



Installation Guide

Access Manager 4.0 SP2

June 2015

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.

© 2014 NetIQ Corporation. All Rights Reserved.

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

Contents

About NetIQ Corporation	7
About this Book and the Library	9
1 NetIQ Access Manager Product Overview	11
1.1 How Access Manager Solves Business Challenges	11
1.1.1 Protecting Resources While Providing Access	12
1.1.2 Managing Passwords with Single Sign-On	13
1.1.3 Enforcing Business Policies	14
1.1.4 Sharing Identity Information	15
1.1.5 Protecting Identity Information	17
1.1.6 Complying with Regulations	18
1.2 How Access Manager Works	19
1.2.1 Authentication	19
1.2.2 Authorization	20
1.2.3 Identity Injection	20
1.2.4 Identity Federation	20
1.3 Access Manager Devices and Their Features	21
1.3.1 Administration Console	21
1.3.2 Identity Servers	21
1.3.3 Access Gateways	22
1.3.4 SSL VPN	24
1.3.5 Policies	24
1.3.6 Certificate Management	24
1.3.7 Embedded Service Provider	25
1.3.8 The User Portal Application	25
1.3.9 Language Support	25
1.4 Differences Between Access Manager and Access Manager Appliance	25
1.5 Recommended Installation Scenarios	29
1.5.1 Basic Setup	30
1.5.2 High Availability Configuration with Load Balancing	31
2 Installing the Administration Console	33
2.1 Installing the Administration Console on Linux	33
2.1.1 Installation Requirements on Linux	33
2.1.2 Installation Procedure	36
2.2 Installing the Administration Console on Windows	39
2.2.1 Installation Requirements on Windows	39
2.2.2 Installation Procedure	39
2.3 Logging In to the Administration Console	42
2.4 Enabling the Administration Console for Multiple Network Interface Cards	43
3 Installing the Identity Servers	45
3.1 Installing the Identity Server on Linux	45
3.1.1 Prerequisites	45
3.1.2 Installation Requirements on Linux	46
3.1.3 Installation Procedure	47
3.2 Installing the Identity Server on Windows	48
3.2.1 Installation Requirements on Windows	48

3.2.2	Installation Procedure	49
4	Installing the Access Gateway	51
4.1	Installing the Access Gateway Appliance	51
4.1.1	Access Gateway Appliance Requirements	51
4.1.2	Installing the Access Gateway Appliance	52
4.2	Installing the Access Gateway Service	55
4.2.1	Installing the Access Gateway Service	55
4.2.2	Installing the Access Gateway Service on Windows	59
5	Installing SSL VPN	63
5.1	SSL VPN Installation Requirements	63
5.2	Installing SSL VPN	63
5.2.1	Installing ESP-Enabled SSL VPN	64
5.2.2	Installing Traditional SSL VPN	67
5.2.3	Installing the Key for High-Bandwidth SSL VPN	72
6	Installing Access Manager Components in NAT Environments	73
6.1	Network Prerequisites	73
6.2	Network Setup Flow Chart	74
6.3	Installing Access Manager Components in NAT Environments	74
6.3.1	Installing the Administration Console	75
6.3.2	Configuring Global Settings	75
6.3.3	Configuring Audit Server	76
6.3.4	Installing and Configuring the Identity Server	77
6.3.5	Installing and Configuring the Access Gateway	77
6.4	Configuring Network Address Translation	77
6.4.1	Configuring the Administration Console Behind NAT	77
6.4.2	Configuring the Identity Server, Access Gateway, and SSL VPN Behind NAT	78
7	Verifying the Installation	79
7.1	Verifying the Identity Server Installation	79
7.2	Verifying the Access Gateway Installation	79
7.3	Verifying the SSL VPN Installation	79
8	Setting Up Firewalls	81
8.1	Required Ports	81
8.2	Restricted Ports	88
8.3	Sample Configurations	89
8.3.1	Access Gateway and Identity Server in DMZ	89
8.3.2	A Firewall Separating Access Manager Components from the LDAP Servers	90
8.3.3	Configuring a Firewall for SSL VPN	91
9	Uninstalling Components	93
9.1	Uninstalling the Identity Server	93
9.1.1	Deleting Identity Server References	93
9.1.2	Uninstalling the Linux Identity Server	93
9.1.3	Uninstalling the Windows Identity Server	94
9.2	Reinstalling an Identity Server to a New Hard Drive	94
9.3	Uninstalling the Access Gateway	95

9.3.1	Uninstalling the Windows Access Gateway Service	95
9.3.2	Uninstalling the Linux Access Gateway Service	95
9.4	Uninstalling the Administration Console.	96
9.4.1	Uninstalling the Linux Administration Console.	96
9.4.2	Uninstalling the Windows Administration Console.	97
9.5	Uninstalling the SSL VPN Server.	97
9.5.1	Deleting the SSL VPN Server References	97
9.5.2	Uninstalling the SSL VPN Server.	98
9.5.3	Uninstalling the RPM Key for High Bandwidth SSL VPN.	98
A	Troubleshooting Installation	99
A.1	Troubleshooting a Windows Administration Console Installation.	99
A.2	Troubleshooting a Windows SSL Renegotiation	100
A.3	Troubleshooting an Identity Server Import and Installation	101
A.3.1	The Identity Server Fails to Import into the Administration Console	101
A.3.2	Reimporting the Identity Server	101
A.3.3	Check the Installation Logs	102
A.4	Troubleshooting the Access Gateway Service Installation.	103
A.4.1	Troubleshooting the Windows Access Gateway Service Installation	103
A.5	Troubleshooting the SSL VPN Installation	104
A.5.1	Manually Uninstalling the Enterprise Mode Thin Client	104
A.5.2	SSL VPN Health Status Is Yellow after an Upgrade	105
A.6	Troubleshooting the Access Gateway Import.	105
A.6.1	Repairing an Import	105
A.6.2	Troubleshooting the Import Process	106
A.7	Troubleshooting a Linux SSL Renegotiation	107
A.8	Secondary Administration Console Installation Fails	108
A.9	Access Gateway Appliance Installation Fails Due to an XML Parser Error	108
A.10	Troubleshooting the Uninstall of the Access Gateway Service	108
A.11	Troubleshooting the Uninstall of the Windows Identity Server	109
A.12	Portal Web Server is not Accessible	109
A.13	Installing RHEL on the Administration Console Fails if IPv6 is Disabled	109
B	Feature Comparison of Different Types of Access Gateways	111
C	Installing Packages and Dependent RPMs on RHEL for Access Manager	119

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

About this Book and the Library

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

Intended Audience

This book is intended for Access Manager administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

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

Other Information in the Library

The library provides the following information resources:

- ♦ [NetIQ Access Manager 4.0 SP1 Setup Guide](#)
- ♦ [NetIQ Access Manager 4.0 SP1 Administration Console Guide](#)
- ♦ [NetIQ Access Manager 4.0 SP1 Identity Server Guide](#)
- ♦ [NetIQ Access Manager 4.0 SP1 Access Gateway Guide](#)
- ♦ [NetIQ Access Manager 4.0 SP1 Policy Guide](#)
- ♦ [NetIQ Access Manager 4.0 SSL VPN Server Guide](#)

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

1 NetIQ Access Manager Product Overview

NetIQ Access Manager is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager also provides seamless single sign-on across technical and organizational boundaries. It uses industry standards including Secure Assertions Markup Language (SAML) and Liberty Alliance protocols. It has a single console for management and configuration. To provide secure access from any location, it supports multi-factor authentication, role-based access control, data encryption, and SSL VPN services.

For information about what's new in Access Manager 4.0, see "[Access Manager 4.0 Hotfix 1 Readme](#)".

This section discusses the following topics:

- [Section 1.1, "How Access Manager Solves Business Challenges," on page 11](#)
- [Section 1.2, "How Access Manager Works," on page 19](#)
- [Section 1.3, "Access Manager Devices and Their Features," on page 21](#)
- [Section 1.4, "Differences Between Access Manager and Access Manager Appliance," on page 25](#)
- [Section 1.5, "Recommended Installation Scenarios," on page 29](#)

1.1 How Access Manager Solves Business Challenges

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

Access Manager lets you provide employees, customers, and partners with secure access to your network resources. If your business faces any of the following access-related challenges, Access Manager can help:

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

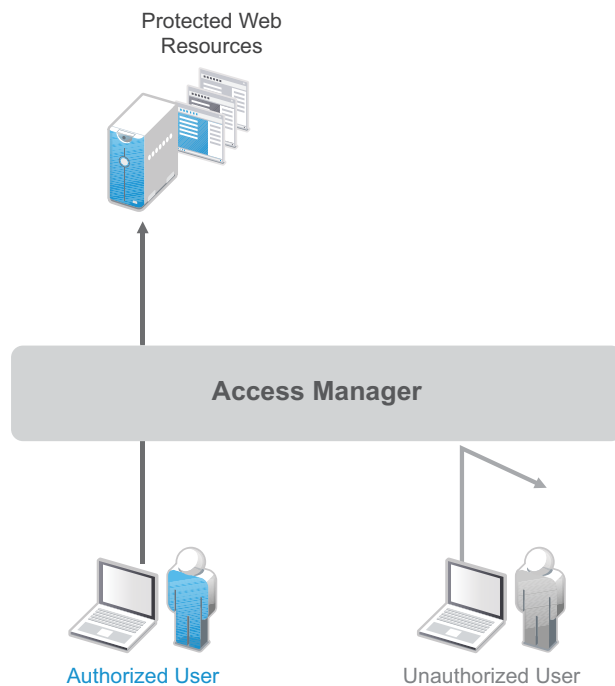
- ♦ Protecting users' privacy and confidential information as they access company resources or partners' resources.
- ♦ Proving compliance with your business policies, privacy laws such as Sarbanes-Oxley, HIPAA, or European Union, and other regulatory requirements.

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

- ♦ [Section 1.1.1, "Protecting Resources While Providing Access," on page 12](#)
- ♦ [Section 1.1.2, "Managing Passwords with Single Sign-On," on page 13](#)
- ♦ [Section 1.1.3, "Enforcing Business Policies," on page 14](#)
- ♦ [Section 1.1.4, "Sharing Identity Information," on page 15](#)
- ♦ [Section 1.1.5, "Protecting Identity Information," on page 17](#)
- ♦ [Section 1.1.6, "Complying with Regulations," on page 18](#)

1.1.1 Protecting Resources While Providing Access

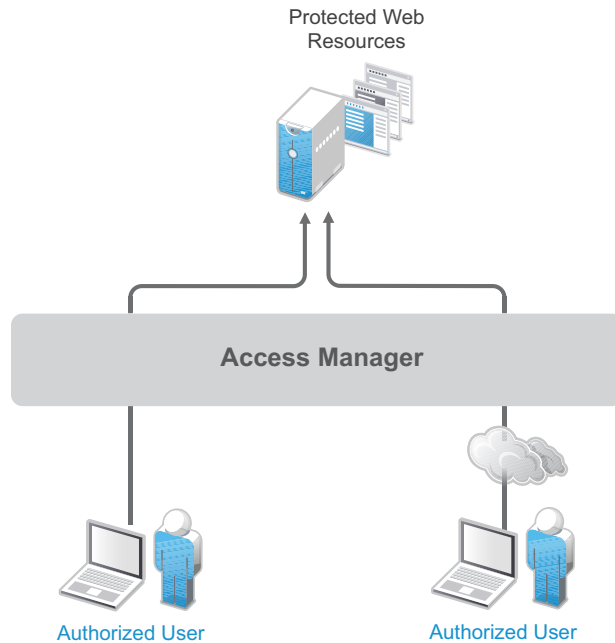
The primary purpose of Access Manager is to protect resources by allowing access only to users you have authorized. You can control access to Web (HTTP) resources and traditional server-based (non-HTTP) resources. As shown in the following illustration, those users who are authorized to use the protected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



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

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

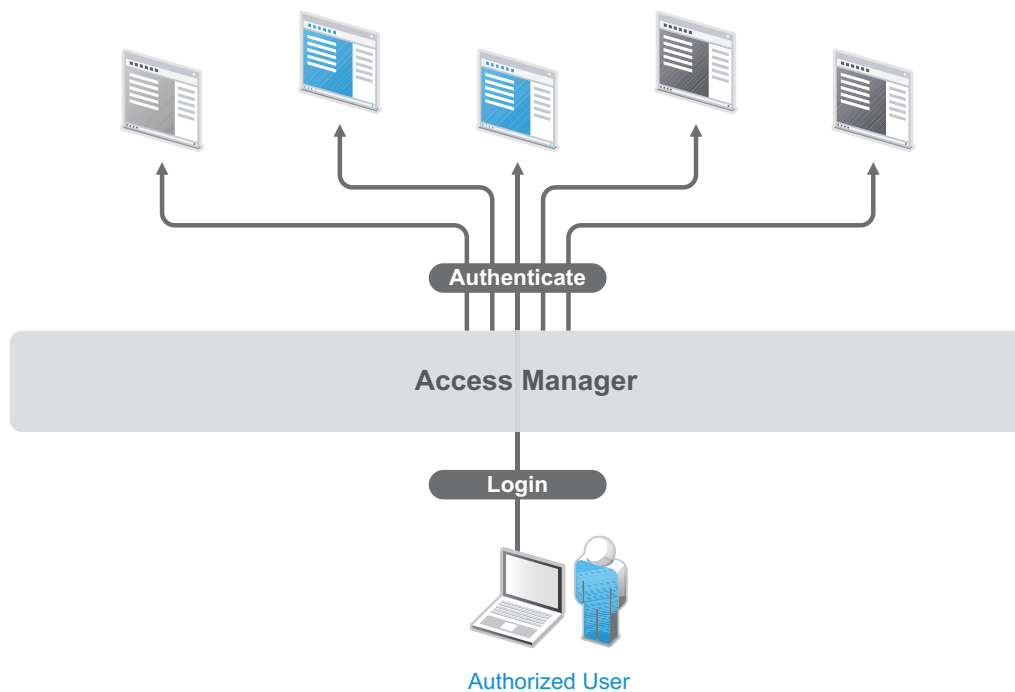
Access to resources is independent of a user's location, as shown in the following illustration. Access Manager provides the same secure access and same experience whether the user is accessing resources from your local office, from home, or from an airport terminal.



1.1.2 Managing Passwords with Single Sign-On

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

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



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

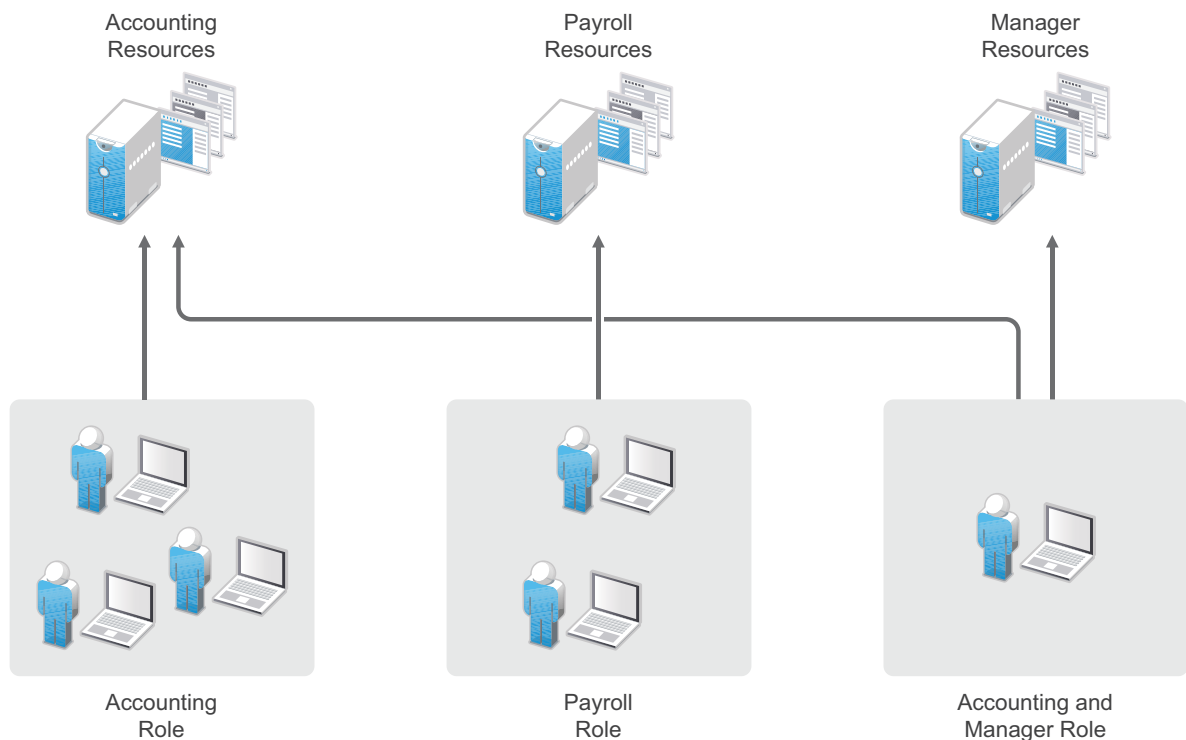
1.1.3 Enforcing Business Policies

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

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



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



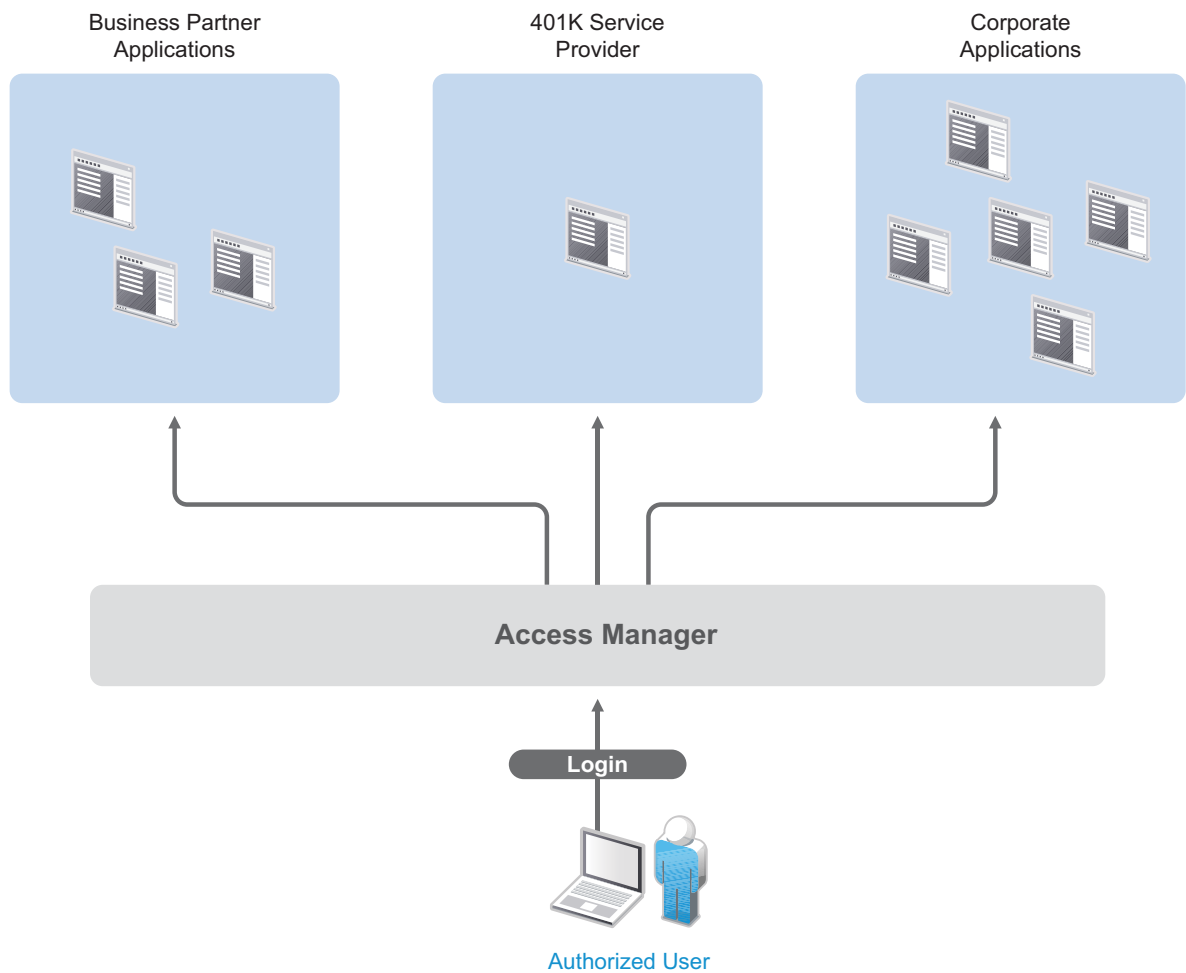
Because access is based on roles, you can grant access in minutes and be certain that the access is consistent with your business policies. And, equally important, you can revoke access in minutes by removing role assignments from users.

