Installation Guide

Access Manager Appliance 4.0 SP2

June 2015

Legal Notice

Contents

About NetIQ Corporation **5**
About this Book and the Library **7**

1 NetIQ Access Manager Appliance Product Overview **9**

1.1 How Access Manager Appliance Solves Business Challenges . . . 9
1.1.1 Protecting Resources While Providing Access . . . 10
1.1.2 Managing Passwords with Single Sign-On . . . 11
1.1.3 Enforcing Business Policies . . . 12
1.1.4 Sharing Identity Information . . . 13
1.1.5 Protecting Identity Information . . . 15
1.1.6 Complying with Regulations . . . 16
1.2 How Access Manager Appliance Works . . . 17
1.2.1 Authentication . . . 17
1.2.2 Authorization . . . 18
1.2.3 Identity Injection . . . 18
1.2.4 Identity Federation . . . 18
1.3 Access Manager Appliance Devices and Their Features . . . 19
1.3.1 Administration Console . . . 19
1.3.2 Identity Servers . . . 19
1.3.3 Access Gateways . . . 20
1.3.4 SSL VPN . . . 21
1.3.5 Policies . . . 22
1.3.6 Certificate Management . . . 22
1.3.7 Embedded Service Provider . . . 22
1.3.8 The User Portal Application . . . 22
1.3.9 Language Support . . . 23
1.4 Differences Between Access Manager and Access Manager Appliance . . . 23

2 Installing Access Manager Appliance **29**

2.1 Installation Requirements . . . 29
2.1.1 Hardware Platform Requirements . . . 29
2.1.2 Browser Support . . . 29
2.1.3 Client Access Requirements . . . 30
2.1.4 Installation Mode . . . 30
2.1.5 Virtual Machine Requirements . . . 30
2.1.6 Network Requirements . . . 31
2.1.7 Basic Setup . . . 32
2.2 Installing Access Manager Appliance . . . 33
2.2.1 Prerequisites . . . 33
2.2.2 Installing Access Manager Appliance . . . 33
2.2.3 Removing the Landing Portal . . . 36
2.2.4 Logging In to the Administration Console . . . 37
2.2.5 Administration Console Conventions . . . 38

3 Setting Up Firewalls **39**

3.1 Required Ports . . . 39
3.2 Restricted Ports . . . 41
3.3 Sample Configurations . . . 42

3.3.1 Access Manager Appliance in DMZ . . . 42

4 Upgrading Access Manager Appliance 45

4.1 Upgrading from the Evaluation Version to the Purchased Version . . . 45
4.2 Upgrading Access Manager Appliance 3.2 SP2, 4.0 to 4.0 SP2 . . . 46
4.3 Applying Access Manager Appliance 4.0 Hotfix* Patch . . . 46
4.3.1 Prerequisites . . . 47
4.3.2 Installing the Patch . . . 47
4.3.3 Administering Patches . . . 48
4.4 Configuring the Access Manager Appliance User Portal . . . 49

5 Upgrading Kernel to the Latest Linux Security Patch 51

5.1 Installing or Updating Security Patches for Access Manager Appliance . . . 51
5.2 Configuring the Subscription Management Tool for Access Manager Appliance . . . 52
5.2.1 SMT Configuration . . . 52
5.2.2 Troubleshooting . . . 53
5.3 Upgrading the Operating System for Access Manager Appliance . . . 54

A Troubleshooting Installation 55

A.1 Checking the Installation Logs . . . 55
A.2 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation . . . 56
A.3 Installation Through Terminal Mode is not Supported . . . 56
A.4 Novell Device Manager Installation Fails During the Appliance Installation . . . 56
A.5 Access Manager Appliance Installation Fails Due to an XML Parser Error . . . 56
A.6 DN Is Added as Provider ID While Installing NMAS SAML Method . . . 57
A.7 Portal Web Server is not Accessible . . . 57
A.8 Installing RHEL on the Administration Console Fails if IPv6 is Disabled . . . 57

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

About this Book and the Library

The *Installation Guide* provides an introduction to NetIQ Access Manager Appliance and describes the installation and upgrade procedures.

Intended Audience

This book 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)

Other Information in the Library

The library provides the following information resources:

- *NetIQ Access Manager Appliance 4.0 SP1 Setup Guide*
- *NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide*
- *NetIQ Access Manager Appliance 4.0 Identity Server Guide*
- *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*
- *NetIQ Access Manager Appliance 4.0 SP1 Policy Guide*
- *NetIQ Access Manager Appliance 4.0 SSL VPN Server Guide*

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

1 NetIQ Access Manager Appliance Product Overview

NetIQ Access Manager Appliance 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 about what's new in Access Manager Appliance 4.0, see "Access Manager Appliance 4.0 Hotfix 1 Readme".

This section discusses the following topics:

- Section 1.1, "How Access Manager Appliance Solves Business Challenges," on page 9
- Section 1.2, "How Access Manager Appliance Works," on page 17
- Section 1.3, "Access Manager Appliance Devices and Their Features," on page 19
- Section 1.4, "Differences Between Access Manager and Access Manager Appliance," on page 23

1.1 How Access Manager Appliance 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.

Access Manager Appliance lets you provide employees, customers, and partners with secure access to your network resources. 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.
- Ensuring that 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.

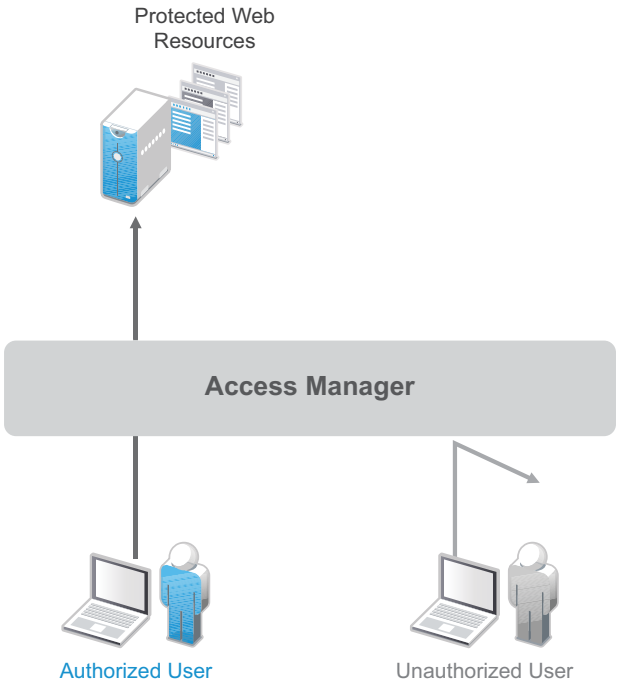
- Protecting users' privacy and confidential information as they access company resources or partners' resources.
- Proving compliance with your business policies, privacy laws such as Sarbanes-Oxley, HIPAA, or European Union, and other regulatory requirements.

The following sections expand on these challenges and introduce the solutions provided by Access Manager.

- Section 1.1.1, "Protecting Resources While Providing Access," on page 10
- Section 1.1.2, "Managing Passwords with Single Sign-On," on page 11
- Section 1.1.3, "Enforcing Business Policies," on page 12
- Section 1.1.4, "Sharing Identity Information," on page 13
- Section 1.1.5, "Protecting Identity Information," on page 15
- Section 1.1.6, "Complying with Regulations," on page 16

1.1.1 Protecting Resources While Providing Access

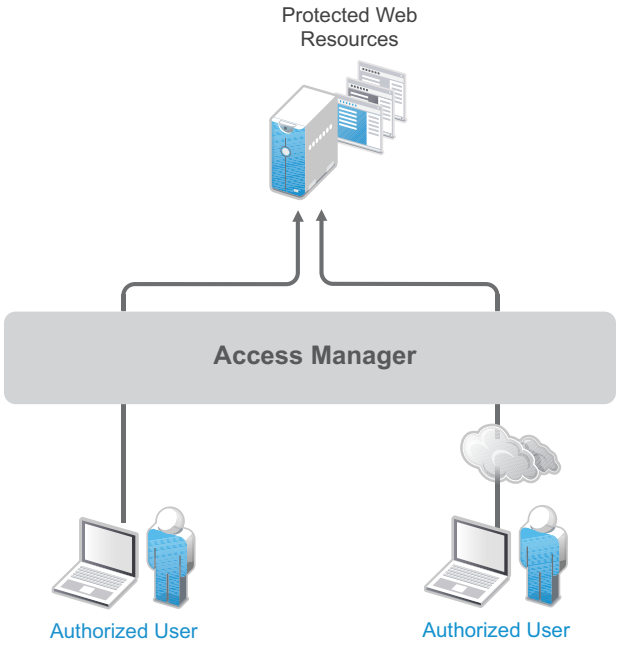
The primary purpose of Access Manager Appliance is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources and traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized to use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



Access Manager Appliance 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 Appliance with authorized credentials.

Access Manager Appliance 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.

