Access Manager
Security Guide

February 2017

NetIQ

Legal Notice

Contents

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
Website:	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
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ webs site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version 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

NetIQ Communities, 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, NetIQ Communities 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 *Security Guide* is intended to help Access Manager administrators, designers, and implementers with several configuration guidelines. These guidelines can be used for enhancing the security of an Access Manager environment. The first half of the guide focuses on tasks for configuring the Access Manager components along with examples and references. The remaining part of the guide provides additional information about the important concepts described in prior sections.

It is recommended that the administrators frequently consult the product documentation (listed in “Other Information in the Library”), Access Manager TIDS, Cool Solutions, and keep up to date on patches and versions of both Access Manager and the host operating system.

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 4.3 Administration Guide
- NetIQ Access Manager 4.3 Best Practices Guide
- NetIQ Access Manager 4.3 Installation and Upgrade Guide
- NetIQ Access Manager 4.3 Developer Guide
- Access Manager Mobile Users Quick Start

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

---

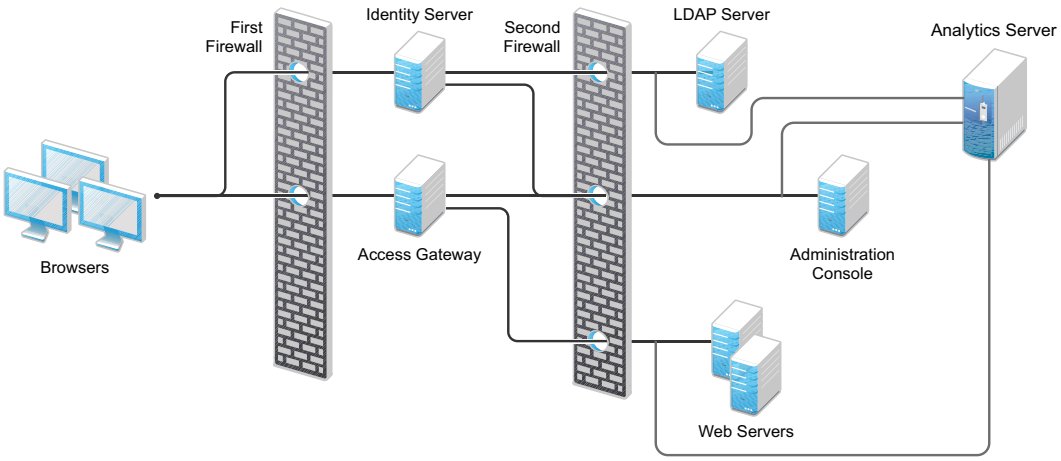
1 Deployment Considerations

This section includes the following topics:

1.1 Protecting Access Manager through Firewall

Access Manager should be used with firewalls. Figure 1-1 illustrates a simple firewall setup for a basic Access Manager configuration of Identity Server, Access Gateway, Analytics Server, and Administration Console.

Figure 1-1 *Access Manager Components between Firewalls*



1.1.1 Access Gateway and Identity Server in DMZ

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 Access Gateway and Identity Server and Identity Server can communicate with other identity providers.

For information about ports required to open in the first firewall, see “First Firewall ” in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

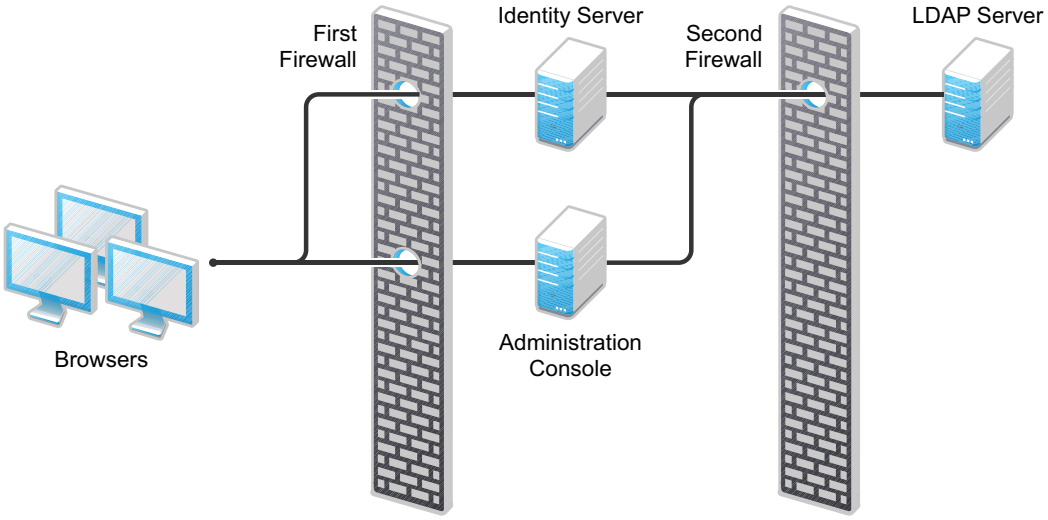
Second Firewall: The second firewall separates web servers, LDAP servers, Analytics Server, and Administration Console from Identity Server and Access Gateway.

For information about ports required to open in the second firewall, see “Second Firewall” in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

1.1.2 A Firewall Separating Access Manager Components from LDAP Servers

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

Figure 1-2 *A Firewall Separating Administration Console and the LDAP Server*



In this configuration, you need to open the required ports in the second firewall for Administration Console and Identity Server.

For information about all required ports, see “Required Ports” in the NetIQ Access Manager 4.3 Installation and Upgrade Guide.

1.2 Protecting Access Manager Setup behind NAT

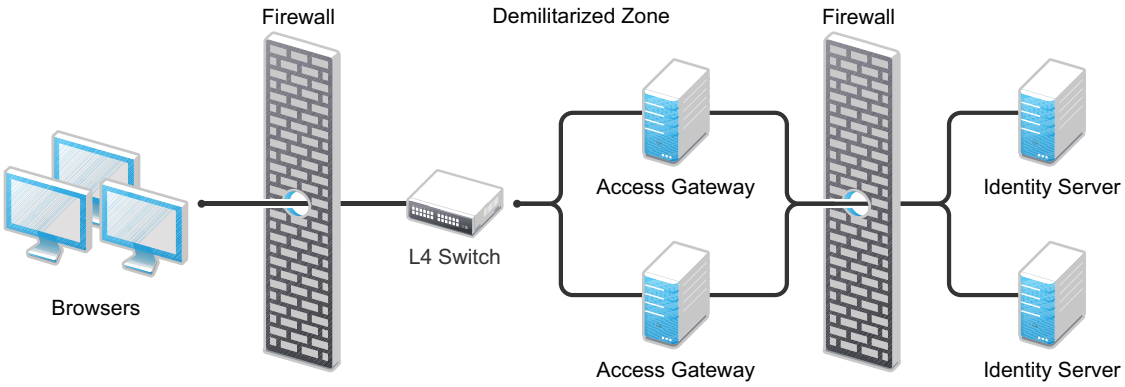
You can configure Access Manager by using Network Address Translation (NAT) to enable the communication between Administration Console from local network to other Access Manager devices such as Identity Server and Access Gateway. The devices can be in the external network or in another private network.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

For information about how to configure Access Manager behind NAT, see Installing Access Manager Components in NAT Environments.

1.3 Protecting Identity Server behind Access Gateway

You can configure Access Manager to protect Identity Server behind Access Gateway. This configuration reduces the number of ports you need to open between the outside world and your network. The following illustrates such a configuration.

Figure 1-3 *Identity Servers behind an Access Gateway*



With this configuration, you need an L4 switch to cluster Access Gateways. However, you do not need an L4 switch to cluster Identity Servers. When Identity Server is configured to be a protected resource of Access Gateway, Access Gateway uses its web server communication channel. Each Identity Server in the cluster must be added to the web server list, and Access Gateway uses its web server load balancing and failover policies for the clustered Identity Servers.

Limitations: The following features are not supported with this configuration:

- Identity Server cannot respond to identity provider introductions.
- Federation to an external service provider that requires the artifact profile with SOAP/Mutual SSL binding cannot be supported with this configuration.
- The proxy service that is protecting Identity Server cannot be configured to use mutual SSL. For example, X.509 authentication cannot be used for any proxy service. To perform X.509 authentication (which is a form of mutual SSL), a user's browser must have direct access to Identity Server.
- The proxy service that is protecting Identity Server cannot be configured to use NMAS.

For configuration details, see Configuring a Protected Identity Server Through Access Gateways in the NetIQ Access Manager 4.3 Administration Guide.

1.4 Configuring Identity Server to Listen on Port 443

Identity Server by default listens on port 8443. It requires port 8443 to be opened in firewall for the communication between a browser and Identity Server. To avoid opening 8443 port in firewall, you can configure Identity Server to listen on standard port 443.

1.4.1 Configuring Identity Server on Windows to Listen on Port 443

1. In Administration Console, click **Devices** > **Identity Server > Edit**, and configure the base URL with HTTPS as the protocol, and the TCP port as 443.
2. Click **OK**, then update Identity Server.
3. In a terminal window, open the `server.xml` file.

   Windows Server 2012 R2: `\Program Files (x86)\Novell\Tomcat\conf`

4 Change the ports from 8080 and 8443 to 80 and 443 respectively.

5 Restart the Tomcat service.

1.4.2 Configuring Identity Server on Linux to Listen on Port 443

On Linux, the Identity Server service (hosted on Tomcat) runs as a non-privileged user and cannot bind to ports below 1024. To allow requests to port 80/443 while Tomcat is listening on 8080/8443, the preferred approach is to use iptables to perform a port translation. Port translation allows the base URL of Identity Server to be configured for port 443 and to listen on this port. iptables translates it to port 8443 when communicating with Tomcat.

The following are two of many possible solutions:

- **Simple iptable Script:** If you have disabled the SUSE Linux Enterprise Server (SLES) firewall and do not have any other Access Manager components installed on the Identity Server machine, you can use a simple iptables script to translate the ports. See "A Simple Redirect Script " in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.
- If you have configured the SLES firewall or have installed other Access Manager components on Identity Server, you use a custom rule script that allows for multiple port translations. See "Configuring iptables for Multiple Components" in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

2 Securing Administration Console

Administration Console contains configuration information for all Access Manager components. If you federate your users with other servers, it stores configuration information about these users. You need to protect Administration Console so that unauthorized users cannot change configuration settings or gain access to the information in the configuration store.

When you develop a security plan for Access Manager, consider the following considerations:

2.1 Restricting Administration Console Access to only Private Network

Sometimes you may need to install Administration Console with multiple IP address. For example, when you install Administration Console and Identity Server on the same machine. Identity Server must be accessible and the services provided by Access Manager must be available on the Internet. This might cause a security issue with Administration Console.

Perform the following steps to secure Administration Console in this scenario:

1. Open the `server.xml` file.

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

   Windows: `\Program Files (x86)\Novell\Tomcat\conf`

2. Add the following lines before the end of the </Host> block:

```
<Context path="/nps">
           <Valve className="org.apache.catalina.valves.RemoteAddrValve"
           allow="xxx.yyy.zzz.www"/>
        </Context>
```

3. The syntax for the allow directive, which can also be changed to a deny directive, is a comma-separated IP regular expressions list (Perl regex format). A simple example is as follows:

   ```
   allow="192.168.10[1-3].[0-9]*"
   ```

   This allows you to access Administration Console following IP addresses:

   192.168.101.0/24, 192.168.102.0/24, 192.168.103.0/24.

