file in the `/root/nambkup` directory. The log file for this backup is located in the `/var/log` directory.
- If the Identity Server is installed on the same machine, the JSP directory was backed up to the `/root/nambkup` directory. The file is prefixed with nidp_jps and then contains the date and time of the backup.

If you encounter an error, see Section A.4.2, “Troubleshooting a Linux Administration Console Upgrade,” on page 166.

7.4.2 Upgrading the Windows Administration Console

If you have installed the Identity Server and the Administration Console on the same machine, you must upgrade both of them at the same time.

1 Make a backup of your current Access Manager configuration. For instructions, see “Backing Up and Restoring Components” in the *Novell Access Manager 3.1 SP1 Administration Console Guide*.

2 (Conditional) If the Identity Server is installed on the same machine, back up any customized JSP pages and related files.

3 Download the upgrade file from Novell (http://support.novell.com/patches.html).

For the filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager31/index.html).

4 Run the executable.

This is the installation program. When it detects an installed version of the Administration Console, it automatically prompts you to upgrade.

5 Read the Introduction, then click *Next*.

6 Accept the license agreement, then click *Next*.

7 Select to install the components that are currently installed, then click *Next*.

8 At the upgrade prompt, click *Continue*.

9 Enter the following information for the administrator account on the Administration Console:

Administration user ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.

10 (Conditional) If you have installed the Identity Server with the Administration Console, you are upgrading from 3.1 to 3.1 SP1, and you have customized the 3.1 login pages, allow the upgrade utility to restore your custom login pages.

For more information on what happens during this process, see Section 7.3, "Upgrading from Access Manager 3.1 to 3.1 SP1," on page 88.

11 Decide whether you want the upgrade program to create a backup of your current configuration:

- If you have a recent backup, click *Continue*.

  If you select to not create a backup when you do not have a recent backup and you encounter a problem during the upgrade, you might be forced to recreate your configuration.

- If you do not have a recent backup, click *Run Config Backup*.

  The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.

12 Review the summary, then click *Install*.

13 When prompted, reboot the machine.

14 (Optional) View the upgrade log file found in the following location:

```
C:\Program Files\Novell\log\AccessManagerServer_InstallLog.log
```

7.5 Upgrading the Identity Server

7.5.1 Upgrading the Linux 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.

If you have installed only the Identity Server on the machine, use the following procedure to upgrade the Identity Server. If you have installed both the Identity Server and the Administration Console on the same machine, see Section 7.4.1, "Upgrading the Linux Administration Console," on page 89

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/novellaccessmanager31/index.html).
5. After downloading the upgrade, unpack the `tar.gz` file using the following command:

   ```
   tar -xzvf <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. 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.
9. (Conditional) If you are upgrading from 3.1 to 3.1 SP1 and you have customized the 3.1 login pages, answer `Y` to the prompt to restore your custom login pages.

   For more information on what happens during this process, see Section 7.3, "Upgrading from Access Manager 3.1 to 3.1 SP1," on page 88.
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.

15 (Conditional) Copy any custom login pages to the `jsp` directory.

`/opt/novell/nids/lib/webapp/jsp`

7.5.2 Upgrading the Windows Identity Server

If you have installed only the Identity Server on the machine, use the following procedure to upgrade the Identity Server. If you have installed both the Identity Server and the Administration Console on the same machine, see Section 7.4.2, "Upgrading the Windows Administration Console," on page 91.

1 (Conditional) Back up any customized JSP pages and related files in the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.

2 (Conditional) If you have modified the `main.jsp` page in 3.1, rename the backed up version of this file to `nidp.jsp`.

3 Download the upgrade file from Novell (http://support.novell.com/patches.html).

  For the filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager31/).

4 Run the executable.

  This is the installation program. When it detects an installed version of the Identity Server, it automatically prompts you to upgrade.

5 At the Introduction page, click *Next*.

6 Accept the license agreement.

7 At the upgrade prompt, click *Continue*.

8 Enter the following information for the Administration Console:

  Administration user ID: Specify the name of the administration user for the Administration Console.

  Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.

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

9 (Conditional) If you have installed the Identity Server with the Administration Console, you are upgrading from 3.1 to 3.1 SP1, and you have customized the 3.1 login pages, allow the upgrade utility to restore your custom login pages.

  For more information on what happens during this process, see Section 7.3, "Upgrading from Access Manager 3.1 to 3.1 SP1," on page 88.

10 Review the summary, click *Install*.

11 (Optional) View the upgrade log file found in the following location:

`C:\Program Files\Novell\log\AccessManagerServer_InstallLog.log`

12 (Conditional) Copy any custom login pages to the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.

7.6 Upgrading the Linux Access Gateway Appliance

Upgrade running time: about five minutes.

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

NOTE: You must use the `lagupgrade.sh` script to upgrade the Linux Appliance. Using the CD to upgrade the Linux Appliance is not supported.

The Linux Appliance 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 Appliance, 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) to download the high bandwidth version. The low bandwidth version of SSL VPN is packaged with the Linux Appliance upgrade file.

NOTE: If you have customized the error pages during 3.0, as mentioned in "Customizing Error Pages on the Gateway Appliance" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*, then copy the images used in the custom error pages to `/var/opt/novell/tomcat5/webapps/LAGERROR/images` from `/var/opt/novell/tomcat4/webapps/LAGERROR/images`, after upgrading to Novell Access Manager 3.1.

This section contains the following information:

7.6.1 Prerequisites

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

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

For the actual filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager31/index.html).

- Copy the Linux Appliance 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 Appliance 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`.

7.6.2 Upgrading the Linux Appliance by Using the Interactive Method

You can interactively upgrade the Linux Appliance 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 the Linux Access Gateway, 2 to upgrade only the SSL VPN server, and 3 to upgrade the Linux Access Gateway and the SSL VPN server installed on the same machine.

   IMPORTANT: If you have installed the Linux Appliance and the SSL VPN server on the same machine:

   - You must select option 3 to upgrade SSL VPN server along with the Linux Appliance. The components must be simultaneously upgraded because the 3.1 version of the Linux Appliance and the 3.0 version of SSL VPN cannot coexist.
   - When you click option 1, the SSL VPN server is also upgraded to 3.1 because there are dependencies. The following message is displayed:

     ```
     You have 3.0 SSLVPN installed. It will now be upgraded to 3.1.
     ```

   - Do not select option 2, because upgrading only the SSL VPN server to 3.1 when the Linux Appliance is running in version 3.0 is not supported. If you select this option, the following message is displayed to you:

     ```
     LAG needs to be upgraded to 3.1 for SSLVPN to be upgraded.
     ```

   ---

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/SP3/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.

7.6.3 Upgrading the Linux Appliance 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 Appliance.

- If you want to upgrade only the Linux Appliance, enter the following command:

  ```
  /chroot/lag/opt/novell/bin/lagupgrade.sh --url http://10.10.10.1/
  publish/upgrades/accessgateway/sp3/lagrpms.tar.gz
  ```

  IMPORTANT: If you have installed the Linux Appliance and the SSL VPN server on the same machine, this option also upgrades the SSL VPN server to 3.1 because the 3.1 version of the Linux Appliance and the 3.0 version of SSL VPN server cannot coexist. The following message is displayed:

  ```
  You have 3.0 SSLVPN installed. It will now be upgraded to 3.1.
  ```

- If you want to upgrade both the Linux Appliance and the SSL VPN server that are installed on the same machine, enter the following command:

  ```
  /chroot/lag/opt/novell/bin/lagupgrade.sh --url http://10.10.10.1/
  publish/upgrades/accessgateway/sp3/lagrpms.tar.gz --upgrade-option LAG
  and SSLVPN
  ```

- If you want to upgrade only the SSL VPN server that is installed with the Linux Appliance, enter the following command:

  ```
  /chroot/lag/opt/novell/bin/lagupgrade.sh --url http://10.10.10.1/
  publish/upgrades/accessgateway/sp3/lagrpms.tar.gz --upgrade-option
  SSLVPN only
  ```

IMPORTANT: Do not use this command to upgrade the SSL VPN server to 3.1 when the Linux Appliance is running version 3.0. This configuration is not supported. If you select this option, the following message is displayed:

```
LAG needs to be upgraded to 3.1 for SSLVPN to be upgraded
```

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.

7.6.4 Upgrading the Linux Appliance by Using the Administration Console

1. In the Administration Console, click *Devices* > *Access Gateways*.
2. Select the name of the Access Gateway (usually the IP address), then click Upgrade.
3. 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
   ```
4. Select either *Upgrade Now* and continue with Step 5, or select *Schedule Upgrade* and skip to Step 9.
5. Click *OK* to start the upgrade.
6. 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.
7. Continue with Step 12.
8. Click *OK*.
9. 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.
10. Click *OK*.
11. Click *Command Status* to view more information about the command.
12. The status of the scheduled command changes from `pending` to `executing` when the upgrade begins.
13. 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.

14 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.

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.

7.6.5 Installing or Updating the Latest Linux Patches

Linux Appliance 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.

WARNING: The Linux Appliance is an appliance. Installing additional packages other than security updates breaks your support agreement with Novell. If you encounter a problem, Novell Support can require you to remove the additional packages and to reproduce the problem before receiving any help with your problem.

NOTE: If you have installed Linux Appliance for the first time on your system, log in as `root` and run `lagupgrade.sh` before you proceed with the following sections.

Installing or Updating the Security Patches

To install or update 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* > *Security Patches* and press Enter.