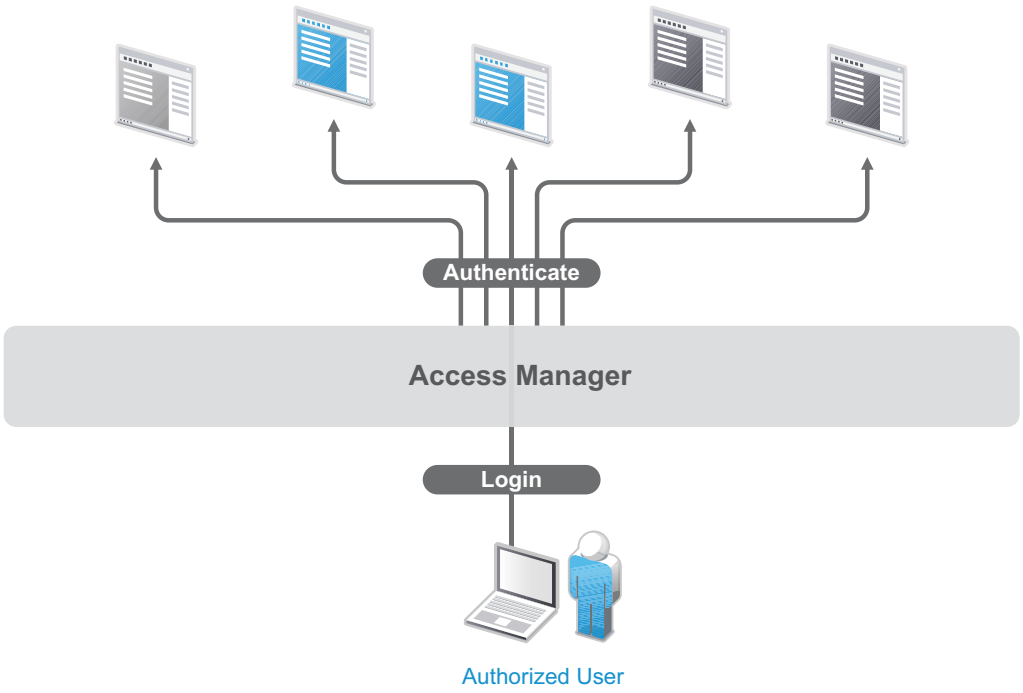
Access to resources is independent of a user's location, as shown in the following illustration. Access Manager Appliance provides the same secure access and same experience whether the user is accessing resources from your local office, from home, or from an airport terminal.



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 Appliance 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 Appliance 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.



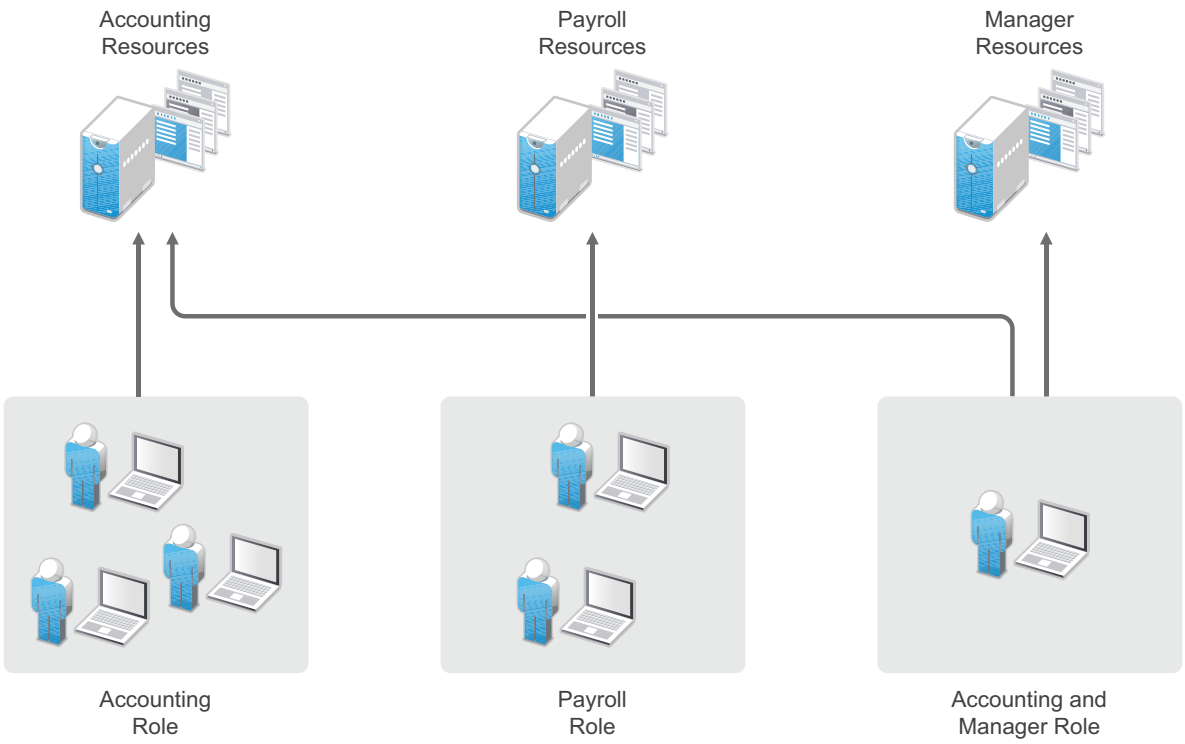
By simplifying the use and management of passwords, Access Manager Appliance helps you enhance the user's experience, increase security, streamline business processes, and reduce system administration and support costs.

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 Appliance 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 Appliance, 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.



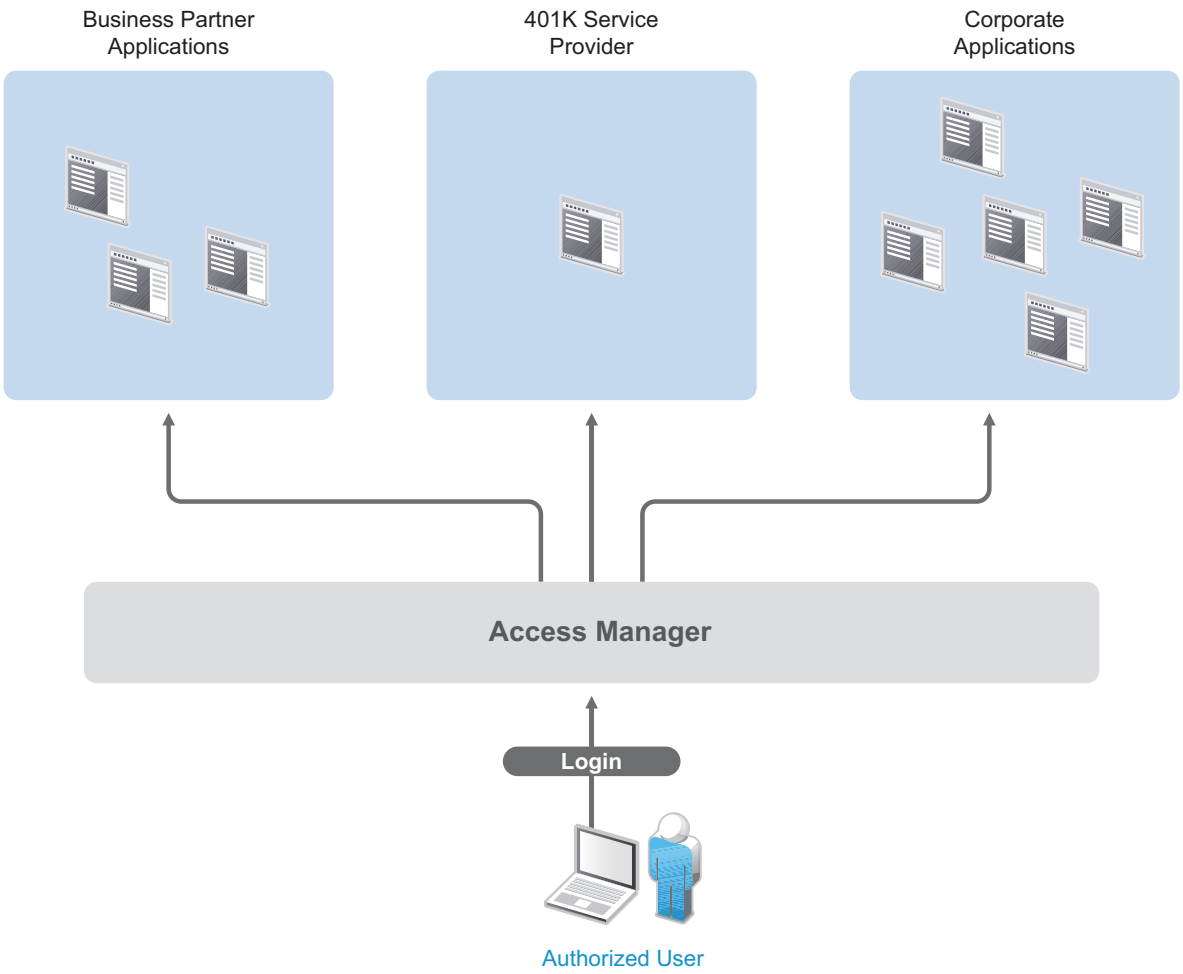
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

