Enabling Transport Layer Security 1.1 and 1.2 for Access Manager

May 2014

Access Manager 4.0 Hotfix 3 and 4.0 SP1 support Transport Layer Security (TLS) version 1.1 and 1.2. Installing either of these Access Manager versions ensures that TLS 1.1 and TLS 1.2 are enabled for all Access Manager components. This ensures privacy of information communicated over the Internet.

NOTE: Access Manager 4.0 SP1 supports enabling TLS on SUSE and RHEL platforms. In 4.0 Hotfix 3, it is supported only on the SUSE platform.

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

- Section 1, "Prerequisite," on page 1
- Section 2, "Enabling Access Gateway for TLS 1.1 and TLS 1.2," on page 1
- Section 3, "Configuring TLS 1.1 and TLS 1.2 for Incoming Connections to the Identity Server," on page 2
- Section 4, "Configuring TLS 1.1 and TLS 1.2 for Outgoing Connections from the Identity Server," on page 4
- Section 5, "Configuring SSL Communication Between the Access Gateway Service and Web Servers," on page 4
- Section 6, "RollBack Apache Gateway from TLS 1.1 or 1.2 in Access Manager 4.0 Hotfix 3 or 4.0 SP1," on page 5
- Section 7, "Upgrading Access Manager 4.0 Hotfix 3 to 4.0 SP1," on page 5
- Section 8, "Legal Notice," on page 5

1 Prerequisite

Ensure that you are currently on Access Manager 4.0 Hotfix 3 or 4.0 SP1.

For information about installing Access Manager, see *NetIQ Access Manager 4.0 Installation Guide*.

For more information about upgrading to Hotfix 3, see Upgrading to Access Manager 4.0 Hotfix 3.

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 includes a package that contains an updated version of the Access Gateway that is capable of communicating by 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.

1. Open a terminal window as a `root` user.
2. **If you are on Access Manager 4.0 Hotfix 3:**
   - **2a** Go to the `/opt/novell/nam/mag/AdditionalFiles` folder and locate the `ag_install_scripts.tar.gz` file.

     Extract the files by using `tar -zxvf ag_install_scripts.tar.gz` command.
   - **2b** From the file contents, locate the `install_AG_Openssl101.sh` file.
   - **2c** Run the script by using the following command:

     ```
     sh install_AG_Openssl101.sh
     ```
3. **If you are on Access Manager 4.0 SP1:**
   - **3a** Go to the `/opt/novell/nam/mag/AdditionalFiles` folder and locate `install_AG_Openssl101.sh`.
   - **3b** Run the script by using the following command:

     ```
     sh install_AG_Openssl101.sh
     ```

     It will install required rpms.
4. After the new package is installed, the Access Gateway can accept connections from clients by 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 by using an advanced option.

   If you do not specify the protocol version in the advanced options, the Access Gateway accepts connections by 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 about how to set an advanced option in the 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 Access Manager 4.0 Hotfix 3 or 4.0 SP1, by default, the Identity Server accepts connections from clients by 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.

Use the following procedure to configure TLS 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 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 by using TLS 1.0.

4 Restart the Identity server by using the `/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, you must configure the Embedded Service Provider (ESP) of Access Gateway to send outgoing connections to the Identity Server over the same TLS version.

Use the following procedure to configure TLS for 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 by 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 Access Manager 4.0 Hotfix 3 or 4.0 SP1, by default, the Identity Server sends connections by 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 by using the `/etc/init.d/novell-idp restart` command.

NOTE: To use TLS 1.2, specify the value `DEFAULT_TLS_VERSION` as *TLSv1.2*.

---

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

After installing Access Manager 4.0 Hotfix 3 or 4.0 SP1, 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 by 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".

6 RollBack Apache Gateway from TLS 1.1 or 1.2 in Access Manager 4.0 Hotfix 3 or 4.0 SP1

IMPORTANT: Ensure that before performing the rollback, all 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 3 and 4.0 SP1. The Access Gateway rollback scripts simplify rollback of the Apache Gateway.

1. Open a terminal window as a `root` user.
2. Traverse to the `/opt/novell/nam/mag/AdditionalFiles` folder, locate `uninstall_AG_Openssl101.sh` and run this script by using the following command:.

   ```
   sh uninstall_AG_Openssl101.sh
   ```

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

7 Upgrading Access Manager 4.0 Hotfix 3 to 4.0 SP1

If you have configured Access Manager 4.0 Hotfix 3 for TLS 1.1 or 1.2 and then you upgrade it to 4.0 SP1, you require to repeat the steps for enabling TLS. After upgrading Access Manager from Hotfix 3 to 4.0 SP1, the TLS configuration gets disabled.

IMPORTANT: Ensure that before upgrading Access Manager from 4.0 Hotfix 3 to 4.0 SP1, all SSLProtocol directives defined as advanced options in the Access Gateway are removed.

8 Legal Notice

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

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

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

© 2014 NetIQ Corporation. All Rights Reserved.

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

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

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