AUTHORIZED DOCUMENTATION

Installation Guide

Novell®
Access Manager

3.1 SP4

October 2011

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, upgrade, and removal procedures.

For information about the J2EE Agents, see the *Novell Access Manager 3.1 SP4 J2EE Agent 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/TLS)
- 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/novellaccessmanager31).

Additional Documentation

- *Novell Access Manager 3.1 SP4 Setup Guide*
- *Novell Access Manager 3.1 SP4 Administration Console Guide*
- *Novell Access Manager 3.1 SP4 Identity Server Guide*
- *Novell Access Manager 3.1 SP4 Access Gateway Guide*
- *Novell Access Manager 3.1 SP4 Policy Guide*
- *Novell Access Manager 3.1 SP4 J2EE Agent Guide*
- *Novell Access Manager 3.1 SP4 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.

What's New in Access Manager 3.1 SP4

1

Novell Access Manager 3.1 SP4 provides a number of platform upgrades, critical issue fixes, and enhancements. These platform upgrades and issue fixes enhance the security. The 3.1 SP4 upgrade will help you in future migration to 3.2 version. This release includes:

1.1 Enhancements

This release provides the following enhancements for the Identity Server component:

Mapping Transient Identifier to Local User with Passwordfetch Class: This enhancement enables you to map a federated user with transient name identifier to a local user using the matching attribute. A new password fetch class extension has been added that can be executed as a post-authentication method after a successful transient federation. You can configure this method to match the transient user to local user based on the attribute values received in the authorized assertion.

For more information, see "Mapping Transient Identifier to Local User "in *Novell Access Manager 3.1 SP4 Identity Server Guide*.

Falling Back to the Name/Password Form Authentication when Kerberos Authentication Fails: This enhancement enables you to configure the clients accessing the kerberos authentication to use the Name/Password form authentication based on the IP address configured.

For more information, see "(Optional) Using the Name/Password Form Authentication " in *Novell Access Manager 3.1 SP4 Identity Server Guide*.

Configuring the Fall Back Authentication Class: You can configure the kerberos authentication to fall back to any custom authentication class instead of always falling back to the Name/Password authentication. You can also configure to skip the kerberos authentication for certain clients.

For more information, see "(Optional) Configuring the Fall Back Authentication Class" in *Novell Access Manager 3.1 SP4 Identity Server Guide*.

1.2 Platform Upgrades

- jdk has been upgraded from jdk1.6.0_22 to jdk1.6.0_26.
- openssl has been upgraded to openssl 0.9.8r.
- httpd has been upgraded to httpd 2.2.21.

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. It uses industry standards including Secure Assertions Markup Language (SAML) and Liberty Alliance protocols. It has a single console for management and configuration. To provide secure access from any location, it supports multi-factor authentication, role-based access control, data encryption, and SSL VPN services.

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.

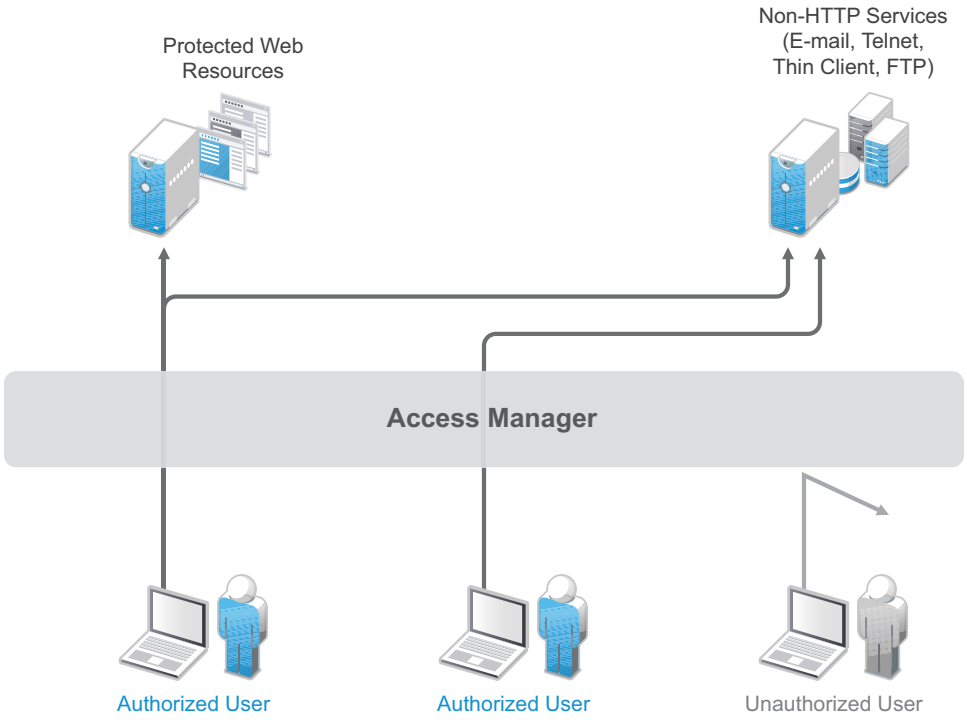
Novell Access Manager lets you provide employees, customers, and partners with secure access to your network resources, whether those resources are Web applications, traditional server-based applications, or other content. If your business faces any of the following access-related challenges, Access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

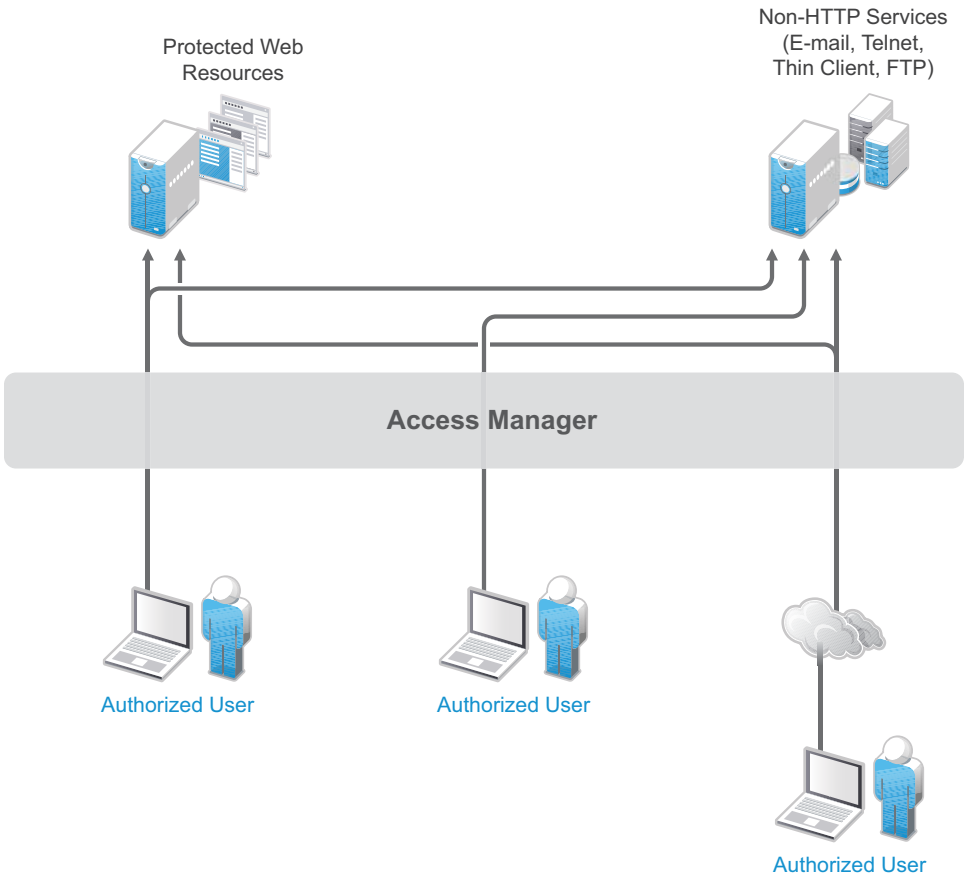
The primary purpose of Access Manager is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources as well as traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized to use the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

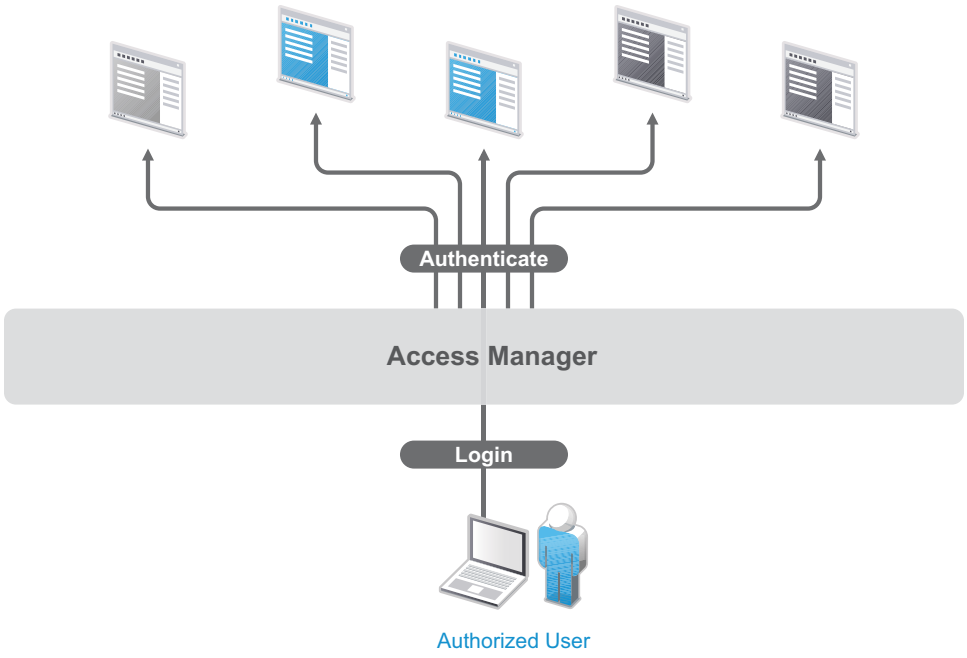
Because not all users work from within the confines of your local network, access to resources is independent of a user's location, as shown in the following illustration. Access Manager provides the same secure access and same experience whether the user is accessing resources from your local office, 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 mean 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 need 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 help desk calls and the reduced likelihood of users resorting to vulnerable written reminders.

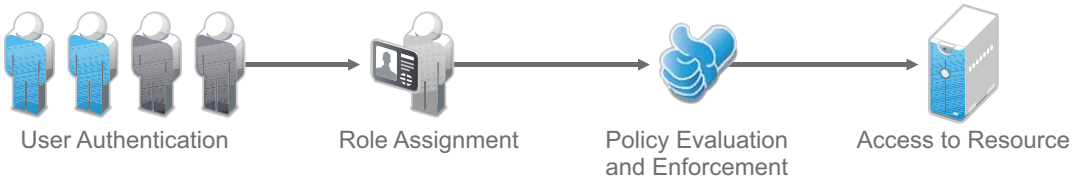


By simplifying the use and management of passwords, Access Manager helps you enhance the user's experience, increase security, streamline business processes, and reduce system administration and support costs.

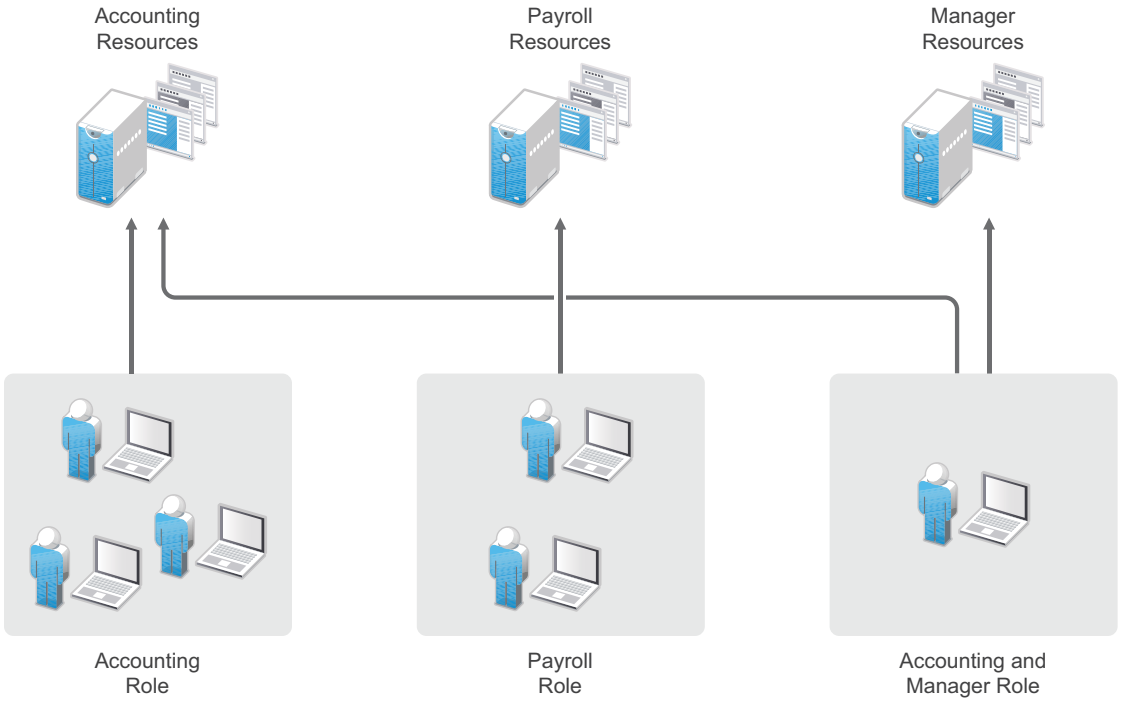
2.1.3 Enforcing Business Policies

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.



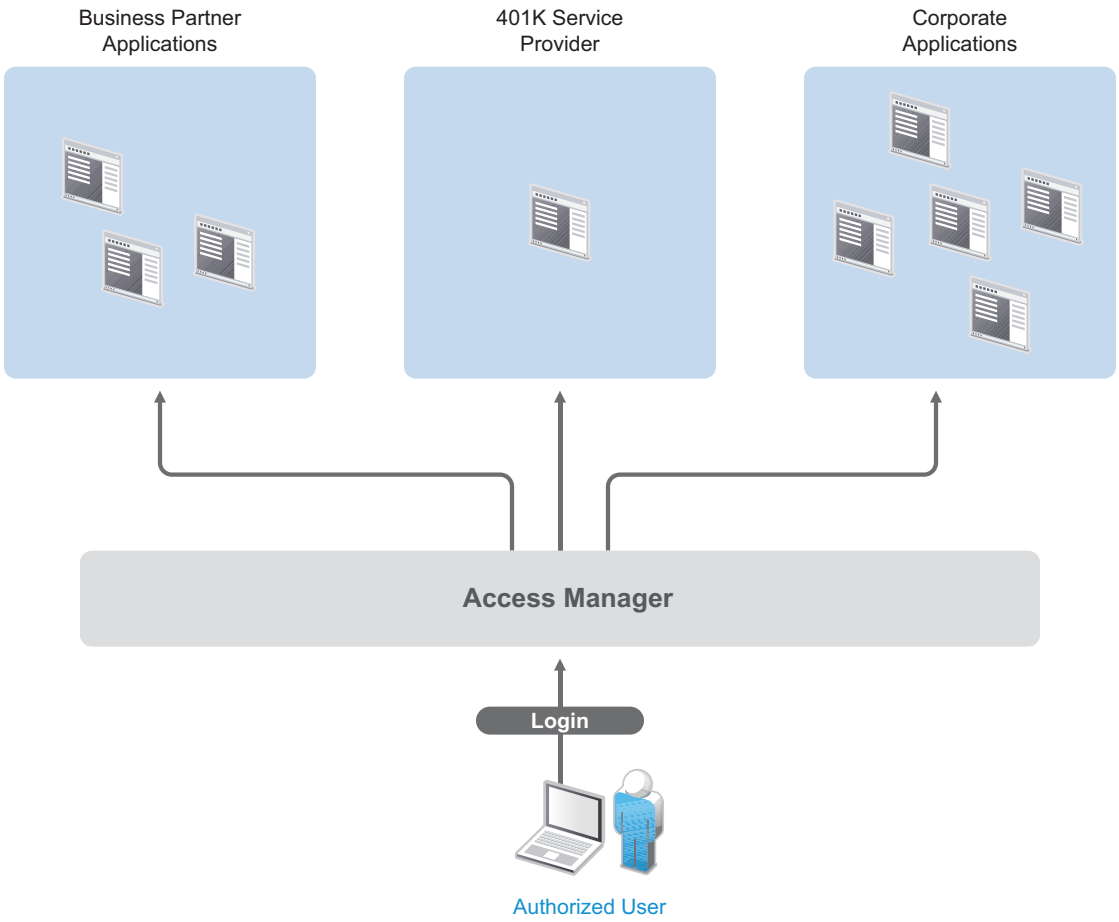
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

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

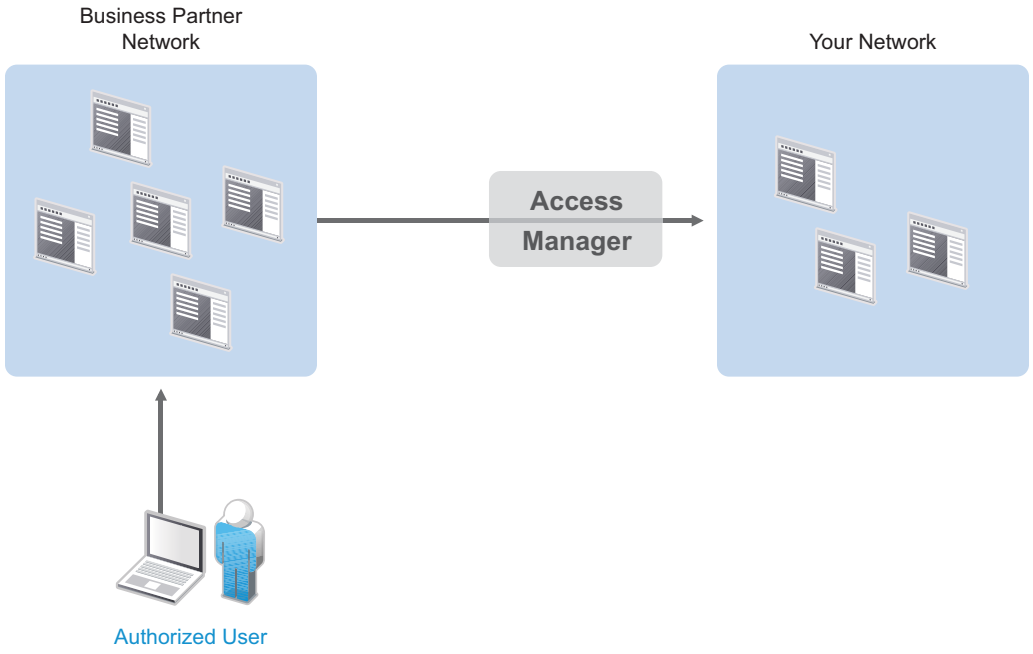
In today's business environment, few organizations stand alone. More than likely, you have trusted business partners with whom you need to shared resources in a secure manner. Or, you have business services, such as a 401k management system, to which you need to provide employee access. Or, maybe your 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.

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.



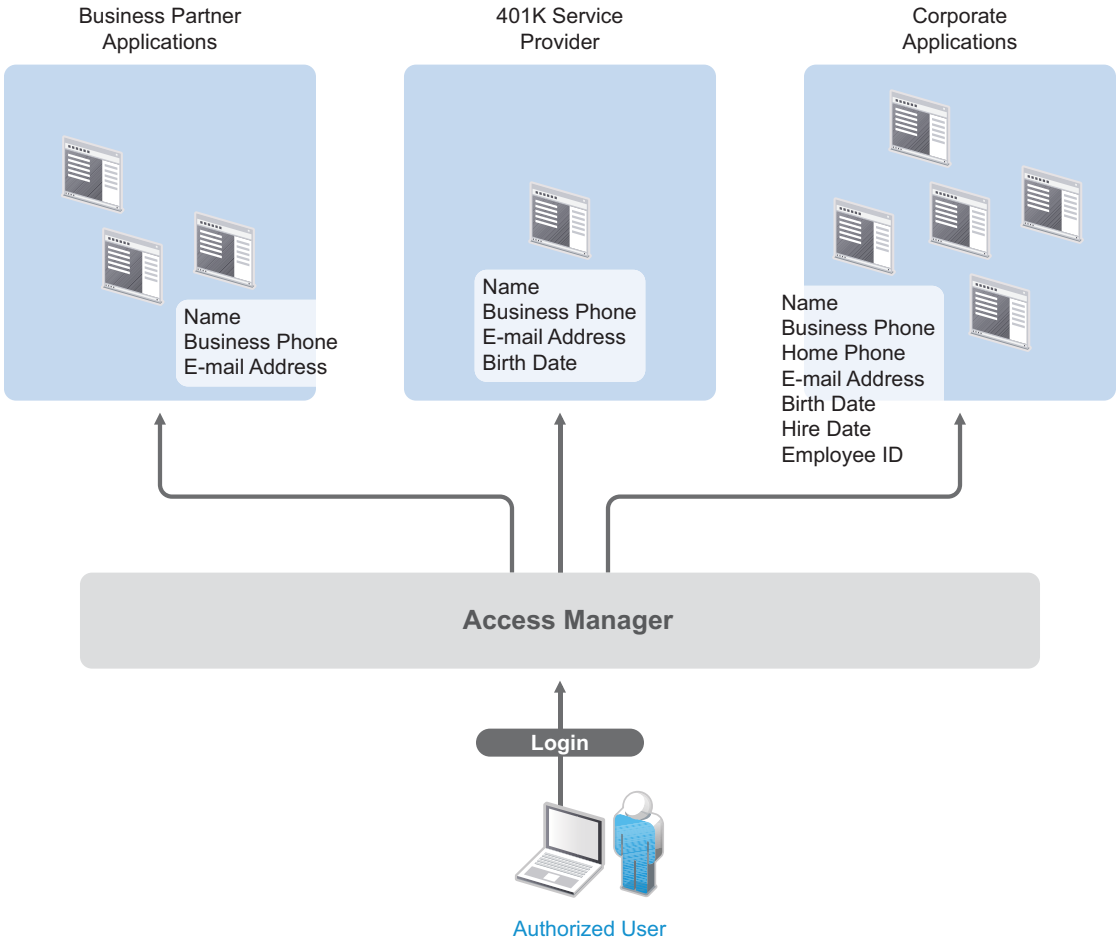
In addition to simply linking user accounts in different identity domains, Access Manager also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization can initiate 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.

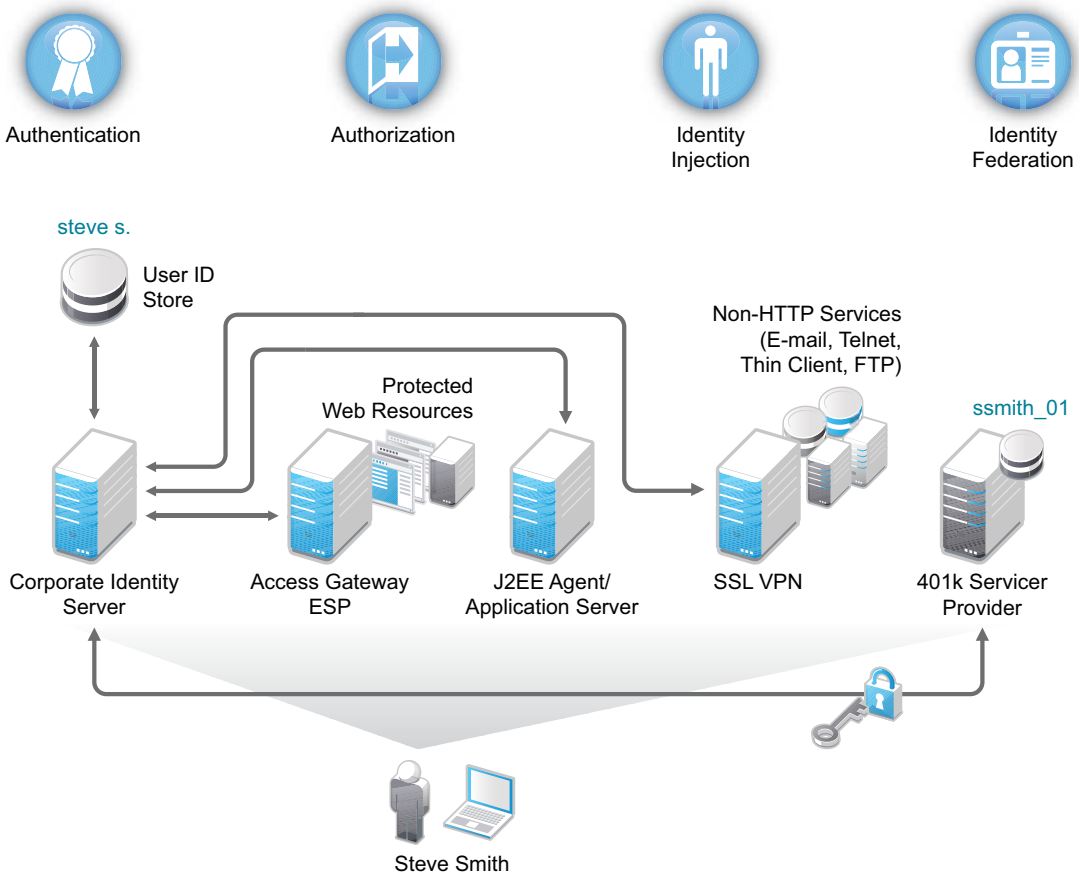
Specifically, Access Manager helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager can generate the reports you need, turning 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, X.509 digital certificates, Kerberos, and OpenID. 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 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 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.

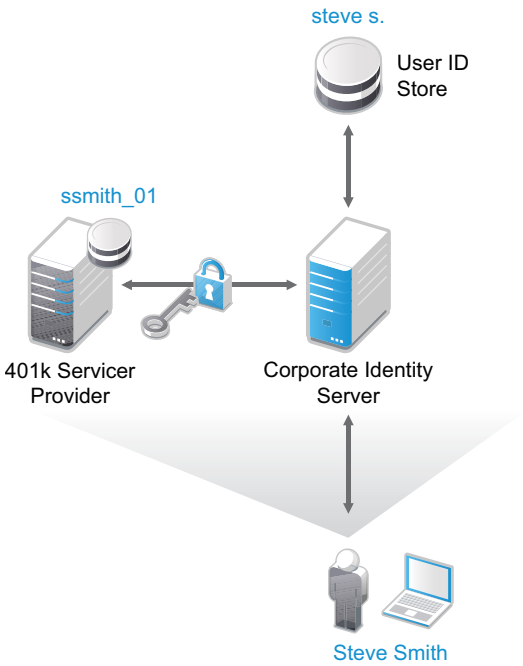
2.2.3 Identity Injection

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.

2.2.4 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.

2.2.5 SSL Renegotiation

SSL renegotiation is the process of establishing a new SSL handshake over an existing SSL connection. The renegotiation messages (ciphers and encryption keys) are encrypted and then sent over the existing SSL connection to establish another session securely and is useful in the following scenarios:

- When you require a client authentication.
- When you require a different set of encryption and decryption keys.
- When you require a different set of encryption and hashing algorithms.

SSL renegotiation is enabled or disabled by the following parameter: `"sun.security.ssl.allowUnsafeRenegotiation.`

This is defined in a registry on Windows and a configuration file on SLES.

Registry key on Windows is `[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Tomcat5\Parameters\Java\Options]`. (How to set the registry key)

Value data for the registry key to enable the SSL renegotiation on Windows is:

`-Dsun.security.ssl.allowUnsafeRenegotiation=true` (procedural format to enable the SSL renegotiation)

To disable the SSL renegotiation on Windows, remove the following entry:

```
"-Dsun.security.ssl.allowUnsafeRenegotiation=true"
```

Configuration file on SLES contains the following parameter:

```
"/var/opt/novell/tomcat5/conf/tomcat5.conf"
```

Value data for the registry key to enable the SSL renegotiation on SLES 11 is:

```
"JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=true"
```

To disable the SSL renegotiation on SLES, remove the following entry:

```
"JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=true"
```

SSL renegotiation can be initiated either by the SSL client or the SSL server. Initiating an SSL renegotiation on the client or the server requires different set of APIs.

2.3 Access Manager Devices and Their Features

2.3.1 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 a Dashboard option, which allows you to assess the health of all Access Manager components.

Figure 2-3 *Novell Access Manager Dashboard Page*

The Administration Console 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 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.
- **Identity 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.