   If you write the syntax as follows:

`deny=="192.168.10[1-3].[0-9]*"`

then Administration Console access is blocked from the following IP address:

192.168.101.0/24, 192.168.102.0/24,192.168.103.0/24

2.2 Managing Administration Console Session Timeout

The default Administration Console session timeout value is 30 minutes. You can modify this value for a longer or a shorter period based on your security needs in the `web.xml` file.

1. Change to the Tomcat configuration directory:

   Linux: `/opt/novell/nam/adminconsole/conf/web.xml`

   Windows Server 2012: `\Program Files (x86)\Novell\Tomcat\conf`
2. Open the `web.xml` file in a text editor and search for the `<session-timeout>` parameter.
3. Modify the value and save the file.
4. Restart Tomcat:

   Linux: `/etc/init.d/novell-ac restart` OR `rcnovell-ac restart`

   Windows: `net stop Tomcat7`

   `net start Tomcat7`

2.3 Securing iManager Login Settings

The default settings of Administration Console login by using iManager are changed in Access Manager 4.1 to ensure higher security. If you upgrade Access Manager from a previous version, you need to manually change the default iManager settings.

To change the default settings in Administration Console, perform the following steps:

1. Click **Administration Console** > **Configure** > **iManager Server** > **Configure iManager** > **Authentication**.
2. Make the following changes:
   - Deselect **Remember login credentials (except password)**.
   - Select **Hide specific reason for login failure**.

2.4 Securing Administrator Accounts

The admin user you create while installing Administration Console has all rights to Access Manager components. We recommend that you secure this account through the following configuration:

- **Password Restrictions:** When the admin user is created, no password restrictions are set. To ensure that the password meets your minimum security requirements, configure the standard eDirectory password restrictions for this account. In Administration Console, select the **Roles and Tasks** view in the iManager header, then click **Users**. Browse to the admin user (found in the novell container), then click **Restrictions**.

- **Intruder Detection:** The admin user is created in the novell container. You should set up an intruder detection policy for this container. In Administration Console, select the **Roles and Tasks** view in the iManager header, then click **Directory Administration** > **Modify Object**. Select **novell,** then click **OK**. Click **Intruder Detection**.
- **Backup Admin User Creation:** Only one admin user is created when you install Access Manager. If you forget the username or password, you cannot access Administration Console. It is recommended that you create a backup user who has the required privileges of an admin user. For more information, see "Creating Multiple Admin Accounts" in the *NetIQ Access Manager 4.3 Administration Guide*.

2.5 Security Measures for Delegated Administrators

Delegated administrators for policy containers have sufficient rights to implement a cross-site scripting attack using the Deny Message in an Access Gateway Authorization policy.

They can also access the configuration datastore with an LDAP browser. Modifications done with an LDAP browser are not logged by Access Manager.

To keep a track of delegated administrators activities, you can configure eDirectory to audit the events that come from LDAP connections to the LDAP server.

For information about how to activate eDirectory auditing for LDAP events, see "Activating eDirectory Auditing for LDAP Events" in the *NetIQ Access Manager 4.3 Administration Guide*.

2.6 Protecting the Configuration Store

The configuration store is an embedded, modified version of eDirectory. It is backed up and restored with command line options, which back up and restore the Access Manager configuration objects in the ou=accessManagerContainer.o=novell object.

You should back up the configuration store on a regular schedule, and store the ZIP file created in a secure place. See "Back Up and Restore" in the *NetIQ Access Manager 4.3 Administration Guide*.

In addition to backing up the configuration store, you should also install at least two Administration Consoles (a primary and a secondary). If the primary console goes down, the secondary console can keep the communication channels open between the various components. You can install up to three Administration Consoles. See "Installing Secondary Versions of Administration Console" in the *NetIQ Access Manager 4.3 Administration Guide*.

It is not recommended to use the configuration store as a user store.

2.7 Running the DHost HTTP Server on localhost

The DHost HTTP server running on HTTP port 8028 and HTTPS port 8030 does not set the X-Frame-Options HTTP Response Header. Therefore, it is prone to clickjacking attacks. To prevent the vulnerabilities, it is recommended to restrict the DHost HTTP Server to localhost.

Perform the following steps to configure the DHost server to run on localhost:

1. In Administration Console, open `/etc/opt/novell/eDirectory/conf/nds.conf`.
2. Search for the following lines and then replace the IP address (for example, 10.0.0.1) with 127.0.0.1.

   ```
   http.server.interfaces=10.0.0.1@8028
   ```

```
https.server.interfaces=10.0.0.1@8030
```

3 After the change these lines will look as follows:

```
http.server.interfaces=127.0.0.1@8028

https.server.interfaces=127.0.0.1@8030
```

4 Restart the eDirectory services:

```
/etc/init.d/ndsd restart
```

2.8 Default Security Settings in Configuration Files

2.8.1 server.xml

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

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

These settings are configured in `NIDP_Name="devman"` and `NIDP_Name="connector"` attributes inside the `Connector` element.

```
<Connector NIDP_Name="connector" SSLEnabled="true" URIEncoding="utf-8
"acceptCount="100" address="10.0.0.0"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" keystoreFile="/opt/novell/
devman/jcc/certs/idp/connector.keystore" keystorePass="xxxxxxxxxxxxxxx"
maxThreads="200" minSpareThreads="5" port="8443" scheme="https" secure="true"
sslImplementationName="com.example.nidp.common.util.net.server.NIDPSSLImplementati
on" useServerCipherSuitesOrder="true" sslProtocol="TLSv1.2"
sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2" />
```

For more information about connector attributes, see Apache Tomcat Configuration Reference.

2.8.2 web.xml

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

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

```
<filter>

   <filter-name>
      httpHeaderSecurity
   </filter-name>

   <filter-class>
      org.apache.catalina.filters.HttpHeaderSecurityFilter
   </filter-class>

   <async-supported>
      true
   </async-supported>

   <init-param>
      <param-name>hstsMaxAgeSeconds</param-name>
      <param-value>31536000</param-value>
   </init-param>

   <init-param>
      <param-name>antiClickJackingOption</param-name>
      <param-value>SAMEORIGIN</param-value>
   </init-param>

</filter>
<filter-mapping>
   <filter-name>httpHeaderSecurity</filter-name>
   <url-pattern>/*</url-pattern>
   <dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

NOTE: You can add these filters at any location in the `web.xml` as long as it is not within any existing tag.

2.8.3 tomcat7.conf

Linux:

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

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

JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.rejectClientInitiatedRenegotiation=true"

JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.ephemeralDHKeySize=2048"
```

Windows:

Navigate to `C:\Program Files (x86)\Novell\Tomcat\bin` and then double-click `tomcat7w`.

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

-Djdk.tls.rejectClientInitiatedRenegotiation=true"

-Djdk.tls.ephemeralDHKeySize=2048"
```

3 Securing Identity Server

This section includes the following topics:

3.1 Disabling Unused Authentication Protocols

You must disable any authentication protocol that is not in use. Enabling additional protocols increases the attack surface area.

Go to **Devices** > **Identity Servers** > **Edit** and ensure that you deselect any unused protocol from the list under **Enabled Protocols**.

3.2 Securing Authentication by Using Strong and Multi-Factor Authentication Methods

One of the strengths of Access Manager is its wide range of support for various means of authentication that goes well beyond simple and commonly used username/password methods including multi-factor and step-up scenarios. Access Manager includes many built-in preconfigured schemes via the combination of classes, methods, and contracts that can be used as is or can be configured to meet your needs. You can assign a contract directly to specific protected resources or federation partners. For more sophisticated security needs, the contract can also be dynamically chosen governed by Access Manager risk policies. Risk policies can allow access, ask for step-up authentication, or deny access based on the risk calculated at the time of the access request.

For more information about the Access Managers risk-based authentication feature, see “Risk-based Authentication” in the *NetIQ Access Manager 4.3 Administration Guide*.

The authentication contract, either assigned directly or determined by risk policies, can come from a variety of sources. Many are included with Access Manager itself. An example of the third-party provider is RADIUS. If you need advance security or you want to focus on both security and mobile users convenience, a variety of single and multi-factor contracts of the Advanced Authentication solution integrated with Access Manager is an ideal option.

For more information configuring the authentication methods, see "Configuring Authentication" in the *NetIQ Access Manager 4.3 Administration Guide*.

For more information about extending the authentication mechanisms, see "Identity Server Authentication API" in the *NetIQ Access Manager 4.3 Developer Guide*.

NOTE: You must not use persistent authentication or social authentication for applications that require high security. If you are using persistent authentication, you should associate the persistent cookie with the client IP address.

For securing the cookies to prevent session replay attacks, enable Advanced session Assurance. For more information, see "Setting Up Advanced Session Assurance" in the *NetIQ Access Manager 4.3 Administration Guide*.

Authentication Contracts

If you have set up Access Manager to require SSL connections among all of its components, delete the Name/Password - Form and the Name/Password - Basic contracts. Deleting the contracts removes them from the list of available contracts to be assigned to protected resources If these contracts are assigned, the user's password can be sent across the wire in the clear text format. If your system needs this type of contract, you can re-create it from the method. To delete these contracts, go to Administration Console and click **Identity Servers > Servers > Edit > Local > Contracts**.

If you are using password-based authentication, you can make it more secure by using second-factor authentication methods such as TOTP method or Advanced authentication methods in the contract.

You can configure advanced authentication by using the Access Manager Advanced Authentication plug-in. The following are supported authentication methods:

- Email Method
- Emergency Password Method
- FIDO U2F Method
- HOTP Method
- Password (PIN) Method
- RADIUS Method
- Security Questions Method
- Smartcard Method Support
- Smartphone Method
- SMS Method
- TOTP Method
- Voice Call Method

For more information about this authentication framework, see the product page and the Advanced Authentication Documentation.

3.3 Configuring SSL Communication between Browsers and Identity Server

See Section 7.1.2, “Enabling SSL between Browsers and Identity Server,” on page 48.

3.4 Configuring SSL Communication with Identity Server and a Service Provider

See Section 7.1.3, “Enabling SSL between Identity Server and a Service Provider,” on page 49.

3.5 Securing Federation

You can secure your federation relationships in numerous ways. The methods available are defined within federation protocols themselves. The method you want to use must be agreed upon by both members of a federation relationship. Specifically, this agreement is required between the identity provider (most often Access Manager’s role) and the service provider (for example, a SaaS service).

The most commonly used means of security includes using HTTPS for communication between parties secured by well-known CA certificates. For information about how to enable HTTPS in Access Manager Identity Server, see Section 7.1.3, “Enabling SSL between Identity Server and a Service Provider,” on page 49.

Another way for SAML is the signing and/or encryption of assertions. For more information, see Section 3.5.2, “Configuring the Encryption Method for the SAML Assertion,” on page 24.

SAML also has options for communicating the assertion data between parties known as protocol bindings. Protocol bindings include Post and Artifact. The Post binding is currently simplest and most popular among SaaS vendors and is typically secured using HTTPS, assertion signing, and encryption. The Artifact binding is considered more secure, but its level of security is not always required for a federation relationship.

Post method versus exchange artifacts: When you set up a federation between an identity provider and a service provider, you can select either to exchange assertions with a post method or to exchange artifacts.

An assertion in a post method might contain the user’s password or other sensitive data, which can make it less secure than an artifact when the assertion is sent to the browser. It is possible for a virus on the browser machine to access the memory where the browser decrypts the assertion.

An artifact is a randomly generated ID, it contains no sensitive data, and only the intended receiver can use it to retrieve assertion data.

If both providers support artifacts, you should select this method because it is more secure. For more details, see the **Response protocol binding** option in “Configuring a SAML 2.0 Authentication Request” and “Configuring A SAML 2.0 Authentication Response” in the *NetIQ Access Manager 4.3 Administration Guide*.

NOTE: To use exchange artifact, the service provider needs to establish a direct communication channel with the identity provider.

Additional SAML protocol options may also need to be configured and matched between the identity provider and service provider. Common options are covered later in this section.

3.5.1 Setting Options

Go to Identity Servers > Servers > Edit > SAML 2.0 > Service Provider > Options and set up the following options:

- **SAML2 SIGN METHODDIGEST SHA256:** Select true. Assertions will use the SHA 256 algorithm as a hashing algorithm for the service provider.
- **SAML2 POST SIGN RESPONSE TRUSTEDPROVIDERS:** Select true. The identity provider will sign the entire SAML 2.0 response for the service provider.
- **SAML2 AVOID AUDIENCE RESTRICTION:** Select true to avoid sending the audience restriction information with assertion to this service provider.
- **IS SAML2 POST SIGN RESPONSE:** Select true to enable the identity provider to send signed SAML 2.0 post responses to all its trusted providers.

NOTE: Configuring `IS SAML2 POST SIGN RESPONSE` is same as configuring the SignPost in `web.xml`. However, configuring it through Administration Console is recommended because it provides more options. You can combine these options with `IS SAML2 POST SIGN RESPONSE` to avoid Access Manager restarts.

3.5.2 Configuring the Encryption Method for the SAML Assertion

By default, AES128 (Advanced Standard Encryption, 128-bit) is used to encrypt SAML assertions. If you require a different encryption method, such as TDES (Triple Data Encryption Algorithm) or AES256 (Advanced Standard Encryption, 256-bit), you can modify the Tomcat `web.xml` file and specify your required method. To use PKCS 2.0 (RSA-OAEP) for encryption, see TID.

1. Open the `web.xml` file.

   Linux: `/opt/novell/nam/idp/webapps/nidp/WEB-INF/`

   Windows Server 2012: `\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF/`

2. Add the following lines to the file:

   ```
   <context-param>
           <param-name>EncryptionMethod</param-name>
           <param-value>TDES</param-value>
   </context-param>
   ```

   You can set the `<param-value>` element to TDES, AES128, or AES256. Because AES128 is the default, specifying this value in the `web.xml` file does not change any behavior.

3. Save the file and copy it to each Identity Server in the cluster.
4. Restart Tomcat on each Identity Server in the cluster.

   Linux: Enter the following command:

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

   ```
   rcnovell-idp restart
   ```

   Windows: Enter the following commands:

   ```
   net stop Tomcat7
   ```

   ```
   net start Tomcat7
   ```

The following algorithms for encryption method are supported:

