Installation Guide

Access Manager Appliance 3.2 SP3

August 2014

www.netiq.com/documentation

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About This Guide

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

Audience

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

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

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Access Manager Appliance Installation Guide*, visit the NetIQ Access Manager Appliance Documentation Web site (https://www.netiq.com/documentation/netiqaccessmanager32_appliance/).

Additional Documentation

- *NetIQ Access Manager Appliance 3.2 SP3 Administration Console Guide*

- *NetIQ Access Manager Appliance 3.2 SP3 Identity Server Guide*
- *NetIQ Access Manager Appliance 3.2 SP3 Access Gateway Guide*

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

1 NetIQ Access Manager Appliance Overview

NetIQ Access Manager Appliance is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager Appliance 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 brings up all components such as Access gateway, Identity Provider, Admin Console, and SSL VPN in a single machine. 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 3.2 SP3, see Access Manager Appliance 3.2 Service Pack 3 Readme.

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. Also, 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, whether those resources are Web applications, traditional server-based applications, or other content. If your business faces any of the following access-related challenges, Access Manager Appliance can help:

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

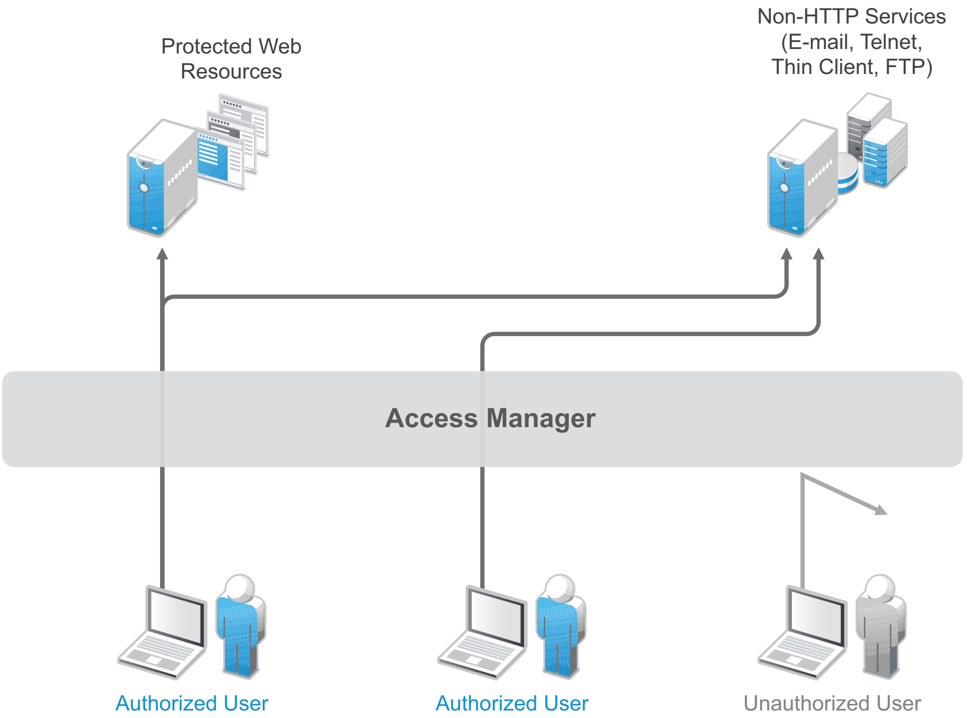
- Protecting users' privacy and confidential information as they access company resources or partners' resources.
- Proving compliance with your business policies, privacy laws such as Sarbanes-Oxley, HIPAA, or European Union, and other regulatory requirements.

The following sections expand on these challenges and introduce the solutions provided by Access Manager. If you are already aware of the business solutions provided by Access Manager, you might want to skip to the technical introduction provided in Section 1.2, "How Access Manager Appliance Works," on page 15.

- Section 1.1.1, "Protecting Resources While Providing Access," on page 8
- Section 1.1.2, "Managing Passwords with Single Sign-On," on page 9
- Section 1.1.3, "Enforcing Business Policies," on page 10
- Section 1.1.4, "Sharing Identity Information," on page 11
- Section 1.1.5, "Protecting Identity Information," on page 13
- Section 1.1.6, "Complying with Regulations," on page 14

1.1.1 Protecting Resources While Providing Access

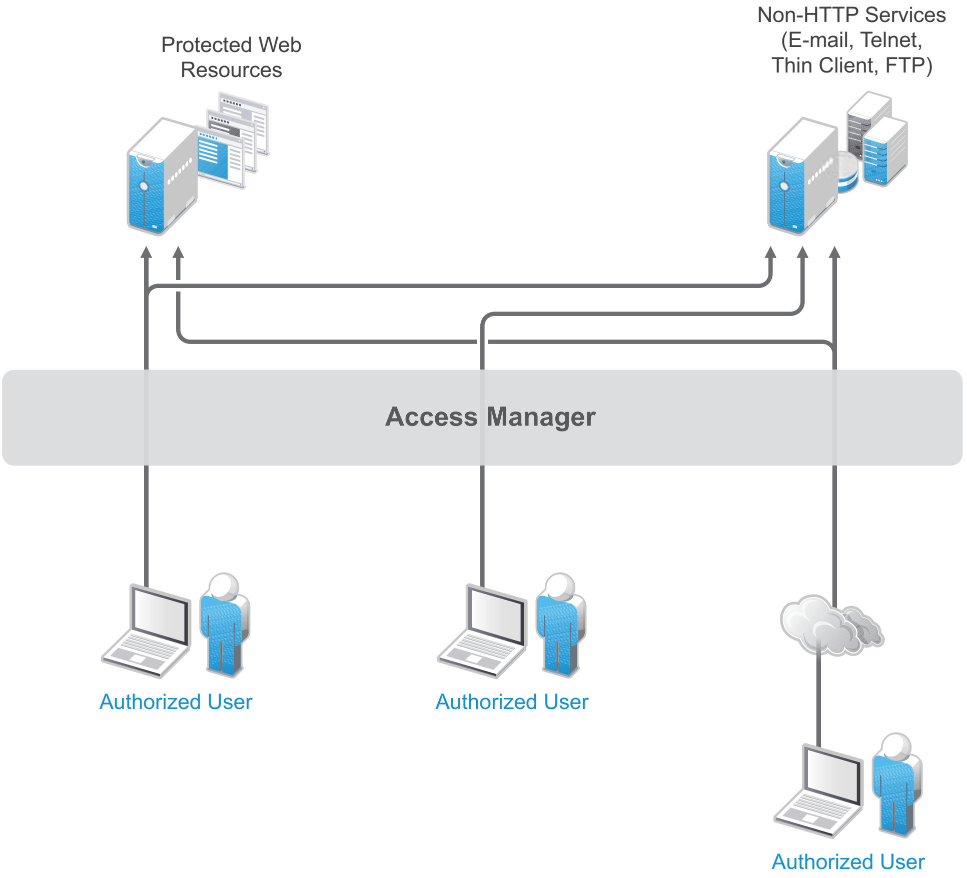
The primary purpose of Access Manager Appliance is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources as well as traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized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



Access Manager 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.

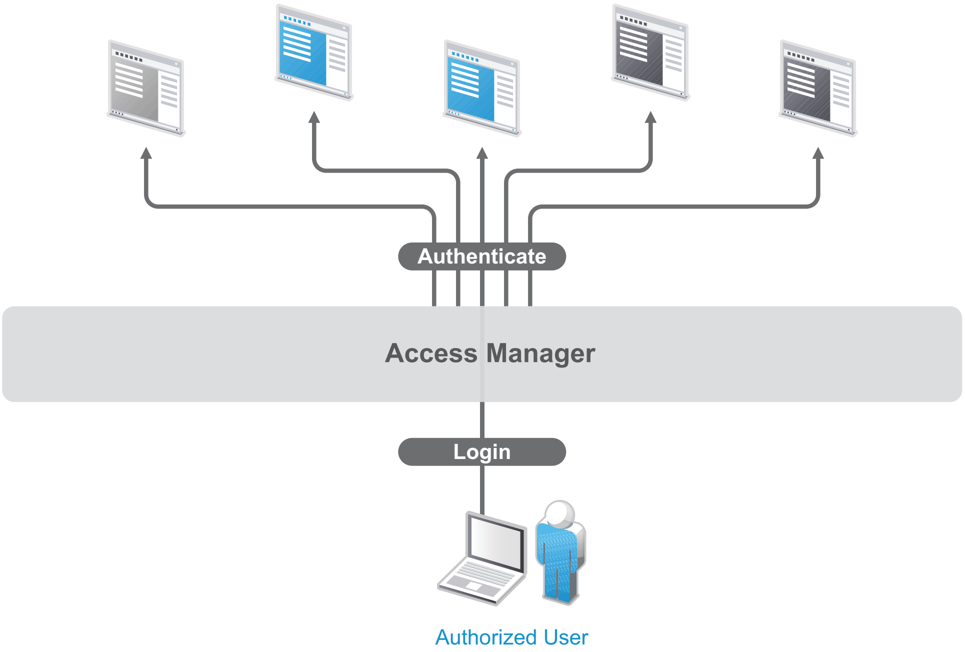
Because not all users work from within the confines of your local network, access to resources is independent of a user's location, as shown in the following illustration. Access Manager Appliance provides the same secure access and same experience whether the user is accessing resources from your local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

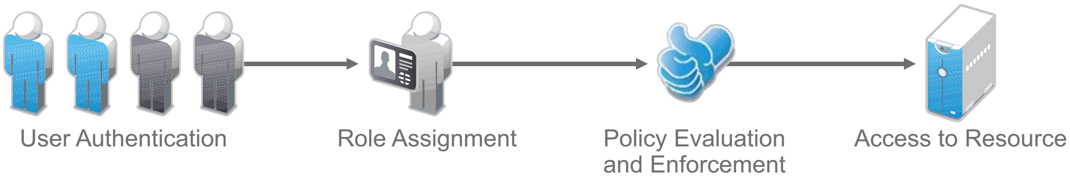


By simplifying the use and management of passwords, Access Manager Appliance helps you enhance the user's experience, increase security, streamline business processes, and reduce system administration and support costs.

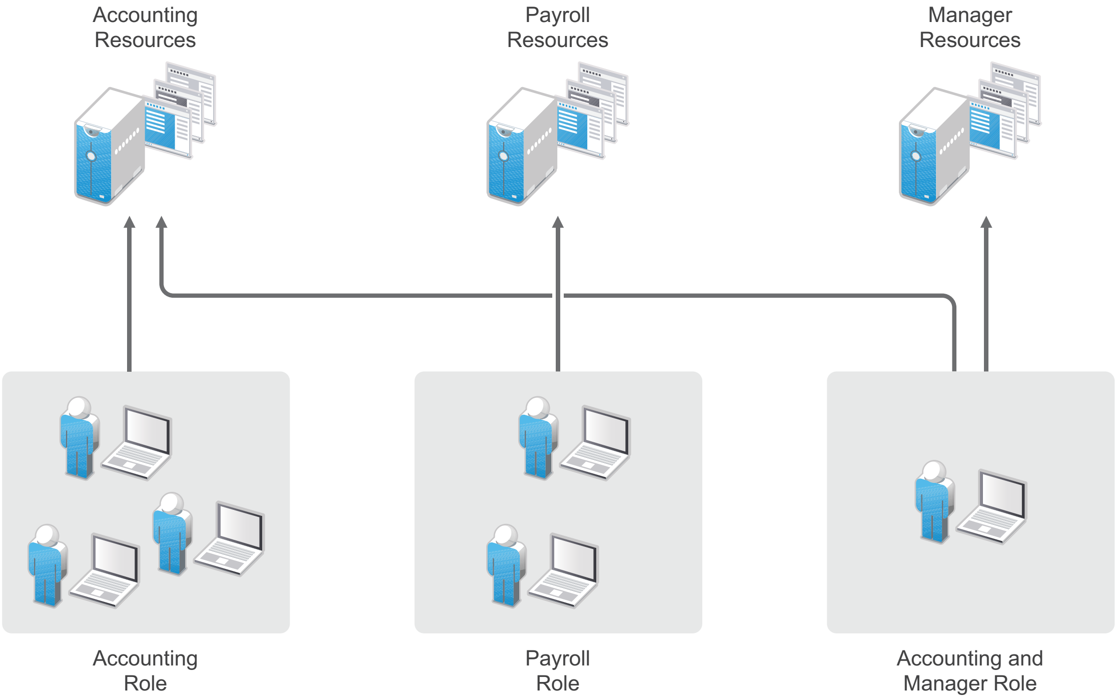
1.1.3 Enforcing Business Policies

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, 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.