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

1.1.4 Sharing Identity Information

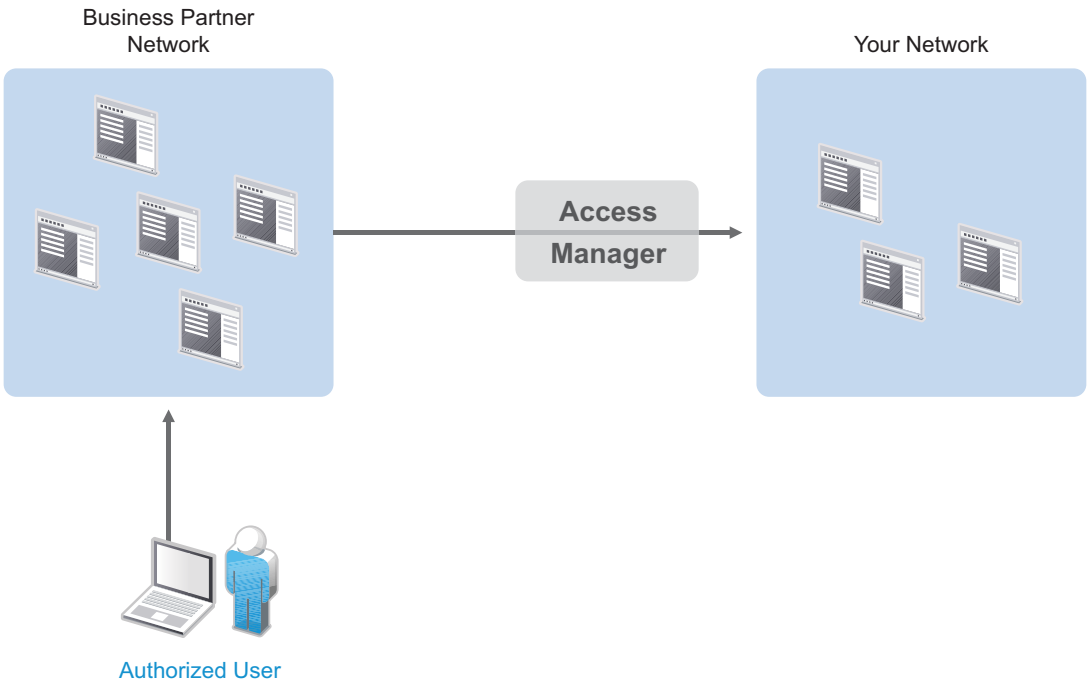
In today's business environment, few organizations stand alone. More than likely, you have trusted business partners with whom you need to shared resources in a secure manner. Or, you have business services, such as a 401k management system, to which you need to provide employee access. Or, maybe your organization is the one providing services to another business. Access Manager Appliance 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 Appliance to establish a trust relationship with the business partner and the 401k service, your employees can log in through Access Manager Appliance to gain access to the authorized resources in all three identity domains.

Access Manager Appliance 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.



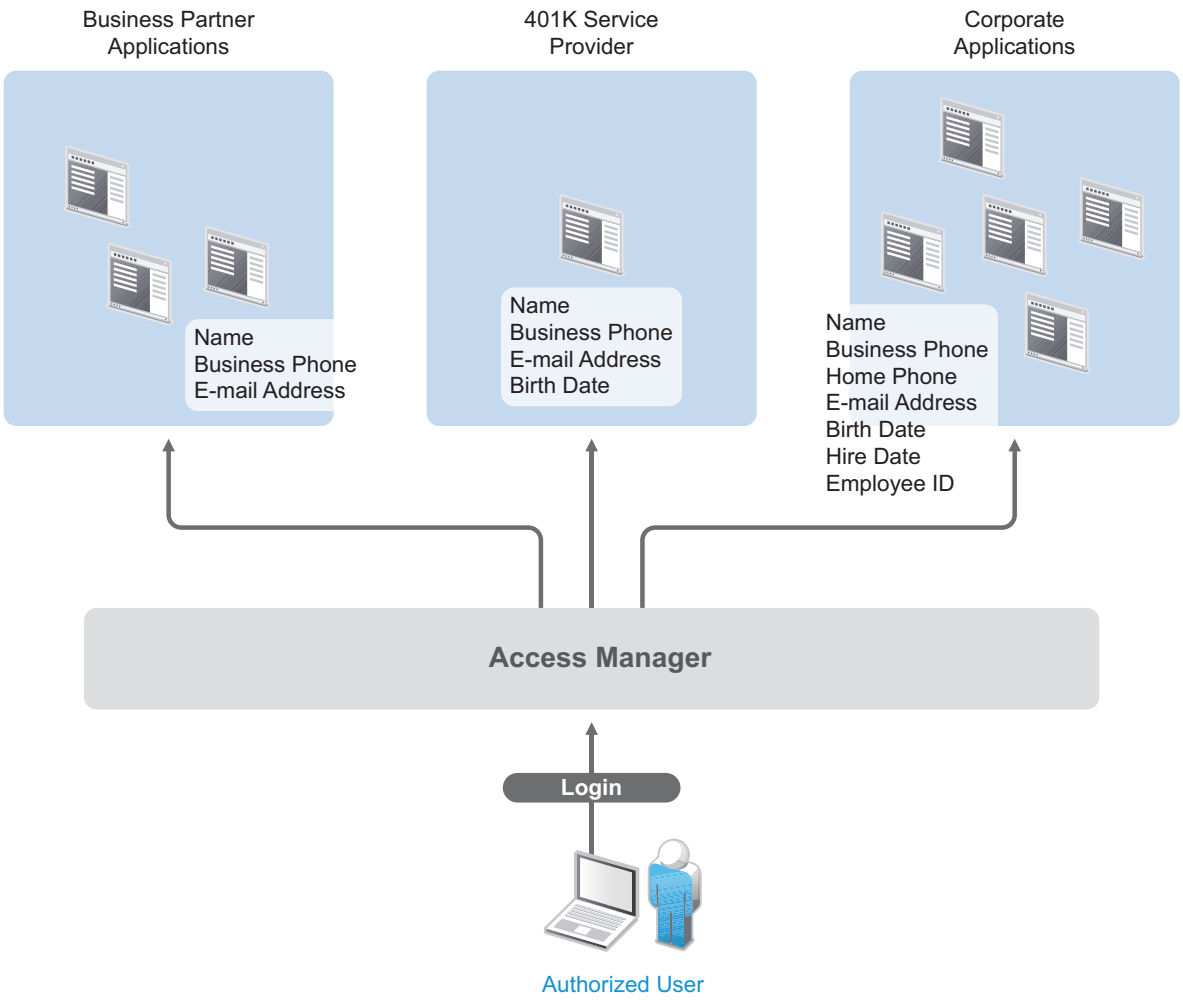
In addition to simply linking user accounts in different identity domains, Access Manager Appliance also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization can initiate the creation of an account in your business partner's system through Access Manager Appliance 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 Appliance 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 Appliance 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 Appliance 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 Appliance offers this built-in privacy protection for your employees, partners, and customers alike, wherever they are working. With Access Manager Appliance in place, your organization can guarantee user confidentiality. And for federated provisioning, Access Manager Appliance 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 Appliance.

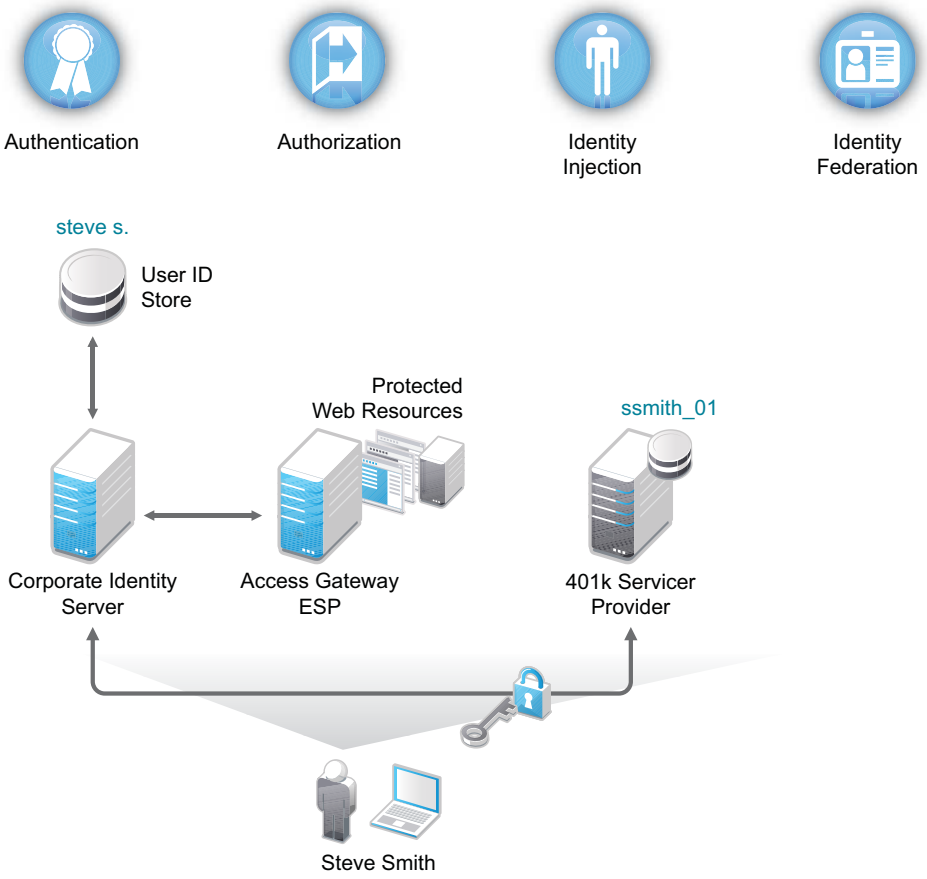
Specifically, Access Manager Appliance helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager Appliance can generate the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

1.2 How Access Manager Appliance Works

Access Manager Appliance deployments typically use Identity Servers and Access Gateways to provide policy-driven access control for HTTP services.