```
<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/
><md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/
><md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/
><md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep"/
><md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/
>
```

3.6 Configuring a Whitelist of Target URL

URL redirection, which many applications and services require, inherently brings in security risks. While redirecting, the request can be tampered to redirect users to an external, malicious site. To prevent such issues, you can configure a list of permissible domains. Redirection is allowed only to the configured domains.

3.6.1 Configuring a Global Whitelist of Target URL

1. Click **Devices** > **Identity Servers** > **Edit** > **Identity Providers**.
2. Under **Redirection White List**, click **New**.
3. Specify **Domain**.

   You can specify a domain name with an asterisk wildcard character (*) that represents the entire DNS subtree. For example, specifying `*.digitalairlines.com` as a domain will allow redirection to all children domain under `digitalairlines.com` including `digitalairlines.com`. The `WWW` prefix is not required. You can specify the `*` wildcard only at the lowest level of the subtree.

   For example:

   Valid domain name: `*.digitalairlines.com`

   Invalid domain name: `innerweb.*.com`You must configure at least one domain to prevent open redirection.

   Liberty: The target parameter is filtered. If the requested target is not the white list, the Identity Server does not login.

   WS-Fed: The wreply parameter is filtered. If the requested wreply is not in the white list, the Identity Server does not login. However, if wreply is same as the provider's single logout or single sign-on URL domain, the request is accepted.

   SAML 2.0: For idpsend, the target parameter is filtered using this list. This list is not applicable for spsend.

3.6.2 Configuring a Whitelist of Intersite Transfer Service Target URL

1. Click **Devices** > **Identity Servers** > **Edit** > *[Liberty, SAML1.1, or SAML 2.0]* > *[Service Provider]* > **Intersite Transfer Service**.
2. In the **Domain List**, click **New**.

3 Specify the domain name.

The domain name must be a full domain name, such as `www.digitalairlines.com`. Wildcard domain names, such as `www.digitalairlines.*.com`, do not work.

3.6.3 Configuring a Whitelist of Assertion Consumer Service URL

When an authentication request from a service provider is not signed, Identity Server cannot validate the authenticity and integrity of the request. So, any intruder can intercept the request and change the Assertion Consumer Service URL in the request and make the Identity Server to send the assertion to malicious sites.

To secure and validate the authentication request from a service provider, you can use the following options in the service provider configuration of Identity Server:

- **SAML2_ACS_URL_RESTRICT:** This option ensures that Identity Server must validate the Assertion Consumer Service URL in the request against the trusted metadata URL before sending the assertion. If the Assertion Consumer URL in the authentication request is tampered by any malicious user, Identity Server terminates the request and assertion is not sent.
- **SAML2_ACS_DOMAIN_WHITELIST:** This option ensures that Identity Server must validate the Assertion Consumer URL in the request against a whitelist of domains. If the Assertion Consumer Service URL does not match with any of the domain URLs in the whitelist, Identity Server terminates the request.

  You must define the `SAML2_ACS_DOMAIN_WHITELIST` along with `SAML_ACS_URL_RESTRICT` for a service provider in Identity Server. `SAML2_ACS_DOMAIN_WHITELIST` does not work if `SAML_ACS_URL_RESTRICT` is not enabled.

To define these options, perform the following steps:

1 Click **Devices** > **Identity Servers** > <*Cluster*> > **Edit** > **SAML 2.0**.

2 Select the required service provider

3 Click **Options** > **New**.

4 Select **OTHER** and specify the following properties:

Property Name	Property Value	Description
SAML2_ACS_URL_RESTRICT	True	If true, Identity Server allows authentication only to the trusted ACS URLs.
SAML2_ACS_DOMAIN_WHITELIST	Domain names separated with semi-colon (;)	Identity Server performs additional validation of the authentication request with the ACS domain whitelist.

3.7 Blocking Access to Identity Server Pages

Identity Server has a couple of pages that authenticated users can access and which contain information about the user and Identity Server that can cause security issues.

For information about how to block user access to these pages, see “Blocking Access to the User Portal Page” and “Blocking Access to the WSDL Services Page” in the *NetIQ Access Manager 4.3 Administration Guide*.

3.8 Preventing the Error Page to Display the Tomcat Version

Accessing a non-existing page or providing wrong credentials on a protected page throws an HTTP 401 error with the Tomcat version. This issue happens on the Windows platform in the following scenarios:

- When Identity Server is the only component installed on the Windows server.
- Access Gateway Service is installed on Windows.

This issue does not happen on the Linux platform.

Perform the following steps to stop error pages to display the Tomcat version:

1. Go to `C:\Program Files\Novell\Tomcat\lib` and run `"C:\Program Files\Java\<jdk version>\bin\jar" -xf catalina.jar`
2. Move `catalina.jar` to another folder.
3. Go to `C:\Program Files\Novell\Tomcat\lib\org\apache\catalina\util` and edit the `serverInfo.properties` file:
   - **3a** Remove `Apache Tomcat/7.0.23` from the line `server.info=`.
   - **3b** Remove `7.0.23.0` from the line`server.number=`.
   - **3c** Remove `Nov 20 2011 07:36:25` from the line `server.built=`.
4. Go to `C:\Program Files\Novell\Tomcat\lib` and run `jar -cf catalina.jar META-INF org`.

3.9 Enabling Advanced Session Assurance

Advanced Session Assurance enables you to prevent session replay attacks by adding an additional layer of security to your sessions. When a session is established, Access Manager creates a unique fingerprint of the device from which the session is established. During the session, at a configurable time interval, Access Manager validates the session to ensure that the fingerprint matches with that the device it originated from.

By default, in a fresh installation, Advanced Session Assurance is enabled for all clusters.

However, in an upgraded setup, it is disabled by default. You must upgrade all nodes in the cluster to version 4.3 before enabling Advance Session Assurance.

For more information, see “Setting Up Advanced Session Assurance” in the *NetIQ Access Manager 4.3 Administration Guide*.

3.10 Securing Identity Server Web Service Interface

By default, the web service interface of Identity Server (`/nidp/services/IDSISCredentialProfile?wsdl`) is accessible by everyone. Identity Servers and Access Gateways use this interface for updating credential profile information. An attacker can use this information to bring Identity Server down.

You can prevent such issues by configuring the `WSInterfaceFilter` filter in `/opt/novell/nids/lib/webapp/WEB-INF/web.xml`. You can modify filter’s values depending on the requirement.

The following table lists parameters associated with the `WSInterfaceFilter` filter:

Parameter	Description
activateWSFFirewall	This activates the WSFFirewall filter. Specify `True` to activate the filter.
shieldAllServices	This specifies whether to shield all web services at `/nidp/services` or only selected services by using values `True` and `False` respectively.
wsfAcceptedDevicesIPList	This is a comma separated list of IP addresses that can access the `/nidp/services` interface. No white space is allowed.
wsURIList	This is a comma separated list of web services who can access to the web service when `shieldAllServices` is set to `False`. No whitespaces are allowed. For example, to filter requests for the `<host>/nidp/services/IDSISAuthenticationProfile` service, specify `IDSISAuthenticationProfile` as param-value for `wsURIList`. Both WSDL and the actual service will be placed behind the firewall.

NOTE: For certain web services, an administrator can also specify a policy from Administration Console. If a policy is defined for a service that is in the `wsURIList` list, the policy is executed after passing this filter.

3.11 Default Security Settings in Configuration Files

3.11.1 server.xml

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

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

These settings are configured in `NIDP_Name="devman"` and `NIDP_Name="connector"` attributes inside the `Connector` element.

```
<Connector NIDP_Name="connector" SSLEnabled="true" URIEncoding="utf-8"
acceptCount="100" address="10.0.0.0"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" keystoreFile="/opt/novell/
devman/jcc/certs/idp/connector.keystore" keystorePass="xxxxxxxxxxxxxxx"
maxThreads="600" minSpareThreads="5" port="8443" scheme="https" secure="true"
sslImplementationName="com.example.nidp.common.util.net.server.NIDPSSLImplementati
on" useServerCipherSuitesOrder="true" sslProtocol="TLSv1.2"
sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2" />
```

For information about connector attributes, see Apache Tomcat Configuration Reference.

3.11.2 web.xml

Linux: /opt/novell/nam/idp/webapps/nidp/WEB-INF/

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

```
<filter>
   <filter-name>
      httpHeaderSecurity
   </filter-name>
   <filter-class>
      org.apache.catalina.filters.HttpHeaderSecurityFilter
   </filter-class>
   <async-supported>
      true
   </async-supported>
   <init-param>
      <param-name>hstsMaxAgeSeconds</param-name>
      <param-value>31536000</param-value>
   </init-param>
   <init-param>
      <param-name>antiClickJackingOption</param-name>
      <param-value>SAMEORIGIN</param-value>
   </init-param>

</filter>
<filter-mapping>
   <filter-name>httpHeaderSecurity</filter-name>
   <url-pattern>/*</url-pattern>
   <dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

NOTE: You can add these filters at any location in the `web.xml` as long as it is not within any existing tag.

