



# NetIQ Advanced Authentication Framework

## **Knowledge Base**

Version 5.1.0

# Table of Contents

	1
Table of Contents .....	2
0001 How to obtain NetIQ debug logs .....	5
0002 Error "You don't have sufficient permissions to perform this operation" .....	6
0003 Enterprise Key Discrediting .....	7
0004 Error Applying License .....	8
0005 Error Obtaining Enterprise Key .....	9
0006 Error Restoring Enterprise Key .....	10
0007 Replica problem in AD LDS (ADAM) configuration .....	11
0008 Freezing of "Preparing to install..." on up to 60 seconds .....	12
0009 How to disable Novell's authentication popup .....	13
0010 Error 17 occurs when using BIO-Key BSP .....	14
0011 BSOD after NetIQ Client installation in case of using Novell .....	15
0012 "Authentication Failed" after disabling the policy "Use domain password as PIN" .....	16
0013 How to find duplicated SPNs .....	17
0014 Error "You do not have sufficient permissions to perform this operation" during loading license .....	18
0015 How to reclaim a license .....	19
0016 How does Authenticore Server discovers work .....	20
0017 Secrets of NetIQ registry settings for Windows Server 2003 .....	21
0018 Reauthentication with ActiveIdentity SecureLogin fails .....	22
0019 Errors during the installation of NetIQ on thin clients running on Windows XP Embedded .....	23
0020 Which port NetIQ uses for communication .....	24
0021 Error "Access is denied" while loading a license file .....	25
0022 The user was not found when logon .....	26
0023 User is able to enroll an authenticator, but can't logon using it .....	27
0024 Error "Could not find Authenticore server" on NetIQ ADUC tab .....	28
0025 Bio-API error during installation .....	29
0026 How often NetIQ will generate a random password for account .....	30
0027 Using RunAs to install the Authenticore Server .....	31
0028 Error "Logon by password was denied" when logon by domain password .....	32
0029 Use authentication providers with own virtual channel .....	34
0030 Location of local cache .....	35
0031 Error extending Active Directory schema .....	36
0032 Operating system freezes after logon by authenticator .....	37
0033 Individual issues with fingerprint authentication .....	38
0034 Recommendations to upgrade the obsolete version .....	39


0035 RADIUS authentication provider doesn't work in disconnected mode .....	40
0036 Delegation of control doesn't work with AD LDS instance on 2008 R2 .....	41
0037 Can't manage authenticators when authenticating by password .....	42
0038 How to configure installation of client components via Group Policies .....	43
0039 How to upgrade NetIQ software via Group Policy with better reliability .....	44
0040 The authentication method doesn't exist in list after installation .....	45
0041 Error when schema extension in configuration with Novell DSfW .....	46
0042 Exception 0xC1020000 when enroll the user using AWA .....	47
0043 How to upgrade NetIQ Client in silent mode .....	48
0044 Missing BIOAPI20.dll error after BIO-Key BSP installation .....	49
0045 Error "The user was authenticated by password" when using NetIQ SDK .....	50
0046 Problem 5012 (DIR_ERROR) during schema extension in case of AD LDS .....	51
0047 Standard Credential Provider after NetIQ Client installation .....	52
0048 "Authentication Failed" during authentication .....	53
0049 Authenticore Server could not create NetIQ.Cipher COM-object .....	54
0050 How to integrate NetIQ with ActivIdentity SecureLogin .....	55
0051 Error "Could not register AuthenticoreService account" .....	56
0052 Don't see NetIQ tab in ADUC .....	57
0053 How to obtain NetIQ Access Manager logs for NetIQ plugin .....	58
0054 One NetIQ component stops working after uninstallation of other .....	59
0055 Error "Could not load the required BioAPI BSP module" .....	60
0056 Requirement of drivers installation for smartcards on Windows 7 .....	61
0057 Error 500 when using Web Service .....	62
0058 Error NetIQ Client is not licensed .....	63
0059 Error "The specified network password is not correct" .....	64
0060 Can't logon using Digital Persona reader .....	65
0061 How DNS Resolves Work .....	66
0062 How to rename an item in the menu of types of authentication .....	67
0063 Empty NSL window after successful authentication using DAS .....	68
0064 Problem with running VDA Profile Editor .....	69
0065 DSfW and Password Filter .....	70
0066 Long delay while authenticating .....	71
0067 Does NetIQ Smartphone Authenticator use the phone number of iOS devices ...	72
0068 Does NetIQ Smartphone Authenticator use the phone number of Android devices .....	73
0069 List of attributes added for NetIQ Advanced Authentication Framework system	74
0070 InvocationTargetException when using NAM AA plugin .....	76
0071 Optimization for NAM AA plugin .....	77
0072 Schema Admin Default Store .....	78
0073 Can't get access to WSDL when using NAM .....	79
0074 Dual authentication using VDA in RDP .....	80
0075 NetIQ authentication at an RDP logon .....	81

---

<b>0076 Long delay while using RTE via Web Service .....</b>	<b>82</b>
<b>0077 No BIO-key settings available in Group Policy .....</b>	<b>83</b>
<b>0078 Using HTTPS in Smartphone Authentication Provider .....</b>	<b>84</b>
<b>0079 Slow performance when using AD LDS .....</b>	<b>85</b>
<b>0080 Deploying NetIQ in eDirectory without AD .....</b>	<b>86</b>
<b>0081 Could not log in as AuthenticoreService .....</b>	<b>87</b>
<b>0082 Initialization error while using Digital Persona .....</b>	<b>88</b>
<b>0083 Lock screen is not supported with user tile screen .....</b>	<b>89</b>
<b>0084 Restart of ClientHelperService service .....</b>	<b>90</b>
<b>0085 Juniper VPN and NetIQ .....</b>	<b>91</b>
<b>0086 How to use authentication via Web Service on a client .....</b>	<b>92</b>
<b>0087 Dynamic RPC cannot be enabled in the domain .....</b>	<b>93</b>
<b>0088 Biometrics and RDP .....</b>	<b>94</b>
<b>0089 Default domain name for SMS authentication in AWA .....</b>	<b>95</b>
<b>0090 Impossible to scan a QR code from laptop .....</b>	<b>96</b>
<b>0091 Authenticore Server was not found while Web Enrollment Wizard authentication .....</b>	<b>97</b>
<b>0092 Error "Can't enroll device: the remote server returned an error: NotFound" on Smartphone .....</b>	<b>98</b>
<b>0093 Test page is not loaded while checking Voice Call AP Server .....</b>	<b>99</b>
<b>0094 Smart card or smart card reader doesn't work inside VMware Workstation .....</b>	<b>100</b>
<b>0095 Web Enrollment Wizard cannot be installed because of ASP.NET 4.5 .....</b>	<b>101</b>
<b>0096 How to use ADMX on Windows Server 2003 .....</b>	<b>102</b>
<b>0097 How to configure AuthenticoreService account with minimal permissions .....</b>	<b>103</b>
<b>0098 HTTP Error 500.19 while checking Voice Call Server .....</b>	<b>104</b>
<b>0099 Logon to Citrix via Microsoft Network Policy Server .....</b>	<b>105</b>
<b>0100 Delay before logon after hibernation .....</b>	<b>106</b>


## 0001 How to obtain NetIQ debug logs

To obtain logs, use **LogCollector** tool that is located in the **\Tools\LogCollector** subfolder of NetIQ distributives.

 Please note, the tool may not work from a network drive.

To obtain logs:

1. Copy **LogCollector.exe** to the local C:\ disk on the faulty computer.
2. Run **LogCollector.exe**.
3. Click **Enable** in the **Debug logs collector** window. As a result, all items in the **Debugged components** section will be selected. Close the window.
4. Reproduce the steps that caused the problem.
5. Run **LogCollector.exe** again and click **Save logs**.
6. Save logs to archive.
7. Click **Disable** after obtaining logs.

 If you have the issue that involves the NetIQ server components or maybe have a network connection cause, please obtain logs from all depending machines (for example, NetIQ Authenticore Server and workstation with NetIQ Client).