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

Figure 1-1 *Access Manager Appliance*



1.2.1 Authentication

The Identity Server facilitates authentication for all Access Manager Appliance components. This authentication is shared with internal or external service providers on behalf of the user, by means of assertions. Access Manager Appliance 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 Appliance, 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 Appliance 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.

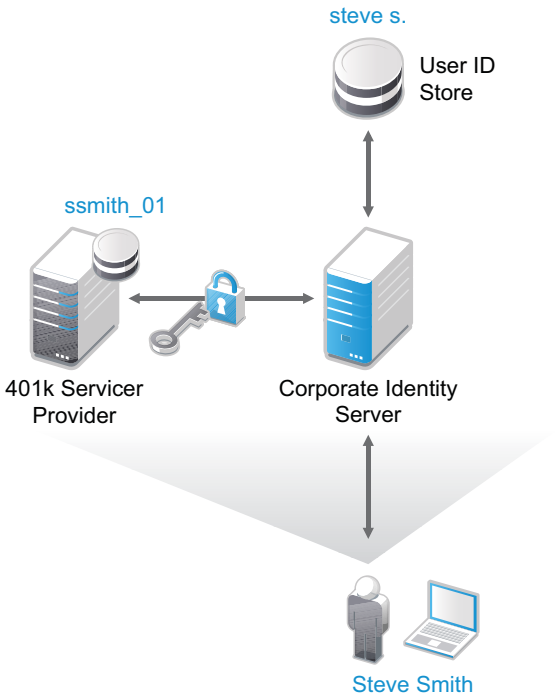
1.2.3 Identity Injection

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 Appliance 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.

1.3 Access Manager Appliance Devices and Their Features

- Section 1.3.1, "Administration Console," on page 19
- Section 1.3.2, "Identity Servers," on page 19
- Section 1.3.3, "Access Gateways," on page 20
- Section 1.3.4, "SSL VPN," on page 21
- Section 1.3.5, "Policies," on page 22
- Section 1.3.6, "Certificate Management," on page 22
- Section 1.3.7, "Embedded Service Provider," on page 22
- Section 1.3.8, "The User Portal Application," on page 22
- Section 1.3.9, "Language Support," on page 23

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

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 Appliance 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 Appliance 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 Appliance and are achieved after the federation and trust model is configured among trusted providers and the components of Access Manager Appliance.
- **Identity Integration:** Provides authentication and identity services to Access Gateways that are configured to protect Web servers. The Access Gateway and other Access Manager Appliance components include an embedded service provider that is trusted by NetIQ Access Manager Appliance 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 to form the basis for granting and restricting access to particular Web resources.

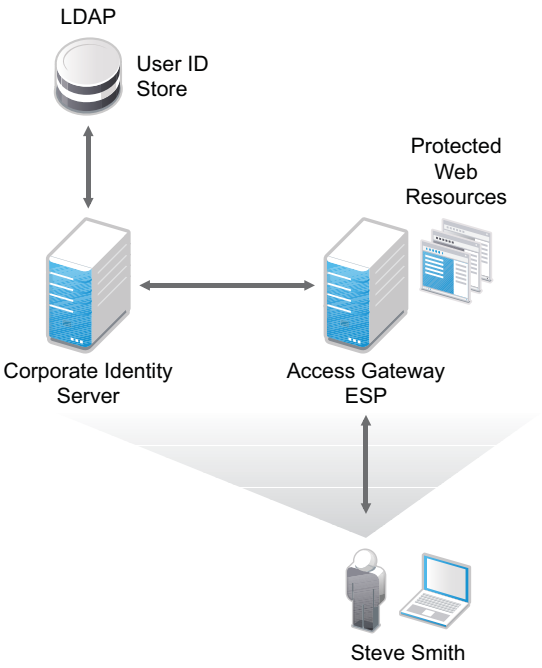
For an overview of Liberty, see “About Liberty” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.

For an overview of SAML, see “Understanding How Access Manager Uses SAML” in the *NetIQ Access Manager Appliance 4.0 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 Appliance.

Figure 1-3 *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.

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 Policies

Policies provide the authorization component of Access Manager Appliance. 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. 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.

The Access Gateway includes an Embedded Service Provider agent that interacts with the Identity Server to provide authentication, policy decision, and enforcement. 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.

1.3.6 Certificate Management

Access Manager Appliance 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.

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

1.3.7 Embedded Service Provider

The Access Gateway and SSL VPN uses an Embedded Service Provider to redirect authentication requests to the Identity Server. The Identity Server requires requests to be digitally signed and encrypted and allows only trusted devices to participate. To become trusted, devices must exchange metadata. The Embedded Service Provider performs this task automatically for the Access Gateway and SSL VPN.

1.3.8 The User Portal Application

The Access Manager Appliance 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.

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.

1.3.9 Language Support

The Access Manager Appliance 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 Appliance 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 User Portal is 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 about customizing these pages, see the following:

- For the Access Gateway, see "Customizing Error Messages and Error Pages on Access Gateway" in the *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*.
- For the Identity Server, see "Customizing Identity Server Messages" in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.

1.4 Differences Between Access Manager and Access Manager Appliance

Access Manager Appliance is a new deployment model introduced in NetIQ Access Manager 3.2. It includes all major components such as Administration Console, Identity Server, and Access Gateway in a single soft appliance. This solution differs from the other Access Manager model where all the components can be installed on separate servers. Access Manager Appliance enables organizations to rapidly deploy and secure Web and enterprise applications. This simplifies access to any application.

You can find Access Manager documentation here: (https://www.netiq.com/documentation/netiqaccessmanager4/)

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

Features	Access Manager Appliance	Access Manager
Installation	All the components, such as the Identity Server and Access Gateway are installed on a single server.	Each Access Manager component such as the Identity Server and Access Gateway can be installed on different machines. To deploy the existing solution in a cluster mode, at least 6 machines are required.
Time to Value	During installation and configuration of Access Manager Appliance, several steps are automated to quickly set up the system.	Installation and configuration of Access Manager requires more time because the components are on different servers.
User Input Required during Installation	Access Manager Appliance is a software appliance that takes only a few basic parameters as input. Several options assume default values.	With Access Manager, you have more flexibility during installation in terms of selectable parameters.

Features	Access Manager Appliance	Access Manager
Installation and Configuration Phases	The installation program 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 is separately configured.
Host Operating System	A soft appliance that includes a pre-installed and configured SUSE Linux operating system. Both the operating system and Access Manager patches are maintained by NetIQ through the patch update channel.	The operating system choice is more flexible. Install Administration Console, Identity Server and Access Gateway on a supported operating system (SUSE, Red Hat, or Windows). The patch update channel maintains the patches for Access Manager. You must purchase, install, and maintain the underlying operating system.
Component Installation Flexibility	Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.	Each Access Manager component such as Administration Console, Identity Server, and Access Gateway are installed on independent host servers. Although the ability to install multiple components on a single host server exists, it is very limited and generally not recommended. A typical highly available deployment requires 6-8 or more virtual or physical servers (two Administration Consoles, two Identity Servers, and two Access Gateways).
Administration Console Access	The Administration Console is installed on Access Manager Appliance along with all other components. If you use two network interfaces, access to the Administration Console can be limited to the private IP network bound to the internal network. The public interface is bound to an externally accessible network.	The Administration Console can be installed on an independent host inside your private network but can still securely manage Access Manager components that reside in your DMZ or external network.
Scalability and Performance	The Access Manager Appliance scales vertically on adding CPU and memory resources to each node. For more information, see Performance and Sizing Guidelines.	The Access Manager scales both vertically and horizontally on adding nodes. For more information, see Performance and Sizing Guidelines.
Mode of release	Access Manager is delivered as a software appliance.	Access Manager is delivered in the form of multiple operating system-specific binaries.
Networking: Port Details	The Administration Console and Identity Server are accelerated by Access Gateways. Only HTTPS port 443 is required in the firewall to deploy Access Manager Appliance.	Multiple ports need to be opened for deployment.

Features	Access Manager Appliance	Access Manager
Networking: General	The Administration Console can be in a DMZ or in a private network. If Administration Console is in a DMZ, restrict access through the private interface.	Because the Administration Console is a separate component, access can be restricted or the Administration Console can be placed in an internal network.
Certificate Management	Certificate management is simplified. All certificates and key stores are stored in one place making replacing or renewing certificates easier. The same certificate is used for all communication. (Signing, encryption, and transport).	Changes are required in multiple places to replace or renew certificates. Because there are multiple key stores, you can configure different certificates for the communication.
Signing Certificates for Service Providers	Associating different signing certificates for each service provider is not supported.	A unique signing certificate can be assigned to each service provider. In environments with a large number of trust relationships, this feature eases the process of replacing expiring certificates.
Associating Different Certificates to Identity Server	This capability is not applicable because the Identity Server is accelerated by the Access Gateway.	This capability is supported. The Identity Server can be behind the Access Gateway or can be placed separately in the DMZ.
Sample Portal	After a successful installation, a sample Web portal is deployed for the administrator's reference. The administrator can access the sample portal by using the http://hostname URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.	A sample portal is not available.
Ready-made Access Manager	The following configuration steps are automatically completed when Access Manager Appliance is installed: ◆ Importing Identity Server and Access Gateway components. ◆ Automatic clustering of Identity Server and Access Gateway components. ◆ Automatic configuration of Identity Server to bring these to the green state. ◆ Automatic configuration of Access Gateways and Identity Server association. ◆ Automatic service creation to accelerate the Identity Server, Administration Console, and portal.	Each component is manually configured and set up before Web applications can be federation enabled, accelerated and protected.