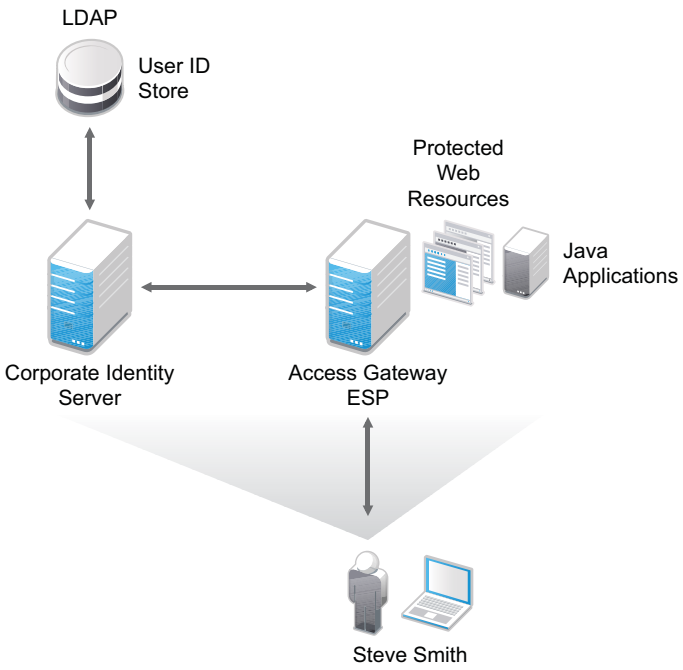
For an overview of Liberty, see "About Liberty" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.

For an overview of SAML, see "Understanding How Access Manager Uses SAML" in the *Novell Access Manager 3.1 SP4 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 single sign-on to protected Web services. The following features facilitate single sign-on to Web servers that are configured to enforce authentication or authorization policies:

- **Identity Injection:** Injects the information the Web server requires into HTTP headers.
- **Form Fill:** Automatically fills in requested form information.

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 can be installed as a soft appliance (which includes the operating system) or as a service (which requires you to provide the operating system). For more information, see *Novell Access Manager 3.1 SP4 Access Gateway Guide*

2.3.4 SSL VPN

The SSL VPN server provides secure access to non-HTTP based applications, such as e-mail servers, FTP services, or Telnet services. The SSL VPN server is a Linux-based service that can be installed in two modes:

- As a resource accelerated by and protected by the Access Gateway, which shares session information with the SSL VPN server
- As a stand-alone device with an Embedded Service Provider, which allows the SSL VPN server to establish its own relationship with the Identity Server.

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. The administrator of the Identity Server can use policies to define 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 policy that permits or denies access to a protected Web site, depending on user roles (such as employee or manager), the value of an LDAP attribute, or the user's IP address.

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 the certificates used for digital signatures and data encryption. You can create locally signed certificates or import externally signed certificates, then assign these certificates to the trust stores and keystores 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 keystore 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.

The Access Manager devices can be configured to send their auditing events to a Sentinel™ or a Sentinel Log Manager server.

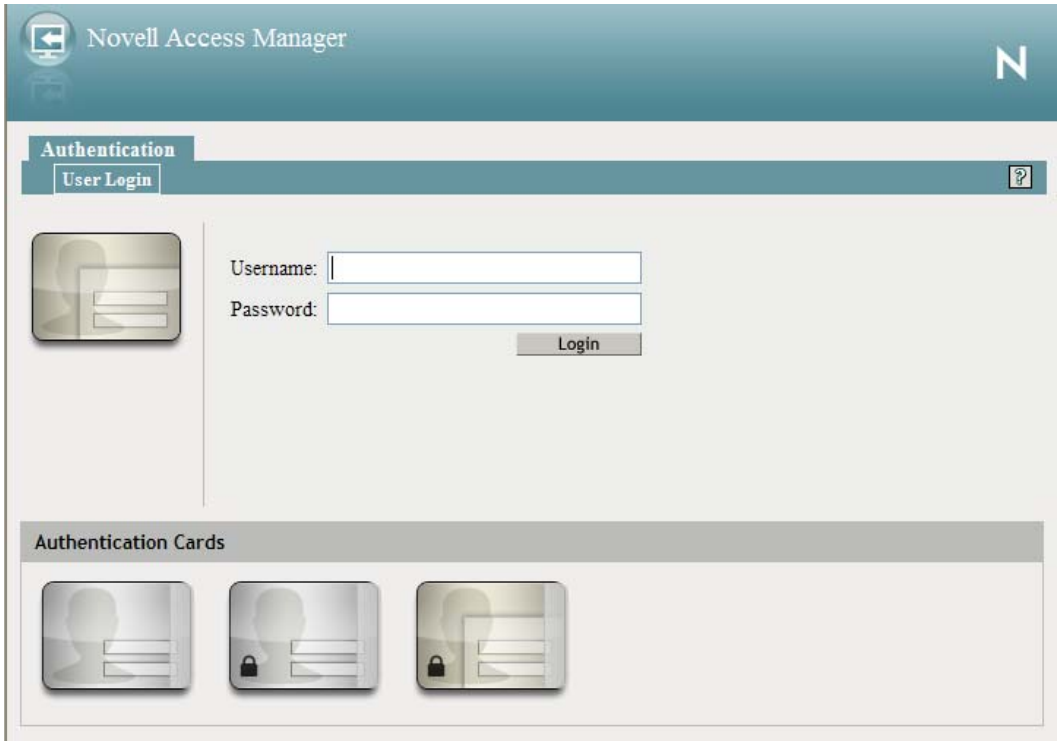
2.3.9 Embedded Service Provider

The Access Gateway, SSL VPN server, 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, SSL VPN server, 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 the Error Pages of the Access Gateway Service" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.
- For the Access Gateway Service, see "Customizing the Error Pages of the Access Gateway Service" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.
- For the Identity Server, see "Customizing Identity Server Messages" in the *Novell Access Manager 3.1 SP4 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/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).

Because all 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, see the *Novell Access Manager 3.1 SP4 J2EE Agent Guide*.

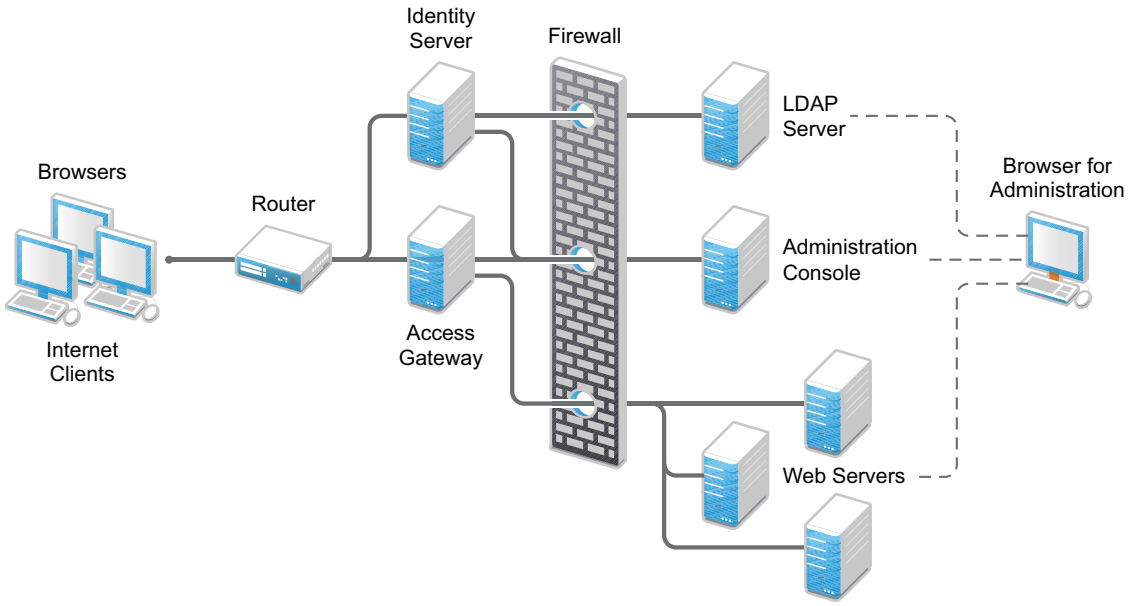
3.1 Recommended Installation Scenarios

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 ISO image.

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 SP4 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 SP4 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 SP4 Setup Guide*.

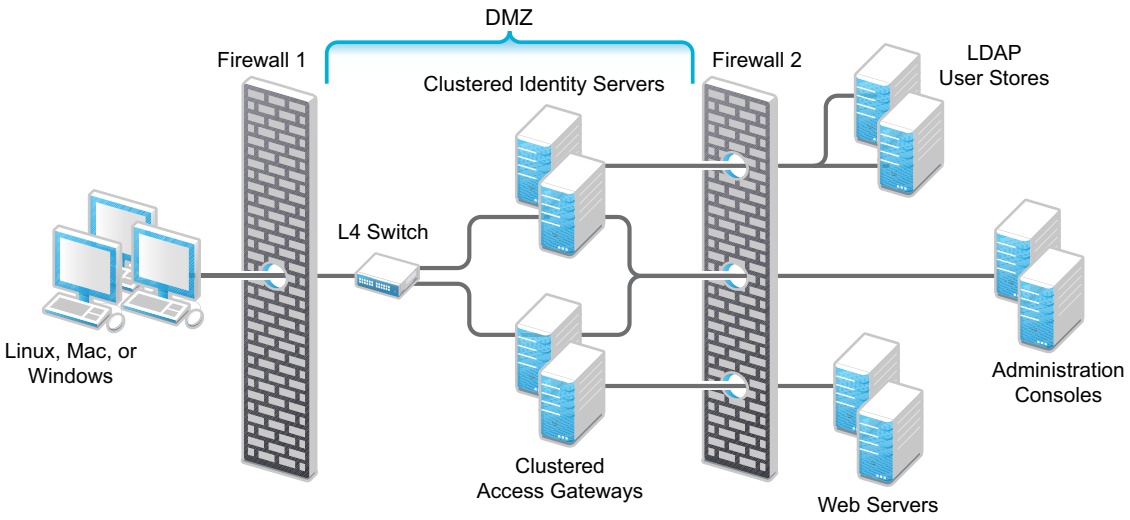
For information about setting up configurations for fault tolerance and clustering, see "Clustering and Fault Tolerance" in the *Novell Access Manager 3.1 SP4 Setup Guide*.

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 High Availability Configuration with Load Balancing

Figure 3-2 illustrates a deployment scenario where Web resources are securely accessible from the Internet. The scenario also provides high availability because both the Identity Servers and the Access Gateways are clustered and have been configured to use an L4 switch for load balancing and fault tolerance.

Figure 3-2 *Clustering Configuration for High Availability*



End users can be configured to communicate with the Identity Servers and Access Gateways through HTTP or HTTPS. The Access Gateways can be configured to communicate with the Web servers through HTTP or HTTPS. The multiple Administration Consoles provide administration and configuration redundancy.

This configuration is scalable. As the number of users increase and the demands for Web resources increase, you can easily add another Identity Server or Access Gateway to handle the load, then add the new servers to the L4 switch. When the new servers are added to the cluster, they are automatically sent the cluster configuration.

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 SLES 11. For the Access Gateway Appliance, you should select a platform supported by SLES 9 or SLES 11. For the Linux Access Gateway Service, you should select a platform supported by SLES 11.

For the Windows components (Identity Server and Administration Console), you should select a platform supported by Windows Server 2003 or Windows Server 2008. For the Windows Access Gateway Service, you should select a platform supported by Windows Server 2008.

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

- Section 3.4, “Administration Console Requirements,” on page 37
- Section 3.5, “Identity Server Requirements,” on page 39
- Section 3.6, “Access Gateway Requirements,” on page 40
- Section 3.7, “SSL VPN Requirements,” on page 46

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 8.8 or later, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- ❑ 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.

  IMPORTANT: 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 (Administration Console, Identity Server, Access Gateway, SSL VPN server, and J2EE Agents) 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 NAT to make sure that all requests continue to go back through 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:

- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 100 GB hard disk.

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
- ❑ One of the following operating systems:
  - SLES 10 SP4, either with 32-bit or 64-bit operating system on x86-32 and x86-64 hardware.
  - SLES 11 SP1 or SP2, either with 32-bit operating system or 64-bit operating system on x86-32 and x86-64 hardware.
- ❑ Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.
- ❑ 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. On SLES 11, the compat-32bit package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119).
  - compat-libstdc++: A required library for the configuration database. On SLES 11, this library is installed as a dependency when you install the compat package.

Use the following command to verify:

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

Use YaST to install the packages.

- ❑ Minimal SLES installation:
  - **SLES 9:** You cannot install the Administration Console on a machine with a minimal SLES 9 installation. The Administration Console requires a GUI (such as the X Windows system), and a minimal SLES installation does not install a GUI
  - **SLES 10 Requirements:** On a minimal install of SLES 10, make sure the following packages (with their dependent packages) are installed before installing the Administration Console: A graphical user interface library 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 for a 64-bit installation)
  - **SLES 11 Requirements:** On a minimal install of SLES 11, make sure the following packages (with their dependent packages) are installed before installing the Administration Console: A graphical user interface library required for the installation of iManager
    - gtk2 (version 2.18.9 or later)

    Use the following command to verify:

    ```
    rpm -qa | grep gtk
    ```
- ❑ OpenLDAP cannot be installed, and if it is installed, it must be removed.
- ❑ Zip and unzip utilities must be available 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 hostname 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 by using the Linux Virtual Services software, you can also install the Administration Console on this machine.

For Administration Console installation instructions, see “Installing the Access Manager Administration Console” on page 49.

3.4.2 Windows Requirements

- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 100 GB hard disk.

This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.

- ❑ One of the following operating systems:
  - Windows 2003 Server SP2, 32-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
  - Windows 2008 Server R2, 64-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
- ❑ 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 can be installed. If you have a version installed, remove it, install the Administration Console, then reinstall the JRE.

For Administration Console installation instructions, see “Installing the Access Manager Administration Console” on page 49.

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 7.x or 8.x
- Firefox* 3.5.x and 3.6.x on Windows and Linux
- Firefox 2 on SLED 10

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

3.5 Identity Server Requirements

The Identity Server is the second component you install, and 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 40

Clients that authenticate 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:

- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 100 GB hard disk.

This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.

- ❑ One of the following operating systems:
  - SLES 10 SP2, SP3, or SP4, either with 32-bit or 64-bit operating system on x86-32 and x86-64 hardware.
  - SLES 11 SP1 or SP2, either with 32-bit operating system or 64-bit operating system 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. On SLES 11, the compat-32bit package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119).
- ❑ 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 59.

3.5.2 Windows Requirements

The Windows machine requires the following software and hardware:

- ❑ One of the following operating systems:
  - Windows Server 2003 SP2, 32-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
  - Windows Server 2008 R2, 64-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
- ❑ No LDAP software, such as eDirectory or OpenLDAP, can be installed.
- ❑ Static IP address.
- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 Ghz or comparable chip).
- ❑ 100 GB hard disk.

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.

For installation instructions, see Chapter 5, “Installing the Novell Identity Server,” on page 59.

3.6 Access Gateway Requirements

- Section 3.6.3, “Windows Access Gateway Service Requirements,” on page 42
- Section 3.6.4, “Client Access Requirements,” on page 42
- Section 3.6.5, “Access Gateway Feature Comparison,” on page 42

In additional to evaluating the differences in software and hardware requirements, you can decide whether to install a Gateway Appliance or a Gateway Service by evaluating the minor functional differences between the two.

The Access Gateway can be installed as an appliance (the operating system is installed with the Access Gateway software) or as a service (the Access Gateway software is installed on a machine with an existing operating system). These Access Gateways have the following requirements:

3.6.1 Access Gateway Appliance Requirements

The Linux Access Gateway Appliance runs on SLES 11, 32-bit operating system on x86-32 and x86-64 hardware. You install it on a separate machine because it clears the hard drive and sets up a soft appliance environment.

The Access Gateway Appliance requires the following hardware:

- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 100 GB hard disk.

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
- ❑ A static IP address for your Access Gateway server and an assigned DNS name (host name and domain name)

For a list of hardware that is supported by SLES 11 for x86-32 and x86-64 hardware, see the YES CERTIFIED Bulletin (http://developer.novell.com/yessearch/Search.jsp), and search for SLES 11 and your other hardware requirements.

The Access Gateway 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.

For installation instructions, see Chapter 6, “Installing the Linux Access Gateway Appliance,” on page 65.

3.6.2 Linux Access Gateway Service Requirements

The Linux Access Gateway Service is installed on an existing Linux system. This machine must meet the following requirements:

- ❑ SLES 11 SP1 or SP2, 64-bit operating system on x86-64 hardware.

NOTE: For the SLES 11 platform, make sure you have the latest security patches and the openssl version is openssl-0.9.8h. To confirm the version of openssl in your system, run the `rpm -qa | grep openssl` command.

- ❑ Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.
- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- ❑ Configured with a static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module fails to start.
- ❑ Other Access Manager components should not be installed on the same machine.

3.6.3 Windows Access Gateway Service Requirements

The Windows Access Gateway Service is installed on an existing Windows system. This machine must meet the following requirements:

- ❑ Windows 2008 R2 Server, 64-bit operating system on 64-bit hardware, in either Standard or Enterprise Edition, with the latest patches applied
- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ 2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- ❑ Configured with a static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module fails to start.
- ❑ Other Access Manager components should not be installed on the same machine.

3.6.4 Client Access Requirements

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

3.6.5 Access Gateway Feature Comparison

Access Manager includes an Access Gateway Appliance and an Access Gateway Service. The Gateway Appliance is a dedicated machine that installs its own embedded Linux operating system. The Gateway Service runs on top of an existing installation of a Linux or Windows operating system. Both types of gateways support the same major functionality, but they differ slightly in the way some of these features are supported. For example, both types can be configured for the following features:

- Protecting Web resources with contracts, Authorization policies, Form Fill, and Identity Injection policies.
- Providing fault tolerance by clustering multiple gateways of the same type.
- Providing fault tolerance by grouping multiple Web servers, so that if one Web server goes down, the content can be retrieved from another server in the group.

- Rewriting URLs so that the names and IP addresses of the Web servers are hidden from the users making requests.
- Generating alert, audit, and logging events with notify options.

Most differences between the Gateway Appliance and the Gateway Service result from the differences required for an appliance and for a service. An appliance can know, control, and configure many features of the operating system. A service that runs on top of an operating system can query the operating system for some information, but it cannot configure or control the operating system. For the service, operating system utilities must be used to configure system parameters and hardware. For the appliance, the operating system features that are important to the appliance, such as time, DNS servers, gateways, and network interface cards, can be configured in the Administration Console.

Table 3-1 describes the differences between the Access Gateway Appliance and the Access Gateway Service. Only your network and Web server configurations can determine whether the differences are significant.

Table 3-1 *Differences between the Gateway Appliance and the Gateway Service*

Feature	Gateway Appliance	Gateway Service
Network configuration - DNS servers - Gateways - Network interface cards - Host names	Can be done from the Administration Console.	Configurable with standard operating system utilities.
Date and time	Can be done from the Administration Console.	Configurable with standard operating system utilities.
Rewriter: number of URLs that can be rewritten	There is a set limit, although the limit has been increased.	No limit.
Rewriter: profiles	Can do word pattern matches in Word profiles and Character profiles.	Can only do word pattern matches in Character profiles.
Rewriter: Word profiles	Case sensitive.	Case insensitive.
Rewriter: Special tokens for Word profiles	Not supported.	Supports the [w]. [ow], [ep], [ew], and [oa] options.
Rewriter: webcal	Unsupported.	Supported.
Cache directory	Separate protected partition (COS).	Uses Apache-caching. The cached files are stored in clear text. The operating system must be configured to protect this directory. For more information on the Apache model, see "Caching Guide" (http://httpd.apache.org/docs/2.2/caching.html).

Feature	Gateway Appliance	Gateway Service
Cache freshness configuration options	Fully supported.	Limited support.
Custom cache control headers	Supported.	Unsupported.
Caching behavior	For more information, see "Configuring Caching Options" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.	
X-Forwarded-For header	Configurable from the Administration Console	Hard coded by Apache to send the X-Forwarded-For header as well as the X-Forwarded-Host and X-Forwarded-Server headers.
Via header	Includes the device ID.	Does not include the device ID. Apache sets the information in the Via header.
NTLM, a Windows challenge and response authentication protocol	Supported.	Not supported by Apache.
Stop and restart commands	Shuts down the operating system or restarts the operating system and the Access Gateway Appliance.	Stops and starts the Access Gateway Service without affecting other services or applications. The operating system can be rebooted or shutdown independently with standard operating system commands.
Protected resource logging	Can configure the directory and stop the proxy service if logging fails.	Cannot configure the directory or stop the proxy service when logging fails.
Web server connections	If the gateway has multiple network cards, you can specify which network card to use for the Web server connection.	Not configurable.
Web server failover	Configurable for simple failover or round robin.	Hard coded to round robin. This is an Apache limitation.
Web server certificate verification	Configurable per proxy service.	Globally configurable. If certificate verification is turned on for one proxy service, it is turned on for all proxy services.
Load balancing cookie	Access Gateway Appliance format.	Apache format.
5-6 byte UTF characters (supported by IIS Web servers)	Supported.	Unsupported.
TCP listen options	Idle timeout.	Keep alive interval.

Feature	Gateway Appliance	Gateway Service
Custom configuration	Touch files.	Advanced options. Click *Access Gateways > Edit > Advanced Options* or *Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > Advanced Options*.
Device logging	`ics_dyn.log`	`ags_error.log` and Apache `error.log`
Device logging configuration	Log level set with options in the nash shell.	Configurable from the Administration Console. Click *Access Gateways > Edit > Logging*.
Sending alerts to an SNMP server	Unsupported.	Supported.
Manipulates cookies so that when a browser retains application cookies from the Web servers after a user logs out, these cookies become invalid.	Unsupported.	Supported.
NetStorage	Browser connections can be used.	Browser and WebDAV connections can be used.

Inconsistency in 302 redirect message between HTTP and HTTPS.	Request to HTTP port 80 is responded with the following HTML document:
	`<HTML><HEAD><TITLE>Novell Proxy</TITLE></HEAD><BODY><b><p>HTTP request is being redirected to HTTPS.<p><A HREF="https://www.lagssl.com:443/">redirect</A> </b></BODY></HTML>`
		Request to HTTP port 80 is responded with the following HTML document:
		<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD>
		`<title>302 Found</title>`
		`</head><body>`
		`<h1>Found</h1>`
		`<p>The document has moved <a href="https://www.magssl.com/">here</a>.</p>`
		`</body></html>`

3.7 SSL VPN Requirements

The SSL VPN server can be installed with the Access Gateway Appliance, with the Linux Identity Server, with the Linux Administration Console, or on its own machine. When installed with another Access Manager component, that component's requirements are sufficient for the SSL VPN server. When installed on its own machine, it has the following hardware and software requirements:

- ❑ 100 GB of disk space.

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
- ❑ 4 GB RAM.
- ❑ Dual CPU or Core (3.0 GHz or comparable chip).
- ❑ One of the following operating systems:
  - SLES 10 SP1, SP2, SP3, or SP4, 32-bit or 64-bit
  - SLES 11, 32-bit or 64-bit
- ❑ `gettext` package
- ❑ Static IP address

3.7.1 Windows Client Limitations

- In Windows 7 32-bit, Kiosk mode does not work in Internet Explorer 8.
- Only Enterprise mode is supported in Windows 64-bit client.
- Enterprise mode clients, running on 64-bit operating systems, cannot use 64-bit browsers for SSL VPN connections.

For a list of supported client operating systems and browsers, see "Client Machine Requirements" in the *Novell Access Manager 3.1 SP4 SSL VPN User Guide*.

3.8 Virtual Machine Requirements

The virtual machine must have enough resources. It needs to match the requirements that a physical machine has 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, each virtual machine should meet the following minimum requirements:

- 100 GB of disk space
- 4 GB RAM
- 2 CPUs

The following virtual machines are supported:

- VMware ESX Server version 3.5 or later
- Xen Virtualization on SUSE Linux Enterprise Server 10 SP2 or later

NOTE: SLES11 Linux Access Gateway does not support XEN para virtualization for the Access Manager 3.1 SP3 release.

The following sections contain a few installation tips for virtual machines:

3.8.1 Keeping Time Synchronized on the Access Manager Devices

Even when virtual machines are configured to use a network time protocol server, time does not stay synchronized because the machines 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.

SLES 10: 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.

SLES 11: The `ntpdate` command is not supported by SLES 11. You can use the `sntp` command in its place. Add the following command to the `/etc/crontab` file of the device:

```
*/5 * * * *   root   /usr/sbin/sntp -P no -r 10.20.30.108 >/dev/null 2>&1
```

Replace 10.20.30.108 with the IP address of your Administration Console.

NOTE: The time keeping for SLES 11 is also applicable for Access Gateway appliance if XEN Full Virtualization is used.

3.8.2 How Many Virtual Machines Per Physical Machine

How you deploy your virtual machines can greatly influence Access Manager performance, especially if you run too many virtual machines on insufficient hardware. As a rough guideline, we recommend that you deploy only four Access Manager virtual machines on a single piece of hardware. When you start deploying more than four, the Access Manager components start competing with each other for same hardware resources at the same time. You can put as many other types of services as the machine can support, as long as they aren’t trying to use the same hardware resources as the Access Manager components.

The configured CPUs must match the hardware CPUs on the machine. Performance is drastically reduced if you allocate more virtual CPUs than actually exist on the machine.

Another potential bottleneck is IO. For best performance, each virtual machine should have its own hard disk, or you need a SAN that is capable of handling the IO traffic.

For example, if you have one 16-CPU machine, you get better performance when you configure the machine to have four Access Gateways with 4 assigned CPUs than you get when you configure the machine to have eight Access Gateways with 2 assigned CPUs. If the machines are dedicated to

Access Manager components, you get better performance from two 8-CPU machines than you get from one 16-CPU machine.The setup really depends on your unique environment and finding the right hardware and virtualization configuration for your cluster.

.

3.8.3 Which Network Adapter to be used for VMWare ESX

Use the E1000 network adapter for Novell Access Manager installation on VMWare ESX.

Installing the Access Manager Administration Console

4

Installation time: about 20 minutes.

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

For a functioning system, you need an Administration Console for configuration and management, an Identity Server for authentication, and an Access Manager device for protecting resources such as an Access Gateway, an SSL VPN server, or a J2EE Agent. The Administration Console must be installed before you install any other Access Manager devices.

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 SP4 Setup Guide*.

4.1 Installation Procedures

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 the Administration Console.
2. Verify that the machine meets the minimum requirements. See Section 3.4, “Administration Console Requirements,” on page 37.
3. Open a terminal window.
4. Log in as the `root` user. A message prompt to enable or disable the SSL renegotiation appears during the installation.

WARNING: This installer is bundled with JDK, which has the SSL renegotiation disabled by default. If you use the x509 certificate based authentication, then SSL renegotiation must be enabled. Would you like to enable SSL renegotiation for this session Y/N [N].

5 SSL renegotiation is disabled by default because the TLS, SSL protocol 3.0 or earlier are vulnerable to the man-in-the-middle attack. Select "N" to disable the SSL renegotiation or "Y" to enable the SSL renegotiation. Enabling the SSL renegotiation leaves the system open to possible man-in-the-middle attacks. We recommend you to disable the SSL renegotiation when using the x509 certificate based authentication under the following scenarios:

5a Browser to identity provider when using the x509 certificate based authentication.

5b Identity provider to identity provider communication when using the x509 certificate for mutual authentication.

5c Secure LDAP connections with mutual authentication in the LDAP user store.

6 Access the install script:

6a Make sure you have downloaded the software or you have the CD available.

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

6b Do one of the following:

- Insert the CD 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 by using the following command:

  `tar -xzvf <filename>`

6c Change to `the novell-access-manager-3.1.2-xxx` directory.

7 At the command prompt, enter the following:

`./install.sh`

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

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

Record the static IP address here: _____

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

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

11 Review and accept the License Agreement.

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

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

13 Specify the administration username.

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

Record the admin username here: _____

14 Specify the administration password.

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

Record the admin password here: _____

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

This can take several minutes, depending upon the speed of your hardware. 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 SP4 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, LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored.
- **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 SP4 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.

16 Record the login URL.

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

```
http://10.10.10.50:8080/nps
```

Record your login URL here: _____

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

17 Continue with Section 4.2, "Configuring the Administration Console Firewall," on page 54.

4.1.2 Installing on Windows

1. Verify that the machine meets the minimum requirements. See Section 3.4, “Administration Console Requirements,” on page 37.
2. Close any running applications and disable any virus scanning programs.
3. (Conditional) To use a remote desktop for installation, use one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
4. Download the software 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. A message prompt to enable or disable the SSL renegotiation appears during the installation.

    WARNING: This installer is bundled with JDK, which has the SSL renegotiation disabled by default. If you use x509 authentication, then SSL renegotiation must be enabled. Would you like to enable SSL renegotiation for this session Y/N [N].

    ---

12. SSL renegotiation is disabled by default because the TLS, SSL protocol 3.0 or earlier are vulnerable to man-in-the-middle attack. Select “N” to disable the SSL renegotiation and “Y” to enable the SSL renegotiation. Enabling the SSL renegotiation leaves the system open to possible man-in-the-middle attacks. The preferred option is to disable the SSL renegotiation when using the x509 certificate based authentication under the following scenarios:

    12a Browser to identity provider when using the x509 certificate based authentication.

12b Identity provider to identity provider communication when using the x509 certificate for mutual authentication.

12c Secure LDAP connections with mutual authentication into the LDAP user store.