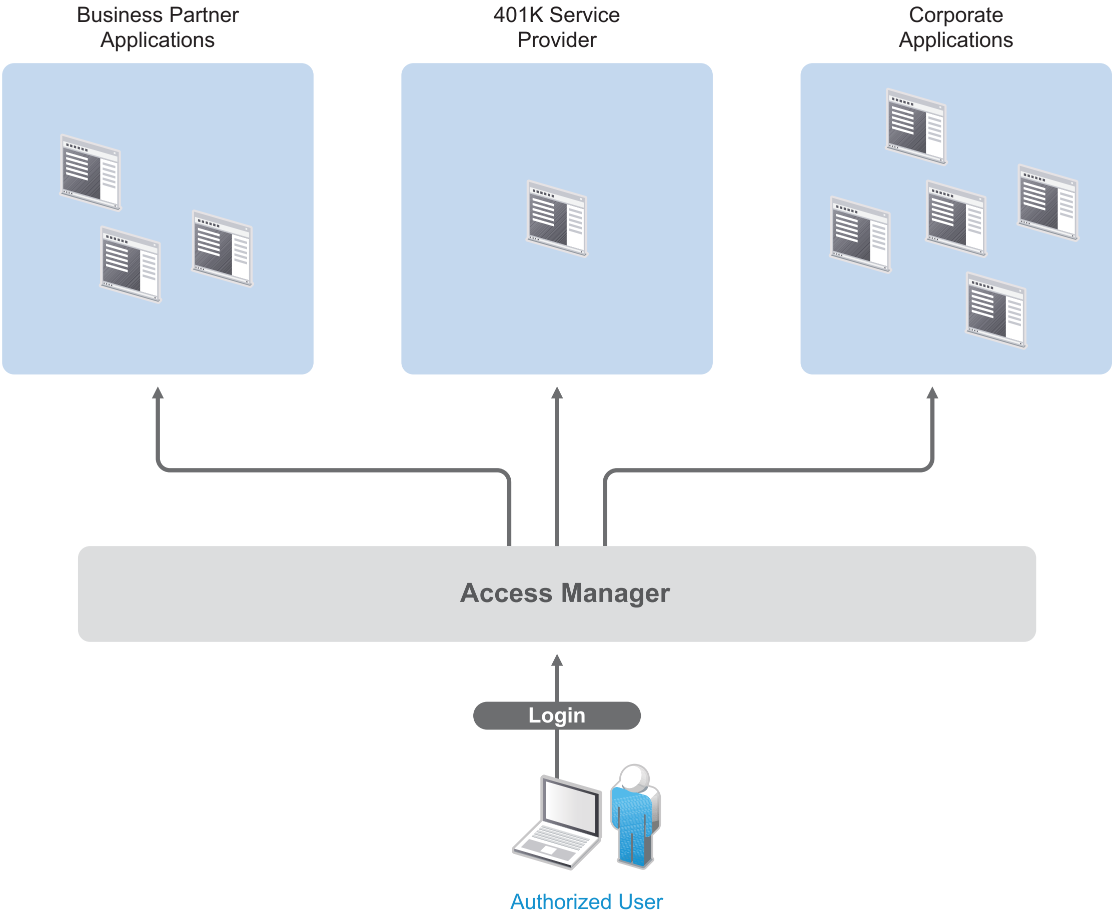
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

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 providing services to another business. Access Manager Appliance provides federated identity management to enable users to seamlessly and securely authenticate across autonomous identity domains.

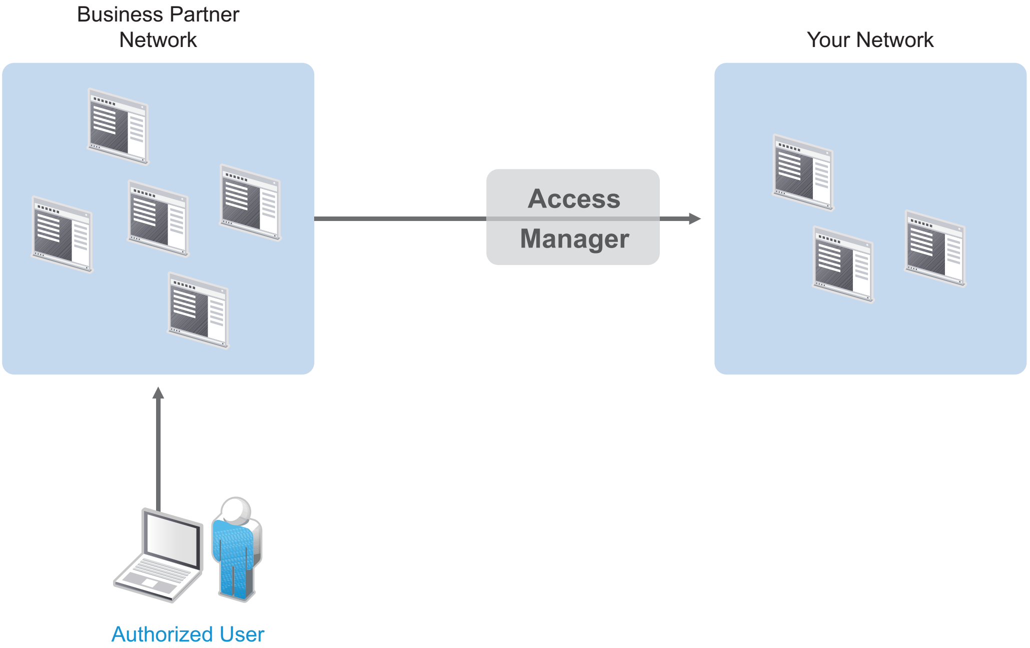
For example, assume that you have employees who need access to your corporate applications, several business partner’s applications, and their 401k service, as shown in the following figure.



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.



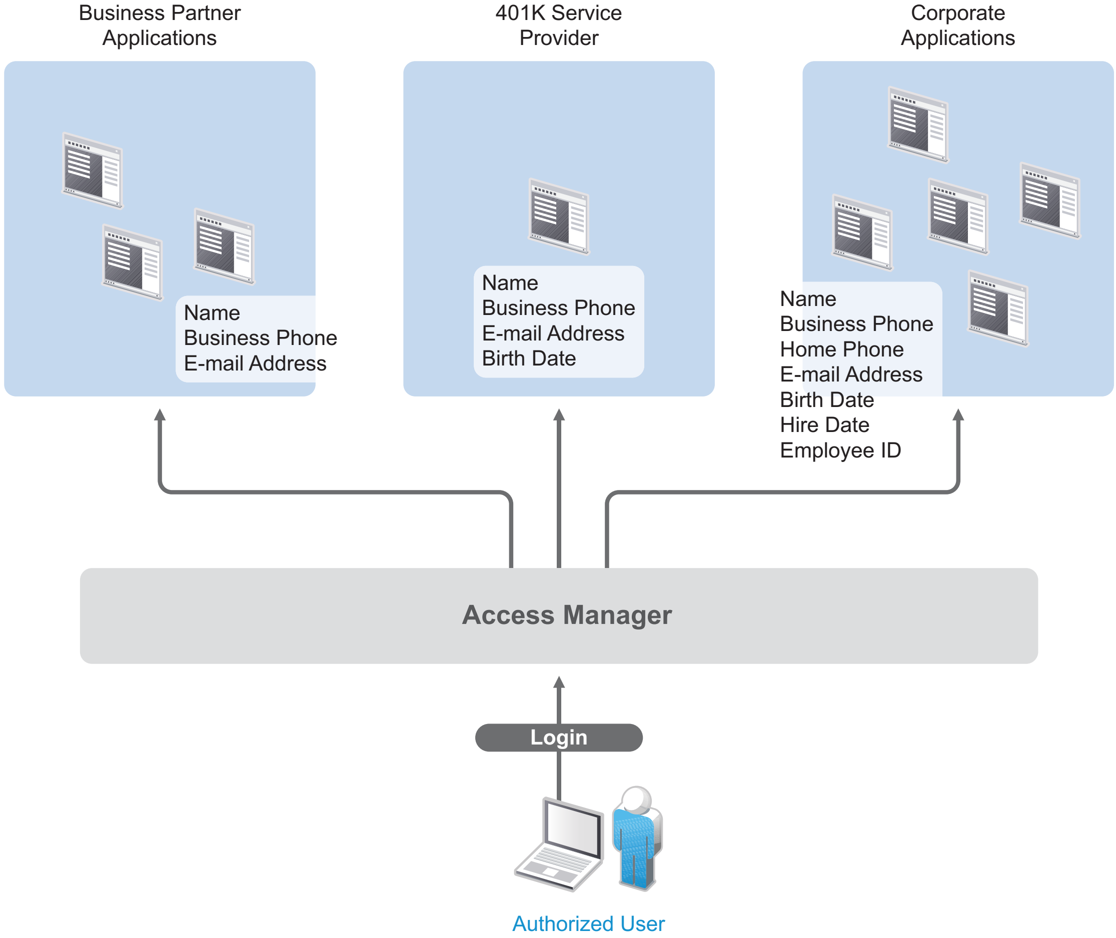
In addition to simply linking user accounts in different identity domains, Access Manager Appliance also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization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

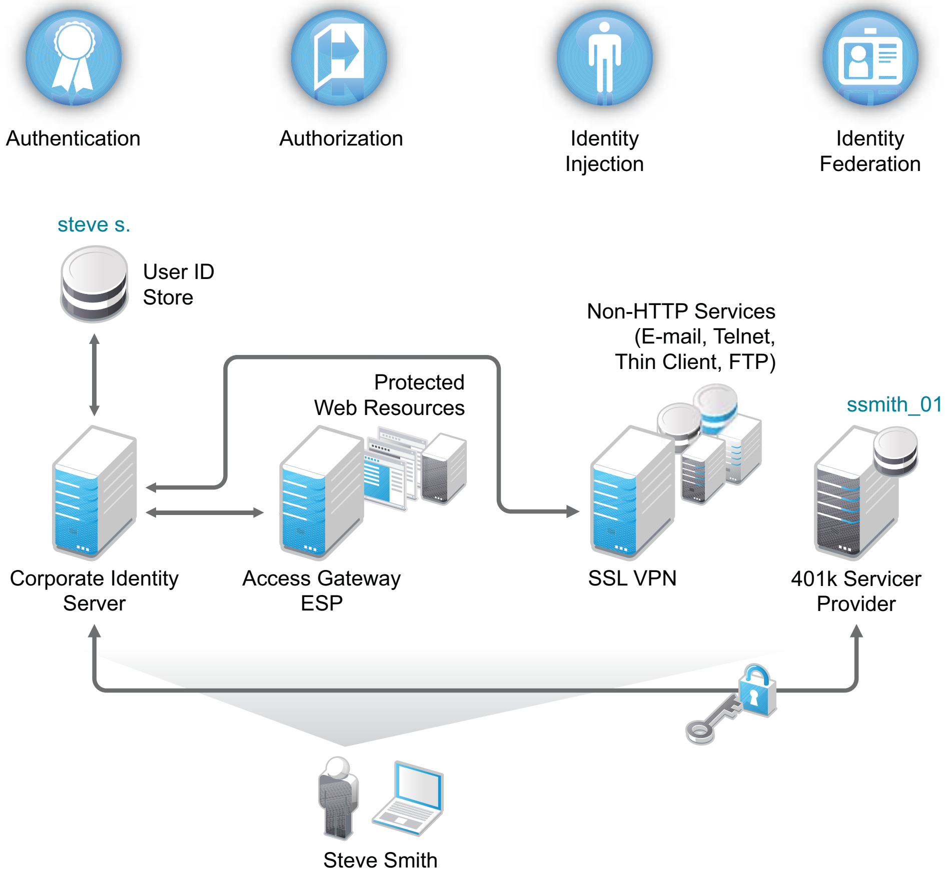
Specifically, Access Manager Appliance helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager Appliance can generate the 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. For non-HTTP services, Access Manager Appliance provides secure VPN.