3.11.3 tomcat.conf

Linux:

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

```
JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=false"
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.rejectClientInitiatedRenegotiation=true"
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.ephemeralDHKeySize=2048"
```

Windows:

Navigate to `C:\Program Files (x86)\Novell\Tomcat\bin` and then double-click `tomcat7w`.

```
-Dsun.security.ssl.allowUnsafeRenegotiation=false"
-Djdk.tls.rejectClientInitiatedRenegotiation=true"
-Djdk.tls.ephemeralDHKeySize=2048"
```

4 Securing Access Gateway

This section includes the following topics:

4.1 Enabling SSL Communication between Access Gateway and Identity Server

See Section 7.3, “Configuring SSL for Authentication between Identity Server and Access Gateway,” on page 52.

4.2 Enabling Secure Cookies

Access Gateway and Embedded Service Provider (ESP) of Access Gateway both use session cookies in their communication with the browser. You must protect these session cookies to prevent from being intercepted by hackers.

NOTE: You can enable secure Access Gateway session cookies when only SSL resources exist. If a mix of HTTP and HTTPS proxy services exist, you cannot enable it as it is a global setting.

4.2.1 Securing the Embedded Service Provider Session Cookie

An attacker can spoof a non-secure browser into sending a JSESSION cookie that contains a valid user session. This might happen because Access Gateway communicates with its ESP on port 9009, which is a non-secure connection. Because ESP does not know whether Access Gateway is using SSL to communicate with the browsers, ESP does not mark the JSESSION cookie as secure when it creates the cookie. Access Gateway receives the Set-Cookie header from ESP and passes it to the

browser as a non-secure clear-text cookie. If an attacker spoofs the domain of Access Gateway, the browser sends the non-secure JSESSION cookie over a non-secure channel where the cookie might be sniffed.

To stop this, you must first configure Access Gateway to use SSL. See Section 7.2.1, “Enabling SSL between Browsers and Access Gateway,” on page 50.

After you have SSL configured, you must perform the following steps to configure Tomcat to secure the cookie:

1. On Access Gateway server, log in as an admin user.
2. Change to the Tomcat configuration directory.

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

   Windows: `/Program Files/Novell/Tomcat/conf`
3. In a text editor, open the `server.xml` file.
4. Search for the connector on port 9009.
5. Add the following parameter within the `Connector` element:

   ```
   secure="true"
   ```
6. Save the `server.xml` file.
7. Restart Tomcat.

4.2.2 Securing the Proxy Session Cookie

Proxy session cookies store authentication information and other information in the temporary memory that is shared between the browser and the proxy. These cookies are deleted when the browser is closed. However if these cookies are sent through a non-secure channel, hackers might intercept the cookies and impersonate a user on websites. you can use the following configuration options:

- Section 4.2.2.1, “Setting an Authentication Cookie with a Secure Keyword for HTTP,” on page 32
- Section 4.2.2.2, “Preventing Cross-Site Scripting Vulnerabilities,” on page 33

4.2.2.1 Setting an Authentication Cookie with a Secure Keyword for HTTP

You can configure Access Gateway to force the HTTP services to authenticate the cookie set with the keyword secure.

To enable this option, perform the following steps:

1. Click **Devices** > **Access Gateways** > **Edit** > **Reverse Proxy / Authentication**.
2. Select **Enable Secure Cookies.**

This option is used to secure the cookie when Access Gateway is placed behind an SSL accelerator, such as the Cisco SSL accelerator, and Access Gateway is configured to communicate by using only HTTP.

4.2.2.2 Preventing Cross-Site Scripting Vulnerabilities

Cross-site scripting vulnerabilities in web browsers allow malicious sites to grab cookies from a vulnerable site. Intruders might perform session fixation or impersonate the valid user. You can configure Access Gateway to set its authentication cookie with the `HttpOnly` keyword to prevent scripts from accessing the cookie.

To enable this option, perform the following steps:

1. Click **Devices** > **Access Gateways** > **Edit** > **Reverse Proxy / Authentication**.
2. Select **Force HTTP-Only Cookies**.

4.3 Disabling Phishing

You can configure Access Gateway ESP to disable the ESP phishing by implementing a context parameter in the `web.xml` file for ESP.

1. Open the `web.xml` file.

   Linux: `/opt/novell/nam/mag/webapps/nesp/WEB-INF/`

   Windows: `\Program Files\Novell\Tomcat\webapps\nesp\WEB-INF`
2. Add the following entry:

```
<context-param>
   <param-name>phishingCheck</param-name>
   <param-value>standard</param-value>
</context-param>
```

3. Restart Tomcat.

4.4 Disabling Weak Protocols between Access Gateway and Web Servers

See the overview of Strengthening TLS/SSL Settings for information about weak protocols.

To restrict Access Gateway to communicate with back end web servers only using TLS 1.1 and TLS 1.2 protocols, click **Devices > Access Gateways > Edit > Advanced Options** and add the following configuration:

```
SSLProxyProtocol TLSv1.1 +TLSv1.2
```

While setting the protocol, ensure that the web server supports the configured protocol. For example, if Access Manager supports TLS1.1, but the web server does not support that, the connection will fail.

For more information about SSLProxyProtocol directives, see SSLProxyProtocol Directive documentation.

4.5 Configuring Stronger Ciphers for SSL Communication between Access Gateway and Web Servers

See the overview of “Strengthening TLS/SSL Settings” on page 53 for information about strong ciphers.

Add or modify the advanced option as follows:

```
SSLProxyCipherSuite ECDHE-RSA-AES256-SHA384:AES256-
SHA256:RC4:HIGH:MEDIUM:!LOW:!EXP:!SSLv2:!aNULL:!EDH:!ECDH:!ECDSA:!AESGCM:!eNULL:!N
ULL
```

While setting the cipher suite, ensure that the web server supports the cipher suite. For example, if Access Manager supports ECDH ciphers, but the web server does not support that, the connection will fail.

4.6 Enabling Perfect Forward Secrecy

Apache simplifies the process with the SSLHonorCipherOrder directive. This directive indicates that Apache must respect the sequence of the encryption processes in SSLCipherSuite that is the first match found must be used. With the SSLCipherSuite list above and the `SSLHonorCipherOrder on` directive in place, PFS is enabled.

Set the following advanced options:

```
SSLHonorCipherOrder On
SSLCipherSuite
ECDH+AESGCM:ECDH+AES256:ECDH+AES128:ECDH+3DES:RSA+AESGCM:RSA+AES:!aNULL:!DES:!MD5:
!DSS
```

For information about Perfect Forward Secrecy (PFS) and prerequisites for enabling it, see Section 8.3, “Enabling Perfect Forward Secrecy,” on page 54.

4.7 Preventing Error Messages to Show the Failure Reason on Browsers

Whenever Identity Server reports a 500 internal error due to an invalid input, the reason for failure is included in the response and visible on the browser.

This might cause a security issue as intruders can use this information to attack against Identity Server and ESP.

Configure the `web.xml` file for ESP as follows:

Linux: `/opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml`

Windows: `/Program Files/Novell/Tomcat/webapps/nesp/WEB-INF/web.xml`

```
<welcome-file-list>
   <welcome-file>index.html</welcome-file>
</welcome-file-list>
<error-page>
   <error-code>500</error-code>
   <location>/index.html</location>
</error-page>
```

index.html can be any custom page. Same as above, you can configure `web.xml` for error-code 404 by adding one more `<error-page>` tag.

4.8 Enabling Advanced Session Assurance

Advanced Session Assurance enables you to prevent session replay attacks by adding an additional layer of security to your sessions. When a session is established, Access Manager creates a unique fingerprint of the device from which the session is established. During the session, at a configurable time interval, Access Manager validates the session to ensure that the fingerprint matches with that the device it originated from.

By default, in a fresh installation, Advanced Session Assurance is enabled for all clusters.

However, in an upgraded setup, it is disabled by default. You must upgrade all nodes in the cluster to version 4.3 before enabling Advance Session Assurance. You should enable Advanced Session Assurance on the need basis. See "Best Practices for Enabling Advanced Session Assurance at the Proxy Service Resource Level" in the *NetIQ Access Manager 4.3 Administration Guide*.

For more information about Advanced Session Assurance and how to enable it, see "Setting Up Advanced Session Assurance" in the *NetIQ Access Manager 4.3 Administration Guide*.

4.9 Configuring Tomcat to Run as a Non-Administrator User

On Windows Access Gateway Service, Tomcat runs with the administrator privileges. This may allow any attacker to gain access to the server. You must configure Tomcat to run as a non-administrator user.

Perform the following steps:

1. Create a `novlwww` user.
   - **1a** Open `services.msc`.
   - **1b** Stop the Tomcat service.
   - **1c** Before performing the next step, ensure that the 'novlwww' user is not already created.
   - **1d** Run the following command:

     ```
     C:\Windows\System32\sc.exe config tomcat8 obj= ".\novlwww" password=
     "novellIman@Sec1"
     ```

     NOTE: This is the password used to create the user. It is available in the `UserUtil.vbs` file.
   - **1e** Change the tomcat folder permissions by running the following command:

     ```
     C:\Windows\System32\icacls.exe  "C:\Program Files\Novell\Tomcat"  /Q /C /T
     /grant:r novlwww:(OI)(CI)F
     ```
   - **1f** Start the Tomcat service.

2 Assign permission to the `novlwww` user to start and stop Tomcat as an administrator.

2a In the command prompt, type `sc sdshow tomcat8`.

This results an output similar to the following:

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLC
SWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)
```

NOTE: It lists all permissions for each user and group on this system.

2b Get the SID of the `novlwww` user to grant novlwww the required permissions to start and stop Windows Services.

Go to Start > regedit > HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\. Select the key pertaining to novlwww and copy it.

2c Include the key in (A;;RPWPCR;;;<KEY_NAME>) and insert it in the output got in step 2a. It will look similar to the following:

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLC
SWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;S-1-5-21-2738286421-
3044359772-2946809952-1001)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

2d To grant the required permission to novlwww on Apache Service, copy the output in step 2c and run the following command:

```
sc sdset Apache2.2
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCL
CSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;S-1-5-21-2738286421-
3044359772-2946809952-1001)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

2e Go to **C:\Program Files** and set the write/modify permission to the Users group for the Novell directory (including all sub folders and files) by right-clicking **Novell** > **Properties** > **Security** > **Edit** > select **Write** and **Modify** permission > **Apply**.