6 A list of Security patches is displayed.

- If you are installing the Security patches for first time, install all the listed patches by selecting each patch and pressing Enter.

  In the Notify message box, select *OK* and press Enter.

  A + symbol is displayed next to the patch that is selected for installation.
- If you are updating the Security patches, ignore the installed patches, which have `i` symbol next to them, in the list. Install only new patches available in the list by selecting each new patch and pressing Enter.

In the Notify message box, select *OK* and press Enter.

A + symbol is displayed next to the patch that is selected for installation.

7 Click *OK* to proceed with the installation.

8 If any of the following warning messages are displayed, select *Install Patch* and press Enter to proceed with the installation.

- Security update for Linux kernel
- Security update for subdomain-parser
- Security update for opensc and opensc-devel

9 After the installation is completed, click *OK*.

10 Restart Linux Access Gateway for Linux kernel update to take effect.

11 Enter the following to check the logs:

```
tailf /var/log/YaST2/y2log
```

7.7 Converting a NetWare Access Gateway

1 Export the NetWare Access Gateway configuration.

1a In the Administration Console, click *Devices* > *Access Gateways*.

1b Click the name of an Access Gateway to access the Server Details page.

1c Click *Configuration* > *Export*.

1d (Optional) Select to password protect the file by selecting the *Password protect* option and specifying a password.

1e Use your browser's process to save the configuration to a file.

2 (Conditional) To use the same IP address for the Linux Appliance, delete the NetWare Access Gateway from the Administration Console.

3 Install a 3.1 version of the Linux Appliance and import it into the 3.1 Administration Console.

For installation instructions, see Chapter 6, "Installing the Linux Access Gateway Appliance," on page 57.

4 Import the NetWare Access Gateway configuration to the Linux Appliance.

4a In the Administration Console, click *Devices* > *Access Gateways*.

4b Click the name of the Linux Appliance to access the Server Details page.

4c Click *Configuration* > *Import*.

4d Browse to the file and import it.

4e Enter the password if you saved the file with a password, then click *OK*.

5 Assign the Linux Appliance to a cluster.

6 For any of the other NetWare Access Gateway machines that belong to this cluster, delete them from the Administration Console, install Linux Appliance software on the machine, then assign them to the cluster you created in Step 5.

7.8 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

8

This section discusses the following topics related to installation:

8.1 Uninstalling the Identity Server

Uninstalling the Novell® Identity Server is a two-step process:

1. Removing the Identity Server from the Administration Console. See Section 8.1.1, “Deleting Identity Server References,” on page 103.
2. Removing the Identity Server software from the Linux or Windows machine. See Section 8.1.2, “Uninstalling the Linux Identity Server,” on page 104 or Section 8.1.3, “Uninstalling the Windows Identity Server,” on page 104.

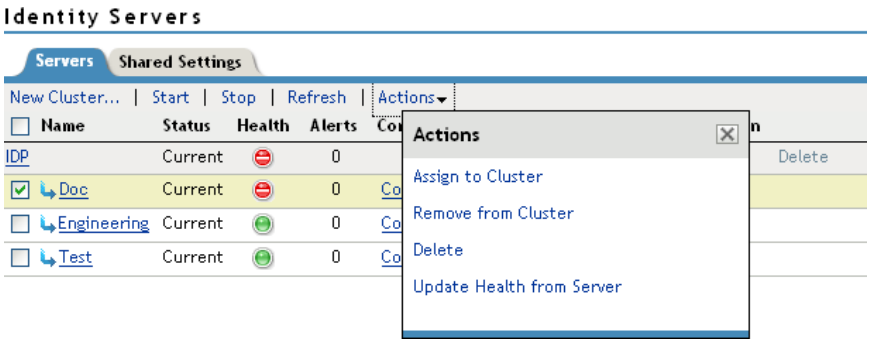
8.1.1 Deleting Identity Server References

As part of the full Identity Server uninstall 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 *Devices* > *Identity Servers*.

2 Select the Identity Server that you want uninstalled, then click *Stop*.

3 Wait for its health to turn red, then select the server and click *Actions* > *Remove from Cluster*.



4 Update the cluster configuration.

5 Select the Identity Server that you are going to uninstall, then click *Actions* > *Delete*.

6 Continue with Section 8.1.2, "Uninstalling the Linux Identity Server," on page 104 or Section 8.1.3, "Uninstalling the Windows Identity Server," on page 104.

8.1.2 Uninstalling the Linux Identity Server

If you have installed the Identity Server with the Administration Console, you can select to only uninstall the Identity Server or to uninstall both.

1 On your Linux Identity Server, 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 Select 2 to uninstall the Identity Server.

5 Enter the name of the admin user.

6 Enter the password of the admin user.

Uninstall removes the Identity Server.

8.1.3 Uninstalling the Windows Identity Server

If you have installed the Identity Server with the Administration Console, you can select to uninstall only the Identity Server or to uninstall both.

1 Exit any applications and disable any virus scanning programs.

2 Access the Control Panel, click *Add or Remove Programs*, then select to remove the AccessManagerServer program.

3 Read the introduction, then click *Next*.

4 Specify the credentials for the admin user, then click *Next*.

5 Select one of the following, then click *Next*.

Complete Uninstall: Select this option if you have installed both the Identity Server and the Administration Console on the same machine and you want to uninstall both.

Uninstall Specific Features: Select this option to uninstall only the Identity Server.

6 (Conditional) If you selected to uninstall specific features, select from the following, then click *Uninstall*.

Administration Console: Select this option to uninstall the Administration Console. You cannot uninstall the Administration Console without also uninstalling the Identity Server.

Identity Server: Select this option to uninstall the Identity Server.

If the unistall fails because the primary Administration Console is not available to validate the credentials, see Section A.5, "Troubleshooting the Uninstall of the Windows Identity Server," on page 167.

8.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall the Identity Server (see Chapter 5, "Installing the Novell Identity Server," on page 53) 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 5, "Installing the Novell Identity Server," on page 53.)
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*.

8.3 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 3.1 SP1 Identity Server 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. Re-image the machine by booting to a CD containing the desired operating system software.

8.4 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 3.1 SP1 Setup Guide*.

IMPORTANT: If you are uninstalling all Access Manager devices, the primary Administration Console should be the last device you uninstall. The uninstall programs for the other devices contact the primary Administration Console and validate the admin's credentials before allowing the device to be removed.

Select the process that corresponds to your platform:

- Section 8.4.1, “Uninstalling the Linux Administration Console,” on page 106
- Section 8.4.2, “Uninstalling the Windows Administration Console,” on page 106

8.4.1 Uninstalling the Linux 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	Novell Access Manager Administration
2	Novell Identity Server
3	Traditional Novell SSL VPN Server
4	ESP-enabled Novell SSL VPN Server
5	Forcefully uninstall all components (not recommended) Use this option after a failed installation; otherwise use 1 through 4 to uninstall Access Manager components. **WARNING:** Using this option when you have a cluster of Administration Consoles can cause synchronization and update problems with the configuration store. If you use it to remove an Administration Console, you need to run dsrepair to remove the missing replica from the replica ring.
Q	Quit without uninstalling

8.4.2 Uninstalling the Windows Administration Console

When you uninstall the Administration Console, any other Access Manager components on the machine must also be uninstalled.

1. Exit any applications and disable any virus scanning programs.
2. Access the Control Panel, click *Add or Remove Programs*, then select to remove the AccessManagerServer program.
3. Read the introduction, then click *Next*.
4. Specify the credentials for the admin user, then click *Next*.
5. Click *Complete Uninstall*, then click *Next*.

   The uninstall begins. If the uninstall hangs, see Section A.5, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 167.

8.5 Uninstalling the SSL VPN Server

NOTE: If you have installed SSL VPN and the Linux Access Gateway on the same machine, you cannot uninstall the SSL VPN server.

Before you uninstall the SSL VPN server installed with the Identity Server, you must first remove it from the cluster configuration, then delete it from the Administration Console.

- Section 8.5.1, "Deleting the Server from the Administration Console and from the Cluster," on page 107
- Section 8.5.2, "Uninstalling the Server," on page 107

8.5.1 Deleting the Server from the Administration Console and from the Cluster

1. In the Administration Console, *Devices* > *Devices* > *SSL VPNs*.
2. Select the SSL VPN server that you want to uninstall.
3. (Optional) If the server is part of a cluster, select *Actions* > *Remove from Cluster*.
4. Update the cluster configuration.
5. Select the SSL VPN Server that you want to uninstall, then click *Actions* > *Delete*.

8.5.2 Uninstalling the Server

IMPORTANT: If you have installed the high-bandwidth SSL VPN key, uninsall the key before proceeding to uninstall the SSL VPN server. For more information on uninstalling the high-bandwidth key, see Section 8.6, "Uninstalling the RPM Containing Key For High Bandwidth SSL VPN," on page 108.

1. Browse and locate the uninstall script `uninstall.sh`.

   The uninstall script is located in the root directory of the installation CD or in the installation directory.
2. At the command prompt, run the following command:

   ```
   ./uninstall.sh
   ```

   NOTE: If you want to run the uninstallation script directly from the CD, insert the CD, then run the command.
3. Do one of the following, depending on your installation type:
   - Enter 4 to uninstall the Traditional Novell® SSL VPN.
   - Enter 5 to uninstall the ESP-enabled Novell SSL VPN.

NOTE: If SSL VPN fails to uninstall gracefully, use option 6 to forcefully uninstall SSL VPN.