13 To start the install, click *Install*.

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

14 (Optional) After the installation completes, view the install log file found in the following location:

Windows Server 2003: `\Program Files\Novell\log\AccessManagerServer_InstallLog.log`

Windows Server 2008: `\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`

15 Reboot the machine.

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

---

16 (Windows Server 2003) In a terminal window, run the `auditext.exe` utility.

16a Change to the `\Program Files\Novell\NSure Audit` directory.

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

16b 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
c:	The drive letter for where the `Program Files` directory is located.
-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).

17 (Windows Server 2008) In a terminal window, run the `auditext.exe` utility.

17a Change to the `\Program Files (x86)\Novell\NSure Audit` directory.

The `.lsc` file required when executing the `auditext.exe` utility is located in the `\Program Files (x86)\Novell\Nsure Audit\LogSchema\nids_en.lsc` directory.

17b Enter the following command:

```
auditext -lsc -u:<admin> -p:<novell> -a:Novell Access Manager -
f:c:\Program Files (x86)\Novell\Nsure Audit\LogSchema\\nids_en.lsc -
l:en
```

Modify the following variables to match your system:

Variable	Description
c:	The drive letter for where the `Program Files (x86)` directory is located.
-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).

18 Continue with Section 4.2, "Configuring the Administration Console Firewall," on page 54.

4.2 Configuring the Administration Console Firewall

Before you can install other Access Manager components and import them 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, specify the following ports to open:

- 8080
- 8443

4 (Conditional) If you are importing an 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 an Access Gateway Appliance, 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 SP4 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 55.

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.

Open the following ports:

- 8080
- 8443

4 (Conditional) If you are importing an 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 SP4 Setup Guide*.

5 (Conditional) If you are importing an Access Gateway Appliance, 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 55:

4.3 Logging In to the Administration Console

The Administration Console supports the following Web browsers:

- Microsoft Internet Explorer 7.x and 8.x
- Mozilla* Firefox 3.5.x and 3.6.x

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 prevent 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 54.

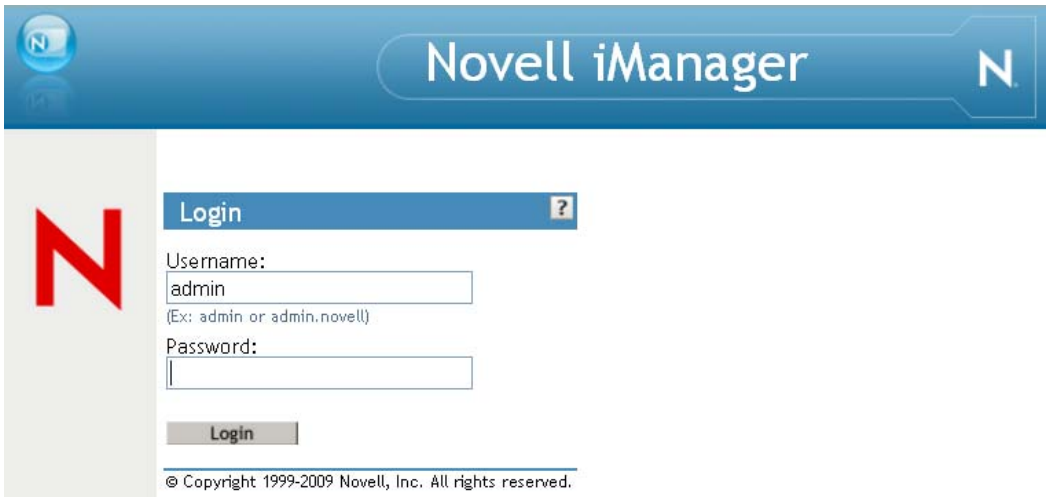
   SUSE Linux Enterprise Server (SLES) comes with a firewall enabled by default, which closes these ports.
3. From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

   Use the IP address established when you installed the Administration Console. It should include 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 the Administration Console for the 3.0 view, see "Configuring the Default View" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

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

---

7 Continue with one of the following:

- 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. The best practice is to next install the Identity Server. See Chapter 5, "Installing the Novell Identity Server," on page 59.
- If your Administration Console machine has multiple interface cards, see Section 4.4, "Enabling the Administration Console for Multiple Network Interface Cards," on page 57.
- To understand the conventions of the Administration Console, see Section 4.5, "Administration Console Conventions," on page 58.

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, which is found in the following directory.

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

Windows Server 2003: `\Program Files\Novell\Tomcat\conf`

Windows Server 2008: `\Program Files (x86)\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 to install the Identity Server	◆ 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 the 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 49.) 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 54.
- ❑ 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. A message prompt to enable or disable the SSL renegotiation appears during the installation.

   WARNING: This installer is bundled with JDK, which has the SSL renegotiation disabled by default. If you use the x509 certificate based authentication, then SSL renegotiation must be enabled. Would you like to enable SSL renegotiation for this session Y/N [N].

4. SSL renegotiation is disabled by default because the TLS, SSL protocol 3.0 or earlier are vulnerable to the man-in-the-middle attack. Select “N” to disable the SSL renegotiation or “Y” to enable the SSL renegotiation. Enabling the SSL renegotiation leaves the system open to possible man-in-the-middle attacks. We recommend you to enable the SSL renegotiation when using the x509 certificate based authentication under the following scenarios:

   4a Browser to identity provider when using the x509 certificate based authentication.

   4b Identity provider to identity provider communication when using the x509 certificate for mutual authentication.

   4c Secure LDAP connections with mutual authentication in the LDAP user store.

5. Access the install script.

   5a Make sure you have downloaded the software or that you have the CD available.

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

   5b Do 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 by using the following command:

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

   5c Change to `the novell-access-manager-3.1.2-xxx` directory.

6. At the command prompt, run the following install script:

   ```
   ./install.sh
   ```

7. When you are 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.

8. If you are prompted, decide whether or not you want to continue the installation without a static IP address. In most production environments, you must establish a static IP address for your Identity Server to reliably connect with other Access Manager components. If the IP address changes, the Identity Server can no longer communicate with the Administration Console.
9. Review and accept the License Agreement.
10. 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.

11 Specify the name of the administrator for the Administration Console.

This is the name you recorded when you installed the Administration Console.

12 Specify the password of the administrator.

This is the password you recorded when you installed the Administration Console.

13 Confirm the password, then wait as the system installs the components. (This takes 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 59.

The following components are installed:

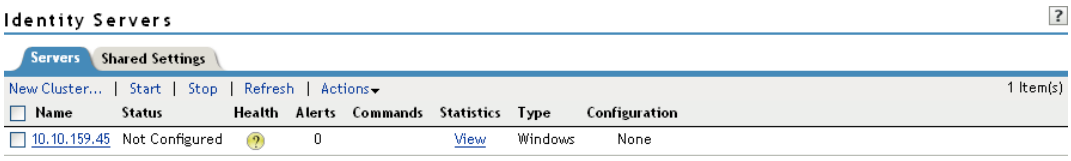
- **Novell Access Manager Server Communications:** Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
- **Novell Identity Server:** Provides authentication and identity services for the other Access Manager components and third-party service providers.
- **Novell Identity Server Configuration:** 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:** 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/inst_lag.log`. These logs are all dated and time-stamped.

14 (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 55).

After you log in to the Administration Console, click *Devices* > *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.

15 Continue with one of the following:

- To install an Access Gateway, see Chapter 6, “Installing the Linux Access Gateway Appliance,” on page 65 or Chapter 7, “Installing the Access Gateway Service,” on page 75.
- To configure the Identity Server, see “Setting Up a Basic Access Manager Configuration” in the *Novell Access Manager 3.1 SP4 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. (Conditional) To use a remote desktop for installation, use one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
5. Download the software file and execute it.

   For software download instructions, see the “Novell Access Manager Readme” (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
6. Read the introduction, then click *Next*.
7. Accept the license agreement, then click *Next*.
8. Select *Novell Identity Server*, then click *Next*.
9. 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.
10. Click *Next*, then review the summary.
11. A message prompt to enable or disable the SSL renegotiation appears during the installation.

    WARNING: This installer is bundled with JDK, which has the SSL renegotiation disabled by default. If you use x509 authentication, then SSL renegotiation must be enabled. Would you like to enable SSL renegotiation for this session Y/N [N].

    ---
12. SSL renegotiation is disabled by default because the TLS, SSL protocol 3.0 or earlier are vulnerable to man-in-the-middle attack. Select “N” to disable the SSL renegotiation and “Y” to enable the SSL renegotiation. Enabling the SSL renegotiation leaves the system open to possible man-in-the-middle attacks. We recommend you to enable the SSL renegotiation when using the x509 certificate based authentication under the following scenarios:

    12a Browser to identity provider when using the x509 certificate based authentication.

    12b Identity provider to identity provider communication when using the x509 certificate for mutual authentication.

    12c Secure LDAP connections with mutual authentication into the LDAP user store.
13. To start the install, click *Install*.

14 (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.

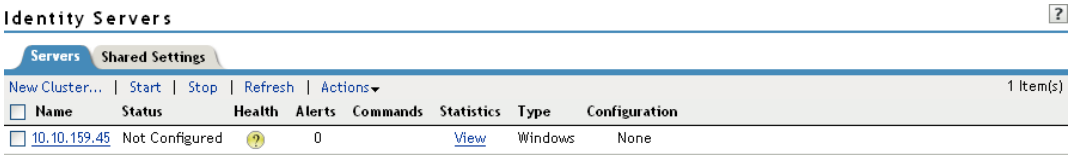
15 (Optional) After the installation finishes, view the install log file found in the following location:

Windows Server 2003: `\Program Files\Novell\log\AccessManagerServer_InstallLog.log`

Windows Server 2008: `\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`

16 (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 55).

After you log in to the Administration Console, click *Devices* > *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.

17 Continue with one of the following:

- To install an Access Gateway, see Chapter 6, "Installing the Linux Access Gateway Appliance," on page 65 or Chapter 7, "Installing the Access Gateway Service," on page 75.
- To configure the Identity Server, see "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Setup Guide*.

Installing the Linux Access Gateway Appliance

6

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

What you need to know	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console. ◆ Static IP address for the Access Gateway. ◆ DNS name (host and domain name) for the Access Gateway that resolves to the IP address. ◆ Subnet mask that corresponds to the IP address for the Access Gateway. ◆ IP address of your network's default gateway. ◆ IP addresses of the DNS servers on your network. ◆ IP address or DNS name of an NTP server.

The Linux Access Gateway Appliance can be installed on all supported hardware platforms for *SUSE Linux Enterprise Server (SLES) 11*.

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 9.6.5, "Installing or Updating the Latest Linux Patches," on page 111.

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

6.1 Prerequisites for the Access Gateway 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 Access Gateway Appliance. See "Installing the Access Manager Administration Console" on page 49.

- ❑ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the SUSE Linux Enterprise Server 11 Installation Guide (http://www.novell.com/documentation/sles11/book_sle_deployment/?page=/documentation/sles11/book_sle_deployment/data/book_sle_deployment_pre.html).
- ❑ If a firewall separates the Access Gateway 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 SP4 Setup Guide*.
  - To import the Access Gateway Appliance into the Administration Console, you must enable the ICMP protocol. For information on how to do this, see Section 4.2, "Configuring the Administration Console Firewall," on page 54.

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 the display language for the installation. However. the Linux Access Gateway supports only the English language.
- **F3:** Lets you select different graphical display modes for the installation. Also included is an entry to select the text mode. Use this mode if there are issues with the installation in the graphical mode.
- **F4:** Lets you choose the installation media if you want to use a different source, such as HTTP or NFS, instead of the installation disk. You are prompted to specify the details of the server and the network settings.

  If you are using HTTP for installation and are prompted to specify the location of the control files, select http://<*serveraddress*>/<*directory_name*>/control_files/.

  Only HTTP and NFS mode of installation are supported by the Access Gateway Appliance.
- **F5:** Lets you select whether to install the Access Gateway Appliance with the *Default Kernel*, *Safe Settings*, *No ACPI*, or with *No Local APIC* options.
- **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 Installing the Access Gateway Appliance

The Linux Access Gateway Appliance is installed with the following default partitions:

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

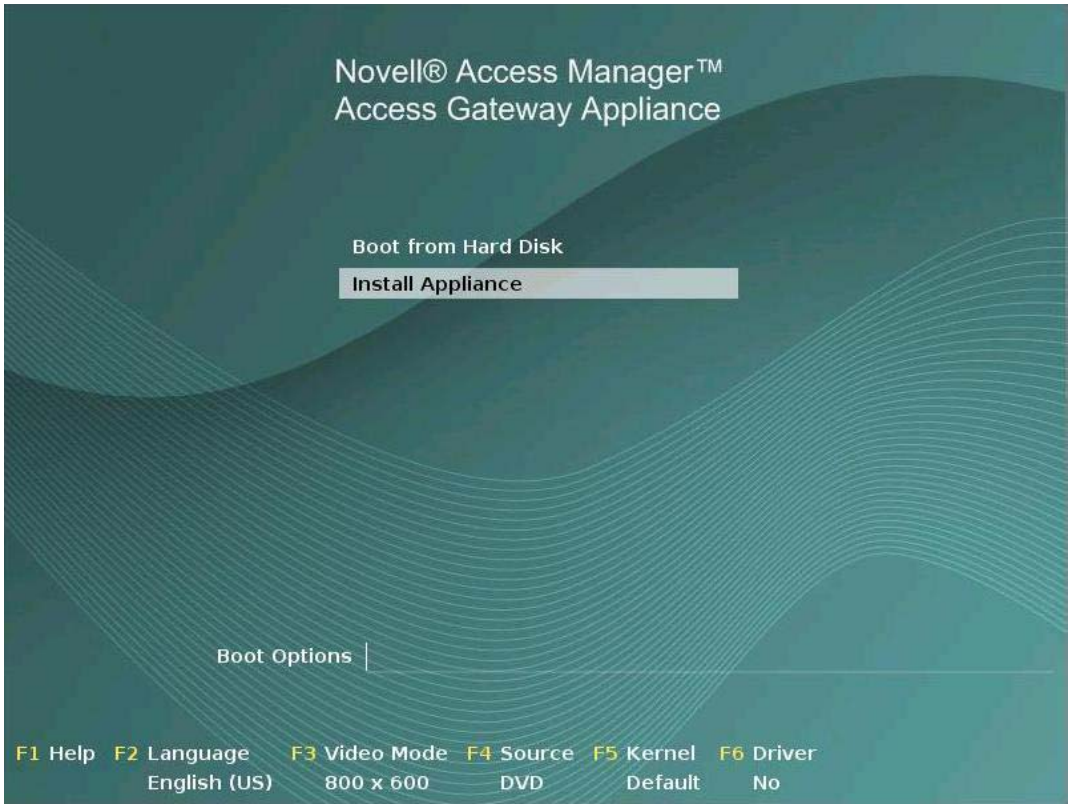
The remaining disk space after the creation of the /boot and swap partitions is allocated as the extended drive. The extended drive has the following partitions:

- **root:** The default size is one-third the size of the 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 (0X68):** Created with the remaining free space on the extended drive.

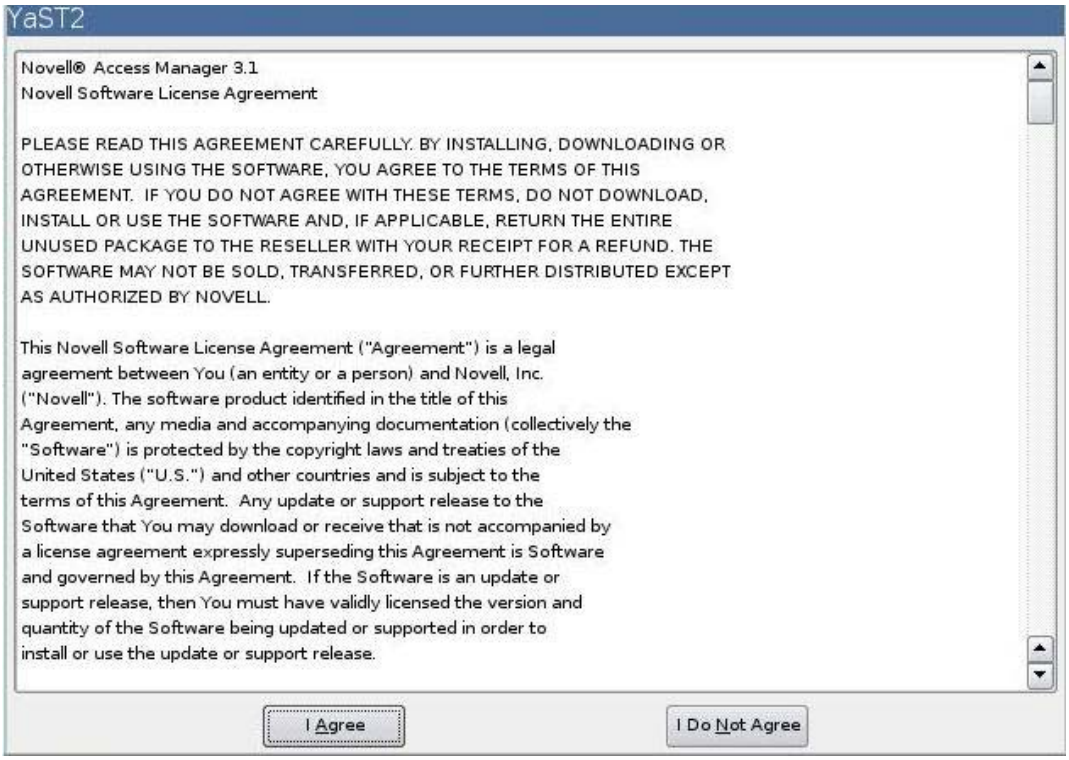
The Linux Access Gateway Appliance does not support configuring multiple network interfaces during installation. The eth0 interface is configured by default, and if you require multiple interfaces, you can configure them through the Administration Console after installation.

1. Insert the Access Gateway 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 *Install Appliance*.
3. (Optional) Use the function key options to change installation settings as desired. For example, you can press F4 to perform a network installation.For more information on these function keys, see Section 6.2, “Boot Screen Function Keys,” on page 66.
4. After you have made your installation selections, press Enter.

   The License Agreement page is displayed.

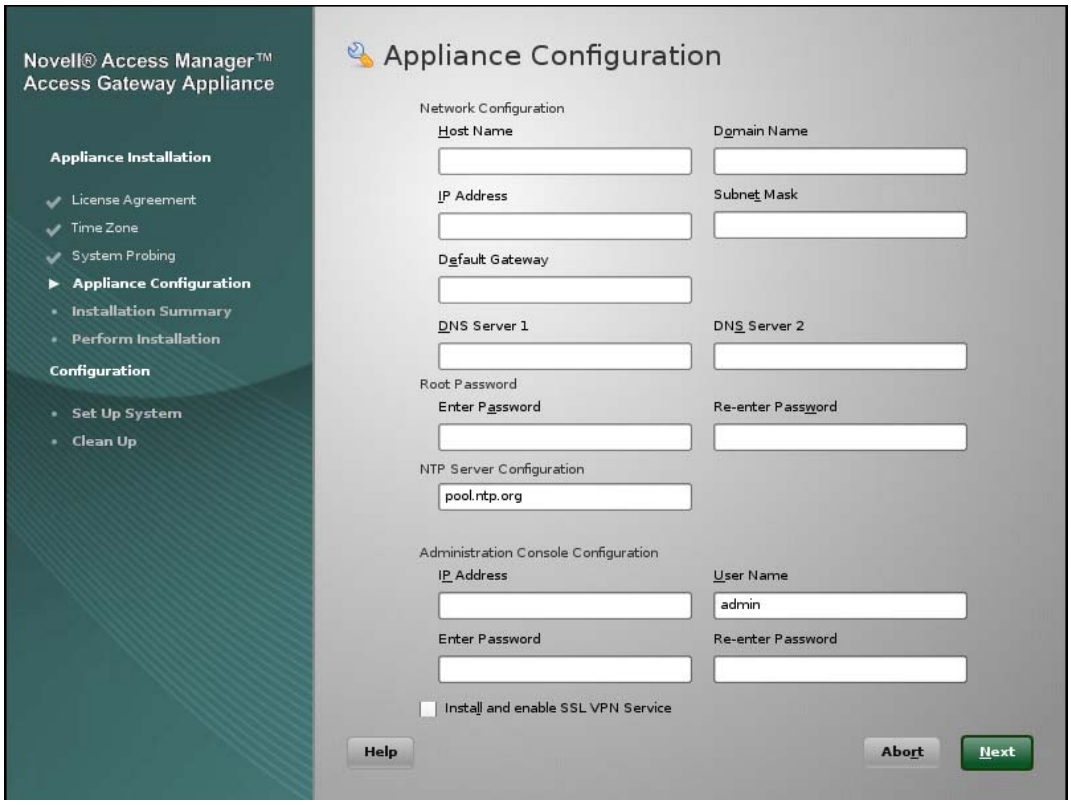


5 Review the agreement on the License Agreement page, then click *I Agree* to accept the agreement. The Clock and Time Zone page is displayed.

6 Select the region and time zone.

7 (Conditional) If the date and time are not the same as the date and time on the Administration Console, click Change, adjust the date and time.

8 Click *Next*. The Appliance Configuration page is displayed.



9 Configure the details on the Appliance Configuration page:

Host Name: The hostname for the Linux Access Gateway Appliance machine.

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

---

Domain Name: The domain name for your network.

IP Address: The IP address of the Access Gateway.

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

Default Gateway: The IP address of the default gateway.

DNS Server 1: The IP address of your DNS server. You must configure at least one DNS server.

DNS Server2: The IP address of your additional DNS server. This is an optional configuration.

Specify the following information in the Root Password section:

Enter Password: Specify a password for the `root` user.

Re-enter Password: Specify the password for `root` user again for verification.

NTP Server Configuration: The name of the NTP server.

Specify the following in the Administration Console configuration section:

IP Address: The IP address of the Administration Console. The Linux Access Gateway Appliance is imported into this Administration Console. If you select the *Install and Enable SSL VPN Service* option, the SSL VPN server is also imported into the Administration Console.

Username: The name of the Administration Console user.

Enter Password: Specify the password for the user.

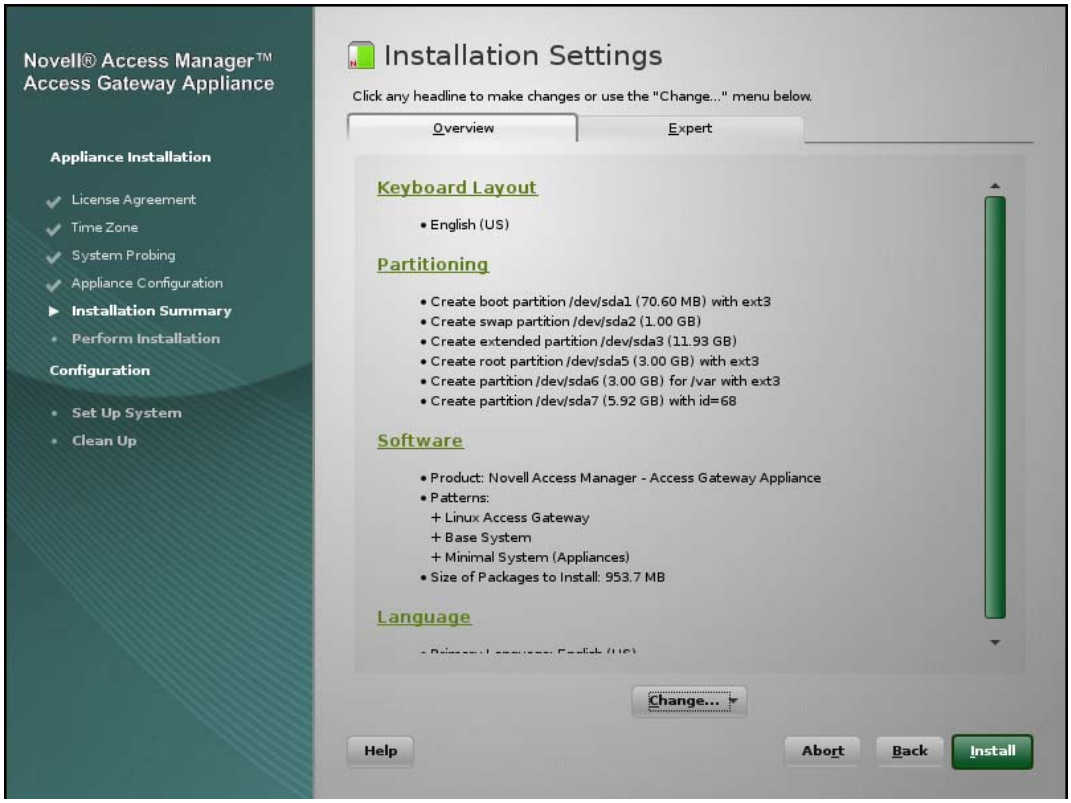
Re-enter Password: Specify the password again for verification.

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

IMPORTANT: You cannot uninstall the SSL VPN server that is installed with the Linux Access Gateway Appliance.

---

10 Click *Next*. The Installation Settings page appears.



This page displays the options and software you selected in the previous steps. Use the Overview tab for a list of selected options, or use the Expert tab for more details.

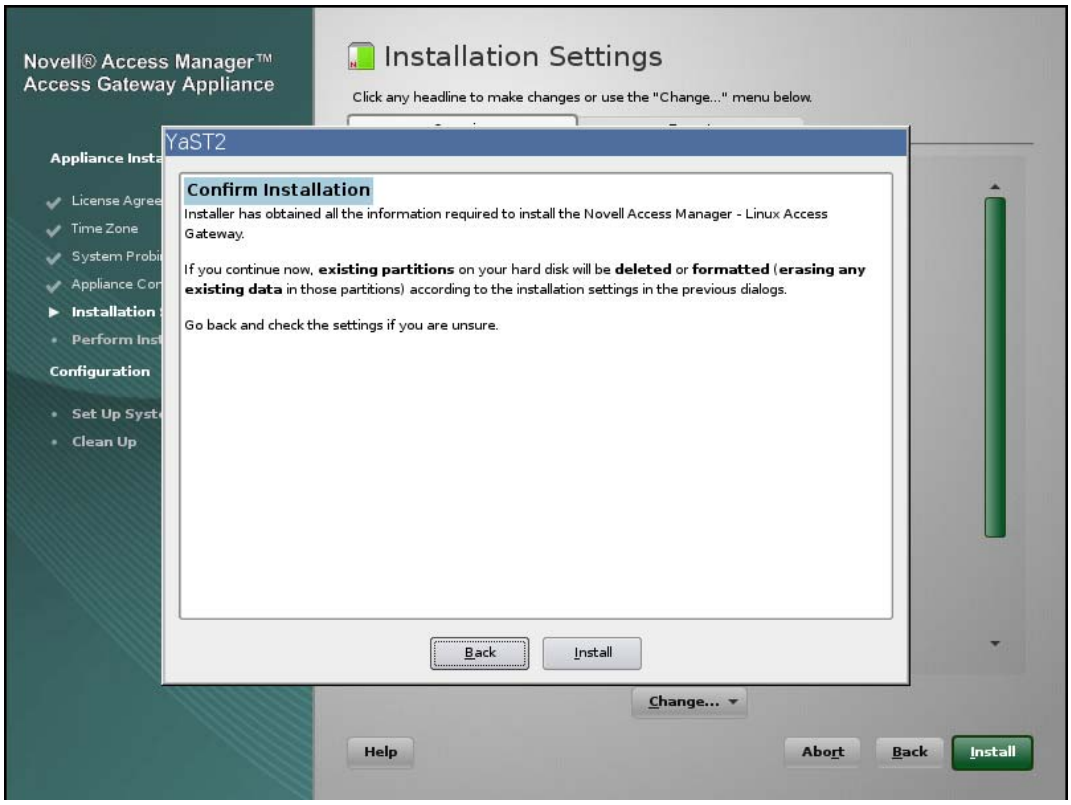
NOTE: Do not change the software selections listed on this screen.

This screen does not display SSL VPN as a selected pattern even when the *Install and enable SSL VPN Service* option is selected.

---

11 (Optional) To modify the installation settings for partitions, click *Change*. For more information on partitions, see Section 6.4, “Creating Custom Partitions,” on page 72.

12 Click *Install* to continue with the installation process.



13 Click *Install* to confirm.

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 import script, and then the Linux Appliance is imported to the Administration Console.

14 (Optional) To verify the installation of the Linux Access Gateway Appliance, log in to the Administration Console (see Section 4.3, “Logging In to the Administration Console,” on page 55), 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.

NOTE: The Access Gateway Appliance health is displayed as green instead of yellow, even before a trust relationship is established between an Embedded Service Provider and the Access Gateway. You must establish a trust relationship with the Identity Server before you proceed with any other configuration.

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 Section A.7, "Troubleshooting the Access Gateway Import," on page 182.

15 Continue with one of the following sections:

- "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Setup Guide*
- Section 6.5, "Viewing the Linux Installation Log," on page 74

6.4 Creating Custom Partitions

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

Table 6-1 *Access Gateway Appliance Partitions*

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	We recommend that you create a swap partition that is twice the size of the RAM installed on the machine.
var	This partition is highly recommended if you turn on logging. The var partition should take about 25% of available disk space.
COS (0X68)	This partition should be as large as possible. This partition holds the caching objects of the Access Gateway.