## 0002 Error “You don’t have sufficient permissions to perform this operation”

### **Description:**

Authenticore Server tray icon is red. After starting the server, the following error appears:

*You don't have sufficient permissions to perform this operation. Please make sure that you (a) are the member of Authenticore Admins group and (b) have administrator privileges on this PC/server.*

### **Solution:**

Besides (a) and (b) please check that at least one Domain Controller is available.

## 0003 Enterprise Key Discrediting


### Description:


The current Enterprise Key has been discredited.

### Solution:

If Enterprise Key is discredited, follow the steps below:

1. Stop all Authenticore servers.
2. Use one of the servers to generate a new Enterprise Key. After the Key has been generated, start the server.
3. Start other Authenticore servers. Obtain the Enterprise Key on each of them.

 After a new Enterprise Key has been generated, all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the **NetIQ** tabs in ADUC snap-in.

 If new enterprise key is generated to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

## 0004 Error Applying License

**Description:**

The selected license is not applied, the error message is displayed.

**Cause:**

- a. The term specified in the license has expired;
- b. The domain name specified in the license does not match the current domain name;
- c. The current number of licensing objects exceeds the limit specified in the license;
- d. The license file is corrupted.

**Solution:**

Check the license details and contact the support service.



## 0005 Error Obtaining Enterprise Key

### **Description:**

The current Enterprise Key cannot be obtained. The error message is displayed:

*Could not obtain Enterprise Key*

*Could not find Authenticore server or establish connection with it.*

### **Cause:**

- a. The Authenticore server is not connected to the network.
- b. Additional Authenticore servers were being restarted or stopped while attempting to obtain the Key.
- c. Attempting to obtain the current Enterprise Key on the only Authenticore server in domain. This is needless.

### **Solution:**

- a. Check whether there is another working Authenticore server in the domain.
- b. Check whether all Authenticore servers are available in the network.
- c. Check whether the Domain Controller is available.

## 0006 Error Restoring Enterprise Key

### **Description:**

The Enterprise Key is not restored from the backup copy. The error message is displayed:

*Could not import Enterprise Key. Authenticore Server will be stopped. In case of Authenticore Server startup, the current Enterprise Key will be used.*


*Data is corrupted.*


### **Cause:**

- a. You have mistyped the password while importing the Key from the backup copy.
- b. The backup copy file is corrupted.

### **Solution:**

- a. Retype the password and retry.
- b. If the Enterprise Key was lost and cannot be restored, generate a new one.

 After a new Enterprise Key has been generated, all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the NetIQ tabs in ADUC snap-in.

 If a new Enterprise Key is generated to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

## 0007 Replica problem in AD LDS (ADAM) configuration

### **Description:**

NetIQ is working correctly, but we are having issues with AD LDS replica. The Event log on the Primary server is getting loaded with Warnings stating:

*The attempt to establish a replication link for the following writable directory partition failed.*

It is also getting another error:

*The directory server has failed to create the AD LDS serviceConnectionPoint object in Active Directory Lightweight Directory Services.*

*This operation will be retried.*

### **Solution:**

The information from this topic indicates that the Instance Service is using a local user instead of a Domain user. That is not accurate. However, it is using Network Service as the user, which seemed like it should have been correct. This is the case on both the Primary and Replica server. Please change this user to the \Administrator and the error will go away.

If you get other errors after it, please add Generate Audit rights to that user and also add it to the Domain Administrators Group, and restart the service. Please do it on the all servers you are using.

## 0008 Freezing of “Preparing to install...” on up to 60 seconds

**Description:**

I get freezing of step “Preparing to install...” on up to 60 seconds.

**Solution:**

Ensure that you have an active online connection. The installation is trying to verify the digital signature of product.

## 0009 How to disable Novell's authentication popup

### **Description:**

We have successfully finished the installation of NetIQ solution and now users can logon using the biometry or cards.

But we also want to disable the additional Novell's authentication popup.

### **Solution:**

You need to put Novell GINA in passive mode and enable NDSLogin in silent mode. If you also need scripts to run, then you need to add an extra key. Check the following webpage for GINA and this webpage for CP to get the detailed information.

## 0010 Error 17 occurs when using BIO-Key BSP

### **Description:**

We are using the BIO-Key BSP. We can't access the fingerprint reader due to an error 17.

### **Solution:**

1. Ensure that your device is properly connected to your PC/notebook. Check that the device is working correctly using Device Manager.
2. Ensure that you are using a compatible socket. Many of devices are not tested with USB 3.0, and requires more transfer speed that USB 1.0/1.1 has.
3. If you are using Windows Vista or newer: Many of authentication devices has two sets of drivers:
  - a. Drivers downloaded via Windows Update service automatically. These drivers do not have any third party interfaces and are highly limited as to their functions.
  - b. Drivers distributed by authentication device producer.

Remove the drivers downloaded via Windows Update using Device Manager and install the drivers distributed by authentication device producer.

4. If you are using the drivers distributed by authentication device producer, check whether third party services are started and are working correctly. E.g.: Authentec service may be set to "manual" by default.

Some of such driver software can contain test utilities. Ensure that device is working correctly using such third party test utilities.

## 0011 BSOD after NetIQ Client installation in case of using Novell

### **Description:**

We use Novell ZCM at workstations. After NetIQ Client installation on some laptops we got blue screen with an error stating that the "Winlogon Process terminated unexpectedly", the error code is 0xC0000005. If we uninstall the NetIQ Client, everything returns to normal.

### **Solution:**

Please use this fix from Novell: <http://www.athasas.com/download/novell-gina-bsod-fix/>

## 0012 “Authentication Failed” after disabling the policy “Use domain password as PIN”

### **Description:**

After disabling group policy “Use domain password as PIN” Card authenticators are not available.

### **Solution:**

It is not allowed to change this policy after cards have been enrolled. You need to re-enroll the authenticators or enable the policy.



## 0013 How to find duplicated SPNs

**Question:**

How I can find duplicated Service Principal Names?

**Answer:**

You can use SetSPN tool from Microsoft Windows Server 2008 R2. Just run it as:

"SetSPN -x" to find duplicates in the current domain or

"SetSPN -x -f" to find duplicates in the entire forest.

## 0014 Error “You do not have sufficient permissions to perform this operation” during loading license

### Description:

I got an error message: “You do not have sufficient permissions to perform this operation.”...

### Solution:


Logged-in user must be a member of the Authenticore Admins Group. Verify that the logged-in user is a member of this group, or a member of a group belonging to the Authenticore Admins Group.

If you do not see this group in CN=Users:

Security Groups and Group membership are not created/assigned during installation on Windows domain operating at Windows 2000 domain functional level(s).

Complete the following steps to create Security Groups and assign Group membership:

1. Open Active Directory Users and Computers.
2. Browse to the Users container.
3. Create a Global Security Group named “Authenticore Admins”.
4. Assign users and groups to administer Authenticore Server, ensuring that your user account is a member of this group.
5. Create a Global Security Group named “NetIQ Advanced Authentication Framework Admins”.
6. Assign users and groups to administer/enroll Advanced Authentication users, ensuring that your user account is a member of this group.
7. Verify that the service account, “AuthenticoreService” exists and is a member of Domain Admins.
8. Reboot server.

 Refer to your Domain Administrator if Universal, Global, or Local Domain group is required for your domain/forest. This will only affect your ability to add another group (such as Domain Admins or Enterprise Admins) to this new security group.

## 0015 How to reclaim a license

### Description:

How is license reclaimed after a user is deleted from AD or a machine is taken down? Is there an additional tool for this?

### Solution:

When unchecking the option **User can use NetIQ Authentication Providers** from the NetIQ tab in ADUC or the NetIQ User Viewer the license gets reclaimed automatically.



The user license becomes unavailable when you delete user from AD without preliminary unchecking the option **User can use NetIQ Authentication Providers**.

## 0016 How does Authenticore Server discovers work

### **Question:**

How does the NetIQ Client discover to which NetIQ Authenticore Server to connect?

### **Explanation:**

The server discovery flow is this:

1. The Client looks into the Authenticore Servers group.
2. Then the Client selects a random server from that group which belongs to the same AD site as the client PC.
3. The Client tries to establish RPC connection with the Authenticore Server on given Server.
4. If the Server is operable, Client caches it and continues to work with it.
5. If it is down, Client gets another Authenticore server from the list which belongs to the AD site and continues from step #3.
6. If there are no servers belonging to the site, the client will try to connect to the servers from another site.