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

1.1.4 Sharing Identity Information

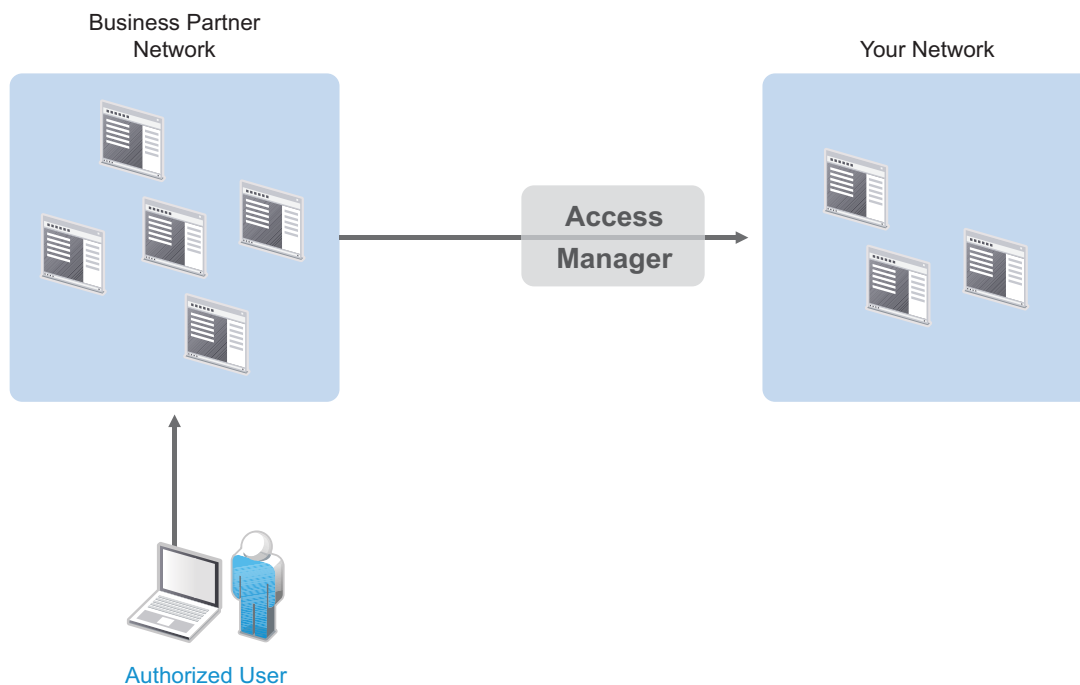
In today's business environment, few organizations stand alone. More than likely, you have trusted business partners with whom you need to share resources in a secure manner. Or, you have business services, such as a 401k management system, to which you need to provide employee access. Or, maybe your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

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



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

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



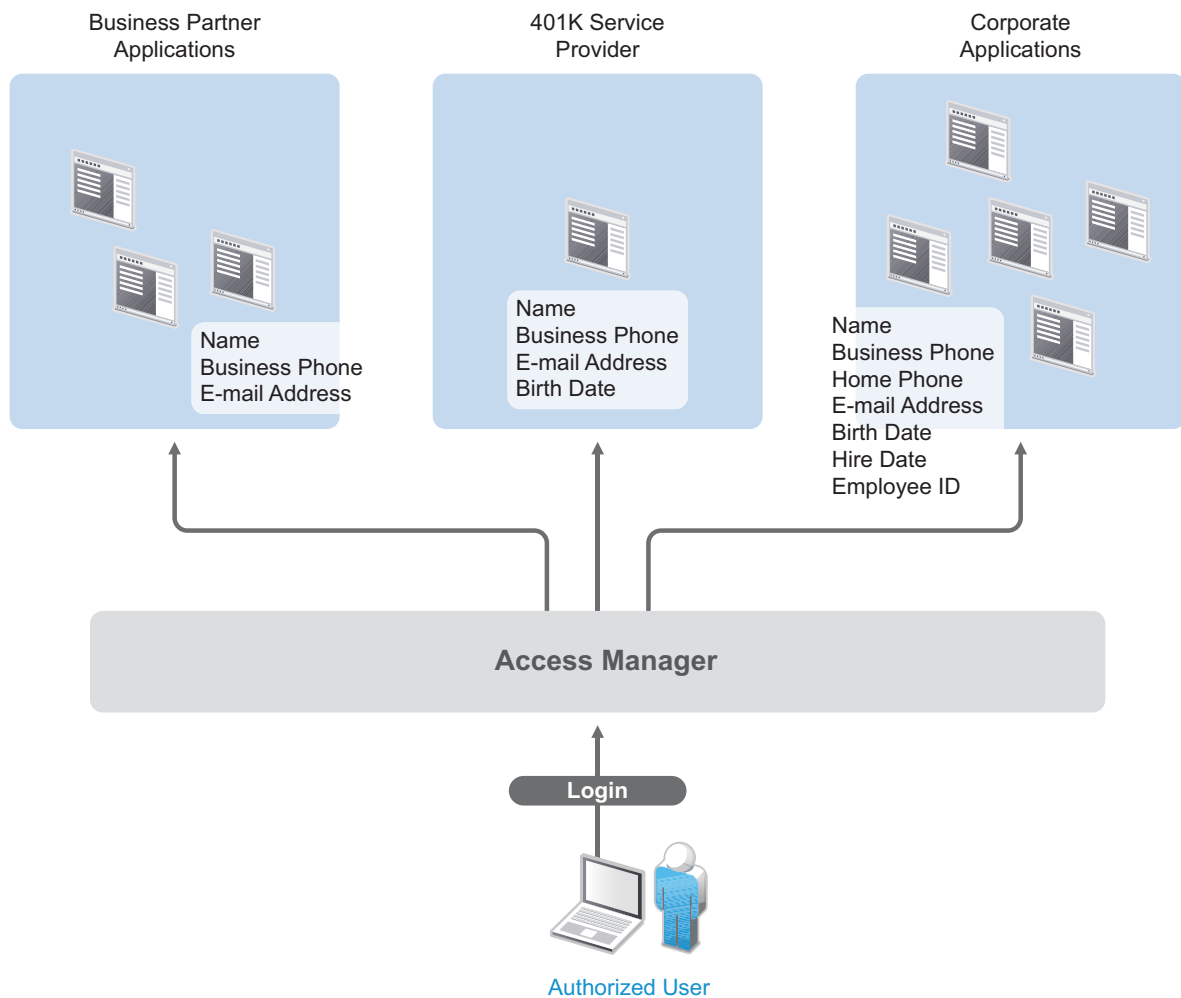
In addition to simply linking user accounts in different identity domains, Access Manager also supports federated provisioning, which means that new user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization can initiate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

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

1.1.5 Protecting Identity Information

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

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



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

1.1.6 Complying with Regulations

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

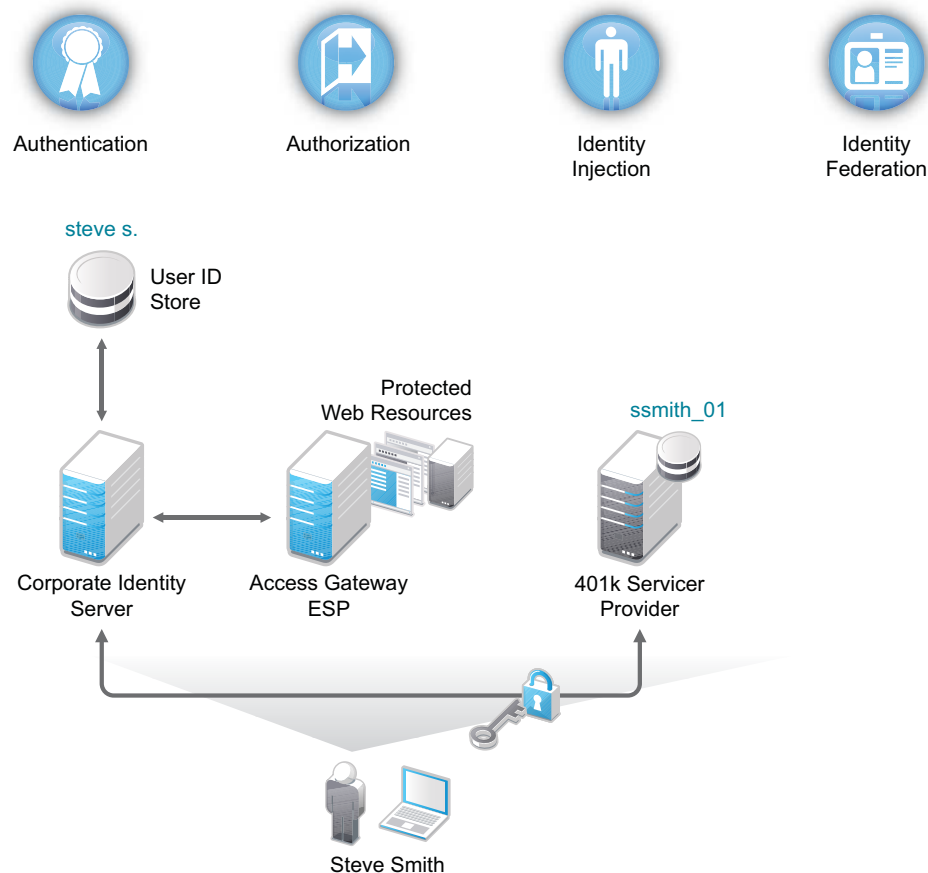
Specifically, Access Manager helps you stay in compliance with Sarbanes-Oxley, HIPAA, European Union privacy laws and other regulatory requirements—and you'll find it easy to prove your compliance. For an internal assessment or an external auditor, Access Manager can generate the reports you need, turning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

1.2 How Access Manager Works

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

Figure 1-1 illustrates the primary purposes of Access Manager: [authentication](#), [identity federation](#), [authorization](#), and [identity injection](#).

Figure 1-1 Access Manager



1.2.1 Authentication

The [Identity Server](#) facilitates authentication for all Access Manager components. This authentication is shared with internal or external service providers on behalf of the user, by means of assertions. Access Manager supports a number of authentication methods, such as name/password, RADIUS token-based authentication, X.509 digital certificates, Kerberos, and OpenID. You specify authentication methods in the contracts that you want to make available to the other components of Access Manager, such as the Access Gateway.

User data is stored in user stores. User stores are LDAP directory servers to which end users authenticate. You can configure a user store with more than one replica to provide load balancing and failover capability.

1.2.2 Authorization

Authentication is the process of determining who a user is. Authorization is the process of determining what a user is allowed to do. Access Manager allows you to configure roles and authorization policies, based on criteria other than authentication, to protect a resource. Authorization policies are dynamically applied after authentication and are enforced when a user attempts to access a protected resource.

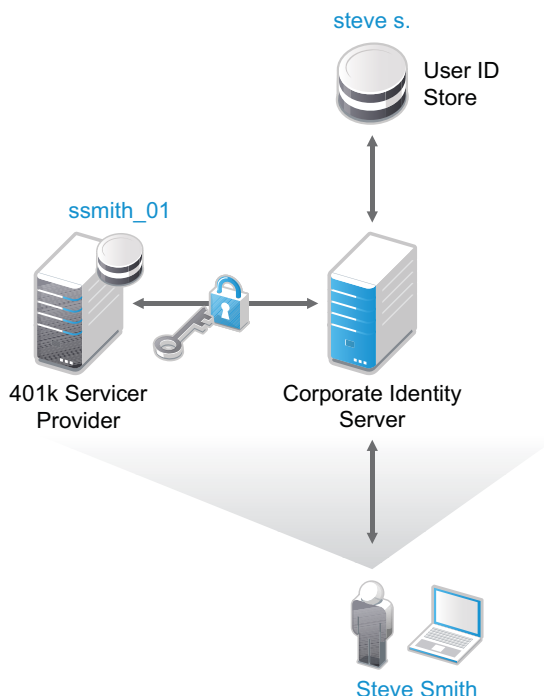
1.2.3 Identity Injection

An [Access Gateway](#) lets you retrieve information from your LDAP directory, use it to inject information into HTML headers, query strings, or basic authentication headers, and send this information to the back-end Web servers. Access Manager calls this technology *identity injection* (iChain calls it object level access control). The Web server uses this information to personalize content, or can use it for additional authorization decisions. Where Web servers require additional authentication, Identity Injection can also provide the necessary credentials to perform a single sign-on.

1.2.4 Identity Federation

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

Figure 1-2 Identity Federation



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

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

1.3 Access Manager Devices and Their Features

- [Section 1.3.1, "Administration Console," on page 21](#)
- [Section 1.3.2, "Identity Servers," on page 21](#)
- [Section 1.3.3, "Access Gateways," on page 22](#)
- [Section 1.3.4, "SSL VPN," on page 24](#)
- [Section 1.3.5, "Policies," on page 24](#)
- [Section 1.3.6, "Certificate Management," on page 24](#)
- [Section 1.3.7, "Embedded Service Provider," on page 25](#)
- [Section 1.3.8, "The User Portal Application," on page 25](#)
- [Section 1.3.9, "Language Support," on page 25](#)

1.3.1 Administration Console

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

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

1.3.2 Identity Servers

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

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

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

- **Authentication:** Verifies user identities through various forms of authentication, both local (user supplied) and indirect (supplied by external providers). The identity information can be some characteristic attribute of the user, such as a role, e-mail address, name, or job description.
- **Identity Stores:** Links to user identities stored in eDirectory, Microsoft Active Directory, or Sun ONE Directory Server.
- **Identity Federation:** Enables user [identity federation](#) and provides access to Liberty-enabled services.

- ♦ **Account Provisioning:** Enables service provider account provisioning, which automatically creates user accounts during a federation request.
- ♦ **Custom Attribute Mapping:** Allows you to define custom attributes by mapping Liberty Alliance keywords to LDAP-accessible data, in addition to the available Liberty Alliance Employee and Person profiles.
- ♦ **SAML Assertions:** Processes and generates SAML assertions. Using SAML assertions in each Access Manager component protects confidential information by removing the need to pass user credentials between the components to handle session management.
- ♦ **Single Sign-on and Logout:** Enables users to log in only once to gain access to multiple applications and platforms. Single sign-on and single logout are primary features of Access Manager and are achieved after the federation and trust model is configured among trusted providers and the components of Access Manager.
- ♦ **Identity Integration:** Provides authentication and identity services to [Access Gateways](#) that are configured to protect Web servers. The Access Gateway and other Access Manager components include an embedded service provider that is trusted by NetIQ Access Manager Identity Servers.
- ♦ **Roles:** Provides RBAC (role-based access control) management. RBAC is used to provide a convenient way to assign a user to a particular job function or set of permissions within an enterprise, in order to control access. The identity provider service establishes the active set of roles for a user session each time the user is authenticated. Roles can be assigned to particular subsets of users based on constraints outlined in a role policy. The established roles can then be used in authorization [policies](#) to form the basis for granting and restricting access to particular Web resources.

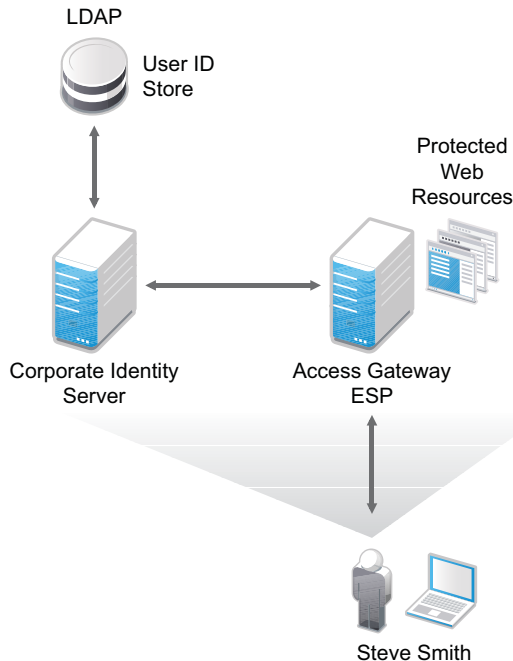
For an overview of Liberty, see “[About Liberty](#)” in the *[NetIQ Access Manager 4.0 SP1 Identity Server Guide](#)*.

For an overview of SAML, see “[Understanding How Access Manager Uses SAML](#)” in the *[NetIQ Access Manager 4.0 SP1 Identity Server Guide](#)*.

1.3.3 Access Gateways

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

Figure 1-3 Access Gateway Component



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

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

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

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

There are two types of Access Gateways. Both are based on the same core technology and differ only in their deployment method.

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

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

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

For more information about the differences, see [Appendix B, “Feature Comparison of Different Types of Access Gateways,” on page 111](#).

For information about how to upgrade or migration your chosen Access Gateway technology, see [“Upgrading Access Manager” in the *NetIQ Access Manager 4.0 SP2 Migration and Upgrade Guide*](#).

1.3.4 SSL VPN

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

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

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

1.3.5 Policies

Policies provide the authorization component of Access Manager. The administrator of the Identity Server can use policies to define how properties of a user's authenticated identity map to the set of active roles for the user. This role definition serves as the starting point for role-based authorization policies of the Access Gateway. Additionally, authorization policies can be defined that control access to protected resources based on user and system attributes other than assigned roles.

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

The Access Gateway includes an Embedded Service Provider agent that interacts with the Identity Server to provide authentication, policy decision, and enforcement. For Web application servers, the Access Gateway provides the ability to inject the user's roles into HTTP headers to allow integration with the Web server's authorization processes.

1.3.6 Certificate Management

Access Manager includes a certificate management service, which allows you to manage the certificates used for digital signatures and data encryption. You can create locally signed certificates or import externally signed certificates, then assign these certificates to the trust stores and keystores of the following components:

- ♦ **Identity Server:** Certificates allow you to provide secure authentication to the Identity Server and enable encrypted content from the Identity Server portal, via HTTPS. They also provide secure communications between trusted Identity Servers and user stores.
- ♦ **Access Gateway:** Uses server certificates and trusted roots to protect Web servers, provide single sign-on, and enable the product's data confidentiality features, such as encryption.
- ♦ **SSL VPN:** Uses server certificates and trusted roots to secure access to non-HTTP applications.

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

1.3.7 Embedded Service Provider

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

1.3.8 The User Portal Application

The Access Manager User Portal is a customizable application where end users can access and manage their authentications, federations, and profile data. The authentication methods you create in the Administration Console are reflected in the Portal.

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

1.3.9 Language Support

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

The User Portal, which appears when the user logs directly into the Identity Server, is localized and so is its help file. The User Portal is localized for German, French, Spanish, Italian, Japanese, Portuguese, Dutch, Chinese (Simplified), and Chinese (Traditional). The language must be set in the client's browser to display a language other than English

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

- ♦ For the Access Gateway, see “[Customizing Error Messages and Error Pages on Access Gateway](#)” in the *NetIQ Access Manager 4.0 SP1 Access Gateway Guide*.
- ♦ For the Identity Server, see “[Customizing Identity Server Messages](#)” in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.

1.4 Differences Between Access Manager and Access Manager Appliance

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

You can find Access Manager Appliance documentation here: (https://www.netiq.com/documentation/netiqaccessmanager4_appliance/)

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

Features	Access Manager Appliance	Access Manager
Installation	All the components, such as the Identity Server and Access Gateway are installed on a single server.	Each Access Manager component such as the Identity Server and Access Gateway can be installed on different machines. To deploy the existing solution in a cluster mode, at least 6 machines are required.
Time to Value	During installation and configuration of Access Manager Appliance, several steps are automated to quickly set up the system.	Installation and configuration of Access Manager requires more time because the components are on different servers.
User Input Required during Installation	Access Manager Appliance is a software appliance that takes only a few basic parameters as input. Several options assume default values.	With Access Manager, you have more flexibility during installation in terms of selectable parameters.
Installation and Configuration Phases	The installation program takes care of configuration for each component. The product is ready for use after it is installed.	Separate installation and configuration phases for each component. After installation, each Access Manager component is separately configured.
Host Operating System	A soft appliance that includes a pre-installed and configured SUSE Linux operating system. Both the operating system and Access Manager patches are maintained by NetIQ through the patch update channel.	The operating system choice is more flexible. Install Administration Console, Identity Server and Access Gateway on a supported operating system (SUSE, Red Hat, or Windows). The patch update channel maintains the patches for Access Manager. You must purchase, install, and maintain the underlying operating system.
Component Installation Flexibility	Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.	Each Access Manager component such as Administration Console, Identity Server, and Access Gateway are installed on independent host servers. Although the ability to install multiple components on a single host server exists, it is very limited and generally not recommended. A typical highly available deployment requires 6-8 or more virtual or physical servers (two Administration Consoles, two Identity Servers, and two Access Gateways).

Features	Access Manager Appliance	Access Manager
Administration Console Access	The Administration Console is installed on Access Manager Appliance along with all other components. If you use two network interfaces, access to the Administration Console can be limited to the private IP network bound to the internal network. The public interface is bound to an externally accessible network.	The Administration Console can be installed on an independent host inside your private network but can still securely manage Access Manager components that reside in your DMZ or external network.
Scalability and Performance	<p>The Access Manager Appliance scales vertically on adding CPU and memory resources to each node.</p> <p>For more information, see Performance and Sizing Guidelines.</p>	<p>The Access Manager scales both vertically and horizontally on adding nodes.</p> <p>For more information, see Performance and Sizing Guidelines.</p>
Mode of release	Access Manager is delivered as a software appliance.	Access Manager is delivered in the form of multiple operating system-specific binaries.
Networking: Port Details	The Administration Console and Identity Server are accelerated by Access Gateways. Only HTTPS port 443 is required in the firewall to deploy Access Manager Appliance.	Multiple ports need to be opened for deployment.
Networking: General	The Administration Console can be in a DMZ or in a private network. If Administration Console is in a DMZ, restrict access through the private interface.	Because the Administration Console is a separate component, access can be restricted or the Administration Console can be placed in an internal network.
Certificate Management	<p>Certificate management is simplified. All certificates and key stores are stored in one place making replacing or renewing certificates easier.</p> <p>The same certificate is used for all communication. (Signing, encryption, and transport).</p>	<p>Changes are required in multiple places to replace or renew certificates.</p> <p>Because there are multiple key stores, you can configure different certificates for the communication.</p>
Signing Certificates for Service Providers	Associating different signing certificates for each service provider is not supported.	<p>A unique signing certificate can be assigned to each service provider.</p> <p>In environments with a large number of trust relationships, this feature eases the process of replacing expiring certificates.</p>
Associating Different Certificates to Identity Server	This capability is not applicable because the Identity Server is accelerated by the Access Gateway.	This capability is supported. The Identity Server can be behind the Access Gateway or can be placed separately in the DMZ.

Features	Access Manager Appliance	Access Manager
Sample Portal	After a successful installation, a sample Web portal is deployed for the administrator's reference. The administrator can access the sample portal by using the http://hostname URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.	A sample portal is not available.
Ready-made Access Manager	<p>The following configuration steps are automatically completed when Access Manager Appliance is installed:</p> <ul style="list-style-type: none"> ♦ Importing Identity Server and Access Gateway components. ♦ Automatic clustering of Identity Server and Access Gateway components. ♦ Automatic configuration of Identity Server to bring these to the green state. ♦ Automatic configuration of Access Gateways and Identity Server association. ♦ Automatic service creation to accelerate the Identity Server, Administration Console, and portal. 	Each component is manually configured and set up before Web applications can be federation enabled, accelerated and protected.
64-bit Support	For better performance and scalability, a 64-bit support has been provided for all components.	Not all components provide 64-bit support.
Upgrade	You can upgrade from one version of Access Manager Appliance to another version. Upgrading from Access Manager to Access Manager Appliance is not supported.	You can upgrade from one version of Access Manager to another version. Upgrading from Access Manager Appliance to Access Manager is not supported.
Migration between Models	During migration from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration should be done manually.	During migration from Access Manager to Access Manager Appliance, the policies can be exported but the rest of the configuration should be done manually.
NIC Bonding	IP address configuration is done through the Administration Console. So, NIC bonding is not supported.	NIC bonding can be done through the operating system and Access Manager uses this configuration
Updating Kernel with Security Patches	Access Manager Appliance supports installation of the latest SLES operating system security patches.	You are fully responsible for all operating system maintenance including patching.

Features	Access Manager Appliance	Access Manager
Clustering	<p>For additional capacity and for failover, cluster a group of NetIQ Access Manager Appliances and configure them to act as a single server.</p> <p>You can cluster any number of Identity Servers, Access Gateways, and up to three Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, and Access Gateway. For the fourth installation onwards, the node has all components except for the Administration Console.</p>	<p>For additional capacity and for failover, cluster a group of Identity Servers and configure them to act as a single server. You can create a cluster of Access Gateways and configure them to act as a single server. Fault tolerance can be achieved by installing up to two secondary consoles.</p> <p>To deploy the existing solution in a cluster mode, at least 6 systems are required.</p>

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

1.5 Recommended Installation Scenarios

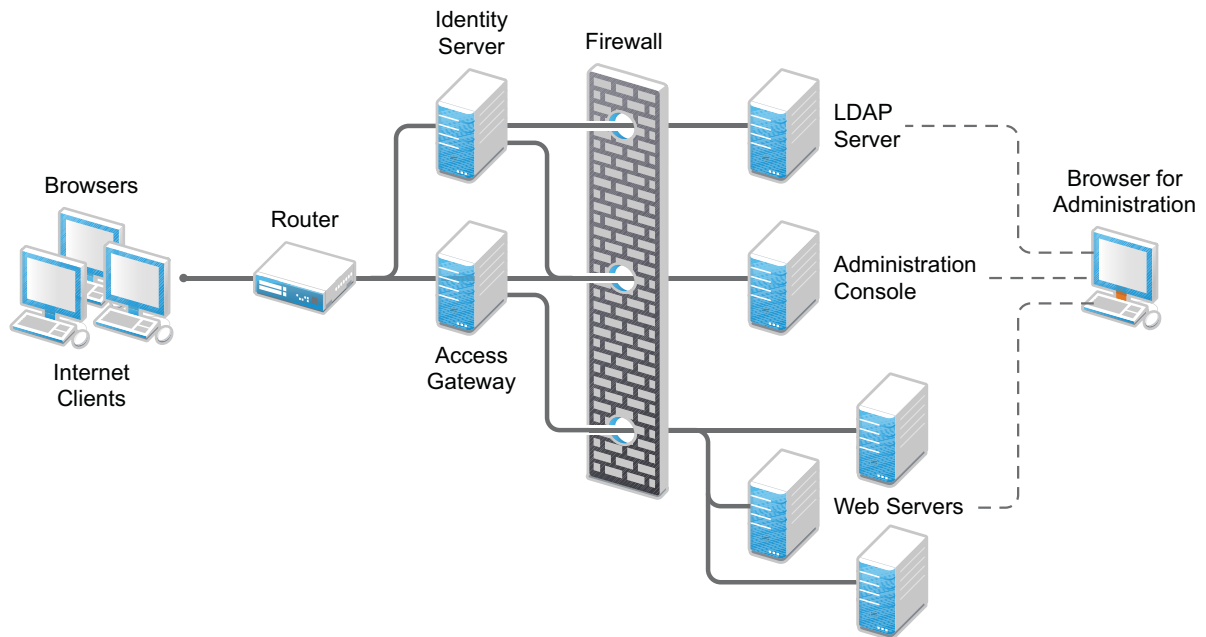
The following scenarios provide an overview of the flexibility built into Access Manager. Use them to design a deployment strategy that fits the needs of your company.

- ♦ [Section 1.5.1, “Basic Setup,” on page 30](#)
- ♦ [Section 1.5.2, “High Availability Configuration with Load Balancing,” on page 31](#)

1.5.1 Basic Setup

For a basic Access Manager installation, you can install the Identity Server and the Access Gateway outside your firewall. [Figure 1-4](#) illustrates this scenario:

Figure 1-4 Basic Installation Configuration



- 1 Install the Administration Console.

The Administration Console and the Identity Server are bundled in the same download file or ISO image.

- 2 If your firewall is set up, open the ports required for the Identity Server and the Access Gateway to communicate with the Administration Console: TCP 1443, TCP 8444, TCP 1289, TCP 524, TCP 636.

For more information about these ports, see [Chapter 8, "Setting Up Firewalls," on page 81](#).