Figure 1-1 illustrates the primary purposes of Access Manager: 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, 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.

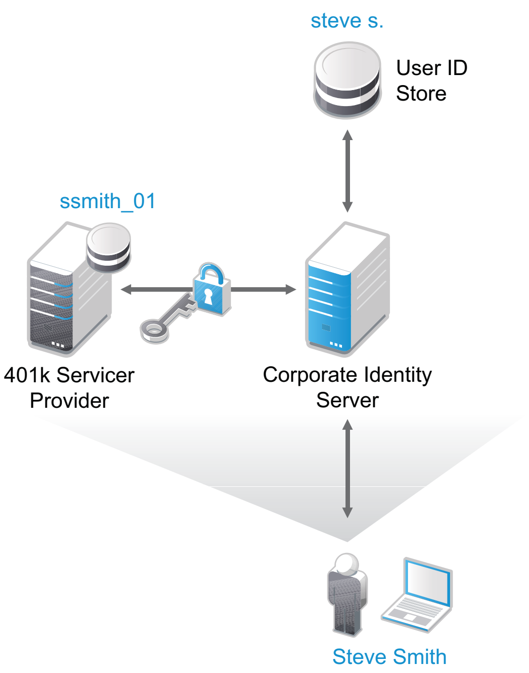
1.2.3 Identity Injection

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.

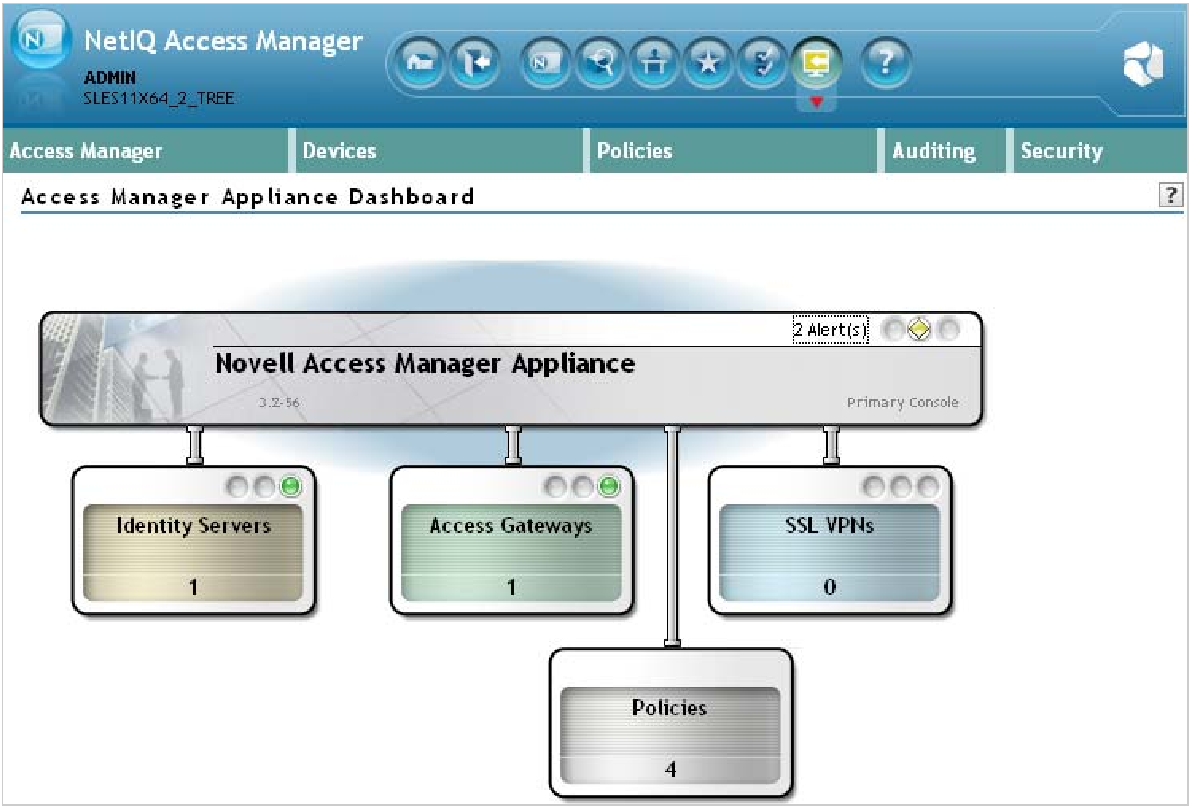
From an administrative perspective, this type of sharing reduces identity management costs, because multiple organizations do not need to independently collect and maintain identity-related data, such as passwords. From the end user’s perspective, this results in an enhanced experience by requiring fewer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

1.3 Access Manager Appliance Components and Their Features

1.3.1 Administration Console

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

Figure 1-3 *Access Manager Appliance Dashboard Page*



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

1.3.2 Identity Servers

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

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

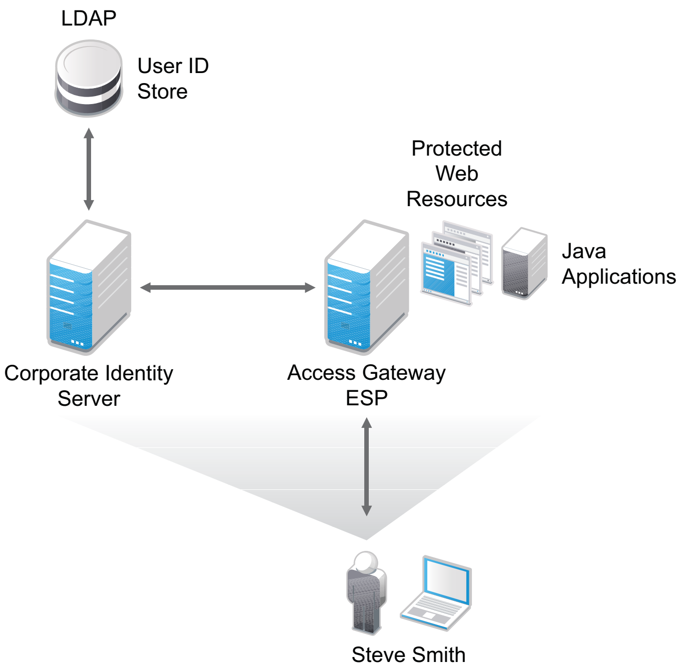
In an Access Manager Appliance configuration, the Identity Server is responsible for managing:

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

1.3.3 Access Gateways

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

Figure 1-4 Access Gateway Component



The Access Gateway is designed to work with the Identity Server to enable single sign-on to protected Web services. The following features facilitate single sign-on to Web servers that are configured to enforce authentication or authorization policies:

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

If your Web servers have not been configured to enforce authentication and authorization, you can configure the Access Gateway to provide these services. Authentication contracts and authorization policies can be assigned so that they protect the entire Web server, a single page, or somewhere in between.

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

The Access Gateway can be installed as a soft appliance (which includes the operating system) or as a service (which requires you to provide the operating system). For more information, see the *NetIQ Access Manager Appliance 3.2 SP3 Access Gateway Guide*.

1.3.4 SSL VPN

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

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

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

1.3.5 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 Manager Appliance. Additionally, authorization policies can be defined that control access to protected resources based on user and system attributes other than assigned roles.

The flexibility built into the policy component is nearly unlimited. You can, for example, set up a policy that permits or denies access to a protected Web site, depending on user roles (such as employee or manager), the value of an LDAP attribute, or the user’s IP address.

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

1.3.6 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 Access Manager Appliance, which in turn makes the certificates available for the Access Manager Appliance 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.

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 Auditing and Logging

Access Manager Appliance supports audit logging and file logging at the component level. To provide compliance assurance logging and to maintain audit log entries that can be subsequently included in reports, the Access Manager Appliance components can be configured to send their auditing events to an external Audit server like Sentinel Log Manager server or a Novell NSure Audit server. Each component creates assurance log entries to show the effect of each policy statement on each access control decision. Log entries include events such as notifications pertaining to the operational state of Access Manager Appliance components, the results of administrator and user requests, and policy actions invoked in determining request results.

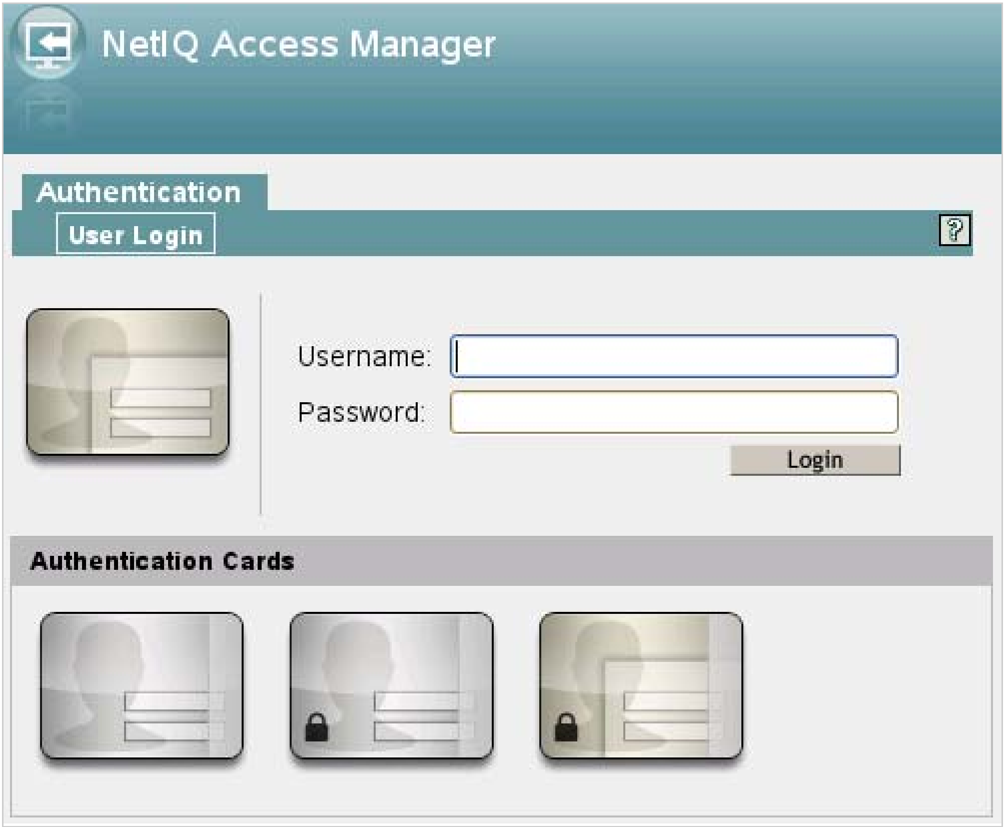
1.3.8 Embedded Service Provider

The Access Gateway, SSL VPN server 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 the SSL VPN server.