4.10 Default Security Settings in Configuration Files

4.10.1 ESP web.xml

Linux: `/opt/novell/nam/mag/webapps/nesp/WEB-INF/`

Windows: `\Program Files\Novell\Tomcat\webapps\nesp\WEB-INF`

```
<context-param>
    <param-name>phishingCheck</param-name>
    <param-value>standard</param-value>
</context-param>

<welcome-file-list>
    <welcome-file>index.html</welcome-file>
</welcome-file-list>
```

```
<error-page>
    <error-code>500</error-code>
    <location>/index.html</location>
</error-page>

<filter>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter
    </filter-class>

<init-param>
    <param-name>antiClickJackingOption</param-name>
    <param-value>SAMEORIGIN</param-value>
</init-param>
</filter>

<filter-mapping>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

4.10.2 Access Gateway Advanced Options

`SSLProtocol TLSv1.1 +TLSv1.2`

`SSLCipherSuite !aNULL:!eNULL:!EXPORT:!DSS:!DES:!RC4:ALL:!EDH`

4.10.3 httpd.conf

Linux: `/etc/opt/novell/apache2/conf`

Windows: C:\Program Files\Novell\apache\conf

The mod_headers library is enabled.

Linux: `LoadModule headers_module libexec/mod_headers.so`

Windows: `LoadModule headers_module modules/mod_headers.so`

4.10.4 NovellAgSettings.conf

Linux: `/etc/opt/novell/apache2/conf`

Windows: C:\Program Files\Novell\apache\conf

The `header set` directive for the HSTS header is added at the bottom of the file:

Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

5 Securing Analytics Server

5.1 Customizing the Size of EDH Keys

For information about why to customize the EDH key size, see Section 8.6, “Customizing the Size of Ephemeral Diffie-Hellman Keys,” on page 55.

1. Open the `/opt/novell/nam/dashboard/conf/tomcat.conf` file.
2. Ensure that the following line exists:

```
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.ephemeralDHKeySize=2048"
```

5.2 Disabling SSL Renegotiations

You should disable SSL renegotiation as it is vulnerable to the man-in-the-middle attacks.

Perform the following steps to disable SSL renegotiations in Analytics Server:

1. Open the `/opt/novell/nam/dashboard/conf/tomcat.conf` file.
2. Ensure that the following lines exist:

```
JAVA_OPTS="${JAVA_OPTS} -Dsun.security.ssl.allowUnsafeRenegotiation=false"
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.rejectClientInitiatedRenegotiation=true"
```

5.3 Default Security Settings in Configuration Files

5.3.1 server.xml

Path: `/opt/novell/nam/dashboard/conf/server.xml`

```
<Connector NIDP_Name="connector" SSLEnabled="true" URIEncoding="utf-8"
acceptCount="100" ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_
WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_C
BC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" keystoreFile="/opt/novell/
devman/jcc/certs/ra/connector.keystore" keystorePass="xxxxxxxxxxxxxxx"
maxThreads="150" minSpareThreads="5" port="8445"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2" sslProtocol="TLSv1.2"/>
```

5.3.2 web.xml

Path: `/opt/novell/nam/dashboard/webapps/kibana/WEB-INF/web.xml`

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter
    </filter-class>
    <async-supported>true</async-supported>
</filter>

<init-param>
    <param-name>hstsMaxAgeSeconds</param-name>
    <param-value>31536000</param-value>
</init-param>

<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
</filter-mapping>

<filter>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter
    </filter-class>
    <init-param>
      <param-name>antiClickJackingOption</param-name>
      <param-value>SAMEORIGIN</param-value>
    </init-param>
</filter>

<filter-mapping>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

6 Hardening Appliance

6.1 Removing Unused Packages

In Access Gateway Appliance 4.2.2 and earlier, many packages that Access Gateway Appliance does not use were installed. Access Manager Update Channel does not provide new version updates for these packages. Hence, these package might be old and may contain potential vulnerability.

The following is the list of unused packages:

- Samba
- libMagicCore1
- netcat
- telnet
- rsh
- gdb
- gdbm
- finger
- gcc
- rpcbind
- rsync
- tcpdump

In a fresh Access Manager 4.3 and later install, these packages have been removed. However, if you are upgrading your Access Manager setup to 4.3, it is recommended to remove these packages manually.

NOTE: The following sections includes the version of packages used during testing. You may have packages of different versions on your system.

- Section 6.1.10, “Removing the rpcbind Packages,” on page 44
- Section 6.1.11, “Removing the rsync Packages,” on page 44
- Section 6.1.12, “Removing the tcpdump Packages,” on page 44

6.1.1 Removing the Samba Packages

1. Query for the samba packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i samba
   ```

   This lists all versions of all samba packages installed on the server.
2. Remove the packages by using the following commands:

   ```
   rpm -e samba-3.6.3
   rpm -e samba-winbind-3.6.3
   rpm -e samba-client-3.6.3
   rpm -e samba-winbind-32bit-3.6.3
   rpm -e samba-client-32bit-3.6.3
   rpm -e yast2-samba-server-2.18.0
   rpm -e yast2-samba-client-2.17.30
   ```

It is recommended to remove the packages in the same sequence (top to down) to avoid dependency issues.

6.1.2 Removing the libMagickCore1 Packages

1. Query for the libMagickCore1 packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i libMagickCore1
   ```
2. Run the following commands:

   ```
   rpm -e yast2-fingerprint-reader-2.17.7-0.1.201
   rpm -e libfprint0-0.0.6-18.22.136
   rpm -e libMagickCore1-6.4.3.6-7.30.1
   ```

It is recommended to remove the packages in the same sequence (top to down) to avoid dependency issues.

6.1.3 Removing the netcat Packages

1. Query for the netcat packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i netcat
   ```
2. Run the following command:

   ```
   rpm -e netcat-1.10
   ```

6.1.4 Removing the telnet Packages

1. Query for the telnet packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i telnet
   ```

2 Run the following commands:

```
rpm –e telnet-1.2
```

6.1.5 Removing the rsh Packages

1 Query for the rsh packages installed on the server by using the following command:

```
rpm -qa | grep -i rsh
```

2 Run the following command:

```
rpm –e rsh-0.17
```

6.1.6 Removing the gdb Packages

1 Query for the gdb packages installed on the server by using the following command:

```
rpm -qa | grep -i gdb
```

2 Run the following command:

```
rpm –e gdb-7.7
```

6.1.7 Removing the gdbm Packages

1 Query for the gdbm packages installed on the server by using the following command:

```
rpm -qa | grep -i gdbm
```

2 Run the following command:

```
rpm -e gdbm-1.8.3-374.25 --nodeps
```

NOTE: The gdbm packages has dependency on several other packages in the system. Before removing this package, ensure that it is not required.

6.1.8 Removing the finger Packages

1 Query for the finger packages installed on the server by using the following command:

```
rpm -qa | grep -i finger
```

2 Run the following command:

```
rpm -e finger-1.3-104.22
```

6.1.9 Removing the gcc Packages

1 Query for the finger packages installed on the server by using the following command:

```
rpm -qa | grep -i gcc
```

2 Run the following commands:

```
rpm -e gcc-32bit-4.3-62.200.2
rpm -e gcc43-32bit-4.3.4_20091019-0.37.30
rpm -e gcc-4.3-62.200.2
rpm -e gcc43-4.3.4_20091019-0.37.30
```

It is recommended to remove the packages in the same sequence (top to down) to avoid dependency issues.

6.1.10 Removing the rpcbind Packages

1. Query for the finger packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i rpcbind
   ```

2. Run the following commands:

   ```
   rpm -e ypbind-1.22-1.17.x86_64
   rpm -e nfs-client-1.2.3-18.38.43.1.x86_64
   rpm -e rpcbind-0.1.6+git20080930-6.20.1
   ```

It is recommended to remove the packages in the same sequence (top to down) to avoid dependency issues.

NOTE: The rpcbind packages has dependency on several other packages in the system. Before removing this package, ensure that it is not required.