8.6 Uninstalling the RPM Containing Key For High Bandwidth SSL VPN

1. Log in as `root`.
2. Enter the following command to uninstall the RPM for the high bandwidth version of SSL VPN:

   ```
   rpm -e novl-sslvpn-hb-key-3.1.0-0.noarch.rpm
   ```

Migrating from iChain to Access Manager

9

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.

9.1 Understanding the Differences between iChain and Access Manager

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

9.1.1 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 and Windows. Access Manager has the following components:

- **Administration Console:** Installed on Linux or Windows 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 or Windows and provides single sign-on authentication, federation with other identity providers, and role and policy distribution. Roles are assigned at authentication time and filter though all components, thus simplifying the definition of authorization policies.
- **Access Gateway:** Installed on Linux 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 need to make is which Access Manager components you need (an Administration Console and Identity Server 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 2, "Novell Access Manager Product Overview," on page 15. For some deployment ideas, see Section 3.1, "Recommended Installation Scenarios," on page 33.

9.1.2 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 9-1 *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
CardSpace	Not supported	CardSpace protocol with personal and managed card support
WS Federation	Not supported	Federation with SharePoint servers
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

Feature	iChain	Access Manager
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, Windows
Citrix* integration	Proxy ICA traffic	SSL VPN

9.2 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 3.1, "Recommended Installation Scenarios," on page 33.
- 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 9.2.1, "Possible Migration Strategies," on page 111.
- 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 9.2.2, "Outlining the Migration Requirements for Each Resource," on page 118.

9.2.1 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

A simple migration works well in the following network environment:

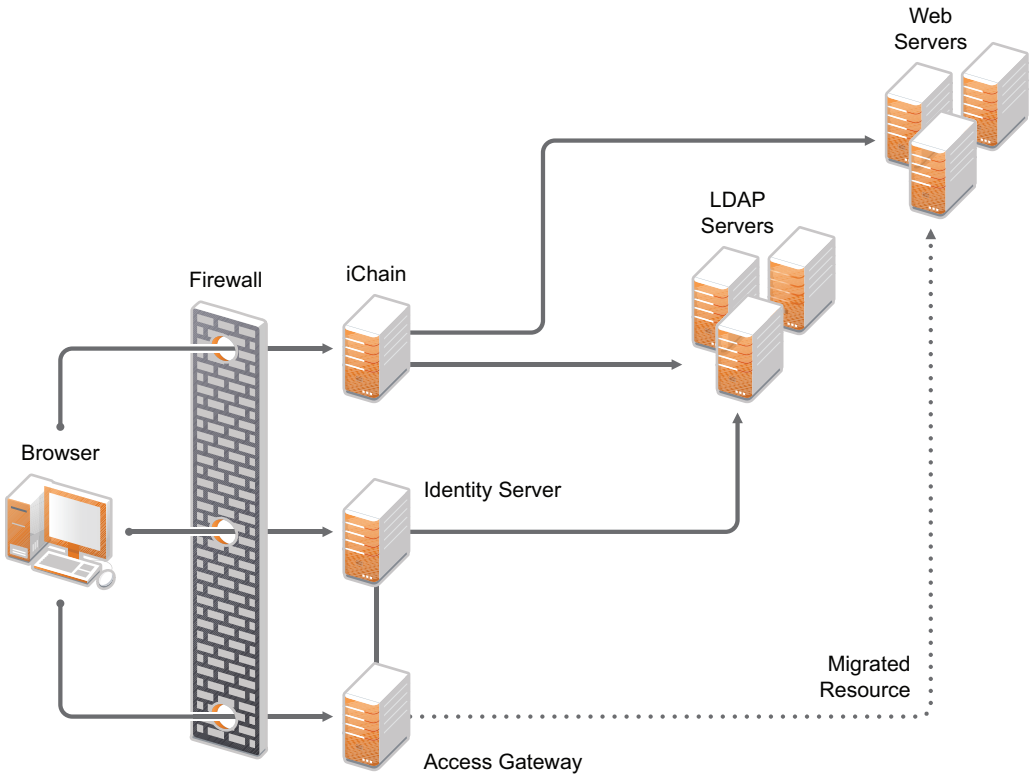
- You use iChain to protect a few Web servers with only one or two applications each.
- The policies that control single sign-on and access are simple.

- 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 9-1 *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 33.
- ❑ You need to configure your firewall to allow access to the Access Manager components. See “Setting Up Firewalls” in the *Novell Access Manager 3.1 SP1 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 3.1 SP1 Setup Guide*.
- ❑ Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See Section 9.3.3, “Configuring the Identity Server for Authentication,” on page 121.
- ❑ Configure the Access Gateway to have the same device settings as iChain. See Section 9.3.4, “Configuring System and Network Settings,” on page 124
- ❑ Migrate an accelerator with its resources from iChain to the Access Gateway. See Section 9.3.5, “Migrating the First Accelerator,” on page 127.
- ❑ Remove iChain. See Section 9.3.9, “Removing iChain,” on page 150.

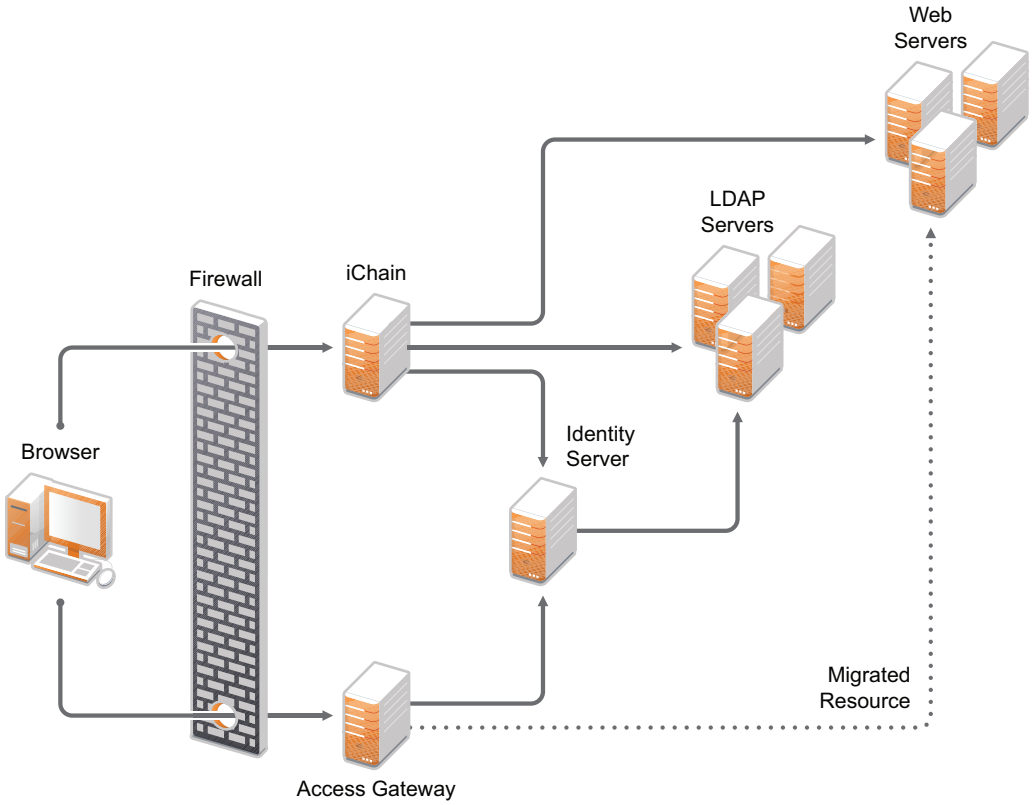
A Phased Migration

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 9-2 illustrates the network layout for this type of migration.

Figure 9-2 *Network Setup for a Phased Migration*

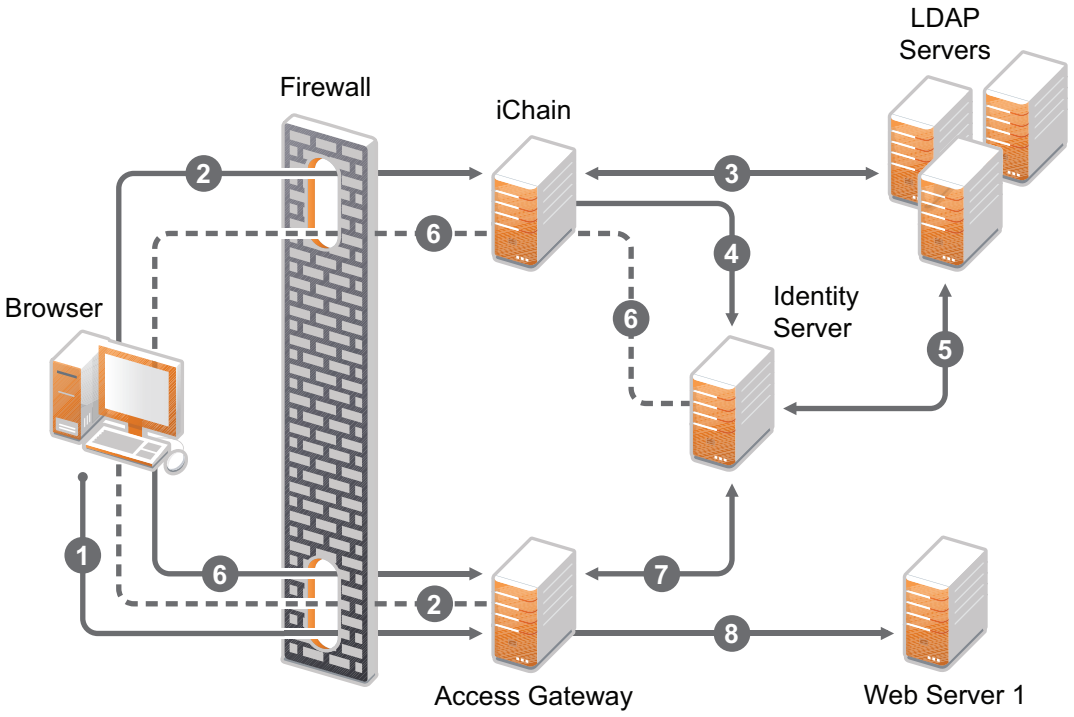


The phased migration uses iChain for authentication and single sign-on to the Identity Server. To do this, you configure the Identity Server to be a restricted resource of iChain, and you configure the Access Gateway to trust the Identity Server as its identity provider. The Access Gateway communicates 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 9-3 illustrates this flow. The dotted lines represent redirected requests.

