

Access Manager 4.0 Service Pack 1 Readme

May 2014



Access Manager 4.0 Service Pack 1 includes new features, improves usability, and resolves several previous issues.

Many of these improvements are made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the [Access Manager forum on Qmunity](#), our community Web site that also includes product notifications, logs, and product user groups.

For the list of software fixes and enhancements in the previous release, see [Access Manager 4.0 Hotfix 3 readme](#).

For more information about this release and for the latest release notes, see the [Documentation](#) Web site. To download this product, see the [Product Upgrade](#) Web site.

- [Section 1, "What's New?," on page 1](#)
- [Section 2, "Installing or Upgrading," on page 9](#)
- [Section 3, "Supported Upgrade Paths," on page 9](#)
- [Section 4, "Verifying Version Numbers," on page 10](#)
- [Section 5, "Known Issues," on page 10](#)
- [Section 6, "Contact Information," on page 12](#)
- [Section 7, "Legal Notice," on page 12](#)

1 What's New?

Access Manager 4.0 Service Pack 1 provides the following enhancements and fixes in this release:

- [Section 1.1, "Enhancements," on page 1](#)
- [Section 1.2, "Code Promotion," on page 4](#)
- [Section 1.3, "Support for Red Hat Enterprise Linux and Windows Server," on page 4](#)
- [Section 1.4, "Fixed Issues," on page 5](#)

1.1 Enhancements

This release introduces the following enhancements:

- [Section 1.1.1, "Office 365 - Active Client Support," on page 2](#)
- [Section 1.1.2, "WS-Trust Enhancements," on page 2](#)
- [Section 1.1.3, "Federation Enhancements," on page 2](#)
- [Section 1.1.4, "Authentication Enhancements," on page 3](#)

1.1.1 Office 365 - Active Client Support

This release introduces active (client-based) access to Office 365 services by using WS-Trust protocol. Client-based services include Lync, Outlook client, MS-Office software, and so on. It also supports passive (browser-based) access by using WS-Federation protocol. Browser-based services include Office 365 portal, Outlook Web Access, SharePoint Online, and so on.

This helps users access both active and passive Office 365 services by using their enterprise credentials.

For more information, see [Configuring Single Sign-On for Office 365 Services](#).

1.1.2 WS-Trust Enhancements

This release introduces the following WS-Trust enhancements:

- ♦ [Section 1.1.2.1, "SAML Authentication Support," on page 2](#)
- ♦ [Section 1.1.2.2, "Support for Renewing Tokens," on page 2](#)
- ♦ [Section 1.1.2.3, "Support for SOAP 1.2," on page 2](#)

1.1.2.1 SAML Authentication Support

This service pack introduces an enhancement that allows WS-Trust STS (Security Token Service) to support authentication by using a SAML token issued by a third-party provider. The tokens can be in SAML 1.1 or SAML 2.0 format. This is an enhancement over the existing functionality where only username tokens are supported for authentication.

For more information, see [Authentication Using SAML Tokens](#).

1.1.2.2 Support for Renewing Tokens

This service pack introduces an enhancement that allows renewing token issued by WS-Trust STS. For more information, see [Renewing a Token](#).

1.1.2.3 Support for SOAP 1.2

This service pack introduces an enhancement that supports SOAP 1.2 as the default binding for the Identity Server. Starting from Access Manager 4.0 Service Pack 1 release, the default binding supported is SOAP 1.2. For more information on using SOAP 1.1 as the binding, see [Changing the Binding to SOAP 1.1](#)

NOTE: If you are using WS-Trust protocol on a 4.0 setup that has SOAP 1.1 set as the default binding, then you must either configure your client to send requests over SOAP 1.2 or modify the Identity Server server to use SOAP 1.1.