For more information on how to setup Active Directory Sites check the [following technet article](#).

## 0017 Secrets of NetIQ registry settings for Windows Server 2003

Consider the key HKEY\_LOCAL\_MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework\gina

It has the following values:

- DefaultUsername – the last user name used to unlock the computer;
- DefaultDomainName – the last domain used to unlock the computer;
- SelectedMode – the last authentication provider GUID used during logon;
- SelectedModeLocked – the last authentication provider GUID used during unlock;
- ModeType – the last logon method id (0 – authentication provider, 1 – password);
- ModeTypeLocked – the last unlock method id (0 – authentication provider, 1 – password);
- PassThrough – stored setting of “Use current settings as defaults” checkbox on logon dialog;
- PassThroughLocked – stored setting of “Use current settings as defaults” checkbox on unlock dialog.

## 0018 Reauthentication with ActivIdentity SecureLogin fails

**Description:**

Cannot perform re-authentication using ActivIdentity SecureLogin.

**Solution:**

Ensure that NSL version 7.0.1 Hotfix 4 or later is installed on the PC. Ensure that NMA5NCP.DLL is present in %SystemDirectory%, if the file is not present, contact us to request the file(s).

## 0019 Errors during the installation of NetIQ on thin clients running on Windows XP Embedded

### **Description:**

Errors during the installation NetIQ Client when installing on thin client running on Windows XP Embedded: during installation you receive errors starting the NAAF Log Broker Service; either user does not have permissions, or a dependent service cannot be started.

### **Solution:**

Officially we don't support Windows XP Embedded, but you can try to install NetIQ on it at your own risk.

NetIQ Client automatically (mandatory) installs the Client Logging components. This is the only NetIQ Client component that is installed as a service. The NAAF Log-Broker Service dependencies include the Remote Procedure Call (RPC) Locator Service, which may appear in the Services list on Windows XP Embedded with startup type = Manual.

Confirm that you can start this service in the Services.msc console. If you receive an error that the file is not found, then you must locate manually and copy the file "Locator.exe" into the C:\Windows\System32\ directory. As most thin clients do not provide Windows XP Embedded installation media, it may be necessary to copy the Locator.exe from a standard Windows XP system. Ensure that the Service Pack level of the Windows XP system is equal to, or newer than the XP Embedded system.

Once you have copied "Locator.exe" into the C:\Windows\System32 directory, attempt to start the RPC Locator Service manually.

If successful, retry installation of the NetIQ Client.

## 0020 Which port NetIQ uses for communication

**Question:**

Which ports are used for the communication between NetIQ components?

**Answer:**

NetIQ uses the Microsoft RPC protocol to communicate. This protocol uses port 135. The port can be changed with the RPCCfg.exe support tool from Microsoft.

For more information, check [this Microsoft KB article](#).



## 0021 Error “Access is denied” while loading a license file

### **Description:**

We get an error “Access is Denied” error while trying to load NetIQ license.

### **Solution:**

NetIQ license data is stored in Active Directory Schema within the “bioLicenses” attribute of the domain object (i.e. dc=domain, dc=com or domain.com).

Write permissions for this attribute are configured, by default, for Domain Admins security group.

While installing the first NetIQ Authenticore Server, several security groups and a service account are created. The created AuthenticoreService account requires Domain Admin privileges in order to write data to the “bioLicenses” attribute.

The AuthenticoreService account may lack the required permissions to write the license data to this attribute.

Verify that the AuthenticoreService account belongs to the Domain Admins security group, restart the Authenticore Server Service, then re-run the license tool from the system tray icon.

## 0022 The user was not found when logon

### **Description:**

When I try to authenticate to logon OS freezes on more than 1 minute, then I get the error: "The user was not found"

### **Solution:**

Check DCs and DNS Server availability.

## 0023 User is able to enroll an authenticator, but can't logon using it

### **Description:**

User is able to enroll authenticator, but cannot logon using it.

### **Solution:**

NetIQ requires an appropriate authentication provider(s) to be installed and registered on Authenticore Servers in order to match enrolled authenticator. Ensure that an appropriate authentication provider is installed on every NetIQ Authenticore Server.

If the authentication provider does appear to be installed on the Authenticore Server, then it is possible that registration of the it was not successful.

1. Open RegBSP11.exe tool from \Tools\BioAPI\_20\_Framework\ subfolder of the NetIQ distributive kits. Check that all authentication providers modules from left panel is registered and exist at the right panel. Register necessary modules manually when needed.
2. Uninstall and re-install the authentication provider from the NetIQ distributive kits. Reboot the Authenticore Server.

## 0024 Error “Could not find Authenticore server” on NetIQ ADUC tab

### Description:

I see the error “Could not find Authenticore server” on NetIQ tab in Active Directory Users and Computers.

### Solution:

1. Check whether the NetIQ Authenticore Server is started.
2. Check whether the NetIQ Authenticore Server is not locked by firewall.
3. Check whether the NetIQ Authenticore Server exists as a member of Authenticore Servers group.
4. Check whether the NetIQ Authenticore Server exists as a member of NetIQ Advanced Authentication Framework ADAM Servers group in case of using ADAM or AD LDS.
5. Run the following command to check the availability of AD from the command line:  
`nltest /server: <servername> /dsgetsite`. The site's name should be returned.

## 0025 Bio-API error during installation

### **Description:**

Bio-API error during installation, "Probably you must reboot your machine" (Workstation or Server).

### **Solution:**

1. Occasionally, network based installations will fail with a BioAPI error, and state that a reboot may be required. Copy the installation media on local disk and re-run the installation program.
2. Microsoft C++ re-distributables and/or runtime components are not present on the machine.

## 0026 How often NetIQ will generate a random password for account

### **Description:**

We need to know where and how to set the number of days before NetIQ will generate a random password.

### **Solution:**

To understand how often password generation occurs, let's consider an example:

These are default domain policy settings: Maximum password age = 42 days, Interactive logon: Prompt user to change password before expiration = 14 days.

So user's password will be changed after  $42 - 14 = 28$  days (for GINA) after last changing (this is a time when notification message about expiring password begins to appear in case when you are not using the random passwords), and after 42 days (for CP).

## 0027 Using RunAs to install the Authenticore Server

### Question:

Can I use RunAs to launch "Autorun.exe" to install NetIQ Authenticore Server or do I need to be logged in to the server as a Domain Administrator?

### Answer:

While installing the first Authenticore Server on the domain, it is recommended that you logon as a Domain Administrator.

You may use RunAs when launching "Autorun.exe" if required, however you may need to validate that security groups and server accounts are created in Active Directory.

Domain.com/Users

- NetIQ Advanced Authentication Framework Admins – by default, the Domain Admins security group should be members;
- Authenticore Admins – by default, the Domain Admins security group should be members;
- AuthenticoreService – this account must belong to Domain Admins security Group.

You may also run the individual .msi installer files from a command prompt using "msiexec.exe /a"

Subsequent Authenticore Servers may be installed using RunAs. The installing user must be a member of the Authenticore Admins security group.

## 0028 Error “Logon by password was denied” when logon by domain password

### **Description:**

Authorization Error “Logon by password was denied” when logging in with domain password.

### **Solution:**

Please first of all check whether the logon by password is allowed for the user on NetIQ tab in Active Directory Users and Computers. This also checks that the NetIQ data in directory is not corrupted for the user.

If you are presented with an error, verify other user objects are not affected by repeating the steps above. Once confirmed that the error seems to only affect a particular user, then it is almost certain that the user’s data has become corrupt and should be recreated.

Manually delete NetIQ data for the user via ADSI Edit MMC Snap-in.

