Enabling Transport Layer Security (TLS) 1.1 and 1.2 for Access Manager 4.0 Hotfix 1

March 2014

Access Manager version 4.0 Hotfix 1 supports Transport Layer Security (TLS) version 1.1 and 1.2. Installing the latest Hotfix ensures that TLS 1.1 and TLS 1.2 are enabled for all the Access Manager components. This ensures privacy of information communicated over the Internet.

This document explains how to install and configure Transport Layer Security (TLS) between the various Access Manager components.

1   Prerequisite

Ensure that you are on Access Manager 4.0 Hotfix 1.

For information on installing, see NetIQ Access Manager 4.0 Installation or NetIQ Access Manager Appliance 4.0 Installation

For more information on upgrading to Hotfix 1, see Upgrading to Access Manager 4.0 Hotfix1

2   Enabling Access Gateway for TLS 1.1 and TLS 1.2

The Access Gateway internally uses mod_ssl module and OpenSSL for SSL support.

Access Manager 4.0 Hotfix 1 includes a package that contains an updated version of the Access Gateway that is capable of communicating using TLS 1.1 and TLS 1.2. With this new package, the Access Gateway supports all SSL and TLS versions. This ranges from SSL 2.0 to TLS 1.2.

Install and configure the new package to enable support for TLS 1.1 and TLS 1.2. The Access Gateway install scripts simplify installation of the package.

IMPORTANT: Enabling Access Gateway for TLS 1.1 and TLS 1.2 is supported only on SuSe Linux platforms.

1 Go to NetIQ Access Manager 4 Documentation website

2 From the **Additional Resources** section, select **Access Gateway Install Scripts for TLS 1.1 and 1.2**. This downloads the `ag_install_scripts.zip` file. Save and extract the `.zip` file to a location on your computer.

3 Open a terminal window as a `root` user.

4 From the `.zip` file contents, locate `install_AG_Openssl101.sh` file.

5 Execute the script using the following command:

   `sh install_AG_Openssl101.sh`

6 After the new package is installed, the Access Gateway can accept connections from clients using any SSL or TLS versions ranging from SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, to TLS 1.2.

   If you want the Access Gateway to accept connection over a specific TLS version, then specify the TLS version using an advanced option.

   If you do not specify the protocol version in the advanced options, Access Gateway accepts connections using SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS1.2.

   For example, to accept connections over only TLS 1.1, specify it as `SSLProtocol TLSv1.1`

   If you want to enable support for multiple TLS versions, indicate the versions in the SSL directive separated by a plus (+) sign.

   For example: If you want to enable support for TLS 1.1 and TLS 1.2, specify it in the following manner:

   `SSLProtocol TLSv1.1 +TLSv1.2`

   For more information about SSLProtocol directives, see Apache Module mod_ssl documentation

   For general information on how to set an advanced option in Access Gateway, see Configuring the Global Advanced Options

3 Configuring TLS 1.1 and TLS 1.2 for Incoming Connections to the Identity Server

The Identity Server uses JSSE (Java Secure Socket Extension) for SSL support.

After installing Hotfix1, by default the Identity Server accepts connections from clients using SSL 2.0, SSL 3.0 and TLS 1.0. If you want to use TLS 1.1 and TLS 1.2, then edit the `server.xml` file and add an SSLProtocol directive using the following procedure:

Configuring TLS 1.1 and TLS 1.2 on the Identity Server:

1 Open a terminal window as a `root` user

2 Open `/opt/novell/nam/idp/conf/server.xml` file.

3 Traverse to the 8443 Connector configuration and add a SSLProtocol directive to the connector as `sslProtocol="TLSv1.1"`

   For example:

```
<Connector NIDP_Name="connector" SSLEnabled="true" URIEncoding="utf-8"
acceptCount="100" address="192.168.0.0"
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_KRB5_WITH_3DES_EDE_CBC_SHA, TLS_KRB5_WITH_RC4_128_SHA"
clientAuth="false" disableUploadTimeout="true" enableLookups="false"
keystoreFile="/opt/novell/devman/jcc/certs/idp/connector.keystore"
keystorePass="XBPO9YO1I9RSjtZ" maxThreads="600" minSpareThreads="5"
port="8443" scheme="https" secure="true"
sslImplementationName="com.novell.nidp.common.util.net.server.NIDPSSLImplement
ation"
sslProtocol="TLSv1.1" />
```

Setting the SSLProtocol to the string *TLSv1.1* allows the Identity Server to accept connections from clients using SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.

If the client or Web browser does not support TLS 1.1, communication is done using TLS 1.0.

4 Restart the Identity server using `/etc/init.d/novell-idp restart` command.

For more information about SSLProtocol configurable parameters, see Tomcat 7 configurable parameters

If you have configured the Identity Server to accept incoming connections in TLS 1.1 and TLS 1.2, it is necessary to configure the Embedded Service Provider (ESP) of Access Gateway to send outgoing connections to the Identity Server over the same TLS version.