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

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

- 4 Install the Access Gateway.

Log in to the Administration Console and verify that the Access Gateway imported successfully.

- 5 Configure the Identity Server and the Access Gateway. See ["Setting Up a Basic Access Manager Configuration"](#) in the [NetIQ Access Manager 4.0 SP1 Setup Guide](#).

In this configuration, the LDAP server is separated from the Identity Server by the firewall. Make sure you open the required ports. See [Chapter 8, "Setting Up Firewalls," on page 81](#).

For information about setting up configurations for fault tolerance and clustering, see ["Clustering and Fault Tolerance"](#) in the [NetIQ Access Manager 4.0 SP1 Setup Guide](#).

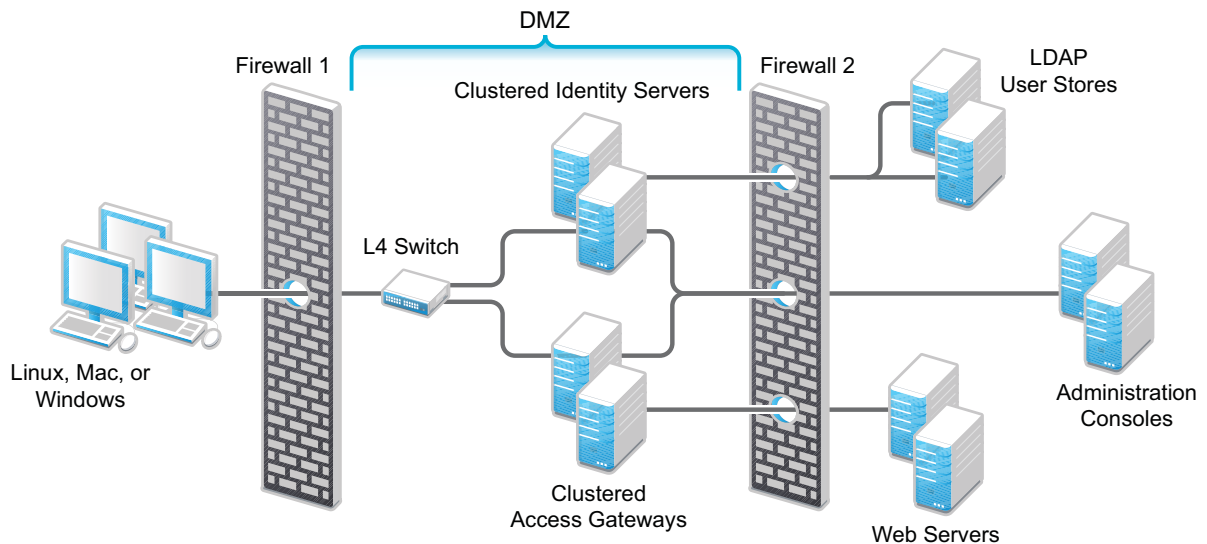
The firewall protects the LDAP server and the Administration Console, both of which contain a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. The Identity Server is not much of a security risk, because it does not permanently store

any user data. This is a configuration that 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.

1.5.2 High Availability Configuration with Load Balancing

Figure 1-5 illustrates a deployment scenario where Web resources are securely accessible from the Internet. The scenario also provides high availability because both the Identity Servers and the Access Gateways are clustered and have been configured to use an L4 switch for load balancing and fault tolerance.

Figure 1-5 Clustering Configuration for High Availability



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

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

2 Installing the Administration Console

Administration Console is the first component you install. If you have iManager installed for other products, you still need to install this version on a separate server. The Administration Console is installed with an embedded version of eDirectory, which is used as the configuration store for Access Manager.

For a functioning system, you need an Administration Console for configuration and management, an Identity Server for authentication, and an Access Gateway for protecting resources. The Administration Console must be installed before you install any other Access Manager devices.

After you have installed the Administration Console, the installation scripts for the other components (Identity Server, Access Gateway, and SSL VPN) auto-import their configurations into the Administration Console.

This chapter explains how to install and configure the Administration Console. Topics include:

- ♦ [Section 2.1, “Installing the Administration Console on Linux,” on page 33](#)
- ♦ [Section 2.2, “Installing the Administration Console on Windows,” on page 39](#)
- ♦ [Section 2.3, “Logging In to the Administration Console,” on page 42](#)
- ♦ [Section 2.4, “Enabling the Administration Console for Multiple Network Interface Cards,” on page 43](#)

For information about installing a secondary Administration Console and fault tolerance, see [“Installing Secondary Versions of the Administration Console”](#) in the [“NetIQ Access Manager 4.0 SP1 Setup Guide”](#).

2.1 Installing the Administration Console on Linux

- ♦ [Section 2.1.1, “Installation Requirements on Linux,” on page 33](#)
- ♦ [Section 2.1.2, “Installation Procedure,” on page 36](#)

2.1.1 Installation Requirements on Linux

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

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

- ♦ If you have custom partitioned your hard disk with partitions as in the table below, ensure that you have free disk space mentioned against each partition:

Partitions	Disk Space
/opt/novell	1 GB
/opt/volera	5 MB

Partitions	Disk Space
/var/opt/novell	1GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10MB
/	512 MB

- ♦ One of the following operating systems:
 - ♦ SUSE Linux Enterprise Server (SLES) 11 SP 2 and SP3 with 64-bit operating system (physical or virtual) x86-64 hardware. Ensure that the following packages are installed:

Package	Description
perl-gettext, gettext-runtime	The required library and tools to create and maintain message catalogs.
python	The basic Python library.
compat	Libraries to address compatibility issues. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogId=68926420&statId=0%200%20130264119) Use the following command to verify: <code>rpm -qa grep <package name></code> Use YaST to install the packages.

- ♦ Red Hat Enterprise Linux (RHEL) 6.4, 6.5 (64-bit) (physical or virtual) and 6.6 (64-bit) (physical or virtual). For installing the RHEL packages, see [Appendix C, “Installing Packages and Dependent RPMs on RHEL for Access Manager,”](#) on page 119.

NOTE: For details about installing Access Manager 4.0 SP1 on RHEL 6.6, see [TID 7016215](#).

- ♦ Install the latest `net-snmp` package from the SLES or RedHat update channel.
- ♦ Zip and unzip utilities must be available for the backup and restore procedure.
- ♦ Ports 389 and 636 need to be free.
- ♦ Static IP address (if the IP address changes after devices have been imported, these devices can no longer communicate with the Administration Console.)

- ♦ The tree for the configuration store is named after the server on which you install the Administration Console. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.
- ♦ The Administration Console can be installed on the same server as the Identity Server. If you are planning to install an L4 switch on a SLES server by using the Linux Virtual Services software, you can also install the Administration Console on this server.

IMPORTANT: You cannot install the following with the Administration Console:

- ♦ OpenLDAP. If it is installed, you must remove it.
 - ♦ LDAP software such as eDirectory.
 - ♦ Other version of iManager. You also cannot add other iManager product plug-ins to this Administration Console.
 - ♦ Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.
 - ♦ JRE. If you have a version installed, uninstall it.
-

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 8.8.8 or later, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- ♦ Web servers with content or applications that need protection.
- ♦ Clients with an Internet browser.
- ♦ An L4 switch if you are going to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- ♦ Static IP addresses for each machine used for an Access Manager component. If the IP address of the machine changes, the Access Manager component or components on that machine cannot start.
- ♦ Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

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

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

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

Browser Support

- ♦ Internet Explorer 8.x and later
- ♦ Mozilla Firefox

Browser pop-ups must be enabled to use the Administration Console. If you are using the latest version of Firefox, use the latest version of Sun (Oracle) JRE.

2.1.2 Installation Procedure

Installation time: about 20 minutes.

What you need to create during installation

A username and password for the Administrator.

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

- 1 If you have Red Carpet or auto update running, stop these programs before you install the Administration Console.
- 2 Verify that the machine meets the minimum requirements. See [Section 2.1.1, “Installation Requirements on Linux,” on page 33](#).
- 3 Open a terminal window.
- 4 Access the install script as root:
 - 4a Ensure that you have downloaded the software or you have the CD available.
For software download instructions, see the “[Access Manager 4.0 Hotfix 1 Readme](#)”.
 - 4b Do one of the following:
 - ♦ Insert the CD into the drive, then navigate to the device. Specify the following:

```
cd /media
```


Change to your CD-ROM drive, which is usually `cdrom` but can be something else such as `cdrecorder` or `dvdrecorder`, depending on your hardware.
 - ♦ If you downloaded the `tar.gz` file, unzip it by using the following command:

```
tar -xzf <filename>
```
 - 4c Change to the `novell-access-manager` directory.
- 5 At the command prompt, specify the following:

```
./install.sh
```


Ensure that you have adequate space in the system before you proceed with installation.
- 6 When you are prompted to install a product, select **1. Install Administration Console** and then press Enter.
- 7 Review and accept the License Agreement.
Novell Base and JDK for NetIQ are installed.
- 8 (Optional) The installer displays a warning if the host name of the system is mapped to the IP address 127.0.0.2 in the `/etc/hosts` file:

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

Specify **Y** to proceed.

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

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

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

- 10 Specify the administration username.

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

NOTE: The Administration Console username does not accept special characters # (hash), & (ampersand), and () (round brackets).

- 11 Specify the administration password.

Use alphanumeric characters only.

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

- 12 Confirm the password, then wait for the system to install components.

This may take several minutes depending on the speed of your hardware.

The following components are installed:

Component	Description
Audit Platform Agent	Responsible for packaging and forwarding the audit log entries to the configured Novell Audit Server. For more information, see “Enabling Auditing” in the “NetIQ Access Manager 4.0 SP1 Administration Console Guide” .
Tomcat for NetIQ	NetIQ packaging of the Java-based Tomcat Web server used to run servlets and JavaServer Pages (JSP) associated with NetIQ Access Manager Web applications.
Access Manager Configuration Store	An embedded version of eDirectory used to store user-defined server configurations, LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored.
iManager	The Web-based Administration Console that provides customized and secure access to server administration utilities. It is a modified version and cannot be used to manage other eDirectory trees.
Audit Server	Audit Server is bundled with the Administration Console to monitor and log all enabled Access Manager components. For more information, see “Enabling Auditing” in the “NetIQ Access Manager 4.0 SP1 Administration Console Guide” .

Component	Description
Administration Console	A modification of iManager that enables management of all aspects of Access Manager. This component is not a standard iManager plug-in. It significantly modifies the tasks that iManager can perform.
Identity Server Administration Plug-In	Works in conjunction with the Administration Console to specifically manage the Identity Server.

13 Record the login URL.

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

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

Use this to configure Access Manager components.

14 Continue with “[Configuring the Linux Administration Console Firewall](#)” on page 38.

Configuring the Linux Administration Console Firewall

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

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

This launches the Firewall Configuration screen.

2 Click **Allowed Services > Advanced.**

3 In the **TCP Ports field, specify the ports to open.**

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

- ♦ 8080
- ♦ 8443
- ♦ 3080
- ♦ 3443

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

- ♦ 2080
- ♦ 2443

4 (Conditional) If you are importing an Access Gateway into the Administration Console, list the following additional ports in the **TCP Ports field:**

- ♦ 1443
- ♦ 8444
- ♦ 1289
- ♦ 524
- ♦ 636

If you are importing an Access Gateway Appliance, specify `icmp` in the **IP Protocols** field.

For specific information about the ports listed in [Step 3](#) and [Step 4](#), see [Table 8-2 on page 82](#).

NOTE: The Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPS) when Identity Server or SSL VPN is installed on the same machine.

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

6 Restart Tomcat by running the following commands from the Administration Console command line.

```
/etc/init.d/novell-ac stop  
/etc/init.d/novell-ac start
```

7 Continue with [Section 2.3, “Logging In to the Administration Console,”](#) on page 42.

2.2 Installing the Administration Console on Windows

- ♦ [Section 2.2.1, “Installation Requirements on Windows,”](#) on page 39
- ♦ [Section 2.2.2, “Installation Procedure,”](#) on page 39

2.2.1 Installation Requirements on Windows

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

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

- ♦ Windows Server 2008 R2 and 2012 R2, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied.
- ♦ Static IP address.
- ♦ Ports 389 and 636 need to be free.

For information about browser support, see [“Browser Support”](#) on page 36.

For information about network requirements, see [“Network Requirements”](#) on page 35.

2.2.2 Installation Procedure

Installation time: about 20 minutes.

What you need to create during installation

A username and password for the Administrator.

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

- 1 Verify that the machine meets the minimum requirements. See [Section 2.2.1, “Installation Requirements on Windows,”](#) on page 39.
- 2 Close any running applications and disable any virus scanning programs.

3 (Conditional) To use a remote desktop for installation, use one of the following:

- ♦ Current version of VNC viewer
- ♦ Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
- ♦ Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3

4 Download software and execute it.

For software download instructions, see the “[Access Manager 4.0 Hotfix 1 Readme](#)”.

5 Read the introduction, then click **Next**.

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

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

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

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

The first Administration Console installed becomes the primary console.

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

9 Specify an administration user ID and password.

10 Specify the static IP address of the machine.

11 Click **Next**, then review the summary.

A message prompt to enable or disable the SSL renegotiation appears during the installation.

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

SSL renegotiation is disabled by default because the TLS, SSL protocol 3.0 or earlier are vulnerable to man-in-the-middle attack. The preferred option is to disable the SSL renegotiation when using the x509 certificate based authentication under the following scenarios:

11a Browser to identity provider when using the x509 certificate based authentication.

11b Identity provider to identity provider communication when using the x509 certificate for mutual authentication.

11c Secure LDAP connections with mutual authentication into the LDAP user store.

12 Click **Install**.

The configuration database takes awhile to install and configure.

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

Windows Server 2008/2012: `\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`

14 Restart the server.

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

15 (Windows Server 2008/2012) In a terminal window, run the `auditext.exe` utility.

15a Change to the `\Program Files\Novell\NSure Audit` directory.

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

15b Run the following command:

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

Modify the following variables to match your system:

Variable	Description
c:	The drive letter for where the Program Files directory is located.
-u:<admin>	This is name of the Administration Console's administrator. Replace <admin> with the name of your administrator
-p:<novell>	This is administrator's password. Replace <novell> with password of your choice.

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

16 (Windows Server 2008/2012) In a terminal window, run the auditext.exe utility.

16a Change to the \Program Files (x86)\Novell\Nsure Audit directory.

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

16b Run the following command:

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

Modify the following variables to match your system:

Variable	Description
c:	The drive letter for where the Program Files (x86) directory is located.
-u:<admin>	This is name of the Administration Console's administrator. Replace <admin> with the name of your administrator
-p:<novell>	This is administrator's password. Replace <novell> with password of your choice.

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

17 Continue with "Configuring the Windows Administration Console Firewall" on page 41.

Configuring the Windows Administration Console Firewall

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

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

Field	Description
Description of service	Specify a name. For example, Admin Console Access for port 8080 or Secure Admin Console Access for port 8443.
Name or IP address	Specify the IP address of the Administration Console.
External Port number for this service	Specify the port. Open the following ports: <ul style="list-style-type: none"> ♦ 8080 ♦ 8443

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

- ♦ 1443
- ♦ 8444
- ♦ 1289
- ♦ 524
- ♦ 636

For specific information about the ports listed in [Step 3](#) and [Step 4](#), see [Table 8-2 on page 82](#).

- 5 (Conditional) If you are importing an Access Gateway Appliance, click **ICMP**, select all options, then click **OK** twice.
- 6 Run the following commands to restart Tomcat:

```
net stop Tomcat7
net start Tomcat7
```

- 7 Continue with [Section 2.3, "Logging In to the Administration Console," on page 42](#):

2.3 Logging In to the Administration Console

IMPORTANT: The Administration Console is a combination of iManager and a device manager. It has been customized for Access Manager so that it can manage the Access Manager components.

You cannot use it to log in to other eDirectory trees and manage them.

You should not download and add iManager plug-ins to this customized version. It may result in destroying the Access Manager schema, which can prevent you from managing Access Manager components. This can also prevent communication among the modules.

You should not start multiple sessions of the Administration Console on the same machine through the same browser. Browser shares session information and this can cause unpredictable issues in the Administration Console. You can, however, start different sessions with different brands of browsers.

To log in to:

- 1 Enable browser pop-ups.
- 2 On the Administration Console, ensure that ports 8080 and 8443 are open.
For information about how to do this, see [“Configuring the Linux Administration Console Firewall” on page 38](#) and [“Configuring the Windows Administration Console Firewall” on page 41](#).
- 3 From a client machine external to your Administration Console server, launch browser and specify the Administration Console URL.

Use the IP address established when you installed the Administration Console. It should include ports 8080 (HTTP) and 8443 (HTTPS) (if it is installed on a separate machine) and ports 2080 (HTTP) and 2443 (HTTPS) (when Identity Server and SSL VPN are installed on the same machine) and the application `/nps`. If the IP address of your Administration Console for example is 10.10.10.50, specify the following:

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

- 4 Click **OK** to accept the certificate. You can select either the permanent or temporary session certificate option.
- 5 On the Login page, specify the administrator name and password that you defined during the Administration Console installation.
- 6 Click **Login**. Access Manager Dashboard opens.

For more information about this view or about configuring the Administration Console, see [“Configuring the Default View”](#) in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

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

- 7 Continue with one of the following:
 - ♦ Before you can configure the system, you need to install other Access Manager components. You need to install at least one Identity Server and one Access Gateway or SSL VPN. It is recommended to next install the Identity Server. See [Chapter 3, “Installing the Identity Servers,” on page 45](#).
 - ♦ If your Administration Console server has multiple interface cards, see [“Enabling the Administration Console for Multiple Network Interface Cards” on page 43](#).

NOTE: You can provide fault tolerance for the configuration store on the Administration Console by installing secondary versions of the console. See [“Installing Secondary Versions of the Administration Console”](#) in the *“NetIQ Access Manager 4.0 SP1 Setup Guide”*.

2.4 Enabling the Administration Console for Multiple Network Interface Cards

Making the Administration Console available for all network interface cards (NICs) is a security risk. However, you might want to allow this situation if, for example, the Identity Server has multiple NICs and is also available on all ports. You must modify the `server.xml` file:

- 1 Open the `server.xml` file, which is found in the following directory.

Linux: `/opt/novell/nam/adminconsole/conf`

Windows Server 2008/2012: \Program Files (x86)\Novell\Tomcat\conf

- 2 Locate the connector with the `NIDP_Name="connector"` set.
- 3 Delete the `address` attribute and save the file.

3 Installing the Identity Servers

Identity Server is the second component you install. You can install it on Linux or Windows. Clients that authenticate directly to the Identity Server can use any browser or operating system.

This chapter explains how to install the Identity Server. Topics include:

- [Section 3.1, “Installing the Identity Server on Linux,” on page 45](#)
- [Section 3.2, “Installing the Identity Server on Windows,” on page 48](#)

3.1 Installing the Identity Server on Linux

- [Section 3.1.1, “Prerequisites,” on page 45](#)
- [Section 3.1.2, “Installation Requirements on Linux,” on page 46](#)
- [Section 3.1.3, “Installation Procedure,” on page 47](#)

3.1.1 Prerequisites

- If you are installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- Ensure that the Administration Console is running. (See [Chapter 2, “Installing the Administration Console,” on page 33.](#))
- Do not perform any configuration tasks in the Administration Console during an Identity Server installation.
- If you installed the Administration Console on a separate machine, ensure that the DNS names resolve between the Identity Server and the Administration Console.
- When you are installing the Identity Server on a separate machine (recommended for production environments), ensure that the following ports are open on both the Administration Console and the Identity Server:

8444
1443
1289
524
636

For information about how to open ports, see [“Configuring the Linux Administration Console Firewall” on page 38](#) and [“Configuring the Windows Administration Console Firewall” on page 41.](#)

IMPORTANT: When you are installing the Identity Server on a machine with the Administration Console (not recommended for production environments), do not run simultaneous external installations of the Identity Server, Access Gateway, or SSL VPN. These installations communicate with the Administration Console. During installation, Tomcat is restarted, which can disrupt the component import process.

- ♦ Verify that the machine meets the minimum requirements. See [Section 3.1, “Installing the Identity Server on Linux,” on page 45](#).
- ♦ You must establish a static IP address for your Identity Server to reliably connect with other Access Manager components. If the IP address changes, the Identity Server can no longer communicate with the Administration Console.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see “[Preventing Cross-site Scripting Attacks](#)” in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.

3.1.2 Installation Requirements on Linux

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

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

- ♦ If you have custom partitioned your hard disk with partitions as in the table below, ensure that you have free disk space mentioned against each partition:

Partitions	Disk Space
/opt/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10MB
/	512 MB

- ♦ One of the following operating systems:
 - ♦ SUSE Linux Enterprise Server (SLES) 11 SP2 and SP3 with 64-bit operating system (physical or virtual) x86-64 hardware.
 - ♦ Red Hat Enterprise Linux (RHEL) 6.4, 6.5 (64-bit) (physical or virtual) and 6.6 (64-bit) (physical or virtual). For installing the RHEL packages, see [Appendix C, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 119](#).

NOTE: For details about installing Access Manager 4.0 SP1 on RHEL 6.6, see [TID 7016215](#).

- ♦ gettext

- ♦ python (interpreter)
- ♦ Static IP address.

IMPORTANT:

- ♦ No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP.)
 - ♦ Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.
-

For information about network requirements, see [“Network Requirements” on page 35](#).

3.1.3 Installation Procedure

Installation time: about 10 minutes.

What you need to know to install the Identity Server

- ♦ Username and password of the administrator.
 - ♦ (Conditional) IP address of the Administration Console if it is installed on a separate machine.
-

- 1 Open a terminal window.
- 2 Log in to as a `root` user.
- 3 Access the install script.
 - 3a Ensure that you have downloaded the software or that you have the CD available.
For software download instructions, see the [“Access Manager 4.0 Hotfix 1 Readme”](#).
 - 3b Do one of the following:
 - ♦ If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be `/media/cdrom`, `/media/cdrecorder`, or `/media/dvdrrecorder`, depending on your hardware.
 - ♦ If you downloaded the `tar.gz` file, unzip the file by using the following command:

```
tar -xvzf <filename>
```
 - 3c Change to the `novell-access-manager` directory.
- 4 At the command prompt, run the following install script:

```
./install.sh
```
- 5 When you are prompted to install a product, specify **2, Install Identity Server**, then press Enter.
This selection is also used for installing additional Identity Servers for clustering behind an L4 switch. You need to run this install for each Identity Server you add to the cluster.

NOTE: The Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPS) if the Identity Server or SSL VPN is installed on the same machine.

The following warning is displayed:

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

For more information about how to configure NAT, see [“Configuring the Administration Console Behind NAT” on page 77](#).

- 6 Specify ∇ to proceed.
- 7 Review and accept the License Agreement.
- 8 Specify the IP address, user ID, and password for of the primary Administration Console. Specify the local NAT IP address if local NAT is available for the Identity Server.

If the installation program rejects the credentials and IP address, ensure that the correct ports are open on both the Administration Console and the Identity Server, as described in [Section 3.1.1, “Prerequisites,” on page 45](#).

- 9 The following components are installed:

Component	Description
Access Manager Server Communication	Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
Identity Server	Provides authentication and identity services for the other Access Manager components and third-party service providers.
Identity Server Configuration	Allows the Identity Server to be securely configured by the Administration Console. If the installation process terminates at this step, the probable cause is a failure to communicate with the Administration Console. Ensure that you specified the correct IP address.
Access Manager Server Communications Configuration	Enables the Identity Server to auto-import itself into the Administration Console.

- 10 Continue with one of the following:
 - ♦ Verify the installation. See [“Verifying the Identity Server Installation” on page 79](#)
 - ♦ Install an Access Gateway. See [Section 4.1.2, “Installing the Access Gateway Appliance,” on page 52](#) or [Section 4.2, “Installing the Access Gateway Service,” on page 55](#).
 - ♦ Configure the Identity Server. See [“Setting Up a Basic Access Manager Configuration” in the “NetIQ Access Manager 4.0 SP1 Setup Guide”](#).

3.2 Installing the Identity Server on Windows

- ♦ [Section 3.2.1, “Installation Requirements on Windows,” on page 48](#)
- ♦ [Section 3.2.2, “Installation Procedure,” on page 49](#)

3.2.1 Installation Requirements on Windows

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

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

- ♦ Windows Server 2008 R2 and 2012 R2 (physical or virtual), 64-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
- ♦ Static IP address.

IMPORTANT: No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP)

For information about network requirements, see [“Network Requirements” on page 35](#).

3.2.2 Installation Procedure

Installation time: about 10 minutes.

