Installation Guide

Access Manager 3.2 SP2

June 2013

Legal Notice

Contents

About This Guide

The purpose of this guide is to provide an introduction to NetIQ Access Manager and to describe the installation, upgrade, and removal procedures.

For information about the J2EE Agents, see the *NetIQ Access Manager 3.2 SP2 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.

Documentation Updates

For the most recent version of the *Access Manager Installation Guide*, visit the NetIQ Access Manager Documentation Web site (https://www.netiq.com/documentation/novellaccessmanager31/).

Additional Documentation

- *NetIQ Access Manager 3.2 SP2 Setup Guide*
- *NetIQ Access Manager 3.2 SP2 Administration Console Guide*
- *NetIQ Access Manager 3.2 SP2 Identity Server Guide*
- *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*
- *NetIQ Access Manager 3.2 SP2 Policy Guide*
- *NetIQ Access Manager 3.2 SP2 J2EE Agent Guide*
- *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*

NOTE: Contact namsdk@netiq.com for any query related to Access Manager SDK.

1 NetIQ Access Manager Product Overview

NetIQ 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.

For information on what's new in Access Manager 3.2 SP2, see Access Manager 3.2 Service Pack 2 Readme.

This section discusses the following topics:

1.1 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.

NetIQ 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:

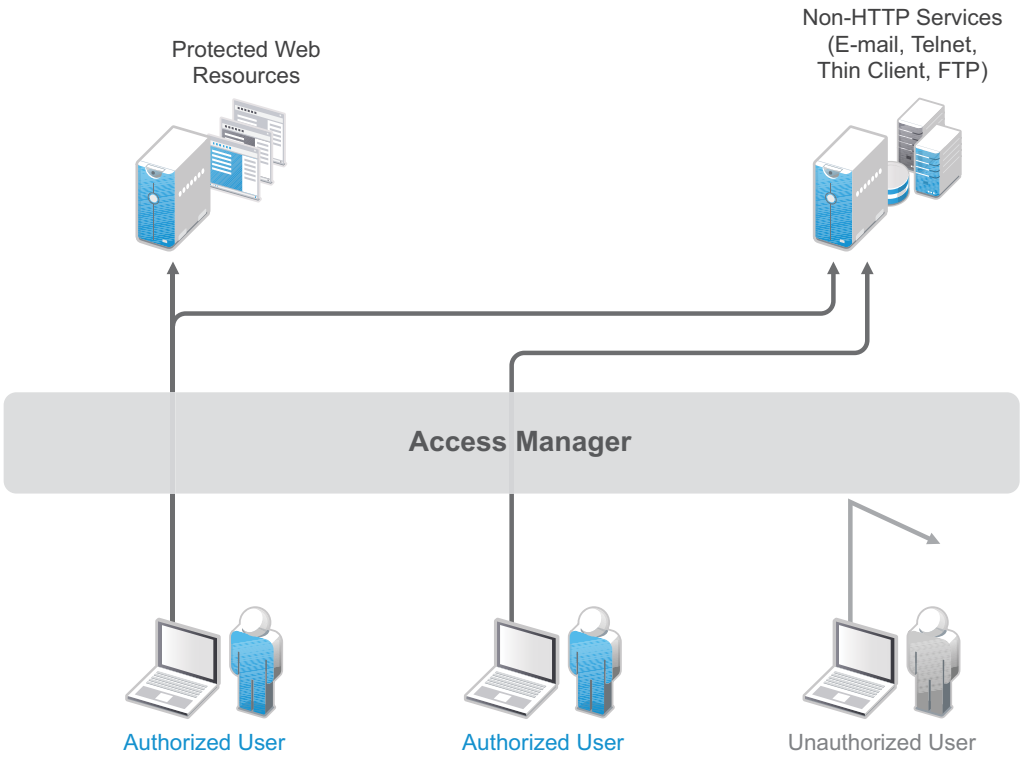
- Protecting resources so that only authorized users can access them, whether those users are employees, customers, or partners.
- Ensuring that the users who are authorized to use a resource can access that resource regardless of where the users are currently located.
- Requiring users to manage multiple 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 1.2, "How Access Manager Works," on page 19.

1.1.1 Protecting Resources While Providing Access

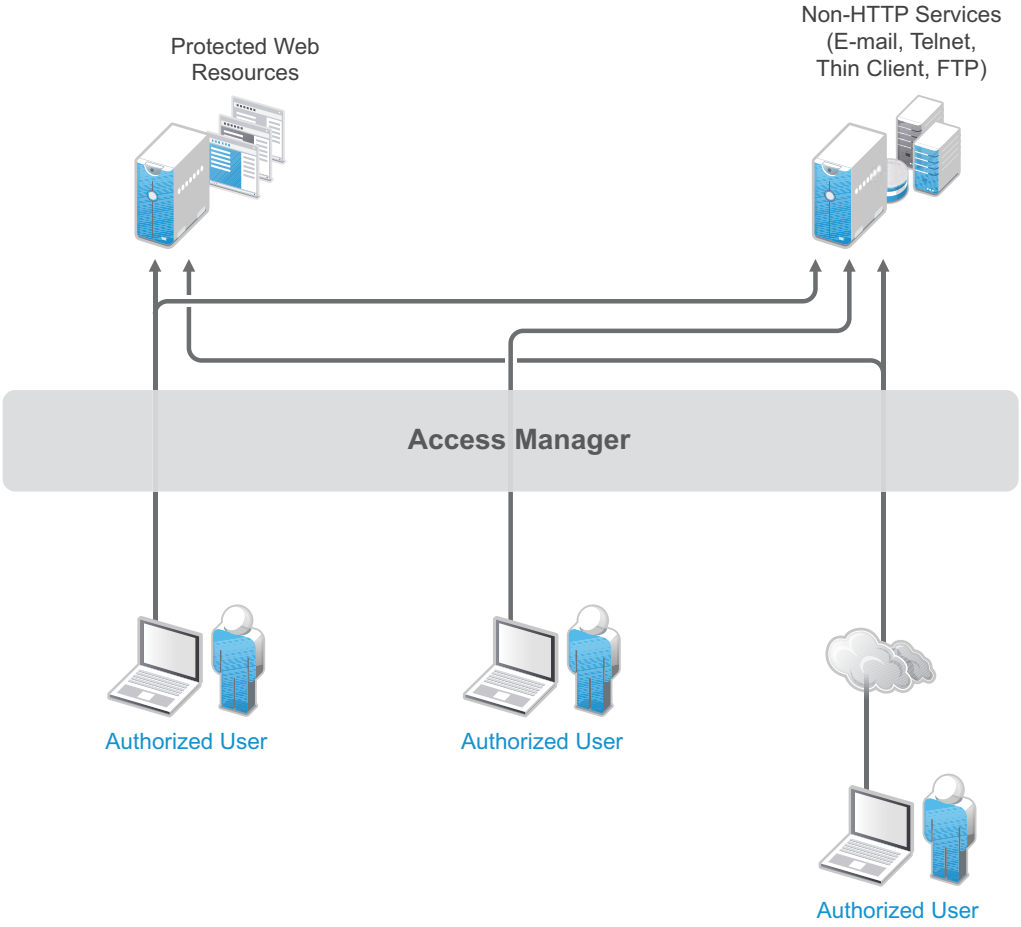
The primary purpose of Access Manager is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources as well as traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized to use the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

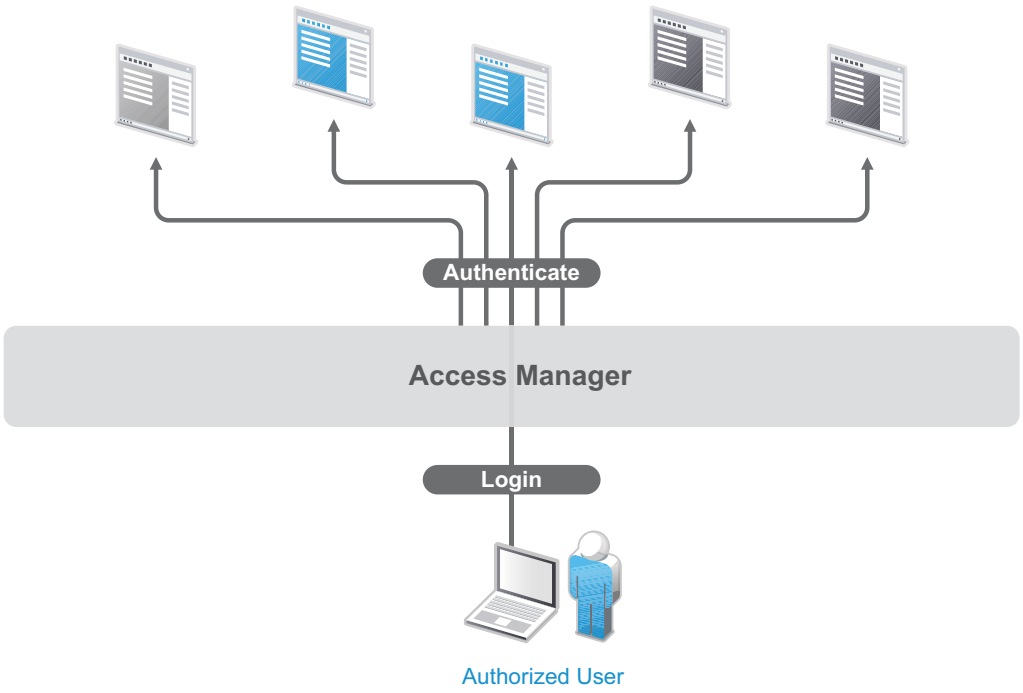
Because not all users work from within the confines of your local network, access to resources is independent of a user's location, as shown in the following illustration. Access Manager provides the same secure access and same experience whether the user is accessing resources from your local office,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



1.1.2 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.



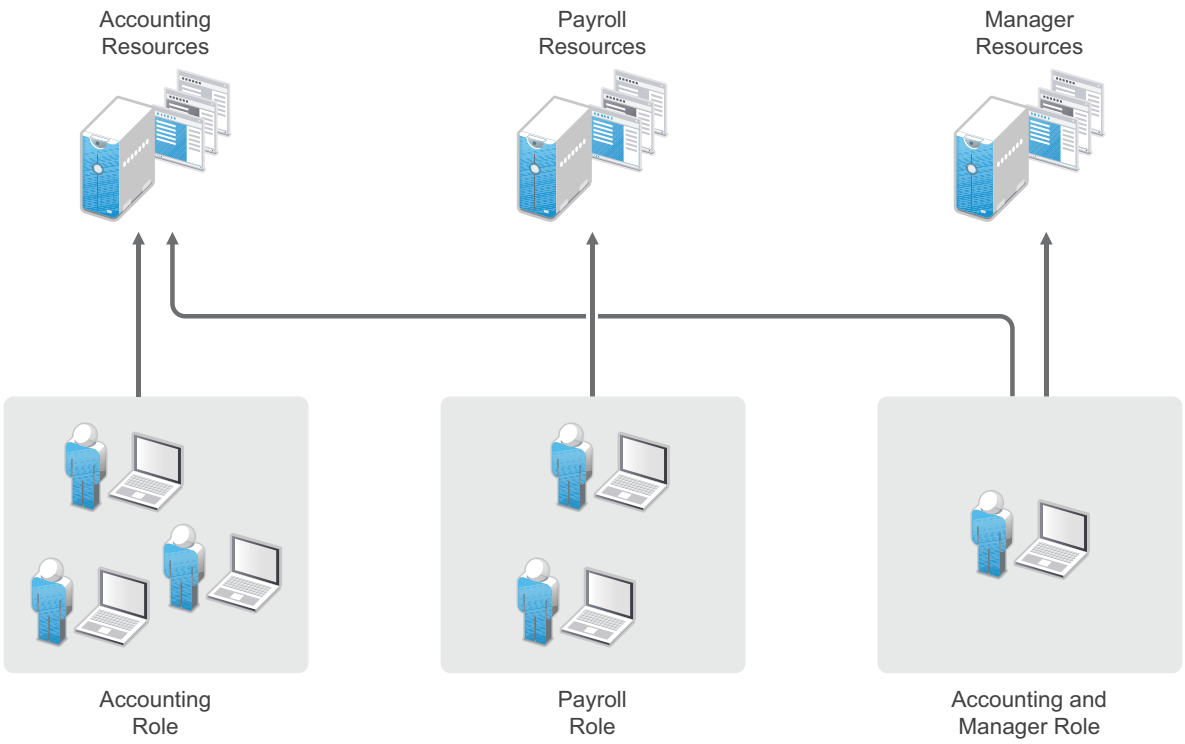
By simplifying the use and management of passwords, Access Manager helps you enhance the user's experience, increase security, streamline business processes, and reduce system administration and support costs.

1.1.3 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.



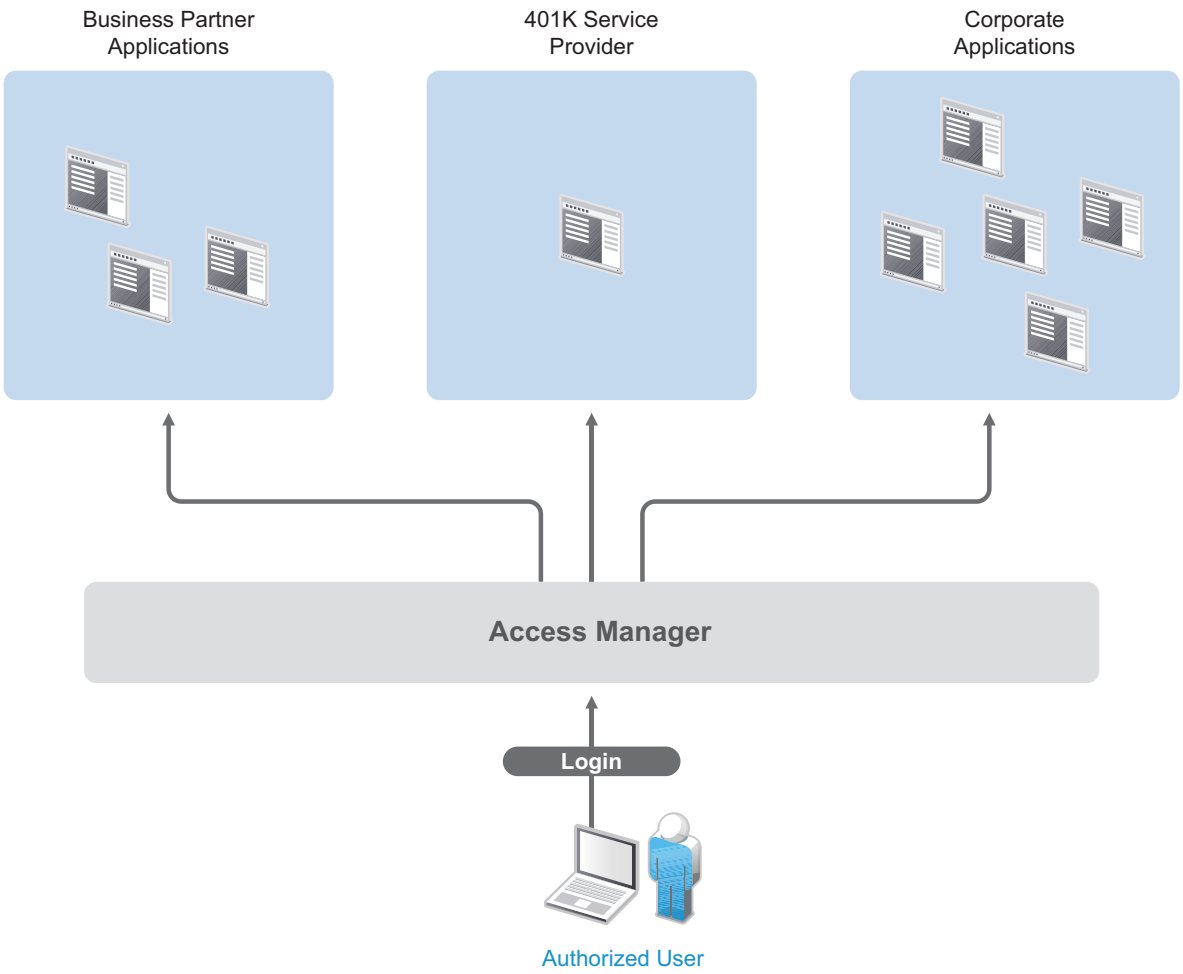
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

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.