1.1.3 Federation Enhancements

This release introduces the following federation enhancements:

- ♦ [Section 1.1.3.1, "Authorization Policy for Service Providers," on page 3](#)
- ♦ [Section 1.1.3.2, "Step Up Authentication for Service Provider-Initiated Request," on page 3](#)

1.1.3.1 Authorization Policy for Service Providers

This service pack introduces an enhancement that allows you to apply an authorization policy to either allow or deny passing of federation tokens to the service provider. The authorization policy can be defined for identity provider-initiated logins as well as service provider-initiated logins.

For more information, see [Executing Authorization Based Roles Policy During SAML 2.0 Service Provider-Initiated Request](#).

1.1.3.2 Step Up Authentication for Service Provider-Initiated Request

This service pack introduces an enhancement that enables you to assign a default contract for the service providers in a federation setup. You can assign the default contract to the service provider in the following scenarios:

- ♦ An authentication request is initiated but contract information is not available to validate the user.
- ♦ The authentication level of the contract requested is less than the desired.

NOTE: Step Up authentication is supported on SAML 1.1 and SAML 2.0 protocols and is not currently supported on WS-Federation protocol.

Identity Provider-initiated requests are supported on SAML 1.1 and Liberty protocol.

For more information, see [Contracts Assigned to SAML 2.0 Service Provider](#).

1.1.4 Authentication Enhancements

- ♦ [Section 1.1.4.1, "Social Authentication," on page 3](#)
- ♦ [Section 1.1.4.2, "Persistent Authentication," on page 3](#)
- ♦ [Section 1.1.4.3, "TOTP Authenticator," on page 4](#)
- ♦ [Section 1.1.4.4, "Delete Old User Sessions on Login," on page 4](#)
- ♦ [Section 1.1.4.5, "Forceful Deletion of User Sessions," on page 4](#)
- ♦ [Section 1.1.4.6, "Login Redirect URL," on page 4](#)

1.1.4.1 Social Authentication

This service pack introduces an enhancement that introduces an authentication class that allows you to configure support for external OAuth providers such as LinkedIn, Facebook, Google+, Twitter, and so on. Social authentication allows external users to access secure resources using their social identity without having to maintain large user stores.

For more information, see [Configuring Social Authentication](#).

1.1.4.2 Persistent Authentication

This service pack introduces an enhancement that introduces an authentication class that helps in saving user session information on the browser after a successful login. When a user is prompted for authentication, this class reuses the information stored in the cookie instead of prompting the user for credentials. The user is prompted for credentials only when the user's password or the cookie lifetime expires.

This authentication class should only be used for applications that do not require very high security.

For more information, see [Configuring Persistent Authentication](#).

1.1.4.3 **TOTP Authenticator**

This service pack introduces an enhancement that helps to configure Google Authenticator Time-Based One-Time Password (TOTP) as a second authentication factor with Access Manager. This method of authentication uses a six-digit number (OTP) in addition to first authentication (for example, username and password), to log into protected services.

For more information, see [Configuring Two-Factor Authentication Using Time-Based One-Time Password](#).

1.1.4.4 **Delete Old User Sessions on Login**

This service pack introduces an enhancement that allows the user to delete the previous user sessions, if the number of open sessions reaches the number of sessions specified in the **Limit User Sessions** field.

For more information, see [Deleting Previous User Sessions](#).

1.1.4.5 **Forceful Deletion of User Sessions**

This service pack introduces an enhancement that helps to forcefully remove all the active sessions associated with an authenticated user in the Identity Server.

For more information, see [Forceful Deletion of User Sessions](#).

1.1.4.6 **Login Redirect URL**

This service pack introduces an enhancement that provides the ability to redirect users to a specific URL after authentication. This option can be used in scenarios where you want users to be directed to a particular home page after successful authentication or want the user to configure a challenge/response question in a password management solution.

For more information, see [Login Redirect URL](#).

1.2 **Code Promotion**

This service pack introduces an enhancement that helps to securely move the configuration data of Access Manager from one environment to another. It allows you to export the configuration data as a password-protected encrypted file. You can then import this file into another Access Manager system and seamlessly replicate the configuration into the target system.