1. Connect to the user object in ADSI Edit by selecting, then right-clicking on ADSI Edit beneath the Console Root.
2. Select “Connect To”.
3. In the Connection Settings Dialog, look for the “Connection Point” section, then select the radio button labeled “Select or type a Distinguished Name or Naming Context.”.
4. Supply your DN Path information, such as “DN=parentdomain,DC=childdomain,DC=com” or “DC=domain,DC=com”, etc.
5. Supply any additional configuration information as may be required by your directory.
6. Click “OK” and allow your directory objects to populate the right window pane.
7. Browse to the affected user object.
8. Select Right Click the affected user object and select “Properties”.
9. Select, press “Edit”, then press “Clear” on each of the following attributes:
  - a. bioAuthenticationSet;
  - b. bioCustom;



- c. bioSubsystemLicense;
- d. bioUserPassword;
- e. bioUserSettings.

10. Now you have cleared the data for this user.

11. Verify that you may now Access the user from the NetIQ User Viewer MMC Snap-in or NetIQ tab in Active Directory Users and Computers.

12. Reset any policies that may have been cleared.

13. Enroll the user, or have the user self-enroll from the NetIQ Client.

## 0029 Use authentication providers with own virtual channel

### **Description:**

How to enable an authentication provider on Citrix with its own virtual channel? This way the NetIQ terminal client doesn't need to be installed on the thin clients.

### **Solution:**

On the Citrix server go to the registry key corresponding the bsp:

```
HKEY_LOCAL_MACHINE\SOFTWARE\BSP\{XXXX}
```

where {XXXX} is a long format

Add the following DWORD value:  
"TSAware" with value "1"

This should disable the check if the NetIQ Terminal Client and authentication providers are installed on the Citrix clients.

## 0030 Location of local cache

**Description:**

What is the location of the NetIQ cache files?

**Solution:**

By default, user cache (including cached authenticators) is located in the %AllUsersProfile%\Application Data\NetIQ\NetIQ Advanced Authentication Framework\Cache\Userdata folder.

## 0031 Error extending Active Directory schema

### Description:

Error occurs while extending AD schema, or returns "Unsuccessful".

### Solution:

Please check the following:

- i. For Windows Server 2003 before extending schema domain functional level should be raised to Windows Server 2003.
- ii. Before extending schema please ensure that you have Remote Server Administration Tools installed on the server. Otherwise you may have a problem with Idifde.exe
- iii. Ensure that you are running the schema updates on the Schema Master and that the logged in user is a member of the Schema Admins Group.

To identify the Schema Master

1. Run the Active Directory Schema MMC Snap-In. Please note that you may need to add this snap-in manually if it does not appear in Administration Tools program folder.
2. Right-Click on "Active Directory Schema" directly under Console Root.
3. Select "Operations Master..." from the menu
4. The current Schema Master will be displayed in the window.
5. Connect to the server identified, and re-run the schema extension tools.

If these steps are unsuccessful, you may need to extend the schema manually from a command line using the Idifde.exe command.

### Example:

Open a command prompt in the Tools\Schema\AD folder located in the distributive kits.

```
ldifde -i -f ExtendSchema.ldf -s DomainController.Domain.Com -c DC=X DC=D-Domain,DC=Com -k -v
```

repeat command for ExtendSchema\_2.ldf, ExtendSchema\_3.ldf, ExtendSchema\_4.ldf and RegisterMMC.ldf files using the same parameters above.

## 0032 Operating system freezes after logon by authenticator

### **Description:**

My OS freezes after logon by authenticator.

### **Solution:**

1. Try to unplug your authentication device.
2. Some kind of software (DLP software) may block USB devices, so try to configure them or uninstall them.

## 0033 Individual issues with fingerprint authentication

### **Description:**

One employee of our company has a problem with fingerprint authentication by correct finger.

### **Solution:**

The cause of the problem may be in physiological characteristics of the human (dry skin, body temperature). If you have a problem with authentication by correct finger, it is recommended to breath on the finger before authentication when your skin is very dry OR wipe your finger before authentication in case of very wet skin.

## 0034 Recommendations to upgrade the obsolete version

### **Description:**

We have NetIQ version 4.0 installed. Yesterday we got the latest release. How could we update our software with saving user's authenticators and other NetIQ settings.

### **Solution:**

We recommend you to update server and administration components at first. If you are using biometry, workstations with old versions of our components will be still working correctly. Then you can update client components. Unfortunately we don't support updating of old client components without preliminary uninstallation of old ones. So you need to uninstall once old components at first.

Also we recommend to use standard group policy feature for the bulk installation and next updating of components in form of msi installers.

## 0035 RADIUS authentication provider doesn't work in disconnected mode

**Description:**

RADIUS authentication provider doesn't work in disconnected mode.

**Solution:**

As designed. RADIUS authentication provider doesn't support authentication by cached authenticators.



## 0036 Delegation of control doesn't work with AD LDS instance on 2008 R2

### **Description:**

While delegation of control I get the error: "The templates could not be applied. One or more of the templates is not applicable. Click Back and select different templates, and then try again".

My configuration: AD LDS, Windows Server 2008 R2.

### **Solution:**

As designed. Delegation of control works only with AD repository in this OS version.

## 0037 Can't manage authenticators when authenticating by password

### **Description:**

I can't manage authenticators when I am authenticated by password.

### **Solution:**

If you are trying to manage authenticators, please authenticate by authenticator, not by password. Authenticator management will be denied when you have one or more enrolled authenticators, and you authenticate by password. It has a security reason: passwords are more weak and less secure than authenticators.

## 0038 How to configure installation of client components via Group Policies

### Description:

How to configure installation of client components via group policies.

### Solution:

1. Open Active Directory Users and Computers.
2. Create Global Security group (installation group).
3. Create Group Policy object (GPO).
4. Link created group with GPO.
  - a. Open GPO properties.
  - b. Go to Security tab.
  - c. Remove Apply Group Policy option for Authenticated Users group.
  - d. Add created group and mark Apply Group Policy option for it.
5. Add MSI package to shared network folder.
6. Open package properties:
  - a. Go to Deployment tab.
  - b. Remove option Uninstall this application when it falls out of the scope of management.
  - c. Press Advanced button.
  - d. Set option Ignore language when deploying this package.
  - e. Remove option Make this 32-bit X86 application available to Win64 machines (only for 32-bit packages).
7. Add computers to installation group.
8. Wait for applying policy (maybe some hours) or make it in hand mode: `gpupdate /force`.
9. Reboot computers to complete installation\*.

\* Sometimes we need to reboot the operating system twice, here you can see explanation of it.

## 0039 How to upgrade NetIQ software via Group Policy with better reliability

### Description:

We have 500+ workstations with NetIQ installed in domain. I want to update client components to a new version. But I'm afraid of simultaneous upgrade of all workstations. What I need to do?

### Solution:

You are right when you worry about simultaneous upgrading.

1. If your employees begin to work at the same time, it will cause increase of load on server where new distributive is shared.
2. We recommend to upgrade workstations gradually. It means that you select several workstations (it can be 5-10 workstations or 1-2% of workstations with different hardware and software configurations) which will be upgraded at first. You upgrade them, then you watch them during a week. So if all is right after a week, you can upgrade 20-30% of workstations. Then you watch them during next week again. After that you can upgrade the rest workstations.

This approach provides reliable upgrading.

How could you do it in practice:

1. You create new installation group and new Group Policy Object (GPO), add a new MSI package in it, [see it in details](#).
2. After step 6.5 you must go to Upgrades tab.
3. Press Add button.
4. In Add Upgrade Package dialog please select A specific GPO option.
5. Select a GPO which was used for installation of previous NetIQ version.
6. Select MSI package name.
7. Select option Uninstall the existing package, then install the upgrade package.

Also make sure that you new GPO is above than old in a GPO list.

## 0040 The authentication method doesn't exist in list after installation

### Description:

The new authentication provider was installed on workstation. But I don't see it in logon methods list.

### Solution:

1. Make sure that you have rebooted workstation after authentication provider was installed on it.
2. Use RegBSP11.exe utility from folder \Tools\BioAPI\_20\_Framework\ of NetIQ distributives: check existence of this authentication provider in BioAPI 2.0 Component Registry list.
3. Find a node for your authentication method here: HKEY\_LOCAL\_MACHINE\SOFTWARE\BSP\{XXXX} and try to set value "1" in TSAware parameter.