Figure 9-3 *The Flow of a Client Request to a Migrated Resource*



1. The user sends a request for a protected resource that has been migrated to the Access Gateway. The DNS server directs the request to the Access Gateway.
2. The Access Gateway determines that the user needs to be authenticated and directs the request to the Identity Server. Because the Identity Server is a restricted resource of iChain, the request is redirected to iChain
3. iChain prompts the user for login information and validates the user's login credentials with the LDAP user store.
4. To enable single sign-on, iChain uses OLAC to forward a basic authentication header to the Identity Server, and the Identity Server is configured to accept the basic authentication header instead of a name and password for authentication. (Form Fill could be used instead of OLAC and basic authentication.)
5. The Identity Server validates the name and password with the LDAP user store.
6. The Access Gateway is sent the credential artifact.
7. The Access Gateway sends the artifact to the Identity Server and uses it to retrieve the authentication information and policy information specific to that user.
8. If the user's credentials match the requirements, the Access Gateway grants the user access to the protected 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 117.

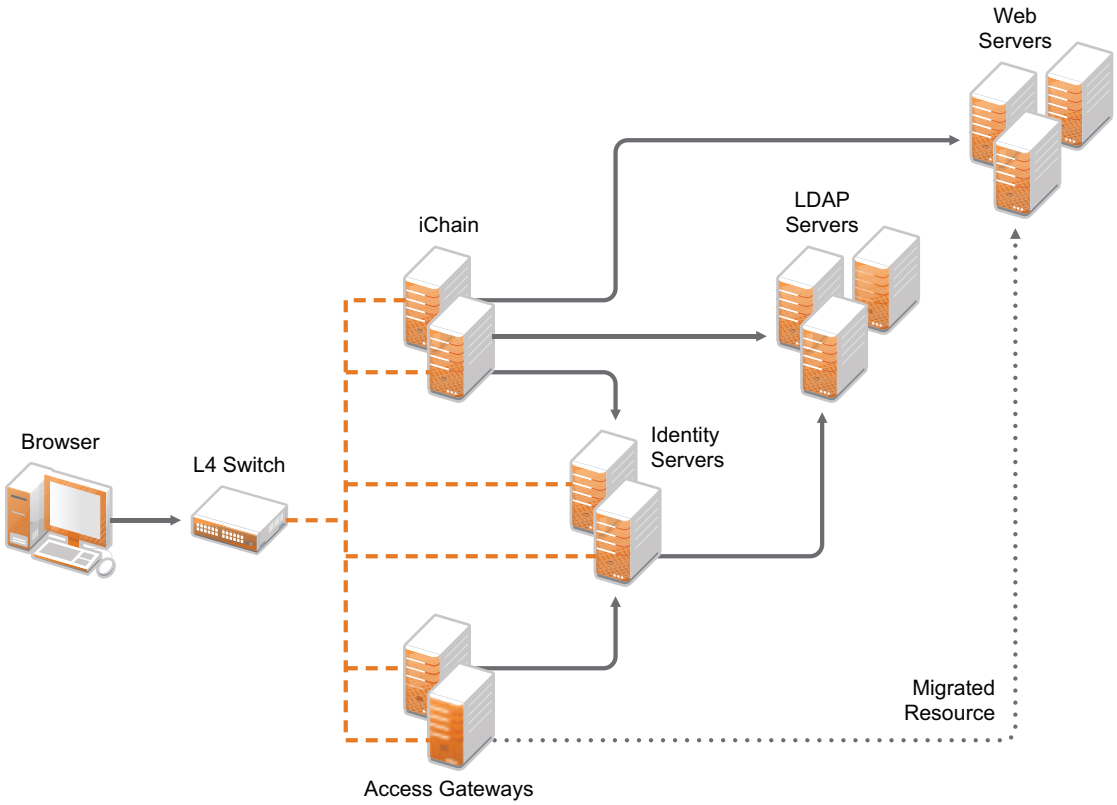
Major Tasks

- ❑ 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 3.1 SP1 Setup Guide*.
- ❑ Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See Section 9.3.3, "Configuring the Identity Server for Authentication," on page 121.
- ❑ Configure the Access Gateway to have the same device settings as iChain. See Section 9.3.4, "Configuring System and Network Settings," on page 124.
- ❑ Migrate an accelerator with its resources from iChain to the Access Gateway. See Section 9.3.5, "Migrating the First Accelerator," on page 127.
- ❑ 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 9.3.6, "Enabling Single Sign-On between iChain and Access Manager," on page 135.

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 9-4 *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 by 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 3.1 SP1 Setup Guide*.
- ❑ Set up a group of Access Gateways. See "Clustering Access Gateways" in the *Novell Access Manager 3.1 SP1 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 9.2.2, "Outlining the Migration Requirements for Each Resource," on page 118

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.

9.2.2 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 118
- “Accelerator” on page 119
- “Protected Resources” on page 119
- “Applications” on page 120

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 3.1 SP1 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 the *Novell Access Manager 3.1 SP1 SSL VPN Server 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.

9.3 Migrating Components

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

9.3.1 Setting Up the Hardware and Installing the Software

For details on hardware requirements and possible software configurations, see "Installation Requirements" on page 33.

For installation instructions, see the following:

- "Installing the Access Manager Administration Console" on page 43
- "Installing the Novell Identity Server" on page 53
- "Installing the Linux Access Gateway Appliance" on page 57

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 3.1 SP1 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 3.1 SP1 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 by using certificates created by the Access Manager CA, see "Enabling SSL Communication" in the *Novell Access Manager 3.1 SP1 Setup Guide*.
- For information on how to use certificates generated by external CAs, see "Using Externally Signed Certificates" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

9.3.2 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:

- "Health Checks for the Access Gateway" in the *Novell Access Manager 3.1 SP1 Setup Guide*
- "Configuration Tips for the L4 Switch " in the *Novell Access Manager 3.1 SP1 Setup Guide*

9.3.3 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 121
- "Migrating the User Store Configuration" on page 122
- "Enabling the User Stores for Authentication Methods" on page 123
- "Migrating Custom Login Pages" on page 123

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 122. 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 122. 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 3.1 SP1 Policy Management 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 3.1 SP1 Policy Management 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 "Configuring Mutual SSL (X.509) Authentication" in the *Novell Access Manager 3.1 SP1 Identity Server 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 "Configuring for RADIUS Authentication" in the *Novell Access Manager 3.1 SP1 Identity Server 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 specify at least one IP address for your LDAP server. If the LDAP directory has been replicated to other servers, specify 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 123.

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 123. Otherwise, continue with Section 9.3.4, "Configuring System and Network Settings," on page 124.

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 "Customizing the Identity Server Login Page" in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

9.3.4 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 Appliance, see "Setting the Date and Time" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.
- 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 124
- "Gateways" on page 124
- "Telnet" on page 125
- "IP Addresses" on page 125

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.

Telnet

iChain Path	Access Gateway Path
Must be enabled from the command line: `set listener telnet enable=yes`	N/A

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 the Access Gateway and use SSH instead, which supports data encryption. The Linux Access Gateway does not support the Telnet and SSH options in the Administration Console. You must use YaST to enable them.

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 3.1 SP1 Administration Console 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 Web App > System > Timezone	Access Gateways > Edit > Date & Time

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 Access Gateway have the same options. You can enter the URL where the upgrade files are located and then select to upgrade immediately, or you can schedule the upgrade for a later date. For more information, see Section 7.6, “Upgrading the Linux Access Gateway Appliance,” on page 95.