6.1.11 Removing the rsync Packages

1. Query for the rsync packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i rsync
   ```

2. Run the following command:

   ```
   rpm -e rsync-3.0.4-2.47.28
   ```

6.1.12 Removing the tcpdump Packages

1. Query for the tcpdump packages installed on the server by using the following command:

   ```
   rpm -qa | grep -i tcpdump
   ```

2. Run the following command:

   ```
   rpm -e tcpdump-3.9.8-1.27.1
   ```

6.2 Reconfiguring Secure Shell Ciphers

In Access Manager 4.3 fresh install, the SSH server is configured only with strong ciphers. However, in an upgraded setup, you should reconfigure SSH to remove the weak ciphers.

Perform the following steps:

1. In `/etc/ssh/sshd_config` (server) and `/etc/ssh/ssh_config` (client), search for `Ciphers`. The following is the default configuration:

   ```
   # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-
   cbc,3des-cbc
   ```

2. Uncomment this line and replace it with the following value:

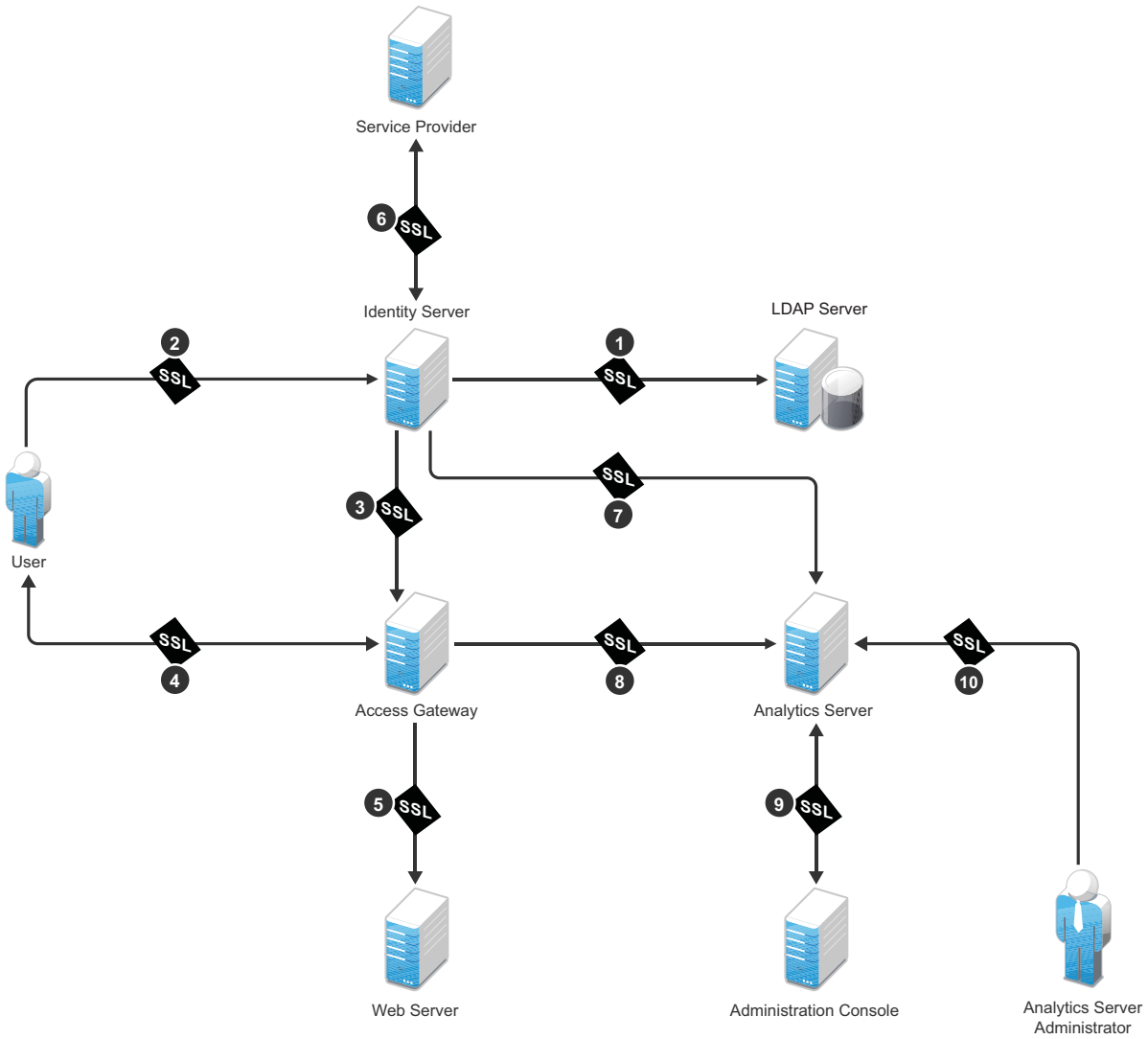
```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
```

3 Restart SSH by running the `service sshd restart` command.

7 Configuring Secure Communication

Access Manager has six communication channels that you can configure for SSL. The following diagram illustrates potential SSL Communication channels:

Figure 7-1 *SSL Communication Channels*



The first channel is set between Identity Server and LDAP servers when you configure user stores. The other channels are configured according to their numeric values. SSL must be configured between Identity Server and browsers before you configure the channel between Access Gateway and Identity Server for SSL.

This section discusses the following topics:

- Configuring SSL in Identity Server
- Configuring SSL in Access Gateway

- Configuring SSL for Authentication between Identity Server and Access Gateway
- Using Trusted Certificates Authority

7.1 Configuring SSL in Identity Server

An attacker can spoof a non-secure browser and send a JSESSION cookie that contains a valid user session. You can prevent this by configuring Identity Server to use a SSL channel for communications.

Topics include:

7.1.1 Configuring a SSL Channel between Identity Server and LDAP Servers

Channel 1 in Figure 7-1, “SSL Communication Channels,” on page 47.

You can set a SSL channel between Identity Server and LDAP servers while configuring user stores. Select the **Use secure LDAP connections** option to change the port from 389 to the secure LDAP port 636.

IMPORTANT: If you use port 389, usernames and passwords are sent in the clear text that is vulnerable to security issues.

To enable the **Use secure LDAP connections** option, perform the following steps:

1. Go to **Identity Servers** > **Servers** > **Edit** > **Local** > **User Stores**.
2. Click [name of the user store] > [name of the replica].
3. Select **Use secure LDAP connections**.

7.1.2 Enabling SSL between Browsers and Identity Server

Channel 2 in Figure 7-1, “SSL Communication Channels,” on page 47.

1. Click **Devices** > **Identity Servers** > **Edit**.
2. Change **Protocol** to HTTPS (the system changes the port to 8443).
3. In the **SSL Certificate** line, click the **Browse** icon > **Replace** and select the Identity Server certificate.
4. Restart Tomcat.

   If your Identity Server and Administration Console are on the same machine, log in to Administration Console again.
5. After the Identity Server health turns green, go to **Access Gateway** > **Edit** > **Service Provider Certificates** > **Trusted Roots**.
6. Click **Add** to select the trusted root certificate of the certificate authority that signed Identity Server certificate.

(Conditional) If you imported intermediate certificates for the CA, select them also.

IMPORTANT: If the external certificate authority writes the DN in reverse order (the cn element is displayed first), you receive an error message that the certificate names do not match. You can ignore this warning, if the order of the DN elements is the cause.

7 Update Access Gateway.

7.1.3 Enabling SSL between Identity Server and a Service Provider

Channel 6 in Figure 7-1, “SSL Communication Channels,” on page 47.

To make the communication between Identity Server and a service provider more secure, you must consider the following settings:

Identity Provider Signing Certificate: Select a certificate from the keystore and assign it to the service provider.

Identity Provider Encryption Certificate: Select a certificate from the keystore and assign it to the service provider.

Signing certificate per service provider: When you assign custom certificates to each service provider while configuring Identity Server, ensure that you export these certificates and custom metadata to the service provider. To retrieve the metadata, click on the metadata link (available in the note on the Trust page).

For more information, see “Configuring Communication Security for a SAML 2.0 Service Provider ” *NetIQ Access Manager 4.3 Administration Guide*.

NOTE: These security considerations are also valid when Identity Server acts as a service provider.

7.2 Configuring SSL in Access Gateway

You can configure Access Gateway to use SSL in its connections to Embedded Service Provider (ESP), browsers, and its web servers.

Enable SSL with ESP: To encrypt the data exchanged for authentication (a communication channel between Identity Server and Access Gateway). This option is available only for the reverse proxy that has been assigned to perform authentication.

If you enable SSL between browsers and Access Gateway, this option is automatically selected. You can enable SSL with the ESP without enabling SSL between Access Gateway and browsers. This allows the authentication and identity information that Access Gateway and Identity Server exchange to use a secure channel. However, it allows the data, that Access Gateways retrieves from the back-end web servers and sends to users, to use a non-secure channel. This saves processing overhead if the data on web servers is not sensitive.

Enable SSL between Browser and Access Gateway: To configure SSL connections between your clients and Access Gateway. SSL must be configured between browsers and Access Gateway before you can configure SSL between Access Gateway and web servers.

Redirect Requests from Non-Secure Port to Secure Port: To determine whether browsers are redirected to a secure port and allowed to establish an SSL connection. If this option is not selected, browsers that connect to the non-secure port are denied service.

This option is only available if you have selected **Enable SSL with Embedded Service Provider**.

For information about how to enable SSL between SSL with ESP and how to redirect requests from a non-secure port to a secure port, see Section 7.2.1, “Enabling SSL between Browsers and Access Gateway,” on page 50.

7.2.1 Enabling SSL between Browsers and Access Gateway

This section explains how to enable SSL communication between Access Gateway and browsers (channel 4 in Figure 7-1 on page 47).

1. In Administration Console, click **Devices** > **Access Gateways** > **Edit** > **[Name of Reverse Proxy]**.
2. Select the following options based on your requirement:
   - **Enable SSL with Embedded Service Provider**
   - **Enable SSL between Browser and Access Gateway**
   - **Redirect Requests from Non-Secure Port to Secure Port**
3. Select the certificate to use for SSL between Access Gateway and browsers.
4. (Conditional) If you selected a certificate in Step 3 that was created by an external CA, click **Auto-Import Embedded Service Provider Trusted Root**, and specify an alias name.

   This option imports the public key from ESP into the trust store of Identity Servers of the selected Identity Server configuration. This sets up a trusted SSL relationship between Identity Server and ESP.

   If you are using certificates signed by the Access Manager CA, the public key is automatically added to this trust store.
5. Configure the ports for SSL:

   Non-Secure Port: Indicates a specific port to listen to HTTP requests. The default port for HTTP is 80.

   - If you selected the **Redirect Requests from Non-Secure Port to Secure Port** option, requests sent to this port are redirected to the secure port. If the browser can establish an SSL connection, the session continues on the secure port. If the browser cannot establish an SSL connection, the session is terminated.
   - If you do not select the **Redirect Requests from Non-Secure Port to Secure Port** option, this port is not used when SSL is enabled.

   Secure Port: Indicates a specific port to listen to HTTPS requests (usually 443). This port needs to match the configuration for SSL. If SSL is enabled, this port is used for all communication with the browsers. The listening address and port combination must not match any combination you have configured for another reverse proxy or tunnel.
6. Click **OK** > **Reverse Proxy / Authentication**.
7. (Conditional) If you are using an externally signed certificate for Identity Server cluster, click **Auto-Import Identity Server Trusted Root** to import the public key of the CA.

7.2.2 Enabling SSL between Access Gateway and Web Servers

Channel 5 in Figure 7-1, “SSL Communication Channels,” on page 47.

SSL must be enabled between Access Gateway and browsers before you can enable it between Access Gateway and its web servers. See Section 7.2.1, “Enabling SSL between Browsers and Access Gateway,” on page 50.

1 Click **Devices** > **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **Web Servers**.

2 Select **Connect Using SSL**.

3 Configure how you want the proxy service to verify the web server certificate:

3a Select one of the following options in **Web Server Trusted Root**:

Do not verify: Use this option when you want the information between Access Gateway and the web server encrypted, but you do not need the added security of verifying the web server certificate.

Continue with Step 4.

Any in Reverse Proxy Trust Store: Use this option to verify the certificate authority of the web server certificate. When this option is selected, the public certificate of the certificate authority must be added to the proxy trust store.

IMPORTANT: For an Access Gateway Service, this is a global option. If you select this option for one proxy service, all proxy services on an Access Gateway Service are flagged to verify the public certificate. This verification is done even when other proxy services are set to **Do not verify**.

If the web server certificate is part of a chain of certificates, select **SSLProxyVerifyDepth** and specify how many certificates are in the chain.

The SSL connection between Access Gateway and a web server may fail if a self-signed certificate is used. To prevent this, import the web server certificates to the proxy trust store and then use the following advanced option:

Windows: `SSLProxyCACertificateFile "C:\Program Files\Novell\apache\cacerts\myserver.pem"`.

Linux: `SSLProxyCACertificateFile /opt/novell/apache2/cacerts/myserver.pem`. This is a service level advanced option.

3b Click **Manage Reverse Proxy Trust Store**.

3c Ensure that the IP address of the web server and the port match your web server configuration and then click **OK**.

If the whole chain is not displayed, import what is displayed. You then need to manually import the missing parents in the chain. A parent is missing if the chain does not include a certificate where the Subject and the Issuer have the same CN.

3d Specify an alias.

All the displayed certificates are added to the trust store.

4 (Optional) Set up mutual authentication so that the web server can verify the proxy service certificate. Click **Select Certificate** to select the certificate you created for the reverse proxy.

You need to import the trusted root certificate of the CA that signed the proxy service’s certificate to the web servers assigned to this proxy service. For instructions, see your Web server documentation.

5 In **Connect Port**, specify the port that your web server uses for SSL communication.

7.3 Configuring SSL for Authentication between Identity Server and Access Gateway

This section explains how to enable SSL communication between Access Gateway and Identity Server (channel 3 Figure 7-1, “SSL Communication Channels,” on page 47).

1. Click **Devices** > **Access Gateways** > **Edit** > **[Name of Reverse Proxy]**.
2. Select **Enable SSL with Embedded Service Provider** and **Enable SSL between Browser and Access Gateway**.
3. In the **Server Certificate** line, click the **Browse** icon to select the Access Gateway certificate.

   IMPORTANT: If the external certificate authority writes the DN in reverse order (the cn element comes first rather than last), you receive an error message that the subject name does not contain the cn of the device. You can ignore this warning, if the order of the DN elements is the cause.

4. Click **Auto-Import Embedded Service Provider Trusted Root**.

   This adds the trusted root of the Access Gateway certificate to the trusted root store of Identity Server.
5. Specify an **Alias** for the certificate.
6. On the Server Configuration page, click **Reverse Proxy / Authentication**.
7. In the **Embedded Service Provider** section, click **Auto-Import Identity Server Configuration Trusted Root** and follow the prompts.

   This imports the trusted root certificate of Identity Server into the trusted root store of the embedded service provider.
8. Update Access Gateway and Identity Server on respective pages.

7.4 Using Trusted Certificates Authority

When Identity Server is configured to use an SSL certificate that is signed externally, the trusted store of the embedded service provider for each component must be configured to trust this new CA. Browsers that are used to authenticate to Identity Server must be configured to trust the CA that created the certificate for Identity Server. Most browsers are already configured to trust certificates from well-known CAs.

To use certificates signed by an external CA, perform the following activities:

1. Obtain externally signed certificates.

   For more information, see “Obtaining Externally Signed Certificates” in the *NetIQ Access Manager 4.3 Administration Guide*.
2. Configure Identity Server to use externally signed certificates.

   For more information, see “Configuring Identity Server to Use an Externally Signed Certificate” in the *NetIQ Access Manager 4.3 Administration Guide*.
3. Configure Access Gateway to use externally signed certificates.

   For more information, see “Configuring Access Gateway to Use an Externally Signed Certificate” in the *NetIQ Access Manager 4.3 Administration Guide*.

8 Strengthening TLS/SSL Settings

Securing TLS/SSL settings have the following three aspects:

- **Protocol:** SSL v2, SSL v3, and TLS1.0 contain known vulnerabilities. Starting with JDK 8u31, SSL v3 has been deactivated and is not available by default. If SSLv3 is required, you can reactivate the protocol at the JRE level. For more information, see The SunJSSE Provider.

  By default, Access Manager 4.3 is configured with only TLS1.1 and TLS1.2.
- **Encryption:** In the encryption algorithms, you need to look at two aspects:
  - **Key Exchange Algorithm:** In these algorithms, DH is vulnerable. By default, Access Manager 4.3 includes only RSA, DHE, or ECDHE.
  - **Bulk Encryption Algorithm:** In these algorithms, cipher suites that contain NULL, DES, 3DES, and RC4 encryptions are vulnerable. By default, Access Manager 4.3 supports cypher suites only with AES.
- **Message Authentication Code (MAC) Algorithm:** In these algorithms, MD5 and SHA1 are vulnerable. By default, Access Manager 4.3 supports cypher suites only with SHA 256 or higher.