What you need to know to install the Identity Server

- ♦ Username and password of the administrator.
 - ♦ (Conditional) IP address of the Administration Console if it is installed on a separate machine.
-

- 1 Verify that the machine meets the minimum requirements. See [Section 3.2.1, “Installation Requirements on Windows,” on page 48](#).

Ensure that you have read and implemented prerequisites specified in [Section 3.1.1, “Prerequisites,” on page 45](#).

- 2 Close any running applications and disable any virus scanning programs.
- 3 (Conditional) If you have installed the Administration Console on this server, ensure that you have restarted the server before installing the Identity Server.
- 4 (Conditional) To use a remote desktop for installation, use one of the following:
 - ♦ Current version of VNC viewer
 - ♦ Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
 - ♦ Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3

- 5 Download software and run it.

For software download instructions, see the [“Access Manager 4.0 Hotfix 1 Readme”](#).

- 6 Read the introduction, then click **Next**.
- 7 Accept the license agreement, then click **Next**.
- 8 Select **Access Manager Identity Provider**, then click **Next**.

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

- 9 Specify the IP address, user ID, and password for the primary Administration Console.
- 10 (Optional) Specify the Identity Server Local NAT IP address, if the device is behind NAT.
- 11 Click **Next**, review the summary, and click **Install**.
- 12 (Conditional) If you are installing the Identity Server on a machine that contains a previous installation of the Administration Console, you are asked whether the program should overwrite an existing file in the `\Program Files\Novell` directory. Specify yes.
- 13 Continue with one of the following:
 - ♦ Verify the installation. See [“Verifying the Identity Server Installation” on page 79](#)

- ♦ Install an Access Gateway. See [Section 4.1.2, “Installing the Access Gateway Appliance,” on page 52](#) or [Section 4.2, “Installing the Access Gateway Service,” on page 55](#).
- ♦ Configure the Identity Server. See “[Setting Up a Basic Access Manager Configuration](#)” in the “[NetIQ Access Manager 4.0 SP1 Setup Guide](#)”.

NOTE: After you install an Identity Server, you must create a cluster configuration. See “[Clustering Identity Servers](#)” in the “[NetIQ Access Manager 4.0 SP1 Setup Guide](#)”.

4 Installing the Access Gateway

You can install the Access Gateway in one of the following two modes:

- ♦ Appliance: Operating system is installed with the Access Gateway software.
- ♦ Service: The Access Gateway installed on a machine with an existing operating system.

For information about the differences among 3.1 SP4 Access Gateway Appliance, Access Gateway Appliance, Access Gateway Service, see [“Feature Comparison of Different Types of Access Gateways” on page 111](#).

You can install a Gateway Appliance or a Gateway Service after evaluating the functional differences between the two.

This chapter explains how to install the Access Gateway. Topics include:

- ♦ [Section 4.1, “Installing the Access Gateway Appliance,” on page 51](#)
- ♦ [Section 4.2, “Installing the Access Gateway Service,” on page 55](#)

4.1 Installing the Access Gateway Appliance

- ♦ [Section 4.1.1, “Access Gateway Appliance Requirements,” on page 51](#)
- ♦ [Section 4.1.2, “Installing the Access Gateway Appliance,” on page 52](#)

4.1.1 Access Gateway Appliance Requirements

The Access Gateway Appliance runs 64-bit operating system on x86-64 hardware supported by SLES 11 SP2 and SP3. Install it on a separate server because it clears the hard drive and sets up a soft appliance environment.

The Access Gateway Appliance requires the following hardware:

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

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

- ♦ A static IP address for your Access Gateway server and an assigned DNS name (host name and domain name).

For information about network requirements, see [“Network Requirements” on page 35](#).

For a list of hardware that SLES 11 SP2 and SP3 for x86-64 hardware supports, open [YES CERTIFIED Bulletin](#) (<http://developer.novell.com/yessearch/Search.jsp>), select Service Pack 2 or Service Pack 3 for SUSE® SLES 11 SP2 and SP3 in NetIQ Product, and search for your other hardware requirements.

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

4.1.2 Installing the Access Gateway Appliance

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

What you need to know	<ul style="list-style-type: none">◆ Username and password of the administrator.◆ IP address of the Administration Console.◆ Static IP address for the Access Gateway.◆ DNS name (host and domain name) for the Access Gateway that resolves to the IP address.◆ Subnet mask that corresponds to the IP address for the Access Gateway.◆ IP address of your network's default gateway.◆ IP addresses of the DNS servers on your network.◆ IP address or DNS name of an NTP server.
-----------------------	--

The Access Gateway Appliance can be installed on all supported hardware platforms for SUSE Linux Enterprise Server (SLES) 11 SP2 or a higher version.

IMPORTANT: After the Access Gateway Appliance installation, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities.

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

- ◆ [“Prerequisites” on page 52](#)
- ◆ [“Installing the Access Gateway Appliance” on page 52](#)
- ◆ [“Creating Custom Partitions” on page 54](#)

Prerequisites

- ◆ Ensure that you have backed up all data and software on the disk to another machine. The Access Gateway Appliance installation completely erases all the data on your hard disk.
- ◆ Ensure that the server meets the minimum hardware requirements. See [Section 4.1.1, “Access Gateway Appliance Requirements,” on page 51](#).
- ◆ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the [SUSE Linux Enterprise Server 11 Installation Guide \(http://www.novell.com/documentation/sles11/book_sle_deployment/?page=/documentation/sles11/book_sle_deployment/data/book_sle_deployment_pre.html\)](http://www.novell.com/documentation/sles11/book_sle_deployment/?page=/documentation/sles11/book_sle_deployment/data/book_sle_deployment_pre.html).

Installing the Access Gateway Appliance

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

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

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

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

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

- 1 Insert the Access Gateway Appliance CD into the CD drive and boot from CD. The boot screen appears.
- 2 By default, the **Boot From Hard Disk** option is selected. Use the Down-arrow key to select **Install Appliance**.
- 3 Press Enter.
- 4 Review the agreement on the License Agreement page, then click **I Agree**.
- 5 Select the region and time zone on the Clock and Time Zone page.
- 6 (Conditional) If the date and time are not the same as the date and time on the Administration Console, click Change, adjust the date and time.
- 7 Click **Next**.
- 8 Configure the following details on the Appliance Configuration page:

Field	Description
Host Name	The hostname of the Access Gateway Appliance server. IMPORTANT: Do not use <code>linux</code> as hostname. If you do, the Access Gateway is not imported
Domain Name	The domain name for your network.
IP Address	The IP address of the Access Gateway.
Subnet Mask	The subnet mask of the Access Gateway Appliance network.
Default Gateway	The IP address of the default gateway.
DNS Server	The IP address of your DNS server. You must configure at least one DNS server. Specify the IP address of additional your additional DNS server, if you have configured. This is an optional configuration.

In the Root Password section, specify password and the name of the NTP server.

In the NAT Settings section, specify the Access Gateway Local NAT IP Address, if the device is behind NAT.

In the Administration Console configuration section, specify the following:

IP Address	The IP address of the Administration Console. The Access Gateway Appliance is imported into this Administration Console. If you select the Install and Enable SSL VPN Service option, SSL VPN is also imported into the Administration Console.
Username	The name of the Administration Console user.
Password	Specify the password for the user.

Field	Description
Install and enable SSL VPN Service	<p>Select this check box to install and configure the SSL VPN service on the Access Gateway Appliance. When SSL VPN is installed on the same system as the Access Gateway, SSL VPN must be configured as a protected resource of the Access Gateway.</p> <p>IMPORTANT: You cannot uninstall SSL VPN that is installed with the Access Gateway Appliance.</p>

- 9 Click **Next**. The Installation Settings page appears.

This page displays the options and software you selected in the previous steps. Use the Overview tab for a list of selected options, or use the Expert tab for more details. Ensure that all default partitions recommended adhere to the guidelines mentioned in [Table 4-1 on page 54](#).

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

- 10 (Optional) To modify the installation settings for partitions, click **Change**. For more information about partitions, see [“Creating Custom Partitions” on page 54](#).
- 11 Click **Install > Install**.
- This process might take 15 to 30 minutes, depending on the configuration and hardware.
- The machine reboots after the installation is completed. It runs an auto import script, and then the Access Gateway Appliance is imported to the Administration Console.
- 12 Continue with one of the following sections:
- Verify the installation. See [“Verifying the Access Gateway Installation” on page 79](#)
 - Configure the Access Gateway. See [“Setting Up a Basic Access Manager Configuration” in the “NetIQ Access Manager 4.0 SP1 Setup Guide”](#).

Creating Custom Partitions

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

Table 4-1 Access Gateway Appliance Partitions

Partition Type	Requirements
root	This partition contains the boot files, system files, and log files. You should assign 40% of available disk space to this partition. This space should be more than 40 GB.
swap	Create a swap partition that is twice the size of RAM installed on the machine.
var	This partition is used for log files and caching objects of the Access Gateway. Allocate the remaining space for this partition, which should be more than 50 GB. Assign the remaining disk space to var.

To create your custom partitions:

- 1 In the Installation Settings page, click **Change**, then select **Partitioning**. (See [Step 10 on page 54](#).)
- This page lists the partition settings as currently proposed.

- 2 Select **Custom partitioning**, then click **Next**.
- 3 (Conditional) If the installation program discovers any existing partitions, select the hard disk, click **Delete**, then confirm the deletion of the partitions.
- 4 Create a root partition as follows:
 - 4a Click **Add**, select the primary or extended partition, then click **OK**.
 - 4b Specify the following details:

Format: Ensure that **Format** is selected.

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

File system: Select **Ext3** for the type.

Custom Size: Specify a value.

Mount Point: Select **/**.
 - 4c Click **Finish**.
- 5 Create a swap partition as follows:
 - 5a Select the hard drive, click **Create**, select the primary or extended partition, then click **OK**.
 - 5b Specify the following details:

Format: Ensure that **Format** is selected.

File system: Select **Swap** for the type.

Custom Size: Specify a value.

Mount Point: Leave the default value of **swap**.
 - 5c Click **Finish**.
- 6 Create a var partition as follows:
 - 6a Select the hard drive, click **Add**, select the primary or extended partition, then click **OK**.
 - 6b Specify the following details:

Format: Ensure that **Format** is selected.

File system: Select **Ext3** for the type.

Custom Size: Specify a value.

Mount Point: Select **/var**.
 - 6c Click **Finish**.
- 7 Click **Accept** to create partitions with the specified values.
- 8 In the installation Summary page, verify that the partitions you specified are listed, then continue with [Step 11 on page 54](#).

4.2 Installing the Access Gateway Service

- ♦ [Section 4.2.1, “Installing the Access Gateway Service,” on page 55](#)
- ♦ [Section 4.2.2, “Installing the Access Gateway Service on Windows,” on page 59](#)

4.2.1 Installing the Access Gateway Service

- ♦ [“Installing the Access Gateway Service on Linux” on page 56](#)
- ♦ [“Installing the Access Gateway Service on Windows” on page 58](#)

Installing the Access Gateway Service on Linux

IMPORTANT: Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

- ♦ [“Linux Requirements” on page 56](#)
- ♦ [“Prerequisites” on page 56](#)
- ♦ [“Installation Procedure” on page 57](#)

Linux Requirements

- ♦ One of the following operating systems:
 - ♦ SUSE Linux Enterprise Server (SLES) 11 SP2 and SP3 (64-bit) (physical or virtual).
 - ♦ Red Hat Enterprise Linux (RHEL) 6.4, 6.5 (64-bit) (physical or virtual) and 6.6 (64-bit) (physical or virtual)

NOTE: For details about installing Access Manager 4.0 SP1 on RHEL 6.6, see [TID 7016215](#).

- ♦ 4 GB RAM.
- ♦ Dual CPU or Core (3.0 GHz or comparable chip).
- ♦ 2 to 10 GB hard disk space per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- ♦ A static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module does not start.
- ♦ Other Access Manager components should not be installed on the same machine.
- ♦ For installing the RHEL packages, see [Appendix C, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 119](#).
- ♦ (Only for SLES) Ensure that the following rpms or higher versions are installed:
 - ♦ libapr-util-1.3.4-12.22.21.2.x86_64.rpm
 - ♦ libapr1-1.3.3-11.18.17.1.x86_64.rpm
 - ♦ unixODBC-2.2.12-198.17.x86_64.rpm

IMPORTANT

- ♦ SLES installation libraries may be distributed across multiple CDs or DVDs. In **YaST > Software > Software Repositories** select the required CD or DVD to install the rpm files. If the rpm files are not available on the SLES server, the Access Manager installation process takes care of installing these rpm files from the SLES repository.
 - ♦ To search if an rpm is installed, use `rpm -qa | grep <rpm name>`. For example, `rpm -qa | grep libapr-util`.
-

For information about network requirements, see [“Network Requirements” on page 35](#).

Prerequisites

- ♦ An Administration Console must be installed before you install the Access Gateway Service. See [Section 2, “Installing the Administration Console,” on page 33](#).

- ♦ An Identity Server must be installed and configured before installing the Access Gateway Service. See, [Section 3, “Installing the Identity Servers,” on page 45.](#)
- ♦ Verify that the server meets the minimum requirements. See [“Installing the Access Gateway Service on Linux” on page 56.](#)
- ♦ Verify that the time on the machine is synchronized with the time on the Administration Console. If the times differ, the Access Gateway Service does not import into the Administration Console.
- ♦ If a firewall separates the machine and the Administration Console, ensure that the required ports are opened. See [Table 8-2 on page 82.](#)
- ♦ Because the Access Gateway Service is running as a service, the default ports (80 and 443), which the Access Gateway Service uses might conflict with the ports of other services running on the machine. If there is a conflict, you need to decide which ports each service can use.
- ♦ (Windows Server 2008/2012) If the Web server (IIS) has been installed by default during the Windows Server 2008/2012 install. The Access Gateway Service installation program detects its presence from the registry and issues a shutdown command. Even if you have never activated the Web server and if even it is not running, the shutdown command is issued. Because the Access Gateway Service cannot be installed while the IIS server is running, the installation program needs to ensure that it is not running.

NOTE: The Access Gateway Service clustering is supported for devices that are on the same operating system.

Installation Procedure

Installation time: about 10 minutes.

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

IMPORTANT: The Access Gateway Service must be installed on a separate machine.

- 1 Log in to the [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) and follow the link that allows you to download software. For an evaluation version, download the media kit from [Novell Downloads \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).
- 2 Copy the file to your machine.
For the filename, see the NetIQ Access Manager Readme.
- 3 Prepare your machine for installation:
Make your operating system installation media available.
The installation program checks for Apache dependencies and installs any missing packages.
- 4 Start installation by running the following script:

```
./ag_install.sh
```
- 5 Review and accept the License Agreement.
- 6 Specify the IP address, user ID, and password of the primary Administration Console.
- 7 (Optional) Specify the local NAT IP address if the local NAT is available for the Access Gateway.

8 Continue with one of the following sections:

- ♦ Verify the installation. See [“Verifying the Access Gateway Installation” on page 79](#)
- ♦ Configure the Access Gateway. See [“Setting Up a Basic Access Manager Configuration”](#) in the [“NetIQ Access Manager 4.0 SP1 Setup Guide”](#).

Installing the Access Gateway Service on Windows

- ♦ [“Windows Requirements” on page 58](#)
- ♦ [“Installation Procedure” on page 58](#)

Windows Requirements

- ♦ Windows Server 2008 R2 or 2012 R2, 64-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied (physical or virtual)
- ♦ 4 GB RAM
- ♦ Dual CPU or Core (3.0 GHz or comparable chip)
- ♦ 2 to 10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure
- ♦ A static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine’s IP address to a DNS name. If the module can’t resolve the IP address, the module does not start.

You can verify this by using the `nslookup` command. Enter this command with hostname in the command prompt and it should return the IP address of the host

- ♦ Other Access Manager components should not be installed on the same machine

For information about network requirements, see [“Network Requirements” on page 35](#).

For prerequisites, see [“Prerequisites” on page 52](#).

Installation Procedure

Installation time: about 10 minutes.

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

IMPORTANT: The Access Gateway Service must be installed on a separate server.

- 1 Log in to the [NetIQ Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) and follow the link that allows you to download software. For an evaluation version, download the media kit from [NetIQ Downloads \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp).
- 2 Copy the file to your machine.
For the filename, see the release-specific NetIQ Access Manager Readme.
- 3 Disable any virus scanning programs.
- 4 To use a remote desktop for installation, use one of the following:
 - ♦ Current version of VNC viewer
 - ♦ Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
 - ♦ Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3

- 5 Double click the executable file.

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

If NAT is configured then ensure that you configure the same in the Administration Console. Else, click **Continue >Next**.

- 6 Review the readme, and click **Next**.
- 7 Review and accept the License Agreement, then click **Next**.
- 8 Specify the IP address, user ID, and password of the primary Administration Console.
- 9 (Conditional) Specify the local IP address, if your machine has more than one IP address, which the Access Gateway Service will use for communication with the Administration Console.
- 10 (Optional) Specify the Access Gateway Local NAT IP address, if the device is behind NAT.
- 11 Click **Next**.
- 12 Configure disk cache. This holds the caching objects of the Access Gateway.

NOTE: The Access Gateway Appliance uses the mod_cache module filesystem provided by Apache 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](#).

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

C:\Program Files\Novell\log

- 16 Click **Next > Done**.
- 17 To verify that the Access Gateway Service imported into the Administration Console, wait for few minutes, log in to the Administration Console, then click **Devices > Access Gateways**.
At this point, the Access Gateway Service is not configured.
- 18 Continue with one of the following:
 - ♦ [“Verifying the Access Gateway Installation” on page 79](#)
 - ♦ Configure the Access Gateway. See [Configuring Logging for a Proxy Service](#) in the [NetIQ Access Manager Administration Guide](#).
 - ♦ Install another Access Manager component.

4.2.2 Installing the Access Gateway Service on Windows

- ♦ [“Windows Requirements” on page 59](#)
- ♦ [“Installation Procedure” on page 60](#)

Windows Requirements

- ♦ Windows Server 2008 R2 and 2012 R2, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied.
- ♦ 4 GB RAM.
- ♦ Dual CPU or Core (3.0 GHz or comparable chip).

- ♦ 2 to 10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- ♦ A static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module does not start.

You can verify this by using the `nslookup` command. Enter this command with hostname in the command prompt and it should return the IP address of the host.

- ♦ Other Access Manager components should not be installed on the same machine.

For information about network requirements, see “[Network Requirements](#)” on page 35.

For prerequisites, see “[Prerequisites](#)” on page 52.

Installation Procedure

Installation time: about 10 minutes.

What you need to know	<ul style="list-style-type: none"> ♦ Username and password of the administrator. ♦ IP address of the Administration Console.
-----------------------	--

IMPORTANT: The Access Gateway Service must be installed on a separate server.

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

- 2 Copy the file to your machine.

For the filename, see the NetIQ Access Manager Readme.

- 3 Disable any virus scanning programs.

- 4 To use a remote desktop for installation, use one of the following:

- ♦ Current version of VNC viewer
- ♦ Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
- ♦ Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3

- 5 Double click the executable file.

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

If NAT is configured then ensure that you configure the same in the Administration Console. Else, click **Continue >Next**.

- 6 Review the readme, and click **Next**.

- 7 Review and accept the License Agreement, then click **Next**.

- 8 Specify the IP address, user ID, and password of the primary Administration Console.

- 9 (Conditional) Specify the local IP address, if your machine has more than one IP address, which the Access Gateway Service will use for communication with the Administration Console.

- 10 (Optional) Specify the Access Gateway Local NAT IP address, if the device is behind NAT.

- 11 Click **Next**.

- 12 Configure disk cache. This holds the caching objects of the Access Gateway.

NOTE: The Access Gateway Appliance uses the mod_cache module filesystem provided by Apache 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](#).

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

14 Click **Install**.

15 Review the log information at the following location:

C:\Program Files\Novell\log

16 Click **Next > Done**.

17 To verify that the Access Gateway Service imported into the Administration Console, wait for few minutes, log in to the Administration Console, then click **Devices > Access Gateways**.

At this point, the Access Gateway Service is not configured.

18 Continue with one of the following:

- ♦ [“Verifying the Access Gateway Installation” on page 79](#)
- ♦ Configure the Access Gateway. See [“Setting Up a Basic Access Manager Configuration”](#) in the [“NetIQ Access Manager 4.0 SP1 Setup Guide”](#).
- ♦ Install another Access Manager component.

5 Installing SSL VPN

This chapter explains how to install SSL VPNs. Topics include:

- ♦ [Section 5.1, “SSL VPN Installation Requirements,” on page 63](#)
- ♦ [Section 5.2, “Installing SSL VPN,” on page 63](#)

5.1 SSL VPN Installation Requirements

You can install SSL VPN on a separate server or with the Access Gateway Appliance, the Linux Identity Server, the Linux Administration Console. When installed with another Access Manager component, that component’s requirements are sufficient for SSL VPN. You can also install the high bandwidth version of SSL VPN after installing SSL VPN, if export laws permit.

When installed separately, it has the following hardware and software requirements:

- ♦ 100 GB of disk space

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

- ♦ 4 GB RAM
- ♦ Dual CPU or Core (3.0 GHz or comparable chip)
- ♦ SLES 11 SP2 and SP3 (64-bit) operating system (physical or virtual)
- ♦ `gettext` package
- ♦ Static IP address

NOTE

- ♦ SSL VPN does not support RHEL.
- ♦ SSL VPN supports Windows 7 only in the Enterprise mode and not in the Kiosk mode.

For information about network requirements, see [“Network Requirements” on page 35](#).

5.2 Installing SSL VPN

Installation time: about 10 minutes.

What you need to know to install SSL VPN

- ♦ Username and password of the administrator.
- ♦ IP address of the Administration Console.

-
- ♦ [Section 5.2.1, “Installing ESP-Enabled SSL VPN,” on page 64](#)
 - ♦ [Section 5.2.2, “Installing Traditional SSL VPN,” on page 67](#)
 - ♦ [Section 5.2.3, “Installing the Key for High-Bandwidth SSL VPN,” on page 72](#)

5.2.1 Installing ESP-Enabled SSL VPN

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

- ♦ [“Deployment Scenarios” on page 64](#)
- ♦ [“Installing ESP-Enabled SSL VPN” on page 66](#)

Deployment Scenarios

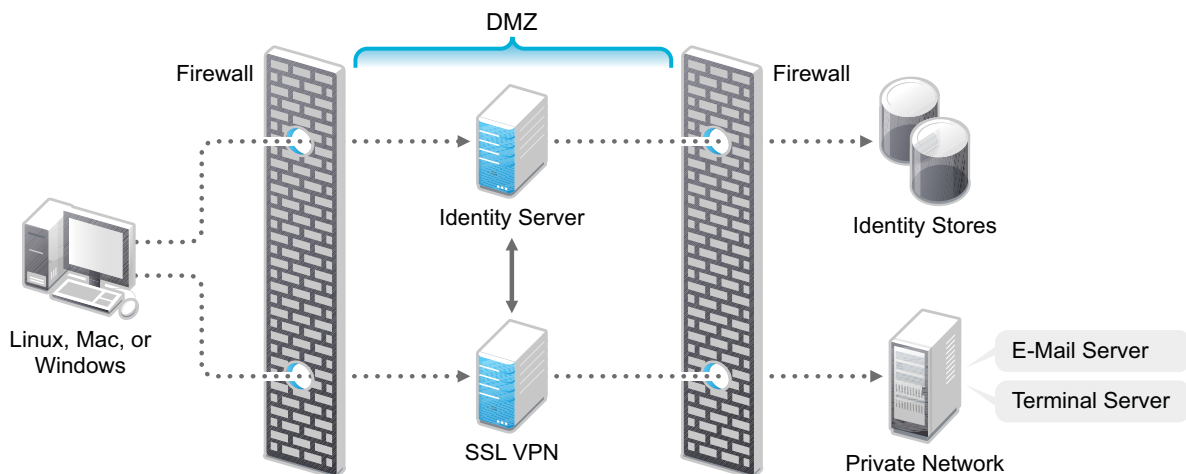
ESP-enabled SSL VPN supports the following installation scenarios:

- ♦ [“Deployment Scenario 1: Installing SSL VPN on a Separate Machine” on page 64](#)
- ♦ [“Deployment Scenario 2: Installing SSL VPN and the Identity Server on the Same Machine” on page 65](#)
- ♦ [“Deployment Scenario 3: Installing SSL VPN and the Administration Console on the Same Machine” on page 65](#)
- ♦ [“Deployment Scenario 4: Installing SSL VPN, the Administration Console, and the Identity Server on the Same Machine” on page 66](#)

Deployment Scenario 1: Installing SSL VPN on a Separate Machine

This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are deployed separately, without the Access Gateway. For installation instructions for this scenario, see [“Installing ESP-Enabled SSL VPN” on page 66](#). In this scenario, SSL VPN is accessible on port 8443. When it is accessed on port 8080, it will be redirected to port 8443.