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 > 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
Web App > System > SNMP	Not supported

9.3.5 Migrating the First Accelerator

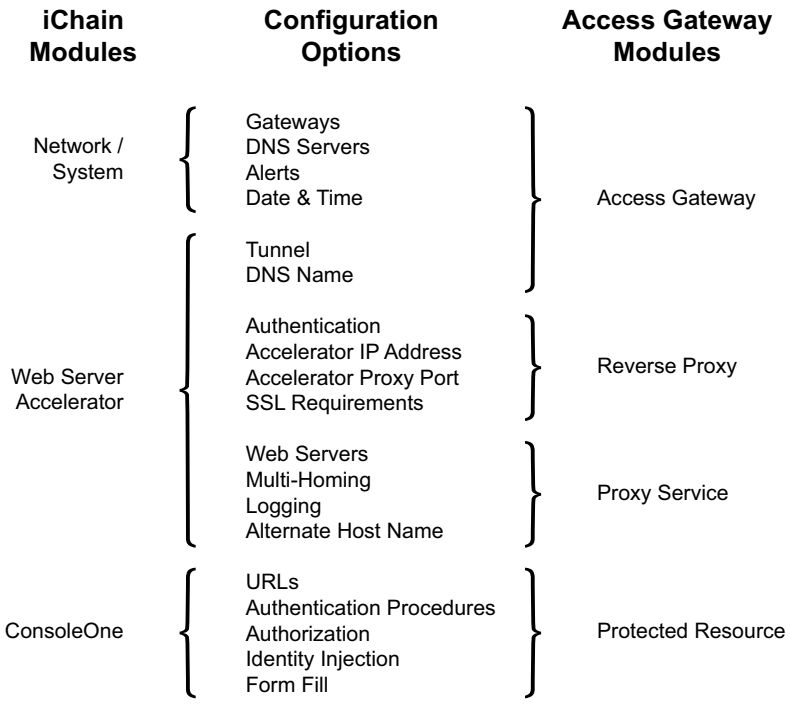
For your first accelerator, we suggest that you select the one with the fewest configuration requirements. If possible, select one that has only a few child accelerators (path-based or domain-based multi-homing accelerators) and does not require Form Fill or have complex access control policies.

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 the Access Gateway, you have a reverse proxy with proxy services that have protected resources. Figure 9-5 illustrates the configuration differences between iChain and Access Gateway.

Figure 9-5 *Configuration Options for iChain and the Access Gateway*



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 128

- "Migrating the Parent Accelerator" on page 128
- "Migrating the Path-Based Multi-Homing Accelerators" on page 131
- "Migrating the Protected Resources" on page 132
- "Testing the Migrated Resources" on page 134
- "Enabling User Access to the Migrated Resources" on page 134

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 3.1 SP1 Administration Console Guide*.
- You can use the certificate authority in Access Gateway to create the certificates. For instructions, see "Creating Certificates" in the *Novell Access Manager 3.1 SP1 Administration Console 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 9.3.3, "Configuring the Identity Server for Authentication," on page 121.

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

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

6 Click *OK* and configure the proxy service.

iChain Accelerator Option	Proxy Service Option
DNS Name	*Published DNS Name*
	Description
Cookie domain	*Cookie Domain*

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

iChain Accelerator Option	HTTP Options
Allow Pages to Be Cached at the Browser	*Allow Pages to Be Cached by the Browser*
Forward Browser IP address in Request Header [X-Forwarded-For]	*Enable X-Forwarded-For*
N/A	Enable Custom Cache Control Header: 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 Option	Web Servers Option
Do not cache objects with ? in the URL	*Enable Caching of Objects with a Question Mark*
Do not cache objects with /cgi in the path	*Enable Caching of Objects with CGI in The Path*
Ignore Refresh Requests from Browser	*Refresh Request from Browser*
	Enable Filter Cookies
Enable Initial Splash Screen	*Enable Initial Splash Screen*
Act as a Single User (Private) Cache	*Act as Single User (private) Cache*
Enable Read-Ahead Images Embedded in the Page	*Enable Read-Ahead Images Embedded in the Page*
	Maximum Number of Concurrent Read-Ahead Requests
Configure > *Tuning* > *Cache Freshness*	*Cache Freshness*: 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 Option	Web Servers Option
Return Error if Host Name Sent by Browser Does Not Match above DNS Name	*Error on DNS Mismatch*
Insert button for Web server addresses	*New* in the *Web Server List* table
Secure Exchange Options > *Enable secure access between the iChain Proxy and the Origin Web Server*	*Connect Using SSL*
Secure Exchange Options > *Port (field between the iChain proxy and the Origin Web Server)*	*Connect Port*
	Web Server Trusted Root

iChain Accelerator Option	Web Servers Option
Authentication Options > [Name of Profile] > Modify	*SSL Mutual Certificate*: 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 131. If doesn't have any child accelerators, continue with "Migrating the Protected Resources" on page 132.

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

3 Click OK and fill in the following fields:

iChain Accelerator Option	Reverse Proxy Option
Multi-homing Options > Remove sub-path from URL	*Remove Path on Fill*
	Reinsert Path in "set-cookie" Header

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 132.

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 132
- "Migrating a Restricted Resource" on page 133
- "Migrating a Secure Resource" on page 134

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 public 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.

IMPORTANT: iChain allows for protected paths such as `/novell/*.css`. Access Manager does not allow a protected path to have a wildcard anywhere except at the end of the path.

---

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 133, or to test the resource you have migrated, continue with "Testing the Migrated Resources" on page 134.

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 restricted 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 or HTTPS 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 121.

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 134, or to test the resource you have migrated, continue with "Testing the Migrated Resources" on page 134.

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 9.3.7, “Migrating Resources with Special Configurations,” on page 138.

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 9.3.6, “Enabling Single Sign-On between iChain and Access Manager,” on page 135.

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.

9.3.6 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, complete Step 1 through Step 6, then see "Using Form Fill instead of OLAC for Single Sign-On" on page 136.

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 137.

6 To save the configuration, click *OK*.

- To use OLAC for single sign-on, continue with Step 7.
- To use Form Fill, see "Using Form Fill instead of OLAC for Single Sign-On" on page 136.

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. It should 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.

9.3.7 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

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 9-2 *Form Fill Policy Tags*

Tag or Tag/Attribute	Access Gateway Field
`<formName>`	In the *Form Selection* section, select *Form Name* and specify the value in the text box.
`<formNum>`	In the *Form Selection* section, select *Form Number* and specify the number in the text box
`<cgiCriteria>`	In the *Form Selection* section, select the *CGI Matching Criteria* field. Copy the text between the `<cgiCriteria>` and the `</cgiCriteria>` tags into the text box.
`<formCriteria>`	In the *Form Selection* section, select the *Page Matching Criteria* field. Copy the text between the `<formCriteria>` and the `</formCriteria>` tags into the text box.
`<input name="">`	Specify the value in the *Input Field Name* of the *Fill Options* section.

Tag or Tag/Attribute	Access Gateway Field
`<select name="">`	Specify the value in the *Input Field Name* of the *Fill Options* section.
`<input type="">`	Select the type in the *Input Field Type* field of the *Fill Options* section. For an `<input>` tag, select *Text, Password, Checkbox*, or *Radio Button*.
`<select type="">`	Select the type in the *Input Field Type* field of the *Fill Options* section. For a `<select>` tag, select *Select*.
`<input value=""> or <select value="">`	To specify a value, use the *Input Field Value* field of the *Fill Options* section. You can select one of the following value types: ◆ **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 prompted 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 *Data Conversion* field of the *Fill Options* section. Select the appropriate value from the drop-down list.
`<injectStaticValue>`	To inject a static value, select *Insert Text in Header* in the *Submit Options* section.
`<debugPost/>`	To enabled a debug post, select the *Debug Mode* field in the *Submit Options* section.
`<maskedPost/>`	To mask the post data, select the *Mask Data* field in the *Submit Options* section.
`<javaScript>`	To retain JavaScript* from the original page, select the *Functions to Keep* field in the *Submit Options* section. The *Enable JavaScript Handling* field must be enabled to modify the *Functions to Keep* field. Copy the text between the `<javaScript>` and the `</javaScript>` tags into the text box of the *Functions to Keep* field.
`<scriptForPost>`	To specify additional functions to be executed prior to posting the form, select the *Statements to Execute on Submit* field of the *Submit Options* section. The *Enable JavaScript Handling* option must be enabled to modify the *Statements to Execute on Submit* field. Copy the text between the `<scriptForPost>` and the `</scriptForPost>` tags into the text box.

Tag or Tag/Attribute	Access Gateway Field
<errorRedirect>	To redirect the user when an LDAP or NSSS error occurs, select the *Redirect to URL* field of the *Error Handling* section. Copy the text between the <errorRedirect> and </errorRedirect> tags to the text box of the *Redirect to URL* 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.

Table 9-3 *Form Login Failure Policy Tags*

Tag or Tag/Attribute	Access Gateway Field
<formName>	In the *Form Selection* section, select *Form Name* and specify the value in the text box.
<formNum>	In the *Form Selection* section, select *Form Number* and specify the number in the text box
<cgiCriteria>	In the *Form Selection* section, select the *CGI Matching Criteria* field. Copy the text between the <cgiCriteria> and the </cgiCriteria> tags into the text box.
<formCriteria>	In the *Form Selection* section, select the *Form Matching Criteria* field. Copy the text between the <formCriteria> and the </formCriteria> tags into the text box.
<redirect>	To redirect the user on login failure, select the *Redirect to URL* field in the *Login Failure Processing* section. Copy the URL between the <redirect> and </redirect> tags to the text box of the *Redirect to URL* field.
<deleteRemembered>	To delete the user's stored data for a Form Fill policy, select the *Clear Shared Secret Data Values from Policy* in the *Login Failure Processing* section.
<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 3.1 SP1 Policy Management 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 148.

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 141
- "Migrating a Policy for the Authorization Header" on page 142
- "Migrating a Policy for Custom Header Variables" on page 142
- "Migrating a Policy for a Query String" on page 143
- "Configuring a Resource to Use an Identity Injection Policy" on page 143

Policy Comparison between iChain and Access Gateway

The following table lists the iChain feature and the equivalent Access Gateway feature.

Table 9-4 *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 3.1 SP1 Policy Management 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 142
   - "Migrating a Policy for a Query String" on page 143
8. To assign this policy to a protected resource, see "Configuring a Resource to Use an Identity Injection Policy" on page 143.

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, the 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 143.

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 143.