## 0041 Error when schema extension in configuration with Novell DSfW

### **Description:**

Our domain is based on Novell DSfW. When I extend the schema for AD LDS, after the 5th [Enter] I got the error:

*Microsoft VBScript runtime error: The remote server machine does not exist or is unavailable: 'GetObject'*

### **Solution:**

This is not a bug. You got this error, because this part of schema extension is for Active Directory, but you have Novell DSfW instead of Active Directory.

## 0042 Exception 0xC1020000 when enroll the user using AWA

### **Description:**

We have an issue with the AWA and enrollment. When I try to enroll the user I get an exception 0xC1020000. Btw: we are using AD-LDS.

### **Solution:**

Open the following folder at the Authenticore Server: %ProgramFiles%\NetIQ\NetIQ Advanced Authentication Framework\ .

Then execute: `schemaadmin.exe -import DefaultSchema .`

## 0043 How to upgrade NetIQ Client in silent mode

### **Description:**

How can we upgrade NetIQ Client manually in silent mode?

### **Solution:**

You can use the following command at Client msi folder (it can be a local or a network folder):  
`msiexec /i client.msi /q .`

But first of all you will need to close all programs because installation will restart the workstation automatically.

P.S. msiexec also has `/norestart` parameter, but if you will use it, you will have to restart workstation manually.



## 0044 Missing BIOAPI20.dll error after BIO-Key BSP installation

### **Description:**

After BIO-Key authentication provider was installed I got an error of missing BIOAPI20.dll.

### **Solution:**

Ensure that you already installed NetIQ Client or NetIQ Authenticore Server or NetIQ Administrative Tools or NetIQ RTE. At least one of these components must be installed before BIO-Key BSP.

## 0045 Error “The user was authenticated by password” when using NetIQ SDK

### **Description:**

I get the error “The user was authenticated by password” while reading the information from a record for user without enrolled authenticators.

### **Solution:**

This error is by design. The field “password” in PasswordStore subsystem is not available if user logged on by domain password.

## 0046 Problem 5012 (DIR\_ERROR) during schema extension in case of AD LDS

### **Description:**

During schema extension I got an error:

"Specified operation failed with ldap error:  
000020D6: SvcErr: <SOMEID>, problem 5012 (DIR\_ERROR), data 0. Operations Error. The system cannot open the device or file specified."

We are using AD LDS. What do I need to do?

### **Solution:**

Please check the following:

1. You have already configured the Repository and ADAM Settings policies in Group Policy Management Console according technical documentation (check the NetIQ Administrative Tools – Administrator's Guide).
2. The policies were successfully applied on the server you are using (you can check it using `gpresult /r`).
3. The Partition name in AD LDS instance matches the LDAP path to root element in ADAM Settings policy.
4. The LDAP port number in AD LDS instance matches the ADAM servers port number in ADAM Settings policy.
5. The LDAP port that you are using is free and unlocked.
6. You have inputted the correct Server name (AD LDS), Port and Root partition in NetIQ Schema Extender.

## 0047 Standard Credential Provider after NetIQ Client installation

### **Description:**

I'm using Windows 7. After the NetIQ Client was successfully installed I restarted the computer. But after pressing Ctrl+Alt+Del I see the standard prompting of password without any NetIQ references and without any way to select another authentication type. I can enroll the authenticator after logon using NetIQ credentials application from Control Panel.

### **Solution:**

1. Please open the NetIQ folder with CredentialProvider.dll at Program Files and register this dll manually: `regsvr32 CredentialProvider.dll`
2. Ensure that you don't have the software that can block the third-party credential providers. It can be any DLP software.

## 0048 “Authentication Failed” during authentication

### Description:

When I try to authenticate in workstation an error “Authentication Failed. Press OK and try again” appears.

### Solution:

Please do the following:

1. Ensure that you have enabled option "User can use NetIQ Authentication Providers" on user's tab in ADUC and have at least one enrolled authenticator.
2. Logon using your password;
3. Right click on NetIQ Client tray icon, select Support;
4. Go to the Servers tab;
5. Ensure that everything is Okay with each of yours NetIQ Authenticore Servers;
6. Ensure that you have all necessary NetIQ Authentication Providers installed on each server;
7. Ensure that you have the same version of NetIQ Authenticore Servers and all necessary NetIQ Authentication Providers on all servers.
8. Check that everything is Okay on the other workstations (with different OS versions)
9. Check the firewall settings on your workstation and servers.
10. Try to reset existing authenticators and re-enroll them.
11. In case of using RFIDEas readers please download [pcProxConfig util](#) and on *Advanced* tab of it set option *Enable quite mode for usage with the Software developer's Kit*.
12. Run the following command to check the availability of AD from the command line:  
`nltest /server: <servername> /dsgetsite`. The site name should be returned.

## 0049 Authenticore Server could not create NetIQ.Cipher COM-object

### **Description:**

We installed an additional Authenticore Server, but it returns an error:

*Could not start Authenticore Server service*

*Error: Authenticore server could not create NetIQ.Cipher COM-object. Either the object was not registered in the process of system installation or it could not get the Enterprise Key”.*

### **Solution:**

You will need to import your existing Enterprise Key on the new server. This key was generated during configuring of the first NetIQ Authenticore Server and likely has an enk extension. You can import it doing the following: Right-click the Authenticore Tray Manager icon and select Enterprise Key > Restore key. Then press Enter to confirm the action. Please specify the path to your existing Enterprise Key.

If you lost the key, you would need to generate the new key and import it on all existing NetIQ Authenticore Servers. Please note you'll lose all existing authenticators and other NetIQ settings in this case.

## 0050 How to integrate NetIQ with ActivIdentity SecureLogin

### **Description:**

How to integrate NetIQ with ActivIdentity SecureLogin?

### **Solution:**

NetIQ provides a customized module (plugin) which is utilized by SecureLogin to deliver the functionality of authentication and re-authentication using NetIQ. The plugin can be downloaded from [NetIQ Resource Center](#).

To integrate NetIQ with ActivIdentity SecureLogin, create ExtAuthModule string param with <Absolute path>\ASASAuth.dll

where, <Absolute path> is the location where you have saved ASASAuth.dll.

To enable kiosk mode, create NSLADAUTH dword param with value "1" in HKEY\_LOCAL\_MACHINE\SOFTWARE\Protocom\SecureLogin .

## 0051 Error “Could not register AuthenticoreService account”

### **Description:**

After generating an Enterprise key I got an error:

*Could not register AuthenticoreService account. I discovered that this user doesn't exist.*

### **Solution:**

1. Create a user AuthenticoreService manually;
2. Uninstall the Authenticore Server;
3. Reboot;
4. Install the Authenticore Server;
5. Generate an Enterprise key;
6. Reboot.



## 0052 Don't see NetIQ tab in ADUC

### Description:

I can't find NetIQ tab of user properties in Active Directory Users and Computers.

### Solution:

1. Please ensure that you have NetIQ Administrative Tools component installed on this server.
2. Ensure that ADUC was closed during installation. Please try to uninstall it, restart the machine and install it again.
3. Try to open ADUC using cmd: dsa.msc
4. Check the existence of registry nodes: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MMC\Snapins\{A1AC2E83-2C4A-4200-A875-170F728152C0} and HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MMC\NodeTypes\{bf967aba-0de6-11d0-a285-00aa003049e2}. If no, please collect the MSI logs: msixec /i "installname".msi /l\*v "full-path-to-the-logfile".
5. Check the existence of NetIQ tab in user's properties in NetIQ UserViewer MMC.
6. Look for any errors in Event Viewer after opening of ADUC.
7. Create a [new ticket](#) and describe what you did and what you got on all of these actions in details.

## 0053 How to obtain NetIQ Access Manager logs for NetIQ plugin

To enable NetIQ Access Manager logs please do the following:

1. Open NetIQ Access Manager web console: <https://<NAMServer-Path>:<NAMServerPort>/nps/>.
2. Follow the menu: **Devices – Identity Servers – IDP-Cluster**.
3. In the **General** tab open the **Logging** menu.
4. Set the following options:
  - **File logging**: Enabled;
  - **Echo to console**: Enabled;
  - Set **Application** and **Liberty** Component File Logger Levels to **debug**.
5. Click **Apply**, then **OK**.
6. Switch to the menu: **Devices – Identity Servers**.
7. In the **Identity Servers** list, click **Update All** for **IDP-Cluster**.
8. Update all configurations. Wait until **Status** becomes **Current**.
9. Switch to the menu: **Devices – Access Gateways**.
10. In the **Access Gateways** list click **Update All** for **AG-Cluster**.