In the Access Manager 4.0 Service Pack 1 release, the Code Promotion feature is enabled by default.

For more information, see [Code Promotion](#).

1.3 **Support for Red Hat Enterprise Linux and Windows Server**

In addition to the platforms introduced in Access Manager 4.0 release, this release adds support for the following operating systems:

- ♦ RHEL 6.5 (Red Hat Enterprise Linux)
- ♦ Windows Server 2012 R2

1.4 Fixed Issues

The following sections outline the issues resolved in this release:

- [Section 1.4.1, “Software Fixes for the Identity Server,” on page 5](#)
- [Section 1.4.2, “Software Fixes for the Access Gateway Service and Access Gateway Appliance,” on page 6](#)
- [Section 1.4.3, “Software Fixes for the Administration Console,” on page 8](#)

1.4.1 Software Fixes for the Identity Server

Following issues are fixed in the Identity Server:

- [Section 1.4.1.1, “Validation Check Fails for Audience Restriction Condition When Two or more SAML 2.0 Service Providers Are Configured with the Same Access Manager Host,” on page 5](#)
- [Section 1.4.1.2, “Single Sign-On to SAML 2.0 Service Provider Fails When SAML 2.0 Assertion Includes LDAP Attributes With Binary Syntax,” on page 5](#)
- [Section 1.4.1.3, “Active Directory Users with an Expired Password Gets Redirected to Password Management URI,” on page 5](#)
- [Section 1.4.1.4, “The Identity Server Does Not Redirect to Target URL After Execution of Post-Authentication Method in SAML 2.0 Federation Setup,” on page 6](#)
- [Section 1.4.1.5, “When an SAML 2.0 Authentication Request Fails, the Error Message Does Not Provide Details,” on page 6](#)
- [Section 1.4.1.6, “Incomplete SAML Authentication Requests Cause High CPU Utilization and Requires Restarting of the Identity Server,” on page 6](#)
- [Section 1.4.1.7, “No Option to Disable Contracts with Equal Levels,” on page 6](#)

1.4.1.1 Validation Check Fails for Audience Restriction Condition When Two or more SAML 2.0 Service Providers Are Configured with the Same Access Manager Host

Issue: If you have configured two or more Access Manager SAML 2.0 service providers with the same Access Manager host, validation check fails for the Audience Restriction condition and therefore the `snamequalifier` attribute should be excluded from `nameidentifier` of the assertion. [Bug 864403]

Fix: In SAML 2.0 Service Provider properties, a new property is added to exclude audience information from a SAML 2.0 assertion. For more information, see [Enabling or Disabling SAML Tags](#).

1.4.1.2 Single Sign-On to SAML 2.0 Service Provider Fails When SAML 2.0 Assertion Includes LDAP Attributes With Binary Syntax

Issue: If the SAML 2.0 assertion includes LDAP attributes with binary syntax (stream) in eDirectory, single sign-on to SAML 2.0 service provider fails. [Bug 864219]

Fix: The Identity Server now sends binary and XML incompatible values with the `xs:base64Binary` datatype in a SAML 2.0 assertion `AttributeStatement`.

1.4.1.3 Active Directory Users with an Expired Password Gets Redirected to Password Management URI

Issue: When an Active Directory user with an expired password logs in to an authentication contract with a Password Expiration servlet configured, the user is redirected to the password management URI. If the Password Management portal is protected by Access Manager, the user is prompted again for authentication and is not permitted to login as the user password has already expired. [Bug 864437]

Fix: With additional configuration in the Identity Server, it is now possible for a user with an expired password to access the protected Password Management Portal. For more information, see [Redirection to Password Management Servlet Protected by Access Gateway When Password Expires](#).

1.4.1.4 **The Identity Server Does Not Redirect to Target URL After Execution of Post-Authentication Method in SAML 2.0 Federation Setup**

Issue: The Identity Server loses the target URL and cannot redirect to the protected resource (or target URL) after execution of post authentication method in a SAML 2.0 federation setup. [Bug 864651]

Fix: The Identity Server redirects to protected resources after execution of the post authentication method.