Features	Access Manager Appliance	Access Manager
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.
Upgrade	You can upgrade from one version of Access Manager Appliance to another version. Upgrading from Access Manager to Access Manager Appliance is not supported.	You can upgrade from one version of Access Manager to another version. Upgrading from Access Manager Appliance to Access Manager is not supported.
Migration between Models	During migration from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration should be done manually.	During migration from Access Manager to Access Manager Appliance, the policies can be exported but the rest of the configuration should be done manually.
NIC Bonding	IP address configuration is done through the Administration Console. So, NIC bonding is not supported.	NIC bonding can be done through the operating system and Access Manager uses this configuration
Updating Kernel with Security Patches	Access Manager Appliance supports installation of the latest SLES operating system security patches.	You are fully responsible for all operating system maintenance including patching.
Clustering	For additional capacity and for failover, cluster a group of NetIQ Access Manager Appliances and configure them to act as a single server. You can cluster any number of Identity Servers, Access Gateways, and up to three Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, and Access Gateway. For the fourth installation onwards, the node has all components except for the Administration Console.	For additional capacity and for failover, cluster a group of Identity Servers and configure them to act as a single server. You can create a cluster of Access Gateways and configure them to act as a single server. Fault tolerance can be achieved by installing up to two secondary consoles. To deploy the existing solution in a cluster mode, at least 6 systems are required.

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

2 Installing Access Manager Appliance

This chapter explains how to install Access Manager Appliance. Topics include:

- Section 2.1, “Installation Requirements,” on page 29
- Section 2.2, “Installing Access Manager Appliance,” on page 33

2.1 Installation Requirements

This section explains requirements for installing Access Manager Appliance. For a list of current filenames and for information about installing the latest release, review “Access Manager Appliance 4.0 Hotfix 1 Readme”.

The Access Manager Appliance installer installs all the components on a single machine, so software and hardware requirements are same for all components. Section 1.4, “Differences Between Access Manager and Access Manager Appliance,” on page 23 lists differences between previously shipped Access Manager versus Access Manager Appliance.

Access Manager Appliance is based on the SUSE Linux Enterprise Server (SLES) 11 SP2 and SP3 64-bit operating system. The hard disk, RAM, and CPU requirements are same for all components.

2.1.1 Hardware Platform Requirements

The following are the hardware requirements:

- Minimum of 8 GB RAM.
- Dual CPU or core (3.0 GHz or comparable chip).
- 100 GB hard disk.

  The hard disk should have ample space for logging in a production environment. This disk space must be local and not remote.

  2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with the rollover options and logging level that you configure.
- The static IP address and an assigned DNS name (hostname and domain name) for your Access Manager Appliance.

2.1.2 Browser Support

The following browsers are supported for users to log in to Access Manager Appliance:

- Internet Explorer 8.*x* or higher
- Mozilla Firefox

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

2.1.3 Client Access Requirements

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

2.1.4 Installation Mode

You must install Access Manager Appliance by burning the Access Manager Appliance ISO on a DVD.

2.1.5 Virtual Machine Requirements

The virtual machine must have enough resources. The requirements for a virtual machine need to match the requirements for a physical machine. To achieve the performance similar to a physical machine, 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
- 8 GB RAM
- 2 CPUs

The following virtual machines are supported:

- VMware ESX Server version 3.5 or later ((same SLES versions as for regular hardware specifications)
- Xen Virtualization on SLES 11 SP1 and SP2 64-bit

NOTE: SLES 11 and SP2 64-bit Access Manager Appliance does not support XEN paravirtualization for the 4.0 release.

The following sections contain installation tips for virtual machines:

- "Keeping Time Synchronized on Access Manager Appliances" on page 30
- "Number of Virtual Machines Per Physical Machine" on page 31
- "Using a Network Adapter for VMWare ESX" on page 31

Keeping Time Synchronized on Access Manager Appliances

Even when virtual machines are configured to use a network time protocol (NTP) server, time does not stay synchronized because the machines periodically lose their connection to the NTP server. The easiest solution is to configure primary Access Manager Appliance to use an NTP server and configure other Access Manager Appliance to use a cron job to synchronize their time with primary Access Manager Appliance.

SLES 11 and SP2: The `ntpdate` command is not supported by SLES 11 64-bit. You can use the `sntp` command. 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 NTP server.

Number of Virtual Machines Per Physical Machine

How you deploy your virtual machines can greatly influence the Access Manager Appliance performance. Deploy maximum of four Access Manager Appliance virtual machines on a single piece of hardware. When you start deploying more than four, components of Access Manager Appliance start competing with each other for same hardware resources at the same time. You can include other types of services that the machine can support if they do not use the same hardware resources that Access Manager Appliance components use.

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

Using a Network Adapter for VMWare ESX

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

2.1.6 Network Requirements

Your network environment must meet the following requirements:

- A server configured with an LDAP directory (eDirectory 8.8.8, 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.
- Static IP addresses for each Access Manager Appliance. If the IP address of the machine changes, Access Manager Appliance components cannot start.
- Domain name server, which resolves DNS names to IP addresses and that has reverse lookups enabled.

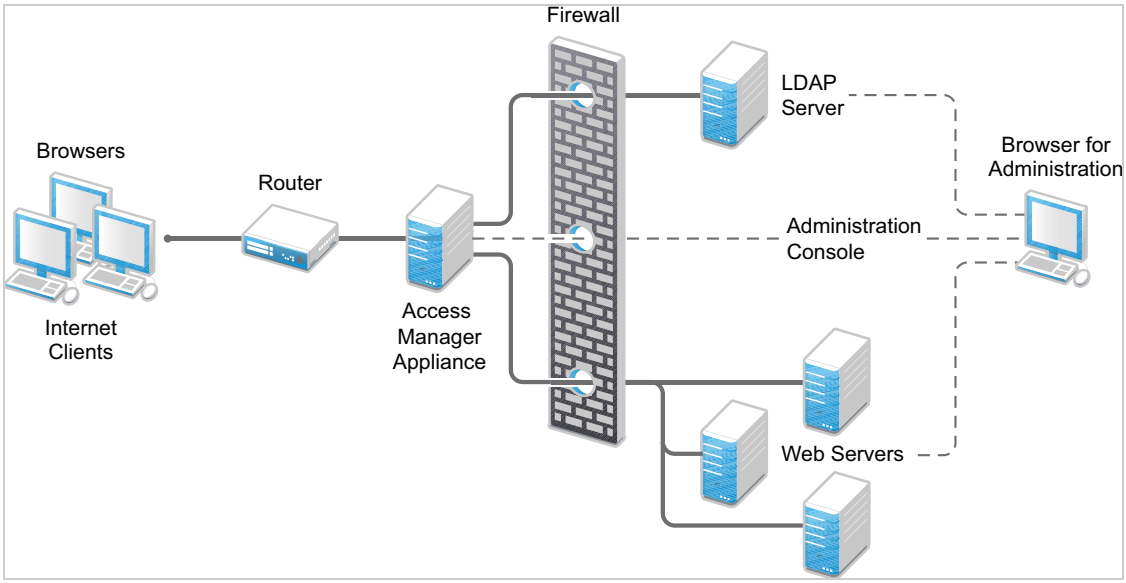
  Access Manager Appliance components know each other by their IP addresses. Some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If the reverse lookups are not available, host table entries can be used.
- Network time protocol (NTP) server 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.

2.1.7 Basic Setup

Figure 2-1 illustrates the basic Access Manager Appliance installation, where Access Manager Appliance is installed outside your firewall. The figure provides an overview of the flexibility built into Access Manager Appliance. You can use it to design a deployment strategy that fits the needs of your company.

Figure 2-1 *Basic Configuration*



For more information, see Section 2.2.2, “Installing Access Manager Appliance,” on page 33.

The firewall protects the LDAP server, which contains a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. This is a tested and recommended configuration. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Access Manager Appliance.

2.2 Installing Access Manager Appliance

Installation time: 45 to 90 minutes, depending on the hardware.

What you need to know	◆ Root password of Access Manager Appliance. ◆ Username and password of the Administration Console administrator. ◆ Static IP address for Access Manager Appliance. ◆ 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 tree for the configuration store is named after the server on which you install Access Manager Appliance. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

Access Manager Appliance can be installed on all supported hardware platforms for SLES 11 SP2 and SP3 (64-bit).

2.2.1 Prerequisites

- ❒ Ensure that you have backed up all data and software on the disk to another machine. The Access Manager Appliance installation completely erases all the data on your hard disk.
- ❒ Ensure that the machine meets the minimum hardware requirements. See Section 2.1, "Installation Requirements," on page 29.
- ❒ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the *Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

2.2.2 Installing Access Manager Appliance

Access Manager 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`.