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 Server 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 3.1 SP1 Policy Management Guide*. For other methods, see "Creating Access Gateway Authorization Policies" in the *Novell Access Manager 3.1 SP1 Policy Management 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 144
- "Creating an Authorization Policy with an Allow and a Deny Rule" on page 145
- "Protecting the Resource with the Authorization Policy" on page 147

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 145.

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 the 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 3.1 SP1 Policy Management Guide*.

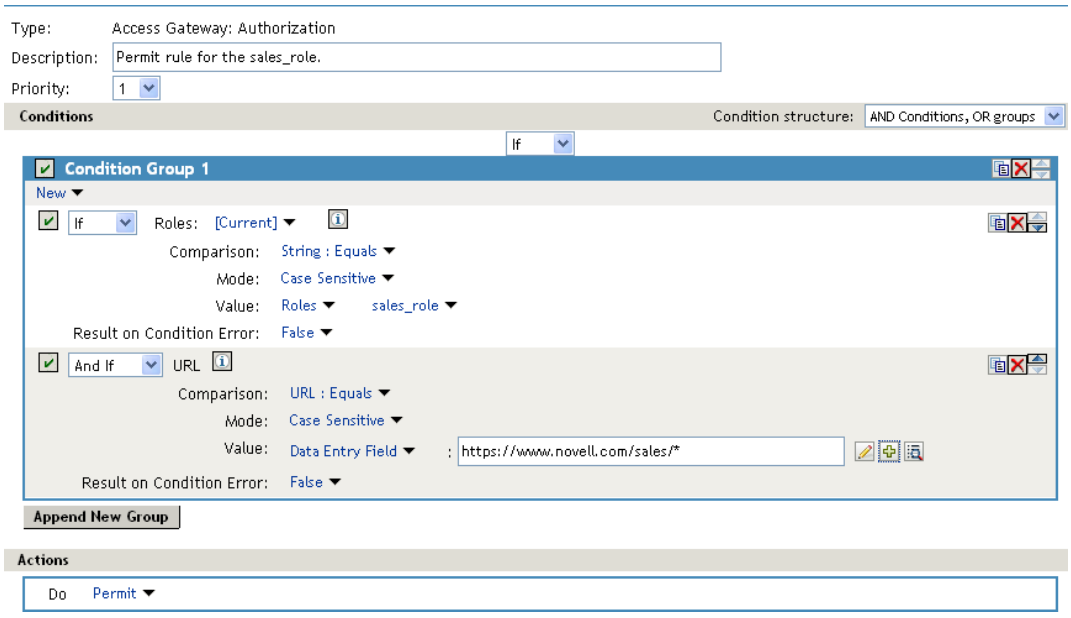
In iChain, the default behavior for secure resources was to deny access unless an ACLCheck rule allowed access. The behavior is different in an Access Gateway. After a user has authenticated, the default behavior is to allow access to resources. Therefore, to restrict access to a resource, you need to 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*.



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*.

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*.

Mode: Select *Case Sensitive*.

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 *Devices > 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 *Devices > Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > HTML Rewriting*.

Table 9-5 shows where to place the information from the iChain file in the Access Gateway profile.

Table 9-5 *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

iChain File Section	Access Gateway Profile Location
`[Alias Host Names]—internal rewriter only`	*Additional URL List* An additional section, *Exclude URL List*, allows you to list the URLs that you do not want rewritten.
`[URL]`	*[Profile Name] > If Requested URL Is*
`[Exclude]`	*[Profile Name] > And Requested URL Is Not*
`[Mime Content-type]`	*[Profile Name] > And Document Content-Type Header Is*
`[Javascript Variables]`	*[Profile Name] > Then Variable or Attribute Name to Search for Is* This option is available only for a Word profile.
`[Javascript Calls]`	*[Profile Name] > And JavaScript Method to Search for Is* This option is available only for a Word profile.
`[Replace]`	*[Profile Name] > Additional Strings to Replace*

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 3.1 SP1 SSL VPN Server 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 3.1 SP1 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 the *Novell Access Manager 3.1 SP1 SSL VPN Server 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 3.1 SP1 Policy Management 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 3.1 SP1 Policy Management Guide*.

9.3.8 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 149
- "Changing the IP Address of an Access Gateway" on page 150

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 *Devices* > *Identity Servers* > *[Name of Server]*, then click the *Management IP Address* link.
   - For an SSL VPN, click *Devices* > *SSL VPNs* > *[Name of Server]*, then click the *Management IP Address* link.
   - For a J2EE Agent, click *Devices* > *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 Appliance" in the *Novell Access Manager 3.1 SP1 Administration Console Guide* for instructions.

If the new IP address is in a different subnet:

1. In the Administration Console, click *Devices* > *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.3.2, "Triggering an Import Retry," on page 159.

9.3.9 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 3.1 SP1 Identity Server 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

A.1 Troubleshooting an Identity Server Installation

A.1.1 The Identity Server Fails to Import into the Administration Console

Check for the following problems if you have installed your Administration Console on one machine and the Identity Server on another machine:

- Is the firewall enabled on the Administration Console or the Identity Sever. The firewall needs to have the following ports opened between the machines so that the Identity Server can import into the Administration Console:

  8444
  1443
  289
  524
  636

  The Identity Server firewall also needs to have ports 8080 and 8443 open between the server and the clients in order for the clients to log into the Identity Server. For more information about firewalls and ports, see “Setting Up Firewalls” in the *Novell Access Manager 3.1 SP1 Setup Guide*.
- Time needs to be synchronized between the two machines. Make sure that both machines have been configured to use a Network Time Protocol server.

A.1.2 Check the Installation Logs

Linux Installation Logs

The installation logs are located in the `/tmp/novell_access_manager` directory. The following log files should contain useful content. Check them for warning and error messages.

Table A-1 *Installation Log Files for the Linux Identity Server*

Log File	Description
`inst_nids_<date&time>.log`	Contains the messages generated for the Identity Server module.
`inst_main_<date&time>.log`	Contains the Tomcat messages generated during the installation.
`inst_jcc_<date&time>.log`	Contains the messages generated for the communications module.
`inst_audit_<date&time>.log`	Contains the messages generated for the Novell auditing components.
`inst_devman_<date&time>.log`	Contains the messages generated for the interaction between the Identity Server and the Administration Console.

Windows Installation Logs

The installation logs are located in the `\Program Files\Novell\Tomcat\webapps \nps\WEB-INF\logs\install` directory. The following log files should contain useful content. Check them for warning and error messages.

Table A-2 *Installation Log Files for the Windows Identity Server*

Log File	Description
`basejar_InstallLog.log`	Contains the messages generated when installing the Identity Server JAR files.
`base_InstallLog.log`	Contains the messages generated during the installation of the Identity Server.
`nauditjar_InstallLog.log`	Contains the messages generated when installing the Novell Audit JAR files.
`nauditjar_InstallLog.log`	Contains the messages generated for the Novell auditing components.
`NIDS_Pluginjar_InstallLog.log`	Contains the messages generated when installing the Identity Server plug-in JAR.
`NIDS_Plugin_InstallLog.log`	Contains the messages for the plug-in component.
`NMASjar_InstallLog.log`	Contains the messages generated when installing the NMAS JAR files.
`NMAS_InstallLog.log`	Contains the messages for the NMAS component.

A.2 Troubleshooting a Linux Access Gateway Appliance Installation

This section contains the following troubleshooting scenarios for Linux Access Gateway:

A.2.1 Some of the New Hardware Drivers or Network Cards 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 6, “Installing the Linux Access Gateway Appliance,” on page 57.
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 After Reinstalling the Access Gateway, SSL Fails

Sometimes after installing an existing Access Gateway, the gateway starts before the SSL certificates are sent to the gateway. When this happens, you need to trigger an update so that the newest configuration is sent to the Access Gateway.

1. In the Administration Console, click *Auditing* > *Troubleshooting*.
2. Scroll to the *Current Access Gateway Configurations* section, select the reinstalled Access Gateway, then click *Re-push Current Configuration*.

A.2.3 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).

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 through 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.2.4 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 through 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_addres*>*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.2.5 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, use the following command to add the hostname and IP address mapping to the `/etc/hosts` file:

hosts <*ip-address*> <*host_name*>

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.2.6 Verifying Component Installation

1 Check the install logs (`inst_`*`component-name_date_time`*`.log`) at the following location:

```
/tmp/novell_access_manager
```

For more information on collecting logs, see "Linux Access Gateway Logs" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*.

2 If the logs contain errors, send the logs to Novell® Support.

A.3 Troubleshooting the Access Gateway Import

When you install 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.3.1, "Repairing an Import," on page 159
- Section A.3.2, "Triggering an Import Retry," on page 159
- Section A.3.3, "Fixing Potential Configuration Errors on the Access Gateway Appliance," on page 160
- Section A.3.4, "Troubleshooting the Import Process," on page 161

A.3.1 Repairing an Import

If the Access Gateway does not appear in the Administration Console within ten minutes of installing an Linux 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 3.1 SP1 Setup Guide*.
2. In the Administration Console, click *Devices* > *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.3.2, "Triggering an Import Retry," on page 159.
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 161 and report the problem to Novell Support.

A.3.2 Triggering an Import Retry

If the import process failed to start (see Step 3 on page 162), 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.

Reimporting the Linux Access Gateway Appliance

1. Verify that 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.

   If the `ping` command is unsuccessful, fix the network communication problem before continuing.
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 Console.
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 Type *I* if you want to restore the initial values configured during the installation.

9b Type *C* if you want to restore the current configuration of Access Gateway.