1.3.9 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.

Figure 1-5 *Access Manager User Portal*



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

1.3.10 Sample Application

The sample application is enabled by default during installation of the Access Manager Appliance. This application is a single place for launching the Administration Console and the Access Manager Appliance help. You can configure the application to learn and experiment the Access Manager Appliance quickly as long as it is not in production. We recommend you to remove the landing application because it is visible for the users.

The sample application demonstrates the following functionalities:

- Role based access control policies
- Automatic authentication header injection
- User attribute propagation using headers
- Automatically filling forms with authenticated user's attributes

The sample application includes a simple Payroll application, where users of role "Employee" and "Manager" can see and edit their basic information. Payroll information of each user is protected. Users with the “Employee” role cannot see the pay info of other users, unless they are assigned the role of "Manager."

By default, the Access Manager Appliance installation creates two users Alice with both “Manager” and “Employee” role and Bob with “Employee” role. Any request without basic authentication headers will be Forbidden. Any request without the required role will also be Forbidden. A default allowance is automatically filled in by Access Manager Appliance as defined in the fill_allowance policy while editing the pay info.

NOTE: A separate database is used for this demo application. The information you modify here does not modify the actual user store. You must remove the portal before moving to production. Also, delete the default users Alice and Bob or change the default password for these users. The default password is `novell`.

Removing the Portal

To remove the portal:

- Delete the proxy service associated with the portal. It is a path based proxy with name namportal.
- Delete the public and protected resources associated with this service. These resources are portal and portal_public.
- Change the default proxy service to point to the production Web server.
- Change the NAM-RP > NAM-Service target Web server to do this.

Steps:

1. Stop the Access Manager Appliance by running the `/etc/init.d/novell-appliance stop` command.
2. Go to the `/opt/novell/nam/` folder and run the `rm -rf namportal` command.
3. Start the Access Manager Appliance by running the `/etc/init.d/novell-appliance start` command.

1.3.11 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 SSL VPN client, which displays when the user establishes an SSL VPN session, is also localized.

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

The Access Gateway and Identity Server, which can send messages to users when an error occurs, allow you to customize the error pages, but you are responsible for supplying the content of the customized pages.

1.4 Differences Between Access Manager and Access Manager Appliance

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

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

Features	Access Manager Appliance	Access Manager
	The Administration Console, Identity Provider, and SSL VPN are accelerated by Access Gateways. Only one open port, - port 443 - is required in the firewall to deploy Access Manager Appliance. Having only one open port in the firewall enhances security.	Multiple ports need to be opened for deployment.
Certificate Management	Certificate management has been simplified. To replace or renew certificates, the administrator updates only one place, which internally updates all certificates and key stores.	The administrator needs to make changes at multiple places to change certificates.
Default Portal	After a successful installation, a default portal is ready for administrator reference. The administrator can access the default portal using the http://hostname URL. This portal provides detailed information of Access Manager Appliance usage.	
Well-Known Trusted Roots	The well-known trusted roots are already available. The administrator does not need to add any trusted roots for well-known certificates.	The administrator needs to explicitly add the trusted roots for the certificates in the trust store.

Features	Access Manager Appliance	Access Manager
Ready-made Access Manager	The following configuration is internally done when Access Manager Appliance is installed: ◆ Importing Identity Provider, Access Gateway, and SSL VPN components. ◆ Automatic clustering of Identity Provider, Access Gateway, and SSL VPN components. ◆ Automatic configuration of Identity Provider and bringing it to the green state. ◆ Automatic configuration of Access Gateways and associating them with an identity provider. ◆ Automatic configuration of SSL VPN and bringing it to the green state. ◆ Automatic service creation to accelerate the identity provider, Administration Console, and portal. Because the configuration is internally taken care of, the administrator only needs to link the user store and Web servers to accelerate his Web servers through Single Box.	The administrator needs to manually configure each component to bring up the system for use.
System Configuration through Administration Console	Administration Console is the single point of reference to configure all the components in the Access Manager Appliance.	
64-bit Support	For better performance and scalability, a 64-bit support has been provided for all components.	Not all components provide 64-bit support.
Platform Upgrade	All the components are supported on the latest Tomcat 7 and Java 1.7.0_04 versions.	All components are supported on Tomcat 1.6.0_22 and Tomcat 5
J2EE Agents	Does not support J2EE agents currently.	You can install and configure the J2EE Agent components when you need fine-grained access control to Java applications.

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

2 Installation Requirements

This section explains the requirements for installing the NetIQ Access Manager Appliance. For a list of current filenames and for information about installing the latest release, review NetIQ Access Manager Appliance 3.2 SP1 Readme.

The appliance installer installs all the components on a single machine, so the software and hardware requirements are same for all components. Section 1.4, "Differences Between Access Manager and Access Manager Appliance," on page 24 lists differences between the previously shipped Access Manager versus the Access Manager Appliance.

- Section 2.1, "System Requirements," on page 27
- Section 2.2, "Virtual Machine Requirements," on page 28
- Section 2.3, "Network Requirements," on page 29
- Section 2.4, "Basic Setup," on page 30

2.1 System Requirements

The Access Manager Appliance is based on the (SUSE Linux Enterprise Server) 11 SP3 64-bit operating system.

The hard disk, RAM, and CPU requirements are the same for all components.

2.1.1 Hardware Platform Requirements

The following are the hardware requirements:

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

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

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

2.1.2 Browser Support

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

- 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 the Access Manager Appliance by burning the Access Manager Appliance ISO on a DVD.

2.2 Virtual Machine Requirements

The virtual machine must have enough resources. It needs to match the requirements that a physical machine has for the Access Manager Appliance. To have performance comparable to a physical machine, you need to increase the memory and CPU requirements.

For the hard disk, RAM, and CPU requirements, each virtual machine should meet the following minimum requirements:

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

The following virtual machines are supported:

- VMware ESX Server version 3.5 or later
- Xen Virtualization on SLES 11 SP1 or SP2 64-bit

NOTE: The SLES 11 SP1 and SP2 64-bit Access Manager Appliance does not support XEN paravirtualization for the 3.2 release.

The following sections contain installation tips for virtual machines:

- Section 2.2.1, “Keeping Time Synchronized on the Access Manager Appliances,” on page 28
- Section 2.2.2, “Number of Virtual Machines Per Physical Machine,” on page 29
- Section 2.2.3, “Using a Network Adapter for VMWare ESX,” on page 29

2.2.1 Keeping Time Synchronized on the Access Manager Appliances

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

SLES 11 SP2 or SP3: The `ntpdate` command is not supported by SLES 11 64-bit. You can use the `sntp` command in its place. Add the following command to the `/etc/crontab` file of the device:

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

Replace 10.20.30.108 with the IP address of your NTP server.

2.2.2 Number of Virtual Machines Per Physical Machine

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

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

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

For example, if you have one 16-CPU machine, you get better performance when you configure the machine to have four Access Gateways with 4 assigned CPUs than you get when you configure the machine to have eight Access Gateways with 2 assigned CPUs. If the machines are dedicated to Access Manager 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 finding the right hardware and virtualization configuration for your cluster.

2.2.3 Using a Network Adapter for VMWare ESX

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

2.3 Network Requirements

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

- A server configured with an LDAP directory (eDirectory 8.8.6, 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, the Access Manager Appliance components cannot start.
- Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

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

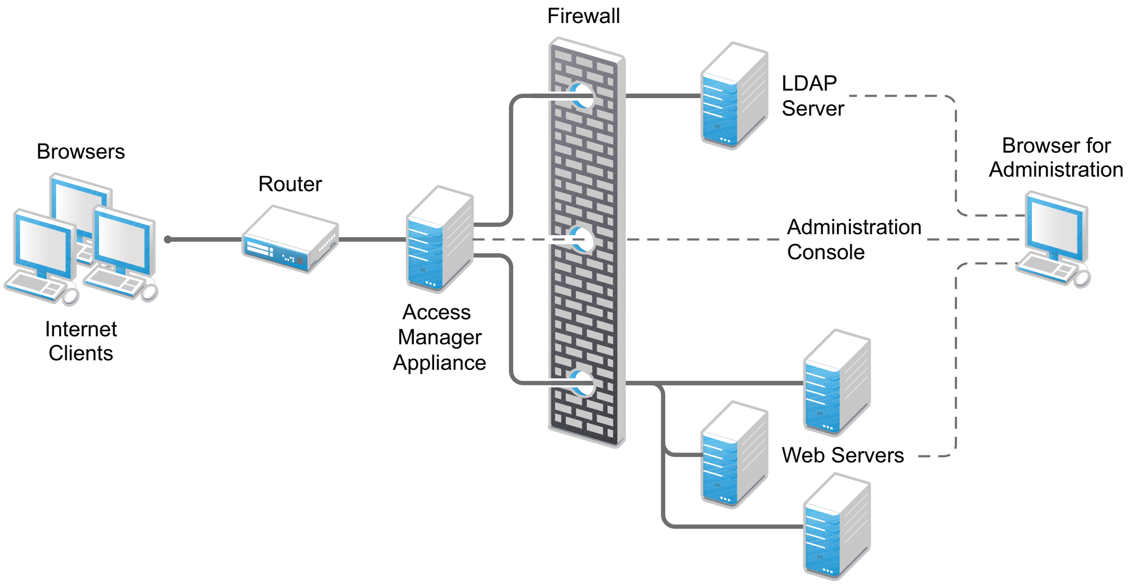
- Network time protocol server, which provides accurate time to the machines on your network. Time must be synchronized within one minute among the components, or the security features of the product disrupt the communication processes. You can install your own or use a publicly available server such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

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

2.4 Basic Setup

Figure 2-1 illustrates the basic Access Manager Appliance installation, where the Identity Server and Access Gateway are installed outside your firewall. The figure provides an overview of the flexibility built into Access Manager. 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 3.3, “Installing the Access Manager Appliance,” on page 32.

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. The Identity Server is not much of a security risk, because it does not permanently store any user data. This is a configuration that NetIQ has tested and can recommend. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Identity Servers and Access Gateways.

3 Installing the Access Manager Appliance

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

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

The Access Manager Appliance can be installed on all supported hardware platforms for SUSE Linux Enterprise Server 11 64-bit SP1.

3.1 Prerequisites for the Access Manager Appliance

□ 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.

□ Make sure the machine meets the minimum hardware requirements. See Section 2.1.1, “Hardware Platform Requirements,” on page 27.

□ (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).

3.2 Boot Screen Function Keys

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

- **F1:** Lets you access the context-sensitive help for the currently active screen element of the boot screen.
- **F2:** Lets you select the display language for the installation. However, the Access Manager Appliance supports only the English language. It also allows to choose a keyboard layout from the available options.
- **F3:** Lets you select different graphical display modes for the installation. Also included is an entry to select the text mode. Use this mode if there are issues with the installation in the graphical mode.
- **F4:** Lets you choose the installation media if you want to use a different source, such as HTTP or NFS, instead of the installation disk. You are prompted to specify the details of the server and the network settings.