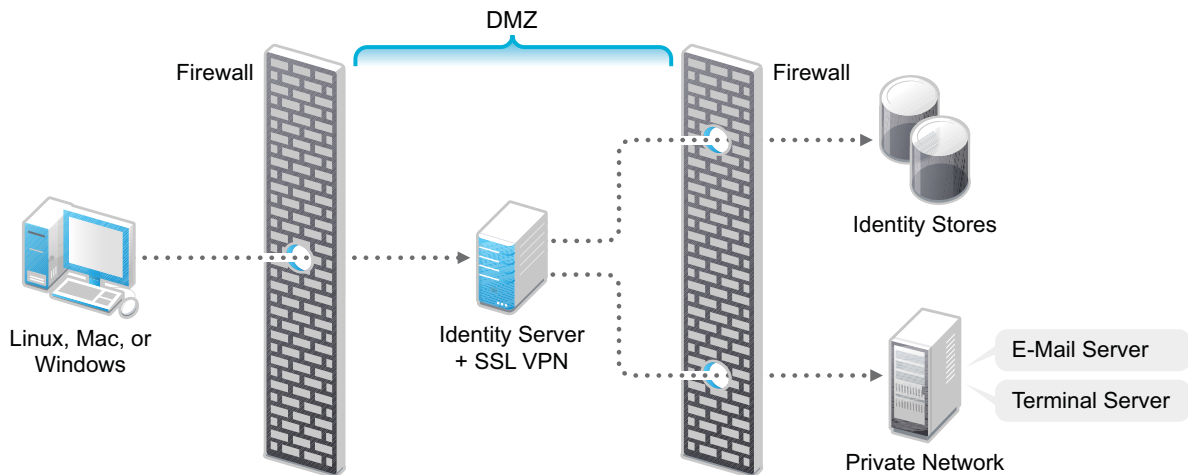
Figure 5-1 Deployment Scenario 1



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

This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on a single machine. The Access Gateway is deployed separately. For installation instructions for this scenario, see [“Installing ESP-Enabled SSL VPN” on page 66](#). In this scenario, SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

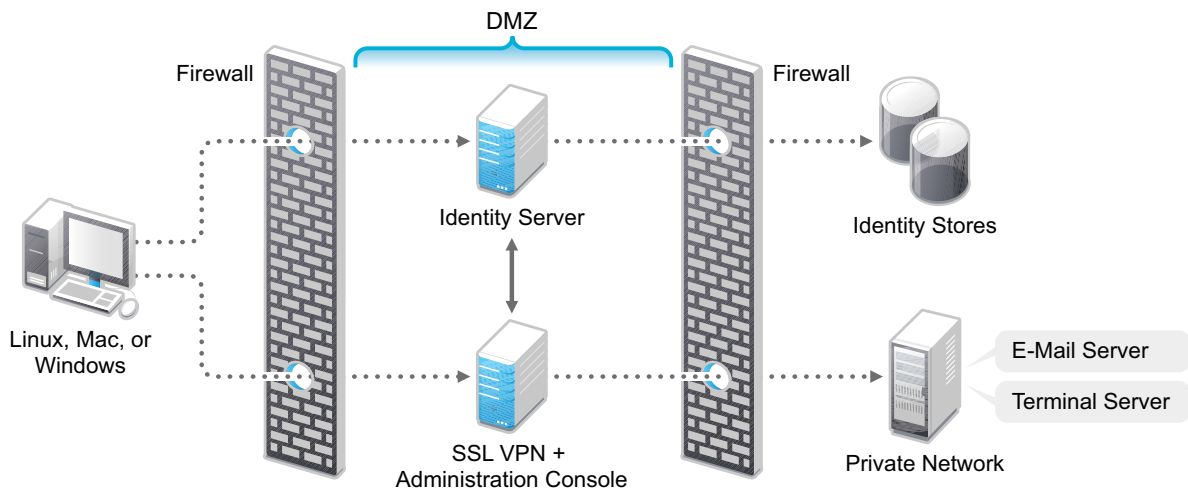
Figure 5-2 Deployment Scenario 2



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

This deployment scenario consists of a demilitarized zone where SSL VPN, and Administration Console are on the same machine and Access Gateway and the Identity servers are deployed separately. For installation instructions for this scenario, see [“Installing ESP-Enabled SSL VPN” on page 66](#). In this scenario, SSL VPN will be accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

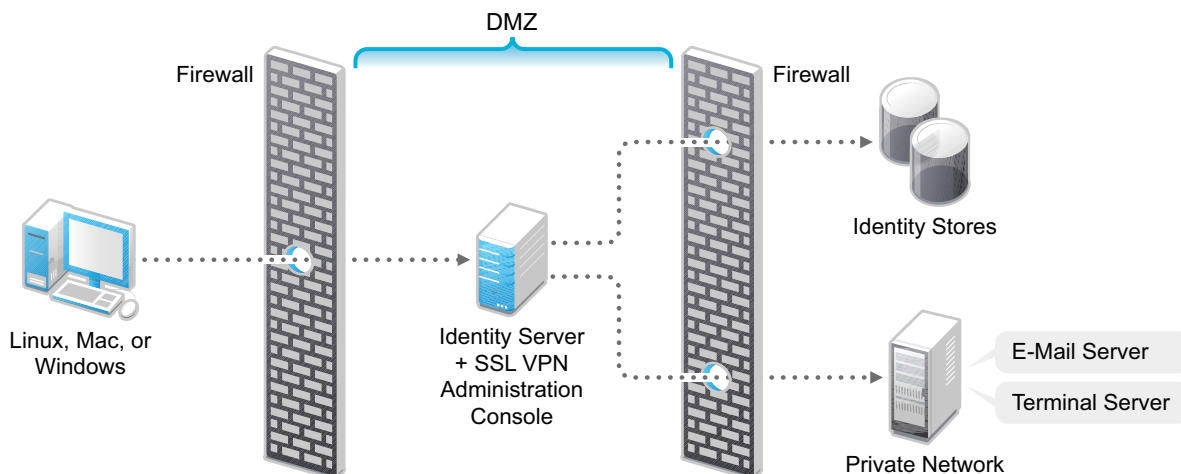
Figure 5-3 Deployment Scenario 3



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

This deployment scenario consists of a demilitarized zone where the Identity Server, SSL VPN, and Administration Console are on the same machine and Access Gateway is deployed separately. For installation instructions for this scenario, see [“Installing ESP-Enabled SSL VPN” on page 66](#). In this scenario SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

Figure 5-4 Deployment Scenario 4



Installing ESP-Enabled SSL VPN

The following installation steps are applicable to all deployment scenarios of ESP-enabled SSL VPN. The individual scenarios are explained in [“Deployment Scenarios” on page 64](#).

- 1 Access the install script.
 - 1a Ensure that you have downloaded the software or that you have the CD available.
For software download instructions, see the [“Access Manager 4.0 Hotfix 1 Readme”](#).
 - 1b Do one of the following:
 - ♦ If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be `/media/cdrom`, `/media/cdrecorder`, or `/media/dvdrrecorder`, depending on your hardware.
 - ♦ If you downloaded the `tar.gz` file, unzip the file by using the following command:

```
tar -xzf <filename>
```
 - 1c Change to the `novell-access-manager` directory.
- 2 Run the following command:

```
./install.sh
```
- 3 Specify 4 to install ESP-Enabled SSL VPN, then press Enter.
- 4 Review and accept the License Agreement.

The following warning is displayed:

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

- 5 Specify **Y** to proceed.
- 6 (Conditional) If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for SSL VPN.
- 7 Specify the IP address, user ID, and password of the primary Administration Console.
- 8 Select the IP address used for the NetIQ Access Manager Server Communications Local Listener. You can select an address, specify a new address, or press Enter to accept the default.
- 9 Select the IP address used for the SSL VPN listening IP address. You can select an address, specify a new address, or press Enter to accept the default.
- 10 If you are installing SSL VPN on the same machine as the Administration Console, you are not prompted for the IP address of the Administration Console. If the Administration Console is on a different machine, provide the IP address when you are prompted for it.

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

The installation ends with the following message: `Installation complete.`
- 11 To verify the installation of SSL VPN, continue with [Section 7.3, “Verifying the SSL VPN Installation,” on page 79](#).
- 12 Add an entry in `/etc/hosts` file to map the SSL VPN IP address with the domain name that the client will use to connect.
- 13 If the export law permits and you want to install high bandwidth version of SSL VPN, proceed with [Section 5.2.3, “Installing the Key for High-Bandwidth SSL VPN,” on page 72](#).

5.2.2 Installing Traditional SSL VPN

Traditional SSL VPN does not have an ESP and must be configured as a protected resource of an Access Gateway. You can install traditional SSL VPN with Access Gateway Appliance, Identity Server, Administration Console, or on a separate machine.

- ♦ [“Deployment Scenarios” on page 67](#)
- ♦ [“Installing Traditional SSL VPN” on page 71](#)

Deployment Scenarios

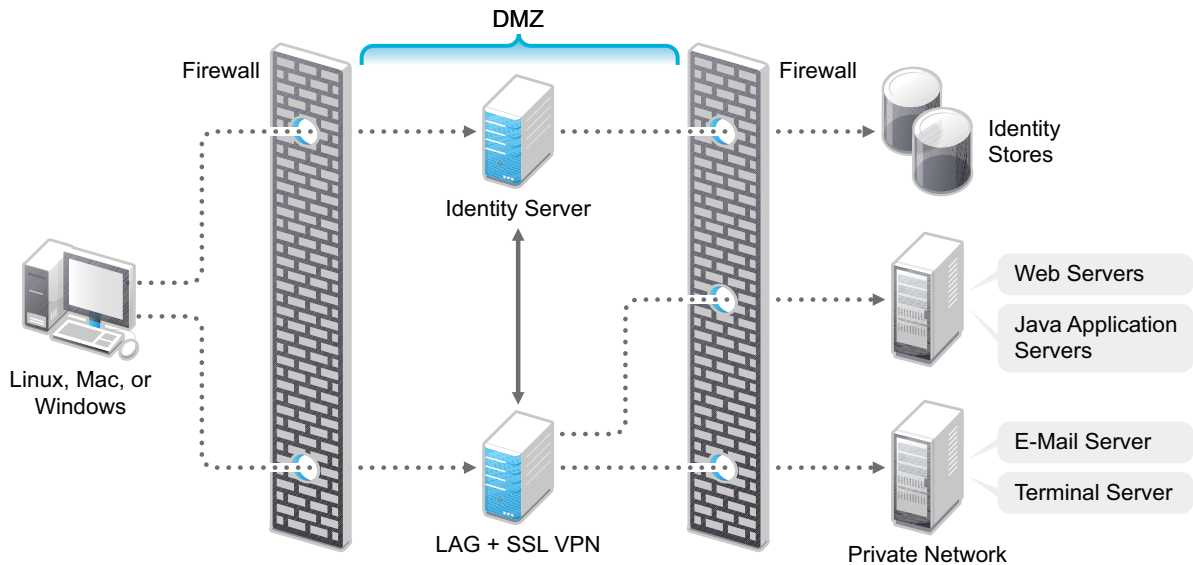
Traditional SSL VPN supports the following installation scenarios:

- ♦ [“Deployment Scenario 1: Access Gateway and SSL VPN on the Same Server” on page 68](#)
- ♦ [“Deployment Scenario 2: SSL VPN Server Installed on a Separate Machine” on page 68](#)
- ♦ [“Deployment Scenario 3: Identity Server and SSL VPN on the Same Server” on page 69](#)
- ♦ [“Deployment Scenario 4: Administration Console and SSL VPN on the Same Server” on page 69](#)
- ♦ [“Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server” on page 70](#)

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

This deployment scenario consists of a demilitarized zone where the Access Gateway and SSL VPN are on the same server and the Identity Server is deployed separately. For installation instructions for this scenario, see [“Installing SSL VPN with Access Gateway Appliance” on page 71](#). In this scenario, SSL VPN is accessible on port 8443. When it is accessed on port 8080, it will be redirected to port 8443.

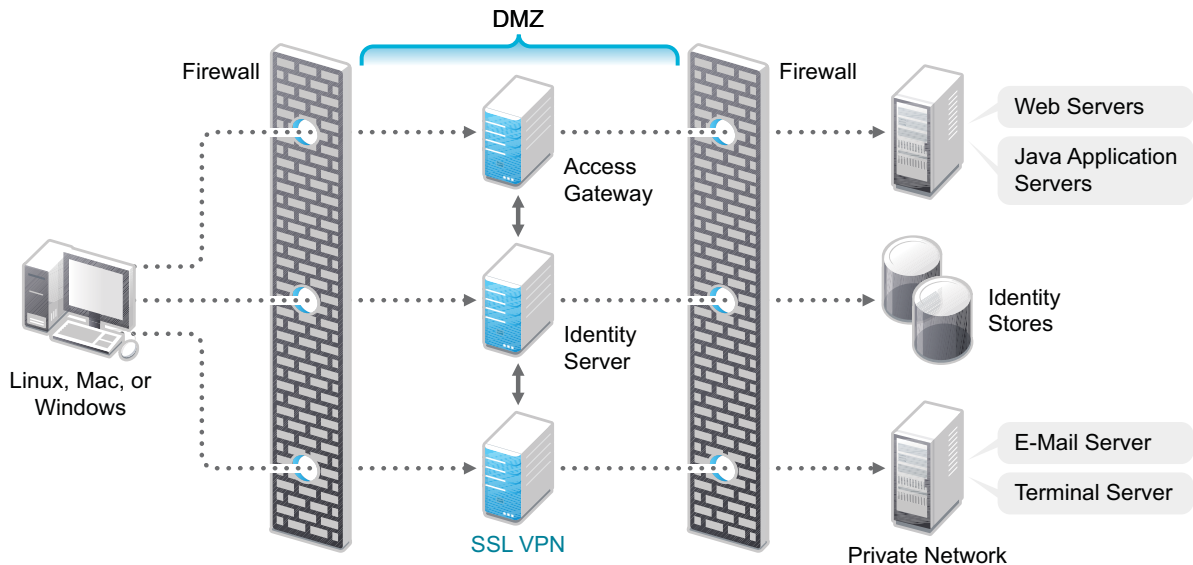
Figure 5-5 Deployment Scenario 1



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

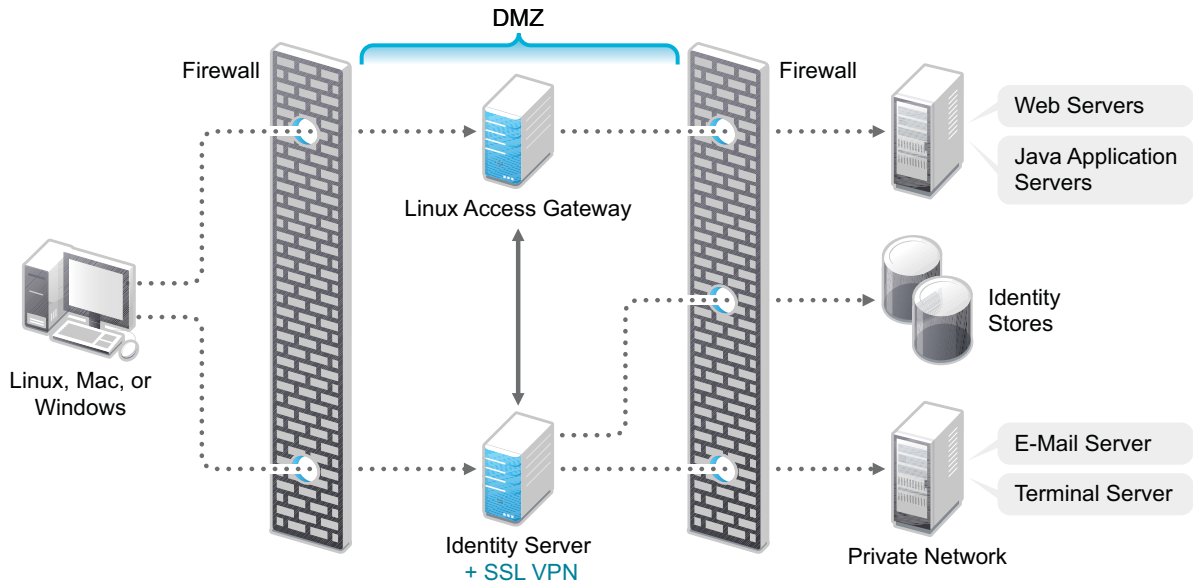
This deployment scenario consists of a demilitarized zone where the Access Gateway, Identity Server, and SSL VPN are deployed separately. For installation instructions, see [“Installing Traditional SSL VPN” on page 71](#). In this scenario, SSL VPN is accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

Figure 5-6 Deployment Scenario 2



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

This deployment scenario consists of a demilitarized zone where the Identity Server and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions, see [“Installing SSL VPN on a Separate Server, with Identity Server, or with Administration Console” on page 71](#). In this scenario, SSL VPN will be accessible on secure port 3443. When this port is accessed on a non-secure port 3080, it will be redirected to port 3443.

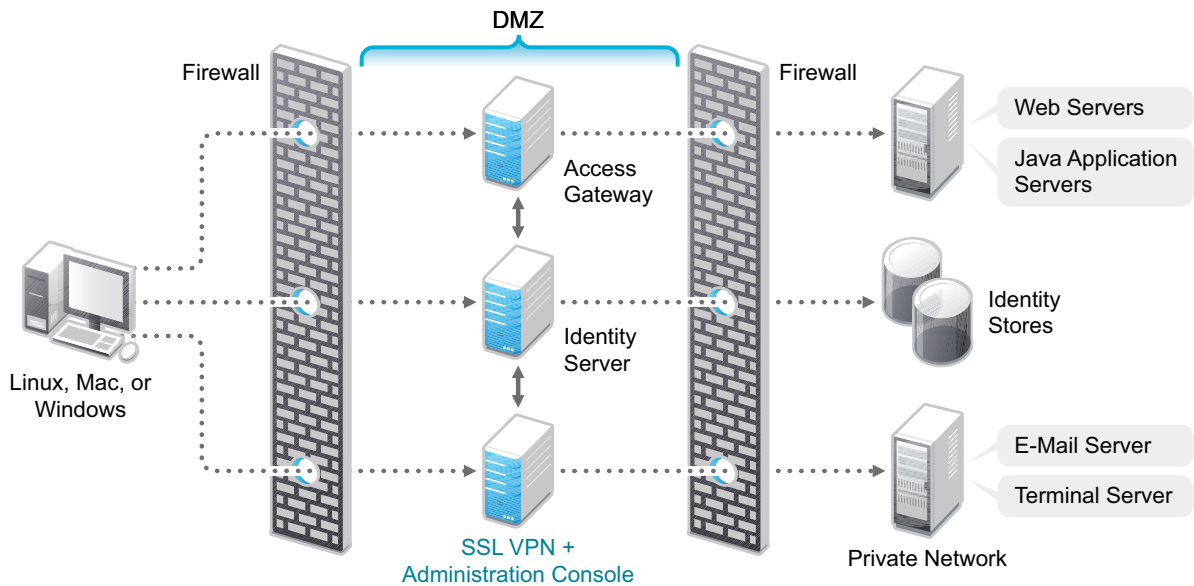


Deployment Scenario 4: Administration Console and SSL VPN on the Same Server

This deployment scenario consists of a demilitarized zone where the Administration Console and SSL VPN are on one machine and the Access Gateway and Identity Server are deployed separately on different machines. For installation instructions, see [“Installing SSL VPN on a Separate Server, with](#)

Identity Server, or with Administration Console” on page 71. In this scenario SSL VPN will be accessible on secure port 8443. When this port is accessed on a non-secure port 8080, it will be redirected to port 8443.

Figure 5-7 Deployment Scenario 4

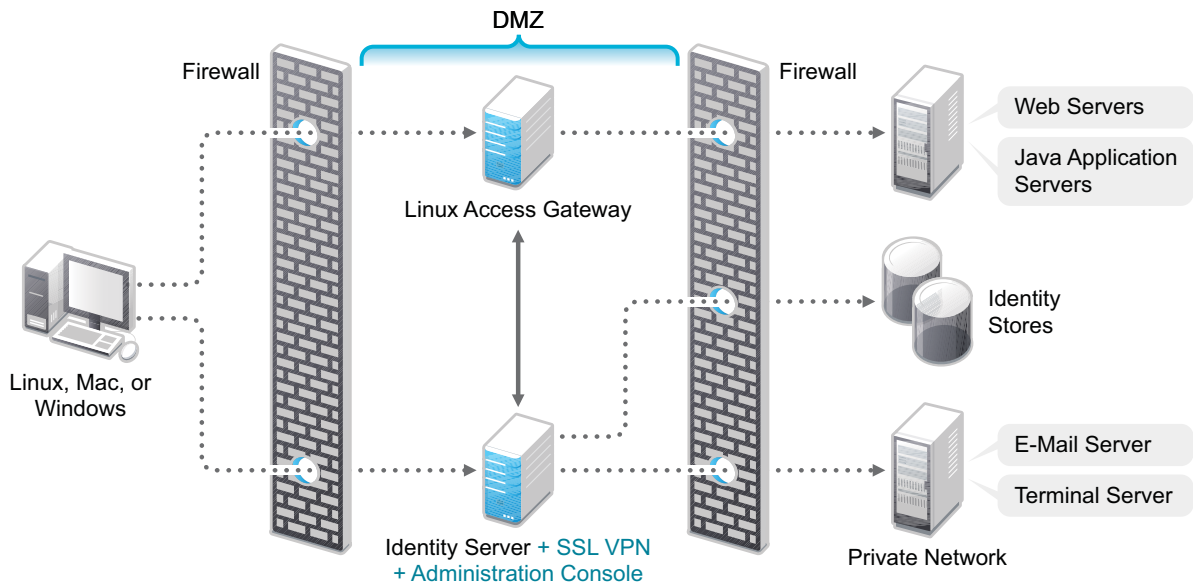


Deployment Scenario 5: Administration Console, Identity Server, and SSL VPN on the Same Server

This deployment scenario consists of a demilitarized zone where the Identity Server, Administration Console, and SSL VPN are on one machine and the Access Gateway is deployed separately. For installation instructions, see [“Installing SSL VPN on a Separate Server, with Identity Server, or with Administration Console”](#) on page 71.

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

Figure 5-8 Deployment Scenario 5



Installing Traditional SSL VPN

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

- ♦ [“Installing SSL VPN with Access Gateway Appliance”](#) on page 71
- ♦ [“Installing SSL VPN on a Separate Server, with Identity Server, or with Administration Console”](#) on page 71

Installing SSL VPN with Access Gateway Appliance

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

- 1 Start the Access Gateway installation.
For more information about installing the Access Gateway, see [Section 4.1.2, “Installing the Access Gateway Appliance,”](#) on page 52.
- 2 In the Access Administrator Configuration section, select the **Install and Enable SSL VPN Server** check box to install and configure SSL VPN with the Access Gateway.
- 3 Follow the on-screen instructions to continue with the Access Gateway installation.
- 4 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with [Section 5.2.3, “Installing the Key for High-Bandwidth SSL VPN,”](#) on page 72.

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

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

1 Access the install script.

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

For software download instructions, see the [“Access Manager 4.0 Hotfix 1 Readme”](#).

1b Do one of the following:

- ♦ If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be `/media/cdrom`, `/media/cdrecorder`, or `/media/dvdrecorder`, depending on your hardware.
- ♦ If you downloaded the `tar.gz` file, unpack the file by using the following command:

```
tar -xzf <filename>
```

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

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

```
./install.sh
```

You are prompted to select an installation.

3 Specify 3 to install traditional SSL VPN, then press Enter.

4 Review and accept the License Agreement.

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

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

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

Specify `y` to proceed.

7 Specify the user ID and password of the Administration Console administrator.

8 Specify the SSL VPN Listening IP address. You can select an address, specify a new address, or press Enter to accept the default.

The following warning is displayed:

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

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

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

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

10 To verify the installation of SSL VPN, continue with [Section 7.3, “Verifying the SSL VPN Installation,” on page 79](#).

11 If the export law permits and you want to install the high bandwidth version of SSL VPN, proceed with [Section 5.2.3, “Installing the Key for High-Bandwidth SSL VPN,” on page 72](#)

5.2.3 Installing the Key for High-Bandwidth SSL VPN

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

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

To install RPM:

- 1 Log in to the [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) and look for the link that allows you to download the RPM containing key for the high bandwidth version.