1.4.1.5 **When an SAML 2.0 Authentication Request Fails, the Error Message Does Not Provide Details**

Issue: In some cases when an service provider's authentication request to the Identity Server fails, a generic error message is displayed even though the reasons for failure might be different. [Bug 860259]

Fix: The `nidp.jsp` file can be modified to customize the error message displayed. You can also customize the `nidp.jsp` file to redirect to a different page when failures occur.

For more information, see [Customizing the nidp.jsp File to Customize Error Messages](#).

1.4.1.6 **Incomplete SAML Authentication Requests Cause High CPU Utilization and Requires Restarting of the Identity Server**

Issue: When the Identity Server receives an incomplete SAML authentication request, it causes the Identity Server to consume high CPU memory and requires a restart. [Bug 860259]

Fix: The wait time the Identity Server waits to completely receive the SAML request is changed from an infinite to a limited time.

1.4.1.7 **No Option to Disable Contracts with Equal Levels**

Issue: For authentication requests, only the requested Identity Server authentication card and higher level authentication cards should be displayed, if **Satisfiable by a contract of equal or higher level** is enabled. [Bug 864228]

Fix: Set the below flag to avoid displaying equal-leveled contracts:

1. Edit `/opt/Novell/nam/idp/webapps/nidp/WEB-INF/classes/nidpconfig.properties` file.
2. Add the following line:

```
HIDE_CARDS_WITH_EQUAL_LEVEL = <Contract Uri>
```

To configure multiple contracts, specify comma separated contract URI.

3. Restart Tomcat.

1.4.2 **Software Fixes for the Access Gateway Service and Access Gateway Appliance**

- ♦ [Section 1.4.2.1, "Form Fill Adds an Extra String if the InPlaceSilentPolicyDoesSubmit Advanced Option Is Enabled," on page 7](#)
- ♦ [Section 1.4.2.2, "Extra Back Slash Added to Web Server Requests Leads to a 404 Error," on page 7](#)
- ♦ [Section 1.4.2.3, "Access Gateway Updates Remain in Pending State After Audit Configuration is Removed," on page 7](#)

- [Section 1.4.2.4, “After Upgrading Access Manager from 3.1 to 4.0, Form Fill Fails If Masked Data Is Enabled,” on page 7](#)
- [Section 1.4.2.5, “Access Requests to Public Resources Are Allowed with a Wrong Host Name,” on page 7](#)
- [Section 1.4.2.6, “The Icache Audit Process on Access Gateway Runs as a Non-Root User After an Unexpected Restart,” on page 8](#)
- [Section 1.4.2.7, “The Access Gateway Does Not Work When Syslog Level Logging to error_log Is Not Enabled,” on page 8](#)
- [Section 1.4.2.8, “After upgrading to 3.2 SP1, Logging out From a Domain Does not Clear the Session,” on page 8](#)
- [Section 1.4.2.9, “When InPlaceSilent Advanced Options are Enabled, Java Script Cannot be Injected Into the Form Fill Auto Submission Policy,” on page 8](#)

1.4.2.1 **Form Fill Adds an Extra String if the InPlaceSilentPolicyDoesSubmit Advanced Option Is Enabled**

Issue: When the `InPlaceSilentPolicyDoesSubmit` global option is enabled on the Access Gateway, an extra string is added and this leads to credential check failure and an unending loop. [Bug 864216]

Fix: The Access Gateway does not add an extra string when the `InPlaceSilentPolicyDoesSubmit` advanced option is enabled.

1.4.2.2 **Extra Back Slash Added to Web Server Requests Leads to a 404 Error**

Issue: The Access Gateway appends Web Server requests with an extra backslash (\) character when the requests have query strings. [Bug 864233]

Fix: The Access Gateway does not add an extra backslash (\) character when the requests have query strings.