9c Press Enter.

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 "Creating a Reverse Proxy and Proxy Service" in the *Novell Access Manager 3.1 SP1 Access Gateway Guide*
- If the Access Gateway was part of a cluster, add it to the cluster. For more information, see "Configuring a Cluster" in the *Novell Access Manager 3.1 SP1 Setup Guide*.
- Configure the certificate for SSL listener. For more information, see "Configuring the Access Gateway for SSL" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

A.3.3 Fixing Potential Configuration Errors on the Access Gateway Appliance

Auto-import fails when the hostname is not configured properly or is not resolvable. To fix these potential problems, see the following sections:

- "Hostname Is Not Configured Properly" on page 160
- "Hostname Is Not Resolvable" on page 160

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. See Section A.2.5, "Manually Configuring the Hostname, Domain Name, and DNS Server," on page 157.

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. See Section A.2.5, "Manually Configuring the Hostname, Domain Name, and DNS Server," on page 157.

A.3.4 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 161
- "Locating the Log Files" on page 161
- "Determining Where the Error Occurred" on page 162

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 and the CLI-updated settings.
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:

  For Linux: `/opt/novell/devman/share/logs/app_sc.0.log`

  For Windows: `C:\Program Files\Novell\log\app_sc.0.log`

- Tomcat Log on the Administration Console:

  For Linux: `/var/opt/novell/tomcat5/logs/catalina.out`

  For Windows: `C:\Program Files\Novell\Tomcat\logs\stdout.log`

- JCC Log on the 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:
   - **1a** Log in as `root`.
   - **1b** Start nash.
   - **1c** Enter the following command:

     ```
     show deviceManager
     ```

   - **1d** Verify that the *bind-address* field is set to a bound address on the server.
   - **1e** 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:
   - **2a** Verify that the `/var/novell/cfgdb/.current/config.xml` file contains the correct information set from the CLI.
   - **2b** 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.3.2, “Triggering an Import Retry,” on page 159.
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
   proxyHttpURLConnection
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
   proxyHttpURLConnection
INFO: Response code: 200 OK
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
   proxyHttpURLConnection
INFO: response body size: 5958 bytes
Jan 30, 2006 3:21:34 PM com.novell.jcc.handler.ProxyHandler
   proxyHttpURLConnection
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
   sendAlert
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.4 Troubleshooting an Upgrade

A.4.1 Pending Commands After an Upgrade

Occasionally during an upgrade, the response to an upgrade command is lost, even though the command succeeds. This results in a pending status for the command, and this status is never updated to success.

To clear a pending command:

1. In the Administration Console, click *Access Manager* > *Access Gateway*.
2. Click the *Commands* link.
3. Select the pending command, then click *Delete*.
4. Click *Close*.

A.4.2 Troubleshooting a Linux Administration Console Upgrade

If your server has multiple IP address, you might see the following error message during a Linux 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 occurs when 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 the multiple directory database (MDB) driver does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address by creating an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

```
/etc/mdb.conf
```

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameters:

```
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, you do not encounter this error message when you upgrade.

A.4.3 Certificate Command Failure

Certificate commands are generated when you upgrade the Administration Console, and you should ensure that they have completed successfully. In the Administration Console, click *Security* > *Command Status*.

If a certificate command fails, note the store, then click *Auditing* > *Troubleshooting* > *Certificates*. Select the store, then click *Re-push certificates* to push the certificates to the store.

A.4.4 New Alerts for Auditing Do Not Appear after Upgrading to Linux Access Gateway 3.1

If you upgrade your Linux Access Gateways from 3.0 SP4 to 3.1, the three new alerts for auditing (*Failure in Audit, Stopping Services, Failure in Audit, Will lose events, but continuing services*, and *Failure in Audit, Server is offline*) are not available. This issue is resolved in Linux Access Gateway 3.1 IR1 and later.

To solve this problem when the Access Gateway is not a member of a cluster, you need to trigger a reimport. For instructions on triggering the reimport, see "Triggering an Import Retry" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/b5wvz2g.html#b3ez46v).

If the Access Gateway is a member of a cluster, complete the following steps:

1. Remove a member from the cluster.
2. Verify whether the Access Gateway has the new alerts.

   In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *Alerts* > *default*.
3. (Conditional) If the Access Gateway has the new alerts, add it to the cluster, then assign it to be the primary cluster member.
4. (Conditional) If the Access Gateway does not have the new alerts, delete the Access Gateway from the Administration Console, reinstall the Access Gateway, add it to the cluster, then assign it to be the primary cluster member.

A.5 Troubleshooting the Uninstall of the Windows Identity Server

When you uninstall a Windows Identity Server, the uninstall program prompts you for the credentials of the admin user for the Administration Console. If the primary Administration Console is not available for the authentication request, the uninstall fails.

To force the uninstall program to skip the authentication request, enter the following command:

```
\Program
Files\Novell\Uninstall_AccessManagerServer\UninstallAccessManagerServer.
exe -DAM_INSTALL_AUTH_BYPASS=true
```

Modifications Required for a 3.0 Login Page

B

The following 3.0 `login.jsp` file has been modified to display line numbers. The lines that require modifications have been highlighted, and a few extra spaces have been added to allow for a better display of the text. For a description of the modifications that need to be made, see Section 7.2.4, “Modifying 3.0 Login Pages for 3.1 SP1,” on page 81.

```
1. <%@ page language="java" %>
2. <%@ page pageEncoding="UTF-8" contentType="text/html; charset=UTF-8"%>
3. <%@ page import="com.novell.nidp.common.provider.*" %>
4. <%@ page import="java.util.*" %>
5. <%@ page import="java.net.*" %>
6. <%@ page import="com.novell.nidp.*" %>
7. <%@ page import="com.novell.nidp.servlets.*" %>
8. <%@ page import="com.novell.nidp.resource.*" %>
9. <%@ page import="com.novell.nidp.resource.jsp.*" %>
10.<%@ page import="com.novell.nidp.common.xml.w3c.*" %>
11.<%
12.    response.setHeader("Pragma", "No-cache");
13.    response.setHeader("Cache-Control", "no-cache");
14.
15.    Locale locale = request.getLocale();
16.    String strLanguageCode = locale.getLanguage();
17.     String strImageDirectory = NIDPResourceManager.getInstance().getImage
Directory(locale);
18.    NIDPResource resource = NIDPResourceManager.getInstance().get
(JSPResDesc.getInstance(), locale);
19.%>
20.
21.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//<%=strLanguage
Code%>">
22.<html lang="<%=strLanguageCode%>">
23.    <head>
24.    <link rel="stylesheet" href="<%= request.getContextPath() %>/images/
hf_style.css" type="text/css">
25.    <style type="text/css" media="screen"><!--
26.      #headimage    { position: relative; top: 0px; left: 0px; z-index: 1}
27.      #title    { position: relative; top: 40px; left: 5px; color: white; z-
index: 4}
28.      #locallabel    { position: relative; top: 78px; left: 10px; z-index:
4}
29.      #login       { text-align: center }
30.         --></style>
31.    <META HTTP-EQUIV="Content-Language" CONTENT="<%=strLanguageCode%>">
32.    <title><%=resource.getString0(JSPResDesc.LOGIN_TITLE)%></title>
33.    <meta http-equiv="content-type" content="text/html;charset=utf-8">
34.    <script type="text/javascript" src="<%= request.getContextPath() %>/
images/showhide_2.js"></script>
35.    <script language="JavaScript">
36.
37.      var i = 0;
38.      function imageSubmit()
39.      {
40.          if (i == 0)
41.          {
42.             i = 1;
43.             document.IDPLogin.submit();
44.          }
45.
46.          return false;
47.      }
48.  </script>
49.    </head>
50.    <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0"
rightmargin="0" onLoad="document.IDPLogin.Ecom_User_ID.focus();" >
51.        <form name="IDPLogin" enctype="application/x-www-form-urlencoded"
```

```
method="POST" action="<%= (String) request.getAttribute("url") %>"
AUTOCOMPLETE="off">
52.        <table style="margin-top: 6em" width="100%" border="0"
cellspacing="0" cellpadding="0">
53.        <tr>
54.            <td width="50%" height="80 px"> </td>
55.        <td colspan="2">
56.            <div id="title"><b><%=resource.getString0(JSPResDesc.
LOGIN_TITLE)%></b></div>
57.        <div id="locallabel"><b><%=resource.getString0(JSPResDesc.
LOCAL_LOGIN)%></b></div>
58.        <div id="headimage"><img src="<%= request.getContextPath() %>/
images/Odyssey_LoginHead.gif" alt="" height="80" width="550" border="0"></div>
59.                    </td>
60.        <td width="100%"> </td>
61.        </tr>
62.        <tr>
63.            <td width="50%"> </td>
64.        <td style="background-color: #efeee9; padding: 10px" colspan="2">
65.<%
66.    String err = (String) request.getAttribute(NIDPConstants.ATTR
_LOGIN_ERROR);
67.    if (err != null)
68.    {
69. %>
70.        <div><label><%=err%></label></div>
71. <%  }
72.
73.   // Determine if this login page is being used for account identification
74.    // purposes
75.    String id = (String) request.getAttribute("identify");
76.    if (id != null && id.equals("true"))
77.    {
78. %>
79.        <div><%=resource.getString0(JSPResDesc.IDENTIFY)%></div>
80. <%  } %>
81.          <span id="login2" style="display: block;">
82.            <table>
83.              <tr>
84.                <td nowrap="nowrap">
85.                  <div>
86.                    <label style="width: 100px"><%=resource.getString0
(JSPResDesc.USERNAME)%></label></label>
87.                  </div>
88.                </td>
89.                <td width="100%" nowrap="nowrap">
90.                  <div>
91.                  <input type="text" class="smalltext" name="Ecom_User_ID"
size="30">
92.                  </div>
93.                </td>
94.              </tr>
95.              <tr>
96.                <td nowrap="nowrap">
97.                  <div>
98.                    <label><%=resource.getString0(JSPResDesc.PASSWORD)%></
label>
99.                  </div>
100.                </td>
```