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

  Only HTTP and NFS mode of installation are supported by Access Manager Appliance.
- **F5:** Lets you select whether to install the Access Manager Appliance with the *Default Kernel, Safe Settings*, *No ACPI*, or *No Local APIC* options.
- **F6:** Lets you communicate to your system that you have an optional disk with a driver update. At the prompt, insert the update disk. A few seconds after starting the installation, a minimal Linux system is loaded to run the installation procedure.

3.3 Installing the Access Manager Appliance

The 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:

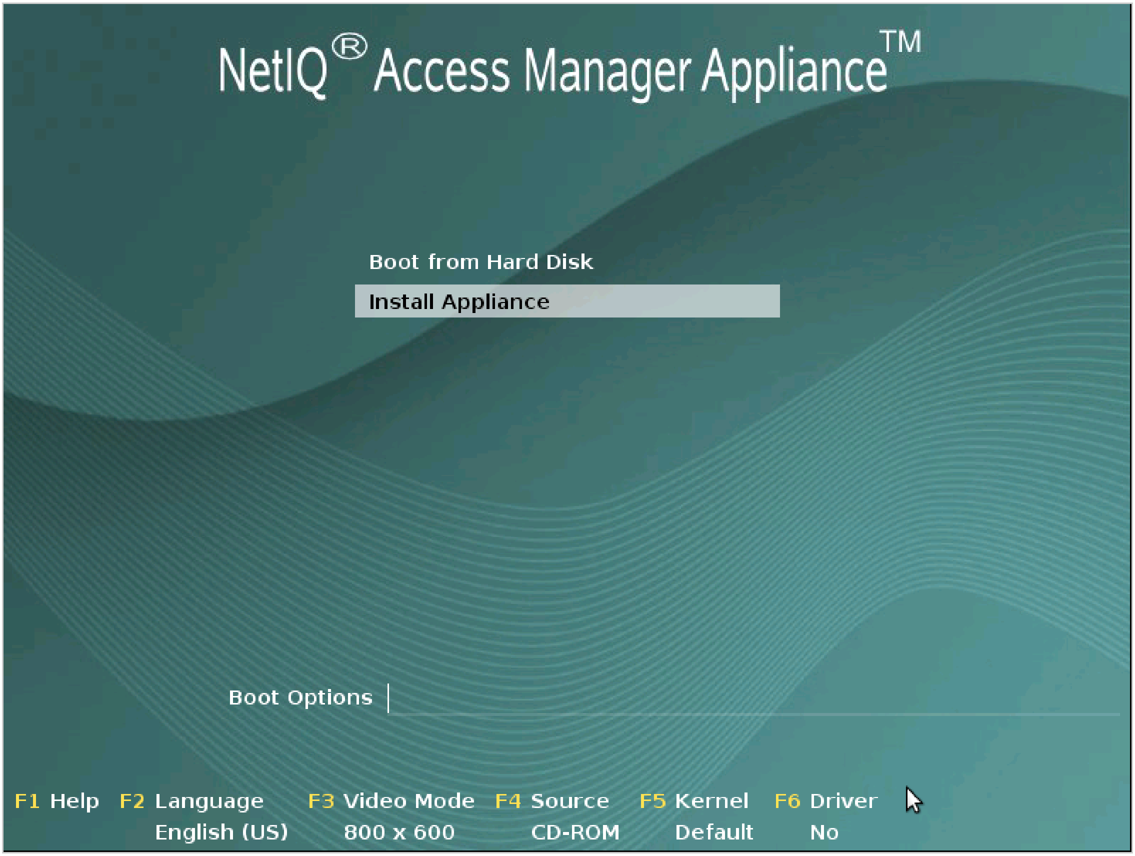
- **root:** The default size is one-third the size of the extended drive and the mount point is `/`.
- **var:** The default size is one-third the size of the extended drive and the mount point is `/var`.

NOTE: Do not install or import any non- 3.2 appliance devices during installation.

The 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.



F1 Help F2 Language English (US) F3 Video Mode 800 x 600 F4 Source CD-ROM F5 Kernel Default F6 Driver No

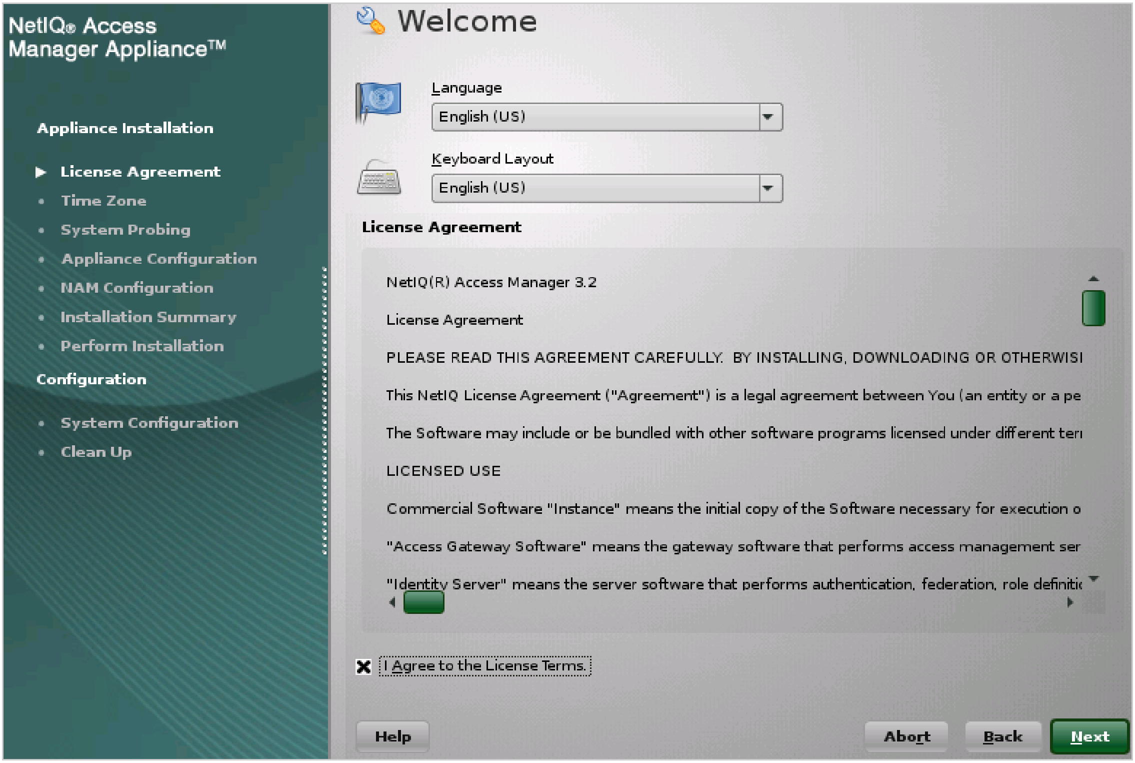
2 By default, the *Boot From Hard Disk* option is selected in the boot screen.

Use the Down-arrow key to select *Install Appliance*.

3 (Optional) Use the function key options to change installation settings as desired.

For example, you can press F4 to perform a network installation. For more information on these function keys, see Section 3.2, “Boot Screen Function Keys,” on page 32.

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



Welcome

Language: English (US)

Keyboard Layout: English (US)

License Agreement

NetIQ(R) Access Manager 3.2

License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY. BY INSTALLING, DOWNLOADING OR OTHERWISI

This NetIQ License Agreement ("Agreement") is a legal agreement between You (an entity or a pe

The Software may include or be bundled with other software programs licensed under different teı

LICENSED USE

Commercial Software "Instance" means the initial copy of the Software necessary for execution o

"Access Gateway Software" means the gateway software that performs access management ser

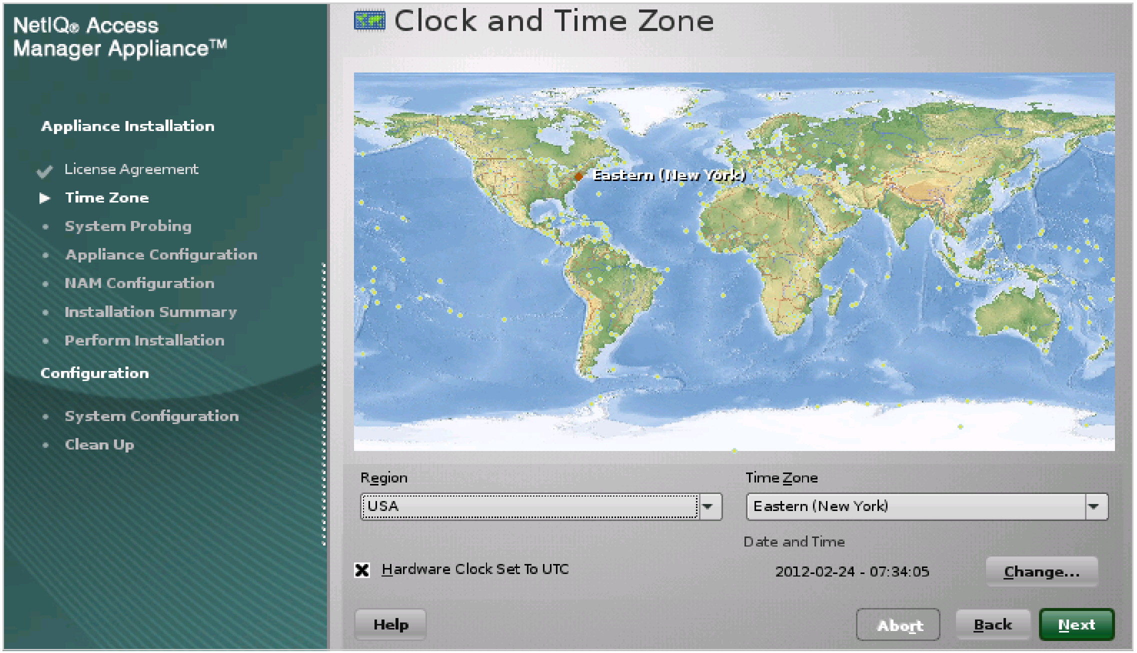
"Identity Server" means the server software that performs authentication, federation, role definitic

☒ I Agree to the License Terms.

The License Agreement page is displayed.

5 Review the agreement on the License Agreement page, then click *I Agree* to accept the agreement.

The Clock and Time Zone page is displayed.