1.4.2.3 **Access Gateway Updates Remain in Pending State After Audit Configuration is Removed**

Issue: When audit configuration is changed through Administration Console, the updates remain in pending state. [Bug 865295]

Fix: The configuration changes are saved without any errors.

1.4.2.4 **After Upgrading Access Manager from 3.1 to 4.0, Form Fill Fails If Masked Data Is Enabled**

Issue: While posting data, content-length is set to the amount of data to be post. However, when the masked data option is enabled, after restoring actual data, length of data to be posted is not reevaluated. Therefore, junk characters are sent. [Bug 866322]

Fix: The content length is re-calculated before sending the data to the backend server.

1.4.2.5 **Access Requests to Public Resources Are Allowed with a Wrong Host Name**

Issue: When a http request is made to public resource by using a wrong domain name and then redirected as an https request, Access Manager does not handle **Error on DNS Mismatch** setting and allows access to the resource. [Bug 872745]

Fix: The `NAGErrorOnDnsMismatch` advanced option is added to resolve this issue. For more information, see [Global Advanced Options](#).

1.4.2.6 **The lcache Audit Process on Access Gateway Runs as a Non-Root User After an Unexpected Restart**

Issue: The lcache audit process runs as a root user. But after an unexpected crash, it stops responding to the requests. [Bug 853794]

Fix: The lcache process always runs as a root user and it does not affect responses to the requests.

1.4.2.7 **The Access Gateway Does Not Work When Syslog Level Logging to error_log Is Not Enabled**

Issue: The Access Gateway has performance and stability issues when the proxy is enabled in the verbose mode and errors are reported regularly in the error_log file. [Bug 846388]

Fix: The performance and stability issues are resolved.

1.4.2.8 **After upgrading to 3.2 SP1, Logging out From a Domain Does not Clear the Session**

Issue: If you are on a system that has been upgraded to 3.2 SP1, logging out from a domain does not clear the session cookie. Therefore it is possible to access the last accessed page. [Bug 833848]

Fix: Logging out from the domain clears the session cookie and does not permit access to the last accessed page.

1.4.2.9 **When InPlaceSilent Advanced Options are Enabled, Java Script Cannot be Injected Into the Form Fill Auto Submission Policy**

Issue: If you have enabled the advanced options, InPlaceSilent and InPlaceSilentPolicyDoesSubmit, it is not possible to inject Java scripts into the form fill auto submission policy. [Bug 868840]

Fix: You can now inject Java scripts into the <head> block and at the start of the <Body> block without using the advanced options.

1.4.3 **Software Fixes for the Administration Console**

- ♦ [Section 1.4.3.1, "Authentication Assertion Fails When Encrypt Assertions is Selected," on page 8](#)
- ♦ [Section 1.4.3.2, "Installation/Upgrade fails with an Naudit Certificate Error," on page 8](#)
- ♦ [Section 1.4.3.3, "Upgrading to Access Manager 4.0 from 3.2 that Has Secret Store Configured Results in an NMAS -1642 Error," on page 9](#)

1.4.3.1 **Authentication Assertion Fails When Encrypt Assertions is Selected**

Issue: If you have imported metadata initially by using a URL or text and edited manually, then no authentication assertions are returned in response when **Encrypt assertions** and **Want assertion to be signed** options are selected. [Bug 846558]

Fix: The Administration Console now sends assertions without errors.

1.4.3.2 **Installation/Upgrade fails with an Naudit Certificate Error**

Issue: This issue is seen in situations where Access Manager binaries are mounted from a shared folder on the network. During installation, the files are extracted to the location where the Access Manager binaries are stored. Due to file permission differences, the installation script fails. [Bug 828659]

Fix: The installation binaries are extracted to a temporary folder and therefore the installation proceeds without any errors.

1.4.3.3 Upgrading to Access Manager 4.0 from 3.2 that Has Secret Store Configured Results in an NMAS -1642 Error

Issue: If you attempt to upgrade to Access Manager 4.0 from Access Manager 3.2 that has secret store configured, it results in an error and logging into secret store fails. [Bug 856052]

Fix: Upgrading from a source that has secret store configured proceeds without errors.