1.1.4 Sharing Identity Information

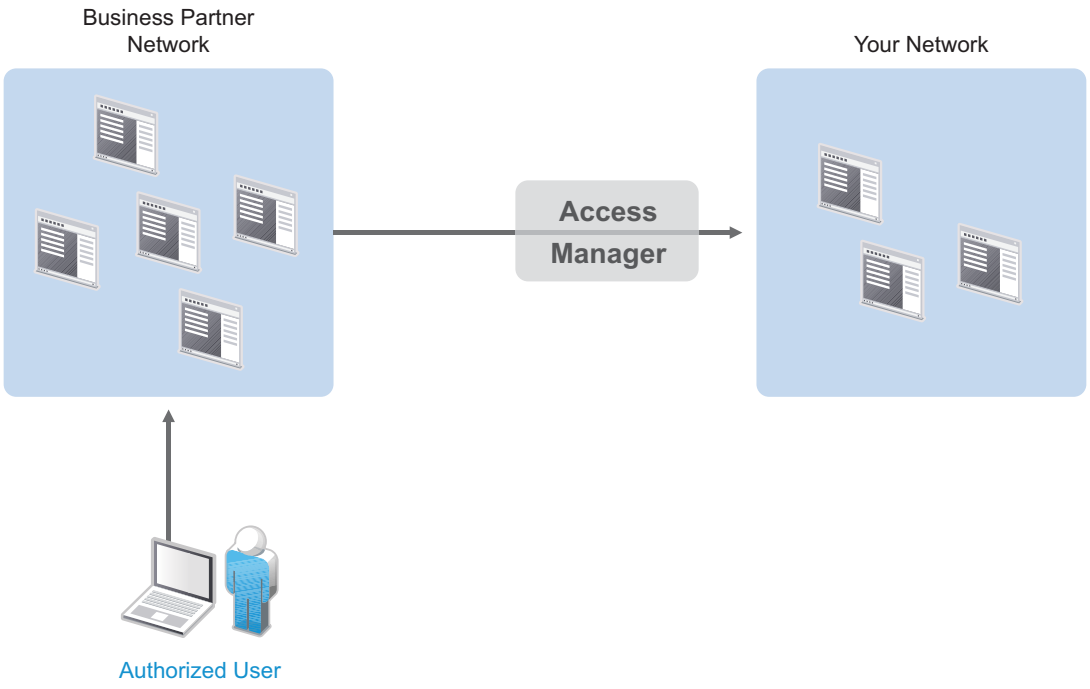
In today's business environment, few organizations stand alone. More than likely, you have trusted business partners with whom you need to shared resources in a secure manner. Or, you have business services, such as a 401k management system, to which you need to provide employee access. Or, maybe your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



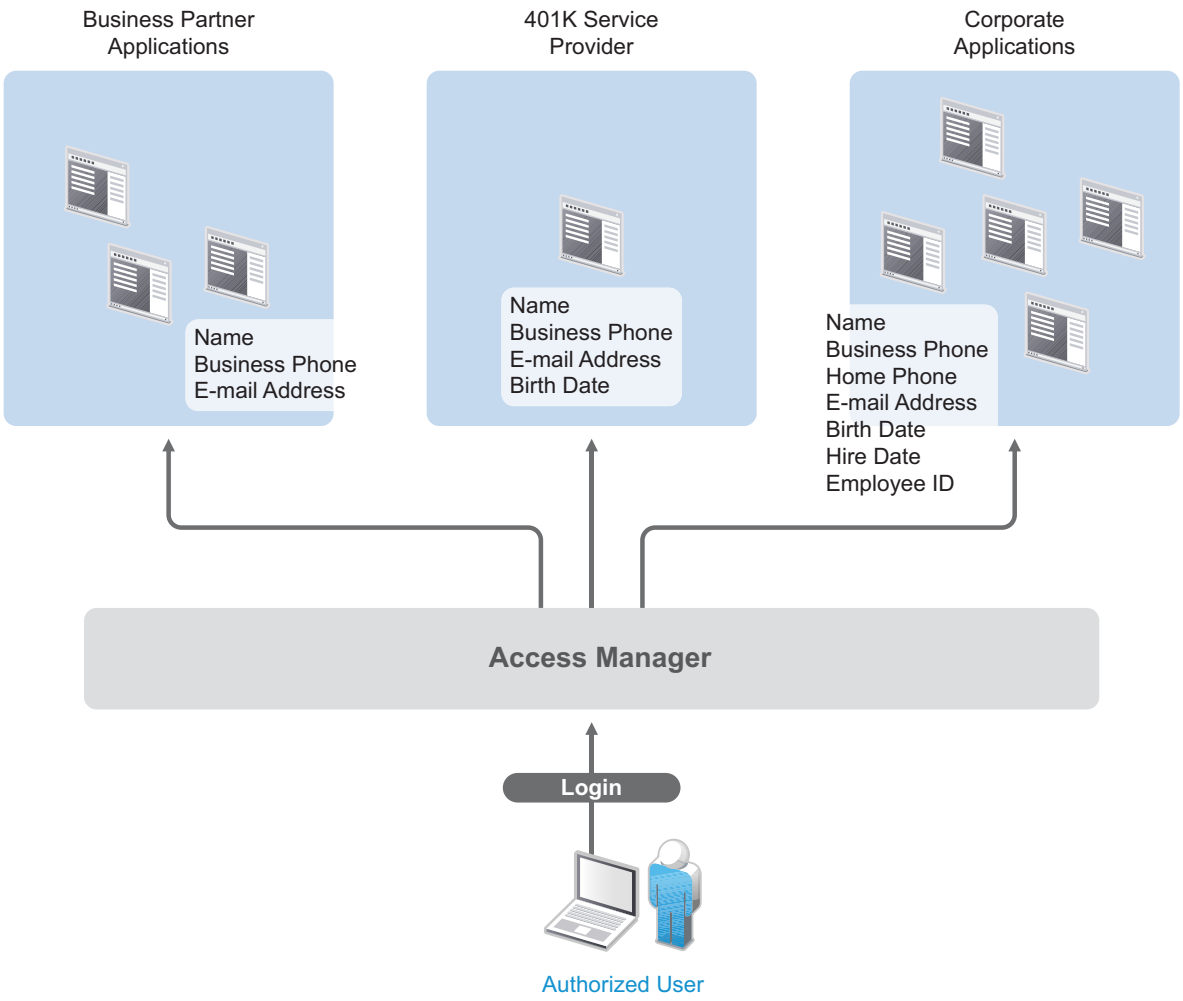
In addition to simply linking user accounts in different identity domains, Access Manager also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization can initiate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

1.1.5 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.

1.1.6 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.

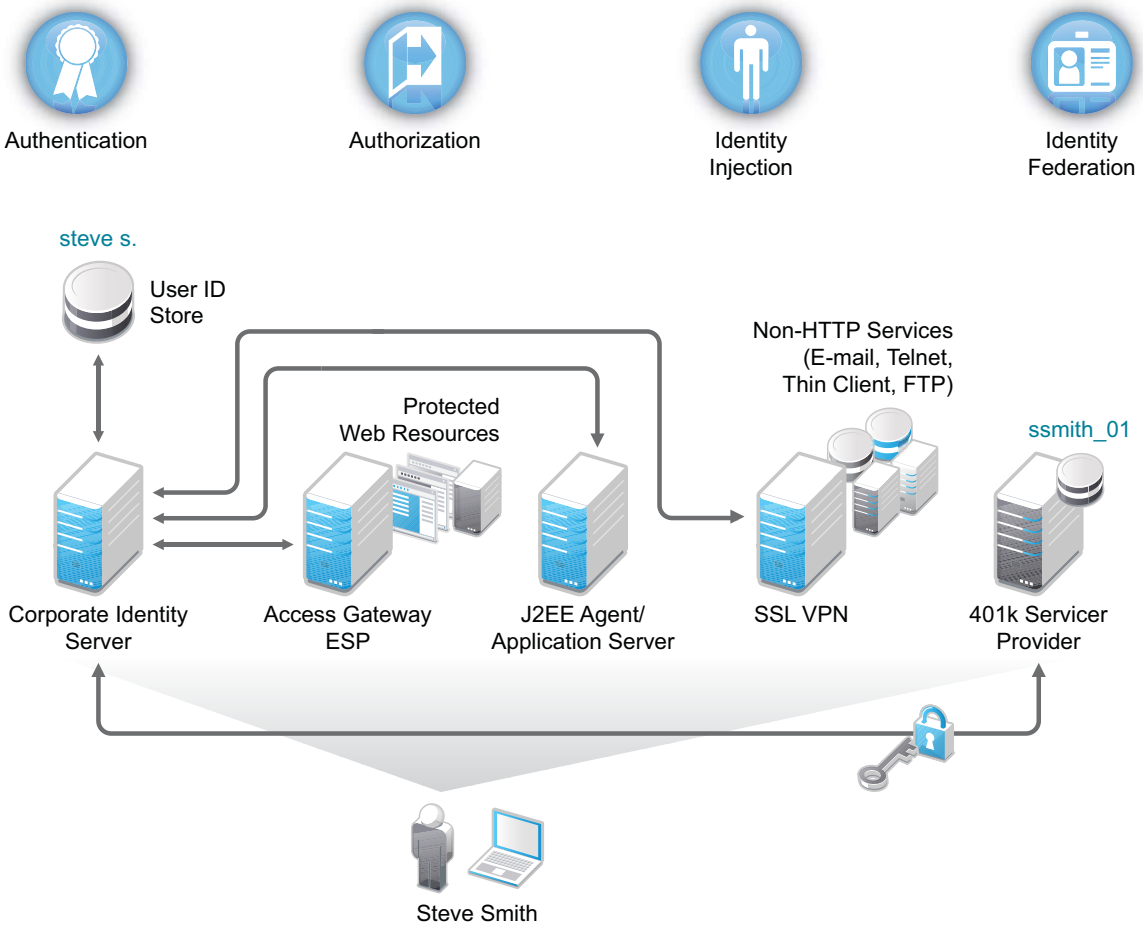
Specifically, Access Manager helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager can generate the reports you need, turning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

1.2 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 1-1 illustrates the primary purposes of Access Manager: authentication, identity federation, authorization, and identity injection.

Figure 1-1 *Access Manager*



1.2.1 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.

1.2.2 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.

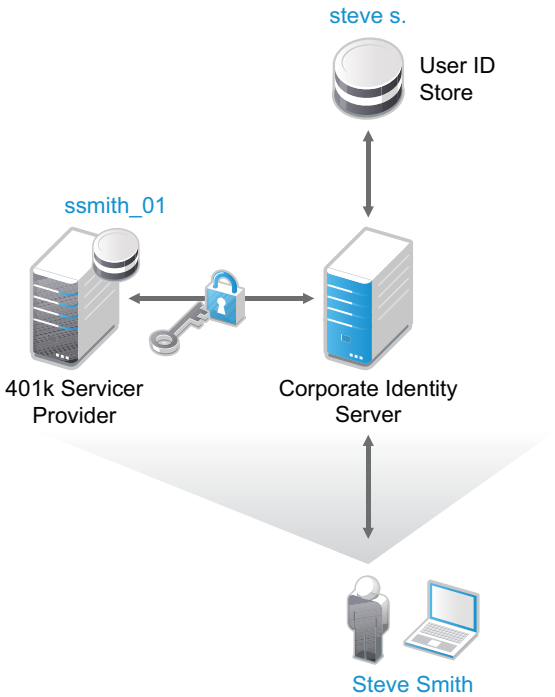
1.2.3 Identity Injection

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.

1.2.4 Identity Federation

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

Figure 1-2 *Identity Federation*



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

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

1.2.5 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\Tomcat7\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:

```
/opt/novell/nam/idp/conf /tomcat7.conf
```

Value data for the registry key to enable the SSL renegotiation on SLES 11 SP1 and SP2 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.

1.3 Access Manager Devices and Their Features

1.3.1 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 1-3 *NetIQ 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.

1.3.2 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 NetIQ 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.

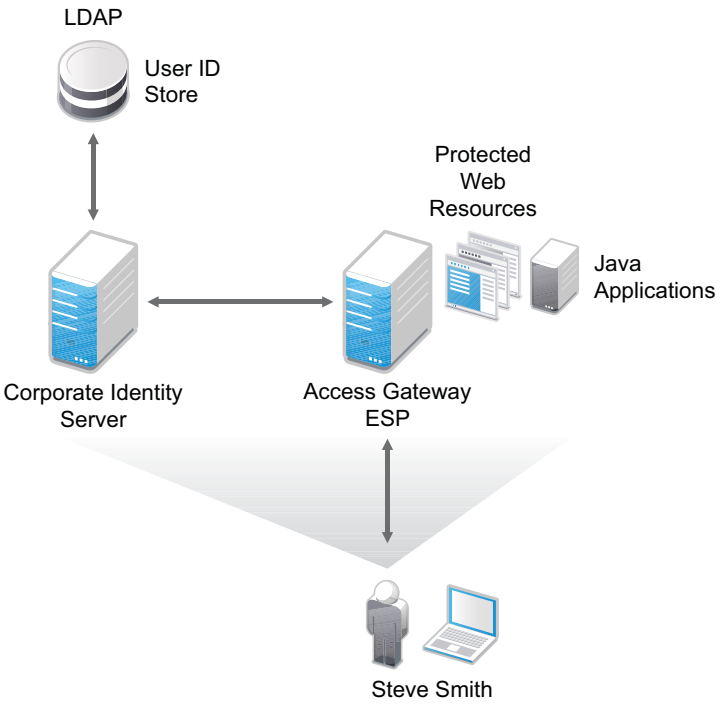
For an overview of Liberty, see "About Liberty" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

For an overview of SAML, see "Understanding How Access Manager Uses SAML" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

1.3.3 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 1-4 *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.

Access Manager 3.2 onwards, there are two types of Access Gateways. Both are based on the same core technology and differ only in their deployment method.

Access Gateway Appliance: It is installed as a soft appliance, which includes the operating system.

Access Gateway Service: It requires you to provide the operating system.

Previous versions of Access Manager also provided a flexible deployment model for the Access Gateway that included both an appliance option (Linux Access Gateway) and a service option (Access Gateway Service). Features of the Access Gateway Appliance and the Access Gateway Service are same but differ from the Linux Access Gateway.

For more information about the differences, see Appendix D, "Feature Comparison of Different Types of Access Gateways," on page 127.

For information about how to upgrade or migration your chosen Access Gateway technology, see "Upgrading Access Manager"in the *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*.

1.3.4 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.

1.3.5 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.

1.3.6 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.

1.3.7 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 NetIQ 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.

1.3.8 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.

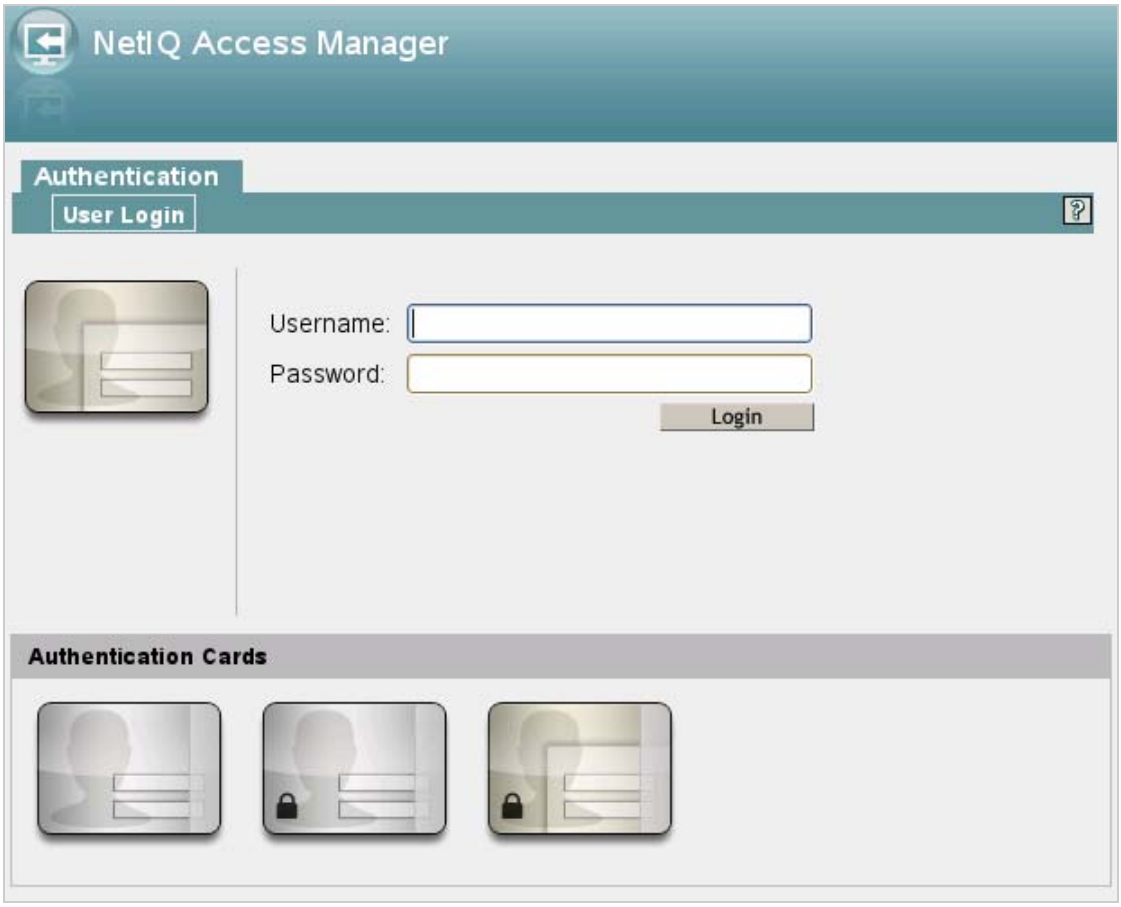
1.3.9 Embedded Service Provider

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.

1.3.10 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 1-5 *Access Manager User Portal*



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

1.3.11 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 Access Gateway Appliance and Service, see "Customizing Error Messages and Error Pages on Access Gateway" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.
- For the Identity Server, see "Customizing Identity Server Messages" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

1.4 Differences Between Access Manager and Access Manager Appliance

The following table lists differences between Access Manager 3.2 and Access Manager Appliance 3.2:

Features	Access Manager Appliance	Access Manager
Installation	All the components, such as the identity provider, Access Gateway, and SSL VPN, are installed on a single machine.	Each Access Manager component such as the identity provider, Access Gateway, and SSL VPN, can be installed on different machines. To deploy the existing solution in a cluster mode, at least 6 machines are required.
Duration of Installation	Automates several configuration steps to quickly set up the system.	Usually takes more time to install and configure each component.
User Input Options	Access Manager Appliance is a software appliance. It takes only a few parameters as input. Several options assume default values.	The user interface has several options, so you need to have a good understanding of all the components.
Installation and Configuration Phases	The installer takes care of configuration for each component. The product is ready for use after it is installed.	Separate installation and configuration phases for each component. After installation, each Access Manager component needs to be separately configured.
Mode of release	Access Manager is released as a software appliance.	Delivered in binaries.

Features	Access Manager Appliance	Access Manager
	The Administration Console, Identity Provider, and SSL VPN are accelerated by Access Gateways. Only one open port, - port 443 - is required in the firewall to deploy Access Manager Appliance. Having only one open port in the firewall enhances security.	Multiple ports need to be opened for deployment.
Certificate Management	Certificate management has been simplified. To replace or renew certificates, the administrator updates only one place, which internally updates all certificates and key stores.	The administrator needs to make changes at multiple places to change certificates.
Default Portal	After a successful installation, a default portal is ready for administrator reference. The administrator can access the default portal using the http://hostname URL. This portal provides detailed information of Access Manager Appliance usage.	
Ready-made Access Manager	The following configuration is internally done when Access Manager Appliance is installed: ◆ Importing Identity Provider, Access Gateway, and SSL VPN components. ◆ Automatic clustering of Identity Provider, Access Gateway, and SSL VPN components. ◆ Automatic configuration of Identity Provider and bringing it to the green state. ◆ Automatic configuration of Access Gateways and associating them with an identity provider. ◆ Automatic configuration of SSL VPN and bringing it to the green state. ◆ Automatic service creation to accelerate the identity provider, Administration Console, and portal. Because the configuration is internally taken care of, the administrator only needs to link the user store and Web servers to accelerate his Web servers through Single Box.	The administrator needs to manually configure each component to bring up the system for use.