Clock and Time Zone

Region: USA

Time Zone: Eastern (New York)

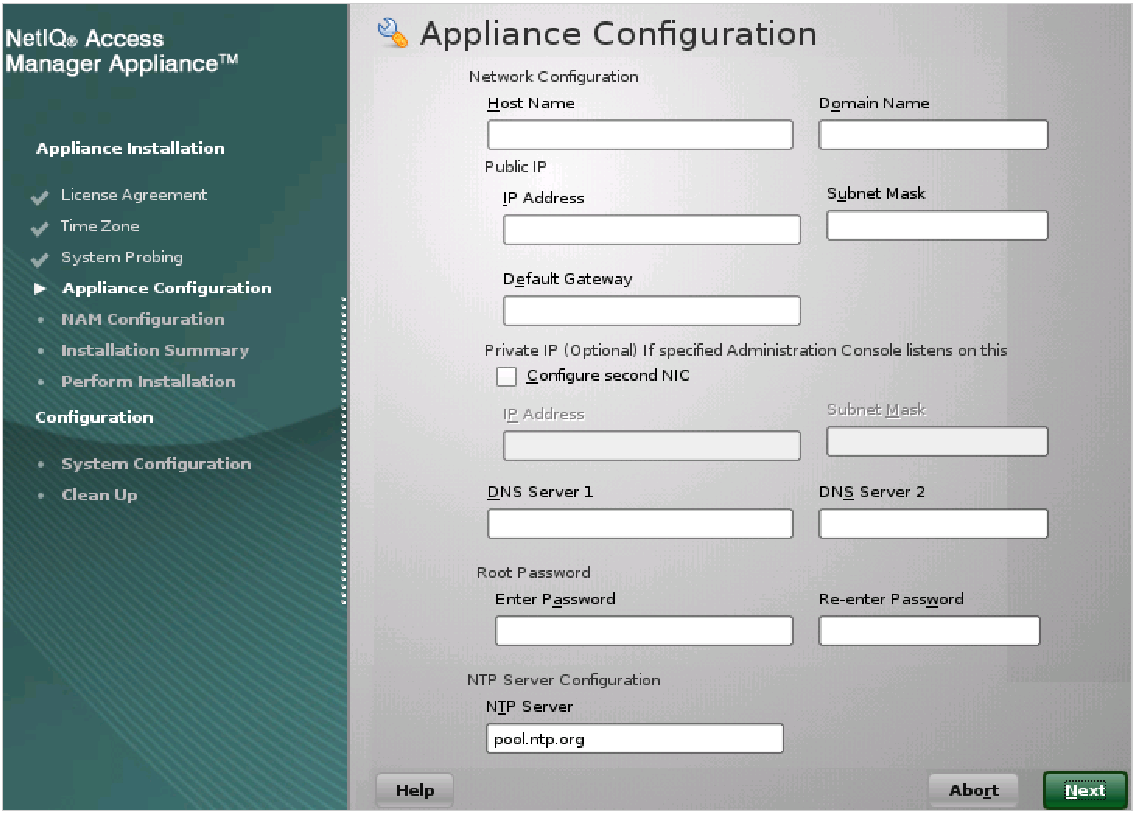
☒ Hardware Clock Set To UTC

Date and Time: 2012-02-24 - 07:34:05

6 Select the region and time zone.

7 Click *Next*.

The Appliance Configuration page is displayed.



NTP Server: pool.ntp.org

8 Configure the details on the Appliance Configuration page:

Host Name: The hostname for the Access Manager Appliance machine.

Domain Name: The domain name for your network.

Public IP: Configure these options for the public IP:

- **IP Address:** The public IP address of the Access Manager Appliance.
- **Subnet Mask:** The subnet mask of the Access Manager Appliance.
- **Default Gateway:** The IP address of the default gateway.

Private IP: Configure these options for the private IP. This is an optional configuration. If this is configured, Administration Console listens on this IP.

- **IP Address:** The private IP address of the appliance.
- **Subnet Mask:** The subnet mask of the Access Manager Appliance.
- **Gateway:** The IP address of the gateway.

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

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

Specify the following information in the Root Password section:

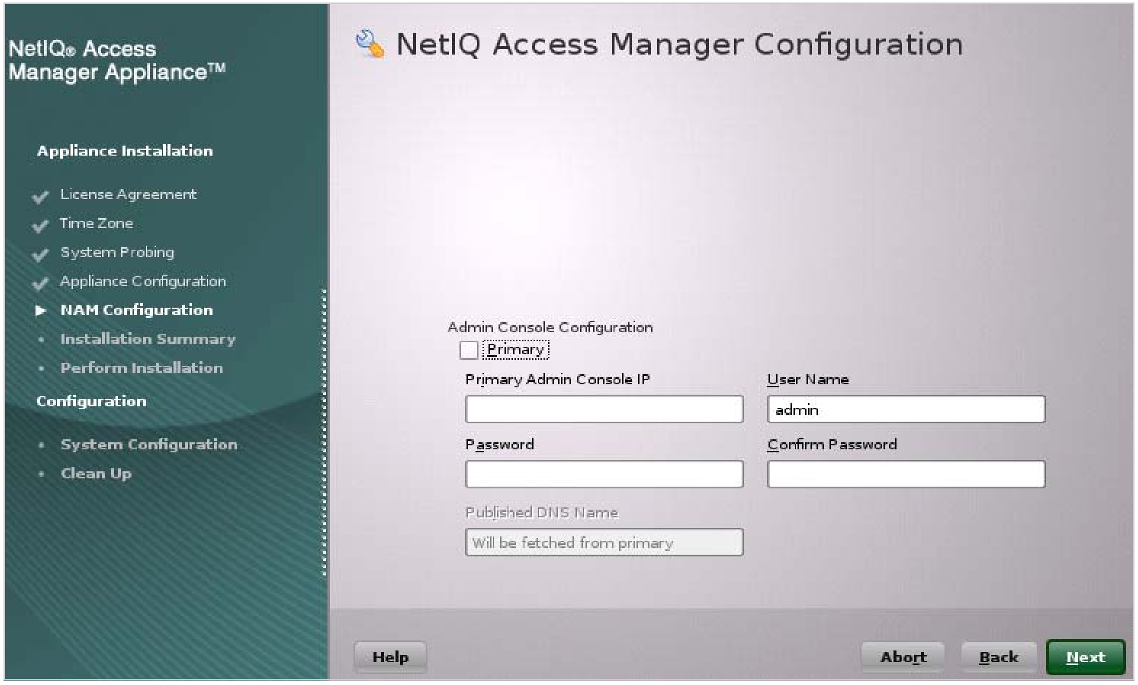
Enter Password: Specify a password for the `root` user.

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

NTP Server Configuration: The name of the NTP server.

9 Click *Next*.

The NetIQ Access Manager Configuration page is displayed.



NetIQ Access Manager Configuration

Admin Console Configuration

□ Primary

Primary Admin Console IP:

User Name: admin

Password:

Confirm Password:

Published DNS Name: Will be fetched from primary

Configure the details under Admin Console Configuration:

Primary: Clear this option to specify if this appliance is not the primary Administration Console.

If you are installing it as a secondary appliance then ensure that the primary Administration Console appliance is reachable.

Admin Console IP: Specify the IP address of the primary Administration Console if this is a secondary Administration Console.

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 the password for the user.

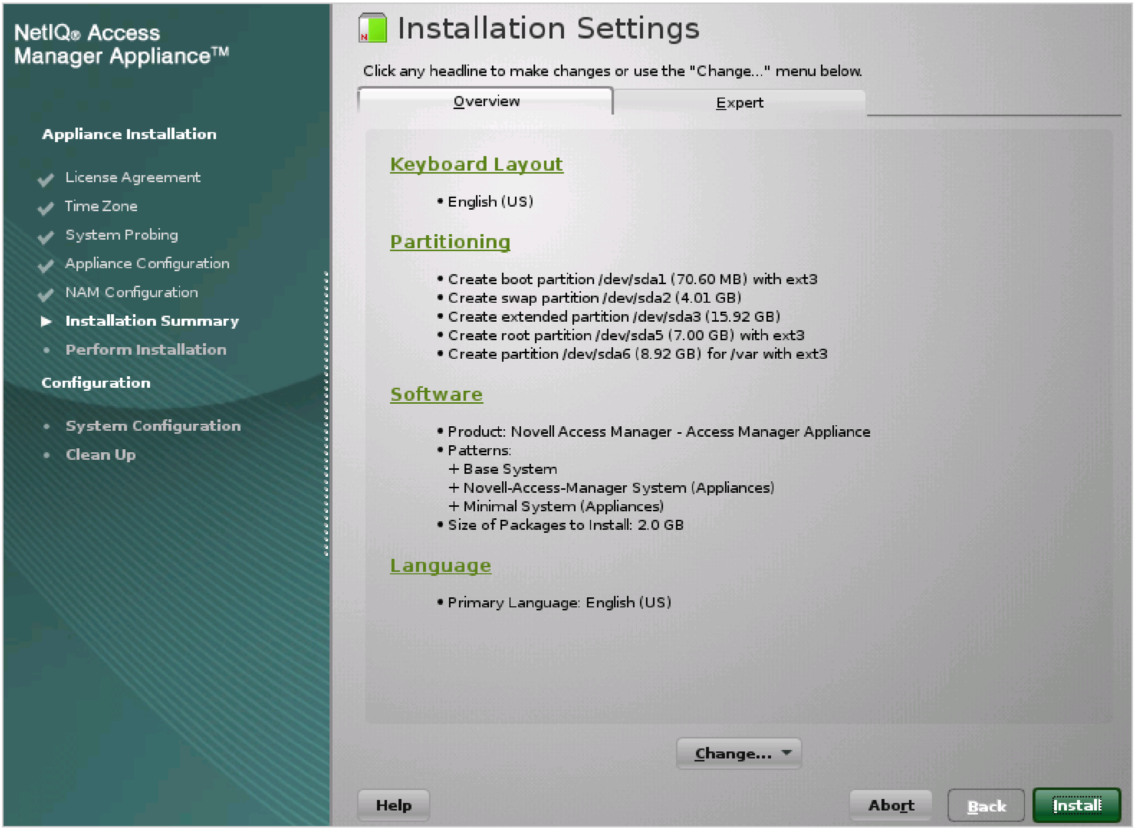
NOTE: Administration Console password does not accept special characters colon (:) and double quotes (“).

Confirm Password: Specify the password again for verification.

10 Click *Next* to display the confirmation dialog box.

11 To modify any of the installation settings that you specified in the previous steps, click *Cancel*; otherwise click *Continue* to proceed with the installation.

The Installation Settings page appears.



Installation Settings

Click any headline to make changes or use the "Change..." menu below.

Keyboard Layout

- English (US)

Partitioning

- Create boot partition /dev/sda1 (70.60 MB) with ext3
- Create swap partition /dev/sda2 (4.01 GB)
- Create extended partition /dev/sda3 (15.92 GB)
- Create root partition /dev/sda5 (7.00 GB) with ext3
- Create partition /dev/sda6 (8.92 GB) for /var with ext3

Software

- Product: Novell Access Manager - Access Manager Appliance
- Patterns:
  + Base System
  + Novell-Access-Manager System (Appliances)
  + Minimal System (Appliances)
- Size of Packages to Install: 2.0 GB

Language

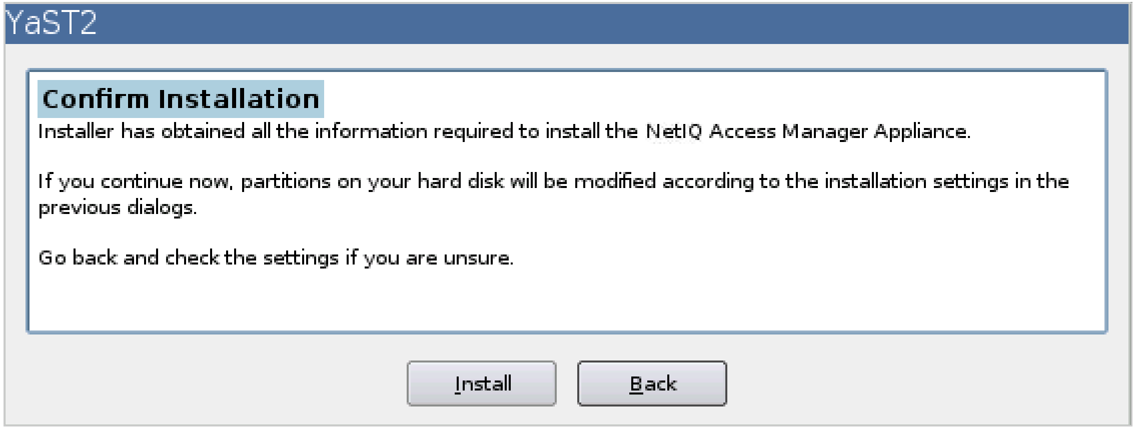
- Primary Language: English (US)

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.