2 Installing or Upgrading

After purchasing Access Manager 4.0 Service Pack 1, log in to the [NetIQ Downloads](#) page and follow the link that allows you to download the software. The following files are available:

Table 1 Files Available for Access Manager 4.0 Service Pack 1.

Filename	Description
AM_40_SP1_AccessManagerService_Linux64.tar.gz	Contains the Identity Server, the Administration Console for Linux, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server for Linux.
AM_40_SP1_AccessManagerService_Win64.exe	Contains the Identity Server and the Administration Console for Windows Server 2008 R2 and 2012 R2.
AM_40_SP1_AccessGatewayAppliance_Linux_SLES11_64.iso	Contains the Access Gateway Appliance and the traditional SSL VPN server ISO.
AM_40_SP1_AccessGatewayAppliance_Linux_SLES11_64.tar.gz	Contains the Access Gateway Appliance tar file.
AM_40_SP1_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008 R2 and 2012 R2.
AM_40_SP1_AccessGatewayService_Linux64.tar.gz	Contains the Access Gateway Service tar file.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.0 Service Pack 1, you need to be either on Access Manager 3.2 Service Pack 2 or on Access Manager 4.0

If you are on Access Manager 3.2.x, the supported upgrade paths are:

- ♦ 3.2 Service Pack 2
- ♦ 3.2 Service Pack 2 IR1
- ♦ 3.2 Service Pack 2 IR2
- ♦ 3.2 Service Pack 2 IR3

To upgrade to Access Manager 4.0 Service Pack 1, you must either be on Access Manager 4.0 or any of the Access Manager 4.0 Hotfixes.

For more information on upgrading/migrating Access Manager 4.0, see [NetIQ Access Manager 4.0 SP1 Migration and Upgrade Guide](#).

4 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrading to Access Manager 4.0 Service Pack 1, verify the existing Access Manager version.

- ♦ [Section 4.1, “Verifying Version Number Before and After Upgrading to 4.0 Service Pack 1,” on page 10](#)

4.1 Verifying Version Number Before and After Upgrading to 4.0 Service Pack 1

Before upgrading, it is important to verify the version number of the existing Access Manager components. This ensures that you have the correct version of files on your system.

Refer the following table to determine if you have the correct version installed.

Access Manager Version	Value in the Version field (Access Manager > Auditing > Troubleshooting> Version)
Access Manager 3.2 Service Pack 2	3.2.2.77
Access Manager 3.2 Service Pack 2 IR1	3.2.2.77 + IR1-108
Access Manager 3.2 Service Pack 2 IR2	3.2.2.77 + IR2-117
Access Manager 3.2 Service Pack 2 IR3	3.2.2.77 + IR3-122
Access Manager 4.0	4.0.0-110
Access Manager 4.0 Hotfix 1	4.0.0-110 + HF1-139
Access Manager 4.0 Hotfix 2	4.0.0-110 + HF2-141
Access Manager 4.0 Hotfix 3	4.0.0-110 + HF3-142

After upgrading to Access Manager 4.0 Service Pack 1, verify that the version number of the component is indicated as **4.0.1-88** in the Version field.

5 Known Issues

NOTE: In Access Manager 4.0 Service Pack 1, SSL renegotiation is enabled by default. It is recommended to disable SSL renegotiation to avoid security threats. For more details about disabling this setting, see [SSL Renegotiation](#).

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact [Technical Support](#).