Features	Access Manager Appliance	Access Manager
System Configuration through Administration Console	Administration Console is the single point of reference to configure all the components in the Access Manager Appliance.	
64-bit Support	For better performance and scalability, a 64-bit support has been provided for all components.	Not all components provide 64-bit support.
Platform Upgrade	All the components are supported on the latest Tomcat 7 and Java 1.7.0_04 versions.	All components are supported on Tomcat 7 and Java 1.7.0_04.

NOTE: Clustering is not supported between Access Manager components and Access Manager Appliance.

2 Installation Requirements

This section explains the requirements for installing the NetIQ 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/beta/novellaccessmanager32/).

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 *NetIQ Access Manager 3.2 SP2 J2EE Agent Guide*.

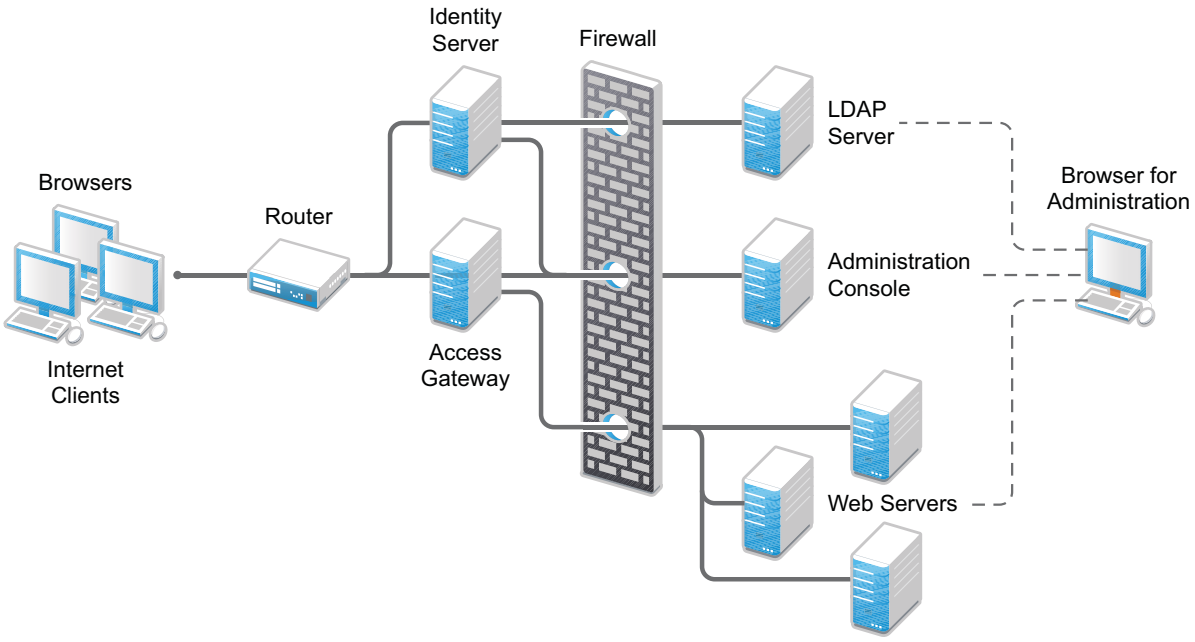
2.1 Recommended Installation Scenarios

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.

2.1.1 Basic Setup

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

Figure 2-1 *Basic Installation Configuration*



1. Install the Administration Console.

   The Administration Console and the Identity Server are bundled in the same download file or 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 1289, TCP 524, TCP 636.

   For more information about these ports, see "Setting Up Firewalls" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

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

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

4. Install the Access Gateway.

   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 *NetIQ Access Manager 3.2 SP2 Setup Guide*.

   In this configuration, the LDAP server is separated from the Identity Server by the firewall. Make sure you open the required ports. See "Setting Up Firewalls" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

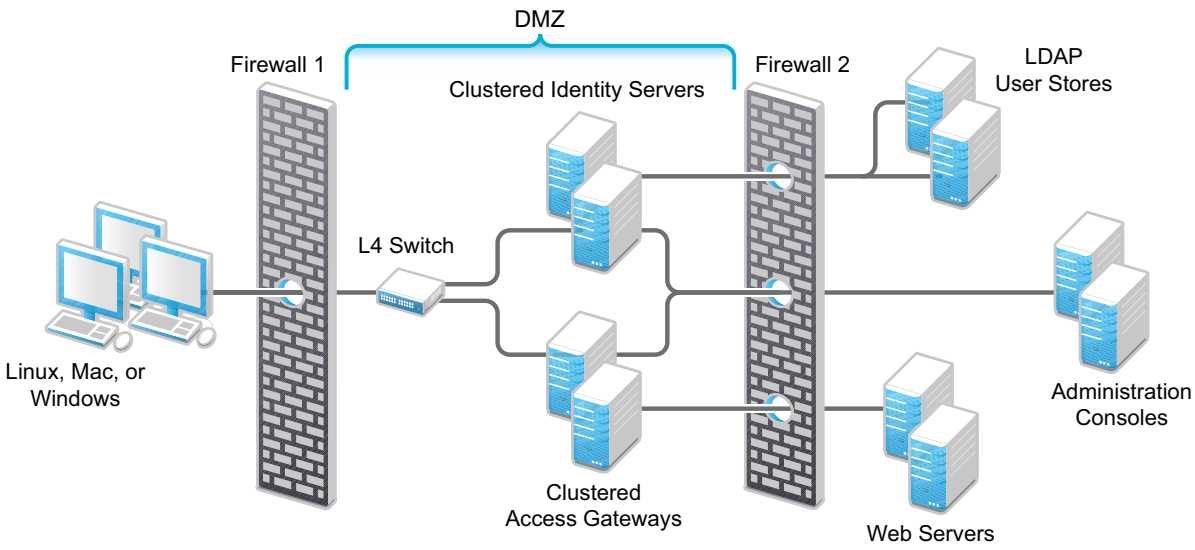
For information about setting up configurations for fault tolerance and clustering, see "Clustering and Fault Tolerance" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

The firewall protects the LDAP server and the Administration Console, both of which contain a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. The Identity Server is not much of a security risk, because it does not permanently store any user data. This is a configuration that NetIQ has tested and can recommend. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Identity Servers and Access Gateways.

2.1.2 High Availability Configuration with Load Balancing

Figure 2-2 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 2-2 *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.

2.2 Hardware Platform Requirements

For the Linux components (Identity Server, Administration Console, SSL VPN, Access Gateway Appliance and Service), you should select a platform supported by SUSE Linux Enterprise Server (SLES) 11 SP1 and SP2 or Red Hat Enterprise Linux (RHEL) versions 6.2, 6.3, or 6.4.

For the Windows components (Identity Server, Administration Console, Access Gateway Appliance and Service), you should select a platform supported by Windows 2008 Server R2 Standard or Enterprise Edition.

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

- Section 2.4, “Administration Console Requirements,” on page 34
- Section 2.5, “Identity Server Requirements,” on page 37
- Section 2.6, “Access Gateway Requirements,” on page 38
- Section 2.7, “SSL VPN Requirements,” on page 40

2.3 Network Requirements

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

- A server configured with an LDAP directory (eDirectory 8.8 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.

2.4 Administration Console Requirements

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.

- Section 2.4.1, “Linux Requirements,” on page 35
- Section 2.4.2, “Windows Requirements,” on page 36
- Section 2.4.3, “Browser Support,” on page 37

2.4.1 Linux Requirements

The Access Manager Administration Console has the same hardware requirements as the SLES 11 SP1 and SP2 operating system with one exception. 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:

- Minimum 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 11 SP1 and SP2 with 64-bit operating system x86-64 hardware.
  - RHEL versions 6.2, 6.3, or 6.4 64-bit.
  - For installing RHEL version 6.4 (out-of-box support), the workaround is provided in TID 7012850.
- Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.
- **SLES:** Make sure the following packages are installed:
  - perl-gettext, gettext-runtime: The required library and tools to create and maintain message catalogs.
  - python: The basic Python library.
  - compat: Libraries to address compatibility issues. 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 the following command to verify:

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

    Use YaST to install the packages.

  RHEL: Ensure that the following rpms or higher versions are installed:
  - glibc-2.12-1.25.el6_1.3.i686.rpm
  - libgcc-4.4.5-6.el6.i686.rpm
  - libstdc++-4.4.5-6.el6.i686.rpm
  - ncurses-libs-5.7-3.20090208.el6.i686.rpm
  - nss-softokn-freebl-3.12.9-3.el6.i686.rpm

    Use the following command to install rpm:

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

    Use the following command to verify:

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

- Minimal SLES 11 SP1 and SP2 installation:
  - **SLES 11 SP1 and SP2:** On a minimal install of SLES 11 SP1 and SP2, 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 server 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 43.

2.4.2 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.
- 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 is installed. If you have a version installed, uninstall it.

For the Administration Console installation instructions, see "Installing the Access Manager Administration Console" on page 43.

2.4.3 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 8.x and later
- Mozilla Firefox

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

If you are using the latest Firefox version, use the latest version of Sun (Oracle) JRE.

2.5 Identity Server Requirements

The Identity Server is the second component you install, and it can be installed on Linux or Windows:

- Section 2.5.1, “Linux Requirements,” on page 37
- Section 2.5.2, “Windows Requirements,” on page 38

Clients that authenticate directly to the Identity Server can use any browser or operating system.

2.5.1 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.
- SLES 11 SP1 and SP2 64-bit operating system or RHEL versions 6.2, 6.3, or 6.4 64-bit.

  RHEL: Ensure that the following rpms or higher versions are installed:
  - glibc-2.12-1.25.el6_1.3.i686.rpm
  - libgcc-4.4.5-6.el6.i686.rpm
  - libstdc++-4.4.5-6.el6.i686.rpm
  - ncurses-libs-5.7-3.20090208.el6.i686.rpm
  - nss-softokn-freebl-3.12.9-3.el6.i686.rpm

    Use the following command to install rpm:

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

    Use the following command to verify:

    ```
    rpm -qa | grep <rpm name>
    ```
- Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.
- gettext
- python (interpreter)

- 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 4, "Installing the NetIQ Identity Server," on page 53.

2.5.2 Windows Requirements

The Windows machine requires the following software and 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.
- 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.

For installation instructions, see Chapter 4, "Installing the NetIQ Identity Server," on page 53.

2.6 Access Gateway Requirements

In addition 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). For information on the differences between Access Gateway Appliance 3.1 SP4 and Access Gateway Appliance 3.2, see Appendix D, "Feature Comparison of Different Types of Access Gateways," on page 127.

These Access Gateways have the following requirements:

2.6.1 Access Gateway Appliance Requirements

The Access Gateway Appliance runs on SLES 11 SP1 and SP2, 64-bit operating system on 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:

- Minimum 4 GB RAM and recommended is 8 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 SP1 and SP2 for x86-64 hardware, open the YES CERTIFIED Bulletin (http://developer.novell.com/yessearch/Search.jsp), select Service Pack 1 or Service Pack 2 for SUSE® SLES 11 SP1 and SP2 in NetIQ Product, and search for 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 5, "Installing the Access Gateway Appliance," on page 59.

2.6.2 Access Gateway Service Requirements

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

- SLES 11 SP1 and SP2 64-bit operating system or RHEL versions 6.2, 6.3, or 6.4 64-bit.

  NOTE: For the SLES 11 SP1 and SP2 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.
- Minimum 4 GB RAM and recommended is 8 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.
- Ensure that the following rpms or higher versions are installed if you have installed Access Gateway Service on RHEL:
  - apr-1.3.9-3.el6.x86_64
  - apr-util-1.3.9-3.el6_0.1.x86_64
  - libtool-ltdl-2.2.6-15.5.e16.x86_64
  - unixODBC-2.2.14-11.el6.x86_64
  - db4-4.7.25-16.el6.x86_64
  - glibc-2.12-1.25.el6_1.3.i686
  - libesmtp-1.0.4-15.el6.x86_64
  - nss-softokn-freebl-3.12.9-3.el6.i686

2.6.3 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, in either Standard or Enterprise Edition, with the latest patches applied.
- Minimum 4 GB RAM and recommended is 8 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.

2.6.4 Client Access Requirements

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

NOTE: For information on the differences between Linux Access Gateway Appliance, Access Gateway Appliance, and Access Gateway Service, see Appendix D, "Feature Comparison of Different Types of Access Gateways," on page 127.

2.7 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.
- Minimum 4 GB RAM and recommended is 8 GB RAM.
- Dual CPU or Core (3.0 GHz or comparable chip).
- SLES 11 SP1 and SP2, 64-bit operating system
- Ensure that the following rpms or higher versions are installed:
  - Zlib-32bit
  - libgcc43-32bit-4.3.4_20091019-0.7.35
  - libstdc++43-32bit-4.3.4_20091019-0.7.35
  - libopenssl0_9_8-32bit-0.9.8j-0.44.1
- `gettext` package
- Static IP address

NOTE: Installation of SSL VPN is not supported on RHEL and Windows.

2.8 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 SP1 and SP2 Access Gateway does not support XEN para virtualization for the Access Manager 3.2 release.

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

- Section 2.8.1, "Keeping Time Synchronized on the Access Manager Devices," on page 41
- Section 2.8.2, "How Many Virtual Machines Per Physical Machine," on page 41
- Section 2.8.3, "Which Network Adapter to be used for VMWare ESX," on page 42

2.8.1 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 11 SP1 and SP2: The `ntpdate` command is not supported by SLES 11 SP1 and SP2. 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 SP1 and SP2 is also applicable for Access Gateway appliance if XEN Full Virtualization is used.

2.8.2 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.

.

2.8.3 Which Network Adapter to be used for VMWare ESX

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

3 Installing the Access Manager Administration Console

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 *NetIQ Access Manager 3.2 SP2 Setup Guide*.

3.1 Installation Procedures

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

NOTE: If Administration Console and Identity Server are installed on different servers, both use 8080 and 8443 ports. If Administration Console and Identity Server are installed on the same server, Identity Server uses 8080 and 8443 ports and Administration Console uses 2080 and 2443 ports.

3.1.1 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 2.4, “Administration Console Requirements,” on page 34.

3 Open a terminal window.

4 Access the install script:

4a Make sure you have downloaded the software or you have the CD available.

For software download instructions, see the "NetIQ Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager32/) .

4b 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>`

4c Change to the `novell-access-manager` directory.

5 At the command prompt, enter the following:

`./install.sh`

It is important that you ensure that you have adequate space in the system before you proceed with the installation. For details, refer

6 When you are prompted to install a product, type `1` for *Install NetIQ Access Manager Administration*, then press the Enter key and select *1. Install Administration Console*.

7 Review and accept the License Agreement.

Novell Base and JDK for NetIQ are installed.

8 (Optional) The installer displays a warning if the host name of the system is mapped to the IP address 127.0.0.2 in the `/etc/hosts` file:

```
An entry of 127.0.0.2 in the /etc/hosts file affects the Access Manager
functionality. Do you want to proceed with removing it (y/n) [y]
```

Click `Y` to proceed.

The host name mapping to 127.0.0.2 may cause certain Access Manager processes to encounter errors when they attempt to resolve the host name of the machine. To avoid these problems, the 127.0.0.2 entry should be removed from the `/etc/hosts` file.

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

```
Note: The administration server failover will not be enabled until a second
server is added to the cluster.
Is this the primary administration server in a failover group (y/n) ? [y]:
```

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.

10 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: _____

11 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.

NOTE: Administration Console password does not accept special characters colon (:) and double quotes (“).

Record the admin password here: _____

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

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

The following components are installed:

- **Novell Audit Platform Agent:** Responsible for packaging and forwarding the audit log entries to the configured Novell Audit Server. For more information, see “Enabling Auditing” in the *NetIQ Access Manager 3.2 SP2 Administration Console Guide*.
- **Tomcat for NetIQ:** The NetIQ packaging of the Java-based Tomcat Web server used to run servlets and JavaServer Pages (JSP) associated with NetIQ 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 *NetIQ Access Manager 3.2 SP2 Administration Console Guide*.
- **NetIQ 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.
- **NetIQ Identity Server Administration Plug-In:** Works in conjunction with the NetIQ Administration Console to specifically manage the NetIQ Identity Server.

13 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.

14 Continue with Section 3.2, “Configuring the Administration Console Firewall,” on page 48.

3.1.2 Installing on Windows

1 Verify that the machine meets the minimum requirements. See Section 2.4, “Administration Console Requirements,” on page 34.

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 "NetIQ Access Manager Readme" (http://www.novell.com/documentation/beta/novellaccessmanager32/).

5 Read the introduction, then click *Next*.

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

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

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

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

   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 2008) 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 3.2, "Configuring the Administration Console Firewall," on page 48.

3.2 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.

3.2.1 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 ports to open.

   (Conditional) If you are installing the Administration Console, Identity Server or SSL VPN on different machine, list the following additional ports in the *TCP Ports* field:

   - 8080
   - 8443
   - 3080
   - 3443

   (Conditional) If you are installing the Administration Console, Identity Server or SSL VPN on the same machine, list the following additional ports in the *TCP Ports* field:

   - 2080
   - 2443
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
   - 1289
   - 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 "Setting Up Firewalls" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

   NOTE: In Access Manager version 3.2 and later, Admin Console will be accessible on ports 2080 (HTTP) and 2443 (HTTPs) when Identity Server or SSL VPN are installed on the same machine.
5. Click *OK*.
6. Click *Next* > *Accept*.
7. Restart Tomcat by entering `/etc/init.d/novell-ac restart` OR `rcnovell-ac restart`from the Administration Console command line.
8. Continue with Section 3.3, "Logging In to the Administration Console," on page 49.