To create your custom partitions:

1 From the Installation Settings page, click *Change*, then select *Partitioning*. (See Step 11 on page 71.)

This page lists the partition settings as currently proposed.

2 Select *Custom partitioning*, then click *Next*.

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

4 Create a root partition as follows:

4a Click *Add*, select the primary or extended partition, then click *OK*.

4b Fill in the following fields:

Format: Make sure that *Format* is selected.

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

File system: Select *Ext3* for the type.

Custom Size: Specify a value.

Mount Point: Select /.

4c Click *Finish*.

5 Create a swap partition as follows:

5a Select the hard drive, click *Create*, select the primary or extended partition, then click *OK*.

5b Fill in the following fields:

Format: Make sure that *Format* is selected.

File system: Select *Swap* for the type.

Custom Size: Specify `a value`.

Mount Point: Leave the default value of *swap*.

5c Click *Finish*.

6 Create a var partition as follows:

6a Select the hard drive, click *Add*, select the primary or extended partition, then click *OK*.

6b Fill in the following fields:

Format: Make sure that *Format* is selected.

File system: Select *Ext3* for the type.

Custom Size: Specify a value.

Mount Point: Select */var*.

6c Click *Finish*.

7 Create a COS partition that uses the remaining space on the hard disk:

7a Select the hard drive, click *Add*, select the primary or extended partition, then click *OK*.

7b Fill in the following fields:

Do Not Format Partition: Select this option.

File system ID: Specify *0x68* as the ID.

Custom Size: Accept the default value for the *End* cylinder value.

Do not Mount the Partition: Select this option.

7c Click *Finish*.

8 Click *Accept* to create partitions with the specified values.

9 In the installation Summary page, verify that the partitions you specified are listed, then continue with Step 12 on page 71.

Limitations of the Disk Size

The Linux Access Gateway has minimum required of a 30GB disk and the recommended size is about 100GB. The COS partition should be at least "4x" as the maximum downloadable file size.

For example - If we have a disk size of X, then our COS partition will be a maximum of Y, and any objects accessed through the Linux Access Gateway of size > Y will not work.

Trying to download Linux Access Gateway files which have a size above 520MB might end up by a browser freeze, slowdown and broken (truncated) files. For more information, see TID 7005294 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7005294&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119)

6.5 Viewing the Linux Installation Log

During installation, the Linux Appliance generates a log file detailing the installation progress. The install log is available at `/tmp/novell_access_manager/inst_lag.log`.

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

The log has the following format:

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

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

Installing the Access Gateway Service

7

Installation time: about 10 minutes.

What you need to know	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console.

7.1 Prerequisites

- ❑ An Administration Console must be installed before you can install the Access Gateway Service. See “Installing the Access Manager Administration Console” on page 49.
- ❑ An Identity Server must be installed and configured before installing the Access Gateway Service. See Chapter 5, “Installing the Novell Identity Server,” on page 59.
- ❑ Verify that the machine meets the minimum requirements. See Section 3.6, “Access Gateway Requirements,” on page 40.
- ❑ Verify that the time on the machine is synchronized with the time on the Administration Console. If the times differ, the Access Gateway Service does not import into the Administration Console.
- ❑ If a firewall separates the machine 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 SP4 Setup Guide*.
- ❑ If you are using a VNC client to connect to the Linux machine, do not use the numeric keypad to enter numbers. Some VNC configurations have key conversion problems.
- ❑ Because the Access Gateway Service is running as a service, you need to be aware that the default ports (80 and 443) that the Access Gateway Service uses might conflict with the ports of other services running on the machine. If there is a conflict, you need to decide which ports each service can use.
- ❑ (Windows Server 2008) If the Web server (IIS) has been installed by default during the Windows Server 2008 install, the Access Gateway Service installation program detects its presence from the registry and issues a shutdown command. Even if you have never activated the Web server and if even it is not running, the shutdown command is issued. Because the Access Gateway Service cannot be installed while the IIS server is running, the installation program needs to ensure that it is not running.

7.2 Installing the Access Gateway Service

1. Log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the software, or for an evaluation version, download the media kit from Novell Downloads (http://download.novell.com/index.jsp).
2. Copy the file to your machine.

   For the filename, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
3. (Linux) Prepare your machine for installation:

   3a Make your Linux installation media available.

   The installation program checks for Apache dependencies and installs any missing packages.

   3b Grant execute rights to the file with the following command:

```
chmod +x <filename>
```

   Replace <*filename*> with the name of the file.
4. (Windows) Disable any virus scanning programs.
5. (Windows) To use a remote desktop for installation, use one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
6. Start the installation program.

   Linux (graphical): Enter the following command:

```
./<filename>
```

   Replace <*filename*> with the name of the file.

   Linux (text-mode): Enter the following command:

```
./<filename> -i console
```

   Replace <*filename*> with the name of the file.

   If you use text mode, answer the questions rather than following the instructions below. When you are prompted for the admin password, ignore the hard-coded asterisk.

   Windows: Double click the executable file.
7. (Linux only) If missing dependencies are found, click *Continue* to install them.
8. Read the welcome page, then click *Next*.
9. View the Readme, then click *Next*.
10. Review and accept the License Agreement.
11. Specify the following information:

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

    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.

Local IP Address: (Conditional) If your machine has more than one IP address, specify the IP address that you want the Access Gateway Service to use.

12 Configure disk cache. This holds the caching objects of the Access Gateway (if you are familiar with the Access Gateway Appliance, this is the COS partition).

Size in MB: Specify from 1024 MB to 20% of your hard disk space. The default is 1 GB.

Directory: (Windows only) Specify the location for the disk cache. This needs to be in a secure location on an NTFS file system. The default is the `C:\apache_cache_root` directory.

13 Click *Next*, then review the installation summary.

14 To start the installation, click *Install*.

15 Review the log information.

Linux: Change to the `/tmp/novell_access_manager/` directory and view the following files:

```
ags_install_<timestamp>.log
AccessGateway_InstallerLog-<timestamp>.log
```

Windows: View the files in the following directories:

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

16 Click *Next*, then click *Done*.

17 (Optional) To verify that the Access Gateway Service imported into the Administration Console, wait two minutes, log into the Administration Console, then click *Devices* > *Access Gateways*.

At this point, the Access Gateway Service is in an unconfigured state.

18 Continue with the one of the following:

- "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Setup Guide*
- Install another Access Manager component.

7.3 Silently Installing the Access Gateway Service

To silently install the Access Gateway Service, you must create a properties file that contains the values that the installation program requires.

1 Log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the software, or for an evaluation version, download the media kit from Novell Downloads (http://download.novell.com/index.jsp).

2 Copy the file to your machine.

For the filename, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)

3 (Linux only) Prepare your machine for installation:

3a Make your Linux installation media available.

The installation program checks for Apache dependencies and installs any missing packages.

3b Grant execute rights to the file with the following command:

```
chmod +x <filename>
```

4 Create the properties file with the information that matches your set up. The following properties are supported:

Property	Description
AM_INSTALL_JCC_ADMIN_SERVER_IP_SERVER	The IP address of the Administration Console.
AM_INSTALL_JCC_ADMIN_NAME	The username of administrator for the Administration Console.
AM_INSTALL_JCC_ADMIN_PASSWORD1 AM_INSTALL_JCC_ADMIN_PASSWORD2	The password of the administrator user for the Administration Console.
AM_INSTALL_JCC_BIND_ADDRESS_TO_USE	The IP address of the Access Gateway Service machine.
DISK_CACHE_SIZE	The amount of disk space to reserve for the caching objects of the Access Gateway. If you are familiar with the Linux Access Gateway Appliance, this is the COS partition.

Your file should look similar to this example:

```
#Server Communications Configuration
#-----------------------------------
AM_INSTALL_JCC_ADMIN_SERVER_IP_SERVER=10.10.159.206
AM_INSTALL_JCC_ADMIN_NAME=admin
AM_INSTALL_JCC_ADMIN_PASSWORD1=novell
AM_INSTALL_JCC_ADMIN_PASSWORD2=novell
AM_INSTALL_JCC_BIND_ADDRESS_TO_USE=10.10.159.41

#Disk Cache Information
#----------------------
DISK_CACHE_SIZE=1024
```

If you want the installation program to generate the file as you install the Access Gateway Server (so you can use it with future installations and upgrades), enter the following installation command:

Linux: `./<filename> -r <filename>.properties`

Windows: `<filename> -r <filename>.properties`

Replace `<filename>` with the name of the executable. Replace `<filename>.properties` with the name of the properties file you want to create, such as `installer.properties`.

The password values are not written to the file. You need to edit the file manually to add them.

The installation program generates the file only for a new installation. If you have already installed the Access Gateway Service, you must create the file manually.

5 (Windows only) Disable any virus scanning programs.

6 To start the silent install, enter the following command:

Linux: `./<filename> -i silent -f <filename>.properties`

Windows: `<filename> -i silent -f <filename>.properties`

Replace *<filename>* with the name of the executable. Replace *<filename>*.properties with the name of the properties file. If the properties file is not in the same directory as the executable, include the path with the filename.

7 When the installation completes, review the log information.

Linux: Change to the /tmp/novell_access_manager/ directory and view the following files:

```
ags_install_<timestamp>.log
AccessGateway_InstallerLog-<timestamp>.log
```

Windows: View the files in the following directories:

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

8 (Optional) To verify that the Access Gateway Service imported into the Administration Console, wait two minutes, log into the Administration Console, then click *Devices* > *Access Gateways*.

At this point, the Access Gateway Service is in an unconfigured state.

9 Continue with the one of the following:

- "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Setup Guide*
- Install another Access Manager component.

Installing the SSL VPN Server

8

Installation time: about 10 minutes.

What you need to know to install the SSL VPN server	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console.

The Novell SSL VPN can be installed as an ESP-enabled SSL VPN, or as a Traditional SSL VPN along with the Access Gateway. You can also install the high bandwidth version of SSL VPN after installing the SSL VPN server, if export laws permit.

8.1 Installing the ESP-Enabled SSL VPN

When SSL VPN is deployed without the Access Gateway, an Embedded Service Provider (ESP) component is installed along with the SSL VPN server. This deployment is called an ESP-enabled Novell SSL VPN. This deployment requires the Administration Console and the Identity Server to be installed before the SSL VP server is installed.

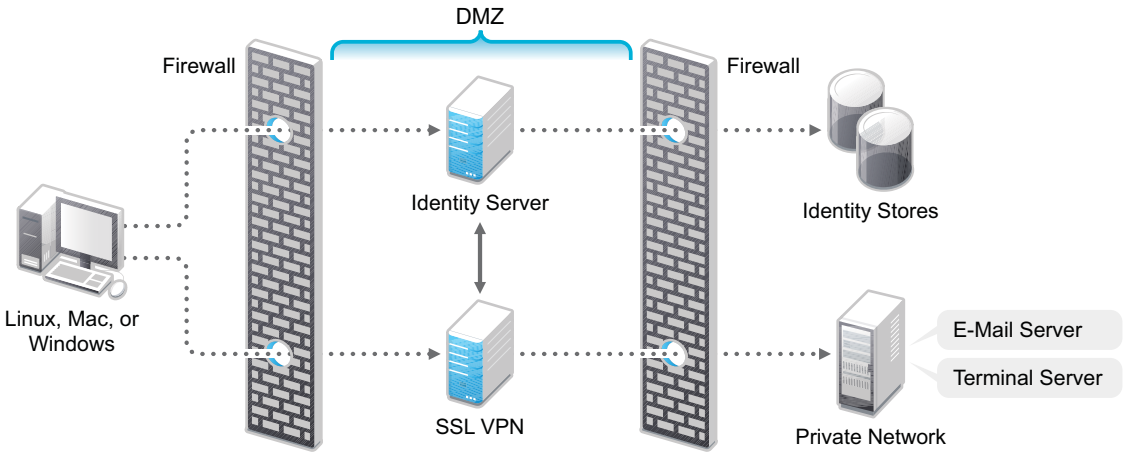
8.1.1 Deployment Scenarios

For installing the ESP-enabled version of SSL VPN, you have the following deployment scenarios:

Deployment Scenario 1: Installing SSL VPN on a Separate Machine

This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are deployed separately, without the Access Gateway. For installation instructions for this scenario, see “Installing the ESP-Enabled SSL VPN” on page 84.

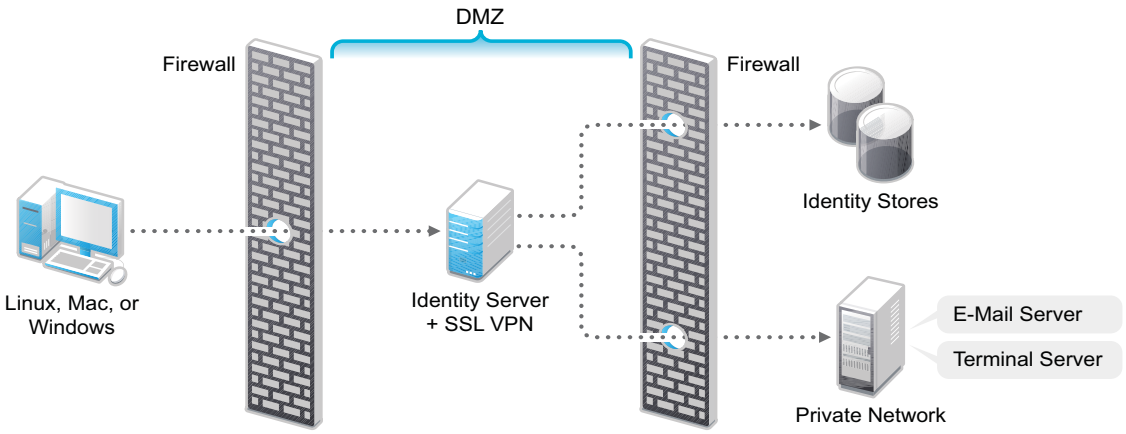
Figure 8-1 *Deployment Scenario 1*



Deployment Scenario 2: Installing SSL VPN and the Identity Server on the Same Machine

This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on a single machine. The Access Gateway is deployed separately. For installation instructions for this scenario, see “Installing the ESP-Enabled SSL VPN” on page 84.

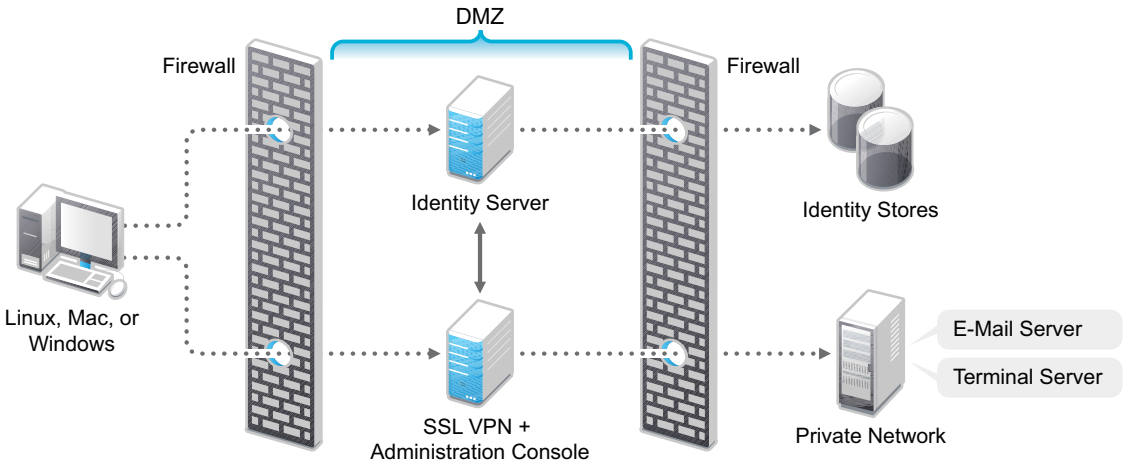
Figure 8-2 *Deployment Scenario 2*



Deployment Scenario 3: Installing SSL VPN and the Administration Console on the Same Machine

This deployment scenario consists of a demilitarized zone where the SSL VPN, and Administration Console are on the same machine and the Linux Access Gateway and the Identity servers are deployed separately. For installation instructions for this scenario, see “Installing the ESP-Enabled SSL VPN” on page 84.

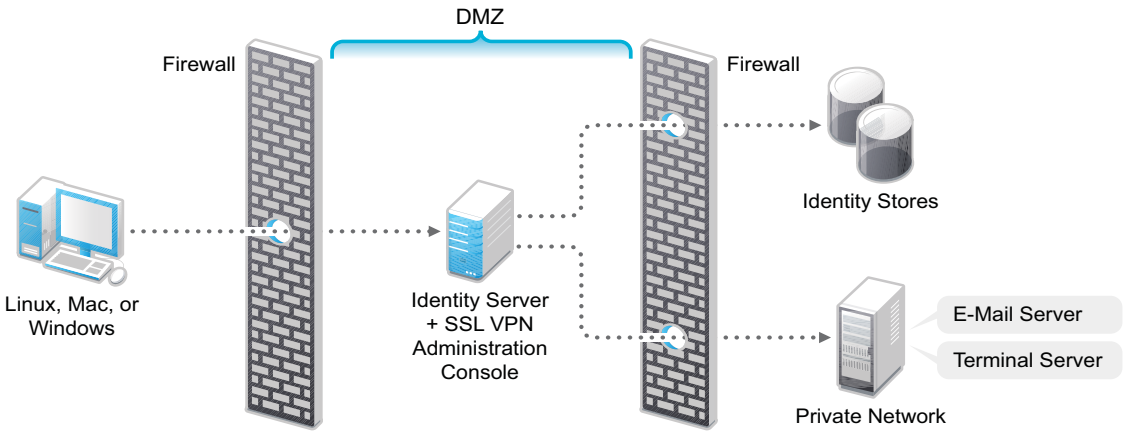
Figure 8-3 *Deployment Scenario 3*



Deployment Scenario 4: Installing SSL VPN, the Administration Console, and the Identity Server on the Same Machine

This deployment scenario consists of a demilitarized zone where the Identity Server, SSL VPN, and Administration Console are on the same machine and the Linux Access Gateway is deployed separately. For installation instructions for this scenario, see “Installing the ESP-Enabled SSL VPN” on page 84.

Figure 8-4 *Deployment Scenario 4*



8.1.2 Installing the ESP-Enabled SSL VPN

The following installation steps are applicable to all the deployment scenarios of the ESP-enabled SSL VPN. The individual scenarios are explained in "Deployment Scenarios" on page 81.

1 Access the install script.

1a Make sure you have downloaded the software or that you have the CD available.

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

1b Do 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 by using the following command:

  `tar -xzvf <filename>`

1c Change to `the novell-access-manager-3.1.2-xxx` directory.

2 At a command prompt, enter the following install script command:

`./install.sh`

You are prompted to select an installation.

3 Type 4 to install the ESP-Enabled SSL VPN, then press Enter.

4 Review and accept the License Agreement.

5 (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.

6 Specify the name of the administrator for the Administration Console.

7 Specify the administration password.

8 Confirm the password.

9 (Conditional) If you are installing the SSL VPN server on the same machine as the Administration Console, you are not prompted for the IP address of the Administration Console. If the Administration Console is on a different machine, provide the IP address when you are prompted for it.

10 Wait while the SSL VPN server is installed on your system and imported into the Administration Console. This takes about 2 minutes.

The installation ends with the following message: `Installation complete.`

11 To verify the installation of the SSL VPN, continue with Section 8.4, "Verifying That Your SSL VPN Service Is Installed," on page 91.

12 Add an entry in `/etc/hosts` file to map the SSLVPN server IP address with the domain name which the client is using to connect.

13 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 8.3, "Installing the Key for the High-Bandwidth SSLVPN," on page 91.

8.2 Installing the Traditional SSL VPN Server

The traditional SSL VPN server does not have an Embedded Service Provider and must be configure as a protected resource of an Access Gateway. You can install the traditional SSL VPN server with the Linux Access Gateway Appliance, with the Identity Server, with the Administration Console, or on a separate machine.

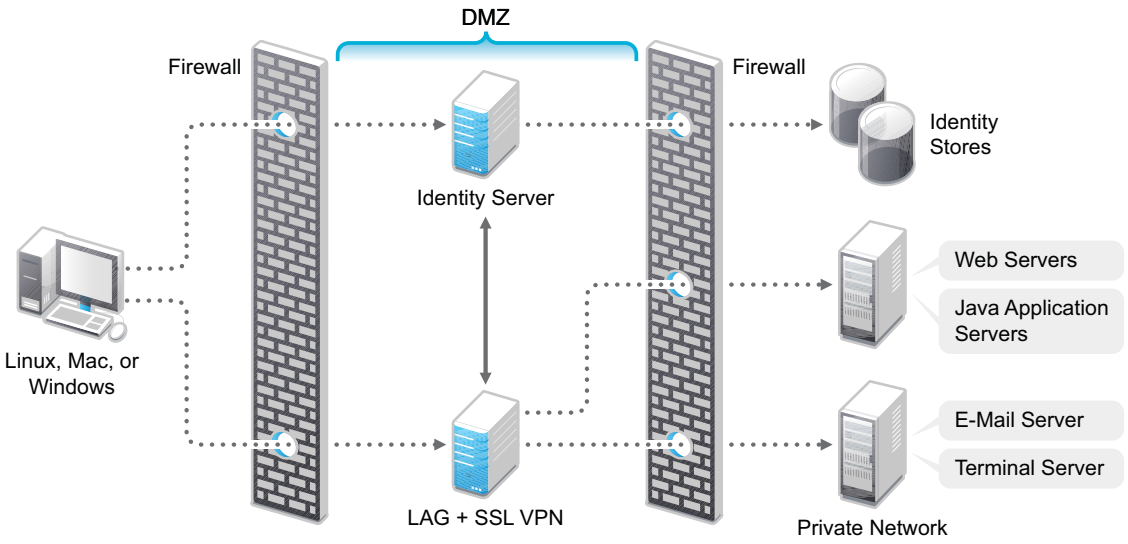
8.2.1 Deployment Scenarios

The traditional SSL VPN server supports the following installation scenarios:

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

This deployment scenario consists of a demilitarized zone where the Linux Access Gateway and SSL VPN are on the same server and the Identity Server is deployed separately. For installation instructions for this scenario, see “Installing SSL VPN with the Linux Access Gateway Appliance” on page 88.

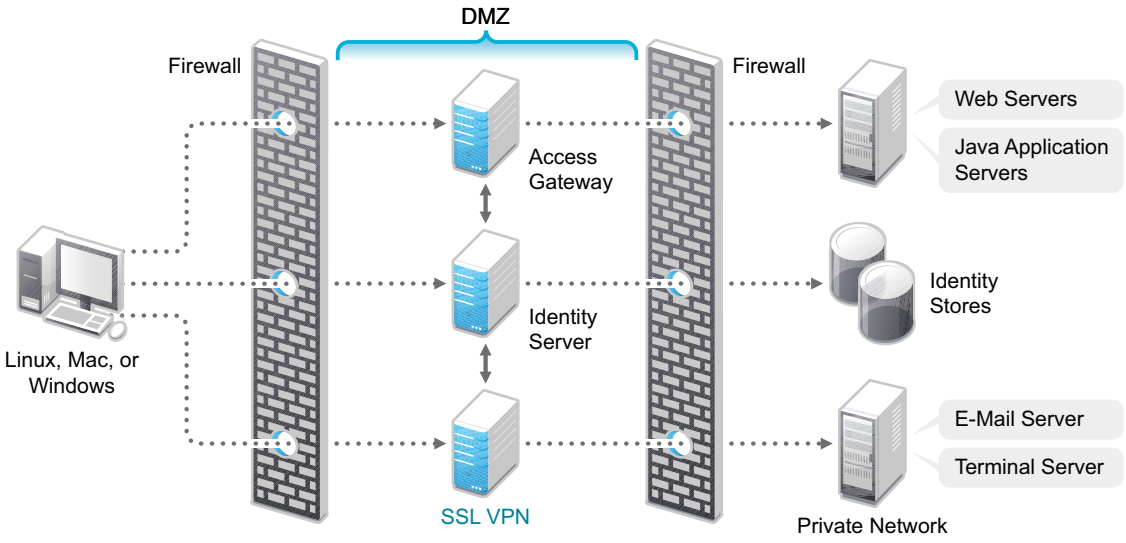
Figure 8-5 *Deployment Scenario 1*



Deployment Scenario 2: SSL VPN Server Installed on a Separate Machine

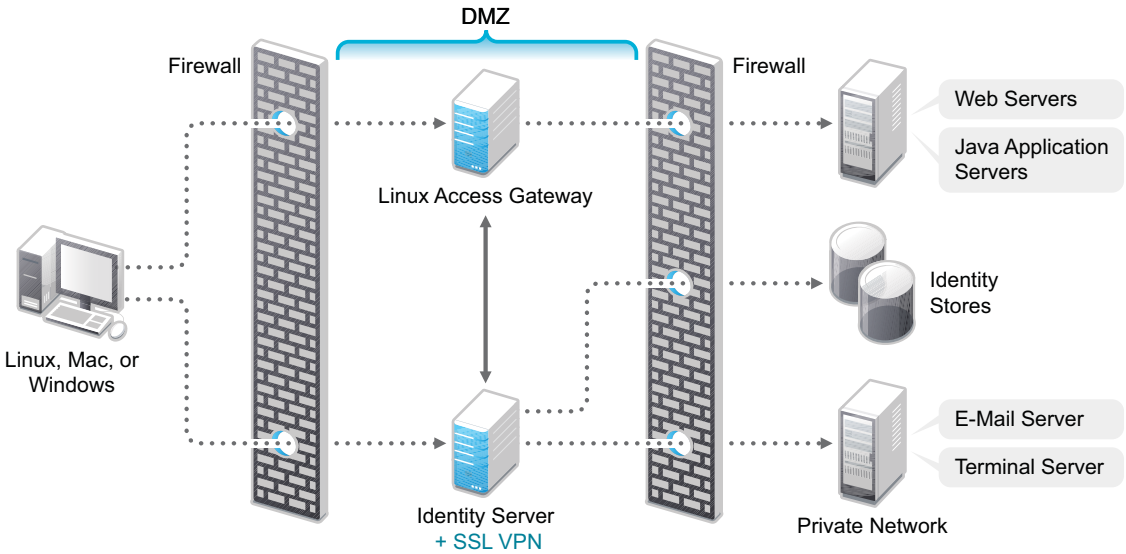
This deployment scenario consists of a demilitarized zone where the Access Gateway, Identity Server, and SSL VPN are deployed separately. For installation instructions for this scenario, see “Installing the Traditional Novell SSL VPN” on page 88.

Figure 8-6 *Deployment Scenario 2*



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

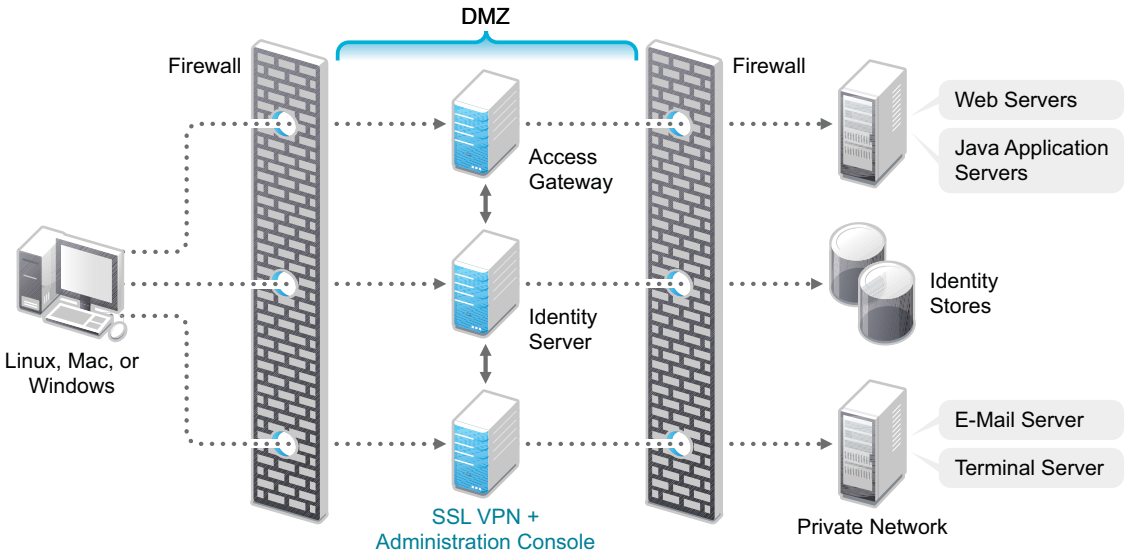
This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see “Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console” on page 89.



Deployment Scenario 4: Administration Console and SSL VPN on the Same Server

This deployment scenario consists of a demilitarized zone where the Administration Console and SSL VPN are on one machine and the Access Gateway and Identity Server are deployed separately on different machines. For installation instructions for this scenario, see “Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console” on page 89.