NOTE: Do not install or import any non- 4.0 Appliance devices during installation.

Access Manager 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 Manager Appliance CD into the CD drive.

   The boot screen appears.
2. By default, the **Boot From Hard Disk** option is selected in the boot screen.

   Use the Down-arrow key to select **Install Appliance**.
3. Press Enter.
4. Review the agreement on the License Agreement page, then click **I Agree**.
5. Select the region and time zone on the Clock and Time Zone page.
6. Click **Next**.
7. Configure the details on the Appliance Configuration page:

Field	Description
Host Name	The hostname for the Access Manager Appliance machine.
Domain Name	The domain name for your network.
Public IP	Configure the following options for the public IP: ◆ **IP Address:** The public IP address of Access Manager Appliance. ◆ **Subnet Mask:** The subnet mask of Access Manager Appliance. ◆ **Default Gateway:** The IP address of the default gateway.
Private IP	Configure the following options for the private IP. This is an optional configuration. If this is configured, the Administration Console listens on this IP. ◆ **IP Address:** Private IP address of Access Manager Appliance. ◆ **Subnet Mask:** Subnet mask of Access Manager Appliance. ◆ **Gateway:** IP address of the gateway.
DNS Server 1	IP address of your DNS server. You must configure at least one DNS server.
DNS Server 2	IP address of your additional DNS server. This is an optional configuration.
In the Root Password section, specify password for the `root` user and name of the NTP server.	

8. Click **Next**.

Configure the following details under the Administration Console Configuration:

Field	Description
Primary	Deselect this option to specify if this Access Manager Appliance is not primary. If you are installing it as a secondary Access Manager Appliance then ensure that the primary Access Manager Appliance is reachable.
Admin Console IP	Specify the IP address of the primary Access Manager Appliance if this is secondary.
Username	The name of the Administration Console user. **NOTE:** The Administration Console username does not accept special characters # (hash), & (ampersand), and ( ) (round brackets).
Password	Specify and confirm the password for the user. **NOTE:** The Administration Console password does not accept special characters : (colon) and " (double quotes).

9 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.

Do not change the software selections listed on this screen.

10 (Optional) To modify the installation settings for partitions, click **Change**.

11 Click **Install** > **Install**.

This process might take 45 to 90 minutes depending on the configuration and hardware.

The machine reboots after the installation is completed. It runs an auto configure script, and then the Access Gateway and Identity Server components are configured.

12 (Optional) Verify if Access Manager Appliance is installed and configured successfully.

Log in to the Administration Console. See Section 2.2.4, “Logging In to the Administration Console,” on page 37), 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.

The Access Gateway health is displayed as green. The configuration takes care of establishing a trust relationship between an embedded service provider and the Access Gateway and also the trust relationship with the Identity Server before you proceed with any other configuration.

12a In a browser, enter the Access Manager Appliance URL. The Access Manager Appliance URL is formed by using the Host Name and Domain Name provided in the Step 8. For example, if the host name is `accessapp` and the domain name is novell.com, then the URL will be `https://accessapp.novell.com`/portal/. You will be redirected to the Sample Portal Page.

12b Click the Administration Console link and log in to.

12c Click **Devices** > **Identity Servers**. The Servers tab displays `IDP-Cluster` with one Identity Server. The IP Address of the Identity Server is same as the Access Manager Appliance IP Address. The health of both the IDP-Cluster and Identity Server should display green.

12d Click **Devices**> **Access Gateways**. The Servers tab displays AG-Cluster with one Access Gateway. The IP Address of the Access Gateway is same as the Access Manager Appliance IP Address. The health of both the AG-Cluster and Access Gateway should display green.

12e Click **Devices** > **SSL VPN**.

12f Install `novl-sslvpn-hb-key-3.1.0-0.noarch.rpm` and then configure the SSL VPN cluster manually.

NOTE: Restarting the appliance will turn off the portal Web server. If you want to start the portal application, use the `/opt/novell/nam/namportal/bin/startNP.sh` command.

13 Continue with one of the following sections:

Section 2.2.3, “Removing the Landing Portal,” on page 36

“Setting up User Stores for Identity Server Configuration” and Configuring the Access Gateway in the NetIQ Access Manager Appliance 4.0 SP1 Setup Guide.

2.2.3 Removing the Landing Portal

The landing portal is enabled by default during the installation of Access Manager Appliance. This portal is a single place for launching Administration Console and Access Manager Appliance help. The portal also has a sample application, which can be configured to start learning Access Manager capabilities. You can experiment with the portal as long as it is not in production. Remove the landing portal because it is visible for the users.

Perform the following steps to remove the landing portal after you have verified all your configurations in a staging environment:

1 In the Administration Console, click **Access Gateway** > **Cluster** > **Edit** > **NAM - RP.**

2 Select the **namportal** path based service.

3 Click **Delete**.

4 Click **Protected Resources**.

Delete the following protected resources:

- portal
- portal_public

5 Click **OK** > **Update**.

6 In the Administration Console, click **Devices** > **Identity Servers** > **Servers** > **Edit** > **Roles**.

7 Select the role policy check box, select the role role_assignment from the Roles Policy List, then click **Disable**.

8 Click **OK** > **Update**.

9 To remove the portal web application from the Access Manager Appliance filesystem, perform the following steps:

9a Log in to Access Gateway Appliance using any SSH client (for example, SSH in Linux and PuTTY in Windows).

9b Remove the portal using the `removeNP.sh` script available at `/opt/novell/nam/namportal/bin`.

10 The portal creates two default users Alice and Bob in the Appliance Configuration store.

You can remove the users by performing the following steps:

10a In the Administration Console, click **Roles and Tasks** > **Users** > **Delete User**.

10b In the Delete User page, specify the Object Name as bob.novell to delete Bob and alice.novell to delete Alice.

10c Click **Ok**.

NOTE: Optional: You can delete basic authorization, fill allowance, fillRole, and role assignment policies on the Policies page.

2.2.4 Logging In to the Administration Console

The Administration Console supports the following Web browsers:

- Microsoft Internet Explorer 8.*x* or higher
- Mozilla Firefox

WARNING: The Administration Console is a combination of iManager and a device manager. It has been customized for Access Manager Appliance so that it can manage the Access Manager Appliance 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 Appliance schema, which can prevent you from managing the Access Manager Appliance 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 to:

1. Enable browser pop-ups.
2. From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

   If the hostname of your Access Manager Appliance is www.host.com, you would enter `http://www.host.com:8080/nps`.
3. Click **OK**. You can select either the permanent or temporary session certificate option.
4. Specify the administrator name and password that you defined during installation and click **Login**. Access Manager Appliance Dashboard opens.

   For more information about this view or about configuring the Administration Console for Access Manager Appliance 4.0 view, see “Configuring the Default View”in the NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide.

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

To understand the conventions of the Administration Console, see Section 2.2.5, “Administration Console Conventions,” on page 38.

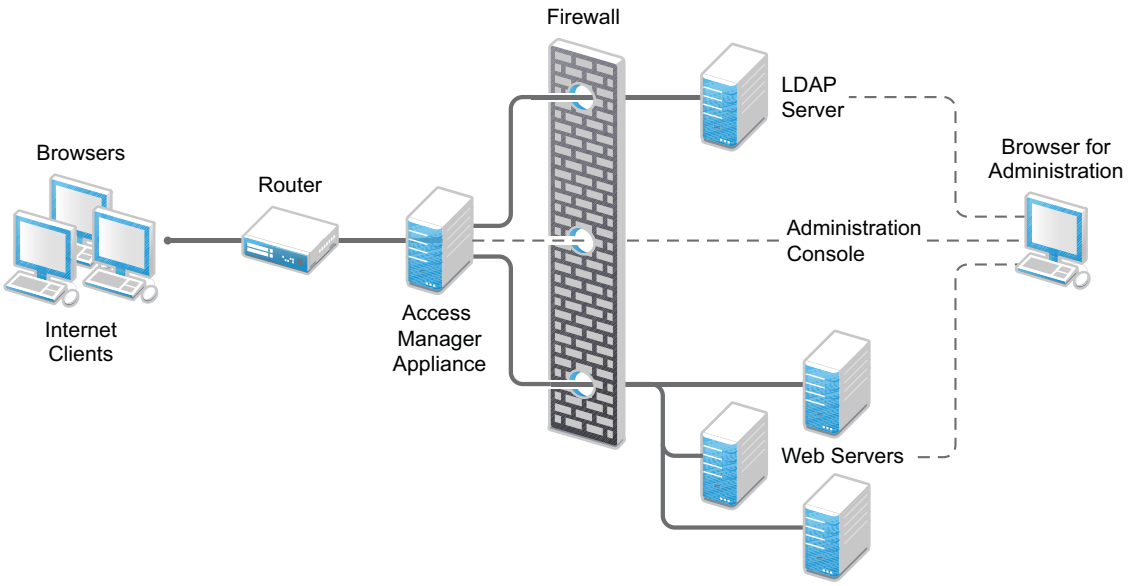
2.2.5 Administration Console Conventions

- 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.

3 Setting Up Firewalls

Access Manager Appliance should be used with firewalls. Figure 3-1 illustrates a simple firewall setup for a basic Access Manager Appliance configuration.