Then reproduce the issue again.

To obtain the logs:

1. Open NetIQ Access Manager web console: <https://<NAMServer-Path>:<NAMServerPort>/nps/>.
2. Follow the menu: **Auditing- General Logging**.
3. Check log `/var/opt/novell/nam/logs/idp/tomcat/catalina.out` in Identity Servers group.
4. Also copy full URL string from browser.

## 0054 One NetIQ component stops working after un-installation of other

**Description:**

After uninstallation of one NetIQ component and restarting the machine, other NetIQ component stopped working.

**Solution:**

Please repair the remaining NetIQ components from *Programs and Features*.

## 0055 Error “Could not load the required BioAPI BSP module”

### **Description:**

I successfully enrolled authenticator, but can't authenticate using it because of the error:

*Could not load the required BioAPI BSP module.*

### **Solution:**

The error “Could not load the required BioAPI BSP module” appears in case when the authentication provider was installed on workstation, but workstation has not been restarted after this installation.

1. So please first of all ensure that workstation has been restarted after provider's installation.
2. Ensure that authentication providers was successfully installed on this workstation.

## 0056 Requirement of drivers installation for smart-cards on Windows 7

### **Description:**

Each time when I put on a card on a reader, I see the message about driver installation for a card. I have Windows 7.

### **Solution:**

This is a feature of Windows 7. It is called Smartcard Plug and Play. Check [how to disable it](#). Scroll down to "Disable Smart Card Plug and Play through Group Policy for managed computers".

## 0057 Error 500 when using Web Service

### Description:

I get a 500 response using Web Service:

```
s:-      1056964604      System.Runtime.InteropServices.COMException      Sys-  
tem.Runtime.InteropServices.COMException -1056964604 Exception from HRESULT:  
0xC1000004
```

### Solution:

When authentication failed we always have error. We have this error documented in Web Service Administrator Guide. 0xC1000004L means LOGON\_E\_WRONG\_AUTHENTICATOR . So please ensure that you use a valid authenticator.

## 0058 Error NetIQ Client is not licensed

### **Description:**

Can't install NetIQ Client due to error:

*NetIQ Advanced Authentication Framework – Client is not licensed.*

### **Solution:**

Starting from version 4.8 NetIQ requires a licensing of separate components.

- Please ensure that you updated NetIQ Authenticore Server to the latest release
- Ensure that you got and have applied a license for 4.8+
- Ensure that this workstation is joined to the domain
- Please try to disable firewall or configure permissions for TCP 135 and ports for Dynamic RPC (for detailed information please check MSDN) on NetIQ Server and NetIQ Client, and then try again.

## 0059 Error “The specified network password is not correct”

### **Description:**

A user gets the following error during logon:

*The specified network password is not correct.*

### **Solution:**

- Please ensure that the computer is joined to the domain.
- Check that DNS works fine on this computer.
- Sync the time between Authenticore Server and computer.
- Ensure that you have NetIQ Password Filter installed on all DCs.
- How many users have this issue? If only one or some, try to reset password for them.



## 0060 Can't logon using Digital Persona reader

### **Description:**

We use Digital Persona readers with BIO-Key BSP, but we see white square when trying to authenticate on Windows 7.

### **Solution:**

We can get the Digital Persona readers working but not in UILess mode. So the user will have to enter their username, select fingerprint and then press the arrow. This will bring the BIO-Key BSP in the foreground and the DP reader will work.

To achieve this remove (or rename) the UILessModule REG\_SZ setting from HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\BSP\{EC4AC729-B969-6E46-BD2F-56B6055E18F8} (x64) or HKEY\_LOCAL\_MACHINE\SOFTWARE\BSP\{EC4AC729-B969-6E46-BD2F-56B6055E18F8} (x86).

## 0061 How DNS Resolves Work

For more information about DNS resolution, go to <http://support.microsoft.com/kb/2834226>

Check [the following article](#) for more information about Forwarders and Conditional Forwarders resolution timeouts.

You can also review the following articles:

<http://blogs.technet.com/b/stdqry/archive/2011/12/02/dns-clients-and-timeouts-part-1.aspx>

<http://blogs.technet.com/b/stdqry/archive/2011/12/15/dns-clients-and-timeouts-part-2.aspx>

## 0062 How to rename an item in the menu of types of authentication

### **Description:**

After the installation of BIO-key and Lumidigm authentication providers on the same workstation, the Fingerprint method of authentication is displayed two times in the Type drop-down menu.

### **Solution:**

To rename an item, open the following registry path `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BSP\GUID` and rename FrName parameter point.

## 0063 Empty NSL window after successful authentication using DAS

### **Description:**

I use DAS in NetIQ Secure Login with Advanced Authentication plugin. After the successful authentication I see an empty window of NetIQ Secure Login. Then request of authentication repeats.

### **Solution:**

Please ensure that:

- you use NSL 8.0 and higher.
- you didn't miss AD authentication part in actions.xml. This is where DAS knows what to do after a successful authentication.

## 0064 Problem with running VDA Profile Editor

### **Description:**

After the launch of VDA Profile Editor, the following error is displayed:

*No plugins were found.*

### **Solution:**

Select all files in the VDA Profile Editor folder, open their Properties and click the Unblock button in the General tab.

## 0065 DSfW and Password Filter

### **Question:**

If a customer uses DSfW would the Password Filter still be required on Domain Controllers? If we used DSfW and pointed NetIQ Advanced Authentication Framework to that what issues might we encounter?

### **Description:**

The Password Filter is a Windows Server component. You can't install it on a SUSE server. When a password is changed without a Password Filter then password can get out of sync and the user needs to get it in sync again using NetIQ Client.

## 0066 Long delay while authenticating

### **Question:**

I have prepared simple test environment with Windows Server 2012 and Windows 8 client. When authenticating just using a password now it takes 15 seconds on the " " screen. Why is it taking such a long time? This is a very simple environment with 1 server and 1 client.

### **Description:**

In our debug logs we see that in your situation we spend 15 seconds on server side in reverse DNS lookup (we need to know name of client PC). So you can fix it by creating reverse lookup DNS zone.

## 0067 Does NetIQ Smartphone Authenticator use the phone number of iOS devices

### **Question:**

Does NetIQ Smartphone Authenticator use the phone number of iOS devices? Is there an enrollment or can it use the AD attribute for mobile device?

### **Description:**

The phone number is not used by NetIQ Smartphone Authenticator. It is possible to use the device without SIM card. NetIQ Smartphone Authenticator uses Apple Push Notification ID (APN ID). All devices are registered in APN ID and are given a unique ID (32-bit array). Using this ID our proxy-server defines the device to which the message should be sent. This ID is saved in AD.



## 0068 Does NetIQ Smartphone Authenticator use the phone number of Android devices

### **Question:**

Does NetIQ Smartphone Authenticator use the phone number of Android devices? Is there an enrollment or can it use the AD attribute for mobile device?

### **Description:**

The phone number is not used by NetIQ Smartphone Authenticator. After the first launch of NetIQ Smartphone Authenticator on the mobile device, ID is automatically generated to AD. Dispatcher receives supplementary data – GCM (Google Cloud Messaging) ID. The device ID and GCM ID are linked in the internal database of Dispatcher.

## 0069 List of attributes added for NetIQ Advanced Authentication Framework system

The list of attributes added for NetIQ Advanced Authentication Framework system:

### **bioBioUser**

Active Directory object: User

Type: Integer

Description: Indicates that the user is allowed to use hardware authentication devices.

### **bioCustom**

Active Directory object: User

Type: Octet string

Description: Stored additional user data (used in NetIQ Advanced Authentication Framework extensions and NetIQ Advanced Authentication Framework SDK).

### **bioAuthenticationSet**

Active Directory object: User

Type: Octet string

Description: Stores the list of user authentication.

### **bioUserSettings**

Active Directory object: User

Type: Octet string

Description: Stores NetIQ Advanced Authentication Framework user settings.