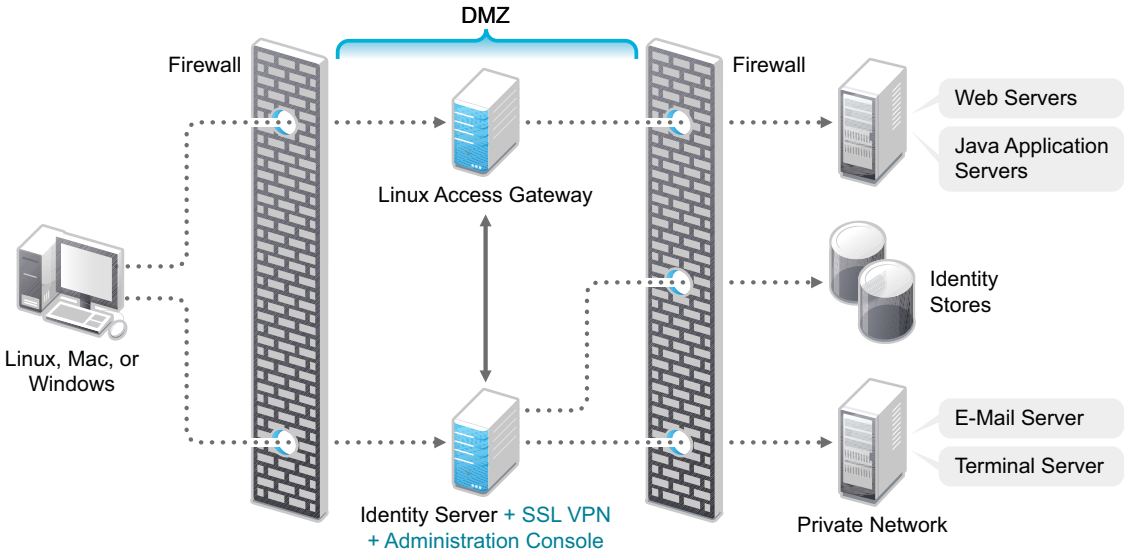
Figure 8-7 *Deployment Scenario 4*



Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server

This deployment scenario consists of a demilitarized zone where the Identity Server, Administration Console, and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see “Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console” on page 89.

Figure 8-8 *Deployment Scenario 5*



8.2.2 Installing the Traditional Novell SSL VPN

This section describes the installation procedures for different SSL VPN deployments:

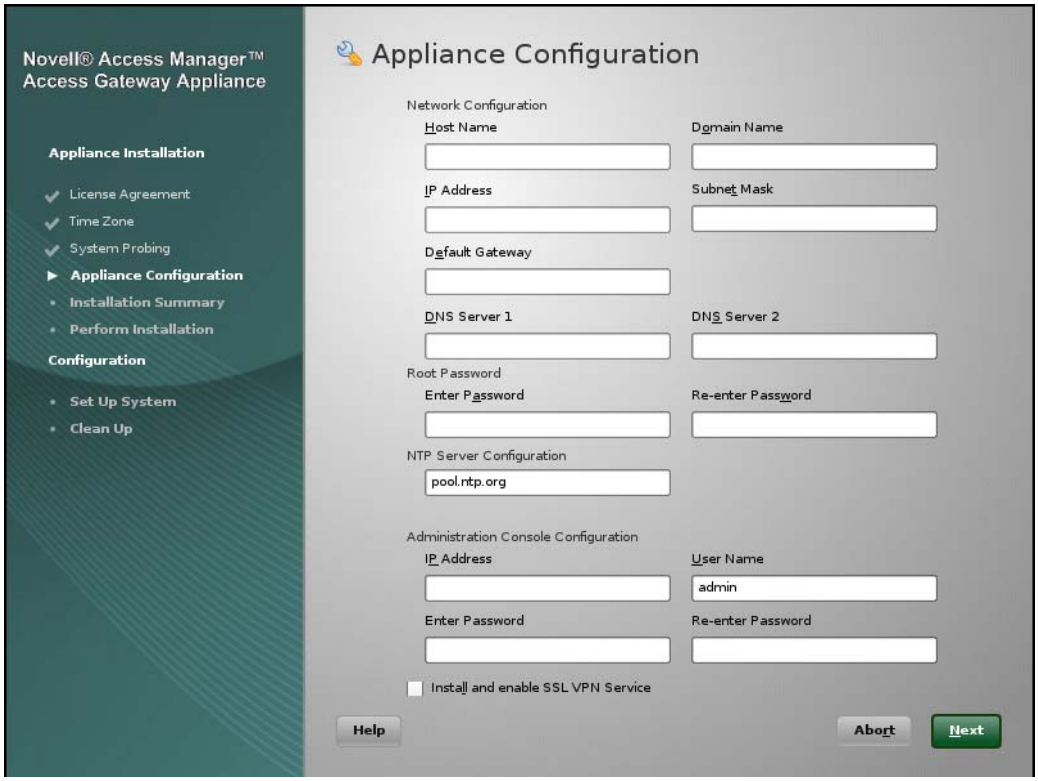
- “Installing SSL VPN with the Linux Access Gateway Appliance” on page 88
- “Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console” on page 89
- “Reinstalling SSL VPN on the Linux Access Gateway” on page 90

Installing SSL VPN with the Linux Access Gateway Appliance

When SSL VPN is installed along with Linux Access Gateway Appliance, the Access Gateway installation process installs SSL VPN along with the Linux Access Gateway.

For more information on installing the Linux Access Gateway, refer to “Section 6.3, “Installing the Access Gateway Appliance,” on page 66” in the *Novell Access Manager 3.1 SP4 Installation Guide*.

1. Start the installation of the Linux Access Gateway. For details, refer to “Section 6.3, “Installing the Access Gateway Appliance,” on page 66” in the *Novell Access Manager 3.1 SP4 Installation Guide*.
2. In the Access Administrator Configuration section in the Novell Linux Access Gateway Configuration page, select the *Install and Enable SSL VPN Server* check box to install and configure SSL VPN on the Linux Access Gateway.



3. Follow the on-screen instructions to continue with the Linux Access Gateway installation.
4. If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 8.3, “Installing the Key for the High-Bandwidth SSLVPN,” on page 91.

Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console

You can use an install script to install the traditional Novell SSL VPN on a separate machine, with the Identity Server, with the Administration Console, or with the Identity Server and the Administration Console.

1. Access the install script.
   - **1a** Make sure you have downloaded the software or that you have the CD available.

     For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html)
   - **1b** Do 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 by using the following command:

       `tar -xzvf <filename>`
   - **1c** Change to `the novell-access-manager-3.1.2-xxx` directory.
2. At a command prompt, enter the following install script command:

   `./install.sh`

   You are prompted to select an installation.
3. Type 3 to install the traditional SSL VPN server, then press Enter.
4. (Optional) When you are prompted to replace the low bandwidth SSL VPN RPM with the high bandwidth RPM, replace it if the security law permits you to do so.

   For more information on the high bandwidth SSL VPN, see "High-Bandwidth and Low-Bandwidth Versions" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*. For more information on installing the high bandwidth SSL VPN, see Section 8.3, "Installing the Key for the High-Bandwidth SSLVPN," on page 91.
5. Review and accept the License Agreement.
6. (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.
7. Specify the name of the administrator for the Administration Console.
8. Specify the administration password.
9. Confirm the password.
10. Specify the IP address of the Administration Console.
11. Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.

    The installation ends with the following message: `Installation complete.`
12. To verify the installation of the SSL VPN, continue with Section 8.4, "Verifying That Your SSL VPN Service Is Installed," on page 91.
13. If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 8.3, "Installing the Key for the High-Bandwidth SSLVPN," on page 91

Reinstalling SSL VPN on the Linux Access Gateway

If you have deleted the SSL VPN server installed along with the Linux Access Gateway from Administration Console, then to re-import it follow the below steps.This is required because SSLVPN does not have a script to import the device to Administration Console.

1. Uninstall the installed SSLVPN rpms by running the `uninstall.sh` script from `/opt/novell/idp-devman-install/` directory. This step is very important. If you have not uninstalled the rpms and try to upgrade the existing rpms, the upgrade is successful but the device does not imported into the Administration Console.
2. Download and copy the Novell Access Manager `tar.gz` files to the Linux Access Gateway machine.

   For the actual filenames and download instructions, see the Novell Access Manager Readme (http://www.novell.com/documentation/novellaccessmanager/readme/accessmanager_readme.html).
3. Unpack the `tar.gz` file by using the following command:

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

4. Change to `novell-access-manager-<release-version>` directory. At the command prompt, enter the following install script command:

   ```
   ./install.sh
   ```
5. You are prompted to select an installation. In case of SSLVPN installed on Linux Access Gateway, you would see only one option to install SSLVPN alone.
6. To install the Novell SSL VPN Agent, press Enter.
7. A note with respect to High-Bandwidth rpm key will be displayed. Press Enter to proceed.

   NOTE: You are attempting to install the SSLVPN server and this install program has detected that the High-Bandwidth Key rpm for SSLVPN is not installed. The High-Bandwidth Key rpm is not packaged with the SSLVPN install media in order to comply with the USA Export Laws. You can install the novl-sslvpn-hb-key rpm at any time later to turn on the High-Bandwidth capability on this machine. Please refer to the documentation to download and install the novl-sslvpn-hb-key rpm.

   ---
8. Review and accept the License Agreement.
9. (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server when you are prompted to do so.
10. Specify the IP address of the Administration Console when prompted.
11. Specify the name of the administrator for the Administration Console.
12. Specify the administration password.
13. Confirm the password.
14. Wait while the SSL VPN server is installed on your system and imported into the Administration Console, which takes about 2 minutes.

    The installation ends with the following message: `Installation complete.`
15. To verify the installation of the Access Gateway, continue with Section 8.4, “Verifying That Your SSL VPN Service Is Installed,” on page 91.

8.3 Installing the Key for the High-Bandwidth SSLVPN

Customers who are eligible to install the high bandwidth SSL VPN can install the key for the high bandwidth SSL VPN after they get the export clearance. This key is installed only once. There is no need to upgrade the RPM every time the servlet and the server RPMs for SSL VPN are upgraded. In the previous releases, you needed to upgrade the high bandwidth RPMs every time the SSL VPN server and servlet RPMs were upgraded. With Access Manager 3.1 or later, you install the key once and can upgrade to new versions without installing the key again.

You must install the high bandwidth SSL VPN if you want to cluster the SSL VPN servers.

To install the RPM:

1. After you have ordered the high bandwidth version, log in to the Novell Customer Center (http://www.novell.com/center) and look for the link that allows you to download the RPM containing key for the high bandwidth version.
2. Download the following high bandwidth RPM:

   `novl-sslvpn-hb-key-3.1.0-0.noarch.rpm`
3. Log in as `root`.
4. Enter the following command to stop all services:

   `/etc/init.d/novell-sslvpn stop`
5. Enter the following command to install the RPM for the high bandwidth version of SSL VPN:

   `rpm -ivh novl-sslvpn-hb-key-3.1.0-0.noarch.rpm`
6. Enter the following command to restart all SSL VPN services:

   `/etc/init.d/novell-sslvpn start`
7. Enter the following command to check the status:

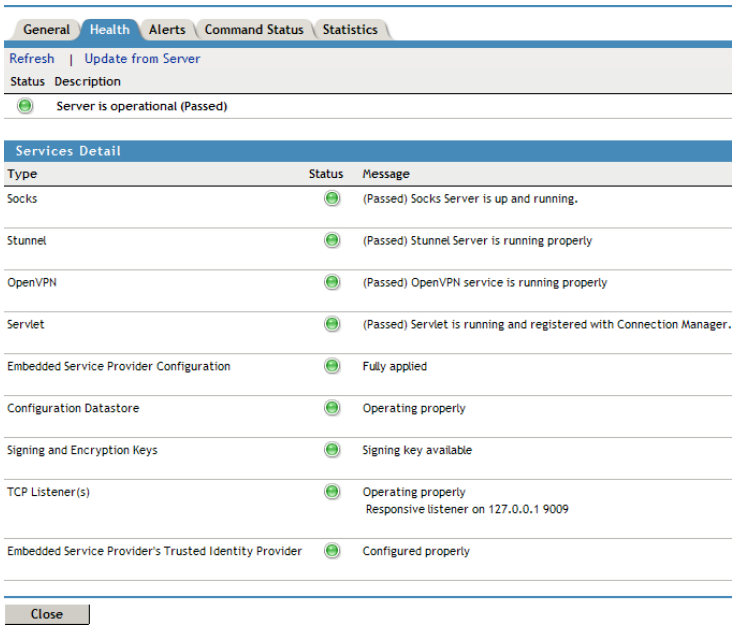
   `/etc/init.d/novell-sslvpn status`

8.4 Verifying That Your SSL VPN Service Is Installed

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

1. In the Administration Console, click *Devices* > *SSL VPNs*.

   A list of SSL VPN servers appears, displaying their status.
2. Select a server, then click the *Health* icon to display the health of the SSL VPN server.



The initial health status of an ESP-enabled SSL VPN shows yellow because the trust relationship between the Identity Server and the Embedded Service Provider is yet to be established. For more information on how to configure the trust relationship, see "Configuring Authentication for the ESP-Enabled Novell SSL VPN" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*

3 (Optional) Continue with "Basic Configuration for SSL VPN" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*, if you have not already configured the SSL VPN server.

Upgrading Access Manager Components

9

WARNING: Before upgrading, make a backup of your configuration. For instructions, see "Backing Up the Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

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 you upgrade 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 following Access Manager components:

9.1 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. Then use the following sections for instructions on upgrading the components:

- Section 9.4, "Upgrading the Administration Console," on page 99
- Section 9.5, "Upgrading the Identity Server," on page 103
- Section 9.6, "Upgrading the Linux Access Gateway Appliance," on page 106

- Section 9.7, “Upgrading the Access Gateway Service,” on page 117
- Section 9.8, “Upgrading the SSL VPN Servers,” on page 118

9.2 Upgrading from Access Manager 3.1 SP3 or 3.1 SP3 IR2 to 3.1 SP4

Access Manager prior to 3.1 SP3 should be first upgraded to 3.1 SP3 or 3.1 SP3 IR2 before upgrading to 3.1 SP4. For more information on upgrading to 3.1 SP3, see Upgrading from Access Manager 3.1 SP2 or 3.1 SP2 IR3 to 3.1 SP3 (https://www.novell.com/documentation/novellaccessmanager313/installation/data/btfgz5h.html). For upgrading Access Manager 3.1 SP3 or 3.1 SP3 IR2 to 3.1 SP4, you need to upgrade the components in the following order:

- Administration Console
- Identity Servers
- Access Gateways
- SSL VPN Servers

IMPORTANT: The J2EE agents upgrade is not supported.

While you are upgrading the components, be aware of the following:

- You should not use any of the new SP4 features until all of your components are upgraded to SP4.
- You must upgrade the components to 3.1 SP4 before you can migrate the components to a new operating system. See Section 9.3, “Migrating to Newer Operating Systems,” on page 94.
- Back up the customized Tomcat files on your Access Manager components.

  If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.
- (Conditional) The location of the keystores on the Administration Console for the Embedded Service Provider of the Access Gateway Appliance changed in Access Manager 3.0.1. If you installed the Access Gateway Appliance with Access Manager 3.0 and upgraded it to 3.1 SP3, the keystores are in the old location. The SLES 9 Access Gateway Appliance works with the keystores in either the old or the new location. However, when you migrate your SLES 9 Access Gateway Appliances to SLES 11, the SLES 11 Access Gateway Appliance ceases to function because it cannot find the Embedded Service Provider keystores. The upgrade script automatically cleans up the keystores for you. After the upgrade, the keystores are in the new location.

9.3 Migrating to Newer Operating Systems

- Section 9.3.1, “Migrating Administration Consoles from SLES 10 to SLES 11,” on page 95
- Section 9.3.2, “Migrating Administration Consoles with or without Identity Servers from Windows 2003 to Windows 2008,” on page 97
- Section 9.3.3, “Migrating Identity Servers from SLES 10 to SLES 11,” on page 98
- Section 9.3.4, “Migrating Stand-Alone Identity Servers from Windows 2003 to Windows 2008,” on page 99
- Section 9.3.5, “Migrating the SSL VPN Server to SLES 11,” on page 99

9.3.1 Migrating Administration Consoles from SLES 10 to SLES 11

The following procedure can be used to migrate a stand-alone Administration Console or an Administration Console installed either with the Identity Server or the SSL VPN server, or both of them:

1. Make a note of the DNS name and the IP address of the primary Administration Console.
2. Back up your 3.1.4 configuration.

   For instructions, see "Backing Up the Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.
3. Move the backup configuration file to a different machine.

   If you are going to re-install on the same machine, all data of the machine is lost. If you install on new hardware, the old machine must be removed from the network.
4. (Conditional) If an Identity Server is installed on the same machine as the Administration Console:

   4a Remove the Identity Server from the L4 switch configuration.

   4b Back up any customized files on the Identity Server.
5. (Conditional) If you are planning to install the primary Administration Console on new hardware, bring down the existing primary Administration Console and remove it from the network.
6. Perform a fresh install of SLES 11.
7. 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. On SLES 11, the compat-32bit package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119).

   Use YaST to install the packages.

   Use the following command to verify:

   ```
   rpm -qa | grep <package name>
   ```
8. Copy the backup configuration file to the machine.
9. Copy the SP4 installation file to the machine.
10. Remove this machine from the network.

    NOTE: This step is required to avoid any traffic from the remote devices to this Administration Console in the current state. This also avoids any conflict between the eDirectory tree names of the primary and secondary Administration Console.
11. Install the 3.1.4 version of the Administration Console.

    Use the same IP address and DNS name. For instructions, see "Installing the Access Manager Administration Console" on page 49.

12 Restore your configuration.

For instructions, see "Restoring an Administration Console Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

13 Open iMonitor on the primary Administration Console:

13a Enter the following URL:

```
https://<ip-address>:8030/nds
```

Replace <ip-address> with the IP address of your Administration Console.

13b Disable the outbound and inbound synchronization in the primary Administration Console eDirectory.

For more information, see "Enabling/Disabling Normal Synchronization" (http://www.novell.com/documentation/edir88/edir88/data/brp2di9.html#brq79ae) in the eDirectory documentation.

14 Connect this machine to the network so that the primary Administration Console is visible to all the devices.

15 (Conditional) If an Identity Server was installed on the same machine as the Administration Console:

15a Remove the Identity Server from the cluster configuration.

15b Delete the Identity Server from the Administration Console.

15c Install the 3.1.4 version of the Identity Server.

15d Restore any customized files to the Identity Server.

15e Add the Identity Server to the cluster configuration.

15f Add the Identity Server to the L4 switch configuration.

16 (Conditional) If an SSL VPN server was installed on the same machine as the Administration Console, install the 3.1.4 version of the SSL VPN server.

17 Bring down any secondary consoles.

18 Re-enable eDirectory synchronization on the primary Administration Console:

18a Enter the following URL:

```
https://<ip-address>:8030/nds
```

Replace *<ip-address>* with the IP address of your primary Administration Console.

18b Enable the outbound and inbound synchronization.

For more information, see "Enabling/Disabling Normal Synchronization" (http://www.novell.com/documentation/edir88/edir88/data/brp2di9.html#brq79ae) in the eDirectory documentation.

19 Remove any secondary consoles from the configuration:

19a In the Administration Console, click *Auditing* > *Troubleshooting*.

19b In the *Other Known Device Manager Servers* section, use the *Remove* button to remove any secondary consoles.

20 Uninstall the secondary consoles. For instructions, see Section 10.4, "Uninstalling the Administration Console," on page 126.

21 Reinstall the secondary consoles as secondary consoles to the new primary console.

Install SLES 11, then install the SP4 version of the Administration Console.

9.3.2 Migrating Administration Consoles with or without Identity Servers from Windows 2003 to Windows 2008

1. Back up your 3.1.4 configuration.

   For instructions, see "Backing Up the Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.
2. (Conditional) Back up any customized files on the Identity Server.
3. (Conditional) Remove the Identity Server from the L4 switch configuration.
4. (Conditional) Remove the Identity Server from the cluster configuration.
5. Perform a fresh install of Windows 2008.
6. If you have secondary consoles, bring them down.
7. Install the 3.1.4 version of the Administration Console.

   Use the same IP address and DNS name.
8. Restore your configuration.

   For instructions, see "Restoring an Administration Console Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.
9. Modify keystore locations in the `server.xml` file:
   - **9a** Log in to the Administration Console machine as the administrator.
   - **9b** Open the `server.xml` file.

     ```
     \Program Files (x86)\Novell\Tomcat\conf\server.xml
     ```
   - **9c** Search for `devman.keystore`.
   - **9d** Change the path from

     ```
     \Program Files\Novell\Tomcat\webapps\roma\WEB-INF\conf\devman.keystore
     ```

     to

     ```
     \Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\conf\
     devman.keystore
     ```
   - **9e** Search for `tomcat.keystore`.
   - **9f** Change the path from

     ```
     C:\Program Files\Novell\Tomcat\webapps\roma\WEB-
     INF\conf\tomcat.keystore
     ```

     to

     ```
     C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-
     INF\conf\tomcat.keystore
     ```
   - **9g** Save the file.
   - **9h** Restart Tomcat.

     ```
     net stop Tomcat5
     ```

     ```
     net start Tomcat5
     ```
10. (Conditional) Install the 3.1.4 version of the Identity Server.
11. (Conditional) Restore any customized files to the Identity Server.
12. (Conditional) Add the Identity Server to the cluster configuration.
13. (Conditional) Add the Identity Server to the L4 switch configuration.

14 Remove any secondary consoles from the configuration:

14a In the Administration Console, click *Auditing* > *Troubleshooting*.

14b In the *Other Known Device Manager Servers* section, use the *Remove* button to remove any secondary consoles.

15 Uninstall the secondary consoles. For instructions, see Section 10.4, “Uninstalling the Administration Console,” on page 126.

16 Reinstall the secondary consoles as secondary consoles to the new primary console.

9.3.3 Migrating Identity Servers from SLES 10 to SLES 11

The following procedure can be used to migrate a stand-alone Identity Server, or the Identity Server installed with the SSL VPN server:

1 Remove the Identity Server from the L4 switch configuration.

2 Remove the Identity Server from the cluster configuration.

3 Back up any customized files.

4 Perform a fresh install of SLES 11.

5 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. On SLES 11, the compat-32bit package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119).

Use YaST to install the packages.

Use the following command to verify:

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

6 Install the 3.1.4 version of the Identity Server.

Use the same IP address and DNS name for the Identity Server.

After the installation it might take 15 - 20 minutes for the health status of Identity Server to turn green.This time is utilized for importing and registering certificates from Administration Console.

IMPORTANT: Do *NOT* restart any device or service until the health status of Identity Server turns green.

---

7 Once the Identity Server's health turns green, restart Tomcat, else NIDP page might not be accessible

8 Restore any customized files.

9 Add the Identity Server to the cluster configuration.

10 Add the Identity Server to the L4 switch configuration.

9.3.4 Migrating Stand-Alone Identity Servers from Windows 2003 to Windows 2008

1. Remove the Identity Server from the L4 switch configuration.
2. Remove the Identity Server from the cluster configuration.
3. Back up any customized files.
4. Perform a fresh install of Windows 2008.
5. Install the 3.1 SP4 version of the Identity Server.

   Use the same IP address and DNS name for the Identity Server.
6. Restore any customized files.
7. Add the Identity Server to the cluster configuration.
8. Add the Identity Server to the L4 switch configuration.

9.3.5 Migrating the SSL VPN Server to SLES 11

If the SSL VPN server was installed along with the Administration Console, Identity Server, or the Linux Access Gateway Appliance, the SSL VPN server is automatically migrated to SLES 11, along with the other components. For more information, see the relevant migration sections:

- Section 9.3.1, “Migrating Administration Consoles from SLES 10 to SLES 11,” on page 95
- Section 9.3.3, “Migrating Identity Servers from SLES 10 to SLES 11,” on page 98
- Section 9.3.5, “Migrating the SSL VPN Server to SLES 11,” on page 99

The following sections explain how to migrate the stand-alone SSL VPN server to SLES 11:

- “Migrating Stand-Alone SSL VPN Servers from SLES 10 to SLES 11” on page 99

Migrating Stand-Alone SSL VPN Servers from SLES 10 to SLES 11

1. Remove the SSL VPN server from the cluster configuration, if the server is part of a cluster.
2. (Conditional) If you have customized the SSL VPN user interface, back up all the files in the `jsp/html` folder.

   For more information on customizing the SSL VPN user interface, see “Customizing the SSL VPN User Interface” in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*.
3. Stop the SLES 10 machine.
4. Perform a fresh install of SLES 11.
5. Install the 3.1.4 version of the SSL VPN Server.

   Use the same IP address and DNS name for the SSL VPN Server.
6. (Conditional) Restore the configuration if you have backed it up in step 2.
7. Add the SSL VPN Server to the L4 switch configuration.

9.4 Upgrading the Administration Console

- Section 9.4.1, “Upgrading the Linux Administration Console,” on page 100
- Section 9.4.2, “Upgrading the Windows Administration Console,” on page 102

9.4.1 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.

If you have installed SSL VPN along with the Administration Console, the SSL VPN server must be upgraded along with the Administration Console.

If you select not to upgrade the SSL VPN server with the Administration Console, the upgrade stops.

To upgrade:

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

   Although the upgrade program backs up the JSP directory and its related files, it is a good practice to back up these files.

2. Back up any customized Tomcat files.

   If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

3. If you have Red Carpet or auto update running, stop these programs before you upgrade the Access Manager Administration Console.

4. Open a terminal window.

5. Log in as the `root` user.

6. (Conditional) If you have installed the SSL VPN server with the Administration Console and you have customized the SSL VPN user interface, back up the customized `sslvpnclient.jsp` file, then save it as `/var/opt/novell/tomcat5/webapps/sslvpnsslvpnclient.jsp.rpmsave` file.

   If a file with that name already exists, then either delete the existing file or move it to another location before saving the current `.jsp` file. See "Customizing the SSL VPN User Interface" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*.

7. 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).

8. 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.

9. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./install.sh
   ```

10 When you are 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.

11 (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 a backup of the files, answer `Y` to the prompt.
- If you do not have a backup of the files, answer `N` to the prompt, which cancels the upgrade. Although the upgrade script automatically backs up the JSP directory, it is a good practice to backup your customized files.

12 (Conditional) If you have installed the Identity Server with the Administration Console and you have customized login pages, decide whether you want your customized pages restored automatically. Be aware of the following problems with the automatic restore:

- Your customized files might not compile without modifications. For example, customized 3.0 login pages cannot compile and run on SP3 without some major modifications.
- Any new features introduced in JSP files that have the same name as your files are lost when your file overwrites the installed file.

You might want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

13 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 not to create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you might be forced to re-create your configuration.

- If you do not have a recent backup, type *Y*, press Enter, then complete the following:

13a Specify the administration password, then press Enter.

13b Confirm the password.

13c Specify a location for the backup files, then press Enter.

13d Specify a password for the encryption key.

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

13e Confirm the password.

14 When you are prompted to upgrade, type `Y`, then press Enter.

15 Review and accept the License Agreement.

16 Specify the administration username.

17 Specify the administration password.

18 Confirm the password.

19 If you have a mutual SSL or X509 certificate authentication configured, type `Y`, then press Enter to enable the SSL renegotiation for this server.

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

21 (Optional) To view the upgrade files:

- 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 contains the date and time of the backup.

If you encounter an error, see Section A.9, "Troubleshooting a Linux Administration Console Upgrade," on page 191.

9.4.2 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 the Access Manager Configuration" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

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

Although the upgrade program backs up the JSP directory and its related files, it is a good practice that you backup these files.

3 Back up any customized Tomcat files.

If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

4 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).

5 Run the executable.

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

6 Read the Introduction, then click *Next*.

7 Accept the License Agreement, then click *Next*.

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

9 At the upgrade prompt, click *Continue*.

10 Specify 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.

11 (Conditional) If you have installed the Identity Server with the Administration Console and you have customized login pages, decide whether you want your customized pages restored automatically. Be aware of the following problems with the automatic restore:

- Your customized files might not compile without modifications. For example, customized 3.0 login pages cannot compile and run on SP3 without some major modifications.
- Any new features introduced in JSP files that have the same name as your files are lost when your file overwrites the installed file.

You might want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

12 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 then encounter a problem during the upgrade, you might be forced to re-create 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.

13 Select the *Enable SSL Renegotiation* check box if you have a mutual SSL or X509 certificate authentication configured for this server, then click *Next*.

14 Review the summary, then click *Install*.

15 (Conditional) If the upgrade seems to hang and you have been performing other tasks on the desktop, click the install screen and check behind it for a warning message.

Some of the subcomponents of Access Manager do not send warning messages to the front when the focus of the mouse is not on the installation window.

16 When you are prompted, reboot the machine.

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

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

9.5 Upgrading the Identity Server

9.5.1 Upgrading the Linux Identity Server

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

- If you are upgrading the Access Manager components on multiple machines, ensure that the 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.

Use the following procedure to upgrade the stand-alone Identity Server or the Identity Server installed along with the SSL VPN server. If you have installed both the Identity Server and the Administration Console on the same machine, see Section 9.4.1, "Upgrading the Linux Administration Console," on page 100

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.

   Even though the upgrade program backs up the JSP directory and its related files, it is a good practice to backup these files.

2. Open a terminal window.

3. Log in as the `root` user.

4. (Conditional) If you have installed the SSL VPN server with the Identity Server and you have customized the SSL VPN user interface, make a backup of the customized `sslvpnclient.jsp` file, then save it as `/var/opt/novell/tomcat5/webapps/sslvpnsslvpnclient.jsp.rpmsave` file.

   If a file with that name already exists, then either delete the existing file or move it to another location before saving the current `.jsp` file. See "Customizing the SSL VPN User Interface" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*.

5. Back up any customized Tomcat files.

   If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

6. 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).

7. 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.

8. Open the unpacked Identity Server file, and enter the following at the terminal window:

   ```
   ./install.sh
   ```

9. When you are 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.

10 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.

11 (Conditional) If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware of the following problems with the automatic restore:

- Your customized files might not compile without modifications. For example, customized 3.0 login pages cannot compile and run on SP2 without some major modifications.
- Any new features introduced in JSP files that have the same name as your files are lost when your file overwrites the installed file.

You might want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

12 Review and accept the License Agreement.

13 Press Enter to accept the current Administration Console IP address.

14 Specify the name of the administrator for the Administration Console.

15 Specify the administration password.

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

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

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

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

9.5.2 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 9.4.2, "Upgrading the Windows Administration Console," on page 102.

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

Even though the upgrade program backs up the JSP directory and its related files, we recommend that you have your own backup of these files.

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 Back up any customized Tomcat files.

If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

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

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

5 Run the executable.

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

6 On the Introduction page, click *Next*.

7 Accept the License Agreement.

8 At the upgrade prompt, click *Continue*.

9 Specify 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.

10 (Conditional) If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware of the following problems with the automatic restore:

- Your customized files might not compile without modifications. For example, customized 3.0 login pages cannot compile and run on SP3 without some major modifications.
- Any new features introduced in JSP files that have the same name as your files are lost when your file overwrites the installed file.

You might want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

11 Review the summary, then click *Install*.

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

Windows Server 2003: `\Program Files\Novell\log\AccessManagerServer_InstallLog.log`

Windows Server 2008: `\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`

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

9.5.3 Access Failure Issues with the Intersite Transfer Service

If the Novell Access Manager is federated with other service providers or if the users are redirected to Access Gateway protected resources from the Identity Server using the target_url, you may see errors regardless of successful authentication. The ConfigUpgrade script enables ‘Allow any target’ for the ‘Intersite Transfer Service’ configuration service for all the service providers.

9.6 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.

You cannot migrate directly from SLES 9 version of the Access Gateway to the SLES 11 version on Access Manager 3.1 SP4. You can migrate from SLES 9 version to SLES 11 version in the Access Manager 3.1 SP2. For migration instructions, see Migrating to the SLES 11 Access Gateway Appliance (http://www.novell.com/documentation/novellaccessmanager312/installation/data/bn7y8xh.html#boqumao) in the *Novell Access Manager 3.1 SP2 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager312/installation/data/bookinfo.html).

The Linux Appliance can be upgraded with the following methods:

- In an interactive method, where you are prompted to enter the required parameters.
- In a silent method, where all the required parameters are passed in the command line.
- By using the Administration Console.

If you have installed SSL VPN along with the Linux Appliance, check 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 customized the error pages for Access Manager 3.0 (as mentioned in "Customizing the Error Pages of the Access Gateway Service" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*), copy the images used in the custom error pages from `/var/opt/novell/tomcat4/webapps/LAGERROR/images` to `/var/opt/novell/tomcat5/webapps/LAGERROR/images`, after upgrading to Novell Access Manager 3.1.

This section contains the following information:

9.6.1 Prerequisites

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

- ❑ If you have installed the SSL VPN server with the Access Gateway Appliance and you have customized the SSL VPN user interface, make a backup of the customized `sslvpnclient.jsp` file, then save it as `/var/opt/novell/tomcat5/webapps/sslvpnsslvpnclient.jsp.rpmsave` file.

  If a file with that name already exists, then either delete or move the existing file to another location before saving the current `.jsp` file. See "Customizing the SSL VPN User Interface" in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*.

- ❑ Back up any customized Tomcat files.

  If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

- ❑ 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`.

- ❑ To run the script, you must provide primary Administrator Console user dn and password. The user dn is `cn = <username>, 0 = Novell`.
- ❑ Ensure to provide the correct password, incorrect passwords may lock the administrator account.
- ❑ The Windows batch file assumes the Administrator Console is installed in the “C” drive. If your installation is not in the “C” drive, then you must edit the batch files accordingly.
- ❑ Stop the Linux primary Administration Console using “/etc/init.d/novell-tomcat5 stop” before running the script ConfigUpgrade.sh.
- ❑ Stop the Tomcat service on Windows primary Administration Console.

9.6.2 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.
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 `/tmp/novell_access_manager/upgr_lag.log` file to verify the results of the upgrade process.

9.6.3 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 Enter the following command:

`/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`

- 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`

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

4 View the `/tmp/novell_access_manager/upgr_lag.log` file to verify the results of the upgrade process.

9.6.4 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.

9.6.5 Installing or Updating the Latest Linux Patches

WARNING: The Linux Access Gateway 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.

Prerequisites

- ❑ The Linux Appliance installs a customized version of SLES 9 SP 3 or SLES 11 depending on the version you have installed. If you want to install the latest patches as they become available, you must have a Novell user account to receive Linux updates.
- ❑ 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.

Select the patch upgrade method that fits your system:

- "Installing or Updating the Security Patches on the SLES 9 Linux Access Gateway Appliance" on page 111
- "Installing or Updating Security Patches for the SLES 11 Linux Access Gateway Appliance" on page 112
- "Configuring the Subscription Management Tool for SLES 11 Access Gateway Appliance" on page 115

Installing or Updating the Security Patches on the SLES 9 Linux Access Gateway Appliance

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 an `i` symbol next to them. 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 the Access Gateway Appliance for Linux kernel update to take effect.

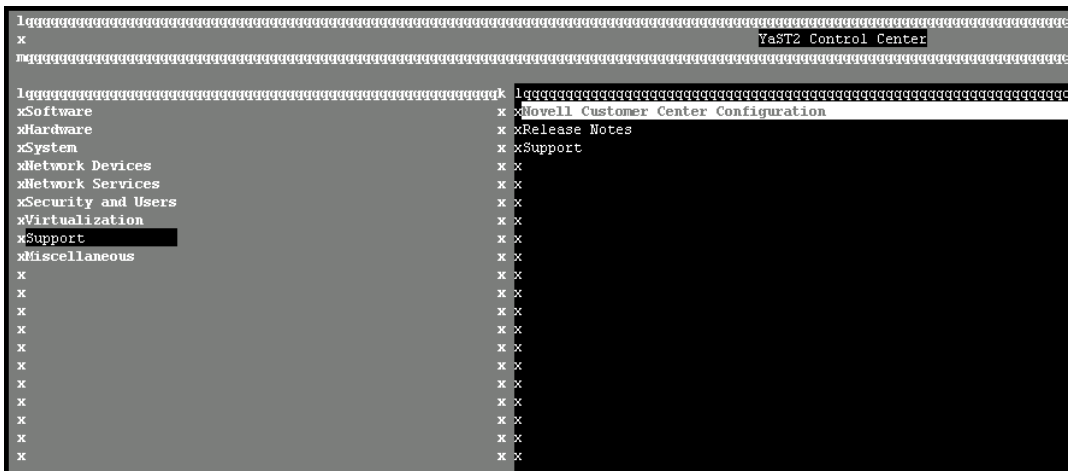
11 Enter the following command to check the logs:

```
tail -f /var/log/YaST2/y2log
```

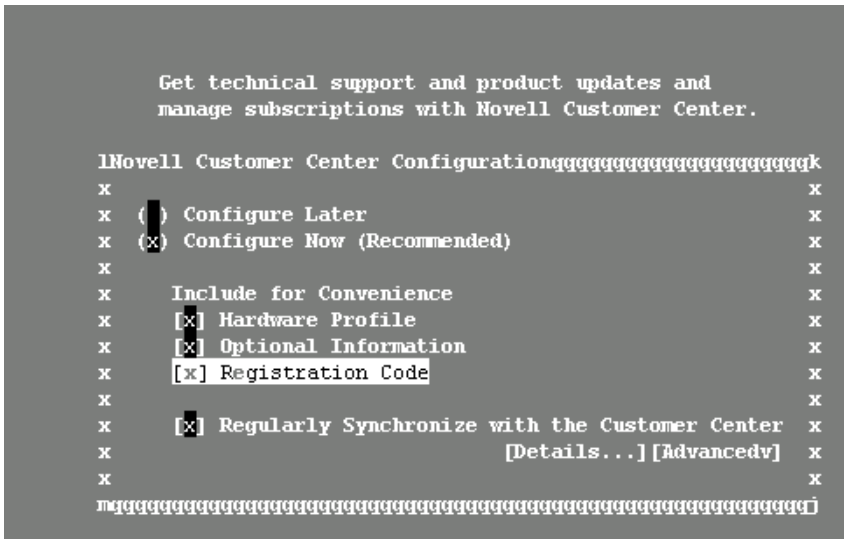
Installing or Updating Security Patches for the SLES 11 Linux Access Gateway Appliance

To get the latest security updates for the SLES 11 Access Gateway Appliance, the user must register with the Novell Customer Center by using the activation code obtained with the product:

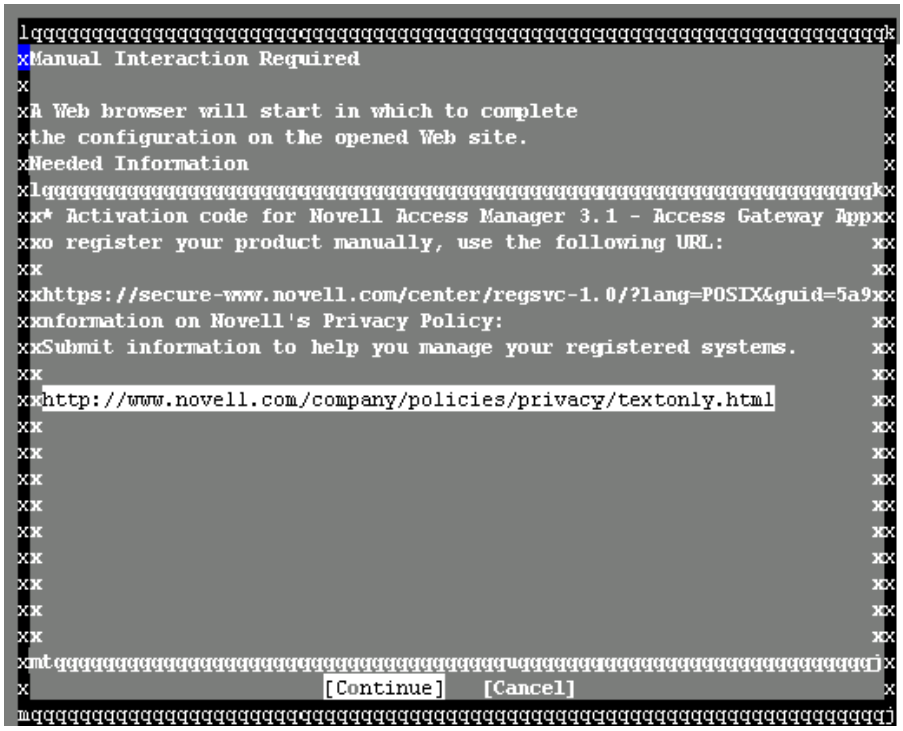
1 Go to *YaST* > *Support* > *Novell Customer Center Configuration*.



2 Select *Configure Now (Recommended)*, then select *Registration Code* in the *Novell Customer Center Configuration* screen.



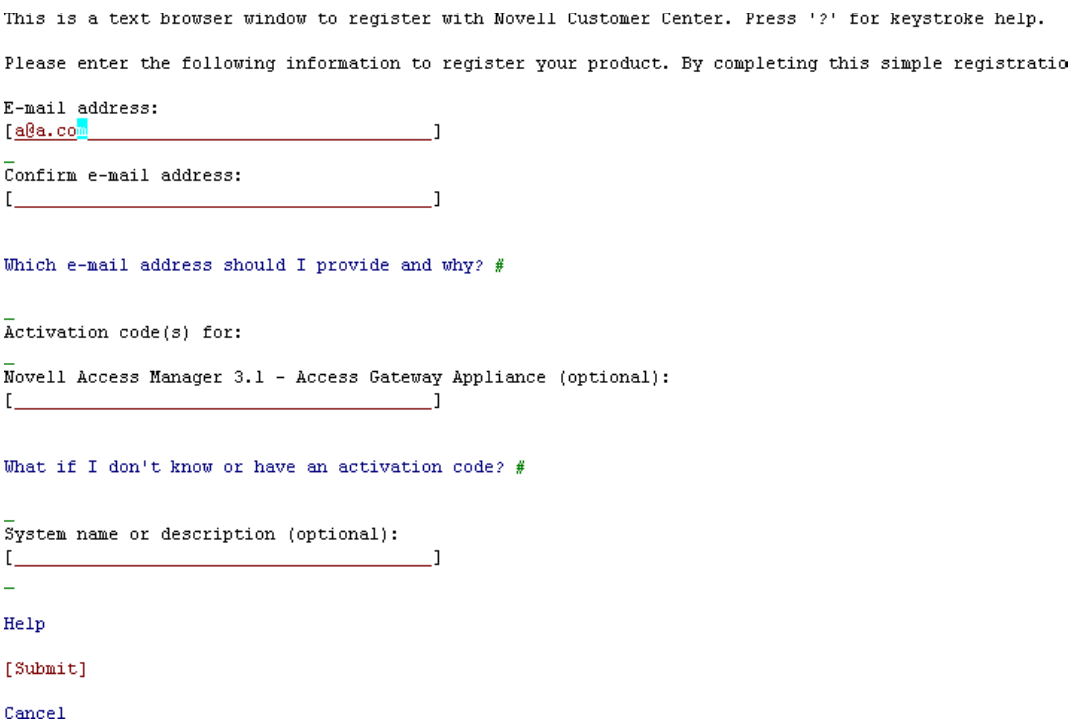
3 Click *Next*.



The Manual Interaction Required screen appears. It might take a few minutes to connect to the server.

This screen indicates that to activate the product, you must provide a valid e-mail ID associated with the Novell account and the activation code.

4 Click *Continue*.



5 To specify the e-mail address, activation code and system name in the relevant fields:

5a Select the relevant option, then press *Enter*. A text field appears in the bottom left corner of the screen.

5b Specify value for the selected option in this text field, then press *Enter* to return to the screen.

5c Repeat these steps for each field.

6 Click *Submit* after you have specified all the relevant information to complete the registration.

7 Enter `Q` to close the window.

8 Enter `Y` to continue.

The Manual Interaction Required screen is displayed. The software repositories are created on the Access Gateway Appliance. You will receive a message from the Novell Customer Center Configuration indicating that the configuration was successful.

9 Click *OK* to return to YaST2 Control Center.

10 Click *Quit* to exit YaST.

11 Open a shell prompt and specify the following command to verify if the SLES 11 repository named `NAM31-AGA-Updates` was created for SLES 11 Access Gateway Appliance:

```
zypper lr
```

An output similar to the following appears:

```
 # | Alias        | Name      | Enabled | Refresh
--+----------------------------------------+----------------------------
1 | NAM-Access-Gateway-Appliance-3.1 3.1.2 | NAM-Access-Gateway-Appliance-
3.1
3.1.2 | Yes      | No
2 | nu_novell_com:NAM31-AGA-Updates       | NAM31-AGA-Updates
    | Yes      | Yes
```

12 Do one of the following:

- To update specific patches, run the following command:

```
zypper in <package-name>
```

  Replace <*package-name*> with the package name, or use a wildcard to get packages starting with a particular name. For example, to get all gcc packages, you can use the following command:

  ```
  zypper in gcc-*
  ```

- To update all the latest patches, do the following:

  1. Specify the following command to get updated security patches for the appliance:

     ```
     zypper patch
     ```

  2. Run the `zypper patch` command again to install any other required patches.

     NOTE: The `zypper patch` command is executed twice because when the command is executed the first time, one of the patches installed affects the package manager. Therefore, the command must be executed again to install any other needed patches.

13 Restart the machine when the following warning message appears:

```
Warning: One of installed patches requires reboot of your machine. Reboot
as soon as possible.
```

14 Go to *YaST* > *Software* > *Online Update* and verify that all the required patches are installed or upgraded.

Configuring the Subscription Management Tool for SLES 11 Access Gateway Appliance

Any machine running SUSE Linux Enterprise Server 11 (SLES11) can be configured to register against local Subscription Management Tool (SMT) server and download software updates from there instead of communicating directly with the Novell Customer Center and the NU servers. The Access Gateway Appliance is built on SLES 11 and you can configure it to get updates from the SMT server.

To use an SMT server for client registration and as a local update source, you must configure the SMT server in your network first. The SMT server software is distributed as an add-on for SUSE Linux Enterprise Server. For information on configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 (http://www.novell.com/documentation/smt11/).

The following sections describe the configuration required for the Access Gateway Appliance:

- “SMT configuration for Linux Access Gateway” on page 115
- “Troubleshooting” on page 117

SMT configuration for Linux Access Gateway

You must configure the SMT server and set up subscription for NAM31-AGA-Updates channel to receive the updates for Novell Access Manager appliance.

SMT Configuration

1. Install the SMT server in a SLES 11 Server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 (http://www.novell.com/documentation/smt11/).
2. Log into you Novell Customer Center account.
3. Select *My Products* > *Mirroring Credentials*, then click *Generate Credentials*.
4. Copy the mirroring credentials before logging out of your Novell Customer Center account.
5. Run the *SMT Configuration* tool from YAST, then specify the mirroring credentials.
6. Run the *SMT Management* tool.

   The NAM31-AGA-Updates repository, *sle-11-i586* is displayed in the *Repositories* tab.

   NOTE: For this release, only 32-bit version of SLES11 based Linux Access Gateway is supported.

   ---
7. Select *sle-11-i586*, then click *Toggle Mirroring* to ensure mirroring is selected for this repository.
8. Click *Mirror Now*. This step ensures that the *NAM31-AGA-Updates* channel updates are mirrored from *nu.novell.com* to your local SMT server.
9. Click *OK* to close the tool, when mirroring is complete.

Configuring the SLES11 Linux Access Gateway

1. Copy `/usr/share/doc/packages/smt/clientSetup4SMT.sh` from the SMT server to the client machine.

   You can use this script to configure a client machine to use the SMT server or to reconfigure it to use a different SMT server.
2. Specify the following command as `root` to execute the script on the client machine:

   ```
   ./clientSetup4SMT.sh --host server_hostname
   ```

   For example,

   ```
   ./clientSetup4SMT.sh --host smt.example.com.
   ```

   You can get the SMT server URL by running the SMT Configuration tool at the server. The URL is set by default.
3. Enter `y` to accept the CA certificate of the server.
4. Enter `y` to start the registration.
5. The script performs all necessary modifications on the client.
6. Execute the following command to perform registration:

   ```
   suse_register
   ```
7. Specify the following command to get online updates from the local SMT server:

   ```
   zypper up
   ```
8. Reboot the machine if prompted at the end of any patch install.

Troubleshooting

Given below are some of the errors that you might see and the steps to resolve these issues:

- During the client configuration, if you see the following error:

  ```
  Repository 'NAM31-AGA-Updates' is invalid.
  [|] Repository type can't be determined.
  Please check if the URIs defined for this repository are pointing to a
  valid repository.
  ```

  it indicates that patches were not properly mirrored at the local SMT server.

  To workaround this issue, start mirroring at the server manually by using the following command:

  ```
  smt mirror -D
  ```

- If you see the following error while running the `smt mirror -D` command in your SMT server `<rpm_name>.src.rpm: 404 Not Found`

  edit `/etc/smt.conf` and set the value `MirrorSRC=false`. Save the file and run the `smt mirror -D` command again.

9.7 Upgrading the Access Gateway Service

9.7.1 Upgrading the Linux Access Gateway Service

You use the same program to upgrade as you used to install the product. The program detects that the Access Gateway Service is already installed and prompts you to upgrade.

1. Back up any customized Tomcat files.

   If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

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

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

3. Grant execute rights to the file with the following command:

   `chmod +x <`*filename*`>`

   Replace <*filename*> with the name of the file.

4. Start the installation program by entering the following command:

   `./<`*filename*`>`

   Replace <*filename*> with the name of the file.

5. Answer Yes to the prompt to upgrade.
6. Review the instructions on how to cancel, then click *Next*.
7. Review the Readme information, then click *Next*.
8. Accept the License Agreement, then click *Next*.

9 Specify the following information:

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 Review the installation summary, then click *Install*.

The Access Gateway Service is upgraded.

11 (Optional) View the log files. The install logs are located in the `/tmp/novell_access_manager/` directory. These logs are all dated and time-stamped.

9.7.2 Upgrading the Windows Access Gateway Service

You use the same program to upgrade as you used to install the product. The program detects that the Access Gateway Service is already installed and prompts you to upgrade.

1 Back up any customized Tomcat files.

If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

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

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

3 Disable any virus scanning programs.

4 Double-click the executable file.

5 Answer Yes to the prompt to upgrade.

6 Review the instructions on how to cancel, then click *Next*.

7 View the Readme, then click *Next*.

8 Review and accept the License Agreement.

9 Specify the following information:

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 Review the installation summary, then click *Install*.

The Access Gateway Service is upgraded.

11 (Optional) View the upgrade files in the following directories:

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

9.8 Upgrading the SSL VPN Servers

Upgrade time: about three minutes.

You can upgrade SSL VPN to 3.1 SP4 version from 3.1 SP3 version.

You can upgrade the Traditional SSL VPN server to the 3.1 SP4 version of the Traditional SSL VPN server. You cannot upgrade the Traditional Novell SSL VPN server to the ESP-enabled SSL VPN. However, you can perform a new installation of ESP-enabled version of SSL VPN and then migrate traffic policies that you configured for the traditional SSL VPN to the ESP-enabled SSL VPN.

9.8.1 Prerequisites

Make sure that you have done the following before you proceed with the upgrade:

- ❑ Download the relevant upgrade file from Novell (http://support.novell.com/patches.html) and extract the file. For the actual filename, see the Readme (http://www.novell.com/documentation/novellaccessmanager31/index.html).
- ❑ Upgrade the Administration Console, Identity Server, and Access Gateway Appliance before upgrading SSL VPN servers that are installed on separate machines.

  If the SSL VPN server was installed with the other Access Manager components, the SSL VPN server is automatically upgraded along with the other components.
- ❑ If you have installed high bandwidth SSL VPN, make sure you download and install the high bandwidth SSL VPN RPM. SSL VPN has a high bandwidth RPM that needs to be installed once to get its capabilities. This RPM should be installed before upgrading the SSL VPN server. For information on how to install the high bandwidth SSL VPN RPM, see Section 8.3, “Installing the Key for the High-Bandwidth SSLVPN,” on page 91.
- ❑ The Access Manager Administration Console must be up and running before you begin upgrading SSL VPN servers. Do not perform any configuration tasks in the Administration Console during an SSL VPN Server upgrade
- ❑ If you have customized the SSL VPN user interface, make a backup of the customized `sslvpnclient.jsp` file, then save it as `/var/opt/novell/tomcat5/webapps/sslvpnsslvpnclient.jsp.rpmsave` file. If a file with that name already exists, then either delete or move the existing file to another location before saving the current `.jsp` file. See “Customizing the SSL VPN User Interface” in the *Novell Access Manager 3.1 SP4 SSL VPN Server Guide*.

9.8.2 Upgrade Scenarios

Table 9-1 on page 120 contains a list of upgrade scenarios available for SSL VPN, along with the procedure to upgrade the server.

Table 9-1 *Upgrade Scenarios*

Installation Scenario	Upgrade Procedure
Traditional SSL VPN, Identity Server, and the Administration Console on the same machine; Linux Access Gateway on a separate machine	The SSL VPN 3.1 SP4 version cannot coexist with other Novell Access Manager components that are running the 3.1 SP3 version. When SSL VPN is installed along with the other Novell Access Manager component on the same machine, the SSL VPN server is automatically upgraded to 3.1 SP4. For more information, see Section 9.5, "Upgrading the Identity Server," on page 103.
Traditional SSL VPN, Identity Server, Linux Access Gateway, and Administration Console on separate machines	To upgrade an SSL VPN server that is installed on a separate machine, see Section 9.8.3, "Upgrading SSL VPN Installed on a Separate Machine," on page 120.
Traditional SSL VPN and the Identity server on the same machine; Administration Console and Linux Access Gateway on separate machines	When SSL VPN is installed along with the Identity Server on the same machine, the SSL VPN server is automatically upgraded to 3.1 SP4. For more information, see Section 9.5, "Upgrading the Identity Server," on page 103.
Traditional SSL VPN and the Administration Console on same machine, Identity Server, Linux Access Gateway on a separate machine	When SSL VPN is installed along with the Administration Console on the same machine, the SSL VPN server is automatically upgraded to 3.1 SP4. For more information, see Section 9.4, "Upgrading the Administration Console," on page 99.
Traditional SSL VPN and the Linux Access Gateway on the same machine, Administration Console and Identity Server on separate machines	When SSL VPN is installed along with the Linux Access Gateway on the same machine, the SSL VPN server is automatically upgraded to 3.1 SP4. For more information, see Section 9.6, "Upgrading the Linux Access Gateway Appliance," on page 106.

9.8.3 Upgrading SSL VPN Installed on a Separate Machine

1. Upgrade the Administration Console, Identity Server, and Linux Access Gateways before you proceed with upgrading the SSL VPN server.
2. 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).
3. 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, which contains the SSL VPN files.
4. Log in as the `root` user.

5. Open the unpacked Identity Server file, and enter the following at the terminal window:

   ```
   ./install.sh
   ```

6. When you are prompted to install a product, type 3 to select SSL VPN, then press the Enter key.

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

7. Type *Y*, then press the Enter key.
8. Review and enter *Y* to accept the License Agreement.
9. (Conditional) If the SSL VPN machine has been configured with multiple IP address, select an IP address for the SSL VPN server when you are prompted to do so.
10. Press Enter to accept the current Administration Console IP address.
11. Specify the name of the administrator for the Administration Console.
12. Specify the administration password.
13. Confirm the password, then wait as the system installs the components. This will take several minutes.
14. (Conditional) View the log files.

    The log file is located in the `/tmp/novell_access_manager/inst_lag.log` file. These log files are all dated and time-stamped.

NOTE: Occasionally, the first SSL VPN user connection might fail after upgrading, especially if you have encountered any problems during the upgrade process. To work around this problem, we recommend that you initiate multiple SSL VPN connections after upgrading.

9.9 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 healthy 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

10

This section discusses the following topics related to installation:

10.1 Uninstalling the Identity Server

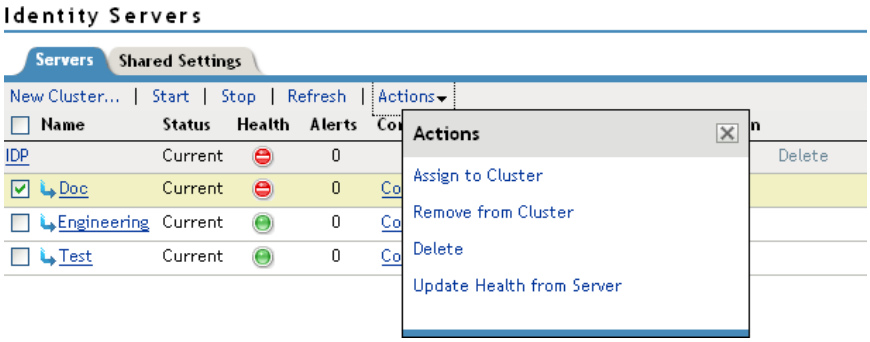
Uninstalling the Novell Identity Server is a two-step process:

1. Removing the Identity Server from the Administration Console. See Section 10.1.1, “Deleting Identity Server References,” on page 123.
2. Removing the Identity Server software from the Linux or Windows machine. See Section 10.1.2, “Uninstalling the Linux Identity Server,” on page 124 or Section 10.1.3, “Uninstalling the Windows Identity Server,” on page 124.

10.1.1 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 10.1.2, “Uninstalling the Linux Identity Server,” on page 124 or Section 10.1.3, “Uninstalling the Windows Identity Server,” on page 124.

10.1.2 Uninstalling the Linux 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. 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.

10.1.3 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 one of 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 only the Identity Server.

   If the unistall fails because the primary Administration Console is not available to validate the credentials, see Section A.11, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 194.
7. (Conditional) If the Administration Console was installed with the Identity Server and you selected only to uninstall the Identity Server, reboot the machine.

10.2 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 59) 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 59.)
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*.

10.3 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*.
3. On the Access Gateways Servers page, select the name of the server, then click *Actions* > *Delete* > *OK*.

   This removes the configuration object for the Access Gateway from the Administration Console.
4. 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 SP4 Identity Server Guide*.
5. Complete one of the following:
   - If you are uninstalling the Access Gateway Appliance machine, re-image the machine by booting to a CD containing the desired operating system software.
   - If you are uninstalling the Windows Access Gateway Service, continue with Section 10.3.1, "Uninstalling the Windows Access Gateway Service," on page 125.
   - If you are uninstalling the Linux Access Gateway Service, continue with Section 10.3.2, "Uninstalling the Linux Access Gateway Service," on page 126.

10.3.1 Uninstalling the Windows Access Gateway Service

1. Exit any applications and disable any virus scanning programs.

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

3 Click *Next*.

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

If the uninstall fails because the program cannot authenticate to the Administration Console, see Section A.10, “Troubleshooting the Uninstall of the Access Gateway Service,” on page 193.

10.3.2 Uninstalling the Linux Access Gateway Service

1 Log in as root.

2 Change to the `/opt/novell/accessgateway` directory, then enter the following command:

```
./removeAccessGateway
```

3 Click *Next*.

4 Click *Done*.

If the uninstall fails, see Section A.10, “Troubleshooting the Uninstall of the Access Gateway Service,” on page 193.

10.4 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 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 SP4 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 10.4.1, “Uninstalling the Linux Administration Console,” on page 126
- Section 10.4.2, “Uninstalling the Windows Administration Console,” on page 127

10.4.1 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

Option	Description
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 options 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

10.4.2 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 stop 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.11, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 194.

10.5 Uninstalling the SSL VPN Server

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

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

10.5.1 Deleting the SSL VPN Server References

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*, then click *OK* to confirm.

4 Update the cluster configuration.

5 Select the SSL VPN Server that you want to uninstall, then click *Actions* > *Delete*.

6 Click *OK*.

7 Proceed with Section 10.5.2, "Uninstalling the SSL VPN Server," on page 128 to uninstall the SSL VPN server.

10.5.2 Uninstalling the SSL VPN Server

IMPORTANT: If you have installed the high-bandwidth SSL VPN key, uninstall the key before proceeding to uninstall the SSL VPN server. For more information on uninstalling the high-bandwidth key, see Section 10.5.3, "Uninstalling the RPM Key for High Bandwidth SSL VPN," on page 128.

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
```

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.