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

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



Confirm Installation

Installer has obtained all the information required to install the NetIQ Access Manager Appliance.

If you continue now, partitions on your hard disk will be modified according to the installation settings in the previous dialogs.

Go back and check the settings if you are unsure.

14 Click *Install* to confirm.

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.

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

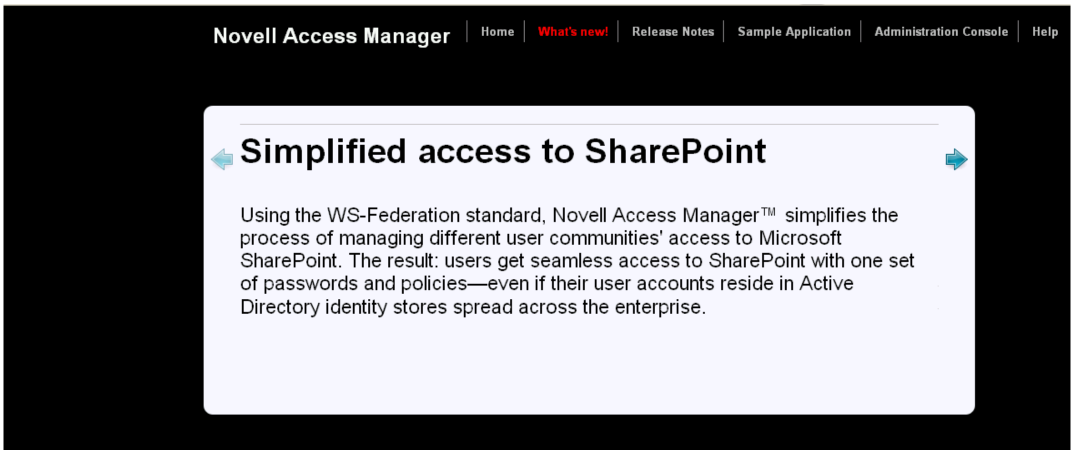
Log in to the Administration Console see Section 3.6, “Logging In to the Administration Console,” on page 40), then click *Devices* > *Access Gateways*.

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.

15a In a browser, enter the Access Manager Appliance URL. Access Manager Appliance URL is formed using the `Host Name` and Domain Name provided in the Step 8 above. For example, if the host name is `accessapp` and the domain name is novell.com, then the URL will be `https://accessapp.novell.com`. You will be redirected to the Sample Portal Page.



Simplified access to SharePoint

Using the WS-Federation standard, Novell Access Manager™ simplifies the process of managing different user communities' access to Microsoft SharePoint. The result: users get seamless access to SharePoint with one set of passwords and policies—even if their user accounts reside in Active Directory identity stores spread across the enterprise.

15b Click on the Administration Console link. Login with User Name and Password.

15c 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.

15d 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.

15e Click *Devices* > *SSL VPN*.

15f Install `novl-sslvpn-hb-key-3.1.0-0.noarch.rpm` and then configure the SSL VPN cluster manually.

16 Continue with one of the following sections:

- Section 3.4, “Removing the Landing Portal,” on page 39
- Section 3.5, “Viewing the Installation Log,” on page 40
- “Setting up User Stores for Identity Server Configuration” in the *NetIQ Access Manager Appliance 3.2 SP3 Setup Guide*.
- “Configuring the Access Gateway” in the *NetIQ Access Manager Appliance 3.2 SP3 Setup Guide*.

NOTE: After installing the Access Manager Appliance, if you want to use the portal application, start the portal using the `/opt/novell/nam/namportal/bin/startNP.sh` command.

3.4 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 quickly. You can experiment with the portal as long as it is not in production. We recommend you to 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* > *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* until the Access Gateway Servers page appears.

6 Click *Update*.

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

8 To disable the role policy, select the role policy check box, select the role role_assignment from the Roles Policy List, then click *Disable*.

9 Click *OK* > *Update*.

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

10a Log in to Access Gateway Appliance using any SSH client (for example, SSH in Linux, and PuTTY in Windows).

10b Stop the portal using the `/opt/novell/nam/namportal/bin/shutdownNP.sh` command.

10c Go to the portal directory by running the `cd /opt/novell/nam/` command.

10d Remove the portal by running the `rm -rf namportal` command.

10e Restart the Administration Console by running the `/etc/init.d/novell-ac restart` command.

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

You can remove the users by performing the following steps:

11a In the Administration Console, click *Roles and Tasks* > *Users* > *Delete User*.

11b In the Delete User page, specify the Object Name as bob.novell to delete Bob and alice.novell to delete Alice.

11c Click *Ok*.

NOTE: Optional: You can go to the Policies page and delete the policies basic authorization, fill allowance, fillRole, and role assignment by selecting the respective policies and clicking delete.

3.5 Viewing the Installation Log

Installation logs are available in the `/tmp/novell_access_manager directory`.

NOTE: From 3.2 onwards, Access Gateway Appliance uses the filesystem provided by Apache mod_cache module for storing the caching objects. If you want to change the size of this cache after installation see TID on Changing the Cache Size of an Access Gateway Appliance after Installation.

3.6 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.

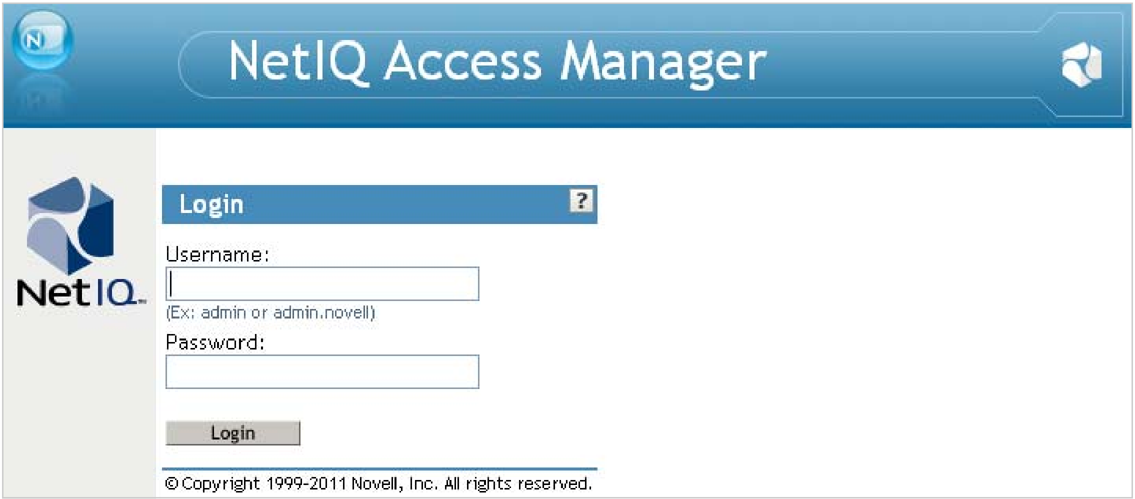
You should not download and add iManager plug-ins to this customized version. If you do, you can destroy the Access Manager Appliance schema, which can prevent you from managing the Access Manager Appliance components. This can also prevent communication among the modules.

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:

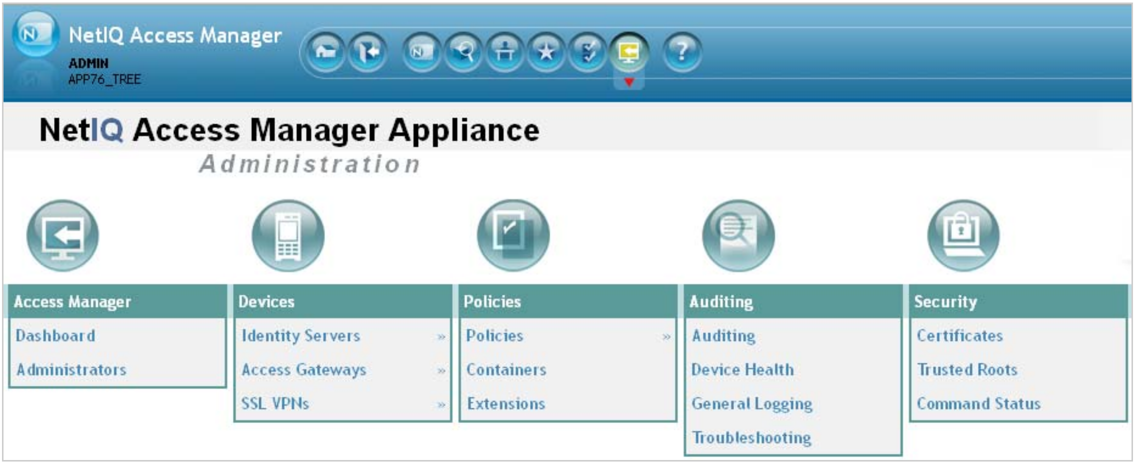
1. Enable browser pop-ups.
2. From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

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


NetIQ Access Manager
NetIQ
Login
Username:
(Ex: admin or admin.novell)
Password:
Login
© Copyright 1999-2011 Novell, Inc. All rights reserved.

5 Click *Login*.

The following view appears:



For more information about this view or about configuring the Administration Console for the Access Manager Appliance 3.2 view, see “Configuring the Default View” in the *NetIQ Access Manager Appliance 3.2 SP3 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 3.7, “Administration Console Conventions,” on page 41.

3.7 Administration Console Conventions

- The required fields on a configuration page contain an asterisk by the field name.
- All actions such as delete, stop, and purge require verification before they are executed.

- Changes are not applied to a server until you update the server.
- Sessions are monitored for activity. If your session becomes inactive, you are asked to log in again and unsaved changes are lost.

4 Upgrading Access Manager Appliance

This section discusses about how to upgrade the Access Manager Appliance 3.2 to 3.2 IR1 or 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 3.2 SP3 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 3.2 SP3 Administration Console Guide*.

NOTE: For Access Manager Appliance, ensure that you upgrade the primary node in the cluster first, followed by the other nodes.

- Section 4.1, “Upgrading Access Manager Appliance from Version 3.2,” on page 43
- Section 4.2, “Upgrading from Access Manager Appliance 3.2 SP1 to 3.2 SP1 IR1a Using the Patch,” on page 44
- Section 4.3, “Upgrading Access Manager Appliance 3.2 SP2 Using the Patch Process,” on page 46
- Section 4.4, “Configuring the Access Manager Appliance User Portal,” on page 49

4.1 Upgrading Access Manager Appliance from Version 3.2

You must be on Access Manager 3.2 to upgrade to a higher version. For the supported upgrade paths see the following table.

Table 4-1 *Supported Upgrade Paths*

Source	Destination
3.2	3.2 SP2
3.2 IR1	3.2 SP2
3.2 SP1	3.2 SP2
3.2 SP1x	3.2 SP2
3.2 SP2	3.2 SP3
3.2 SP2x	3.2 SP3

1. Log in as `root`.
2. Download the upgrade file from Patches and Security 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 (Optional) Before upgrading the Access Manager Appliance it is important to upgrade the version of the underlying operating system. The upgrade script displays the following prompt:

```
It is recommended that you upgrade the Appliance OS before continuing. Do you
want to continue?
```

Type *Y* to continue upgrading the Access Manager Appliance without upgrading the base operating system. If you select *N* the upgrade will terminate.

IMPORTANT: Even though upgrading the base operating system of Access Manager Appliance is optional, it is recommended to upgrade the base operating system to SLES 11 SP3. Follow the instructions in Section 5.2, “Upgrading the Operating System for Access Manager Appliance,” on page 54 to upgrade the operating system.

---

5 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 3.2 SP3 Identity Server Guide.