### **bioUserPassword**

Active Directory object: User

Type: Octet string

Description: Stores Active Directory user password (encrypted with Enterprise Key).

### **bioSubsystemLicenses**

Active Directory object: User

Type: Octet string

Description: Stores information about NetIQ Advanced Authentication Framework extensions.

### **bioCacheEnable**

Active Directory object: Computer

Type: Integer

Description: Indicates that authenticators caching is allowed on the computer.

**bioLicenses**

Active Directory object: Domain

Type: Octet string

Description: Stores the list of licenses.

**bioSchemes**

Active Directory object: Domain

Type: Domain

Description: Stores the information about server extensions.

## 0070 InvocationTargetException when using NAM AA plugin

It is not recommended to install Java Runtime Environment 7.0 Update 45 due to the problem (<https://forums.oracle.com/thread/2594401>).

## 0071 Optimization for NAM AA plugin

Starting with Java Runtime Environment 7.0 Update 25 there is an option that impacts the performance. To optimize the performance of NAM AA Plugin, it is required to switch off the option for trusted networks. This option impacts the performance of any applet.

After the start of any applet Java Runtime Environment connects to the Internet for certificate revocation check. To disable certificate revocation checks, open the Java Control Panel, switch to Advanced tab, select the Do not check radio button from the Perform certificate revocation checks on menu.

To switch off only online certificate revocation check, deselect the Online Certificate Status Protocol (OCSP) and the Both CRLs and OCSP from the Check for certificate revocation using menu.

The detailed setting of certificate revocation check is available on [http://java.com/en/download/help/revocation\\_options.xml](http://java.com/en/download/help/revocation_options.xml).

## 0072 Schema Admin Default Store

If user's custom data should be saved while using SDK, then it is required to execute in advance the SchemaAdmin - import Default Schema command to import default password store in the subsystem. The SchemaAdmin utility is installed together with Authenticore Server. It is located in %ProgramFiles%\NetIQ\NetIQ Advanced Authentication Framework.

## 0073 Can't get access to WSDL when using NAM

### Question:

I have no NAM appliance, I have only IDP server on Linux. While loading of NAM authentication page, I get an error: *Failed to access the WSDL at https://<FQDNofWebService>:8232/Service.svc?wsdl.*

### Solution:

1. Try to disable firewall or create a rule to enable HTTPS on port 8232.
2. Check ping of WebService from IDP Server.
3. Add FQDNofWebService to /etc/hosts on IDP Server.

## 0074 Dual authentication using VDA in RDP

### **Question**

Using NetIQ VDA we should authenticate twice: first one is VDA's pre-session authentication, second one is authentication inside RDP session.

### **Solution**

To refuse the additional RDP authentication just disable filtering for Microsoft CP using our group policies settings. You need to do it for pass-through logon.



## 0075 NetIQ authentication at an RDP logon

### Question:

Do you know if it is possible to require an NetIQ authentication at an RDP logon?

The use case is:

- admin logs into PC/laptop;
- admin attempts RDP connection to server;
- RDP challenge appears (replaced by AAA - OTP challenge);
- admin supplies OTP and is authenticated.

The client is unable to predict the PC/laptop the admin might use. Therefore any agent at the remote connecting point would not be effective. It requires a change to the servers that are being accessed.

### Solution:

There are 2 ways to solve this without installing extra software on client devices:

1. Use RADIUS authentication with the RD Gateway and have it authenticate to a NPS server with the NAAF plugin installed. You can use this thread: [http://www.experts-exchange.com/OS/Microsoft\\_Operating\\_Systems/Server/Windows\\_Server\\_2008/Q\\_27092309.html](http://www.experts-exchange.com/OS/Microsoft_Operating_Systems/Server/Windows_Server_2008/Q_27092309.html)
2. Install NAAF client on the Terminal server(s) and authenticate when a user hits the session.

## 0076 Long delay while using RTE via Web Service

### Question:

While using RTE connected to Web Service, we have 10 seconds delay after presenting card and PIN before authentication.

### Solution:

It can happen due to missing internet connection on RTE side. It is trying to check server certificate. You can follow one of the following ways:

- how to disable CRL checking on machine: **Control Panel -> Internet Options -> Advanced -> Under security**, clear the **Check for publisher's certificate revocation** check box.
- how to disable CRL checking for a specific .NET application: check the Microsoft article: <http://support.microsoft.com/kb/936707>.

## 0077 No BIO-key settings available in Group Policy

### Question:

We have no BIO-key settings in Group Policy. Windows Server 2003.

### Solution:

In **Group Policy Management Editor** you should enable showing of preferences. To do it:

1. Launch **Group Policy Management Editor**.
2. Select **Administrative Templates**.
3. Right click and select the **View\Filtering...** menu item.
4. Clear the **Only show policy settings that can be fully managed** check box.
5. Click **OK**.

## 0078 Using HTTPS in Smartphone Authentication Provider

### **Question:**

Is it possible to use HTTPS in Smartphone Authentication Provider?

### **Solution:**

HTTPS is supported only for interaction between Smartphone Authentication Provider and Dispatcher. To enable HTTPS support, it is necessary to install server certificate on server with the installed Smartphone Dispatcher and then add thumbprint of this certificate to the option `HttpsCertThumbprint` in the file `Sa.Dispatcher.exe.config`.

However the RPC will be much faster and it uses security/authentication features embedded in Active Directory.

For smartphones HTTPS is not supported because not all smartphone devices support it.

## 0079 Slow performance when using AD LDS

### **Question:**

When using AD-LDS, it takes about 3 seconds to bind to the AD-LDS instance. It results in slow performance.

### **Solution:**

Add IP address with hostname of AD LDS in the hosts file on Authenticore Servers.

## 0080 Deploying NetIQ in eDirectory without AD

### **Question:**

We use eDirectory. How can we deploy NetIQ on LDS without AD?

### **Solution:**

We always need an Active Directory because it is used for permissions, transport, encryption, etc. This Active Directory can either be Native AD, DSfW or Samba4. While using AD-LDS, we only do not store credentials in Active Directory, but store them in the AD-LDS instance, but we still need Active Directory.

If you cannot use DSfW, then it should work if you were able to sync the eDir users and passwords with AD (Native or Samba4) and then have AD-LDS as data storage. But again we currently can not work with LDS without AD.

In version 5.0 we plan to implement a completely new Server which will not be dependent on AD.

## 0081 Could not log in as AuthenticoreService

### Question:

I cannot start the NetIQ Server. The following error is displayed:

Could not start Authenticore Server service. Error is described in Event Log.  
Could not log in as AuthenticoreService.

Possible error causes:

- there is no AuthenticoreService account in the domain;
- account password and AuthenticoreService account unsynchronized;
- AuthenticoreService account was automatically blocked;
- AuthenticoreService account does not have "batch job" logon privileges on this computer.

### Solution:

The problem can be solved in the following ways:

- please check that the AuthenticoreService account still exists;
- if you have changed password for it, please reset password to the previous one;
- set "Password never expires" for AuthenticoreService account;
- click the Authenticore Server tray icon -> Enterprise Key -> Restore key... -> restore key from existing enk file.

## 0082 Initialization error while using Digital Persona

### **Question:**

Sometimes I get initialization error while using Digital Persona.

### **Solution:**

Please wait 30 seconds and try to authenticate again. Sometimes user can lock the session on authentication screen and in 30 seconds that authentication screen will be closed automatically.



## 0083 Lock screen is not supported with user tile screen

### Question:

We have found that lock screen is not shown in user tile screen (Windows 8).

### Solution:

It can be fixed in two ways:

#### 1. Disable the lock screen:

- Open registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization
- Create a new DWORD parameter "NoLockScreen" and set it to 1 to disable the lock screen.

#### 2. Enable secure lock screen:

- Secure lock screen requires Ctrl+Alt+Del to go to next screen (or presenting card).
- Open registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- Create a new DWORD parameter "DisableCAD" and set it to 0 to enable secure sign-in.

## 0084 Restart of ClientHelperService service

**Question:**

When we restart NetIQ Advanced Authentication Framework - ClientHelperService, device events stop working.