10.5.3 Uninstalling the RPM 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

11

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.

11.1 Understanding the Differences between iChain and Access Manager

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

11.1.1 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 operating systems such as Linux and Windows.

Access Manager has the following components:

- **Administration Console:** Installed on Linux or Windows to provide 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 to provide 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 or on Linux and Widows as a service. It provides single sign-on to Web servers and uses policies assigned to the resources on the Web servers to enforce access control. 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 to provide single sign-on to private networks with non-HTTP applications.
- **J2EE Agent:** Installed on a J2EE sever to provide fine-grained authorization for J2EE applications and single sign-on. Access Manager currently has agents for WebSphere, WebLogic, and JBoss servers installed on Linux, Windows, and AIX.

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), which components you are going to install on separate machines, which components 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.

11.1.2 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 11-1 *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, Sun ONE), RADIUS, NMAS, OCSP/CLR Server, Custom
Supported operation systems	NetWare	Linux, Windows
Citrix* integration	Proxy ICA traffic	SSL VPN

11.2 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 migration strategy that fits the needs of your environment. For some ideas, see Section 11.2.1, “Possible Migration Strategies,” on page 131.
- 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 11.2.2, “Outlining the Migration Requirements for Each Resource,” on page 138.

11.2.1 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:

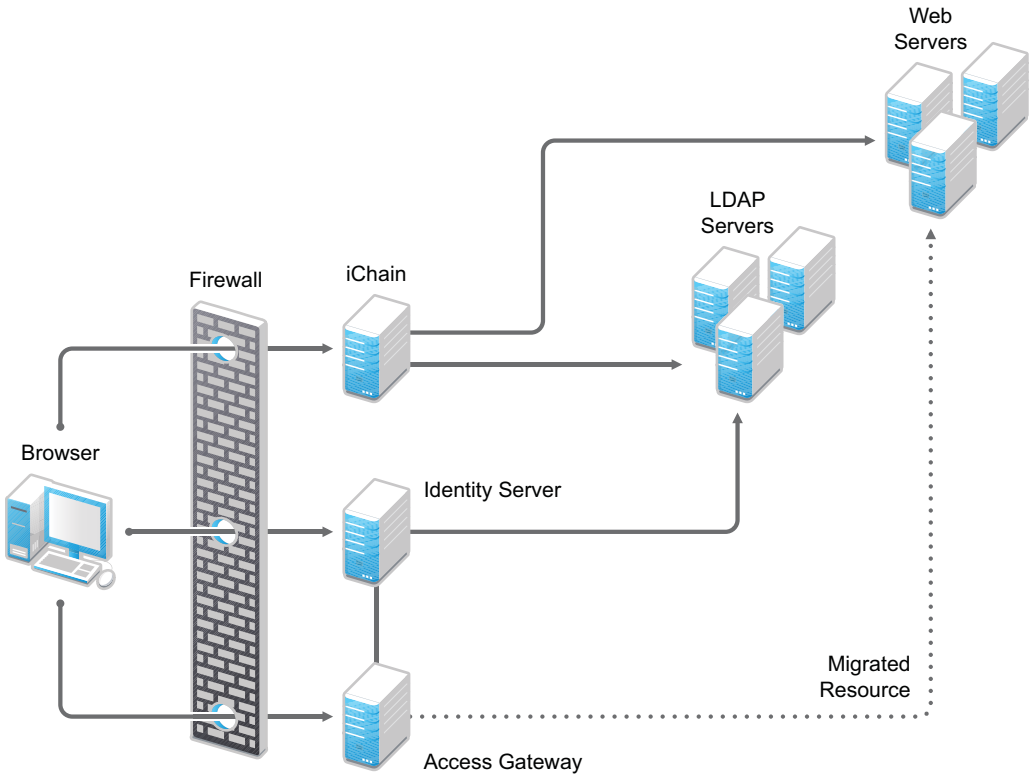
- You use iChain to protect a few Web servers with only one or two applications each.
- The policies that control single sign-on and access are simple.

- 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 11-1 *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 SP4 Setup Guide*.

Major Tasks: Complete the following tasks in the order listed.

1. Install the software. You need an Administration Console (the Access Manager version of iManager), an Identity Server, and an Access Gateway.
2. Set up a basic configuration. For instructions, see “Setting Up a Basic Access Manager Configuration” in the *Novell Access Manager 3.1 SP4 Setup Guide*.
3. Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See Section 11.3.3, “Configuring the Identity Server for Authentication,” on page 141.
4. Configure the Access Gateway to have the same device settings as iChain. See Section 11.3.4, “Configuring System and Network Settings,” on page 143
5. Migrate an accelerator with its resources from iChain to the Access Gateway. See Section 11.3.5, “Migrating the First Accelerator,” on page 147.
6. Remove iChain. See Section 11.3.9, “Removing iChain,” on page 168.

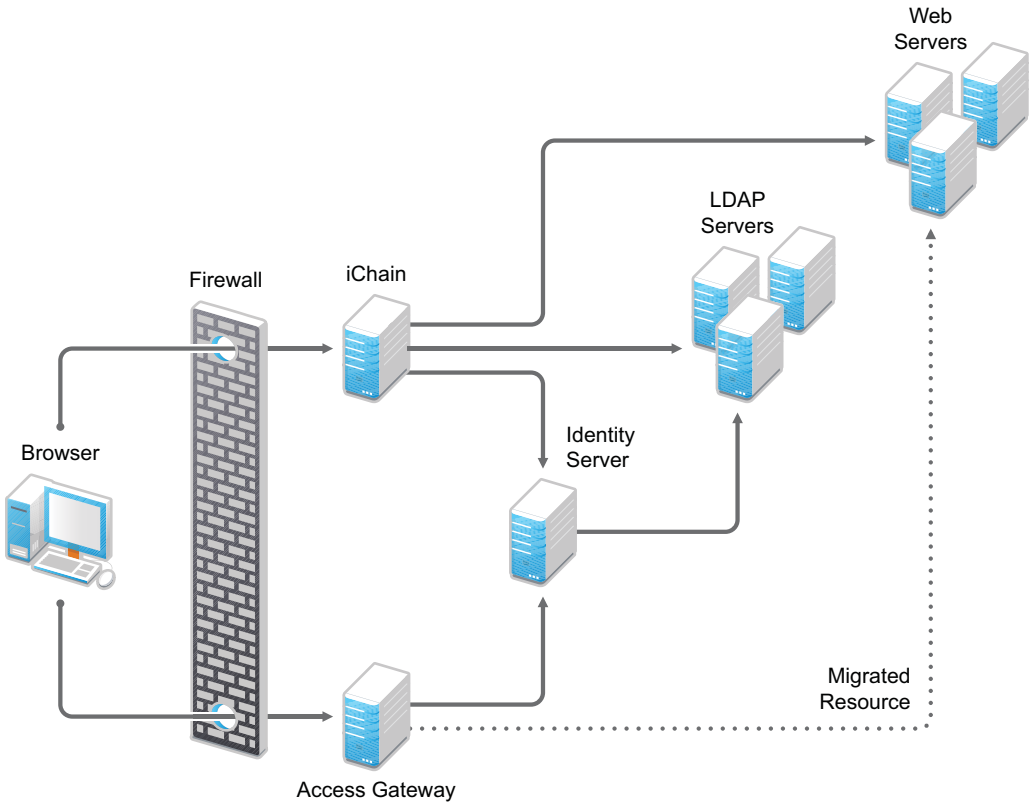
A Phased Migration

You can use a phased migration if iChain is protecting multiple resources that require Form Fill policies, SSL methods, and access control methods. While you are 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 11-2 illustrates the network layout for this type of migration.

Figure 11-2 *Network Setup for a Phased Migration*



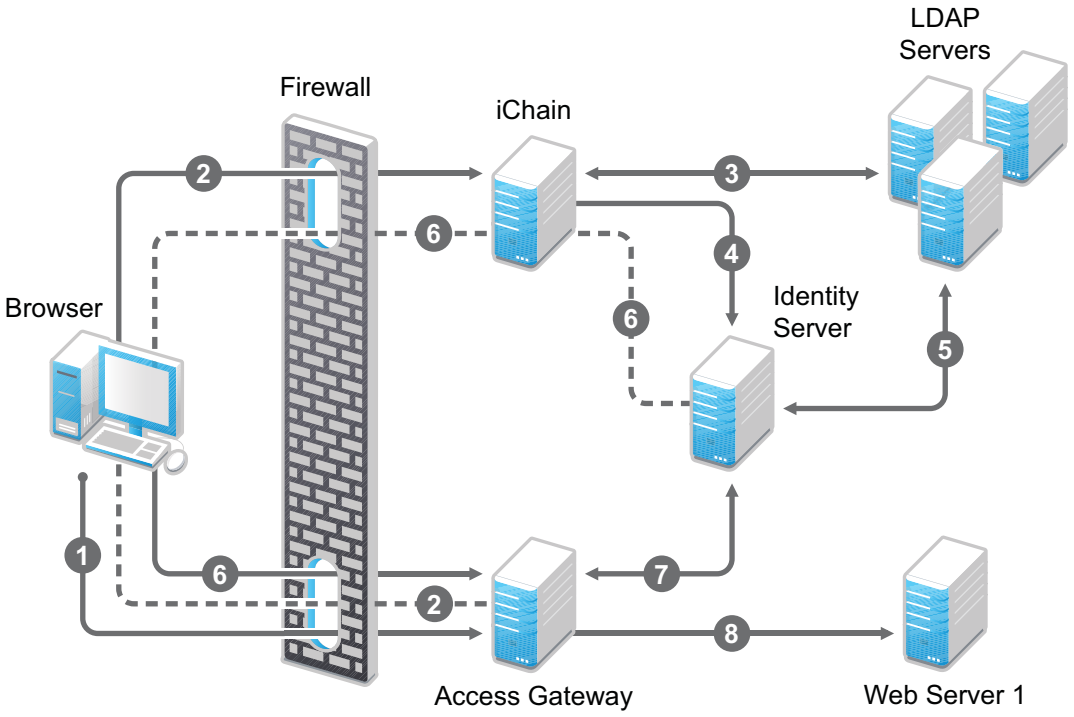
The phased migration uses iChain for authentication and single sign-on to the Identity Server. To do this, you configure the Identity Server to be a restricted resource of iChain, and you configure the Access Gateway to trust the Identity Server as its identity provider. The Access Gateway communicates 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 the credentials are 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 11-3 illustrates this flow. The dotted lines represent redirected requests.

Figure 11-3 *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.

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)

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 137.

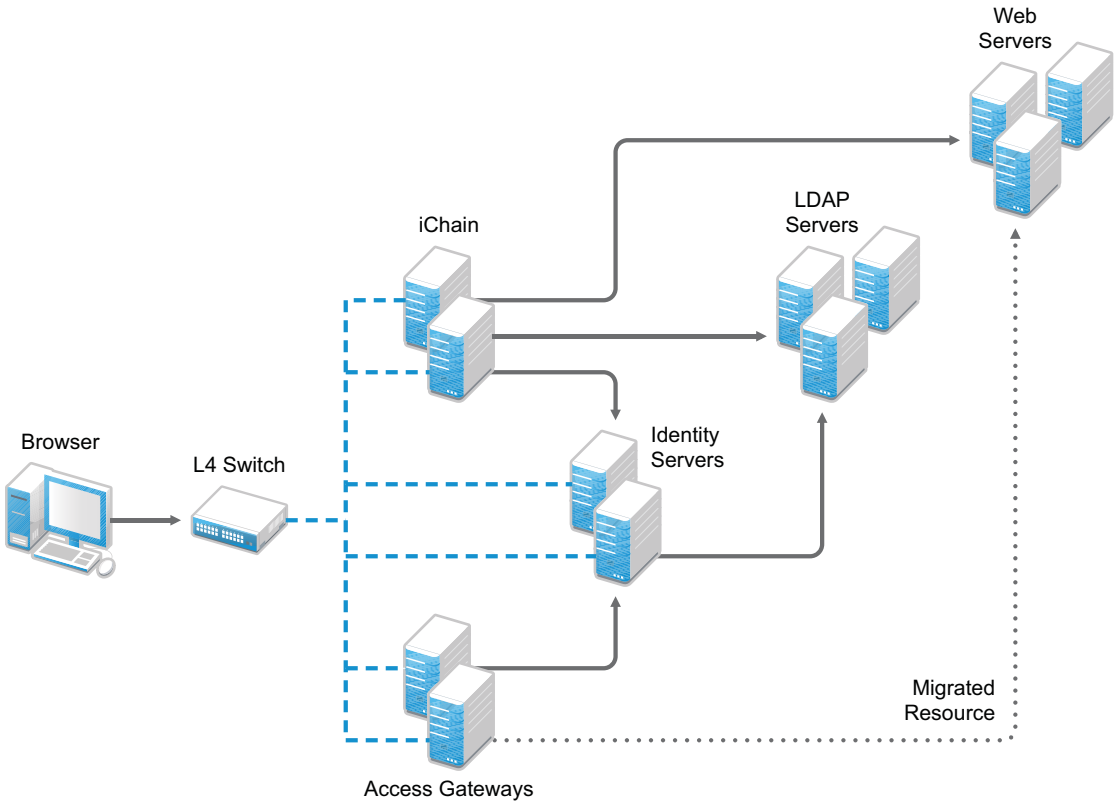
Major Tasks: Complete the following tasks in the order listed.

1. Install the software. You need an Administration Console (the Access Manager version of iManager), an Identity Server, and an Access Gateway.
2. Set up a basic configuration. For instructions, see “Setting Up a Basic Access Manager Configuration” in the *Novell Access Manager 3.1 SP4 Setup Guide*.
3. Set up the Identity Server to use the same LDAP directories and authentication methods as iChain. See Section 11.3.3, “Configuring the Identity Server for Authentication,” on page 141.
4. Configure the Access Gateway to have the same device settings as iChain. See Section 11.3.4, “Configuring System and Network Settings,” on page 143.
5. Migrate an accelerator with its resources from iChain to the Access Gateway. See Section 11.3.5, “Migrating the First Accelerator,” on page 147.
6. 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 11.3.6, “Enabling Single Sign-On between iChain and Access Manager,” on page 154.

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 11-4 *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: Complete the following tasks in the order listed.

1. Set up a cluster of Identity Servers. See "Clustering Identity Servers" in the *Novell Access Manager 3.1 SP4 Setup Guide*.
2. Set up a cluster of Access Gateways. See "Clustering Access Gateways" in the *Novell Access Manager 3.1 SP4 Setup Guide*.
3. Configure the L4 switch for the servers in the Identity Server cluster and the Access Gateway group. See your L4 switch documentation.
4. Migrate a resource. See Section 11.2.2, "Outlining the Migration Requirements for Each Resource," on page 138

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.

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. For information on this process, see "Converting a Secondary Console into a Primary Console" in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

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.

11.2.2 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 138
- "Accelerator" on page 139
- "Protected Resources" on page 139
- "Applications" on page 140

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, then list how each 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

  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. In Access Manager, this feature is called the *Refresh Data* option, and you configure it on the Authorization policy.
- 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 SP4 J2EE Agent Guide*.
- For non-HTTP applications, investigate SSL VPN and determine if you want to use the SSL VPN server to protect these applications. See the *Novell Access Manager 3.1 SP4 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 the Access Gateway. If your iChain environment uses NetIdentity authentication to support ZENworks for Desktops or simple background authentication for proxy login, you 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 continues to work.

11.3 Migrating Components

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

11.3.1 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 49
- “Installing the Novell Identity Server” on page 59
- “Installing the Linux Access Gateway Appliance” on page 65
- “Installing the Access Gateway Service” on page 75
- “Installing the SSL VPN Server” on page 81

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 SP4 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 SP4 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 SP4 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 SP4 Setup Guide*.

11.3.2 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 SP4 Setup Guide*
- "Configuration Tips for the L4 Switch " in the *Novell Access Manager 3.1 SP4 Setup Guide*

11.3.3 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 141
- "Migrating the User Store Configuration" on page 142
- "Enabling the User Stores for Authentication Methods" on page 143
- "Migrating Custom Login Pages" on page 143

Migrating Your Authentication Profiles

You need to migrate authentication profiles that you set up in iChain. If you set up only 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 142. 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 supports this feature with the ORed Credential class. For more information, see "Creating an ORed Credential Class" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.

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 142. 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 SP4 Policy 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 SP4 Policy 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 SP4 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 SP4 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 143.

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 143. Otherwise, continue with Section 11.3.4, "Configuring System and Network Settings," on page 143.

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.

iChain uses HTML for its login page. Access Manager uses JSP. The default login page for Access Manager is the `nidp.jsp` file. The easiest way to create a new login page is to copy this default page, rename it, then modify it to match your requirements.

For more information, see "Customizing the Identity Server Login Page" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.

11.3.4 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. Authentication requests fail if time is not configured accurately and synchronized between the Identity Server and the Access Gateway.

- To configure the time for the Access Gateway Appliance, see "Setting the Date and Time" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.
- To configure the time for the Identity Server or the Access Gateway Service, use operating system utilities.

Network Settings

This section describes the differences between network settings for iChain and Access Gateway Appliance:

- "DNS Servers" on page 144
- "Gateways" on page 144
- "Telnet" on page 144
- "IP Addresses" on page 145

For the Access Gateway Service, you need to use operating system utilities to configure network settings.

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 use SSH instead, which supports data encryption. The Access Gateway Appliance does not support 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 Admin ACL option.

Both products allow you to configure the following system settings:

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

For the Access Gateway Service, date and time must be set with operating system utilities, and upgrade is not currently supported from the Administration Console. The other features can be configured from the Administration Console.

The Access Gateway Appliance does not support SNMP.

Date & Time

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

Both products allow you to set the date and time, set up an NTP server, and configure the time zone. Time synchronization is critical. 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.

For the Access Gateway Service, you must use operating system utilities to configure date and time.

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 9.6, “Upgrading the Linux Access Gateway Appliance,” on page 106.

For the Access Gateway Service, you cannot upgrade the device from the Administration Console. For upgrade information, see Section 9.7, “Upgrading the Access Gateway Service,” on page 117.

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. For the Access Gateway Service, the restart and stop options restart or stop the service. You need to use system utilities to restart or stop the operating system.

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 Service Path
Web App > System > SNMP	Access Gateways > Edit > Alerts > [Profile]

The Access Gateway Appliance does not support SNMP. It is supported by the Access Gateway Service.

11.3.5 Migrating the First Accelerator

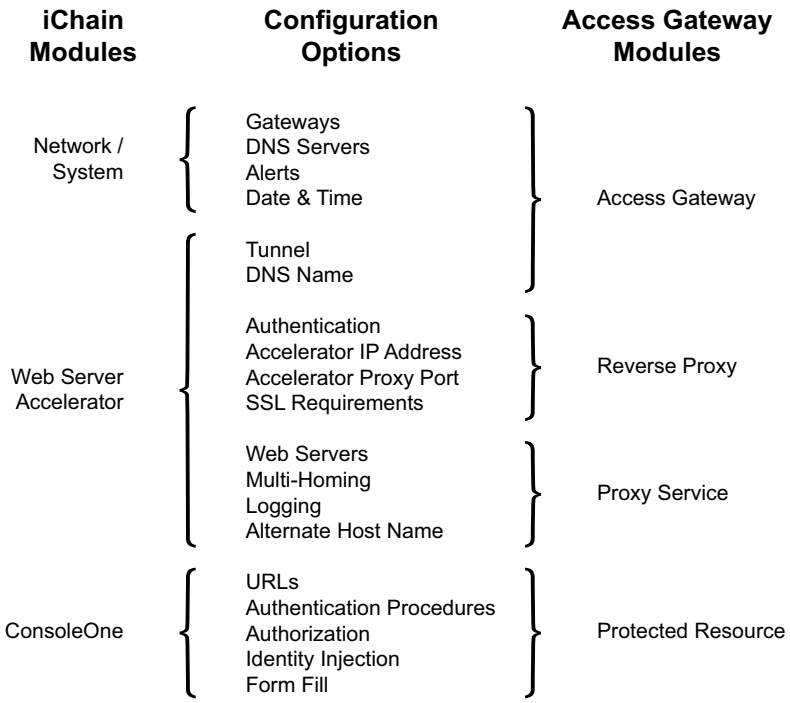
For your first accelerator, we suggest that you select the one with the fewest configuration requirements. If possible, select one that has only a few child accelerators (path-based or domain-based multi-homing accelerators) and does not require Form Fill or have complex access control policies.

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 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 11-5 illustrates the configuration differences between iChain and Access Gateway.

Figure 11-5 *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 148
- “Migrating the Parent Accelerator” on page 148
- “Migrating the Path-Based Multi-Homing Accelerators” on page 150

- “Migrating the Protected Resources” on page 151
- “Testing the Migrated Resources” on page 153
- “Enabling User Access to the Migrated Resources” on page 153

Setting Up Certificates

To enable SSL for Access Gateway connections (from the browser to the Access Gateway and from the 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 the 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 the Access Gateway, see “Importing a Private/Public Key Pair” in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.
- You can use the certificate authority in the Administration Console to create the certificates. For instructions, see “Creating Certificates” in the *Novell Access Manager 3.1 SP4 Administration Console Guide*. When you are finished 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 hostname 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 use the common domain name and other prepended hostnames 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 11.3.3, “Configuring the Identity Server for Authentication,” on page 141.

   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, access the Web App, then 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 cluster, you need to select each cluster member and configure a listening address.
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*: This feature is supported only by the Access Gateway Appliance. iChain does not support this feature, which allows you to add custom headers to your HTML pages and specify a caching policy.

8 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
Authentication Options > [Name of Profile] > Modify	*SSL Mutual Certificate*: In iChain, the certificate is part of the authentication profile.

9 Click *TCP Connect Options* and configure the fields.

To view how you configured the fields in iChain, click *Network* > *IP Addresses* > *TCP Options* in the Web App. The Access Gateway Appliance and the Access Gateway Service support only a few of the iChain options.

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

11 If this accelerator has child accelerators, continue with "Migrating the Path-Based Multi-Homing Accelerators" on page 150. If doesn't have any child accelerators, continue with "Migrating the Protected Resources" on page 151.

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 151.

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 can additionally use LDAP information to authorize access.

In the Access Gateway, protected resources are not global like iChain; they are assigned to a specific proxy service (which is like an iChain accelerator). 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 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 are 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 152
- "Migrating a Restricted Resource" on page 152
- "Migrating a Secure Resource" on page 153

Examine your iChain protected resources, 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.
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 152, or to test the resource you have migrated, continue with "Testing the Migrated Resources" on page 153.

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 by 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 141.

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 153, or to test the resource you have migrated, continue with "Testing the Migrated Resources" on page 153.

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). For migration procedures, see Section 11.3.7, "Migrating Resources with Special Configurations," on page 157.

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 11.3.6, "Enabling Single Sign-On between iChain and Access Manager," on page 154.

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 users 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.

11.3.6 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 156.

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 *Default 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 *Default 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 157.

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 156.

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. Add an entry so that the Access Gateway can directly resolve to the DNS name of the Identity Server. For an Access Gateway Appliance, you need to modify the `hosts` file from the Administration Console. Click *Devices* > *Access Gateways* > *Edit* > *Hosts*.

   This entry 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 be used only 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.

11.3.7 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 11-2 *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.
`<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 LDAP, X509, or SAML 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.

Tag or Tag/Attribute	Access Gateway Field
<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.
<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 11-3 *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.

Tag or Tag/Attribute	Access Gateway Field
`<urlPolicy>`	This is the Form Fill policy.
`<url>`	You assign the Form Fill policy to a protected resource. The protected resource page has a URL Path List where you specify the URL of the page containing the form.

For more information, see "Creating Form Fill Policies" in the *Novell Access Manager 3.1 SP4 Policy 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 167.

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.

iChain and Access Gateway Policy Comparison

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

Table 11-4 *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 LDAP, X509, and SAML 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 SP4 Policy 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 162
- "Migrating a Policy for a Query String" on page 162

8 To assign this policy to a protected resource, see "Configuring a Resource to Use an Identity Injection Policy" on page 163.

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 an 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 163.

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 163.

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, group memberships, and objects in the user’s DN, 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 SP4 Policy Guide*. For other methods, see “Creating Access Gateway Authorization Policies” in the *Novell Access Manager 3.1 SP4 Policy 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 164
- “Creating an Authorization Policy with an Allow and a Deny Rule” on page 164
- “Protecting the Resource with the Authorization Policy” on page 166

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 164.
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*.

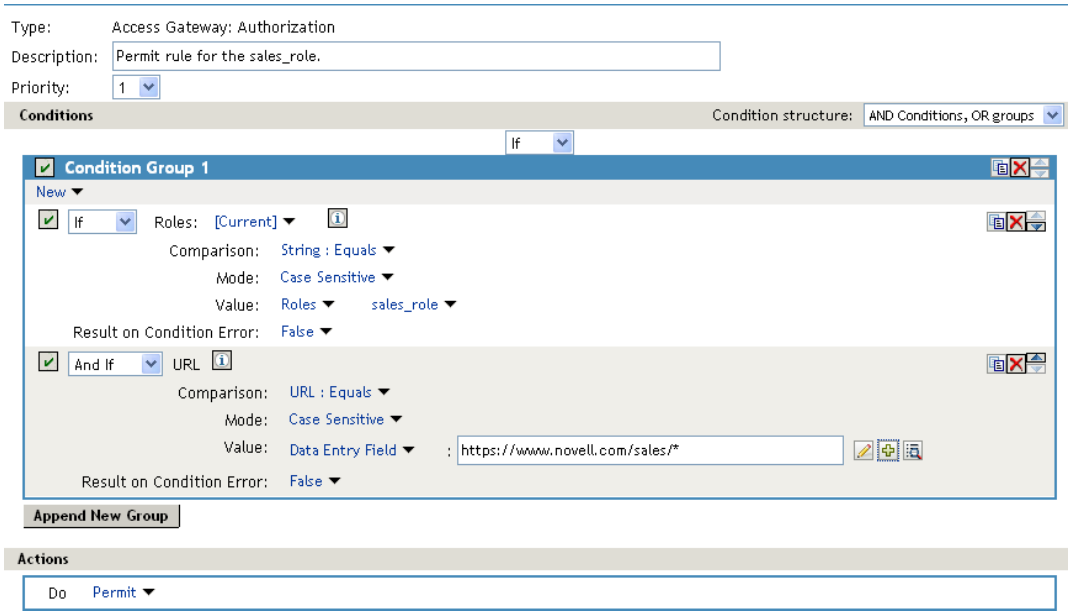
Creating an Authorization Policy with an Allow and a Deny Rule

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 SP4 Policy 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 11-5 shows where to place the information from the iChain file in the Access Gateway profile.

Table 11-5 *Converting an iChain Rewriter File to an Access Gateway Profile*

iChain File Section	Access Gateway Profile Location
`[Name]`	Name specified for the HTML rewriter profile
`[Extension]`	N/A
`[Alias Host Names]—internal rewriter only`	*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 SP4 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 Enterprise JavaBeans 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 SP4 J2EE Agent Guide*.

Migrating Protected Non-HTTP Applications

If you have created protected resources in iChain for non-HTTP applications, you should use the SSL VPN server rather than migrating these resources to the Access Gateway as protected resources.