Figure 3-1 *Access Manager Appliance and Firewall*



The first firewall separates the Access Manager Appliance from the Internet, allowing browsers to access the resources through specific ports. This is one of many possible configurations. This section describes the following:

- Section 3.1, “Required Ports,” on page 39
- Section 3.2, “Restricted Ports,” on page 41
- Section 3.3, “Sample Configurations,” on page 42

3.1 Required Ports

The following table lists the ports that need to be opened when a firewall separates Access Manager Appliance from Internet.

With these tables, you should be able to place Access Manager Appliance of your system anywhere within your existing firewalls and know which ports need to be opened in the firewall.

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time synchronized else the authentication fails. We highly recommend that all components be configured to use an NTP (network time protocol) server. Depending upon where your NTP server is located in relationship to your firewalls, you might need to open UDP 123 so that the Access Manager component can use the NTP server.
DNS Servers	UDP 53	Access Manager components must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53 so that the Access Manager component can resolve DNS names.
Remote Linux Administration Workstation	TCP 22	If you use SSH for remote administration and want to use it for remote administration of Access Manager components, you need to open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.
Access Manager Appliance	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from the devices to the Administration Console.
	TCP 1289	For communication from the devices to the Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
	TCP 636	For secure LDAP communication from the devices to the Administration Console.
	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for secure LDAP communication.
	TCP 8080, 8443	Used for Tomcat communication.
LDAP User Store	TCP 524	Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. It is not used in day-to-day operations.

Component	Port	Description
Browsers	TCP 8080	For HTTP communication from browsers to the Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from browsers to the Administration Console.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.
	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to the Web servers. This is configurable.

NOTE: On SLES 11, you can edit this file or use YaST to configure UDP ports and internal networks.

3.2 Restricted Ports

The following ports are reserved for internal use only and other applications should not use these ports:

22
111
524
1443
2443
3443
8028
8030
8080
8443
8444
9000
9001
55982
61222
61613
61616
61617

If required, use port redirection by using IP tables.

3.3 Sample Configurations

- Section 3.3.1, “Access Manager Appliance in DMZ,” on page 42

3.3.1 Access Manager Appliance in DMZ

- “First Firewall” on page 42
- “Second Firewall” on page 42

First Firewall

If you place a firewall between browsers and Access Manager Appliance, you need to open ports so that browsers can communicate with the Access Gateway and the Identity Server and the Identity Server can communicate with other identity providers.

See, Figure 3-1 on page 39

Table 3-1 *Ports to Open in the First Firewall*

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	
TCP 8080	For HTTP communication with the Identity Server.
TCP 8443	For HTTPS communication with the Identity Server.
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.

SSL VPN needs the following port opened on the first firewall if clients are accessing SSL VPN directly:

Table 3-2 *Ports to Open in the First Firewall for SSL VPN*

Port	Purpose
TCP 7777	For client communication. This is the default port, but it can be configured to use TCP 443.

Second Firewall

The second firewall separates Web servers, LDAP servers, and the Administration Console from the Identity Server and the Access Gateway. You need the following ports opened in the second firewall:

Table 3-3 *Ports to Open in the Second Firewall*

Port	Purpose
TCP 80	For HTTP communication with Web servers.
TCP 443	For HTTPS communication with Web servers.
Any TCP connect port assigned to a Web server or to a tunnel.	
TCP 1443	For communication from the Administration Console to the devices.
TCP 8444	For communication from the devices to the Administration Console.
TCP 1289	For communication from the devices to the Audit server installed on the Administration Console. If you do not enable auditing, you do not need to open this port.
TCP 524	For NCP certificate management in NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
TCP 636	For secure LDAP communication of configuration information.

You need to open ports on the second firewall according to the offered services.

Table 3-4 *Ports to Open in the Second Firewall for SSL VPN*

Port	Purpose
TCP 22	For SSH
TCP 23	For Telnet

4 Upgrading Access Manager Appliance

This section discusses about how to upgrade the Access Manager Appliance to a higher version. When you upgrade the Access Manager Appliance, start the process by first backing up your configuration. For instructions, see "Backing Up the Access Manager Appliance Configuration" in the *NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide*. This is useful in case upgrade fails and you need to recover your previous configuration. For more information, see "Restoring the Access Manager Appliance Configuration" in the *NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide*.

- Section 4.1, "Upgrading from the Evaluation Version to the Purchased Version," on page 45
- Section 4.2, "Upgrading Access Manager Appliance 3.2 SP2, 4.0 to 4.0 SP2," on page 46
- Section 4.3, "Applying Access Manager Appliance 4.0 Hotfix* Patch," on page 46
- Section 4.4, "Configuring the Access Manager Appliance User Portal," on page 49

4.1 Upgrading from the Evaluation Version to the Purchased Version

1. Log in as `root`.
2. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file by using the following command: `tar -xzvf <filename>`
3. Change to the directory where you extracted the file, then run the following command:

   ```
   ./sb_upgrade.sh
   ```
4. The system displays a message regarding restoring customized files.

   For more information about how to sanitize jsp pages, see "Preventing Cross-site Scripting Attacks" in the NetIQ Access Manager Appliance 4.0 Identity Server Guide.
5. A confirmation message is displayed.

   ```
   Would you like to continue this upgrade?
   ```

   Type **Y** to continue.
6. Enter the Access Manager Administration Console user ID.
7. Enter the Access Manager Administration Console password.
8. Re-enter the password for verification.

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

   ```
   Upgrade completed successfully.
   ```

NOTE: Installing patches are not supported on the evaluation version. To install patches, upgrade to the licensed version using information at Upgrading from the Evaluation Version to the Licensed Version (https://www.netiq.com/documentation/netiqaccessmanager4_appliance/target_installation/data/b16jpw50.html)

4.2 Upgrading Access Manager Appliance 3.2 SP2, 4.0 to 4.0 SP2

Prerequisite: Before upgrading Access Manager Appliance from 3.2 SP2 and 4.0 to 4.0 SP2, perform the following:

1. Before upgrading to 4.0 SP2, you must first upgrade the base operating system of the 4.0 Access Gateway appliance to the latest operating system that is included in the 4.0 SP2 Access Gateway appliance ISO. For more information about how to upgrade, see Section 5.3, “Upgrading the Operating System for Access Manager Appliance,” on page 54.
2. Follow the procedure given below to upgrade the Access Manager Appliance.

NOTE: If you do not upgrade the base operating system before upgrading to 4.0 SP2, upgrade will display an error message and terminates.

Perform the following steps to upgrade Access Manager Appliance.

1 Log in as `root`.

2 Change to the directory where you extracted the file, then run the following command:

```
./sb_upgrade.sh
```

3 A confirmation message is displayed.

```
Would you like to continue this upgrade?
```

Type **Y** to continue.

4 The system displays a message regarding restoring customized files:

```
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?
```

Type **Y** to confirm.

For more information about how to sanitize jsp pages, see “Preventing Cross-site Scripting Attacks” in the NetIQ Access Manager Appliance 4.0 Identity Server Guide.

5 Enter the Access Manager Administration Console user ID.

6 Enter the Access Manager Administration Console password.

7 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

4.3 Applying Access Manager Appliance 4.0 Hotfix* Patch

You can upgrade Access Manager 4.0 to 4.0 Hotfix by applying the Hotfix patch.

NOTE: Hotfix* is used to represent the hotfix number released for Access Manager Appliance 4.0.

Installing patches are not supported on the evaluation version. To install patches, upgrade to the licensed version using information at Upgrading from the Evaluation Version to the Licensed Version (https://www.netiq.com/documentation/netiqaccessmanager4_appliance/target_installation/data/b16jpw50.html)

The patch helps you upgrade to the latest Access Manager Appliance patches with ease. Instead of downloading tar files that contain the entire set of binaries, you can download a `.zip` file that contains incremental changes in form of a patch file. You can use this patch file to update all components of your Access Manager Appliance.

IMPORTANT: In a cluster setup, ensure that you install the patch on each node of the Access Manager Appliance setup.

4.3.1 Prerequisites

Ensure that you have installed the latest version of the product. Refer to the following readmes for verifying the version numbers of a specific Hotfix release:

- Access Manager Appliance HF1 Readme
- Access Manager Appliance HF2 Readme
- Access Manager Appliance HF3 Readme

4.3.2 Installing the Patch

Perform the following steps before applying the patch:

1. Save the hotfix file to the server running Access Manager Appliance. If you have multiple servers in your set up, ensure that you copy this `.zip` file to all the servers.
2. Extract the patch file by using the `unzip <patch name>.zip` command.

   After extraction, the following files and folders are created in the <*patch name*> folder:

File/Folder Name	Description
`rpm`	Contains rpm files for the patch to run on a Linux server.
`Patchtool`	Contains logging properties file and files necessary for the patch to run on a Windows server.
`installPtool.sh`	Script to install the patch and the patch tool on a Linux server.
`installPatch.sh`	Script to install the HF patch tool and the updated binaries on a Linux server.
`installPtool.cmd`	Script to install the patch on a Windows server.
<*patch name*>-*xxx*.patch	The patch file. The name of the patch file changes for each HF release. **NOTE:** xxx represents the build number which is available in the respective release readme.

3. Log in as the root user.

4 Go to the location where you have extracted the patch files.

5 Run the `sh installPatch.sh` command.

This command installs the patch and the bundled binaries.