**Solution:**

It is a normal behavior. Please restart the workstation.

## 0085 Juniper VPN and NetIQ

### **Question:**

We are using Juniper VPN. Does NetIQ have a document with information on how to configure authentication in it?

### **Solution:**

For Juniper VPN it is just normal Radius configuration. Configure NPS as the Radius server and your Juniper VPN as the Radius client. It should be documented in Juniper administrator's guide.



## 0086 How to use authentication via Web Service on a client

### Question:

How to use authentication via Web Service on a client?

### Solution:

1. Create the registry keys in product key on workstation:
  - IsWSLogon=1 to enable logon via webservice
  - WebAuthServer="https://<webserviceaddress>:<webserviceport>/Service.svc/bsc"
2. Restart the workstation

-  A first logon will be long, because we need to have IIS and .NET elements started.
-  Authenticators' enrollment is not supported in this case.

## 0087 Dynamic RPC cannot be enabled in the domain

### **Question:**

Dynamic RPC cannot be enabled in the domain. According to security policies dynamic RPC cannot be used. What can be done in such case?

### **Solution:**

Please, configure the RPC static port selection allowed policy.

## 0088 Biometrics and RDP

### Question:

Is it possible to have my laptop reader or a USB reader attached and authenticate via RDP to a remote system?

### Solution:

It is possible to perform 2 actions with RDP sessions:

1. **Pre-session authentication using VDA.** This will authenticate you to Web Service and then push your credentials in the RDP client (also it works for Citrix and VMware).
2. **In-session authentication.** It is required to install the client component (and only terminal client component is required) and the Authentication Provider locally. Then the RTE (or client) inside the RDP session should be installed. This way the device will be visible inside the RDP session.

## 0089 Default domain name for SMS authentication in AWA

### Question:

How is it possible to configure the usage of default domain name for SMS authentication in AWA? By default it is required to enter domain name in the Username textfield every time during web authentication.

### Solution:

1. Open the web.config file in AWASMS.
2. Specify your domain name instead of <default domain name>:

```
<appSettings>  
<add key="defaultDomain" value="<default domain name>"/>
```

## 0090 Impossible to scan a QR code from laptop

**Question:**

I'm not able to scan a QR code from my laptop.

**Solution:**

Please, connect the laptop to power adapter or increase a contrast of laptop's screen.



## 0091 Authenticore Server was not found while Web Enrollment Wizard authentication

### Question:

During authentication using Web Enrollment Wizard the following error occurs: "*Could not find Authenticore Server*".

### Solution:

The following error occurs when none of Authenticore Servers could be accessed. The problem can be solved in the following ways:

- Check whether at least one Authenticore Server (from the Authenticore Server group in CN=Users in Active Directory) is running and firewall tools don't block an interaction.
- Open the following folder at the Authenticore Server:  
%ProgramFiles%\NetIQ\NetIQ Advanced Authentication Framework\  
Then execute: schemaadmin.exe -import DefaultSchema.

## 0092 Error “Can't enroll device: the remote server returned an error: NotFound” on Smartphone

### **Question:**

While scanning the QR code, the following error is displayed: “Can't enroll device: the remote server returned an error: NotFound”. Unlike <localhost>:8757, <localIPAddress>:8757 and <publicIPAddress>:8757 cannot be accessed in browser, even though access is being checked on the same server.

### **Solution:**

Probably you have configured the Direct Access on the server. Please, remove the feature and try again.

## 0093 Test page is not loaded while checking Voice Call AP Server

### **Question:**

The test page is not loaded while checking the functioning of Voice Call Authentication Provider Server.

### **Solution:**

1. Check whether URL that is entered in the browser's navigation bar contains the Voice Call Authentication Provider Server port that corresponds to the specified port in the registry.
2. Ensure that Web Server (IIS) server role was installed before the installation of .NET Framework.

## 0094 Smart card or smart card reader doesn't work inside VMware Workstation

### Question:

Smart card or smart card reader doesn't work inside VMware workstation.

### Solution:

VMware Workstation has 2 modes of assigning smart card readers in virtual machines:

- Shared mode;
- USB Passthrough mode.

By default, the shared mode is enabled. If smart card or smart card reader doesn't work inside VMware workstation, it is required to disable the shared mode. For more information on how to disable the shared mode, check the following article: <http://pubs.vmware.com/workstation-10/index.jsp?topic=/com.vmware.ws.using.doc/GUID-78E5618F-BD2D-4169-91A4-8FDDCD4C823B.html>.

## 0095 Web Enrollment Wizard cannot be installed because of ASP.NET 4.5

### Question:

I am not able to install the Web Enrollment Wizard because the installer shows an error about missing ASP.NET 4.5.

### Solution:

Please check the following:

1. Ensure that you have installed Microsoft .NET Framework 4.5
2. Please turn ON Server Roles -> Web Server (IIS) -> Application Development -> ASP.NET (4.5)
3. Try to do the following:
  - uninstall ASP.NET  
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet\_regiis.exe -u
  - install ASP.NET back  
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet\_regiis.exe -i

## 0096 How to use ADMX on Windows Server 2003

### **Question:**

How is it possible to use ADMX on Windows Server 2003? Normally ADMX can be used only from Windows Server 2008.

### **Solution:**

For more information on how to use ADMX on Windows Server 2003, check the following article: [http://technet.microsoft.com/en-us/library/cc748955\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc748955(v=ws.10).aspx).

## 0097 How to configure AuthenticoreService account with minimal permissions

### Question:

We don't want to add the AuthenticoreService account to Domain Admins and other admins groups. What are the minimal necessary permissions?

### Solution:

AuthenticoreService account should be in Account Operators group because it should be able to reset and change user passwords. Also AuthenticoreService should be in Server Operators group because it should have local admins group permissions and the group doesn't exist on DC. On the other hand we forbid the installation of Authenticore Server on DCs. So local admins permissions should be enough.

Please, also delegate Authenticore Admins necessary permissions for bioLicense attribute:

1. Open **Active Directory Users and Computers**.
2. Click **View** and select **Advanced Features**.
3. Right-click the domain object. The **Properties** window will be displayed.
4. Click the **Security** tab.
5. Click the **Advanced** button.
6. Click the **Add** button in the **Permissions** tab of the **Advanced Security Settings** window.
7. Select principal object type.
8. Enter the object name. Click **OK**.
9. Click **Manage permission entries** in the **Advanced Security Settings** window.
10. Click the **Object** tab in the **Permission Entry** window.
11. Select **This object only** from the **Apply to** drop-down list.
12. Click the **Properties** tab in the **Permission Entry** window.
13. Scroll down and check the **Read bioLicenses** and the **Write bioLicenses** boxes .
14. Click **OK** to close all dialog boxes.

## 0098 HTTP Error 500.19 while checking Voice Call Server

### **Question:**

While checking the functioning of Voice Call Server, I am getting the following error: "*HTTP Error 500.19 - Internal Server Error*".

### **Solution:**

Probably Microsoft .NET Framework was installed before Web Server (IIS) server role. It is required to use the tool [http://msdn.microsoft.com/en-us/library/k6h9cz8h\(v=vs.80\).aspx](http://msdn.microsoft.com/en-us/library/k6h9cz8h(v=vs.80).aspx) to register .NET Framework in IIS or to reinstall .NET Framework.



## 0099 Logon to Citrix via Microsoft Network Policy Server

### Question:

How to configure Citrix Web Interface to work with Microsoft Network Policy Server?

### Solution:

The following link will be helpful to configure the common side: <http://support.citrix.com/article/CTX125063/?supportcase=true>.

As a result, you should have the following settings on Citrix Web Interface :

1. Restrict access to the required domain:
2. Select the required credential format:
3. Specify Radius server addresses (in order):
4. XenApp Web Site will be successfully added:

Then you just need to install NetIQ NPS plugin on the Microsoft Network Policy Server and configure its policy (see the [NPS Logon Method Selection](#) chapter of the NPS Plugin - Administrator's Guide).

## 0100 Delay before logon after hibernation

**Question:**

While using offline logon, there may occur a lengthy delay before logon after hibernation.

**Solution:**

If there are used VMware virtual network adapters, there should be disabled 802.11 authentication in their parameters.