- 2 Download the following high bandwidth RPM:

```
novl-sslvpn-hb-key-3.2-0.noarch.rpm
```

- 3 Log in as `root`.

- 4 Run the following command to stop all services:

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

- 5 Run the following command to install RPM:

```
rpm -ivh novl-sslvpn-hb-key-3.2.0-0.noarch.rpm
```

- 6 Run the following command to restart all SSL VPN services:

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

- 7 Run the following command to check the status:

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

6 Installing Access Manager Components in NAT Environments

This chapter provides information about deploying Access Manager components in a multi-tenant or service provider environment, where Network Address Translation (NAT) protocol is used as one of the network configuration. Topics include:

- ♦ [Section 6.1, “Network Prerequisites,” on page 73](#)
- ♦ [Section 6.2, “Network Setup Flow Chart,” on page 74](#)
- ♦ [Section 6.3, “Installing Access Manager Components in NAT Environments,” on page 74](#)
- ♦ [Section 6.4, “Configuring Network Address Translation,” on page 77](#)

6.1 Network Prerequisites

Service Provider Network Setup

- ☐ Obtain Static IP addresses for Administration Console, Identity Server, and Sentinel. If the IP address of the machine changes, the Access Manager components on that machine cannot start.
- ☐ Install operating system, configure Network Time Protocol (NTP) server, and check connectivity.
- ☐ NTP 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 and data corruption can also happen in user stores.

- ☐ An L4 switch if you are going to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- ☐ There should be IP connectivity between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

Customer Network Setup

- ☐ A server configured with an LDAP directory (eDirectory 8.7 or later, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- ☐ Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

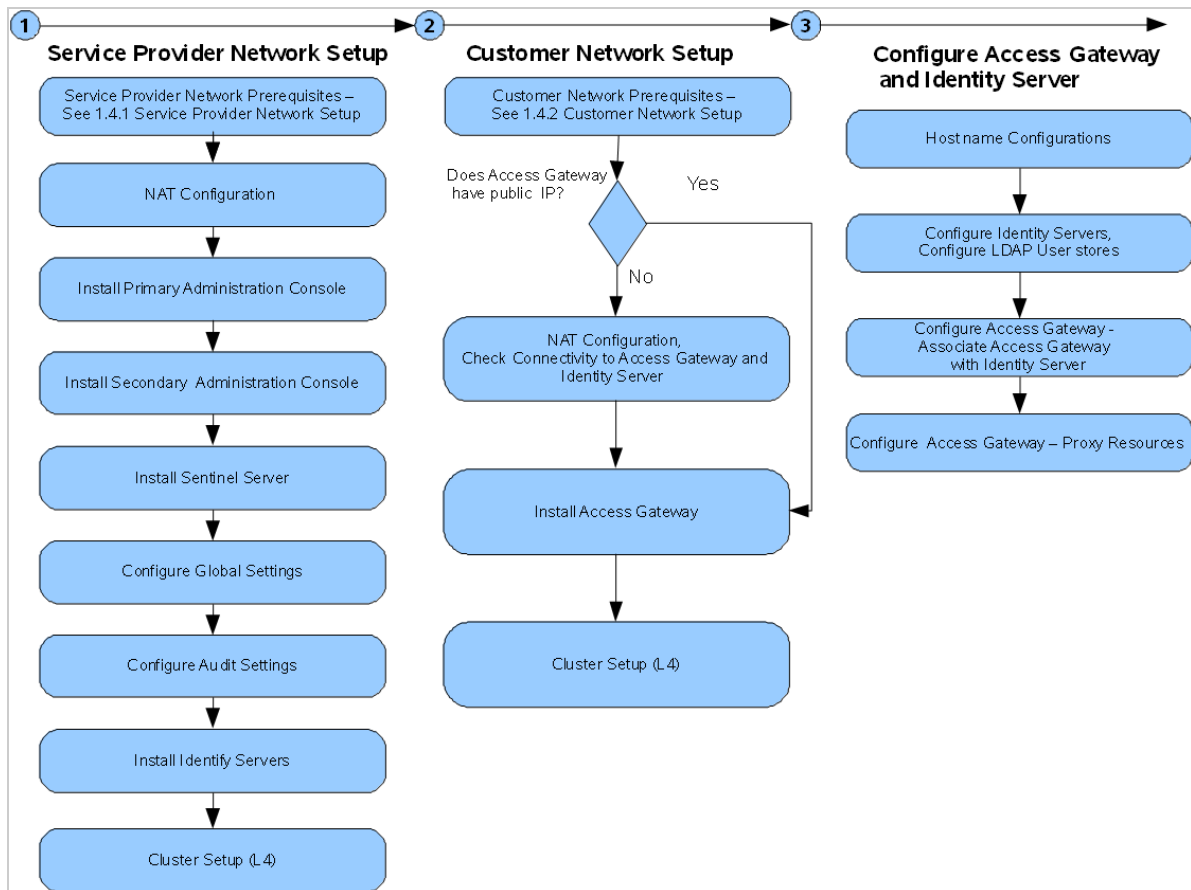
Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not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

- ❑ Obtain Static IP addresses for Administration Console, Identity Server, and Sentinel. If the IP address of the machine changes, the Access Manager components on that machine cannot start.
- ❑ There should be IP connectivity between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

6.2 Network Setup Flow Chart

The network setup flow chart provides information about installing Access Manager components and configuring NAT in a multi-tenant or service provider network.

Figure 6-1 Network Setup Flow Chart



6.3 Installing Access Manager Components in NAT Environments

Installing Access Manager in the NAT environment consists of the following steps:

1. [“Installing the Administration Console” on page 75.](#)
2. [“Configuring Global Settings” on page 75](#)
3. [“Configuring Audit Server” on page 76](#)

4. [“Installing the Identity Servers” on page 45](#)
5. [“Installing the Access Gateway” on page 51](#)

6.3.1 Installing the Administration Console

For installation requirements, see [Chapter 2, “Installing the Administration Console,” on page 33](#).

- 1 Before installing Access Manager components, check the network connectivity across these machines.
- 2 Verify the link latency and ensure that it is less than 100 milliseconds.
If the link latency is greater than 100ms, it might lead to performance degradation.
- 3 Synchronize time across all Access Manager components.
The primary Administration Console should be configured to synchronize time with the corporate Network Time Protocol (NTP) server. The remaining machines should be configured to synchronize time with the primary Administration Console.
 - 3a Add the following entry to the `/etc/crontab` file on the primary Administration Console:

```
*/5 * * * * root sntp -P no -r <corporate NTP_Server> >/dev/null 2>&1
```
 - 3b Add the following entry to the `/etc/crontab` file of other Access Manager machines:

```
*/5 * * * * root sntp -P no -r <Primary_Admin_Console_IP> >/dev/null 2>&1
```
- 4 Install the primary Administration Consoles by providing the listening IP address for the primary Administration Console.
For more information about installing the Administration Console, see the [Section 2.2, “Installing the Administration Console on Windows,” on page 39](#).
- 5 Install the secondary Administration Console and repeat the above procedures for secondary Administration Console IP address.
- 6 Continue with [Section 6.3.2, “Configuring Global Settings,” on page 75](#) to add both the primary and secondary Administration Consoles to the **Global Settings** configuration.

6.3.2 Configuring Global Settings

You need to map the private IP address of the Administration Console and to the public NAT IP address. You need to specify the NAT IP addresses before importing the Identity Server and the Access Gateway. You have to specify the NAT IP Addresses prior to importing devices. The devices that cannot reach the Private Administration Console IP address will use the NAT IP address.

- 1 Log in to the Administration Console.
- 2 Select **Access Manager > Global Settings**.
- 3 Click **New**.
- 4 Select the Administration Console Listening IP address from the drop-down list.
- 5 Specify the corresponding Public NAT IP address.
If you do not specify a Public NAT IP address or if a mapping already exists for the selected Administration Console IP address, the following message is displayed:

```
IP Address is not valid
```

- 6 Click **OK** to continue and apply the configuration changes.
- 7 Continue with [Section 6.3.3, “Configuring Audit Server,” on page 76](#) to configure auditing and logging.

6.3.3 Configuring Audit Server

The Secure Logging Server manages the flow of information to and from the auditing system. It receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. You can configure the Secure Logging Server to automatically reset the critical system attributes according to the specified policy.

- 1 Log in to the Administration Console.
- 2 Select **Access Manager > Auditing > Auditing**.
- 3 Specify the following details:

Server Listening IP Address: Specify the private listening IP address. Specify the IP address or DNS name of the audit logging server that you want to use. By default, the system uses the primary Administration Console IP address. If you want to use a different Secure Logging Server, specify the IP address of that server.

Server Public NAT IP Address: Specify the NAT IP address of the relevant server. For example, if you want to use the Sentinel private IP address on Server Listening Address 11.0.0.124, then you need to specify the NAT IP address of the Sentinel server in Server NAT IP Address to map the private address to a public address. To use a Sentinel server or a Sentinel Log Manager server instead of Novell Audit, specify the IP address or DNS name of the Sentinel Collector.

- ♦ For more information about Sentinel, see the [Sentinel 6.1](http://www.novell.com/documentation/sentinel61/index.html) (<http://www.novell.com/documentation/sentinel61/index.html>).
- ♦ For more information about Sentinel Log Manager, see the [Sentinel Log Manager 1.0](http://www.novell.com/documentation/novelllogmanager10/) (<http://www.novell.com/documentation/novelllogmanager10/>).

Port: Specify the port that the Platform Agents use to connect to the Secure Logging Server. The default port value is 1289. The Sentinel servers listens on port 1289

Stop Service on Audit Server Failure: If you select this check box, audit events are always sent to Audit Server. If Audit Server is offline or not reachable, when an audit event is generated the apache services will be shut down.

If you want to use a Sentinel server or a Sentinel Log Manager server instead of the Novell Audit Server, specify the port number of your Sentinel Collector.

IMPORTANT: Whenever you change the port or IP address of the Secure Logging Server, you must update all Access Gateways, then restart the Identity Server, Administration Console, and Access Gateways before the configuration changes take affect.

- 4 In the **Management Console Audit Events** section, specify any or all of the following options to generate events:
 - Health Changes:** Generates events whenever the health of server changes.
 - Server Imports:** Generates events whenever a server is imported into the Administration Console.
 - Server Deletes:** Generates whenever a server is deleted from the Administration Console.
 - Configuration Changes:** Generates events whenever you change the server configuration.
- 5 Click **OK**.

If you did not change the address or port of the Secure Logging Server, this completes the process. It might take up to 15 minutes for the events you selected to start appearing in the audit files.

- 6 Restart all Access Manager components imported into the Administration Console.

The Identity Server and Access Gateway do not start reporting events until they have been restarted.

6.3.4 Installing and Configuring the Identity Server

For information about how to install the Identity Server, see [Chapter 3, “Installing the Identity Servers,” on page 45](#).

User stores are LDAP directory servers to which end users authenticate. You must specify an initial user store when creating an Identity Server configuration. You use the same procedure for setting up the initial user store, adding a user store, or modifying an existing user store.

For information about how to configure the Identity Server, see “[Configuring Identity User Stores](#)” in the [NetIQ Access Manager 4.0 SP1 Identity Server Guide](#).

6.3.5 Installing and Configuring the Access Gateway

For information about how to install Access Gateway, see [Chapter 4, “Installing the Access Gateway,” on page 51](#).

When you are setting up the Access Gateway to protect Web resources, you create and configure reverse proxies, proxy services, and protected resources. The authentication contract, authentication procedure, Authorization policy, Identity Injection policy, and Form Fill policy are configured at the resource level so that you can enable exactly what the resource requires.

For information about configuring Access Gateway, see the [NetIQ Access Manager 4.0 SP1 Access Gateway Guide](#).

6.4 Configuring Network Address Translation

NetIQ Access Manager can be configured by using Network Address Translation (NAT), which enables the communication between the Administration Console from local network to other Access Manager devices such as Identity Server and Access Gateway. The devices can be in the external network or in another private network. The NAT address needs be to configured in router.

See your router documentation for more information.

- ♦ [Section 6.4.1, “Configuring the Administration Console Behind NAT,” on page 77](#)
- ♦ [Section 6.4.2, “Configuring the Identity Server, Access Gateway, and SSL VPN Behind NAT,” on page 78](#)

6.4.1 Configuring the Administration Console Behind NAT

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

- 4 Enter the respective NAT IP address for primary and secondary Administration Console in **Public NAT IP Address**.

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

- 5 Click **OK**.

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

For more information about configuring NAT, see “[Global Settings](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

6.4.2 Configuring the Identity Server, Access Gateway, and SSL VPN Behind NAT

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

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

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

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

7 Verifying the Installation

This chapter discusses the steps to verify Access Manager components after installation. Topics include:

- ♦ [Section 7.1, “Verifying the Identity Server Installation,” on page 79](#)
- ♦ [Section 7.2, “Verifying the Access Gateway Installation,” on page 79](#)
- ♦ [Section 7.3, “Verifying the SSL VPN Installation,” on page 79](#)

You can verify whether the Administration Console is working by logging in to it. See [Section 2.3, “Logging In to the Administration Console,” on page 42](#).

7.1 Verifying the Identity Server Installation

- 1 Log in to the Administration Console.
See [Section 2.3, “Logging In to the Administration Console,” on page 42](#).
- 2 Click **Devices > Identity Servers**.

7.2 Verifying the Access Gateway Installation

- 1 Log in to the Administration Console.
See [Section 2.3, “Logging In to the Administration Console,” on page 42](#).
- 2 Click **Devices > Access Gateways**.
If the installation was successful, the IP address of your Access Gateway appears in the Server list.
The Health status indicates the health state after the Access Gateway is imported and registers with the Administration Console.

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

If an Access Gateway starts to import into the Administration Console but fails to complete the process, the following message appears:

Server gateway-<name> is currently importing. If it has been several minutes after installation, click **repair import** to fix it.

If you have waited at least ten minutes, but the message doesn't disappear and the Access Gateway does not appear in the list, click the **repair import** link.

7.3 Verifying the SSL VPN Installation

- 1 Log in to the Administration Console.

See [Section 2.3, “Logging In to the Administration Console,”](#) on page 42.

2 Click *Devices* > *SSL VPNs*.

3 Select a server, then click the *Health* icon to display the health of SSL VPN.

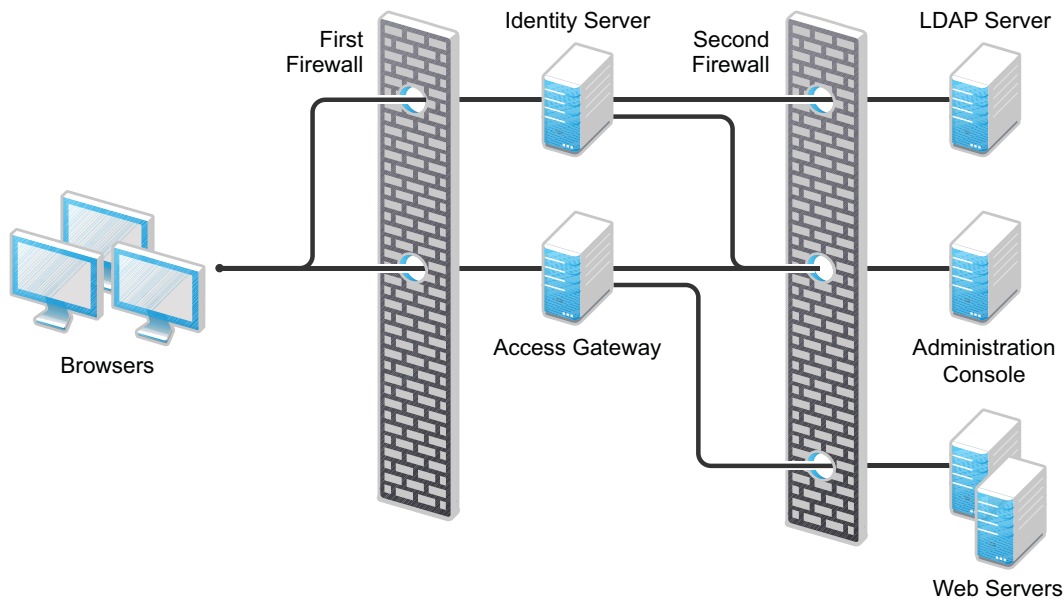
The initial health status of an ESP-enabled SSL VPN shows yellow because the trust relationship between the Identity Server and the Embedded Service Provider is yet to be established.

For more information on how to configure the trust relationship, see “[Configuring Authentication for the ESP-Enabled NetIQ SSL VPN](#)” in the “[NetIQ Access Manager 4.0 SSL VPN Server Guide](#)”.

8 Setting Up Firewalls

Access Manager should be used with firewalls. [Figure 8-1](#) illustrates a simple firewall setup for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console.

Figure 8-1 Access Manager Components between Firewalls



The first firewall separates the Access Manager from the Internet, allowing browsers to access the resources through specific ports. The second firewall separates Access Manager components from Web servers they are protecting and the Administration Console. This is one of many possible configurations. This section describes the following:

- ♦ [Section 8.1, “Required Ports,” on page 81](#)
- ♦ [Section 8.2, “Restricted Ports,” on page 88](#)
- ♦ [Section 8.3, “Sample Configurations,” on page 89](#)

8.1 Required Ports

The following tables list the ports that need to be opened when a firewall separates one component from another. Some combinations appear in more than one table. This allows you to discover the required ports whether a firewall is separating an Access Gateway from the Administration Console or a firewall is separating an Administration Console from the Access Gateway.

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

Table 8-1 When a Firewall Separates an Access Manager Component from a Global Service

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time synchronized else the authentication fails. We recommend that you configure all components to use an network time protocol (NTP) server. Depending upon where your NTP server is located, you might need to open UDP 123, so that Access Manager components can use the NTP server.
DNS Servers	UDP 53	Access Manager components must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53, so that Access Manager components can resolve DNS names.
Remote Linux Administration Workstation	TCP 22	If you want to use SSH for remote administration of Access Manager components, open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.
Remote Windows Administration Workstation	Configurable	<p>If you want to use RDP or VNC for remote administration of Access Manager components, open the ports required by your application from the remote administration workstation to your Access Manager components. You need to open ports for console access and for file sharing.</p> <p>For console access, VNC usually uses TCP 5901 and RDP uses TCP 3389. For file sharing, UDP 135-139 are the default ports.</p>

Table 8-2 When a Firewall Separates the Administration Console from a Component

Component	Port	Description
Access Gateway, Identity Server, SSL VPN	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from devices to the Administration Console.
	TCP 1289	For communication from devices to the Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
	TCP 636	For secure LDAP communication from devices to the Administration Console.
Importing an Access Gateway Appliance	ICMP	During an import, the Access Gateway Appliance sends two pings through ICMP to the Administration Console. When the import has finished, you can disable the ICMP echo requests and echo replies.

Component	Port	Description
LDAP User Store	TCP 524	Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. It is not used in day-to-day operations.
Administration Console	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for secure LDAP communication.
	TCP 427	Used for SLP (Service Location Protocol) communication.
	TCP 8080, 8443	Used for Tomcat communication.
	TCP 705	Used by Sub Agent-Master Agent communication inside the Administration Console.
Browsers	UDP 161	Used for communication by an external Network Monitoring System with the Administration Console by using SNMP.
	TCP 8080	For HTTP communication from browsers to the Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from browsers to the Administration Console. NOTE: 2443 and 2080 are optional ports required when the Administration Console and Identity Server are collocated.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.

Table 8-3 When a Firewall Separates the Identity Server from a Component

Component	Port	Description
Access Gateway	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. The default ports for the Identity Server are TCP 8080 and 8443. They are configurable. You need to open the port that you configured for the base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to ESP of the Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443.

Component	Port	Description
ESP Enabled SSL VPN	TCP 8080 or 8443	<p>For authentication communication from SSL VPN to the Identity Server. TCP 8080 and 8443 are the default ports for the Identity Server. They are configurable. You need to open the port of the base URL of the Identity Server.</p> <p>Also for communication from the Identity Server to ESP SSL VPN. This is the <i>Embedded Service Provider Base URL</i> on the Configuration page. The default values are TCP 8080 and 8443.</p>
Traditional SSL VPN	N/A. Traditional SSL VPN never communicates directly with the Identity Server.	
Administration Console	TCP 1443	For communication from the Administration Console to devices. This is configurable.
	TCP 8444	For communication from the Identity Server to the Administration Console.
	TCP 1289	For communication from the Identity Server to the Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPki from the Identity Server to the Administration Console.
	TCP 636	For secure LDAP communication from the Identity Server to the Administration Console.
Identity Server	TCP 8443 or 443	For HTTPS communication. You can use iptables to configure this for TCP 443. See “Translating the Identity Server Configuration Port” in the <i>NetIQ Access Manager 4.0 SP1 Identity Server Guide</i> .
	TCP 7801, 7802	<p>For back-channel communication with cluster members. You need to open two consecutive ports for the cluster, for example 7801 and 7802.</p> <p>The initial port (7801) is configurable.</p>
LDAP User Stores	TCP 636	For secure LDAP communication from the Identity Server to the LDAP user store.
Service Providers	TCP 8445	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service consumer.

Component	Port	Description
Browsers	TCP 8080, 3080, 3443	For HTTP communication from a browser to the Identity Server. You can use iptables to configure this for TCP 80. See “Translating the Identity Server Configuration Port” in the <i>NetIQ Access Manager 4.0 SP1 Identity Server Guide</i> . NOTE: 3080 and 3443 are optional ports. These are required when SSL VPN and Identity Server are collocated.
	TCP 8443	For HTTPS communication from a browser to the Identity Server. You can use iptables to configure this for TCP 443. See “Translating the Identity Server Configuration Port” in the <i>NetIQ Access Manager 4.0 SP1 Identity Server Guide</i> .
CRL and OCSP Servers	Configurable	If you are using x.509 certificates that include an AIA or CRL Distribution Point attribute, you need to open the port required to talk to that server. Ports 80/443 are the most common ports, but the LDAP ports 389/636 can also be used.
Active Directory Server with Kerberos	TCP 88, UDP 88	For communication with the KDC on the Active Directory Server for Kerberos authentication.

Table 8-4 When a Firewall Separates the Access Gateway from a Component

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. The default ports are TCP 8080 and 8443, which are configurable. You need to open the port of the base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to ESP of the Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443.
Administration Console	TCP 1443	For communication from the Administration Console to the Access Gateway. This is configurable.
	TCP 8444	For communication from the Access Gateway to the Administration Console.
	TCP 1289	For communication from the Access Gateway to the Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPki from the Access Gateway to the Administration Console.
	TCP 636	For secure LDAP communication from the Access Gateway to the Administration Console.
ESP Enabled SSL VPN	N/A. ESP-enabled SSL VPN never communicates directly with the Access Gateway.	

Component	Port	Description
Traditional SSL VPN	TCP 8080	(Access Gateway Appliance) For HTTP communication from the Access Gateway to SSL VPN.
	TCP 8443	(Access Gateway Appliance) If SSL has been enabled between the Access Gateway and SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to SSL VPN.
Access Gateway	TCP 7801, 7802	For back-channel communication with cluster members. You need the first port plus 1. The initial port (7801) is configurable. It is set by the Identity Server cluster configuration that the Access Gateway trusts. See “Configuring a Cluster with Multiple Identity Servers” in the “NetIQ Access Manager 4.0 SP1 Identity Server Guide” .
Browsers/Clients	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to Web servers. This is configurable.

NOTE: On SLES 11 SP2 (or a higher version), you can use YaST to configure UDP ports and internal networks.

Table 8-5 When a Firewall Separates Traditional SSL VPN from a Component

Component	Port	Description
Access Gateway	TCP 8080	For HTTP communication from the Access Gateway to SSL VPN.
	TCP 8443	If SSL has been enabled between the Access Gateway and SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to SSL VPN.
Identity Server	N/A.	SSL VPN never communicates directly with the Identity Server.