Follow this procedure to configure the ESP to send outgoing connections:

Configuring TLS 1.1 and TLS 1.2 for the ESP:

1 On each Access Gateway server, open the `nidpconfig.properties` located at `/opt/novell/nesp/lib/webapp/WEB-INF/classes/`

2 Add the following text to the `nidpconfig.properties` file:

```
# Define the default TLS version that is used for outgoing connections from the
ESP
# Possible values are TLS, TLSv1, TLSv1.1, TLSv1.2. Only a single TLS version
#can be specified

DEFAULT_TLS_VERSION = TLSv1.1

# Define the fallback TLS version to use if the TLS version defined above
#fails. This should be used only for cases where the default value above has
been changed, and is set to something other than "TLS".
# Most commonly used when the default has been changed to a higher version like
#TLSv1.1 or TLSv1.2. With the higher protocol setting, connection to a server
#may fail because the server may not support the new TLS version. When that
#occurs, the ESP will use the TLS version
#defined below to retry the connection

FALLBACK_TLS_VERSION = TLS
```

3 Restart ESP using the `/etc/init.d/novell-mag restart` command.

NOTE: To use *TLSv1.2*, specify the value of the `DEFAULT_TLS_VERSION` as *TLSv1.2*.

---

4 Configuring TLS 1.1 and TLS 1.2 for Outgoing Connections from the Identity Server

After installing Hotfix 1, by default, the Identity Server sends connections using SSL 2.0, SSL 3.0 or TLS 1.0. For example, while communicating with other Service Providers.

You can configure the Identity Server to use TLS 1.1 and TLS 1.2 for outgoing connections. Verify that the service provider is capable of accepting connections over the specified TLS version.

IMPORTANT: If you have configured the Access Gateway to accept connections only over TLS 1.1 or TLS 1.2, you must also configure the Identity Server to use the corresponding TLS version for outgoing connections.

If the TLS versions do not match, it can result in failures in user authentication.

Configuring TLS 1.1 and TLS 1.2 on the Identity Server:

1 On the Identity Server machine, open the `nidpconfig.properties` file located at `/opt/novell/nids/lib/webapp/WEB-INF/classes/`

2 Add the following text to the `nidpconfig.properties` file:

```
#Define the default TLS version that is used for outgoing connections from IDP
#Possible values are TLS, TLSv1, TLSv1.1, TLSv1.2. Only a single TLS version
#can be specified. If you do not specify a TLS version using the directive
below, the default version is TLS

DEFAULT_TLS_VERSION = TLSv1.1

# Define the fallback TLS version to use if the TLS version defined above
fails.
# This should be used only for cases where the default above has been changed,
#and is set to something other than "TLS". Most commonly used when the default
#has been changed to a higher version like TLSv1.1 or TLSv1.2. With the higher
#protocol setting, connection to a server may fail because the server may not
#support the new TLS version.
# When that occurs, the Identity server will use the TLS version
#defined below to retry the connection

FALLBACK_TLS_VERSION = TLS
```

3 Restart the Identity Server using `/etc/init.d/novell-idp restart` command.

NOTE: To use TLS 2.0, specify the value of the `DEFAULT_TLS_VERSION` as *TLSv1.2*.

5 Configuring SSL Communication Between the Access Gateway Service and Web Servers

After installing Access Manager Hotfix 1, if you have enabled SSL communication between the Access Gateway and the Web server, the Access Gateway uses the highest version of the TLS that the Web server supports. For example, if you have configured the Web server to use TLS 1.1 or TLS 1.2, the Access Gateway sends requests to the Web server using the specified TLS version.

For general information about enabling SSL between the Access Gateway and the Web server, see Configuring the Access Gateway for SSL and Other Security Features and for Access Manager Appliance, see Configuring the Access Gateway for SSL and Other Security Features.

6 RollBack Apache Gateway to Access Manager 4.0 Hotfix 1

IMPORTANT: Ensure that before performing the rollback, all the SSLProtocol directives defined as advanced options in the Access Gateway are removed.

The following procedure allows you to roll back to the default version of the Apache Gateway that is included with Access Manager 4.0 Hotfix 1. The Access Gateway rollback scripts simplify rollback of the Apache Gateway.

1 Go to NetIQ Access Manager 4 Documentation website

2 From the **Additional Resources** section, select **Access Gateway Install Scripts for TLS 1.1 and 1.2**. This downloads the `ag_install_scripts.zip` file. Save and extract the `.zip` file to a location on your computer.

3 Open a terminal window as a `root` user.

4 From the `.zip` file contents, locate `uninstall_AG_Openssl101.sh` file.

5 Execute the script using the following command:

`sh uninstall_AG_Openssl101.sh`

You can safely ignore any warnings displayed during the rollback process.

7 Legal Notice