3.2.2 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
   - 1289
   - 524
   - 636

   For specific information about the ports, see "When a Firewall Separates the Administration Console from a Component" in the *NetIQ Access Manager 3.2 SP2 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 Tomcat7
   net start Tomcat7
   ```
7. Continue with Section 3.3, "Logging In to the Administration Console," on page 49:

3.3 Logging In to the Administration Console

The Administration Console supports the following Web browsers:

- Microsoft Internet Explorer 7.x and later
- Mozilla* Firefox

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.

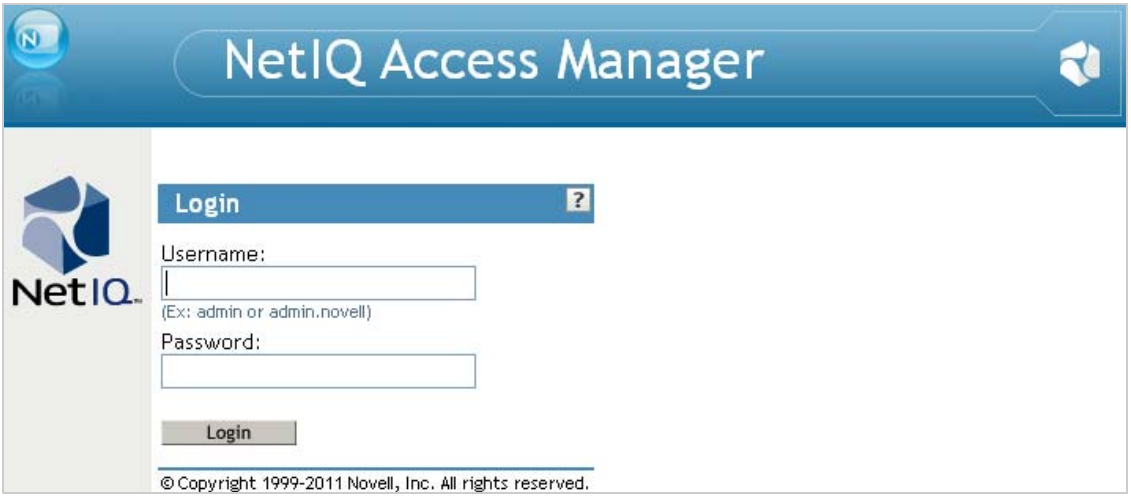
   For information on how to do this, see Section 3.2, "Configuring the Administration Console Firewall," on page 48.

   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 ports `8080` (HTTP) and `8443` (HTTPs) (if it is installed on a separate machine) and ports `2080` (HTTP) and `2443` (HTTPs) (when Identity Server and SSL VPN are installed on the same machine) and the application `/nps`. If the IP address of your Administration Console for example 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*. The following view appears.

For more information about this view or about configuring the Administration Console for the 3.0 view, see "Configuring the Default View" in the *NetIQ Access Manager 3.2 SP2 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 4, "Installing the NetIQ Identity Server," on page 53.
- If your Administration Console machine has multiple interface cards, see Section 3.4, "Enabling the Administration Console for Multiple Network Interface Cards," on page 51.
- To understand the conventions of the Administration Console, see Section 3.5, "Administration Console Conventions," on page 52.

3.4 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: `/opt/novell/nam/adminconsole/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.

3.5 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.

4 Installing the NetIQ Identity Server

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.

4.1 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 43.) However, you must not perform any configuration tasks in the Administration Console during an Identity Server installation.
- If you installed the Administration Console on a separate machine, ensure that the DNS names resolve between the Identity Server and the Administration Console.
- When you are installing the Identity Server on a separate machine (recommended for production environments), you need to ensure that the following ports are open on both the Administration Console and the Identity Server:

  8444
  1443
  1289
  524
  636

  For information on how to open ports, see Section 3.2, “Configuring the Administration Console Firewall,” on page 48.
- 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 because these installations 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 2.5, "Identity Server Requirements," on page 37.
- 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.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see "Preventing Cross-site Scripting Attacks" in the NetIQ Access Manager 3.2 SP2 Identity Server Guide.

4.2 Installing on Linux

1. Open a terminal window.
2. Log in as the `root` user.
3. Access the install script.
   - **3a** Make sure you have downloaded the software or that you have the CD available.

     For software download instructions, see the "NetIQ Access Manager Readme" (http://www.novell.com/documentation/beta/novellaccessmanager32/)
   - **3b** 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>`
   - **3c** Change to `the novell-access-manager-3.2.0-xxx` directory.
4. At the command prompt, run the following install script:

   `./install.sh`
5. When you are prompted to install a product, type `2`, *Install 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.

   NOTE: In Access Manager version 3.2 and later, the Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPs) if the Identity Server or SSL VPN are installed on the same machine.

   The following warning is displayed:

   ```
   Warning: If NAT is present between this machine and Administration Console,
   configure NAT in the Administration Console.
   Exit this installation if NAT is not configured in the Administration Console.
   Would you like to continue (y/n) ?
   ```

   For more information about how to configure NAT, see Section C.1, "Configuring the Administration Console Behind NAT," on page 125.
6. Enter `Y` to proceed.
7. Review and accept the License Agreement.

Specify the following information:

Enter the Primary Admin Console IP Address: Specify the IP address of the primary Administration Console.

Enter the Access Manager Administration User ID: Specify the name of the administration user for the Administration Console.

Enter the Access Manager Administration Password: Specify the password and re-enter the password for the administration user account.

Confirm the password, then wait till 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 4.1, "Prerequisites," on page 53.

Is Local NAT Available for Identity Server: Specify `N` if local NAT is not available for the Access Gateway.

Specify `Y` if the local NAT is available for the Access Gateway. If you specify Y then you need to enter the Local NAT IP address.

8 The following components are installed:

- **NetIQ Access Manager Server Communications:** Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
- **NetIQ Identity Server:** Provides authentication and identity services for the other Access Manager components and third-party service providers.
- **NetIQ 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.
- **NetIQ Access Manager Server Communications Configuration:** Enables the Identity Server to auto-import itself into the Administration Console.

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

9 (Optional) To verify that the Identity Server installation was successful, log in to the Administration Console (see Section 3.3, "Logging In to the Administration Console," on page 49).

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.

10 Continue with one of the following:

- To install an Access Gateway, see Chapter 5, "Installing the Access Gateway Appliance," on page 59 or Chapter 6, "Installing the Access Gateway Service," on page 69.
- To configure the Identity Server, see "Setting Up a Basic Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

4.3 Installing on Windows

1 Verify that the machine meets the minimum requirements. See Section 2.5, "Identity Server Requirements," on page 37.

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 "NetIQ Access Manager Readme" (http://www.novell.com/documentation/beta/novellaccessmanager32/).

6 Read the introduction, then click *Next*.

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

8 Select *Access Manager Identity Provider*, then click *Next*.

A warning is displayed: `If NAT is present between this machine and Administration Console, the NAT configuration needs to be done in Administration Console.`

9 Specify the following information:

Primary Administration Console IP Address: Specify the primary Administration Console IP address.

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.

Local Server IP Address: This field is populated with the local IP address of the system.

10 (Optional) Provide Identity Server Local NAT IP address, if the device is behind NAT.

11 Click *Next*, then review the summary.

12 Click *Install*.

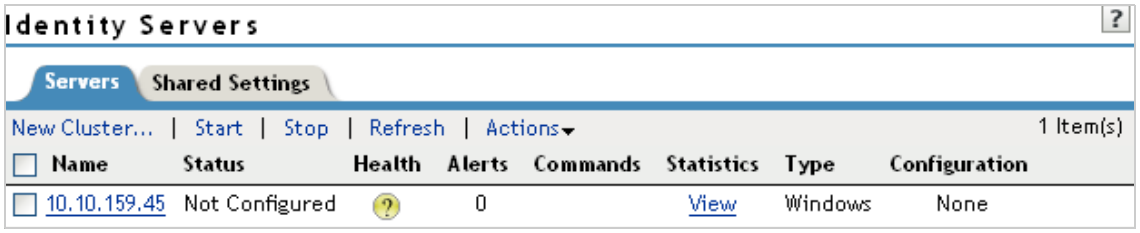
13 (Conditional) If you are installing the Identity Server on a machine that contains a previous installation of the Administration Console, you are asked whether the program should overwrite an existing file in the `\Program Files\Novell` directory. Answer yes to the prompt.

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

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

15 (Optional) To verify that the Identity Server installation was successful, log in to the Administration Console (see Section 3.3, "Logging In to the Administration Console," on page 49).

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.

16 Continue with one of the following:

- To install an Access Gateway, see Chapter 5, "Installing the Access Gateway Appliance," on page 59 or Chapter 6, "Installing the Access Gateway Service," on page 69.
- To configure the Identity Server, see "Setting Up a Basic Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

5 Installing the Access Gateway Appliance

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 Access Gateway Appliance can be installed on all supported hardware platforms for *SUSE Linux Enterprise Server (SLES) 11 SP1 and SP2*.

IMPORTANT: After you have completed installing the Access Gateway Appliance, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities.

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

5.1 Prerequisites for the Access Gateway Appliance

- Ensure that you have backed up all data and software on the disk to another machine. The Access Gateway Appliance installation completely erases all the data on your hard disk.
- Make sure the machine meets the minimum hardware requirements. See Section 2.6, "Access Gateway Requirements," on page 38.
- (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).

5.2 Boot Screen Function Keys

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

- **F1:** Lets you access the context-sensitive help for the currently active screen element of the boot screen.
- **F2:** Lets you select the display language for the installation. However. 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.

5.3 Installing the Access Gateway Appliance

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

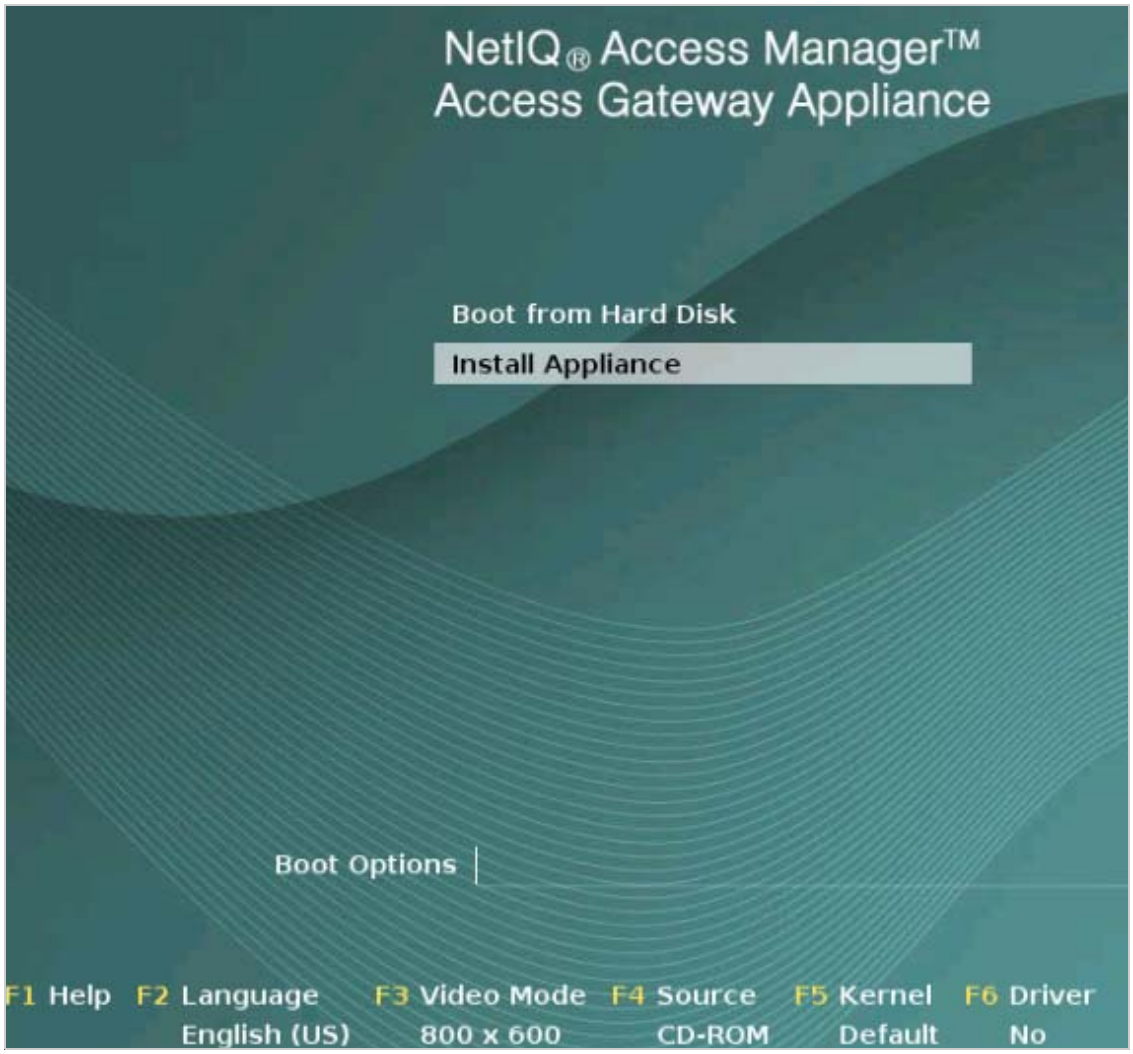
- **boot:** The size is automatically calculated and the mount point is `/boot`.
- **swap:** The size is double the size of the RAM and the mount point is `swap`.

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`.

The 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 and boot from CD. The boot screen appears.

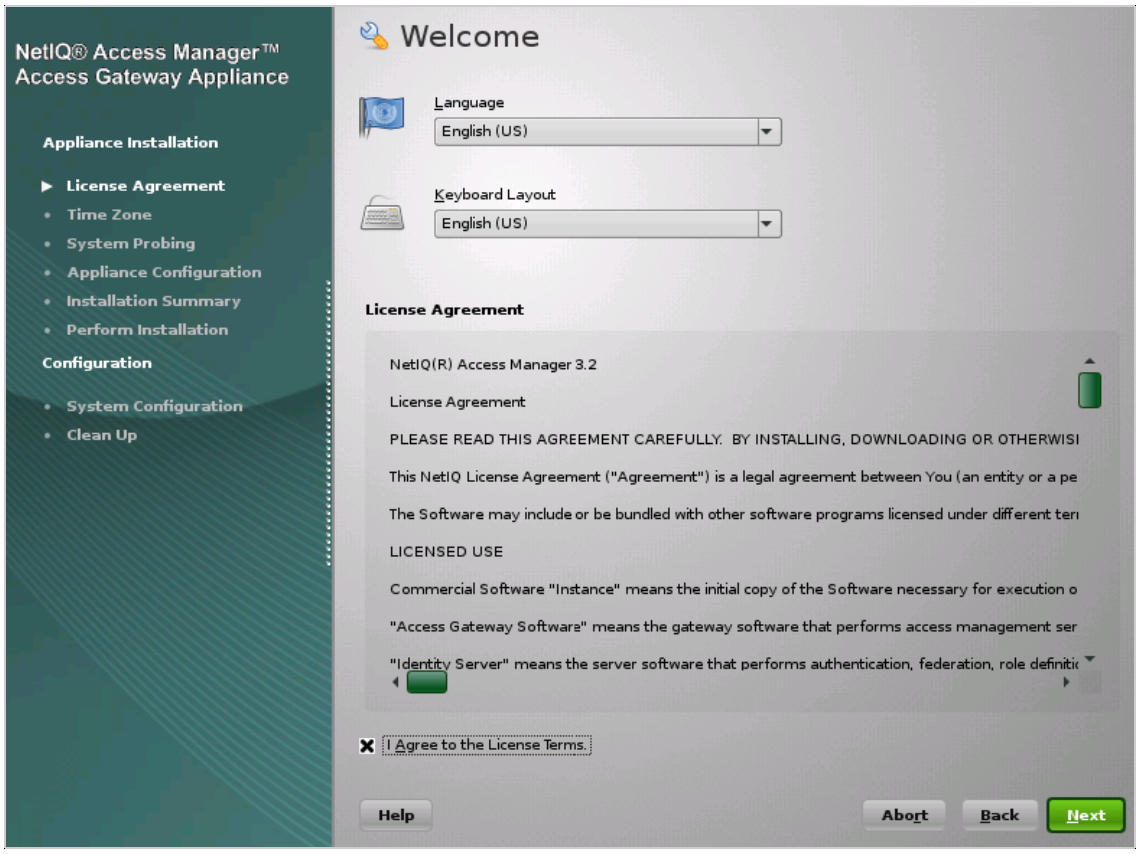


2 By default, the *Boot From Hard Disk* option is selected in the boot screen. Use the Down-arrow key to select *Install Appliance*.

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 5.2, "Boot Screen Function Keys," on page 60.

4 After you have made your installation selections, press Enter.

The License Agreement page is displayed.

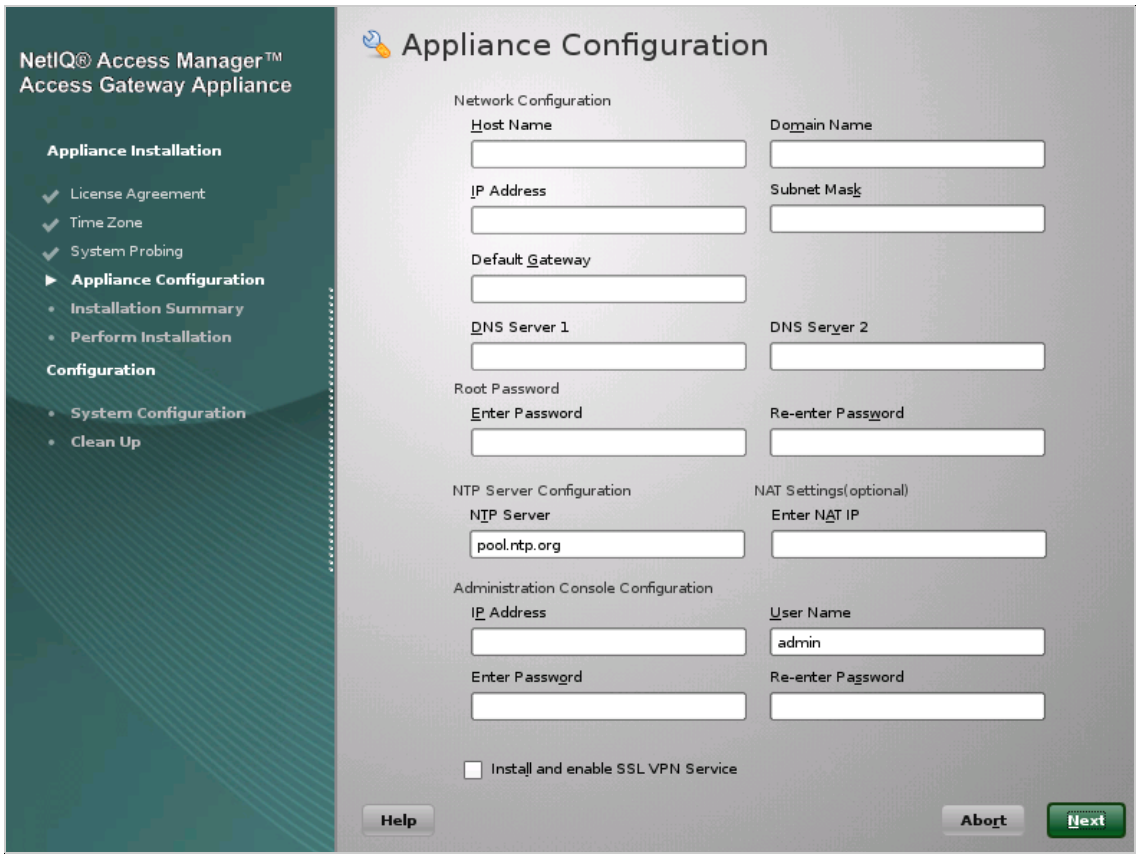


5 Review the agreement on the License Agreement page, then click *I Agree* to accept the agreement. The Clock and Time Zone page is displayed.

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 Access Gateway Appliance machine.

IMPORTANT: Do not use `linux` as the hostname. If you do, the 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 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 NAT Settings section:

Enter NAT IP: (optional) Provide Access Gateway Local NAT IP Address, if the device is behind NAT.

Specify the following in the Administration Console configuration section:

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

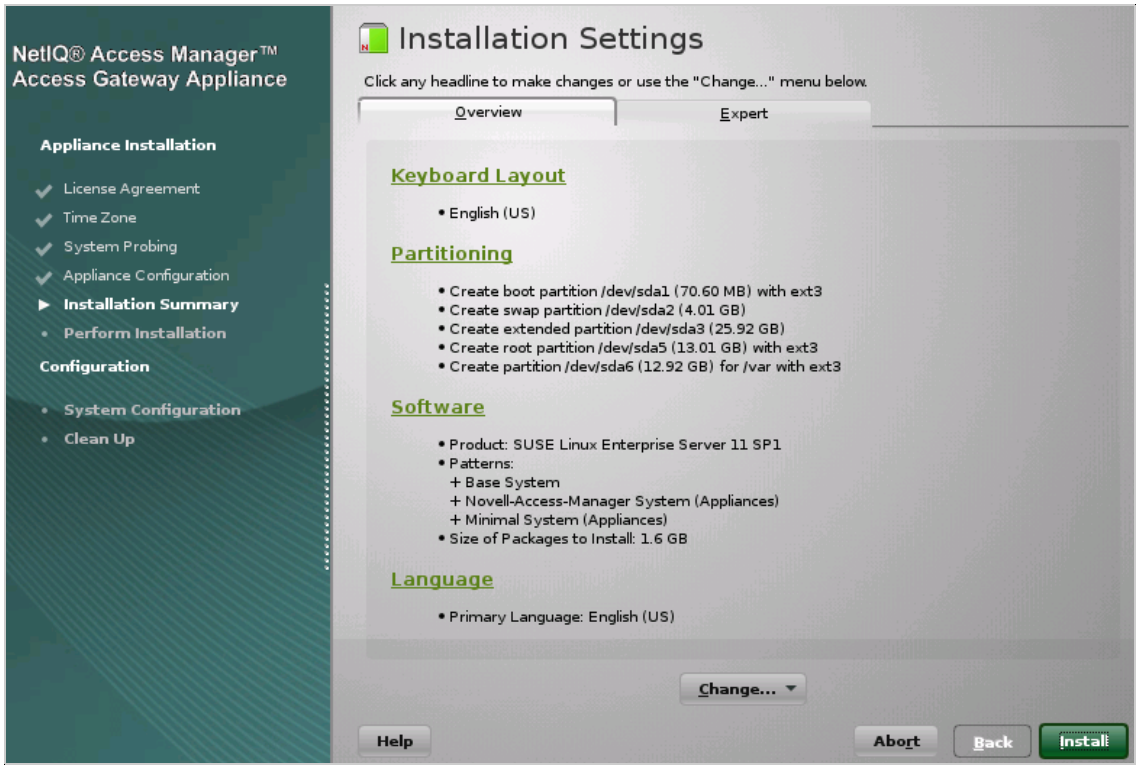
Re-enter Password: Specify the password again for verification.

Install and enable SSL VPN Service: Select this check box to install and configure the SSL VPN service on the 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 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. Ensure that all the default partitions recommended adhere to the guidelines mentioned in Table 5-1 on page 66.

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 5.4, “Creating Custom Partitions,” on page 66.

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 Access Gateway Appliance is imported to the Administration Console.

14 (Optional) To verify the installation of the Access Gateway Appliance, log in to the Administration Console (see Section 3.3, “Logging In to the Administration Console,” on page 49), 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.6, “Troubleshooting the Access Gateway Import,” on page 111.

15 Continue with one of the following sections:

- “Setting Up a Basic Access Manager Configuration” in the *NetIQ Access Manager 3.2 SP2 Setup Guide*
- Section 5.5, “Viewing the Installation Log,” on page 67

5.4 Creating Custom Partitions

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

Table 5-1 *Access Gateway Appliance Partitions*

Partition Type	Requirements
root	This partition contains the boot files, the system files, and the log files. You should assign 40% of available disk space to this partition. We recommend that the space should be more than 40 GB.
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 used for log files and caching objects of Access Gateway. Allocate the remaining space for this partition which should be more than 50 GB. Assign the remaining disk space to var.

To create your custom partitions:

1. From the Installation Settings page, click *Change*, then select *Partitioning*. (See Step 11 on page 65.)

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

8 In the installation Summary page, verify that the partitions you specified are listed, then continue with Step 12 on page 65.

5.5 Viewing the Installation Log

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

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

The log has the following format:

```
'component/module name' 'date' 'time'
```

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

6 Installing the Access Gateway Service

Installation time: about 10 minutes.

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

6.1 Prerequisites

- An Administration Console must be installed before you can install the Access Gateway Service. See “Installing the Access Manager Administration Console” on page 43.
- An Identity Server must be installed and configured before installing the Access Gateway Service. See, Chapter 4, “Installing the NetIQ Identity Server,” on page 53.
- The Access Gateway Service must be installed on a separate machine.
- Verify that the machine meets the minimum requirements. See Section 2.6, “Access Gateway Requirements,” on page 38.
- 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 *NetIQ Access Manager 3.2 SP2 Setup Guide*.
- 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.
- The Access Gateway Service clustering is supported for devices that are on the same operating system.

6.2 Installing the Access Gateway Service on Linux

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 "NetIQ Access Manager 3.2 Readme".
3. Prepare your machine for installation:

   Make your operating system installation media available.

   The installation program checks for Apache dependencies and installs any missing packages.
4. Start the installation program by using the following command:

   ```
   ./ag_install.sh
   ```
5. Review and accept the License Agreement.
6. (Only for RHEL). If you have not installed the dependent rpms mentioned in the prerequisites, you may get an error message. Ensure that you have installed the required rpms.

   See Section 2.6.2, "Access Gateway Service Requirements," on page 39.
7. Specify the following information:

   Is Local NAT Available for Access Gateway: Specify `N` if local NAT is not available for the Access Gateway.

   Specify `Y` if the local NAT is available for the Access Gateway. If you specify Y then you need to enter the Local NAT IP address

   Enter the Primary Admin Console IP Address: Specify the IP address of the primary Administration Console.

   Enter the Access Manager Administration User ID: Specify the name of the administration user for the Administration Console.

   Enter the Access Manager Administration Password: Specify the password and re-enter the password for the administration user account.
8. After installation is complete, you will see the following message:

   ```
   Installation is complete
   ```
9. You can review the log files here: `/tmp/novell_access_manager/`.

   These logs are all dated and time-stamped.
10. To verify that the Access Gateway Service imported into the Administration Console, wait for few minutes, log into the Administration Console, then click *Devices* > *Access Gateways*.

    At this point, the Access Gateway Service is in an unconfigured state.
11. Continue with the one of the following:
    - "Setting Up a Basic Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*
    - Install another Access Manager component.

6.3 Installing the Access Gateway Service on Windows

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 "NetIQ Access Manager 3.2 Readme".
3. Disable any virus scanning programs.
4. 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. Start the installation program by double clicking the executable file.

   A warning is displayed stating `If NAT is present between console, the NAT configuration needs to be done in Administration Console.`

   If NAT is configured then make sure that you configure the same in the Administration Console. Else, click *Continue* to proceed
6. On the Welcome page, click *Next*.
7. Review the readme, and click *Next*.
8. Review and accept the License Agreement, then click *Next*.
9. Specify the following information:

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

   Administration Console Login 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.

   Access Gateway 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 for communication with the Administration Console.
10. (Optional) Provide Access Gateway Local NAT IP address, if the device is behind NAT.
11. Click *Next*.
12. Configure disk cache. This holds the caching objects of the Access Gateway.

    NOTE: From 3.2 onwards, Access Gateway Appliance uses the filesystem provided by Apache mod_cache module for storing the caching objects. If you want to change the size of this cache after installation see TID on Changing the Cache Size of an Access Gateway Appliance after Installation. (http://www.novell.com/support/kb/doc.php?id=7011374).

    ---
13. Click *Next*, then review the installation summary.
14. To start the installation, click *Install*.
15. Review the log information at the following location:

    ```
    C:\Program Files\Novell\log
    ```
16. Click *Next*, then click *Done*.

17 To verify that the Access Gateway Service imported into the Administration Console, wait few 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 one of the following:

   - "Setting Up a Basic Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*
   - Install another Access Manager component.

7 Installing the SSL VPN Server

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 NetIQ 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.

7.1 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 NetIQ SSL VPN. This deployment requires the Administration Console and the Identity Server to be installed before the SSL VPN server is installed.

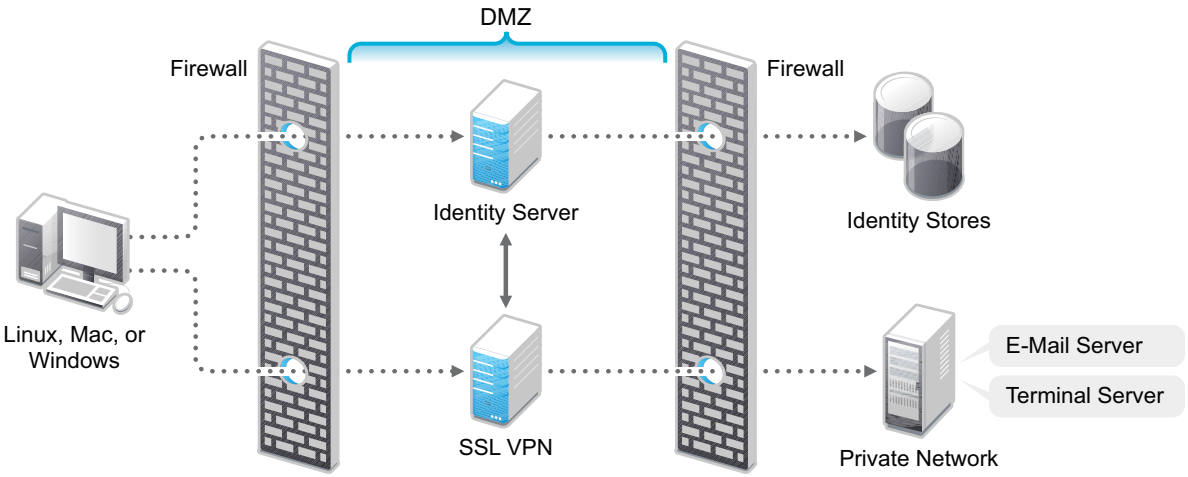
7.1.1 Deployment Scenarios

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 76. In this scenario, SSL VPN will be accessible on port 8443. When it is accessed on port 8080 it will be redirected to port 8443.

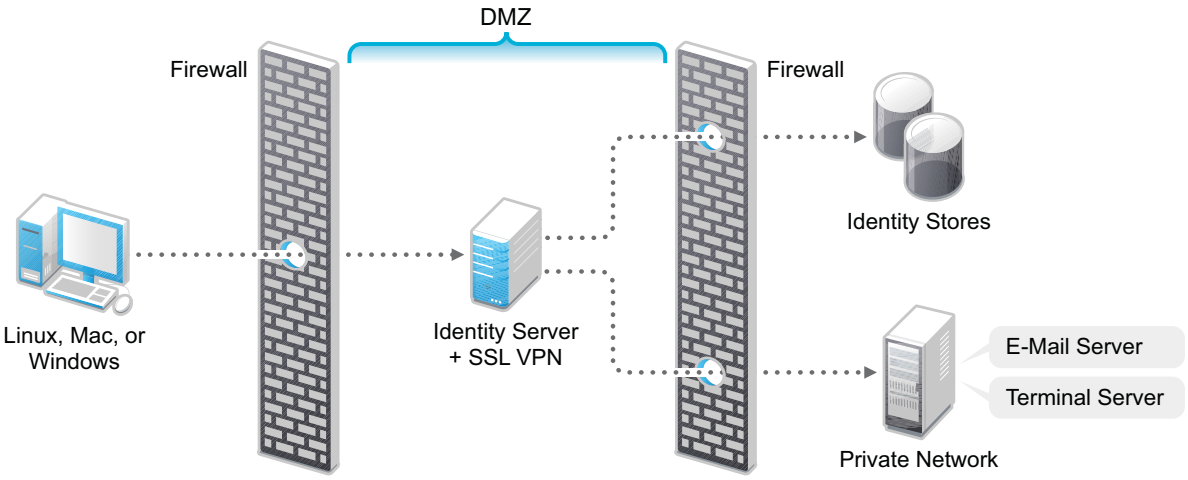
Figure 7-1 *Deployment Scenario 1*



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 76. In this scenario, SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

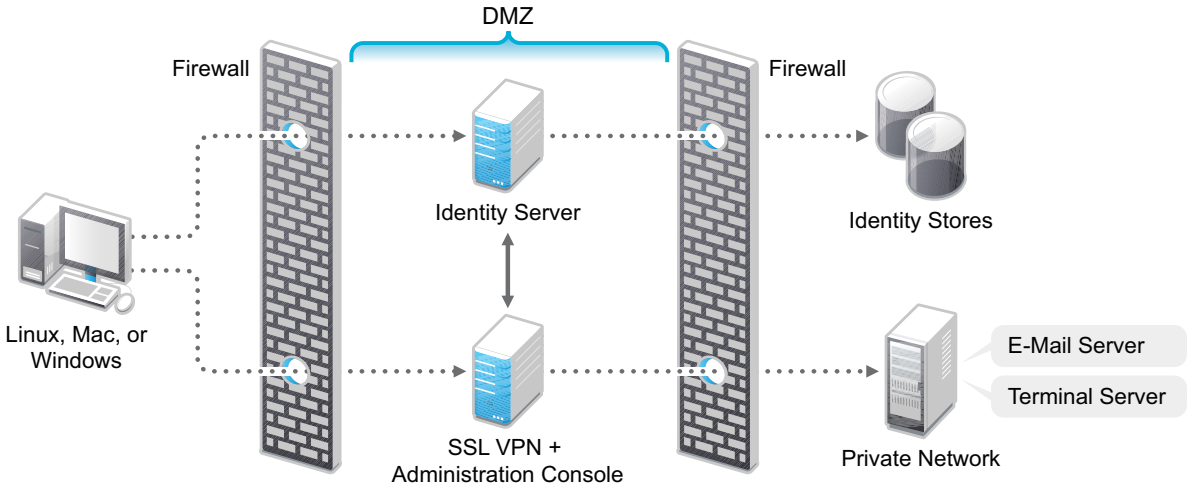
Figure 7-2 *Deployment Scenario 2*



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 Access Gateway and the Identity servers are deployed separately. For installation instructions for this scenario, see "Installing the ESP-Enabled SSL VPN" on page 76. In this scenario, SSL VPN will be accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

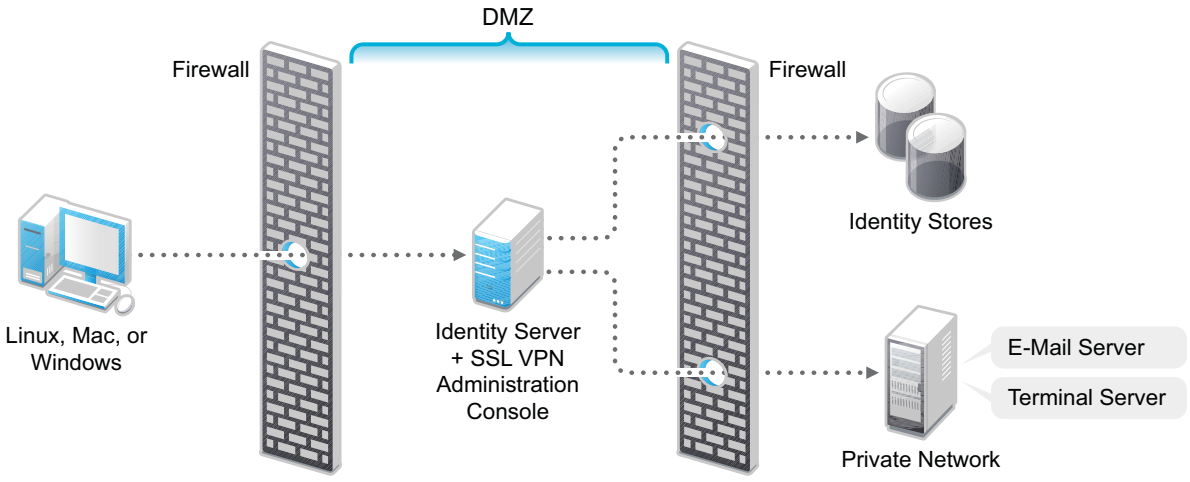
Figure 7-3 *Deployment Scenario 3*



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 Access Gateway is deployed separately. For installation instructions for this scenario, see "Installing the ESP-Enabled SSL VPN" on page 76. In this scenario SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

Figure 7-4 *Deployment Scenario 4*



7.1.2 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 73.

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 "NetIQ Access Manager Readme" (https://www.netiq.com/documentation/novellaccessmanager32/readme/data/accessmanager32_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-3.2-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.

The following warning is displayed:

```
An entry of 127.0.0.2 in the /etc/hosts file affects the Access Manager
functionality. Do you want to proceed with removing it (y/n)
```

5 Enter `Y` to proceed.

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 following details:

Enter the Primary Admin Console IP address: Specify the IP address of the primary Administration console.

Enter the Access Manager Administration user ID: Specify the name of the administrator for the Administration Console.

Enter the Access Manager Administration password Specify the administration password and confirm it by re-entering.

Select the IP address used for the NetIQ Access Manager Server Communications Local Listener. Choose your server IP address from the list of addresses. Select an address, type a new address, or press Enter to accept the default.

Select the IP address used for the SSL VPN listening IP address. Choose your server IP address from the list of addresses found. Select an address, type a new address, or press Enter to accept the default.

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

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

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

10 To verify the installation of the SSL VPN, continue with Section 7.4, "Verifying That Your SSL VPN Service Is Installed," on page 84.

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

12 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 7.3, "Installing the Key for the High-Bandwidth SSL VPN," on page 83.

7.2 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 Access Gateway Appliance, with the Identity Server, with the Administration Console, or on a separate machine.

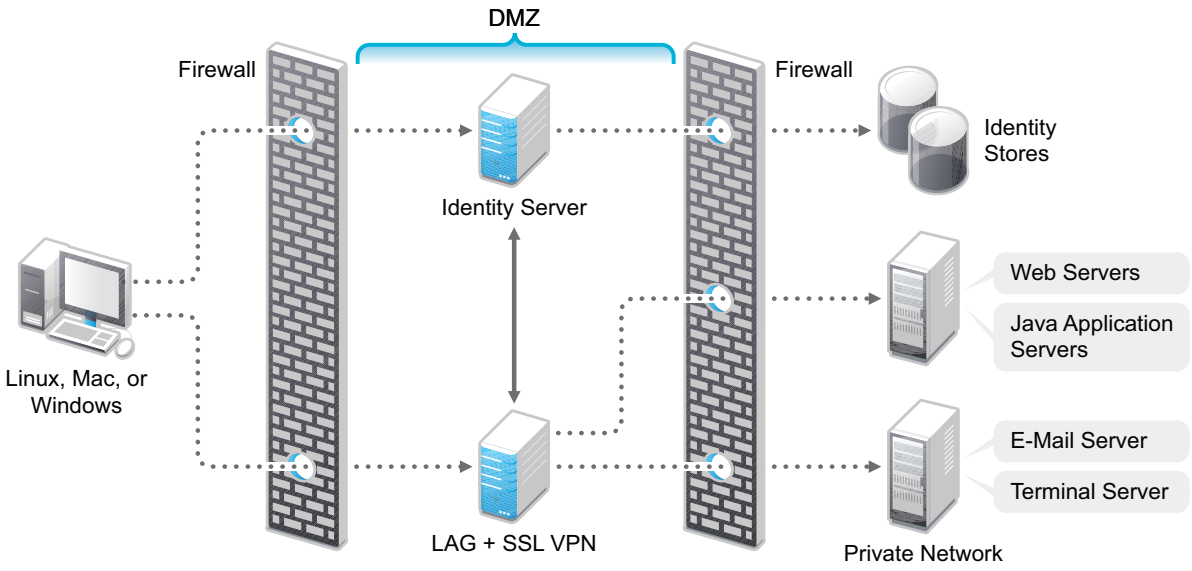
7.2.1 Deployment Scenarios

The traditional SSL VPN server supports the following installation scenarios:

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

This deployment scenario consists of a demilitarized zone where 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 Access Gateway Appliance" on page 81. In this scenario, SSL VPN will be accessible on port 8443. When it is accessed on port 8080 it will be redirected to port 8443.

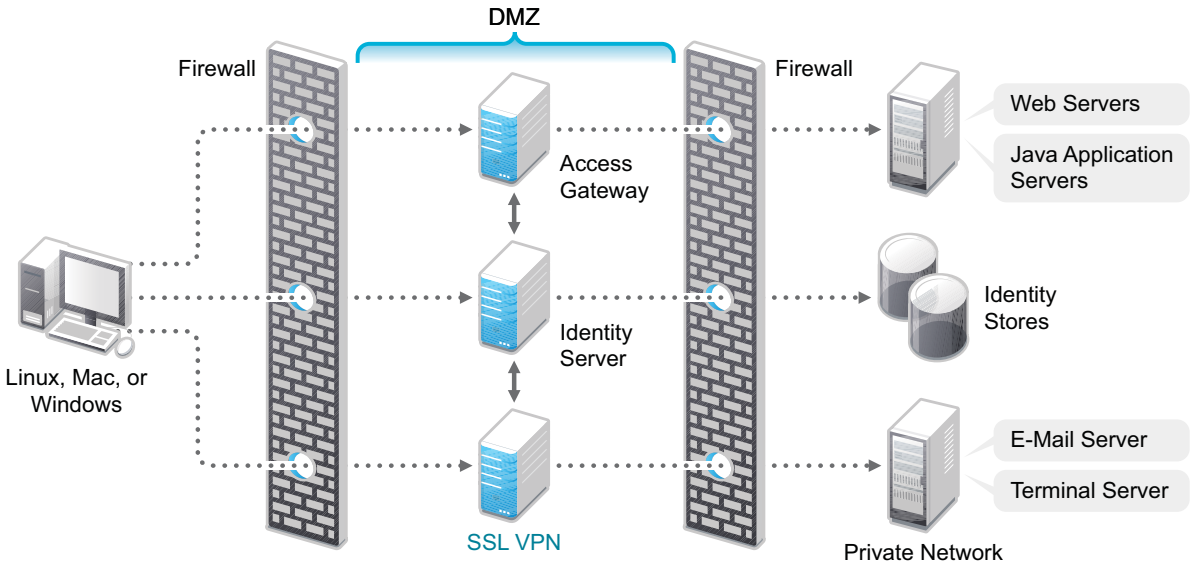
Figure 7-5 *Deployment Scenario 1*



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

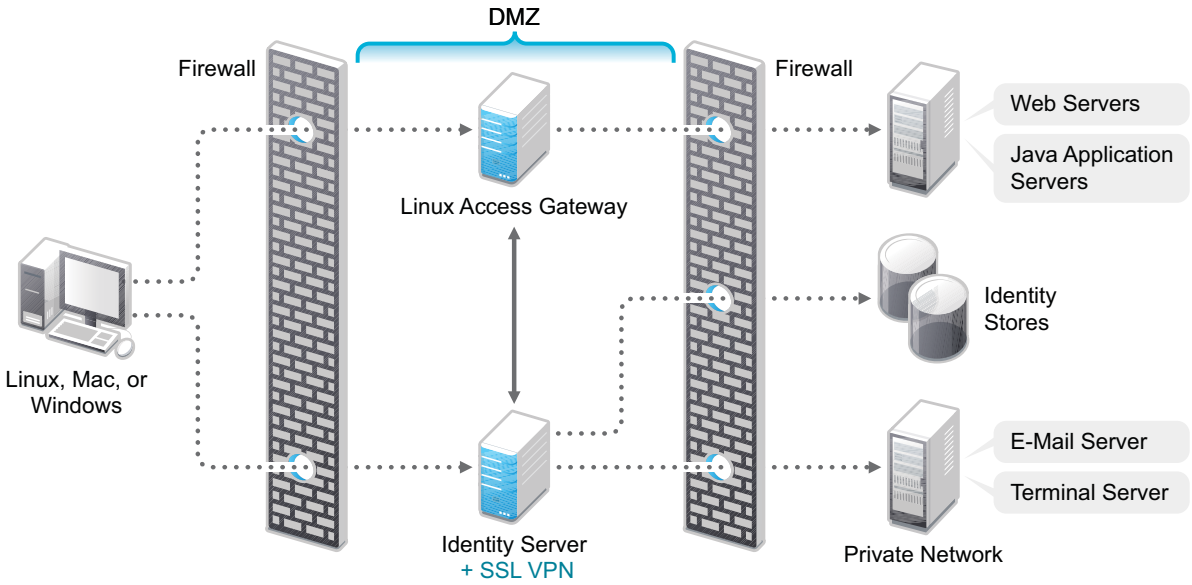
This deployment scenario consists of a demilitarized zone where the Access Gateway, Identity Server, and SSL VPN are deployed separately. For installation instructions for this scenario, see "Installing the Traditional NetIQ SSL VPN" on page 81. In this scenario, SSL VPN will be accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

Figure 7-6 *Deployment Scenario 2*



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

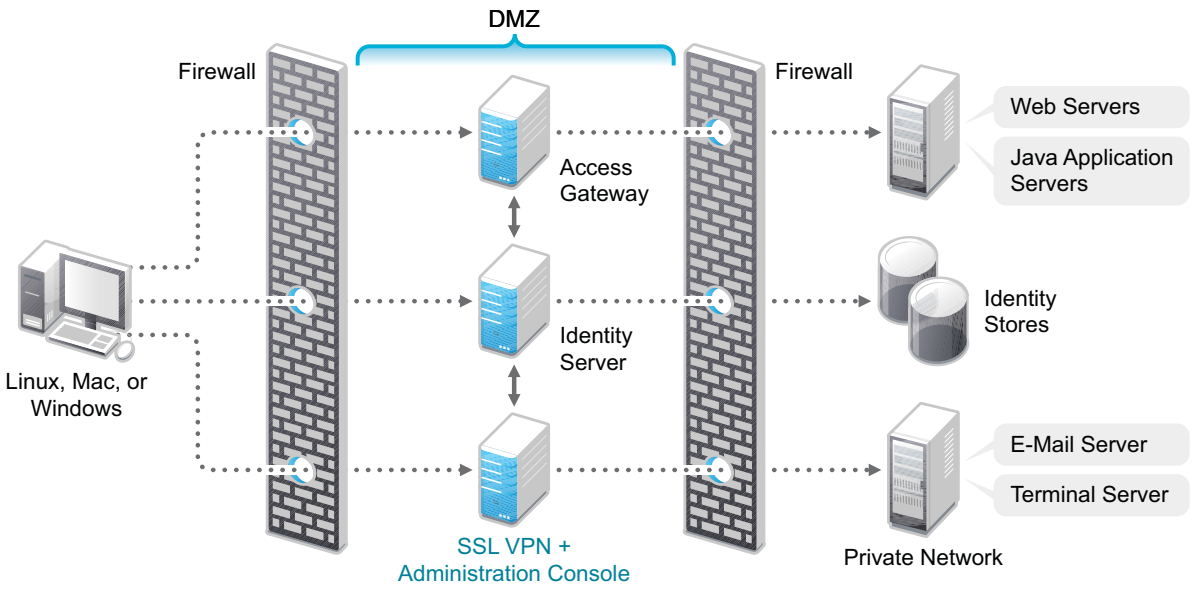
This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions for this scenario, see "Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console" on page 82. In this scenario, SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.



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 82. In this scenario SSL VPN will be accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

Figure 7-7 *Deployment Scenario 4*

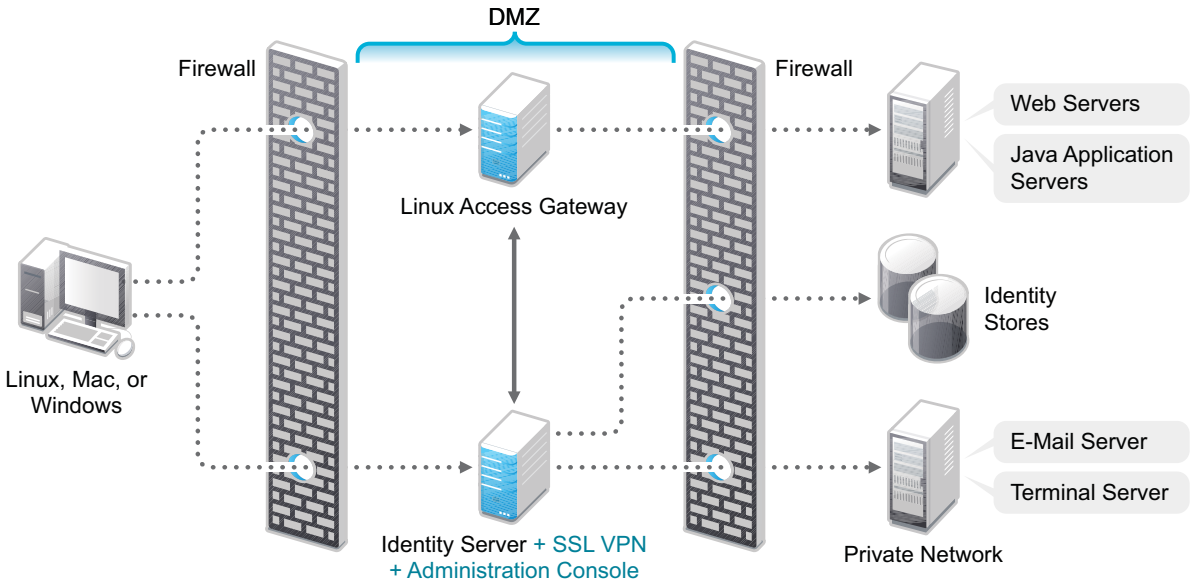


Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server

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 82.

In this scenario SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

Figure 7-8 *Deployment Scenario 5*



7.2.2 Installing the Traditional NetIQ SSL VPN

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

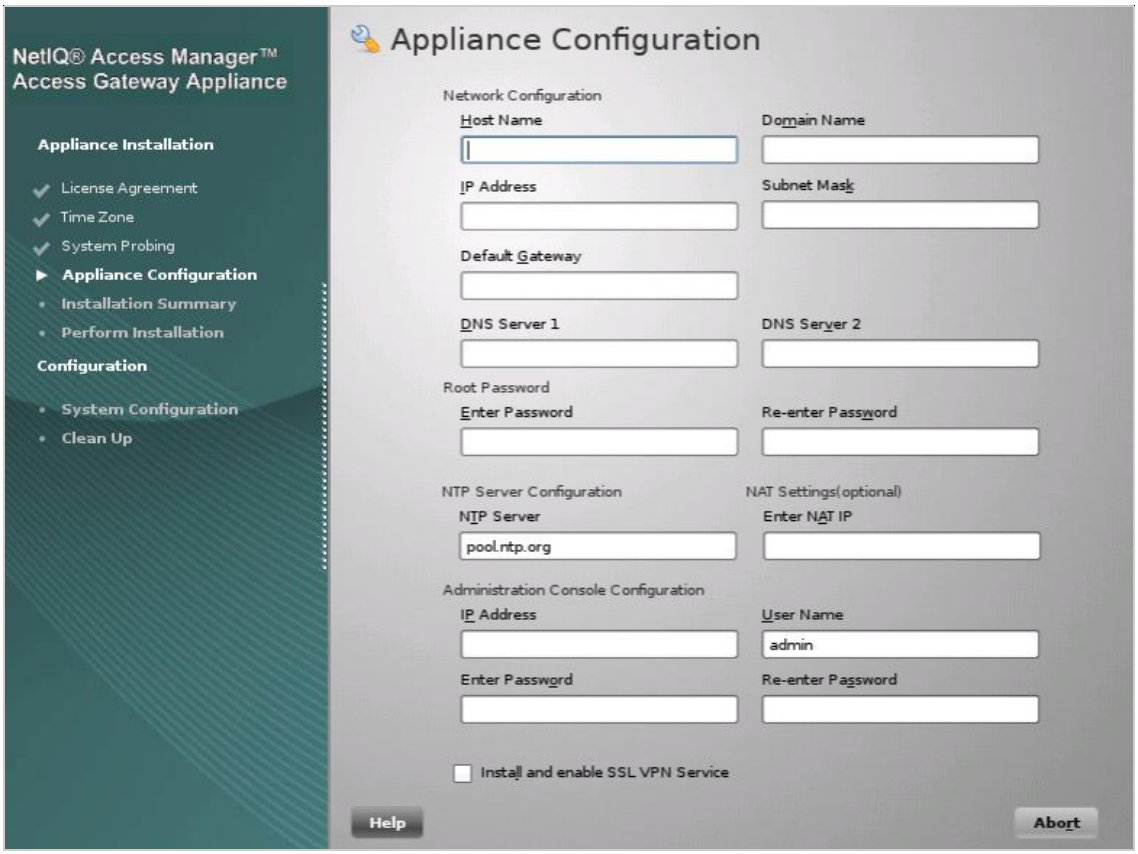
- "Installing SSL VPN with Access Gateway Appliance" on page 81
- "Installing SSL VPN on a Separate Machine, with the Identity Server, or with the Administration Console" on page 82

Installing SSL VPN with Access Gateway Appliance

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

For more information on installing Access Gateway, refer to "Section 5.3, "Installing the Access Gateway Appliance," on page 60" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1. Start the installation of Access Gateway. For details, refer to "Section 5.3, "Installing the Access Gateway Appliance," on page 60" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.
2. In the Access Administrator Configuration section in the NetIQ Access Gateway Configuration page, select the *Install and Enable SSL VPN Server* check box to install and configure SSL VPN on Access Gateway.



3 Follow the on-screen instructions to continue with the Access Gateway installation.

4 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 7.3, "Installing the Key for the High-Bandwidth SSL VPN," on page 83.

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 NetIQ 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 "NetIQ Access Manager 3.2 Readme".

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-3.2-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 Review and accept the License Agreement.

5 (Optional) If the SSL VPN is not installed on same machine as the Administration Console, specify the IP address of the Administration Console.

6 (Optional) This warning is displayed if an entry of 127.0.0.2 is found in the /etc/hosts file.