Component	Port	Description
Administration Console	TCP 1443	For communication from the Administration Console to SSL VPN. This is configurable.
	TCP 8444	For communication from SSL VPN to the Administration Console.
	TCP 1289	For communication from SSL VPN to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPki from SSL VPN to the Administration Console.
	TCP 636	For secure LDAP communication from SSL VPN to the Administration Console.
SSL VPN Server	TCP 8900	For communication between the cluster members. This is a default port. You can use any other free port.
Browsers	TCP 8080	For HTTP communication.
	TCP 8443	For HTTPS communication.
SOCKS server	TCP 7777	For SOCKS communication from SSL VPN to the SOCKS server. This is the default port for access to SSL VPN, but it can be configured to use TCP 443.
OpenVPN	UDP 7777	For OpenVPN server communication. This is the default port for access to SSL VPN, but it can be configured to use UDP 443.
Application Servers (E-mail, Telnet, Thin Client)	TCP 22	For SSH communication from SSL VPN to the application server.
	TCP 23	For Telnet communication from SSL VPN to the application server.
	Application ports	Specific to the application that SSL VPN is providing access to.
Firewall on same machine as SSL VPN	tun0	SSL VPN creates a tunnel that needs to be open on the internal networks list of the machine.

Table 8-6 When a Firewall Separates ESP-Enabled SSL VPN from a Component

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from SSL VPN to the Identity Server. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the base URL of the Identity Server.
		For communication from the Identity Server to the Embedded Service Provider of SSL VPN. This is the <i>Embedded Service Provider Base URL</i> on the Configuration page. The default values are TCP 8080 and 8443.

Component	Port	Description
Administration Console	TCP 1443	For communication from the Administration Console to SSL VPN. This is configurable.
	TCP 8444	For communication from SSL VPN to the Administration Console.
	TCP 1289	For communication from SSL VPN to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPki from SSL VPN to the Administration Console.
	TCP 636	For secure LDAP communication from SSL VPN to the Administration Console.
ESP-Enabled SSL VPN	TCP 7801 and 8900	For communication between the cluster members. 8900 is a default port. You can use any other free port instead of 8900.
Browsers	TCP 8080	For HTTP communication.
	TCP 8443	For HTTPS communication.
SOCKS server	TCP 7777	For SOCKS communication from SSL VPN to the SOCKS server. This is the default port for access to SSL VPN, but it can be configured to use TCP 443.
OpenVPN	TCP 7777	For OpenVPN server communication. This is the default port for access to SSL VPN, but it can be configured to use UDP 443.
Application Servers (E-mail, Telnet, Thin Client)	TCP 22	For SSH communication from SSL VPN to the application server.
	TCP 23	For Telnet communication from SSL VPN to the application server.
	Application ports	Specific to the application that SSL VPN is providing access to.
Firewall on same machine as SSL VPN	tun0	SSL VPN creates a tunnel that needs to be open on the internal networks list of the machine. For configuration information, see the following Note.

8.2 Restricted Ports

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

22
111
524
1443
2443
3443
8028
8030

8080
8443
8444
9000
9001
55982
61222
61613
61616
61617

If required, use port redirection by using IP tables.

8.3 Sample Configurations

- ♦ [Section 8.3.1, “Access Gateway and Identity Server in DMZ,” on page 89](#)
- ♦ [Section 8.3.2, “A Firewall Separating Access Manager Components from the LDAP Servers,” on page 90](#)
- ♦ [Section 8.3.3, “Configuring a Firewall for SSL VPN,” on page 91](#)

8.3.1 Access Gateway and Identity Server in DMZ

- ♦ [“First Firewall” on page 89](#)
- ♦ [“Second Firewall” on page 90](#)

First Firewall

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

See, [Figure 8-1 on page 81](#)

Table 8-7 Ports to Open in the First Firewall

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	
TCP 8080	For HTTP communication with the Identity Server. For information about redirecting the Identity Server to use port 80, see “Translating the Identity Server Configuration Port” in the <i>NetIQ Access Manager 4.0 SP1 Identity Server Guide</i> .
TCP 8443	For HTTPS communication with the Identity Server. For information about redirecting the Identity Server to use port 443, see “Translating the Identity Server Configuration Port” in the <i>NetIQ Access Manager 4.0 SP1 Identity Server Guide</i> .
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.

Second Firewall

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

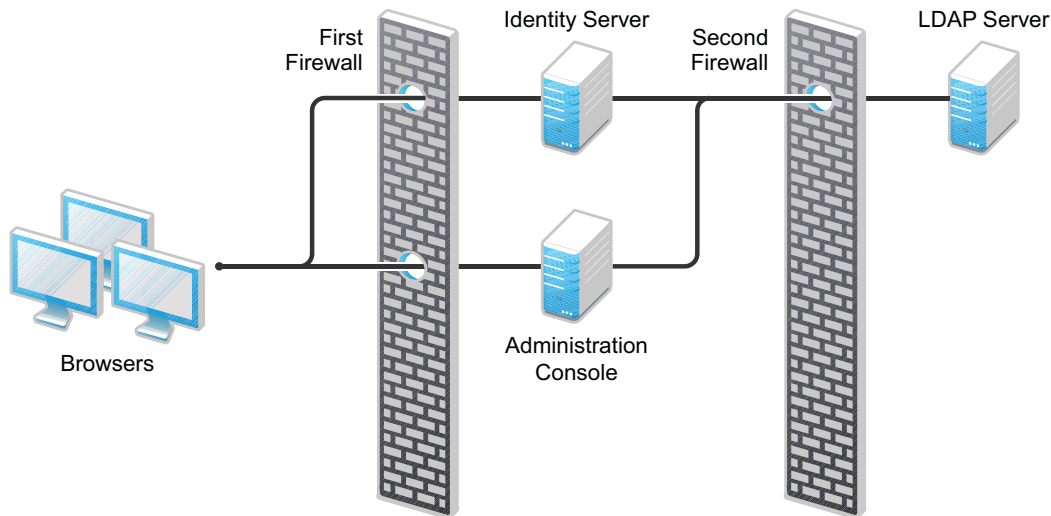
Table 8-8 Ports to Open in the Second Firewall

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

8.3.2 A Firewall Separating Access Manager Components from the LDAP Servers

You can configure your Access Manager components so that your Administration Console is on the same side of the firewall as your Access Manager components and have a firewall between them and the LDAP servers.

Figure 8-2 A Firewall Separating the Administration Console and the LDAP Server



In this configuration, you need to have the following ports opened in the second firewall for the Administration Console and the Identity Server.

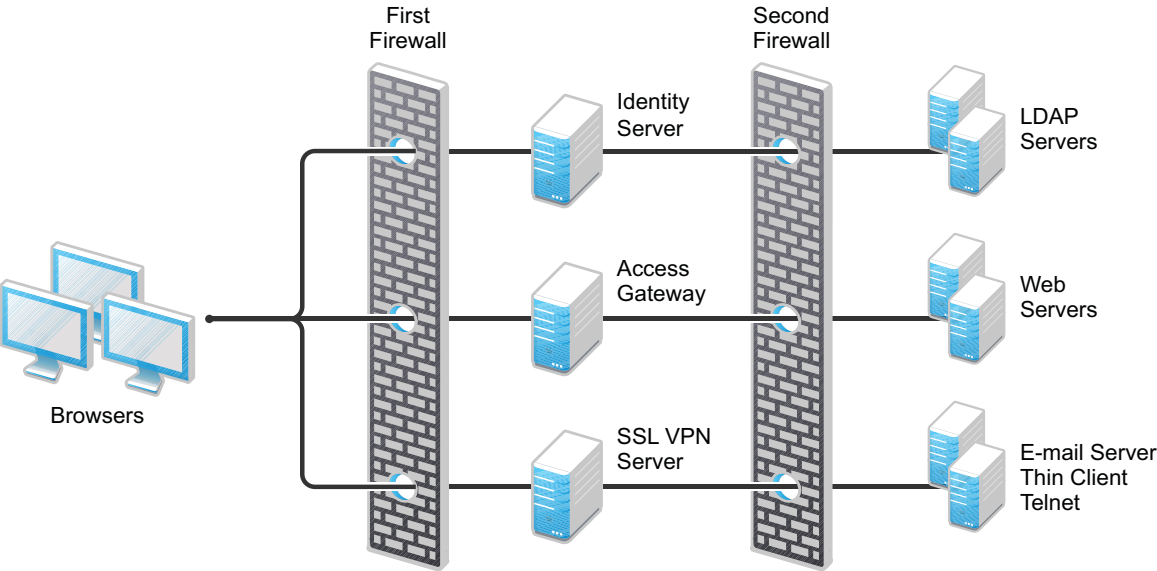
Table 8-9 Ports to Open in the Second Firewall

Ports	Purpose
TCP 636	For secure LDAP communication. This is used by the Identity Server and the Administration Console.
TCP 524	For configuring eDirectory as a new User Store. NCP is used to enable SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. During day-to-day operations, this port is not used. If your LDAP server is Active Directory or Sun ONE, this port does not need to be opened.

8.3.3 Configuring a Firewall for SSL VPN

SSL VPN can be installed as a separate machine or as a component running on the Linux Access Gateway. Although it is configured to be a protected resource of the Access Gateway, it also allows direct communication with client browsers.

Figure 8-3 SSL VPN Server and Firewalls



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

Table 8-10 Ports to Open in the First Firewall for SSL VPN

Port	Purpose
TCP 7777	For client communication. This is the default port. You can configure it to use TCP 443.

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

Table 8-11 Ports to Open in the Second Firewall for SSL VPN

Port	Purpose
TCP 22	For SSH.
TCP 23	For Telnet.
Ports specific to an application.	

9 Uninstalling Components

This section discusses the following topics related to installation:

- ♦ [Section 9.1, “Uninstalling the Identity Server,” on page 93](#)
- ♦ [Section 9.2, “Reinstalling an Identity Server to a New Hard Drive,” on page 94](#)
- ♦ [Section 9.3, “Uninstalling the Access Gateway,” on page 95](#)
- ♦ [Section 9.4, “Uninstalling the Administration Console,” on page 96](#)
- ♦ [Section 9.5, “Uninstalling the SSL VPN Server,” on page 97](#)

9.1 Uninstalling the Identity Server

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

1. Removing the Identity Server from the Administration Console. See [Section 9.1.1, “Deleting Identity Server References,” on page 93](#).
2. Removing the Identity Server software from the Linux or Windows machine. See [Section 9.1.2, “Uninstalling the Linux Identity Server,” on page 93](#) or [Section 9.1.3, “Uninstalling the Windows Identity Server,” on page 94](#).

9.1.1 Deleting Identity Server References

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

- 1 In the Administration Console, click **Devices > Identity Servers**.
- 2 Select the Identity Server that you want uninstalled, then click **Stop**.
- 3 Wait for its health to turn red, then select the server and click **Actions > Remove from Cluster**.
- 4 Update the cluster configuration.
- 5 Select the Identity Server that you are going to uninstall, then click **Actions > Delete**.
- 6 Continue with [Section 9.1.2, “Uninstalling the Linux Identity Server,” on page 93](#) or [Section 9.1.3, “Uninstalling the Windows Identity Server,” on page 94](#).

9.1.2 Uninstalling the Linux Identity Server

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

- 1 On your Linux Identity Server, insert the Access Manager installation CD.
- 2 Navigate to the `novell-access-manager` directory.
- 3 Enter `./uninstall.sh` to initiate the uninstallation script.
- 4 Select 2 to uninstall the Identity Server.

- 5 Enter the name and password of the admin user. (When Administration Console and Identity Server are installed on the same server)

Uninstall removes the Identity Server. A log file is created at `/tmp/novell_access_manager_uninstall.log`.

9.1.3 Uninstalling the Windows Identity Server

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

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

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

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

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

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

If the uninstall fails because the primary Administration Console is not available to validate the credentials, see [Section A.11, "Troubleshooting the Uninstall of the Windows Identity Server," on page 109](#).

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

9.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall the Identity Server (see [Chapter 3, "Installing the Identity Servers," on page 45](#)) and leave the Identity Server configuration intact in the Administration Console. In order to preserve the existing keystores, perform the following steps before installing the Identity Server on the new hard drive.

- 1 Stop the server.
In the Administration Console, click **Access Manager > Identity Servers**. Select the server and click **Stop**. Allow a few seconds for the server to stop.
- 2 Select the server, then click **Actions > Remove from configuration**.
- 3 Select the server, then click **Actions > Delete**.
- 4 Reinstall the Identity Server. (See [Chapter 3, "Installing the Identity Servers," on page 45](#).)
- 5 On the Identity Servers page, select the server, then click **Actions > Assign to Cluster**.

- 6 Select the Identity Server cluster configuration, then click **Assign**.
- 7 Click **OK**.

9.3 Uninstalling the Access Gateway

- 1 In the Administration Console, click **Access Gateways**.
- 2 If the Access Gateway belongs to a cluster, you need to remove it from the cluster.
 - 2a Select the Access Gateway, then click **Actions > Remove from Cluster**:
 - 2b Confirm the action, then click **OK**.
- 3 On the Access Gateways Servers page, select the name of the server, then click **Actions > Delete > OK**.

This removes the configuration object for the Access Gateway from the Administration Console.
- 4 On the Identity Servers page, update the Identity Server status for the Identity Server cluster configuration that was using this Access Gateway.

See [“Updating an Identity Server Configuration”](#) in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.
- 5 Complete one of the following:
 - ♦ If you are uninstalling the Access Gateway Appliance machine, re-image the machine by booting to a CD containing the desired operating system software.
 - ♦ If you are uninstalling the Windows Access Gateway Service, continue with [Section 9.3.1, “Uninstalling the Windows Access Gateway Service,”](#) on page 95.
 - ♦ If you are uninstalling the Linux Access Gateway Service, continue with [Section 9.3.2, “Uninstalling the Linux Access Gateway Service,”](#) on page 95.

9.3.1 Uninstalling the Windows Access Gateway Service

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

If the uninstall fails because the program cannot authenticate to the Administration Console, see [Section A.10, “Troubleshooting the Uninstall of the Access Gateway Service,”](#) on page 108.

9.3.2 Uninstalling the Linux Access Gateway Service

- 1 On your Linux Access Gateway Service, insert the Access Manager installation CD.
- 2 Navigate to the `novell-access-gateway` directory.
- 3 Enter `./uninstall.sh` to initiate the uninstallation script.
- 4 Enter the name of the admin user.
- 5 Enter the password of the admin user.

Uninstall removes the Access Gateway Service. A log file is created at `/tmp/novell_access_manager_uninstall.log`.

If the uninstall fails, see [Section A.10, “Troubleshooting the Uninstall of the Access Gateway Service,” on page 108](#).

9.4 Uninstalling the Administration Console

Only the primary version of the Administration Console contains the certificate authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You need to promote a secondary console to be the primary console. See [“Installing Secondary Versions of the Administration Console”](#) in the *NetIQ Access Manager 4.0 SP1 Setup Guide*.

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

Select the process that corresponds to your platform:

- ♦ [Section 9.4.1, “Uninstalling the Linux Administration Console,” on page 96](#)
- ♦ [Section 9.4.2, “Uninstalling the Windows Administration Console,” on page 97](#)

9.4.1 Uninstalling the Linux Administration Console

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

```
./uninstall.sh
```

- 4 Select one of the following options:

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

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

A log file is created at `/tmp/novell_access_manager_uninstall.log`.

9.4.2 Uninstalling the Windows Administration Console

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

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

The uninstall begins. If the uninstall hangs, see [Section A.11, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 109](#).

9.5 Uninstalling the SSL VPN Server

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

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

- ♦ [Section 9.5.1, “Deleting the SSL VPN Server References,” on page 97](#)
- ♦ [Section 9.5.2, “Uninstalling the SSL VPN Server,” on page 98](#)
- ♦ [Section 9.5.3, “Uninstalling the RPM Key for High Bandwidth SSL VPN,” on page 98](#)

9.5.1 Deleting the SSL VPN Server References

- 1 In the Administration Console, *Devices > Devices > SSL VPNs*.
- 2 Select the SSL VPN server that you want to uninstall.
- 3 (Optional) If the server is part of a cluster, select *Actions > Remove from Cluster*, then click *OK* to confirm.
- 4 Update the cluster configuration.
- 5 Select the SSL VPN Server that you want to uninstall, then click *Actions > Delete*.
- 6 Click *OK*.
- 7 Proceed with [Section 9.5.2, “Uninstalling the SSL VPN Server,” on page 98](#) to uninstall the SSL VPN server.

9.5.2 Uninstalling the SSL VPN Server

IMPORTANT: If you have installed the high-bandwidth SSL VPN key, uninstall the key before proceeding to uninstall the SSL VPN server. For more information on uninstalling the high-bandwidth key, see [Section 9.5.3, “Uninstalling the RPM Key for High Bandwidth SSL VPN,”](#) on page 98.

- 1 Browse and locate the uninstall script `uninstall.sh`.
The uninstall script is located in the root directory of the installation CD or in the installation directory.
- 2 At the command prompt, run the following command:

```
./uninstall.sh
```
- 3 Do one of the following, depending on your installation type:
 - ♦ Enter 4 to uninstall the Traditional NetIQ SSL VPN.
 - ♦ Enter 5 to uninstall the ESP-enabled NetIQ SSL VPN.

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

9.5.3 Uninstalling the RPM Key for High Bandwidth SSL VPN

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

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

A Troubleshooting Installation

- ♦ [Section A.1, “Troubleshooting a Windows Administration Console Installation,” on page 99](#)
- ♦ [Section A.2, “Troubleshooting a Windows SSL Renegotiation,” on page 100](#)
- ♦ [Section A.3, “Troubleshooting an Identity Server Import and Installation,” on page 101](#)
- ♦ [Section A.4, “Troubleshooting the Access Gateway Service Installation,” on page 103](#)
- ♦ [Section A.5, “Troubleshooting the SSL VPN Installation,” on page 104](#)
- ♦ [Section A.6, “Troubleshooting the Access Gateway Import,” on page 105](#)
- ♦ [Section A.7, “Troubleshooting a Linux SSL Renegotiation,” on page 107](#)
- ♦ [Section A.8, “Secondary Administration Console Installation Fails,” on page 108](#)
- ♦ [Section A.9, “Access Gateway Appliance Installation Fails Due to an XML Parser Error,” on page 108](#)
- ♦ [Section A.10, “Troubleshooting the Uninstall of the Access Gateway Service,” on page 108](#)
- ♦ [Section A.11, “Troubleshooting the Uninstall of the Windows Identity Server,” on page 109](#)
- ♦ [Section A.12, “Portal Web Server is not Accessible,” on page 109](#)
- ♦ [Section A.13, “Installing RHEL on the Administration Console Fails if IPv6 is Disabled,” on page 109](#)

A.1 Troubleshooting a Windows Administration Console Installation

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

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

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

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

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

A terminal window opens to display standard output.

Additional verbose information is sent to the `\am32setup_debug.txt` file.

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

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

4a Delete the temporary packages in the `\pkgdirs` directory, then delete the directory.

4b Delete the `\am32setup_debug.txt` file.

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

Windows 2008/2012 Server: `\am32setup.log`

Windows 2008/2012 Server: `\Program Files (x86)\Novell\log`

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

A.2 Troubleshooting a Windows SSL Renegotiation

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

- 1 Launch Registry Editor by executing the **Start > Run** regedit command.
- 2 In the left pane of Registry Editor, navigate to **My Computer > HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java**.
- 3 Double-click **Options** in the right pane of the Registry Editor.
- 4 Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
 - ♦ If `-Dsun.security.ssl.allowUnsafeRenegotiation` is available, set the value to true. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=true`
 - ♦ If `-Dsun.security.ssl.allowUnsafeRenegotiation` is not available, add `-Dsun.security.ssl.allowUnsafeRenegotiation=true`
- 5 Go to `C:\Program Files(x86)\Novell\Tomcat\conf\server.xml > Server > Service > Connector`, then search for the connector 8443 and check if the connector has the port 8443.
- 6 Add the `allowUnsafeLegacyRenegotiation=true` string.
- 7 Restart Tomcat to enable the SSL renegotiation.

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

- 1 Launch Registry Editor by executing the command regedit in **Start > Run**.
- 2 In the left pane of Registry Editor, navigate to **My Computer > HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java**.
- 3 Double-click **Options** in the right pane of registry editor.
- 4 Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
 - ♦ If `-Dsun.security.ssl.allowUnsafeRenegotiation` is available, set the value to true. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=true`.
 - ♦ If `-Dsun.security.ssl.allowUnsafeRenegotiation` is not available, add `-Dsun.security.ssl.allowUnsafeRenegotiation=true`.
- 5 Go to `C:\Program Files(x86)\Novell\Tomcat\conf\server.xml > Server > Service > Connector.`, then search for the connector 8443 and check if the connector has the port 8443.
- 6 Add the `allowUnsafeLegacyRenegotiation=true` string.
- 7 Restart Tomcat to enable the SSL renegotiation.

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

- 1 Launch Registry Editor by executing the command regedit in **Start > Run**.
- 2 In the left pane of Registry Editor, navigate to **My Computer > HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java**.
- 3 Double-click **Options** in the right pane of registry editor.

- 4 Search for the `-Dsun.security.ssl.allowUnsafeRenegotiation` string.
- 5 In `-Dsun.security.ssl.allowUnsafeRenegotiation`, set the value to false. For example, `-Dsun.security.ssl.allowUnsafeRenegotiation=false`
- 6 Restart Tomcat to disable the SSL renegotiation.

A.3 Troubleshooting an Identity Server Import and Installation

- ♦ [Section A.3.1, “The Identity Server Fails to Import into the Administration Console,” on page 101](#)
- ♦ [Section A.3.2, “Reimporting the Identity Server,” on page 101](#)
- ♦ [Section A.3.3, “Check the Installation Logs,” on page 102](#)

A.3.1 The Identity Server Fails to Import into the Administration Console

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

- ♦ Is the firewall enabled on the Administration Console or the Identity Server?

The firewall needs to have the following ports opened between the machines so that the Identity Server can import into the Administration Console:

8444
1443
1289
524
636

The Identity Server firewall also needs to have ports 8080 and 8443 open between the server and the clients in order for the clients to log into the Identity Server. For more information about firewalls and ports, see [Chapter 8, “Setting Up Firewalls,” on page 81](#).

- ♦ Time needs to be synchronized between the two machines. Make sure that both machines have been configured to use a Network Time Protocol server.
- ♦ If firewalls and time synchronization do not solve the problem, run the reimport script. See [Section A.3.2, “Reimporting the Identity Server,” on page 101](#) for instructions.

A.3.2 Reimporting the Identity Server

- 1 Verify that the Administration Console is up by logging into the Administration Console from a Web browser.
- 2 Verify that you can communicate with the Administration Console. From the command line of the Identity Server machine, enter a `ping` command with the IP address of the Administration Console.

If the `ping` command is unsuccessful, fix the network communication problem before continuing.
- 3 In the Administration Console, delete the Identity Server.

For more information about how to delete the Identity Server in the Administration Console, see [“Managing an Identity Server” in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*](#).

- 4 On the Identity Server machine, change to the `jcc` directory:
Linux: `/opt/novell/devman/jcc`
Windows: `\Program Files\Novell\devman\jcc`
- 5 Run the reimport script for `jcc`:
Linux: `./conf/reimport_nidp.sh jcc`
Windows: `conf\reimport_nidp.bat jcc`
- 6 Run the reimport script for the Administration Console:
Linux: `./conf/reimport_nidp.sh nidp`
Windows: `conf\reimport_nidp.bat nidp <admin>`
Replace `<admin>` with the name of your administrator for the Administration Console.
- 7 If these steps do not work, reinstall the device.

A.3.3 Check the Installation Logs

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

- ♦ [“Linux Installation Logs” on page 102](#)
- ♦ [“Windows Installation Logs” on page 102](#)

Linux Installation Logs

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

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

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

Windows Installation Logs

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

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

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

A.4 Troubleshooting the Access Gateway Service Installation

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

- ♦ [Section A.4.1, “Troubleshooting the Windows Access Gateway Service Installation,” on page 103](#)

A.4.1 Troubleshooting the Windows Access Gateway Service Installation

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

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

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

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

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

A terminal window opens to display standard output.

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

- 3 Use the output and the log file to discover the cause of the problem.
- 4 After you run the installation in debug mode, you must clean up the results:
 - 4a Delete the `\agsinstall_debug.txt` file.
 - 4b Delete the installation log files in the following directories:

Windows 2008/2012 Server: \agsinstall.log

Windows 2008/2012 Server: \Program Files (x86)\Novell\log

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

A.5 Troubleshooting the SSL VPN Installation

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

- ♦ [Section A.5.1, “Manually Uninstalling the Enterprise Mode Thin Client,” on page 104](#)
- ♦ [Section A.5.2, “SSL VPN Health Status Is Yellow after an Upgrade,” on page 105](#)

A.5.1 Manually Uninstalling the Enterprise Mode Thin Client

To manually uninstall the Enterprise mode thin client, do one of the following, depending on your operating software:

- ♦ **Windows:** If you are a Windows user, log in as admin and run `uninstall.exe` located in the `c:\Program Files\Novell sslvpn service` directory. You can also uninstall the SSL VPN service through *Start > Control Panel > Add or Remove Programs*.