6 A confirmation message is displayed.

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

Type *Y* to continue.

7 Enter the Access Manager Administration Console user ID.

8 Enter the Access Manager Administration Console password.

9 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

4.2 Upgrading from Access Manager Appliance 3.2 SP1 to 3.2 SP1 IR1a Using the Patch

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 the form of a patch file. This patch file can be used to update all your Access Manager Appliance components.

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

4.2.1 Prerequisites

- Before upgrading, back up your current configuration. If the upgrade fails for any reason, you can use the backup file to recover your configuration.

  To back up your Access Manager Appliance configuration, do the following on the primary Administration Console go to the `/opt/novell/devman/bin` directory. Run ambkup.sh script

- To use the patch to upgrade to the latest Access Manager Appliance patches, verify that your current version of Access Manager Appliance is 3.2.1-57.
  1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.
  2. Examine the value of the *Version* field to see if it displays 3.2 SP1 version `3.2.1-57`.

4.2.2 Downloading the Patch

To download the patch:

1. Go to download.novell.com/patch/finder and specify `AM_32_SP1_IR1a.zip` in the *Keywords* field and click *Search*.
2. Download and save the 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.
3. Unzip the file using the `unzip AM_32_SP1_IR1a.zip` command.
4. After extraction, the following files and folders are created in the `AM_32_SP1_IR1a` 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 on a Linux server.
`installPtool.cmd`	Script to install the patch on a Windows server.
`AM_32_SP1_IR1a_201.patch`	The patch file. The name of the patch file changes for each IR release.

4.2.3 Installing the Patch

Install the patch after extracting files from the `AM_32_SP1_IR1a.zip` file.

1. Log in as the root user.
2. Run the `sh installPtool.sh` command.

   This command installs the patch and the bundled patch file.

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

If the patch is already installed, the existing patch files are replaced.

4.2.4 Installing and Administering Patches

After the patch is installed, go to the `/opt/novell/nam/patching/bin` folder.

Use the following options to administer the Access Manager Appliance patch file.

Option	Description	Command on Linux server
`-qa`	Lists all the installed patches.	`./patch -qa`

Option	Description	Command on Linux server
`-q`	Lists the details of a patch that is installed.	`./patch –q` Example: If you have installed `AM_32_SP1_IR1a_201.patch`, use the following command: `./patch –q IR1a-201`
`-i`	Installs a patch. During installation of the patch, all running services are stopped temporarily. After the patch is installed, all the services are restarted and details of the operation are written to log files.	`./patch –i <`*`location and name of the patch`*`>` Example: `./patch –i /tmp/AM_32_SP1_IR1a_201.patch`
`-e`	Removes a patch. Use this option to remove an installed patch. The patch maintains content relationship between 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 the running services are stopped temporarily.	`./patch –e <`*`patch name`*`>` Example: `./patch –e IR1a-201`
`-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 name of the patch`*`>` Example: `./patch –qpl /tmp/AM_32_SP1_IR1a_201.patch`
`-v`	Verifies a patch. Use this option to verify the integrity of a patch file.	`./patch –v <`*`location and name of the patch`*`>` Example: `./patch –v /tmp/AM_32_SP1_IR1a_201.patch`
`-t`	Verifies if services can be restored by the installer.	`./patch –t <`*`location and name of the patch`*`>` Example: `./patch –t /tmp/AM_32_SP1_IR1a_201.patch`

4.3 Upgrading Access Manager Appliance 3.2 SP2 Using the Patch Process

You can upgrade the following versions of Access Manager using the patch process:

- 3.2 SP2 to 3.2 SP2 IR1
- 3.2 SP2 or 3.2 SP2 IR1 to 3.2 SP2 IR2

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 the form of a patch file. This patch file can be used to update all your Access Manager Appliance components.

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

4.3.1 Prerequisites

- Before upgrading, back up your current configuration. If the upgrade fails for any reason, you can use the backup file to recover your configuration.

  To back up your Access Manager Appliance configuration, do the following on the primary Administration Console go to the `/opt/novell/devman/bin` directory. Run ambkup.sh script
- To use the patch to upgrade to the latest Access Manager Appliance patches, verify the installed product version is as per the latest release.
  1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.
  2. Examine the value of the *Version* field to see if it displays as follows:
     - 3.2 SP2: `3.2.2-77`
     - 3.2 SP2 IR1:`3.2.2-77 + IR1-107`

4.3.2 Downloading the Patch

To download the patch

1. Go to download.novell.com/patch/finder and specify `AM_32_SP2_IR2.zip` in the *Keywords* field and click *Search*.
2. Download and save the 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.
3. Unzip the file using the `AM_32_SP2_IR2.zip` command.
4. After extraction, the following files and folders are created in the `AM_32_SP2_IR2` 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 patch on Linux server.
`installPatch.sh`	Script to install this IR patch tool and the updated binaries on a Linux server.
`installPtool.cmd`	Script to install patch on a Windows server.
`AM_32_SP2_IR2-117.patch`	The patch file. Name of the patch file changes for each IR release.

4.3.3 Installing the Patch

Install the patch after extracting files from the `AM_32_SP2_IR2.zip` file.

1. Log in as the root user.
2. Go to the location where you have extracted the patch files.

3 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.

4.3.4 Administering Patches

After the patch is installed, go to the `/opt/novell/nam/patching/bin` folder.

Use the following options to administer the Access Manager Appliance patch file.

Option	Description	Command on Linux server
`-qa`	Lists all the installed patches.	`./patch -qa`
`-q`	Lists the details of a patch that is installed.	`./patch –q` Example: If you have installed `AM_32_SP2_IR1-107.patch`, use the following command:`./patch –q IR2-117`
`-i`	Installs a patch. During installation of the patch, all running services are stopped temporarily. After the patch is installed, all the services are restarted and details of the operation are written to log files.	`./patch –i <`*`location and name of the patch`*`>` Example:`./patch –i /tmp/.patch AM_32_SP2_IR2-117.patch`
`-e`	Removes a patch. Use this option to remove an installed patch. The patch maintains content relationship between 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 the running services are stopped temporarily.	`./patch –e <`*`patch name`*`>` Example:`./patch –e IR2-117`
`-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 name of the patch`*`>` Example:`./patch –qpl /tmp/AM_32_SP2_IR2-117.patch`
`-v`	Verifies a patch. Use this option to verify the integrity of a patch file.	`./patch –v <`*`location and name of the patch`*`>` Example:`./patch –v /tmp/.patch AM_32_SP2_IR2-117.patch`

Option	Description	Command on Linux server
`-t`	Verifies if services can be restored by the installer.	`./patch –t <location and name of the patch>` Example:`./patch –t /tmp/.patch AM_32_SP2_IR2-117.patch`

4.4 Configuring the Access Manager Appliance User Portal

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

1 In the Administration Console, go to *Access Gateways* > *Edit* > *NAM-RP*.

   1a Click on *Protected Resources* and select *portal* from the list.

   1b Click *New* and add a new `/portal/users` in the *URL Path*.

2 Click on the *Web Server Addresses* for the namportal in the *Proxy Service List*.

   2a Disable the option *Connect Using SSL*.

   2b Change the *Connect Port* from 80 to 8020.

3 Apply the changes.

NOTE: If you want to start the portal application, use the `/opt/novell/nam/namportal/bin/startNP.sh` command.

5 Upgrading Kernel to the Latest Security Patch

5.1 Installing or Updating the Latest Linux Patches

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

- Section 5.1.1, “Installing or Updating Security Patches for the Access Manager Appliance,” on page 51
- Section 5.1.2, “Configuring the Subscription Management Tool for Access Manager Appliance,” on page 53

Prerequisites

❒ The latest security patches are only available to customers who are on Access Manager 3.2 SP3 with operating system SLES 11 SP3. If you are on an Access Manager version older than 3.2 SP3 with operating system SLES 11 SP1, it is mandatory that you upgrade the operating system to SLES 11 SP3 and also upgrade to Access Manager 3.2 SP3 to get the latest security patches. For details on upgrading to Access Manager 3.2 SP3, see. Chapter 4, “Upgrading Access Manager Appliance,” on page 43

❒ Ensure that you have a Novell user account to receive the Linux updates.

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

5.1.1 Installing or Updating Security Patches for the Access Manager Appliance

To get the latest security updates for the 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 `NAM323-APP-Updates` was created:

    ```
    zypper lr
    ```

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

    NOTE: If you are not on Access Manager 3.2 SP3, no patches are displayed for installation.

13. After the patches are installed, restart the machine.

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

Setting Up the 3.2 SP3 Channel

To get the latest SLES security patches for Access Manager Appliance, you must upgrade the operating system to SLES 11 SP3 and add a new Access Manager 3.2 SP3 channel to the appliance.

NOTE: If you had an existing channel for an older version of Access Manager and SLES operating system (not Access Manager 3.2 SP3 with SLES 11 SP3), then after upgrading to the latest operating system and Access Manager 3.2 SP3, you must re?register the new channel.

Perform the following steps to set up the SLES 11 SP3 channel.

1. Upgrade the base Operating System to SLES 11 SP3. For more information about upgrading the base operating system, see Section 5.2, “Upgrading the Operating System for Access Manager Appliance,” on page 54

2. Upgrade the Access Manager Appliance.

3. Edit `/etc/products.d/NAM_APP.prod` and change the version to 3.2.3. The line will look like the following:

   ```
   <version>3.2.3</version>
   ```

4. Remove all the old NCC credentials using the following commands:

   ```
   rm /etc/zypp/credentials.d/NCCcredentials
   rm /etc/zypp/repos.d/nu*
   rm /etc/zypp/services.d/nu*
   ```

5. Use the `zypper lr` command to verify that channel `NAM32-APP-Updates` is removed
6. Re-register to get the latest updates. For more information, see Section 5.1.1, “Installing or Updating Security Patches for the Access Manager Appliance,” on page 51.
7. Use the `zypper lr` command to verify if the new channel `NAM323-APP-Updates` is added.

5.1.2 Configuring the Subscription Management Tool for Access Manager Appliance

The 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 on configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 (https://www.suse.com/documentation/smt11/).

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

- “SMT Configuration” on page 53
- “Troubleshooting” on page 54

SMT Configuration

You must configure the SMT server and set up subscription for `NAM323-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 (https://www.suse.com/documentation/smt11/).
2. Log into you Novell Customer Center account.
3. Select *My Products* > *Mirroring Credentials*, then click *Generate Credentials*.
4. Copy the mirroring credentials before logging out of your Novell Customer Center account.
5. Run the *SMT Configuration* tool from YAST, then specify the mirroring credentials.
6. Run the *SMT Management* tool.

   The `NAM323-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 *NAM323-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.

Troubleshooting

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

5.2 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. During upgrade, you must upgrade the base Operating System before upgrading the Access Manager appliance.

NOTE: Access Manager appliance channel updates are only available over the base Operating System version of SLES 11 SP3.

Perform the following steps to upgrade the base Operating System.

1 Get the Access Manager 3.2 SP3 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/ 323appiso
```

3 Refresh the 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 323appiso
```

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

A.1 Checking the Installation Logs

If the 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 component.
`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 component.
`install_idp_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring the Identity Server module.
install_sslvpn_2011-06-06_17:38:36.log	Contains messages generated for installing and configuring the SSL VPN module.
`configure_cluster_2011-06-06_17:28:19.log`	Contains messages generated for configuring Identity Server and Access Gateway.

A.2 Troubleshooting the Access Manager Appliance Installation

A.2.1 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.2.2 Novell Device Manager Installation Fails During the Appliance Installation

To workaround this issue, reinstall the appliance.

A.2.3 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.