In Access Manager 4.3, security is strengthened. These security measures can impact performance. For example, DHE and ECDHE ciphers are more secure, but they need more computation and therefore impacts performance. Between DHE and ECDHE, ECDHE reduces some computational cost comparatively and in turn it is better than DHE ciphers in terms of performance. You can configure the cipher optimally based on your security and performance requirements by referring to The Sun JSSE Provider.

If you want to restore the previous security settings, see Chapter 12, “Restoring Previous Security Level After Upgrading Access Manager,” on page 63.The

This section discusses the following topics:

8.1 Disabling SSLv2 and SSLv3 Protocols

In Access Manager 4.3, SSL v2 and SSL v3 protocols have been disabled by default for Administration Console, Identity Server, and between browsers and Access Gateway.

To disable SSL v2 and SSL v3 between Access Gateway and web servers, see Section 4.4, “Disabling Weak Protocols between Access Gateway and Web Servers,” on page 33.

8.2 Optimizing SSL Configuration with Ciphers

In addition to setting up Transport Level Security (TLS), using a cipher suite provides additional security to client-server communications from Identity Server, Access Gateway to the web browsers.

IMPORTANT: The settings specified in this section indicate an SSL configuration that provides an optimal level of security. If you plan to make any changes in the cipher information, ensure that you test the configuration before you deploy it in the production setup.

In Access Manager 4.3, stronger ciphers for SSL communications have been configured for Administration Console, Identity Server, and communication between browsers and Access Gateway.

For information about how to specify SSL Configuration for communication between Access Gateway and web servers, see Section 4.5, “Configuring Stronger Ciphers for SSL Communication between Access Gateway and Web Servers,” on page 34

8.3 Enabling Perfect Forward Secrecy

When an SSL handshake is performed, SSL information regarding the capabilities of browser/client and server is exchanged and validated. An SSL session key that meets both the client’s and server’s criteria is established. After the session key is established, all subsequent communication between the client and the site is encrypted and thus secured.

The most common method for negotiating the session key is the RSA public-key cryptosystem. The RSA approach uses the server’s public key to protect the session key parameters created by the client after the key parameters are sent to the server. The server decrypts this handshake with its corresponding private key. If an attacker ever steals the server’s private key, they can decrypt your SSL session and any saved SSL sessions. This approach allows Wireshark or ssldump tools to decrypt the saved SSL communication by using an exported server certificate with private key.

Perfect Forward Secrecy (PFS) removes this shortcoming of the RSA approach. When PFS is enabled, no link between the server’s private key and each session key is established. If an attacker ever gets access to your server’s private key, the attacker cannot use the private key to decrypt any of your archived sessions.

In Access Manager 4.3, PFS has been enabled by default for Administration Console and Identity Server. For information about how to enable PFS in Access Gateway, see Section 4.6, “Enabling Perfect Forward Secrecy,” on page 34.

8.4 Adding HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that protects HTTPS websites against downgrade attacks. Downgrade attacks are often implemented as part of a man-in-the-middle attack such as Poodle. HSTS also protects against cookie hijacking. It enables web servers to mandate that web browsers (or other complying user agents) should interact with it by using only secure HTTPS connections, and never through the insecure HTTP protocol.

In Access Manager 4.3, HSTS has been enabled by default for all components.

8.5 Disabling SSL Renegotiations

SSL renegotiation is vulnerable to the man-in-the-middle attacks. In Access Manager 4.3, it has been disabled by default for all components except Analytics Server.

For information about how to disable it in Analytics Server, see Section 5.2, “Disabling SSL Renegotiations,” on page 39.

8.6 Customizing the Size of Ephemeral Diffie-Hellman Keys

It is recommended not to use keys of sizes less than 1024 bits because of their insufficient strength. In Access Manager 4.3, the default EDH key size in Administration Console and Identity Server is 2048.

For information about how to customize the size of EDH keys in Analytics Server, see Section 5.1, “Customizing the Size of EDH Keys,” on page 39.

8.7 Configuring Unlimited Strength Jurisdiction Policy Files

By default, JDK is restricted to use the Advanced Encryption Standard (AES) 128-bit key encryption and not the higher strength keys. This restriction is because of policies in some countries for permitted key strength of imported encryption software.

If your country permits, you can remove the restriction by overriding the security policy files with others that Oracle provides.

To configure the unlimited strength jurisdiction policy files, perform the following steps:

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from Oracle.

   Ensure that you download the correct policy file updates for your version of Java.
2. Extract the downloaded file.

   The download includes two .jar files with the same names as the existing policy files.
3. Locate the following two existing policy files:
   - `local_policy.jar`
   - `US_export_policy.jar`

     Linux: `<java-home>/lib/security/`

     Windows: `C:/Program Files/Java/jre<version>/lib/security/`
4. Replace the existing policy files with the unlimited strength policy files you extracted.

9 Strengthening Certificates

This section discusses the following topics:

9.1 Key Size and Signature Algorithm Considerations

Access Manager ships with a CA that can create certificates with a key size of 512, 1024, 2048, or 4096. Select the maximum size supported by the applications that you are protecting with Access Manager. Security increases with the increase in key size length. The default certificates created by Access Manager 4.2 and later are of 2048 key size. If you are upgrading Access Manager from a version older than 4.2, ensure that certificates with small key sizes are replaced with 2048 or above.

In signature algorithms, SHA1 is no longer considered secure. Access Manager supports creation of a certificate only with SHA-256 and SHA-512. When you are importing external certificates signed by a well-known third-party CA into Access Manager, ensure that they are of SHA-256 or above.

9.2 Trusted Certificate Authorities

Access Manager ships with a CA. During installation, Access Manager CA creates and distributes certificates. For added security, replace these certificates with certificates from a well-known CA.

To use certificates signed by an external CA, perform the following activities:

1. Obtain externally signed certificates.

   For more information, see “Obtaining Externally Signed Certificates” in the *NetIQ Access Manager 4.3 Administration Guide*.
2. Configure Identity Server to use externally signed certificates.

   For more information, see “Configuring Identity Server to Use an Externally Signed Certificate” in the *NetIQ Access Manager 4.3 Administration Guide*.
3. Configure Access Gateway to use externally signed certificates.

   For more information, see “Configuring Access Gateway to Use an Externally Signed Certificate” in the *NetIQ Access Manager 4.3 Administration Guide*.

9.3 Certificate Renewal

Ensure that you renew certificates before it gets expired. Your security needs might allow for a longer or shorter period. You can configure to get certificate expiration notifications.

For more information, see “Getting the Certificate Expiration Notification” in the *NetIQ Access Manager 4.3 Best Practices Guide*.

When you install Administration Console, the following test certificates are automatically generated:

test-signing
test-encryption
test-connector
test-provider
test-consumer
test-stunnel

For strong security, it is recommended that you replace these certificates, except the test-stunnel certificate, with certificates from a well-known certificate authority.

Ten years after you install Administration Console, new versions of these certificates are automatically generated as the old certificates expire. If you are using any of the test certificates in your configuration, Administration Console cannot use the new version until you reboot the machine.

Access Manager renews test-* certificate for both primary and secondary Administration Console including the edir certificate on secondary Administration Console automatically.

Certificates created manually by using Access Manager CA does not get renewed automatically.

Perform the following steps to renew manually created certificates. Lets assume that a certificate with the alias *signing* in the Identity Server signing keystore is about to expire.

1. Create a new certificate. (**Security** > **Certificates** > **New**)
2. Add the new certificate to the keystore with the alias of the certificate that will expire (*signing*). (**Actions** > **Add Certificate to Keystores**)
3. Select the option to overwrite.

10 XSS, XFS, and Clickjacking Attacks

This section included the following topics:

10.1 Cross-site Scripting Attacks

By default, Access Manager performs extensive checks to prevent Cross-site Scripting (XSS) attacks. However, Access Manager does not validate a JSP file if you have customized it. If you modify JSP files to customize the login, logout, error pages, and so forth, you must sanitize the respective JSP file to prevent XSS attacks.

Perform either one of the following options to sanitize the customized JSP file:

- HTML Escaping. See Option 1: HTML Escaping in the NetIQ Access Manager 4.3 Administration Guide.
- Filtering. See Option 2: Filtering in the NetIQ Access Manager 4.3 Administration Guide

10.2 Cross-Frame Scripting Attacks

Any intruder can call Identity Server portal login pages or the pages delivered by Access Gateway ESP with the default Identity Server configuration from an HTML iFrame. To prevent this vulnerability, Cross-Frame Scripting (XFS) has been disabled for both Identity Server and Access Gateway ESP in Access Manager 4.3.

The configuration to prevent this attack is enabled by default in Access Manager 4.3.

10.3 Clickjacking Attacks

Web applications allow external sites to include content by using IFrames. This enables an attacker to embed the malicious code beneath legitimate clickable content. An attacker can trick a web user into clicking the malicious content that the attacker can control.

The configuration to prevent this attack is enabled by default in Access Manager 4.3.

11 Getting the Latest Security Patches

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Gateway and Analytics Server use the OpenSSL library for cryptographic functions. It is recommended to update Access Gateway and Analytics Server with the latest OpenSSL patch.

Getting the Latest Security Updates for Access Gateway and Analytics Server

Follow any of these options:

- Novell Customer Center

  For more information, see “Installing or Updating Security Patches for the Access Gateway Appliance and Analytics Server”in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

- Local Subscription Management Tool

  For more information, see “Configuring Subscription Management Tool”in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

Getting the Latest Security Updates for Access Gateway Service

See “Updating Security Patches for Access Gateway Service ” in the *NetIQ Access Manager 4.3 Installation and Upgrade Guide*.

12 Restoring Previous Security Level After Upgrading Access Manager

All protocols, ciphers, and filter configurations in all components are made highly secure by default in Access Manager 4.3. If your Access Manager setup is configured with less secure settings, upgrading it to 4.3 may result in communications issues. The following are few example scenarios when you may need to restore your previous security settings:

- When browsers do not support TLS1.1 or TLS1.2 protocol or secure ciphers suites.
- When third-party service provider does not support TLS1.1 or TLS1.2 protocol or secure cipher suites along with the following configuration:
  - A SAML or Liberty federation with artifact binding between Access Manager and third-party service provider.
  - WS-Trust federation between Access Manager and third-party service provider.
- When OAuth clients or OAuth resource servers do not support TLS1.1 or TLS1.2 protocol or secure cipher suites.

Backed Up Configuration Files

When you upgrade to Access Manager 4.3, the upgrade script backs up the following files to enable you restoring the previous configuration:

- **Administration Console:** tomcat7.conf (tomcat7w.exe on Windows), server.xml, web.xml
- **Identity Server:** tomcat.conf (tomcat7w.exe on windows), server.xml, web.xml
- **Access Gateway:** web.xml, httpd.conf, NovellAGSettings.conf, tomcat.conf (tomcat8w.exe on Windows), sever.xml

The backup files are located at the following location:

Linux: `/root/nambkup` (separate folders for Administration Console, Identity Server, and Access Gateway)

Windows: `C:\nambkup` (Backed up files are available in `tomcat_conf.zip`). Name of the backed up Identity Server web.xml is `nidp_web.xml` and Administration Console web.xml is `ac_web.xml`.

NOTE: Compare each upgraded configuration file with the corresponding backup file. If your backup file includes the similar configuration as it is in the upgraded file, you do not need to make any changes.

This section includes the following topics:

12.1 Restoring Previous Security Settings for Administration Console

12.1.1 Restoring the Previous Protocols Settings

1. Open the backup `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the sslProtocol attribute in `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `Connector` element and copy the attribute values.
3. Change to the Tomcat configuration directory and open the 4.3 `server.xml` file:

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

   Windows Server 2012: `\Program Files (x86)\Novell\Tomcat\conf`
4. Search for the sslProtocol attribute in the `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `Connector` element. You will see the following value:

   ```
   sslProtocol="TLSv1.2" sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2"
   ```
5. Replace this attribute value with the previous value that you copied in step 2.

12.1.2 Restoring the Previous Settings of Ciphers for SSL Communication

1. Open the backup `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the cipher attribute in `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `Connector` element and copy the list of ciphers.
3. Change to the Tomcat configuration directory:

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

   Windows Server 2012: `\Program Files (x86)\Novell\Tomcat\conf`
4. Open the `server.xml` file. Search for the cipher attribute in `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `Connector` element.
5. Replace this list of ciphers with the list copied in step 2.

12.1.3 Disabling Perfect Forward Secrecy

1. Open the backup `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the cipher attribute in `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `<Connectors>` element and copy the list of ciphers

3 Change to the Tomcat configuration directory:

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

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

4 Open the `server.xml` file. Search for the cipher attribute in `NIDP_Name="devman"` and `NIDP_Name="connector"` inside the `<Connectors>` element.

5 Replace the list of ciphers with the value you copied in step 2.

6 Remove the `useServerCipherSuitesOrder` attribute.

12.1.4 Restoring the Previous Size of EDH Keys

Linux:

1 Open the `/opt/novell/nam/adminconsole/conf/tomcat7.conf` file.

2 Remove the following line:

```
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.ephemeralDHKeySize=2048"
```

Windows:

1 Navigate to `C:\Program Files (x86)\Novell\Tomcat\bin` and then double-click `tomcat7w`.

2 Under the Java tab, remove the following line in **Java Options**:

```
-Djdk.tls.ephemeralDHKeySize=2048
```

12.1.5 Removing HTTP Strict Transport Security

1 Change to the Tomcat configuration directory:

Linux: `/opt/novell/nam/adminconsole/conf/web.xml`

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

2 Open the `web.xml` file and comment out the `httpHeaderSecurity` filter definition.

```
<filter>
<filter-name>httpHeaderSecurity</filter-name>
<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
filter-class>
<async-supported>true</async-supported>
</filter>
```

3 Comment out the following parameter that sets up an appropriate maximum age value:

```
<init-param>
<param-name>hstsMaxAgeSeconds</param-name>
<param-value>31536000</param-value>
</init-param>
```

4 Comment out the filter mapping.

```
<filter-mapping>
<filter-name>httpHeaderSecurity</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

12.2 Restoring Previous Security Settings for Identity Server

12.2.1 Restoring the Previous Protocols Settings

1. Open the backup `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the sslProtocol attribute and copy the attribute value.
3. Change to the Tomcat configuration directory:

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

   Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\conf`
4. Open the 4.3 `server.xml` file.

   Search for the `sslProtocol` attribute. You will see the following value:

   ```
   sslProtocol="TLSv1.2" sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2"
   ```
5. Replace this attribute value with the previous value that you copied.

12.2.2 Restoring the Previous Settings of Ciphers for SSL Communication

1. Open the backup `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the cipher attribute in `NIDP_Name="connector"` inside the `<Connectors>` element and copy the list of ciphers.
3. Using command prompt, change to the Tomcat configuration directory:

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

   Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\conf`
4. Open the 4.3 `server.xml` file.

   Search for the `cipher` attribute in `NIDP_Name="connector"` inside the `<Connector>` element.
5. Replace this list of ciphers with the list copied in step 2.
6. (Conditional) If you have multiple Identity Servers in your cluster configuration, repeat these steps on each Identity Server.

12.2.3 Disabling Perfect Forward Secrecy

1. Open the backed up `server.xml`. For location of the backup file, see “Backed Up Configuration Files” on page 63.
2. Search for the cipher attribute in `NIDP_Name="connector"` inside the `<Connectors>` element and copy the list of ciphers
3. Using command prompt, change to the Tomcat configuration directory:

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

   Windows Server: `\Program Files (x86)\Novell\Tomcat\conf`
4. Open the `server.xml` file. Search for the cipher attribute in `NIDP_Name="connector"` inside the `<Connectors>` element.
5. Replace the list of ciphers with the value you copied in step 2.

12.2.4 Restoring the Previous Settings of the Size of EDH Keys

Linux:

1. Open the `/opt/novell/nam/idp/conf/tomcat.conf` file.
2. Remove the following line:

   ```
   JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.ephemeralDHKeySize=2048"
   ```

Windows:

1. Navigate to `C:\Program Files (x86)\Novell\Tomcat\bin` and then double-click `tomcat7w`.
2. Under the Java tab, remove the following line in **Java Options**:

   ```
   -Djdk.tls.ephemeralDHKeySize=2048
   ```

12.2.5 Removing HTTP Strict Transport Security

1. Change to the Tomcat configuration directory:

   Linux: `/opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml`

   Windows Server: `\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF`
2. Open the `web.xml` file and comment out the `httpHeaderSecurity` filter definition.

   ```
   <filter>
       <filter-name>httpHeaderSecurity</filter-name>
       <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
   filter-class>
       <async-supported>true</async-supported>
   </filter>
   ```
3. Comment out the hstsMaxAgeSeconds parameter:

   ```
   <init-param>
       <param-name>hstsMaxAgeSeconds</param-name>
       <param-value>31536000</param-value>
   </init-param>
   ```

4 Comment out the filter mapping.

```
<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

12.2.6 Removing the Clickjacking Filter

1 In the `web.xml` file, comment out the following tomcat filter configuration:

Linux: `/opt/novell/nids/lib/webapp/WEB-INF/`

Windows: `\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEBINF\`

```
<filter>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
filter-class>
    <init-param>
        <param-name>antiClickJackingOption</param-name>
        <param-value>SAMEORIGIN</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

2 Restart Identity Server.

Linux: `/etc/init.d/novell-idp restart`.

Windows: Enter the following commands:

```
net stop Tomcat7
```

```
net start Tomcat7
```

12.3 Restoring Previous Security Settings for Access Gateway

12.3.1 Restoring the Previous Protocol Settings between Browsers and Access Gateway

1 In the `nambkup` folder, open the `NovellAGSettings.conf` file from the `mag <time stamp of upgrade>/conf` folder.

2 Search for `SSL Protocol` and copy the value associated with it.

3 Click **Devices** > **Access Gateways** > **Edit** > **Advanced Options** and replace the following configuration with the value copied in `NovellAGSettings.conf` in step 2:

```
SSLProtocol TLSv1.1 +TLSv1.2
```

12.3.2 Restoring the Previous Ciphers Settings between Browsers and Access Gateway

1 In the `nambkup` folder, open the `NovellAGSettings.conf` file from the `mag <time stamp of upgrade>/conf` folder.

2 Search for SSL and copy the value

3 Click **Devices** > **Access Gateways** > **Edit** > **Advanced Options** and replace the following configuration with the value copied in `NovellAGSettings.conf` in step 2:

```
SSLCipherSuite !aNULL:!eNULL:!EXPORT:!DSS:!DES:!RC4:ALL:!EDH
```

If `NovellAGSettings.conf` does not contain this line, delete this line in Access Gateway Advanced Options.

12.3.3 Removing the Clickjacking Filter

1 In the `/opt/novell/nesp/lib/webapp/WEB-INF/web.xml` file, comment out the following tomcat filter configuration:

```
<filter>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
filter-class>
    <init-param>
        <param-name>antiClickJackingOption</param-name>
        <param-value>SAMEORIGIN</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>TomcatSameOriginFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

2 Restart ESP by running the following command:

Linux: `/etc/init.d/novell-mag restart OR rcnovell-mag restart`

Windows: `net stop Tomcat8`

`net start Tocmat8`

NOTE: You can also restart ESP through Administration Console. Select the cluster node > **Action** > **Service Provider** > **Restart Service Provider**.

12.3.4 Removing HTTP Strict Transport Security

You need to perform the following two actions to disable the HTTP Strict Transport Security setting:

- Set the `SetStrictTransportSecurity` option to off.
- Disable the `httpHeaderSecurity` filter definition in ESP `web.xml`.

Setting SetStrictTransportSecurity to off

1. Click **Devices** > **Access Gateways** > **Edit** > **Advanced Options**.
2. Set the following option:

   ```
   SetStrictTransportSecurity off
   ```

3. Restart Apache.

   Linux: `/etc/init.d/novell-apache2 restart OR rcnovell-apache2 restart`

   Windows: `net stop apache2.2`

   `net start apache2.2`

Disabling httpHeaderSecurity in ESP web.xml

1. Change to the Tomcat configuration directory:

   Linux: `/opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml`

   Windows Server: `\Program Files\Novell\Tomcat\webapps\nesp\WEB-INF\WEB-INF`\web.xml

2. Open the `web.xml` file and comment out the `httpHeaderSecurity` filter definition.

   ```
   <filter>
       <filter-name>httpHeaderSecurity</filter-name>
       <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</
   filter-class>
       <async-supported>true</async-supported>
   </filter>
   ```

3. Comment out the `hstsMaxAgeSeconds` parameter:

   ```
   <init-param>
       <param-name>hstsMaxAgeSeconds</param-name>
       <param-value>31536000</param-value>
   </init-param>
   ```

4. Comment out the filter mapping.

   ```
   <filter-mapping>
       <filter-name>httpHeaderSecurity</filter-name>
       <url-pattern>/*</url-pattern>
       <dispatcher>REQUEST</dispatcher>
   </filter-mapping>
   ```