- ♦ [Section 5.1, “Error While Accessing a Protected Resource With a Shared Secret Having a Remote Secret Store,” on page 11](#)
- ♦ [Section 5.2, “After Upgrading From 4.0 to 4.0 SP1, the WS-Trust Service Provider Attributes Sets Have to be Reconfigured,” on page 11](#)

- [Section 5.3, “SAML Token in RSTR Does Not Contain the Attributes if the Selected Attribute is of Type Credential Profile,” on page 11](#)
- [Section 5.4, “Single Sign-On to Box.com Throws An Error About Invalid Namespace,” on page 11](#)
- [Section 5.5, “Upgrading the Primary or Secondary Administration Console to 4.0 SP1 Throws an LDAP Bind Error,” on page 11](#)

5.1 Error While Accessing a Protected Resource With a Shared Secret Having a Remote Secret Store

Issue: If the existing production cluster configuration is overwritten by code promotion and the exported Identity Server cluster is configured to use secret store on a remote LDAP store, attempting to access the protected resource with a shared secret results in an error. [Bug 856240]

Workaround: To resolve this issue, after the code promotion configuration is imported to the production cluster, install the NMAS method. This extends the schema to support secret store on a remote LDAP store.

5.2 After Upgrading From 4.0 to 4.0 SP1, the WS-Trust Service Provider Attributes Sets Have to be Reconfigured

Issue: While upgrading from 4.0 to 4.0 SP1, any attribute sets that are configured for WS-Trust Service Providers are no longer assigned. [Bug 866231]

Workaround: To resolve this issue, configure the Attribute Set and the Authentication Response. For more information, see [Modifying Service Providers](#).

5.3 SAML Token in RSTR Does Not Contain the Attributes if the Selected Attribute is of Type Credential Profile

Issue: If you have defined an attribute set with a Local attribute of type [Credential Profile] in the attribute mapping and configured it to be sent during authentication, the SAML token in the RSTR response does not contain the attribute. [Bug 872016]

Workaround: None

5.4 Single Sign-On to Box.com Throws An Error About Invalid Namespace

Issue: Box.com cannot process the Identity Server response when the user authorization is denied in the SAML 2.0 Service Provider send request. [Bug 879437]

Workaround: None.

5.5 Upgrading the Primary or Secondary Administration Console to 4.0 SP1 Throws an LDAP Bind Error

Issue: Upgrading the primary/secondary Administration Console throws an `ldap_bind : Can't contact LDAP server error`. [Bug 880538]

Workaround: One of the causes of this issue is because the validity of the eDirectory server certificate has expired.

SLES and RHEL servers:

From the eDirectory server terminal execute the following commands:

1. `ndsconfig upgrade` [This creates new certificates for the server]
2. `nldap -u` [This unloads and stops LDAP services]
3. `nldap -l` [This command starts and loads the LDAP services]

After executing these commands, the upgrade will proceed without issues.

Windows servers:

1. Login in to iManager as an administrator.
2. Select **Roles and Tasks > Novell Certificate Server > Repair Default Certificates**
3. Select the server(s) that own the certificates and click **Next**.
4. Select **Yes All Default Certificates will be overwritten** and click **Next**.
5. Review the tasks to be performed and select **Finish**.

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (<mailto:Documentation-Feedback@netiq.com>). We value your input and look forward to hearing from you.

For detailed contact information, see the [Support Contact Information Web site](http://www.netiq.com/support/process.asp#phone) (<http://www.netiq.com/support/process.asp#phone>).

For general corporate and product information, see the [NetIQ Corporate Web site](http://www.netiq.com/) (<http://www.netiq.com/>).

For interactive conversations with your peers and NetIQ experts, become an active member of [Qmunity](http://community.netiq.com/) (<http://community.netiq.com/>), our community Web site that offers product forums, product notifications, blogs, and product user groups.

7 Legal Notice

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

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

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
989 Windows XP Enhanced Cryptographic Provider (RSAENH)
990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
997 Microsoft Windows XP
1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)
1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)
1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)
1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
1006 Windows Server 2008 Code Integrity (ci.dll)
1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)
1008 Microsoft Windows Server 2008
1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
1010 Windows Server 2008 Enhanced Cryptographic Provider
1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

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

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

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

© 2013 NetIQ Corporation. All Rights Reserved.

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