```
101.                <td style="white-space: nowrap">
102.                  <div>
103.                    <input type="password" class="smalltext" name="Ecom_
Password" size="30">  
104.                  <input alt="<%=resource.getString0(JSPResDesc.LOGIN)%>"
border="0" name="loginButton2" src="<%= request.getContextPath() %>/images/
<%=strImageDirectory%>/btnlogin_<%=strImageDirectory%>.gif" type="image"
value="Login" onClick="return imageSubmit()">
105.                  </div>
106.                </td>
107.              </tr>
108.<%
109.  String prov = (String) request.getAttribute("provision");
110.  if (prov != null)
111.  {
112.%>
113.              <tr>
114.                <td colspan=2>
115.                  <div>
116.                    <label><a href="<%=prov%>"><%=resource.getString0
(JSPResDesc.CREATE_ACCT)%></a></label>
117.                  </div>
118.                </td>
119.              </tr>
120.<%      } %>
121.            </table>
122.          </span>
123.        </td>
124.        <td width="100%"> </td>
125.      </tr>
126. <%
127.  DisplayableProvider[] list = (DisplayableProvider[]) request.get
Attribute("providers");
128.     if (list != null && list.length > 0)
129.     {
130.%>
131.      <tr>
132.        <td width="50%"></td>
133.        <td style="background-color: #efeeec; padding-left: 10px; padding-
bottom: 10px"colspan="2">
134.          <div style="margin-left: -10px; background: url(<%=
request.getContextPath() %>/images/dotline_bg.gif) repeat-x"> </div>
135.          <div><b><%=resource.getString0(JSPResDesc.FEDERATED_LOGIN)%></
b></div>
136.<%
137.    for (int i = 0; i < list.length; i++)
138.    {
139.%>
140.          <a style="padding: 5px" href="<%=list[i].getAuthenticationUrl
(request.getContextPath())%>">
141.<%
142.        if (list[i].hasIcon())
143.        {
144.%>
145.          <img border=0 class="margin4" alt="<%=XMLUtil.stringToHTML
String(list[i].getDisplayName())%>" src="<%=XMLUtil.stringToHTMLString
(list[i].getIcon(request))%>" align="absmiddle"></a>
146.<%
147.          }
```

```
148.        else
149.        {
150.%>
151.          <%=XMLUtil.stringToHTMLString(list[i].getDisplayName())%></a>
152.<%
153.        }
154.
155.     } %>
156.        </td>
157.        <td width="100%"></td>
158.      </tr>
159.<%  } %>
160.        <tr>
161.            <td width="50%"></td>
162.        <td style="background-color: #E6D88C; padding-left: 10px"><img
style="padding-right: 200px" src="<%= request.getContextPath() %>/images/
LAP_interoperable_logo_100.gif" align="absmiddle" border="0"></td>
163.        <td style="background-color: #E6D88C; padding-right: 10px"
align="right" width="100">
164.
165.<%
166.  String cancel = (String) request.getAttribute("cancel");
167.  if (cancel != null)
168.  {
169.%>
170.                      <input alt="<%=resource.getString0(JSPResDesc.
CANCEL)%>" border="0" name="Cancel" src="<%= request.getContextPath() %>/
images/<%=strImageDirectory%>/btncancel_<%=strImageDirectory%>.gif"
type="image" value="Cancel" tabindex="4">
171.<%    }
172.      else
173.      {
174.%>
175.             
176.<%    }   %>
177.        </td>
178.            <td width="100%"></td>
179.        </tr>
180.<%
181.  if (NIDPCripple.isCripple())
182.  {
183.%>
184.        <tr>
185.               <td colspan=4 width="100%" align="center"><%=NIDPCripple.
getCrippleAdvertisement(locale)%></td>
186.        </tr>
187.<%
188.  }
189.%>
190.         </table>
191.        </form>
192.    </body>
193.</html>
```

The following file shows all the changes that allow 3.0 login.jsp to compile on a 3.1 SP IR1 Identity Server. The deleted lines have been replaced with returns, so you can line this file up with the original to see the modifications.

```
<%@ page language="java" %>
<%@ page pageEncoding="UTF-8" contentType="text/html; charset=UTF-8"%>
<%@ page import="com.novell.nidp.common.provider.*" %>
<%@ page import="java.util.*" %>
<%@ page import="com.novell.nidp.ui.*" %>
<%@ page import="com.novell.nidp.*" %>
<%@ page import="com.novell.nidp.servlets.*" %>
<%@ page import="com.novell.nidp.resource.*" %>
<%@ page import="com.novell.nidp.resource.jsp.*" %>
<%@ page import="com.novell.nidp.common.xml.w3c.*" %>
<%
ContentHandler handler = new ContentHandler(request,response);









%>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//
<%=handler.getLanguageCode()%>">
<html lang="<%=handler.getLanguageCode()%>">
    <head>
    <link rel="stylesheet" href="<%= request.getContextPath() %>/images/
hf_style.css" type="text/css">
    <style type="text/css" media="screen"><!--
      #headimage    { position: relative; top: 0px; left: 0px; z-index: 1}
      #title    { position: relative; top: 40px; left: 5px; color: white; z-
index: 4}
      #locallabel    { position: relative; top: 78px; left: 10px; z-index: 4}
      #login       { text-align: center }
         --></style>
    <META HTTP-EQUIV="Content-Language"
CONTENT="<%=handler.getLanguageCode()%>">
    <title><%=handler.getResource(JSPResDesc.TITLE)%></title>
    <meta http-equiv="content-type" content="text/html;charset=utf-8">
    <script type="text/javascript" src="<%= request.getContextPath() %>/
images/showhide_2.js"></script>
    <script language="JavaScript">

      var i = 0;
      function imageSubmit()
      {
          if (i == 0)
          {
             i = 1;
             document.IDPLogin.submit();
          }

          return false;
      }
  </script>
    </head>
    <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0"
rightmargin="0" onLoad="document.IDPLogin.Ecom_User_ID.focus();" >
        <form name="IDPLogin" enctype="application/x-www-form-urlencoded"
method="POST" action="<%= (String) request.getAttribute("url") %>"
AUTOCOMPLETE="off">
```

```
       <table style="margin-top: 6em" width="100%" border="0" cellspacing="0"
cellpadding="0">
        <tr>
            <td width="50%" height="80 px"> </td>
        <td colspan="2">
           <div id="title"><b><%=handler.getResource(JSPResDesc.TITLE)%></b></
div>
        <div id="locallabel"><b><%=handler.getResource(JSPResDesc.PRODUCT)%></
b></div>
        <div id="headimage"><img src="<%= request.getContextPath() %>/images/
Odyssey_LoginHead.gif" alt="" height="80" width="550" border="0"></div>
                    </td>
        <td width="100%"> </td>
        </tr>
        <tr>
            <td width="50%"> </td>
        <td style="background-color: #efeee9; padding: 10px" colspan="2">
<%
    String err = (String)
request.getAttribute(NIDPConstants.ATTR_LOGIN_ERROR);
    if (err != null)
    {
%>
        <div><label><%=err%></label></div>
<%  }









%>
          <span id="login2" style="display: block;">
            <table>
              <tr>
                <td nowrap="nowrap">
                  <div>
                    <label style="width:
100px"><%=handler.getResource(JSPResDesc.USERNAME)%></label></label>
                  </div>
                </td>
                <td width="100%" nowrap="nowrap">
                  <div>
                    <input type="text" class="smalltext" name="Ecom_User_ID"
size="30">
                  </div>
                </td>
              </tr>
              <tr>
                <td nowrap="nowrap">
                  <div>
                    <label><%=handler.getResource(JSPResDesc.PASSWORD)%></
label>
                  </div>
                </td>
                <td style="white-space: nowrap">
                  <div>
```

```
                    <input type="password" class="smalltext"
name="Ecom_Password" size="30">  
                    <input alt="<%=handler.getResource(JSPResDesc.LOGIN)%>"
border="0" name="loginButton2"
src="<%=handler.getImage("btnlogin.gif",true)%>" type="image" value="Login"
onClick="return imageSubmit()">
                  </div>
                </td>
              </tr>









            </table>
          </span>
        </td>
        <td width="100%"> </td>
      </tr>
```

```
        <tr>
            <td width="50%"></td>
        <td style="background-color: #E6D88C; padding-left: 10px"><img
style="padding-right: 200px" src="<%= request.getContextPath() %>/images/
LAP_interoperable_logo_100.gif" align="absmiddle" border="0"></td>
        <td style="background-color: #E6D88C; padding-right: 10px"
align="right" width="100">









        </td>
            <td width="100%"></td>
        </tr>
<%
  if (NIDPCripple.isCripple())
  {
%>
        <tr>
               <td colspan=4 width="100%"
align="center"><%=NIDPCripple.getCrippleAdvertisement(request.getLocale())%><
/td>
        </tr>
<%
  }
%>
        </table>
        </form>
    </body>
</html>
```