TIP: To manage the Access Manager Appliance patch file, go to `/opt/novell/nam/patching/bin` folder.

If the patch is already installed, the installer exits with a message.

4.3.3 Administering Patches

1. After the patch is installed, go to the `/opt/novell/nam/patching/bin` folder.
2. Use the following options to administer the Access Manager Appliance patch file.

NOTE: xxx represents the build number which is available in the respective release readme.

Option	Description	Command on Linux server
`-qa`	Lists all installed patches.	`./patch -qa`
`-q`	Lists the details of an installed patch.	`./patch –q` Example: If you have installed <*latest release patch name*>, use the following command: `./patch –q HF*-xxx`
`-i`	Installs a patch. During installation of a patch, all running services are stopped temporarily. After a patch is installed, all services are restarted and details of the operation are written to log files.	`./patch –i <location and patch name>` Example: `./patch –i /tmp/AM_400_HF*-xxx.patch`
`-e`	Removes an installed patch. The patch maintains content relationship among patches. So, if you have installed patch 1 and patch 2, patch 1 cannot be removed without removing patch 2. This is because patch 2 contains details of patch 1 as well. During the patch process, all running services are stopped temporarily.	`./patch –e <patch name>` Example: `./patch –e HF*-xxx`
`-qpl`	Lists details of a patch that is not installed. If you want to view the changes that are included in the patch file without installing it on your server, use this option	`./patch –qpl <location and patch name>` Example: `./patch –qpl /tmp/AM_400_HF*-xxx.patch`

Option	Description	Command on Linux server
`-v`	Verifies integrity of a patch.	`./patch –v <location and patch name>` Example: `./patch –v /tmp/AM_400_HF*-xxx.patch`
`-t`	Verifies if services can be restored by the installer.	`./patch –t <location and patch name>` Example: `./patch –t /tmp/AM_400_HF*-xxx.patch`

4.4 Configuring the Access Manager Appliance User Portal

After upgrading Access Manager Appliance, use the following procedure to access the user portal:

1. In the Administration Console, go to **Access Gateways** > **Edit** > **NAM-RP**.
   - **1a** Click **Protected Resources** and select **portal** from the list.
   - **1b** Click **New** and add a new `/portal/users` in the **URL Path**.
2. Click **Web Server Addresses** for the namportal in the **Proxy Service List**.
   - **2a** Disable the option **Connect Using SSL**.
   - **2b** Change **Connect Port** from 80 to 8020.
3. Apply the changes.

NOTE: Restarting the Appliance will turn off the portal Web server. If you want to start the portal application, use the `/opt/novell/nam/namportal/bin/startNP.sh` command.

5 Upgrading Kernel to the Latest Linux Security Patch

Prerequisites

- ❒ Access Manager 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.
- ❒ Ensure that you have obtained the activation code for Access Manager Appliance from Novell Customer Center.

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.

- Section 5.1, “Installing or Updating Security Patches for Access Manager Appliance,” on page 51
- Section 5.2, “Configuring the Subscription Management Tool for Access Manager Appliance,” on page 52
- Section 5.3, “Upgrading the Operating System for Access Manager Appliance,” on page 54

5.1 Installing or Updating Security Patches for Access Manager Appliance

To get the latest security updates for Access Manager 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 `NAM4x-APP-Updates` was created:

```
zypper lr
```

An output similar to the following appears

```
# | Alias                                  | Name
| Enabled | Refresh
--+----------------------------------------+-----------------------------------
1 | NetIQAccessManagerAppliance-4.x.x-x | NetIQAccessManagerAppliance-4.x.x-x
| Yes     | No
2 | nu_novell_com:NAM4x-APP-Updates      | NAM4x-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.

5.2 Configuring the Subscription Management Tool for Access Manager Appliance

Access Manager 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 about configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

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

- Section 5.2.1, “SMT Configuration,” on page 52
- Section 5.2.2, “Troubleshooting,” on page 53

5.2.1 SMT Configuration

You must configure the SMT server and set up subscription for `NAM4x-APP-Updates` channel to receive the updates for Access Manager Appliance.

1 Install the SMT server in a SLES 11 Server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

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 `NAM4x-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 *NAM4x-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 Manager 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.

5.2.2 Troubleshooting

If you face issues while using the activation code to register, see Resetting your ZEN Updater and Novell Customer Center Key Registration.

5.3 Upgrading the Operating System for Access Manager Appliance

The Access Manager appliance bundles the latest SUSE kernel. During fresh installation of Access Manager appliance, the latest kernel will be installed automatically. While upgrading, you must upgrade the base operating system before upgrading the Access Manager appliance. Perform the following steps to upgrade the base operating system.

1. Get the Access Manager 4.0 SP1 appliance ISO and mount it in the Access Manager server where you want to upgrade. For example, if you want to mount on `/root/iso`, use the following command.

   ```
   mount -o loop /dev/dvd /root/iso/
   ```

   NOTE: Create `/root/iso` using `mkdir -p /root/iso` command before executing the above command.

2. Use the following command to add the mounted ISO as the upgrade repository.

   ```
   zypper ar /root/iso/ 40appiso
   ```

3. Refresh the new repository using the following command.

   ```
   zypper ref
   ```

4. Use the following command to upgrade the base operating system from the repository you added.

   ```
   zypper dup --from 40appiso
   ```

5. You will be prompted a dependency resolution for usbutils. Select **1** from the solutions.
6. Accept the license. The operating system will start upgrading.
7. After upgrade, view the notification.
8. Restart the Access Manager Appliance server.

A Troubleshooting Installation

- Section A.1, “Checking the Installation Logs,” on page 55
- Section A.2, “Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation,” on page 56
- Section A.3, “Installation Through Terminal Mode is not Supported,” on page 56
- Section A.4, “Novell Device Manager Installation Fails During the Appliance Installation,” on page 56
- Section A.5, “Access Manager Appliance Installation Fails Due to an XML Parser Error,” on page 56
- Section A.6, “DN Is Added as Provider ID While Installing NMAS SAML Method,” on page 57
- Section A.7, “Portal Web Server is not Accessible,” on page 57
- Section A.8, “Installing RHEL on the Administration Console Fails if IPv6 is Disabled,” on page 57

A.1 Checking the Installation Logs

If Access Manager Appliance fails to install, check the 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.

Log File	Description
`install_main_2011-06-06_17:28:19.log`	Contains messages generated for installing and configuring Access Manager Appliance.
`iinstall_edir_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring the Administration Console configuration store.
`install_audit_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring NetIQ Auditing components.
`Novell_iManager_2.7_InstallLog.log`	Contains messages generated for installing and configuring iManager.
`install_iman_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring iManager.
`install_adminconsole_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring the Administration Console.
`install_jcc_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring the Communications module.
`install_mag_2011-06-06_17:38:37.log`	Contains messages generated for installing and configuring the Access Gateway.

Log File	Description
`install_idp_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring the Identity Server.
`configure_cluster_2011-06-06_17:28:19.log`	Contains messages generated for configuring Identity Server and Access Gateway.

A.2 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation

Installation of Access Manager Appliance might fail if some of the hardware drivers or network cards are not detected. If this happens, you must upgrade the hardware drivers manually:

1. Start the Access Manager Appliance installation.

   See Chapter 2, “Installing Access Manager Appliance,” on page 29.
2. Select **Kernel Module (Hardware Driver)** in the main menu, then click **OK**.
3. Select **Add Driver Update**, then click **OK**.
4. Select the driver update medium.

   The driver update medium can be CD-ROM or floppy disk.
5. Click **OK**.

   The hardware driver is updated.
6. Continue with the Access Manager Appliance installation.

A.3 Installation Through Terminal Mode is not Supported

Installation through terminal mode is supported on GUI mode only. To work around this issue, initiate the installation in the GUI mode. After entering the required input, switch to the terminal mode. The installation is completed successfully.

A.4 Novell Device Manager Installation Fails During the Appliance Installation

To workaround this issue, reinstall the appliance.

A.5 Access Manager 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.

A.6 DN Is Added as Provider ID While Installing NMAS SAML Method

While installing the NMAS SAML method in an external user store, DN is added as Provider ID instead of the metadata URL.

To resolve this issue, perform the following steps:

1. Log in to the Administration Console which has the external user store.
2. Go to **Roles and Tasks** > **NMAS** > **NMAS Login Methods** > **SAML Assertion** > **Affiliates**.
3. Select the respective Affiliate and change the provider ID to the identity provider metadata URL. For example, https://www.trunk2.com:8443/nidp/idff/metadata.

A.7 Portal Web Server is not Accessible

Restarting the appliance will turn off the portal Web server. If you want to start the portal application, use the `/opt/novell/nam/namportal/bin/startNP.sh` command.

A.8 Installing RHEL on the Administration Console Fails if IPv6 is Disabled

By default, IPv6 is enabled on RHEL 6.4. When IPv6 is partially disabled, eDirectory installation fails. You can disable IPv6 by adding the below entries to `/etc/sysctl.conf` file:

- `net.ipv6.conf.all.disable_ipv6 = 1`
- `net.ipv6.conf.default.disable_ipv6 = 1`

Use the `lsmod | grep ipv6` command to verify if some of the IPv6 modules are still running. If this command returns any output, proceed with the installation only after disabling it.