The SSL VPN server uses the Identity Server for authentication, so single sign-on is enabled between the Access Gateway protected resources and the SSL VPN protected resources.

For more information, see the *Novell Access Manager 3.1 SP4 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 SP4 Policy Guide*.

If the 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 SP4 Policy Guide*.

11.3.8 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 can change the IP addresses. See the following sections in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

- "Changing the IP Address of an Identity Server"
- "Changing the IP Address of the Access Gateway Appliance"
- "Changing the IP Address of the Access Gateway Service"

11.3.9 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 your Identity Server to use port 80 or 443. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.1 SP4 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 and Upgrade

A

A.1 Troubleshooting a Windows Administration Console Installation

The following instructions explain how to run the installation program in debug mode and how to clean up after such an installation.

1. Use the following command to start the installation program:

   `<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true`

   Replace <*filename*> with the name of the executable.
2. Press the Ctrl key until the progress bar reaches 100% and goes away.

   A terminal window opens to display standard output.

   Additional verbose information is sent to the `\am31setup_debug.txt` file.
3. Use the output and the log file to discover the cause of the problem.
4. After you run the installation in debug mode, you must clean up the results:
   - **4a** Delete the temporary packages in the `\pkgdirs` directory, then delete the directory.
   - **4b** Delete the `\am31setup_debug.txt` file.
   - **4c** Delete the installation log files in the following directories:

     Windows 2003 Server and Windows 2008 Server: `\am31setup.log`

     Windows 2003 Server: `\Program Files\Novell\log`

     Windows 2008 Server: `\Program Files (x86)\Novell\log`

IMPORTANT: You need to delete the log files because they contain sensitive information in clear text.

A.2 Troubleshooting a Windows SSL Renegotiation

Perform the following steps to enable the SSL renegotiation on Windows 64-bit platform:

1. Launch Registry Editor by executing the *Start* > *Run* regedit command.
2. In the left pane of Registry Editor, navigate to *My Computer* > `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Tomcat5\Parameters\Java\`.
3. Double-click *Options* in the right pane of the Registry Editor.
4. Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
   - If `-Dsun.security.ssl.allowUnsafeRenegotiation` is available, set the value to true. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=true`
   - If `-Dsun.security.ssl.allowUnsafeRenegotiation` is not available, add `-Dsun.security.ssl.allowUnsafeRenegotiation=true`
5. Go to `C:\Program Files(x86)\Novell\Tomcat\conf\server.xml > Server > Service > Connector`, then search for the connector 8443 and check if the connector has the port 8443.
6. Add the `allowUnsafeLegacyRenegotiation=true string`.
7. Restart Tomcat to enable the SSL renegotiation.

Perform the following steps to enable the SSL renegotiation on Windows 32-bit platform:

1. Launch Registry Editor by executing the command regedit in *Start* > *Run*.
2. In the left pane of Registry Editor, navigate to *My Computer* > `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\Tomcat5\Parameters\Java\`.
3. Double-click *Options* in the right pane of registry editor.
4. Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
   - If `-Dsun.security.ssl.allowUnsafeRenegotiation` is available, set the value to true. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=true`.
   - If `-Dsun.security.ssl.allowUnsafeRenegotiation` is not available, add `-Dsun.security.ssl.allowUnsafeRenegotiation=true`.
5. Go to `C:\Program Files(x86)\Novell\Tomcat\conf\server.xml > Server > Service > Connector`., then search for the connector 8443 and check if the connector has the port 8443.
6. Add the `allowUnsafeLegacyRenegotiation=true string`.
7. Restart Tomcat to enable the SSL renegotiation.

The following instructions explain how to disable the SSL renegotiation in Windows 32- bit and Windows 64-bit platform:

1. Launch Registry Editor by executing the command regedit in Start > Run.
2. In the left pane of Registry Editor, navigate to My Computer > `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\Tomcat5\Parameters\Java\`.
3. Double-click *Options* in the right pane of registry editor.
4. Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
5. In `-Dsun.security.ssl.allowUnsafeRenegotiation`, set the value to false. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=false`
6. Restart Tomcat to disable the SSL renegotiation.

A.3 Troubleshooting an Identity Server Import and Installation

A.3.1 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 Server?

  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 SP4 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.
- If firewalls and time synchronization do not solve the problem, run the reimport script. See Section A.3.2, “Reimporting the Identity Server,” on page 174 for instructions.

A.3.2 Reimporting the Identity Server

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 Identity Server 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. In the Administration Console, delete the Identity Server.
4. On the Identity Server machine, change to the `jcc` directory:

   Linux: `/opt/novell/devman/jcc`

   Windows: `\Program Files\Novell\devman\jcc`
5. Run the reimport script for jcc:

   Linux: `./conf/reimport_nidp.sh jcc`

   Windows: `conf\reimport_nidp.bat jcc`
6. Run the reimport script for the Administration Console:

   Linux: `./conf/reimport_nidp.sh nidp`

   Windows: `conf\reimport_nidp.bat nidp <admin>`

   Replace <*admin*> with the name of your administrator for the Administration Console.
7. If these steps do not work, reinstall the device.

A.3.3 Check the Installation Logs

If the Identity Server fails to install, check the installation logs.

- “Linux Installation Logs” on page 174
- “Windows Installation Logs” on page 175

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.

Log File	Description
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.4 Troubleshooting a Linux Access Gateway Appliance Installation

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

- Section A.4.1, “Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation,” on page 176
- Section A.4.2, “After Reinstalling the Access Gateway, SSL Fails,” on page 176
- Section A.4.3, “Reverting to an Earlier Snapshot of the Access Gateway Appliance Can Cause Multiple Crashes,” on page 176
- Section A.4.4, “Manually Configuring a Network Interface,” on page 177
- Section A.4.5, “Manually Setting and Deleting the Default Gateway,” on page 178

A.4.1 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation

Sometimes, the installation of the Access Gateway Appliance fails 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 installation of the Linux Access Gateway. See Chapter 6, “Installing the Linux Access Gateway Appliance,” on page 65.
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.4.2 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.4.3 Reverting to an Earlier Snapshot of the Access Gateway Appliance Can Cause Multiple Crashes

If you are using a VM environment such as ESXi 4.0, reverting to an earlier snapshot of the Access Gateway Appliance can result in multiple crashes after the server is restarted with the older snapshot.

To work around the issue:

1. Revert to the earlier snapshot.
2. Clear the cache:

   ```
   rm /var/novell/.~newInstall
   ```
3. Restart novell-vmc:

   ```
   /etc/init.d/novell-vmc restart
   ```

A.4.4 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 through 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 rebooted the system after installation.

1. Log in as `root`.
2. At the command prompt, enter the following command:

   ```
   nash
   ```

3. At the nash shell prompt, run the following command to enter the configuration mode:

   ```
   configure .current
   ```

4. To display the current IP address for the eth0 network card, enter the following:

   ```
   show interface eth0
   ```

5. To change the IP address of eth0, enter the following:

   ```
   interface eth0
   ```

6. 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.

   ---

7. To return to the configuration mode, enter the following command:

   ```
   exit
   ```

8. To save the configuration, enter the following command:

   ```
   save .current
   ```

9. For the configuration to take effect, enter the following command:

   ```
   apply
   ```

10. To exit from the configuration mode, enter the following command:

    ```
    exit
    ```

11. To exit from the nash shell, enter the following command:

    ```
    exit
    ```

A.4.5 Manually Setting and Deleting the Default Gateway

NOTE: If Access Gateway Appliance is not imported, modifications to the Access Gateway Appliance configuration should be done through nash. If the Access Gateway Appliance 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_address*> 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.4.6 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.4.7 Verifying Component Installation

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

```
/tmp/novell_access_manager
```

- For logs on RPM installation and network configuration, see `/tmp/novell_access_manager/inst_lag.log`
- For logs on configuration and import during installation, see `/tmp/novell_access_manager/inst_lag_import_<timestamp>.log`
- For all the re-import logs generated while running `lagconfigure.sh` manually, see `/tmp/novell_access_manager/lag_import.log`
- For all the upgrade logs, see `/tmp/novell_access_manager/upgr_lag_<time stamp>.log`

For more information on collecting logs, see "Access Gateway Logs" in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.

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

A.4.8 Signature Error in SLES 11 Network Mode of Installation

When you try to install the SUSE Linux Enterprise Server (SLES) 11 Linux Access Gateway ISO over the network by using the SLES 11 bootable CD, you get a signature error.

To workaround this issue, use the SLES11 Linux Access Gateway bootable DVD.

A.5 Troubleshooting the Access Gateway Service Installation

If your Access Gateway Service fails to install, use one of the following procedures to discover the cause:

- Section A.5.1, “Troubleshooting the Linux Access Gateway Service Installation,” on page 180
- Section A.5.2, “Troubleshooting the Windows Access Gateway Service Installation,” on page 180

A.5.1 Troubleshooting the Linux Access Gateway Service Installation

The following instructions explain how to run the installation program in debug mode and how to clean up after such an installation:

1. Use the following command to start the installation program:

   ```
   LAX_DEBUG=true ./<filename>.bin -DAM_INSTALL_DEBUG=true -
   DAM_INSTALL_DEBUG_JAVA=true
   ```

   Replace <*filename*> with the name of the executable.

   The output is displayed as the execution occurs.

   Additional information is logged to the `/tmp/novell_access_manager/ags_installxxxxx.log` file.
2. Use the output and the log file to discover the cause of the problem.
3. After you run the installation in debug mode, you must clean up the results

   3a Change to the `/tmp/novell_access_manager/`directory.

   3b Delete the following files:

   ```
   ags_installxxxxx.log
   AccessGateway_InstallerLog-<timestamp>.log
   ```

   IMPORTANT: You need to delete the log files because they contain sensitive information in clear text.

A.5.2 Troubleshooting the Windows Access Gateway Service Installation

The following instructions explain how to run the installation program in debug mode and how to clean up after such an installation.

1. Use the following command to start the installation program:

`<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true`

Replace <*filename*> with the name of the executable.

2. Press the Ctrl key until the progress bar reaches 100% and goes away.

   A terminal window opens to display standard output.

   Additional verbose information is sent to the `\agsinstall_debug.txt` file.

3. Use the output and the log file to discover the cause of the problem.

4. After you run the installation in debug mode, you must clean up the results:

   4a Delete the `\agsinstall_debug.txt` file.

   4b Delete the installation log files in the following directories:

   Windows 2003 Server and Windows 2008 Server: `\agsinstall.log`

   Windows 2003 Server: `\Program Files\Novell\log`

   Windows 2008 Server: `\Program Files (x86)\Novell\log`

   IMPORTANT: You need to delete the log files because they contain sensitive information in clear text.

A.6 Troubleshooting the SSL VPN Installation

This section has information on how you can troubleshoot problems while you are installing the SSL VPN server.

- Section A.6.1, “Manually Uninstalling the Enterprise Mode Thin Client,” on page 181
- Section A.6.2, “SSL VPN Health Status Is Yellow after an Upgrade,” on page 182

A.6.1 Manually Uninstalling the Enterprise Mode Thin Client

To manually uninstall the Enterprise mode thin client, do one of the following, depending on your operating software:

- **Windows:** If you are a Windows user, log in as admin and run `uninstall.exe` located in the `c:/Program Files/Novell sslvpn service` directory. You can also uninstall the SSL VPN service through *Start* > *Control Panel* > *Add or Remove Programs*.
- **Linux:** If you are a Linux user, log in as `root` and enter the following command on the Linux workstation:

  ```
  rpm -e novl-sslvpn-service
  ```

- **Macintosh:** If you are a Macintosh user, log in as `root` and do the following on the Macintosh workstation:

  1. Enter the following command to stop the SSL VPN services:

     ```
     /System/Library/StartupItems/novell-sslvpn-service/novell-sslvpn-service stop
     ```

  2. Enter the following command to remove all the contents of the package:

     ```
     rm -rf /System/Library/StartupItems/novell-sslvpn-service
     rm -rf /Library/Receipts/novl-sslvpn-service.pkg
     rm -f /usr/sbin/novl-sslvpn-service
     ```

```
rm -f /usr/sbin/novl-sslvpn-service-upgrade
rm -f /etc/novell-sslvpn-serv.conf
```

NOTE: If you are an administrator or a `root` user of the machine, you cannot switch from Enterprise mode to Kiosk mode unless your system administrator has configured you to connect only in Kiosk mode.

A.6.2 SSL VPN Health Status Is Yellow after an Upgrade

If the status of SSL VPN server installed with Linux Access Gateway is yellow and the *Health* tab displays the following message:

```
The HTTP Reverse Proxy service "soapbc" is functioning properly. The HTTP
Reverse Proxy service <reverse proxy> might not be functioning properly. Few
of the webservers being accelerated are unreachable <Webserver IP>:8080.
```

Modify the existing path-based service accelerating SSL VPN server and configure the loopback IP 127.0.0.1 as the Web server IP.

A.7 Troubleshooting the Access Gateway Import

When you install the 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 sections explain 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.7.1, “Repairing an Import,” on page 182
- Section A.7.2, “Triggering an Import Retry,” on page 183
- Section A.7.3, “Fixing Potential Configuration Errors on the Access Gateway Appliance,” on page 185
- Section A.7.4, “Troubleshooting the Import Process,” on page 185

A.7.1 Repairing an Import

If the Access Gateway does not appear in the Administration Console within ten minutes of installing an Access Gateway, complete the following steps:

1. If a firewall separates the Administration Console and the Access Gateway, make sure the correct ports are opened. See “When a Firewall Separates the Administration Console from a Component” in the *Novell Access Manager 3.1 SP4 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.7.2, “Triggering an Import Retry,” on page 183.

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 185 and report the problem to Novell Support.

A.7.2 Triggering an Import Retry

If the import process failed to start (see Step 3 on page 187), 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.

You are prompted to specify if you want to retain the current configuration or return to the initial configuration.

9 Type `I` if you want to restore the initial values configured during the installation.

or

Type `C` if you want to restore the current configuration of the Access Gateway.

10 Press Enter.

11 Wait 30 seconds, then log in to the Administration Console.

12 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 "Managing Reverse Proxies and Authentication" in the *Novell Access Manager 3.1 SP4 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 SP4 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 SP4 Setup Guide*.

Reimporting the Access Gateway Service

1. Verify that the Administration Console is up by logging into the Administration Console from a Web browser.
2. Verify that you have a configured Identity Server.

   Reimport fails in Access Manager 3.1 SP2 if you do not have a configured Identity Server.
3. 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.
4. In the Administration Console, delete the Access Gateway Service.
5. On the Access Gateway machine, change to the `jcc` directory.

   Linux: `/opt/novell/devman/jcc`

   Windows: `\Program Files\Novell\devman\jcc`
6. Run the reimport script for jcc:

   Linux: `./conf/reimport_ags.sh jcc`

   Windows: `conf\reimport_ags.bat jcc`
7. Run the reimport script for the Access Gateway:

   Linux: `./conf/reimport_ags.sh agm`

   Windows: `conf\reimport_ags.bat agm <admin>`

   Replace <*admin*> with the name of your administrator for the Administration Console.
8. 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 "Managing Reverse Proxies and Authentication" in the *Novell Access Manager 3.1 SP4 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 SP4 Setup Guide*.
- Configure the certificate for the SSL listener. For more information, see "Configuring the Access Gateway for SSL" in the *Novell Access Manager 3.1 SP4 Setup Guide*.

A.7.3 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 185
- “Hostname Is Not Resolvable” on page 185

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.4.6, “Manually Configuring the Hostname, Domain Name, and DNS Server,” on page 178.

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.4.6, “Manually Configuring the Hostname, Domain Name, and DNS Server,” on page 178.

A.7.4 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 185
- “Locating the Log Files” on page 186
- “Determining Where the Error Occurred on the Access Gateway Appliance” on page 186

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 Embedded Service Provider (ESP) of the Access Gateway 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 Administration Console.

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:

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

  Windows Server 2003: `\Program Files\Novell\log\app_sc.0.log`

  Windows Server 2008: `\Program Files (x86)\Novell\log\app_sc.0.log`
- Tomcat Log on the Administration Console:

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

  Windows Server 2003: `\Program Files\Novell\Tomcat\logs\stdout.log`

  Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\logs\stdout.log`
- JCC log on the Access Gateway:

  Linux Appliance or Service: `/opt/novell/devman/jcc/logs/`

  Windows Service: `\Program Files\Novell\devman\jcc\logs`

Determining Where the Error Occurred on the Access Gateway Appliance

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, 2010 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, 2010 3:19:34 PM com.novell.jcc.server.ClientRegistry
   register
INFO: registering ag-AEF62A32 in client registry
Jan 30, 2010 3:19:34 PM com.novell.jcc.server.JCCServerImpl
   processRegisterAlerts
INFO: Sending new device alert to Device Manager for ag-AEF62A32
Jan 30, 2010 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.7.2, “Triggering an Import Retry,” on page 183.

4 In the JCC log, an entry for a successful Access Gateway configuration import should look similar to the following:

```
Jan 30, 2010 3:21:34 PM com.novell.jcc.handler.ProxyHandler
   handleRequest
INFO: This is a request from Device Manager.
Jan 30, 2010 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, 2010 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, 2010 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, 2010 3:21:34 PM com.novell.jcc.handler.ProxyHandler
   proxyHttpURLConnection
INFO: Response code: 200 OK
Jan 30, 2010 3:21:34 PM com.novell.jcc.handler.ProxyHandler
   proxyHttpURLConnection
INFO: response body size: 5958 bytes
Jan 30, 2010 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, 2010 1:54:46 PM com.novell.jcc.client.JCCClientImpl <init>
INFO: Starting client esp-AEF62A32 of type idp
Jan 30, 2010 1:54:46 PM com.novell.jcc.sockets.CipherSocketUtils
   getKey
INFO: loading the secret key from /jcc/conf/jcc.keystore
Jan 30, 2010 1:54:47 PM com.novell.jcc.client.JCCClientImpl$
   ServerConnectionThread run
INFO: server connection thread started
Jan 30, 2010 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$JCCRMIClient_Stub[RemoteStub [ref:
   [endpoint:[10.155.164.14:1029,com.novell.jcc.sockets.
   CipherSocketFactory@6a3960]remote),objID:[134ce4a:1091d189f37
   :-8000, 1]]]]
Jan 30, 2010 3:19:37 PM com.novell.jcc.server.ClientRegistry
   register
INFO: registering idp-esp-AEF62A32 in client registry
Jan 30, 2010 3:19:37 PM com.novell.jcc.server.JCCServerImpl
   processRegisterAlerts
INFO: Sending new device alert to Device Manager for
   idp-esp-AEF62A32
Jan 30, 2010 3:21:34 PM com.novell.jcc.client.AlertDispatcher$
   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, 2010 3:21:34 PM com.novell.jcc.client.AlertDispatcher
   $AlertQueueThread sendAlert
INFO: alert sent successfully
Jan 30, 2010 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, 2010 3:21:34 PM com.novell.jcc.servlet.DispatchServlet
```

```
   dispatchHandler
INFO: looking up handler: Config
Jan 30, 2010 3:21:34 PM com.novell.jcc.handler.HandlerUtils
   verifyCredentials
INFO: login successful
Jan 30, 2010 3:21:34 PM com.novell.jcc.handler.ConfigHandler
   handleRequest
INFO: <romaIDPConfiguration/>
Jan 30, 2010 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 2010(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 2010(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 2010(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 2010(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 2010(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 2010(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 2010(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 2010(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 2010(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.8 Troubleshooting an Access Gateway Appliance Upgrade

A.8.1 Embedded Service Provider Issues After Upgrading

After you upgrade to Access Manager 3.1 SP2, the health status might display *ESP Halted* or *Server Not Responding* errors. This issue might occur because both Tomcat 4 and Tomcat 5 RPMs are present in the system. To verify which versions are present, run the following command:

```
rpm -a | grep tomcat
```

If both the versions of Tomcat are found, then you need to kill the `tomcat4` process manually:

1 Log in as `root`.

2 Specify the following command to stop JCC:

```
/etc/init.d/novell-jcc stop
```

3 Specify the following command to stop Tomcat 4:

```
/etc/init.d/novell-tomcat4 stop
```

4 Specify the following command to stop Tomcat 5:

```
/etc/init.d/novell-tomcat5 stop
```

5 Specify the following command to kill the Tomcat 4 process:

```
rpm -e novell-tomcat4 --nodeps --noscripts
```

6 Specify the following command to start Tomcat 5:

```
/etc/init.d/novell-tomcat5 start
```

7 Specify the following command to start JCC:

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

NOTE: You can verify that Tomcat 4 is removed by executing the following command:

```
rpm -a | grep tomcat
```

A.8.2 Proxy Stops Responding after Trying to Upgrade with the Wrong Upgrade RPM

If you try to upgrade a SUSE Linux Enterprise Server (SLES) 9 Access Gateway Appliance with the SLES 11 RPMs, or a SLES 11 Access Gateway Appliance with the SLES 9 RPMs, the upgrade fails with an RPM level error. The error messages are logged in the `/var/log/laguprade.log` file. The Access Gateway Appliance goes into a non-responsive mode after the failed upgrade.

If this issue occurs, restart the machine and use the appropriate RPMs to upgrade your Access Gateway Appliance.

A.8.3 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.8.4 Upgrading the Access Gateway Appliance Causes Session Stickiness Issues

After upgrading, you might see random errors on services that have more than one web server. This occurs if the back end server expects a user's session to use the same server. To work around this issue, extract and run the zip file `AM_31_SP3_ConfigurationUpgrade.zip` which contains the script that enables session stickiness.

A.9 Troubleshooting a Linux Administration Console Upgrade

A.9.1 After You Upgrade from SLES 9 to SLES 10, Access Manager 3.1 SP2 Fails to Install

If you perform an operating system upgrade rather than a fresh install of the operating system, you need to verify the UID of the D-BUS (messagebus) user on your secondary Administration Consoles. The SLES upgrade creates this user with the same ID as the novlwww user. You need to change this ID before continuing with the upgrade process.

IMPORTANT: If the IDs are the same, Access Manager 3.1 SP2 fails to install.

---

1. Access the control center, then click *User Management*.
2. Set the filter to *System Users*.
3. Select the messagebus (User for D-BUS) user.
4. Click *Edit*.
5. Click the *Details* tab.
6. Change the UID to another ID that is unique.
7. Click *Accept*.
8. Click *Finish*.
9. To continue the upgrade process, see Section 9.4.1, “Upgrading the Linux Administration Console,” on page 100.

A.9.2 Upgrade Hangs

If the upgrade program encounters an error while installing a component or encounters an unexpected condition that requires user input, the installation appears to hang.

1. View the installation screen and determine which component is being upgraded.
2. Change to the `/tmp/novell_access_gateway` directory.
3. View the log file of the component that is being upgraded.

   Solve the problem described in the log file before continuing with the upgrade.

   For example, if the eDirectory health check fails, the `edir` log file indicates that the upgrade program is waiting for a response on whether the upgrade should continue. You should abort the upgrade, run `ndsrepair` to repair the configurations store, then restart with the upgrade process.
4. If the log file of the current component does not contain any errors, use the time stamps of the log files to determine which component just finished its upgrade and check it for errors.

   If you cannot determine which component is causing the problem:

   4a Abort the upgrade.

   4b Enter the following command:

   ```
   tail -f /tmp/novell_access_gateway
   ```

   This command tails all the files created in the specified directory.

   4c Restart the upgrade.

A.9.3 Multiple IP Addresses

If your server has multiple IP addresses, 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.9.4 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.10 Troubleshooting the Uninstall of the Access Gateway Service

When you uninstall an Access Gateway, 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:

Linux Access Gateway Service

```
/opt/novell/accessgateway/removeAccessGateway -DAM_INSTALL_AUTH_BYPASS=true
```

Windows Access Gateway Service:

```
\Program Files\Novell\UninstallData\remove_AccessGateway.exe -
DAM_INSTALL_AUTH_
BYPASS=true
```

A.11 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
```

A.12 Troubleshooting a Linux SSL Renegotiation

To enable the SSL renegotiation on SLES 11, add the parameter `JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=true` in the configuration file `/var/opt/novell/tomcat5/conf/tomcat5.conf if the parameter does not exist. .`

Restart Tomcat to enable SSL renegotiation.

To disable the SSL renegotiation on SLES 11, add the parameter `JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=false` in the configuration file `/var/opt/novell/tomcat5/conf/tomcat5.conf if the parameter does not exist.`

Restart Tomcat to disable SSL renegotiation.

Modifications Required for a 3.0 Login Page

B

B.1 Modifying the File

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.

```
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>
```

B.2 Sample Modified File

The following file shows all the changes that allow 3.0 `login.jsp` to compile on a 3.1 SP2 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>
```

What's New in Previous Releases

C

Novell Access Manager 3.1 SP3 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:

C.1 Identity Server Enhancements

- **Federation Enhancements:** The following features are enhanced in the SAML and Liberty protocols:
  - **NIDP Principal Consistency:** Allows you to set the identity provider session timeout, configure assertion validity time, overwrite the temporary user, and identify real users. For more information, see "Configuring Authentication Methods" and "Configuring the Attribute Matching Method for SAML 1.1" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Whitelist of Target URLs:** Allows you to access only the target URL which is available in the domain list. For more information, see "Configuring Whitelist of Target URLs" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Local Method Execution Post Federation:** This feature authenticates the user as the local service provider after the remote password authentication. This features also configures the assertion validity time and overwrites the temporary user and real user identifications. For more information, see "Defining User Identification for Liberty and SAML 2.0" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Mapping Between Types and Contracts:** The Identity Server is contract-based and this setting permits an association to be made between a contract and the external provider assertion. For more information, see "Modifying the Authentication Card for Liberty or SAML 2.0" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Password Fetch Class Extensions:** The Novell Access Manager supports password retrieval of the users who are mapped based on the CN of the user object and attribute value of the user object in different ways. For more information see, "Configuring Password Retrieval" in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
- **SP Brokering:** The Novell Access Manager Identity Service acts as a federation gateway or a service provider broker (SP Broker). This feature is used along with the Intersite Transfer Service of the identity provider, which enables authentication at a trusted service provider. The SP Broker feature helps control the authentication flow between several identity providers and service providers in a federation circle by allowing the administrator to configure policies that control Intersite Transfers. For example, an administrator can configure a policy with SP

Broker that allows only certain users from an identity provider to be authenticated at a given service provider.For more information, see “SP Brokering ” in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.

- **A-Select Feature Enhancements:** The following sections provides information about A-Select feature.
  - **Defining Session Synchronization for Liberty or SAML 2.0:** You need to configure the properties for the session synchronization between the service provider and the target identity provider. For more information, see “Defining Session Synchronization for the A-Select SAML 2.0 Identity Provider” in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Defining Options for Liberty or SAML 2.0:** According to Single Logout Profile in OASIS SAML V2.0 profiles, the session users can use a front channel binding. This profile is initiated to maximize the successful logout to all users which is propagated by the session authority. For more information, see “Defining Options for Liberty or SAML 2.0” in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.
  - **Configuring Liberty or SAML 2.0 Session Timeout:** You can configure the `web.xml` parameter in the ESP (Embedded Service Provider). When timeout is reached, the ESP creates a SAML 2.0 logout request to remote Identity Provider over SOAP backchannel. For more information, see “Configuring the Liberty or SAML 2.0 Session Timeout” in the *Novell Access Manager 3.1 SP4 Identity Server Guide*.

C.2 Access Gateway Enhancements

- **Load Balancing Feature:** The load balance feature at session level helps you to configure the web servers at different levels. For more information, see “Configuring Web Servers” in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.
- **Configuring High Availability:** The High Availability option of the Linux Access Gateway helps improve overall reliability. This section provides information on hardware requirements, configuration details about fresh installation and upgrade scenarios, and functionality details of the High Availability option. For more information, see “Configuring the High Availability Feature” in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.
- **Session Stickiness Option:** You can use the session stickiness option if multiple Web Servers are configured for a service. Selecting this option makes the proxy server to use the same web server for all fills during a session. For more information, see “Configuring Web Servers” in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.

C.3 Administration Console Enhancements

- **Policy View Administrator:** A policy view administrator has rights only to view policy containers. The super administrators can create a special type of delegated administrators called policy view administrators who can only view the policies in the policy container assigned to them. They policy view administrators can login to Access Manager with their credentials and they are allowed to view only the policy containers assigned to them. For more information, see “Administration Console” in the *Novell Access Manager 3.1 SP4 Administration Console Guide*.

C.4 NAT Support

The Network Address Translation (NAT) protocol maps all the public IP addresses to communicate with a single private IP address. The network administrators create a NAT table to map the public-to-private and private-to-public IP address. The IP address can be static or dynamic.

Access Manager can be configured by using NAT, which enables the communication between the Administration Console from local network to other Access Manager devices such as Identity Server and Access Gateway. The devices can be in the external network or in another private network. The NAT address needs be to configured in router.

C.5 LDAP Rebind

Once a new LDAP SSL connection is made, it is kept open for reuse. For every new user requests, the same LDAP SSL connection can be used to rebind to a different user. The connection establishment overhead for every LDAP request is removed which boosts the performance in slow links. The maximum number of connections in the pool and the interval for which a connection can be kept open (LDAP timeout) can be configured.