```
Warning: An entry of 127.0.0.2 in the /etc/hosts file affects the Access
Managerfunctionality.Doyouwanttoproceedwithremovingit(y/n)[y]?
```

Enter `Y` to proceed.

7 Specify the following details:

Access Manager Administration User ID: The name of the administrator for the Administration Console.

Access Manager Administration Password Specify the administration password.

Confirm the password.

IP address Used for the SSL VPN Listening IP Address: Select an address, type a new address, or press Enter to accept the default.

The following warning is displayed:

```
WARNING!! In 3.2 and later, SSL VPN will be accessible on ports 3080 (HTTP) and
3443 (HTTPs) when it is installed on the same machine as that of Identity
Server.
```

8 (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.

9 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.`

10 To verify the installation of the SSL VPN, continue with Section 7.4, "Verifying That Your SSL VPN Service Is Installed," on page 84.

11 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with Section 7.3, "Installing the Key for the High-Bandwidth SSL VPN," on page 83

7.3 Installing the Key for the High-Bandwidth SSL VPN

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-3.2-0.noarch.rpm`

3 Log in as `root`.

4 Enter the following command to stop all services:

`/etc/init.d/novell-sslvpn stop` OR `rcnovell-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-3.2.0-0.noarch.rpm`

6 Enter the following command to restart all SSL VPN services:

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

7 Enter the following command to check the status:

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

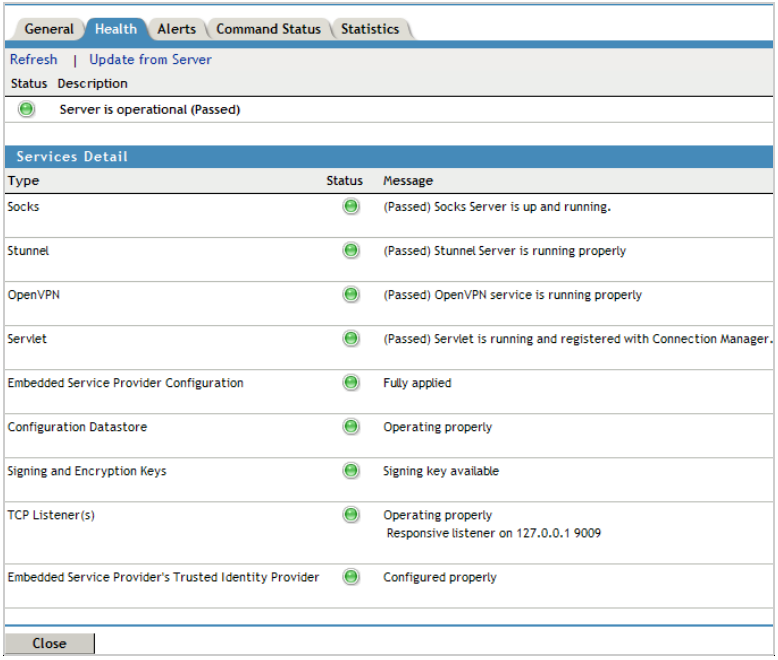
7.4 Verifying That Your SSL VPN Service Is Installed

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 NetIQ SSL VPN" in the *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*

3 (Optional) Continue with "Basic Configuration for SSL VPN" in the *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*, if you have not already configured the SSL VPN server.

8 Uninstalling Components

This section discusses the following topics related to installation:

8.1 Uninstalling the Identity Server

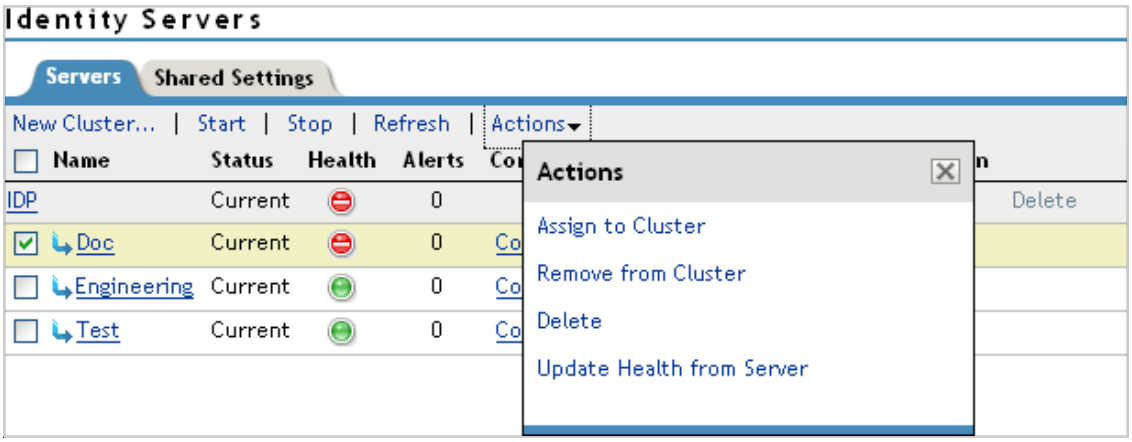
Uninstalling the NetIQ Identity Server is a two-step process:

1. Removing the Identity Server from the Administration Console. See Section 8.1.1, "Deleting Identity Server References," on page 85.
2. Removing the Identity Server software from the Linux or Windows machine. See Section 8.1.2, "Uninstalling the Linux Identity Server," on page 86 or Section 8.1.3, "Uninstalling the Windows Identity Server," on page 86.

8.1.1 Deleting Identity Server References

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

1. In the Administration Console, click *Devices* > *Identity Servers*.
2. Select the Identity Server that you want uninstalled, then click *Stop*.
3. Wait for its health to turn red, then select the server and click *Actions* > *Remove from Cluster*.



4 Update the cluster configuration.

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

6 Continue with Section 8.1.2, "Uninstalling the Linux Identity Server," on page 86 or Section 8.1.3, "Uninstalling the Windows Identity Server," on page 86.

8.1.2 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.

8.1.3 Uninstalling the Windows Identity Server

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

1 Exit any applications and disable any virus scanning programs.

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

3 Read the introduction, then click *Next*.

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

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

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

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

6 (Conditional) If you selected to uninstall specific features, select 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.9, "Troubleshooting the Uninstall of the Windows Identity Server," on page 115.

7 (Conditional) If the Administration Console was installed with the Identity Server and you selected only to uninstall the Identity Server, reboot the machine.

8.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall the Identity Server (see Chapter 4, "Installing the NetIQ Identity Server," on page 53) and leave the Identity Server configuration intact in the Administration Console. In order to preserve the existing keystores, perform the following steps before installing the Identity Server on the new hard drive.

1 Stop the server.

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

2 Select the server, then click *Actions* > *Remove from configuration*.

3 Select the server, then click *Actions* > *Delete*.

4 Reinstall the Identity Server. (See Chapter 4, "Installing the NetIQ Identity Server," on page 53.)

5 On the Identity Servers page, select the server, then click *Actions* > *Assign to Cluster*.

6 Select the Identity Server cluster configuration, then click *Assign*.

7 Click *OK*.

8.3 Uninstalling the Access Gateway

1 In the Administration Console, click *Access Gateways*.

2 If the Access Gateway belongs to a cluster, you need to remove it from the cluster.

2a Select the Access Gateway, then click *Actions* > *Remove from Cluster*:

2b Confirm the action, then click *OK*.

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 *NetIQ Access Manager 3.2 SP2 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 8.3.1, "Uninstalling the Windows Access Gateway Service," on page 88.
- If you are uninstalling the Linux Access Gateway Service, continue with Section 8.3.2, "Uninstalling the Linux Access Gateway Service," on page 88.

8.3.1 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.8, "Troubleshooting the Uninstall of the Access Gateway Service," on page 115.

8.3.2 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.8, "Troubleshooting the Uninstall of the Access Gateway Service," on page 115.

8.4 Uninstalling the Administration Console

Only the primary version of the Administration Console contains the certificate authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You need to promote a secondary console to be the primary console. See "Installing Secondary Versions of the Administration Console" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

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

Select the process that corresponds to your platform:

- Section 8.4.1, "Uninstalling the Linux Administration Console," on page 88
- Section 8.4.2, "Uninstalling the Windows Administration Console," on page 89

8.4.1 Uninstalling the Linux Administration Console

1. Insert CD 1 into the drive.
2. Log in as the `root` user or equivalent.
3. At the command prompt of the Access Manager directory, enter the following:

```
./uninstall.sh
```

4 Select one of the following options:

Option	Description
1	NetIQ Access Manager Administration
2	NetIQ Identity Server
3	Traditional NetIQ SSL VPN Server
4	ESP-enabled NetIQ 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

5 After running the `./uninstall.sh` script, go to *Auditing* > *Troubleshooting* > *Other Known Device Manager Servers*, then remove the entry for this secondary Administration Console from the servers list.

8.4.2 Uninstalling the Windows Administration Console

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

1 Exit any applications and 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.9, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 115.

8.5 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.

8.5.1 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 8.5.2, "Uninstalling the SSL VPN Server," on page 90 to uninstall the SSL VPN server.

8.5.2 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 8.5.3, "Uninstalling the RPM Key for High Bandwidth SSL VPN," on page 90.

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 NetIQ SSL VPN.
   - Enter 5 to uninstall the ESP-enabled NetIQ SSL VPN.

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

8.5.3 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
   ```

9 Upgrading Access Manager Components

WARNING: Before upgrading, make a backup of your configuration. For instructions, see "Backing Up the Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP2 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 NetIQ 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.

9.1 Upgrading on Linux

9.1.1 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 NetIQ Customer Center and follow the link that allows you to download the product. Then use the following sections for instructions on upgrading the components:

Upgrading the Administration Console

If the Identity Server and SSL VPN are installed on the same machine as the Administration Console, the Identity Server and SSL VPN are automatically upgraded with the Administration Console.

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5. The system displays the confirmation message along with the list of installed components. For example, if the Administration Console and Identity Server are installed on the same machine, the following message is displayed:

   ```
   The following components were installed on this machine

   1. Access Manager Administration Console
   2. Identity Server
   Do you want to upgrade the above components (y/n)?
   ```

6. Type *Y* and press Enter.
7. Enter the Access Manager Administration Console user ID.
8. Enter the Access Manager Administration Console password.
9. Re-enter the password for verification.
10. The system displays the following message when the upgrade is complete:

    ```
    Successfully upgraded.
    ```

    The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

If you encounter an error, see "Troubleshooting a Linux Administration Console Upgrade" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

Upgrading the Identity Server

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 "Upgrading the Administration Console" on page 94.

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5 The system displays the following confirmation message:

```
The following components were installed on this machine

1. Identity Server

Do you want to upgrade the above components (y/n)?
```

6 Type *Y* and press Enter.

7 Enter the Access Manager Administration Console user ID.

8 Enter the Access Manager Administration Console password

9 Re-enter the password for verification

10 The system displays the following message when the upgrade is complete:

```
Successfully upgraded.
```

The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

Upgrading the Access Gateway Appliance

1 Open a terminal window.

2 Log in as the `root` user.

3 Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

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

```
./ma_upgrade.sh
```

5 Enter the Access Manager Administration Console user ID.

6 Enter the Access Manager Administration Console password

7 Re-enter the password for verification

NOTE: For upgrading the Access Gateway Service, see "Upgrading the 3.1 SP4 Access Gateway Service "in the *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*.

The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

Upgrading the SSL VPN

If you have installed both the SSL VPN and the Administration Console on the same machine, see "Upgrading the Administration Console" on page 94.

1 Open a terminal window.

2 Log in as the `root` user.

3 Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

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

```
./upgrade.sh
```

5 The system displays the following confirmation message:

```
Do you want to upgrade the above components (y/n)?
```

6 Type *Y* and press Enter.

7 Enter the Access Manager Administration Console user ID.

8 Enter the Access Manager Administration Console password

9 Re-enter the password for verification

10 The system displays the following message when the upgrade is complete:

```
Successfully upgraded.
```

The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

9.1.2 Upgrading from Access Manager 3.2, 3.2 SP1, and 3.2 SP1 IR1a to 3.2 SP2

You must be on Access Manager 3.2 to upgrade to a higher version. For upgrading, you need to upgrade the components in the following order:

- "Upgrading the Administration Console" on page 94
- "Upgrading the Identity Server" on page 95
- "Upgrading the Access Gateway Appliance" on page 97
- "Upgrading the SSL VPN" on page 98

IMPORTANT: The J2EE agents upgrade is not supported.

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

- Ensure that you are on Access Manager 3.2 or a higher version.
- You must backup the files that you have customized.

Upgrading the Administration Console

If the Identity Server and SSL VPN are installed on the same machine as the Administration Console, the Identity Server and SSL VPN are automatically upgraded with the Administration Console.

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.

1 Back up any customized JSP pages and related files.

Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.

```
/var/opt/novell/tomcat7/webapps/nidp/jsp
```

2 Open a terminal window.

3 Log in as the `root` user.

4 Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

5 (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/tomcat7/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.

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

```
./upgrade.sh
```

7 The system displays the confirmation message along with the list of installed components. For example, if the Administration Console and Identity Server are installed on the same machine, the following message is displayed:

```
The following components were installed on this machine

1. Access Manager Administration Console
2. Identity Server
Do you want to upgrade the above components (y/n)?
```

8 Type *Y* to upgrade. A Warning message regarding backup and restore of JSP files is displayed.

9 Type *Y* to continue with the upgrade, then press Enter.

10 Type *Y* to restore the custom login pages.

11 Enter the Access Manager Administration Console user ID.

12 Enter the Access Manager Administration Console password.

13 Re-enter the password for verification.

14 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

15 (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 "Troubleshooting a Linux Administration Console Upgrade" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

Upgrading the Identity Server

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 "Upgrading the Administration Console" on page 94.

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.

1. Back up any customized JSP pages and related files.

   Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.
2. Open a terminal window.
3. Log in as the `root` user.
4. Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.
5. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```
6. The system displays the following confirmation message:

   ```
   The following components were installed on this machine

   1. Identity Server

   Do you want to upgrade the above components (y/n)?
   ```
7. Type *Y* and press Enter. A Warning message regarding backup and restore is displayed.
8. Would you like to continue this upgrade? Type *Y* to upgrade.
9. The system displays the following message:

   ```
   If old jsp pages need to be restored, ensure that you sanitize them to prevent
   possible Cross-site Scripting attacks. You can sanitize jsp pages after
   restoring them. Do you want to restore custom login pages? (y/n):
   ```

   Type *Y* to restore.
10. Enter the Access Manager Administration Console user ID.
11. Enter the Access Manager Administration Console password
12. Re-enter the password for verification
13. The system displays the following message when the upgrade is complete:

    ```
    Upgrade completed successfully.
    ```
14. Restore any customized files from the backup taken earlier. To restore files, copy files to the respective locations:
    - `/opt/novell/nam/idp/webapps/nidp/jsp`
    - `/opt/novell/nam/idp/webapps/nidp/html`
    - `/opt/novell/nam/idp/webapps/nidp/images`
    - `/opt/novell/nam/idp/webapps/nidp/config`
    - `/opt/novell/nam/idp/webapps/nidp/WEBINF/lib`

- /opt/novell/nam/idp/webapps/nidp/WEBINF/web.xml
- /opt/novell/nam/idp/webapps/nidp/WEBINF/classes
- /opt/novell/nam/idp/webapps/nidp/WEBINF/conf
- /opt/novell/java/jre/lib/security/bcslogin.conf
- /opt/novell/java/jre/lib/security/nidpkey.keytab
- /opt/novell/nam/idp/webapps/nidp/classUtils
- /opt/novell/nam/idp/conf/server.xml
- /opt/novell/nam/idp/conf/tomcat7.conf

Upgrading the Access Gateway Appliance

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/tomcat7/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 SSL VPN User Interface" in the *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*.