- ♦ **Linux:** If you are a Linux user, log in as `root` and enter the following command on the Linux workstation:

```
rpm -e novl-sslvpn-service
```

- ♦ **Macintosh:** If you are a Macintosh user, log in as `root` and do the following on the Macintosh workstation:

1. Enter the following command to stop the SSL VPN services:

```
/System/Library/StartupItems/novell-sslvpn-service/novell-sslvpn-service  
stop
```

2. Enter the following command to remove all the contents of the package:

```
rm -rf /System/Library/StartupItems/novell-sslvpn-service  
rm -rf /Library/Receipts/novl-sslvpn-service.pkg  
rm -f /usr/sbin/novl-sslvpn-service  
rm -f /usr/sbin/novl-sslvpn-service-upgrade  
rm -f /etc/novell-sslvpn-serv.conf
```

NOTE: If you are an administrator or a `root` user of the machine, you cannot switch from Enterprise mode to Kiosk mode unless your system administrator has configured you to connect only in Kiosk mode.

A.5.2 SSL VPN Health Status Is Yellow after an Upgrade

If the status of SSL VPN server installed with Linux Access Gateway is yellow and the *Health* tab displays the following message:

The HTTP Reverse Proxy service "soapbc" is functioning properly. The HTTP Reverse Proxy service <reverse proxy> might not be functioning properly. Few of the webserver being accelerated are unreachable <Webserver IP>:8080.

Modify the existing path-based service accelerating SSL VPN server and configure the loopback IP 127.0.0.1 as the Web server IP.

A.6 Troubleshooting the Access Gateway Import

When you install the Access Gateway, it should automatically be imported into the Administration Console you specified during installation. If the Access Gateway does not appear in the server list, you need to repair the import.

If the repair option does not correct the problem, the following sections explain what should happen and how you can discover what went wrong. This information can be used to accurately report the problem to NetIQ Support.

- ♦ [Section A.6.1, "Repairing an Import," on page 105](#)
- ♦ [Section A.6.2, "Troubleshooting the Import Process," on page 106](#)

A.6.1 Repairing an Import

If the Access Gateway does not appear in the Administration Console within ten minutes of installing an Access Gateway, complete the following steps:

- 1 If a firewall separates the Administration Console and the Access Gateway, make sure the correct ports are opened. See [Table 8-2, "When a Firewall Separates the Administration Console from a Component," on page 82](#)
- 2 In the Administration Console, click **Devices > Access Gateways**.
- 3 Wait a few minutes, then click **Refresh**.
- 4 Look for a failed import message.

If the device starts an import but fails to finish, a message similar to the following appears at the bottom of the table:

Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

- 5 Click **repair import**.
- 6 If the device still does not appear or you do not receive a repair import message, continue with ["Triggering an Import Retry" on page 107](#).
- 7 If triggering an import retry does not solve the problem, reinstall the device.

A.6.2 Troubleshooting the Import Process

If a step in the import process does not complete successfully, the device does not show up in the Access Gateway list. The sections below describe the import process, where to find the log files, and how to use them to determine where the failure occurred so you can accurately report the problem.

- ♦ [“Understanding the Import Process” on page 106](#)
- ♦ [“Locating the Log Files” on page 106](#)
- ♦ [“Triggering an Import Retry” on page 107](#)

Understanding the Import Process

The following operations are performed during the import process:

1. A user specifies the IP address for the Administration Console during installation.
2. A Java process called “JCC” (Java Communication Channel) detects that the Administration Console IP address/port has changed between its own configuration and the CLI-updated settings.
3. An import message is sent to Administration Console, notifying it of the IP, port, and ID of the Access Gateway device.
4. The Administration Console then connects to the Access Gateway device, asking for its configuration and version information. The Access Gateway portion of the import process is now complete.
5. As a separate asynchronous operation, the Embedded Service Provider (ESP) of the Access Gateway connects and registers itself with the JCC.
6. When the ESP connects to the JCC, a similar import message is sent to the Administration Console notifying it to import into the system.
7. The Administration Console connects to the JCC, asking for the ESP configuration and version information. On the Administration Console, an LDIF (Lightweight Directory Interchange Format) file containing the default configuration for the ESP is applied on the local eDirectory configuration store.
8. The Administration Console then makes a link between the ESP and its configuration.
9. If the entire process completed properly, the Access Gateway device appears in the list of Access Gateways in the Administration Console.

Locating the Log Files

Various Access Manager components produce log files. You use the following logs on either the Administration Console or the Access Gateway.

- ♦ Administration Console log:

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

Windows Server 2008/2012: `\Program Files (x86)\Novell\log\app_sc.0.log`

- ♦ Tomcat Log on the Administration Console:

Linux: `/opt/novell/nam/device_name/logs/catalina.out`

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

Windows Server 2008/2012: `\Program Files (x86)\Novell\Tomcat\logs\stdout.log` and `\Program Files (x86)\Novell\Tomcat\logs\stderr.log`

- ♦ JCC log on the Access Gateway:
Linux Appliance or Service: /opt/novell/devman/jcc/logs/
Windows Service: \Program Files\Novell\devman\jcc\logs

Triggering an Import Retry

- 1 Go to the directory /opt/novell/devman/jcc/
`cd /opt/novell/devman/jcc/`
- 2 Run the `sh conf/reimport_ags.sh jcc` script and enter the details against the following prompts:
 - ♦ Choose a local listener IP address [x.x.x.x]:
 - ♦ (Optional) Choose a local NAT IP address [optional]:
 - ♦ Choose Administration Console's IP address []:
 - ♦ Enter Admin User's DN [cn=admin,o=novell]:
 - ♦ Enter Admin Password: *****

Wait for a few minutes for the configuration to finish.
- 3 Run the `sh conf/reimport_ags.sh agm` script and enter details against the following prompts:
 - ♦ Do you want to import the device with current configuration or initial configuration after installation (Enter C for current configuration, I for initial configuration).
 - ♦ Enter Admin User's DN [cn=admin,o=novell]:
 - ♦ Enter Admin password:

A.7 Troubleshooting a Linux SSL Renegotiation

To enable the SSL renegotiation on SLES 11 SP2 and SP3, add the parameter `JAVA_OPTS="{JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=true` in the configuration file `/var/opt/novell/tomcat7/conf/tomcat7.conf` if the parameter does not exist.

Restart Tomcat to enable SSL renegotiation.

To disable the SSL renegotiation on SLES 11 SP2 and SP3, add the parameter `JAVA_OPTS="{JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=false` in the configuration file `/var/opt/novell/tomcat7/conf/tomcat7.conf` if the parameter does not exist.

Restart Tomcat to disable SSL renegotiation.

A.8 Secondary Administration Console Installation Fails

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

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

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

A.9 Access Gateway Appliance Installation Fails Due to an XML Parser Error

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

A.10 Troubleshooting the Uninstall of the Access Gateway Service

When you uninstall an Access Gateway, the uninstall program prompts you for the credentials of the admin user for the Administration Console. If the primary Administration Console is not available for the authentication request, the uninstall fails.

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

Linux Access Gateway Service

```
/opt/novell/accessgateway/removeAccessGateway -DAM_INSTALL_AUTH_BYPASS=true
```

Windows Access Gateway Service:

```
\Program Files\Novell\UninstallData\remove_AccessGateway.exe -DAM_INSTALL_AUTH_BYPASS=true
```

A.11 Troubleshooting the Uninstall of the Windows Identity Server

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

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

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

A.12 Portal Web Server is not Accessible

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

A.13 Installing RHEL on the Administration Console Fails if IPv6 is Disabled

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

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

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

B Feature Comparison of Different Types of Access Gateways

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

- ♦ Protecting Web resources with contracts, Authorization, Form Fill, and Identity Injection policies.
- ♦ Providing fault tolerance by clustering multiple gateways of the same type.
- ♦ Providing fault tolerance by grouping multiple Web servers, so that if one Web server goes down, the content can be retrieved from another server in the group.
- ♦ Rewriting URLs so that the names and IP addresses of the Web servers are hidden from the users making requests.
- ♦ Generating alert, audit, and logging events with notify options.

Most differences among 3.1 Access Gateway, Access Gateway Appliance, and Access Gateway Service result from the differences required for an appliance and for a service. An appliance can know, control, and configure many features of the operating system. A service that runs on top of an operating system can query the operating system for some information, but it cannot configure or control the operating system. For the service, operating system utilities must be used to configure system parameters and hardware. For the appliance, the operating system features that are important to the appliance, such as time, DNS servers, gateways, and network interface cards, can be configured in the Administration Console.

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

Table B-1 Differences among the 3.1 Access Gateway, Access Gateway Appliance, and Access Gateway Service:

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
System architecture	32-bit	64-bit only	64-bit only
Platform support	SLES only	SLES only	SLES 11 SP2 and SP3, Red Hat Enterprise Linux, Windows

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Network configuration	Can be done from the Administration Console.	Can be done from the Administration Console. By default after the installation, only one network interface card will be displayed in the Administration Console. To detect other network interface card, do the following: <ul style="list-style-type: none"> ◆ Configure a primary IP Address in YaST for the remaining interfaces. ◆ Click Devices > Access Gateways > Select the device > New IP > click OK. 	Configurable with standard operating system utilities.
<ul style="list-style-type: none"> ◆ DNS servers ◆ Gateways ◆ Network interface cards ◆ Host names 			
Date and time	Can be done from the Administration Console.	Can be done from the Administration Console.	Configurable with standard operating system utilities.
Rewriter: Number of URLs that can be rewritten	There is a set limit.	No limit	No limit
Rewriter: Profiles	Can do word pattern matches in Word profiles and Character profiles.	Can only do word pattern matches in Character profiles.	Can only do word pattern matches in Character profiles.
Rewriter: Word profiles	Case-sensitive	Case-insensitive	Case-insensitive
Rewriter: Special tokens for Word profiles	Not supported	Supports the [w], [ow], [ep], [ew], and [oa] options.	Supports the [w], [ow], [ep], [ew], and [oa] options.
Rewriter: webcal	Not supported	Supported	Supported
Cache directory	Separate protected partition.	Uses Apache-caching. The cached files are stored in clear text. The operating system must be configured to protect this directory. For more information about the Apache model, see "Caching Guide" (http://httpd.apache.org/docs/2.2/caching.html) .	Uses filesystem provided by Apache mod_cache module. For more information about the Apache model, see "Caching Guide" (http://httpd.apache.org/docs/2.2/caching.html) .
Cache freshness configuration options	Supported	Limited support. You can achieve the following with Advanced Options: <ul style="list-style-type: none"> ◆ HTTP Maximum Cache Time ◆ HTTP Minimum Cache Time Continue Fill Time and HTTP Retries are not available.	Similar to Access Gateway Appliance

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Custom cache control headers	Supported	Not supported	Not supported
Caching behavior	For more information, see “Configuring Caching Options” in the <i>NetIQ Access Manager 4.0 SP1 Access Gateway Guide</i> .	For more information, see “Configuring Caching Options” in the <i>NetIQ Access Manager 4.0 SP1 Access Gateway Guide</i> .	For more information, see “Configuring Caching Options” in the <i>NetIQ Access Manager 4.0 SP1 Access Gateway Guide</i> .
X-Forwarded-For header	Can enable/disable from the Administration Console	Cannot disable. By default, it is sent by Apache along with X-Forwarded-Host and X-Forwarded-Server headers.	Cannot disable. By default, it is sent by Apache along with X-Forwarded-Host and X-Forwarded-Server headers.
Via header	Includes the device ID and version number.	Includes the device ID.	Includes the device ID.
Stop and restart commands	Shuts down the operating system or restarts the operating system and the Access Gateway Appliance.	Stops and starts the Access Gateway Service without affecting other services or applications. The operating system can be rebooted or shutdown independently with standard operating system commands.	Stops and starts the Access Gateway Service without affecting other services or applications. The operating system can be rebooted or shutdown independently with standard operating system commands.
Access logs for proxy service:	Stop the proxy service if logging fails.	Cannot stop the proxy service if logging fails.	Cannot stop the proxy service if logging fails.
When protected resource logging fails		For more information about access logging, see “Configuring Logging for a Proxy Service” in the <i>NetIQ Access Manager 4.0 SP1 Access Gateway Guide</i> .	For more information about access logging, see “Configuring Logging for a Proxy Service” in the <i>NetIQ Access Manager 4.0 SP1 Access Gateway Guide</i> .
Web server connections	If the gateway has multiple network cards, you can specify which network card to use for the Web server connection.	Use standard routing table on the right device to route the traffic for that Web server on the device.	Use standard routing table on the device to route the traffic for that Web server on the right device.
Web server certificate verification	Configurable per proxy service.	Globally configurable. If certificate verification is turned on for one proxy service, it is turned on for all proxy services.	Globally configurable. If certificate verification is turned on for one proxy service, it is turned on for all proxy services.
Load balancing cookie	Access Gateway Appliance format.	Access Gateway Appliance format.	Access Gateway Appliance format.

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
5-6 byte UTF characters (supported by IIS Web servers)	Supported	Not supported	Not supported
Custom configuration	Touch files	Advanced options. Click Access Gateways > Edit > Advanced Options or Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > Advanced Options .	Similar to Access Gateway Appliance
Device logging	ics_dyn.log Uses Syslog	ags_error.log and Apache error.log All logs are now in a central location /var/opt/novell/logs	Similar to Access Gateway Appliance
Device logging configuration	Log level set with options in the nash shell.	Configurable from the Administration Console. Click Access Gateways > Edit > Logging .	Similar to Access Gateway Appliance
Sending alerts to an SNMP server	Not supported	Supported	Supported
Manipulates cookies so that when a browser retains application cookies from the Web servers after a user logs out, these cookies become invalid.	Not supported	Supported	Supported
NetStorage	Browser connections can be used.	Browser and WebDAV connections can be used.	Browser and WebDAV connections can be used.

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Inconsistency in 302 redirect message between HTTP and HTTPS.	<p>Request to HTTP port 80 is responded with the following HTML document:</p> <pre> <HTML> <HEAD> <TITLE>Novell Proxy</TITLE> </HEAD> <BODY> <p>HTTP request is being redirected to HTTPS.<p> redirect </p> </BODY> </HTML> </pre>	<p>Similar to Access Gateway Service</p>	<p>Request to HTTP port 80 is responded with the following HTML document:</p> <pre> <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML> <HEAD> <title>302 Found</title> </head> <body> <h1>Found</h1> <p>The document has moved here </p> </body> </html> </pre>
Customizing Error Pages	<p>ErrorPageTemplate.html.<lang> is modified for customizing error pages.</p> <p>ErrorMessages.xml.<lang> is available under</p> <p>/var/novell/cfgdb/ErrorPagesConfig</p>	<p>Similar to Access Gateway Service</p>	<p>/opt/novell/apache2/share/apache2/doc/errors/<http_status_code>.var</p> <p>Edit top.html, bottom.html</p> <p>ErrorMessages.xml.<lang> is available under</p> <p>/opt/novell/nam/mag/webapps/mag/WEB-INF/config/current</p>
Advanced Options configuration	<p>The error page from origin server is forwarded to the browser.</p>	<p>Access Gateway overrides the origin server error page with Access Gateway's error page. This is turned off by default to behave like the Linux Access Gateway. If you do not want to send the origin server's error page, but a customized error page in the Access Gateway, you can enable this as ProxyErrorOverride on.</p>	<p>Access Gateway overrides the origin server error page with Access Gateway's error page. For the error page to behave like Linux Access Gateway configure the ProxyErrorOverride off in Advanced Options.</p>

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Alerts	<p>The warning message log file format has changed. The log file has fewer columns displayed when compared to Access Gateway Appliance/ Service.</p> <p>For example, (Mon Jan 30 12:31:41 2012): Proxy configuration has changed</p>	<p>The log file has more information than the file in the Linux Access Gateway Appliance. For example,</p> <pre><amLogEntry> 2012-01-30T12:17:22Z</pre> <p>WARN ALERT: AMDEVICEID#ag-02EC8D7D5B8A8291:</p> <p>DateTime=1327906042643,</p> <p>Severity=Warn, ServiceType=ag,</p> <p>Message=Access Gateway configuration has changed </amLogEntry></p>	Similar to Access Gateway Appliance
Cache Control options	<p>Enable Custom Cache Control Header</p> <p>When objects reach the Custom Cache Control Expiration Time:</p> <ul style="list-style-type: none"> ♦ opt1: Revalidate the object with a "Get-If-Modified" ♦ opt2: Always obtain a fresh copy of the object. <p>Cache Control Headers</p>	<p>Enable Custom Cache Control Header</p> <p>When objects reach the Custom Cache Control Expiration Time:</p> <ul style="list-style-type: none"> ♦ opt1: Revalidate the object with a "Get-If-Modified" ♦ Unsupported <p>The Cache Control Headers can be injected by using apache <code>mod_headers</code> module directives.</p>	Similar to Access Gateway Appliance
Unreachable webserver	Checks health of Web servers that are marked as unreachable every 30 seconds.	<p>The proxy checks the Web server for each new session request at an interval of 1 minute, by default.</p> <p>You can configure the advanced option for a different interval.</p> <p>For example,</p> <pre>AdditionalBalancerMemberOptions retry=180</pre> <p>where 180 is in seconds.</p>	Similar to Access Gateway Appliance
Client IP mismatch error	On receiving IPC cookie from browser, Linux Access Gateway asks the user to authenticate if it is a protected resource that needs authentication, or, just treats the request for public resources as if the cookie was not received.	On receiving IPC cookie from browser, Access Gateway checks for client IP address in the cookie. If the IP address in the cookie and the client IP address from which the request came do not match, Access Gateway displays an error page.	Similar to Access Gateway Appliance

Feature	3.1 Access Gateway Appliance	Access Gateway Appliance	Access Gateway Service
Chunk response behavior	Linux Access Gateway collects the complete chunk response and sends response with the Content-Length header to the client.	Access Gateway forwards the chunked response as it is to the client.	Similar to Access Gateway Appliance
Search and replace	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are not replaced.	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are replaced.	If you are doing a search and replace of for example, abc with xyz. and if in the page abc is prefixed with characters like <, >, and &, they are replaced.
PostParking Size Limit	The size limit is 50 KB. NOTE: With 3.1.5 the PostParking Size limit is increased to 64 KB.	The size limit is 64 KB.	The size limit is 64KB.
Adapter List Options	Supported	Not Supported	Not supported
Allows to change the speed, duplex, and NAT behavior.			

C Installing Packages and Dependent RPMs on RHEL for Access Manager

The following table lists RHEL packages and their dependent RPMs required for each component.

NOTE: To avoid RPM dependency issues, NetIQ Corporation recommends installing the package along with its respective dependent RPMs.

You must install these RPMs in the same sequence as they appear in the table:

Package	Dependent RPM
iManager	
glibc-2.12-1.107.el6.i686.rpm	♦ nss-softokn-freebl-3.12.9-11.el6.i686.rpm
compat-libstdc++-33-3.2.3-69.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm ♦ libgcc-4.4.7-3.el6.i686.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm ♦ libgcc-4.4.7-3.el6.x86_64.r
libstdc++-4.4.7-3.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm ♦ libgcc-4.4.7-3.el6.i686.rpm
These RPMs are required for the Administration Console also.	
libstdc++-4.4.7-3.el6.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm ♦ libgcc-4.4.7-3.el6.x86_64.rpm
(Part of the RHEL base installation)	
libXau-1.0.6-4.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm
libxcb-1.8.1-1.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm ♦ libXau-1.0.6-4.el6.i686.rpm
libX11-1.5.0-4.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm ♦ libXau-1.0.6-4.el6.i686.rpm
libXext-1.3.1-2.el6.i686.rpm	♦ libX11-1.5.0-4.el6.i686.rpm ♦ glibc-2.12-1.107.el6.i686.rpm
libXi-1.6.1-3.el6.i686.rpm	♦ libX11-1.5.0-4.el6.i686.rpm ♦ libXext-1.3.1-2.el6.i686.rpm ♦ glibc-2.12-1.107.el6.i686.rpm

Package	Dependent RPM
libXtst-1.2.1-2.el6.i686.rpm	<ul style="list-style-type: none"> ♦ libX11-1.5.0-4.el6.i686.rpm ♦ libXext-1.3.1-2.el6.i686.rpm ♦ libXi-1.6.1-3.el6.i686.rpm ♦ glibc-2.12-1.107.el6.i686.rpm
Administration Console	
glibc-2.12-1.107.el6.i686.rpm	♦ nss-softokn-freebl-3.12.9-11.el6.i686.rpm
libstdc++-4.4.7-3.el6.i686.rpm	<ul style="list-style-type: none"> ♦ glibc-2.12-1.107.el6.i686.rpm ♦ libgcc-4.4.7-3.el6.i686.rpm
ncurses-libs-5.7-3.20090208.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm
libgcc-4.4.7-3.el6.i686.rpm	♦ No dependency
Identity Server	
glibc-2.12-1.107.el6.i686.rpm	♦ nss-softokn-freebl-3.12.9-11.el6.i686.rpm
libstdc++-4.4.7-3.el6.i686.rpm	<ul style="list-style-type: none"> ♦ glibc-2.12-1.107.el6.i686.rpm ♦ libgcc-4.4.7-3.el6.i686.rpm
ncurses-libs-5.7-3.20090208.el6.i686.rpm	♦ glibc-2.12-1.107.el6.i686.rpm
libgcc-4.4.7-3.el6.i686.rpm	♦ No dependency
Access Gateway	
glibc-2.12-1.107.el6.i686.rpm	♦ nss-softokn-freebl-3.12.9-11.el6.i686.rpm
db4-4.7.25-17.el6.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm
(Part of the RHEL base installation)	
apr-1.3.9-5.el6_2.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm
apr-util-1.3.9-3.el6_0.1.x86_64.rpm	<ul style="list-style-type: none"> ♦ apr-1.3.9-5.el6_2.x86_64.rpm ♦ glibc-2.12-1.107.el6.x86_64.rpm
libtool-ltdl-2.2.6-15.5.el6.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm
unixODBC-2.2.14-12.el6_3.x86_64.rpm	<ul style="list-style-type: none"> ♦ libtool-ltdl-2.2.6-15.5.el6.x86_64.rpm ♦ glibc-2.12-1.107.el6.x86_64.rpm
libesmtplib-1.0.4-15.el6.x86_64.rpm	♦ glibc-2.12-1.107.el6.x86_64.rpm

Use the following command to verify whether a package is installed on RHEL:

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

Use the following command to install a RPM:

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

Use the following command to install all RPMs together:

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

NOTE: The version of RPMs varies based on the base operating system version of RHEL.

Perform the following steps to install packages and their dependent RPMs while installing RHEL:

- 1 Mount the RHEL 6.X CD-ROM by running the following command and go to the `Packages` folder.:

```
mount /dev/cdrom /mnt
```

NOTE: If the RHEL CD-ROM is auto mounted, the mount path will be `/media/RHEL_6.x x86_64 Disc 1`. Unmount the default mount path by using the `umount /media/RHEL_6.x\ x86_64\ Disc\ 1/` command and then mount the RHEL CD-ROM by using `mount /dev/cdrom /mnt`.

- 2 If you have a locally mounted ISO image, you can install RPMs for Access Manager by providing the mount path to the installer. The `install.sh` scripts prompts for the mounted disc if it identifies that the required RPMs are not installed. Provide the mount path to the installer with an ending `/`. For example, `/mnt/`.

NOTE: Installer will install only RPMs required for Access Manager components. You need to install iManager RPMs separately.

Install RPMs for SNMP after installing RPMs for the Administration Console. See [“RHEL Packages and Their Dependent RPMs for SNMP” on page 121](#).

You must install RPMs in the same sequence as these appear in the table.

RHEL Packages and Their Dependent RPMs for SNMP

The RHEL base installation does not install the `net-snmp` package by default. Install the following packages manually to make the `net-snmp` service (Master Agent) functional:

- ♦ `net-snmp-libs-5.5-44.el6.x86_64.rpm`
- ♦ `net-snmp-5.5-44.el6.x86_64`

Use the following procedure to install these packages to avoid any dependency issue:

- 1 Mount the RHEL 6.x CD-ROM by running the following command:

```
mount /dev/cdrom /mnt
```

- 2 Run the following commands:

```
yum install --nogpgcheck net-snmp-libs-5.5-44.el6.x86_64.rpm
```

```
yum install --nogpgcheck net-snmp-5.5-44.el6.x86_64
```

- 3 After installation, run `/etc/init.d/novell-snmpd start`. This will succeed for a successful installation.