1. Back up any customized JSP pages and related files.

   Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.
2. Open a terminal window.
3. Log in as the `root` user.
4. Download the upgrade file from Patches and Security (http://support.novell.com/patches.html) and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.
5. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./ma_upgrade.sh
   ```
6. A Warning message regarding backup and restore is displayed. If you have customized any files, take a backup and restore them after installation.
7. Would you like to continue this upgrade? Type *Y* to continue.
8. Do you want to restore custom login pages? Type *Y* to confirm.
9. Enter the Access Manager Administration Console user ID.
10. Enter the Access Manager Administration Console password
11. Re-enter the password for verification

NOTE: For upgrading the Access Gateway Service, see "Upgrading the 3.1 SP4 Access Gateway Service "in the *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*.

12 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

13 Restore any customized files from the backup taken earlier. To restore the files, copy the files to the respective locations below:

- `/opt/novell/nam/mag/tomcat7/conf/web.xml`
- `/opt/novell/nam/mag/tomcat7/webapps/nesp/WEB-INF/web.xml`
- `/opt/novell/nam/mag/tomcat7/webapps/nesp/jsp`
- `/opt/novell/nam/mag/tomcat7/webapps/nesp/html`
- `/opt/novell/nam/mag/tomcat7/webapps/nesp/images`
- `/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current`
- `/opt/novell/nam/mag/tomcat7/webapps/nesp/config`
- `/opt/novell/devman/jcc/scripts/presysconfig.sh`
- `/opt/novell/devman/jcc/scripts/postsysconfig.sh`

Upgrading the SSL VPN

If you have installed both the SSL VPN and the Administration Console on the same machine, see "Upgrading the Administration Console" on page 94.

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

- 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 7.3, "Installing the Key for the High-Bandwidth SSL VPN," on page 83.
- 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/tomcat7/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 SSL VPN User Interface" in the *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*.

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from Patches and Security and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5. The system displays the following confirmation message:

   ```
   Do you want to upgrade the above components (y/n)?
   ```

6. A Warning message regarding backup and restore is displayed. If you have customized any files, take a backup and restore them after installation. For more information, see
7. Would you like to continue this upgrade? Type *Y* to continue.
8. Enter the Access Manager Administration Console user ID.
9. Enter the Access Manager Administration Console password
10. Re-enter the password for verification
11. The system displays the following message when the upgrade is complete:

    ```
    Upgrade completed successfully.
    ```

12. Restore any customized files from the backup taken earlier. To restore the files, copy the files to the respective locations below:
    - `/var/opt/novell/tomcat7/conf/server.xml`
    - `/var/opt/novell/tomcat7/conf/tomcat7.conf`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/WEB-INF/web.xml`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/WEB-INF/conf`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/*.jsp`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/pages*`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/jsp`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/html`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/images`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/common`
    - `/var/opt/novell/tomcat7/webapps/sslvpn/SSLVPNClientHelp`

9.2 Upgrading on Windows

9.2.1 Upgrading from 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: <<link to migration guide>>

For verifying that the Access Manager components have been upgraded, see "Verifying the Upgrade" in *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*.

9.2.2 Upgrading from Access Manager 3.2, 3.2 SP1, and 3.2 SP1 IR1a to 3.2 SP2

Log in to the Novell Downloads page and follow the link that allows you to download the product. For instructions on upgrading the components, see "Upgrading on Windows" in the *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*..

9.3 Verifying the Access Manager Components

For verifying that the Access Manager components have been upgraded, see the NetIQ Access Manager 3.2 SP2 Readme.

10 Upgrading Kernel to the Latest Security Patch

10.1 Installing or Updating the Latest Linux Patches

WARNING: 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 Access Gateway Appliance installs a customized version of SLES 11. If you want to install the latest patches as they become available, you must have a Novell user account to receive the Linux updates.
- ❒ If you are on an older version of Access Manager and attempt to install security patches, SSLVPN will not come up. For details on upgrading from an older version of Access Manager to 3.2 SP1 IR1a, see Chapter 9, "Upgrading Access Manager Components," on page 91.
- ❒ Ensure that you have obtained the activation code for Access Manager from Novell Customer Center

10.1.1 Installing or Updating Security Patches for the Access Gateway Appliance

To get the latest security updates for the 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)*. In addition to the options that are selected by default, select *Registration Code*.
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` at the prompt.

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

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

10 Click *Quit* to exit YaST.

11 Open a shell prompt and specify the following command to verify if the repository named `NAM32-APP-Updates` was created:

```
zypper lr
```

An output similar to the following appears

```
# | Alias                                    | Name
| Enabled | Refresh
--+------------------------------------------+-----------------------------------
1 | NetIQAccessGatewayAppliance-3.2.1-57 | NetIQAccessGatewayAppliance-3.2.1-
57 | Yes     | No
2 | nu_novell_com:NAM32-APP-Updates      | NAM32-APP-Updates
| Yes     | Yes
```

12 Run the `zypper up` command to install the patches

13 After the patches are installed, restart the machine.

14 Confirm that all the patches are installed by running `zypper up` command again.

10.1.2 Configuring the Subscription Management Tool for Access Gateway Appliance

The Access Gateway Appliance 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.

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 (https://www.suse.com/documentation/smt11/).

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

- "SMT Configuration" on page 103
- "Troubleshooting" on page 104

SMT Configuration

You must configure the SMT server and set up subscription for `NAM32-APP-Updates` channel to receive the updates for Access Gateway Appliance.

1. Install the SMT server in a SLES 11 Server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 (https://www.suse.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 `NAM32-APP-Updates, sle-11-x86_64` repository is displayed in the *Repositories* tab.
7. Select `sle-11-x86_64`, then click *Toggle Mirroring* to ensure mirroring is selected for this repository.
8. Click *Mirror Now*. This step ensures that the *NAM32-APP-Updates* channel updates are mirrored from *nu.novell.com* to your local SMT server.
9. When mirroring is complete, click *OK* to close the tool.

Configuring the Access Gateway Appliance

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.
9. Confirm that all the patches are installed by running `zypper up` command once again.

Troubleshooting

If you face issues while using the activation code to register, see Resetting your ZEN Updater and Novell Customer Center Key Registration (http://www.novell.com/support/kb/doc.php?id=3303599)

A Troubleshooting Installation and Upgrade

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 `\am32setup_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 `\am32setup_debug.txt` file.
   - **4c** Delete the installation log files in the following directories:

     Windows 2008 Server: `\am32setup.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\Tomcat7\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\Tomcat7\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\Tomcat7\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
  1289
  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 *NetIQ Access Manager 3.2 SP2 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 107 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.

  For more information about how to delete the Identity Server in the Administration Console, see "Managing an Identity Server" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

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 108
- "Windows Installation Logs" on page 108

Linux Installation Logs

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

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

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

Windows Installation Logs

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

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

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

A.4 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.4.1, "Troubleshooting the Windows Access Gateway Service Installation," on page 109

A.4.1 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 2008 Server: `\agsinstall.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.5 Troubleshooting the SSL VPN Installation

This section has information on how you can troubleshoot problems while you are installing the SSL VPN server.

A.5.1 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.5.2 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.6 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 NetIQ Support.

A.6.1 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 *NetIQ Access Manager 3.2 SP2 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 "Triggering an Import Retry" on page 112.
7. If triggering an import retry does not solve the problem, reinstall the device.

A.6.2 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

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 2008: `\Program Files (x86)\Novell\log\app_sc.0.log`

- Tomcat Log on the Administration Console:

  Linux: `/opt/novell/nam/`*`device name`*`/logs/catalina.out`

  The device name can be `idp`, `mag`, `sslvpn` or `adminconsole`.

  Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\logs\stdout.log` and \Program Files (x86)\Novell\Tomcat\logs\stderr.log

- JCC log on the Access Gateway:

  Linux Appliance or Service: `/opt/novell/devman/jcc/logs/`

  Windows Service: `\Program Files\Novell\devman\jcc\logs`

Triggering an Import Retry

1 Go to the directory `/opt/novell/devman/jcc/`

```
cd /opt/novell/devman/jcc/
```

2 Run the `sh conf/reimport_ags.sh jcc` script and enter the details against the following prompts:

- Choose a local listener IP address [x.x.x.x]:
- (Optional) Choose a local NAT IP address [optional]:
- Choose Administration Console's IP address []:
- Enter Admin User's DN [cn=admin,o=novell]:
- Enter Admin Password: *****

  Wait for a few minutes for the configuration to finish.

3 Run the `sh conf/reimport_ags.sh agm` script and enter details against the following prompts:

- Do you want to import the device with current configuration or initial configuration after installation (Enter C for current configuration, I for initial configuration).
- Enter Admin User's DN [cn=admin,o=novell]:
- Enter Admin password:

A.7 Troubleshooting a Linux Administration Console Upgrade

A.7.1 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*.

A.7.2 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.7.3 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.7.4 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.8 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.9 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.10 Troubleshooting a Linux SSL Renegotiation

To enable the SSL renegotiation on SLES 11 SP1 and SP2, add the parameter `JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=true` in the configuration file `/var/opt/novell/tomcat7/conf/tomcat7.conf if the parameter does not exist`.

Restart Tomcat to enable SSL renegotiation.

To disable the SSL renegotiation on SLES 11 SP1 and SP2, add the parameter `JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=false` in the configuration file `/var/opt/novell/tomcat7/conf/tomcat7.conf if the parameter does not exist.`

Restart Tomcat to disable SSL renegotiation.

A.11 Secondary Administration Console Installation Fails

The secondary Administration Console installation fails with a message "'Verifying time synchronization". If you are installing the secondary Admin Console, ensure that time is in sync with the primary Admin console, prior to installation.

If the time is in sync and the secondary Administration Console installation fails or takes a long time, see the eDirectory install logs under `/tmp/novell_access_manager`. The log file name will be similar to `install_edir_xxxxxx`. If at the end of the log you see an entry "Verifying time synchronization" multiple times, you should repair the eDirectory. To repair the eDirectory:

1. Log in to the primary Administration Console and execute the `ndsrepair -T` command.

   The replica servers and their time sync status is displayed.
2. Execute the `ndsrepair -N` command and select the server which has the problem.
3. Log in to the secondary Administration Console and you can see that the installation has proceeded. You need not to re-run the installer.

A.12 Access Gateway Appliance Installation Fails Due to an XML Parser Error

This error may happen if the Appliance is installed by using a remotely mounted installer. Use a locally mounted installer to avoid this issue.

B Modifications Required for a 3.2 Login Page

B.1 Modifying the File

The following 3.2 `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 3.2 `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>
```

C Configuring Network Address Translation

NetIQ Access Manager can be configured by using Network Address Translation (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.

See your router documentation for more information.

C.1 Configuring the Administration Console Behind NAT

1. Log in to the Administration Console.
2. Go to *Access Manager* > *Global Settings*, then click *New*.
3. Select an IP address from the *Administration Console Public IP Address* list.

   This list contains primary and secondary Administration Console IP addresses.
4. Enter the respective NAT IP address for primary and secondary Administration Console in *Public NAT IP Address*.

   NOTE: If the NAT IP address is not provided or if a mapping exists for the selected Administration Console IP, a message `IP Address is not valid` is displayed.
5. Click *OK*.

   The Administration Console NAT IP is shared to other Access Manager devices.

For more information about configuring NAT, see "Global Settings"in the *NetIQ Access Manager 3.2 SP2 Administration Console Guide*.

C.2 Configuring the Identity Server, Access Gateway, and SSL VPN Behind NAT

During installation, the system prompts the following message to specify the NAT address for the component:

```
Is local NAT available for the <device name> y/n? [n]:
```

Enter `Y` and specify the NAT address. This enables the Administration Console to use this NAT address when communicating to this device.

Alternatively, if the device is already installed, then run the `reimport_nidp.sh` or `reimport_ags.sh` script to specify the NAT address.

D Feature Comparison of Different Types of Access Gateways

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

- Protecting Web resources with contracts, Authorization, 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 among 3.1 SP4 Access Gateway, Access Gateway Appliance, and Access 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.

This table describes the differences among the 3.1 SP4 Access Gateway, Access Gateway Appliance, and Access Gateway Service. Only your network and Web server configurations can determine whether the differences are significant.

Table D-1 *Differences among the 3.1 SP4 Access Gateway, Access Gateway Appliance, and Access Gateway Service:*

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
System architecture	32-bit	64-bit only	64-bit only
Platform support	SLES only	SLES 11 SP1 and SP2, Red Hat Enterprise Linux	SLES 11 SP1 and SP2, Red Hat Enterprise Linux, Windows

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Network configuration • DNS servers • Gateways • Network interface cards • Host names	Can be done from the Administration Console.	Can be done from the Administration Console. By default after the installation, only one network interface card will be displayed in the Administration Console. To detect other network interface card, do the following: • Configure a primary IP Address in YaST for the remaining interfaces. • Click *Devices* > *Access Gateways* > *Select the device* > *New IP* > *click OK*.	Configurable with standard operating system utilities.
Date and time	Can be done from the Administration Console.	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.	No limit.	No limit.
Rewriter: Profiles	Can do word pattern matches in Word profiles and Character profiles.	Can only do word pattern matches in Character profiles.	Can only do word pattern matches in Character profiles.
Rewriter: Word profiles	Case-sensitive.	Case-insensitive.	Case-insensitive.
Rewriter: Special tokens for Word profiles	Not supported.	Supports the [w]. [ow], [ep], [ew], and [oa] options.	Supports the [w]. [ow], [ep], [ew], and [oa] options.
Rewriter: webcal	Not supported.	Supported.	Supported.
Cache directory	Separate protected partition.	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).	Uses filesystem provided by Apache mod_cache module. For more information on the Apache model, see "Caching Guide" (http://httpd.apache.org/docs/2.2/caching.html).

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Cache freshness configuration options	Supported.	Limited support. You can achieve the following with Advanced Options: ◆ HTTP Maximum Cache Time ◆ HTTP Minimum Cache Time Continue Fill Time and HTTP Retries are not available.	Limited support. You can achieve the following with Advanced Options: ◆ HTTP Maximum Cache Time ◆ HTTP Minimum Cache Time Continue Fill Time and HTTP Retries are not available.
Custom cache control headers	Supported.	Not supported.	Not supported.
Caching behavior	For more information, see "Configuring Caching Options" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.	For more information, see "Configuring Caching Options" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.	For more information, see "Configuring Caching Options" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.
X-Forwarded-For header	Can enable/disable from the Administration Console	Cannot disable. By default, it is sent by Apache along with X-Forwarded-Host and X-Forwarded-Server headers.	Cannot disable. By default, it is sent by Apache along with X-Forwarded-Host and X-Forwarded-Server headers.
Via header	Includes the device ID and version number.	Includes the device ID.	Includes the device ID.
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.	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.
Access logs for proxy service: When protected resource logging fails	Stop the proxy service if logging fails.	Cannot stop the proxy service if logging fails. For more information on access logging, see "Configuring Logging for a Proxy Service" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.	Cannot stop the proxy service if logging fails. For more information on access logging, see "Configuring Logging for a Proxy Service" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.
Web server connections	If the gateway has multiple network cards, you can specify which network card to use for the Web server connection.	Use standard routing table on the right device to route the traffic for that Web server on the device.	Use standard routing table on the device to route the traffic for that Web server on the right device.

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
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.	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.	Access Gateway Appliance format.	Access Gateway Appliance format.
5-6 byte UTF characters (supported by IIS Web servers)	Supported.	Unsupported.	Unsupported.
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*.	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` Uses `Syslog`	`ags_error.log` and Apache `error.log` All logs are now in a central location `/var/opt/novell/logs`	`ags_error.log` and Apache `error.log` All logs are now in a central location `/var/opt/novell/logs`
Device logging configuration	Log level set with options in the nash shell.	Configurable from the Administration Console. Click *Access Gateways* > *Edit* > *Logging*.	Configurable from the Administration Console. Click *Access Gateways* > *Edit* > *Logging*.
Sending alerts to an SNMP server	Unsupported.	Supported.	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.	Supported.
NetStorage	Browser connections can be used.	Browser and WebDAV connections can be used.	Browser and WebDAV connections can be used.

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
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> HT TP request is being redirected to HTTPS. <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> Found The document has moved here. </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> Found The document has moved here. </body></html>
Customizing Error Pages	◆ ErrorPageTemplate. html.<lang> should be modified to for customizing error pages. ◆ ErrorMessages.xml. <lang> is available under /var/ novell/cfgdb/ ErrorPagesConfi g	◆ /opt/novell/ apache2/share/ apache2/doc/ errors/ <http_status_co de>.var and edit top.html, bottom.html ◆ ErrorMessages.xml. <lang> found at / opt/novell/nam/ mag/webapps/ mag/WEB-INF/ config/current	◆ /opt/novell/ apache2/share/ apache2/doc/ errors/ <http_status_co de>.var and edit top.html, bottom.html ◆ ErrorMessages.xml. <lang> found at / opt/novell/nam/ mag/webapps/ mag/WEB-INF/ config/current
Advanced Options configuration	The error page from origin server is forwarded to the browser.	Access Gateway overrides the origin server error page with Access Gateway's error page. This is turned off by default to behave like the Linux Access Gateway. If you do not want to send the origin server's error page, but a customized error page in the Access Gateway, you can enable this as ProxyErrorOverride on.	Access Gateway overrides the origin server error page with Access Gateway's error page. For the error page to behave like Linux Access Gateway configure the *ProxyErrorOverride off* in Advanced Options.

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Alerts	The warning message log file format has changed. The log file has fewer columns displayed when compared to Access Gateway Appliance/ Service. For example, `(Mon Jan 30 12:31:41 2012): Proxy configuration has changed`	The log file has more information than the file in the Linux Access Gateway Appliance. For example, `<amLogEntry> 2012-01-30T12:17:22Z WARN ALERT: AMDEVICEID#ag-02EC8D7D5B8A8291:DateTime=132790604264 3, Severity=Warn, ServiceType=ag, Message=Access Gateway configuration has changed </ amLogEntry>`	The log file has more information than the file in the Linux Access Gateway Appliance. For example, `<amLogEntry> 2012-01-30T12:17:22Z WARN ALERT: AMDEVICEID#ag-02EC8D7D5B8A8291:DateTime=132790604264 3, Severity=Warn, ServiceType=ag, Message=Access Gateway configuration has changed </ amLogEntry>`
Cache Control options	Enable Custom Cache Control Header When objects reach the Custom Cache Control Expiration Time: ◆ opt1: Revalidate the object with a "Get-If-Modified" ◆ opt2: Always obtain a fresh copy of the object. Cache Control Headers	Enable Custom Cache Control Header When objects reach the Custom Cache Control Expiration Time: ◆ opt1: Revalidate the object with a "Get-If-Modified" ◆ Unsupported The Cache Control Headers can be injected using apache `mod_headers` module directives.	Enable Custom Cache Control Header When objects reach the Custom Cache Control Expiration Time: ◆ opt1: Revalidate the object with a "Get-If-Modified" ◆ Unsupported The Cache Control Headers can be injected using apache `mod_headers` module directives.
Unreachable webserver	Checks health of Web servers that are marked as unreachable every 30 seconds.	The proxy checks the Web server for each new session request at an interval of 1 minute, by default. You can configure the advanced option for a different interval, for example, `AdditionalBalancerMemberOptions retry=180`, where 180 is in seconds.	The proxy checks the web server for each new session request at an interval of 1 minute, by default. You can configure the advanced option for a different interval, for example, `AdditionalBalancerMemberOptions retry=180`, where 180 is in seconds.

Feature	3.1 SP4 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Client IP mismatch error	On receiving IPC cookie from browser, Linux Access Gateway asks the user to authenticate if it is a protected resource that needs authentication, or, just treats the request for public resources as if the cookie was not received.	On receiving IPC cookie from browser, Access Gateway checks for client IP address in the cookie. If the IP address in the cookie and the client IP address from which the request came do not match, Access Gateway displays an error page.	On receiving IPC cookie from browser, Access Gateway checks for client IP address in the cookie. If the IP address in the cookie and the client IP address from which the request came do not match, Access Gateway displays an error page.
Chunk response behavior	Linux Access Gateway collects the complete chunk response and sends response with the Content-Length header to the client.	Access Gateway forwards the chunked response as it is to the client.	Access Gateway forwards the chunked response as it is to the client.
Search and replace	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are not replaced.	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are replaced.	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are replaced.
PostParking Size Limit	The size limit is 50 KB. **NOTE:** With 3.1.5 the PostParking Size limit is increased to 64 KB.	The size limit is 64 KB.	The size limit is 64KB.
Adapter List Options Allows to change the speed, duplex, and NAT behavior.	Supported.	Unsupported.	Unsupported.