



NetIQ Advanced Authentication Framework

Knowledge Base

Version 5.1.0

Table of Contents

	1
Table of Contents	2
NetIQ Advanced Authentication Framework v4	6
0001 How to obtain NetIQ debug logs	6
0002 Error "You don't have sufficient permissions to perform this operation"	7
0003 Enterprise Key Discrediting	8
0004 Error Applying License	9
0005 Error Obtaining Enterprise Key	10
0006 Error Restoring Enterprise Key	11
0007 Replica problem in AD LDS (ADAM) configuration	12
0008 Freezing of "Preparing to install..." on up to 60 seconds	13
0009 How to disable Novell's authentication popup	14
0010 Error 17 occurs when using BIO-Key BSP	15
0011 BSOD after NetIQ Client installation in case of using Novell	16
0012 "Authentication Failed" after disabling the policy "Use domain password as PIN"	17
0013 How to find duplicated SPNs	18
0014 Error "You do not have sufficient permissions to perform this operation" during loading license	19
0015 How to reclaim a license	20
0016 How does Authenticore Server discovers work	21
0017 Secrets of NetIQ registry settings for Windows Server 2003	22
0018 Reauthentication with ActiveIdentity SecureLogin fails	23
0019 Errors during the installation of NetIQ on thin clients running on Windows XP Embedded	24
0020 Which port NetIQ uses for communication	25
0021 Error "Access is denied" while loading a license file	26
0022 The user was not found when logon	27
0023 User is able to enroll an authenticator, but can't logon using it	28
0024 Error "Could not find Authenticore server" on NetIQ ADUC tab	29
0025 Bio-API error during installation	30
0026 How often will NetIQ generate a random password for account	31
0027 Using RunAs to install the Authenticore Server	32
0028 Error "Logon by password was denied" when logon by domain password	33
0029 Use authentication providers with own virtual channel	35
0030 Location of local cache	36
0031 Error extending Active Directory schema	37
0032 Operating system freezes after logon by authenticator	38
0033 Individual issues with fingerprint authentication	39
0034 Recommendations to upgrade the obsolete version	40
0035 RADIUS authentication provider doesn't work in disconnected mode	41
0036 Delegation of control doesn't work with AD LDS instance on 2008 R2	42
0037 Can't manage authenticators when authenticating by password	43
0038 How to configure installation of client components via Group Policies	44
0039 How to upgrade NetIQ software via Group Policy with better reliability	45

0040 The authentication method doesn't exist in list after installation	46
0041 Error when schema extension in configuration with Novell DSfW	47
0042 Exception 0xC1020000 when enroll the user using AWA	48
0043 How to upgrade NetIQ Client in silent mode	49
0044 Missing BIOAPI20.dll error after BIO-Key BSP installation	50
0045 Error "The user was authenticated by password" when using NetIQ SDK	51
0046 Problem 5012 (DIR_ERROR) during schema extension in case of AD LDS	52
0047 Standard Credential Provider after NetIQ Client installation	53
0048 "Authentication Failed" during authentication	54
0049 Authenticore Server could not create NetIQ.Cipher COM-object	55
0050 How to integrate NetIQ with ActiveIdentity SecureLogin	56
0051 Error "Could not register AuthenticoreService account"	57
0052 Don't see NetIQ tab in ADUC	58
0053 How to obtain NetIQ Access Manager logs for NetIQ plugin	59
0054 One NetIQ component stops working after uninstallation of other	60
0055 Error "Could not load the required BioAPI BSP module"	61
0056 Requirement of drivers installation for smartcards on Windows 7	62
0057 Error 500 when using Web Service	63
0058 Error NetIQ Client is not licensed	64
0059 Error "The specified network password is not correct"	65
0060 Can't logon using Digital Persona reader	66
0061 How DNS Resolves Work	67
0062 How to rename an item in the menu of types of authentication	68
0063 Empty NSL window after successful authentication using DAS	69
0064 Problem with running VDA Profile Editor	70
0065 DSfW and Password Filter	71
0066 Long delay while authenticating	72
0067 Does NetIQ Smartphone Authenticator use the phone number of iOS devices	73
0068 Does NetIQ Smartphone Authenticator use the phone number of Android devices	74
0069 List of attributes added for NetIQ Advanced Authentication Framework system	75
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
0076 Long delay while using RTE via Web Service	82
0077 No BIO-key settings available in Group Policy	83
0078 Using HTTPS in Smartphone Authentication Provider	84
0079 Slow performance when using AD LDS	85
0080 Deploying NetIQ in eDirectory without AD	86
0081 Could not log in as AuthenticoreService	87
0082 Initialization error while using Digital Persona	88
0083 Lock screen is not supported with user tile screen	89
0084 Restart of ClientHelperService service	90
0085 Juniper VPN and NetIQ	91

0086 How to use authentication via Web Service on a client	92
0087 Dynamic RPC cannot be enabled in the domain	93
0088 Biometrics and RDP	94
0089 Default domain name for SMS authentication in AWA	95
0090 Impossible to scan a QR code from laptop	96
0091 Authenticore Server was not found while Web Enrollment Wizard authentication	97
0092 Error "Can't enroll device: the remote server returned an error: NotFound" on Smartphone ..	98
0093 Test page is not loaded while checking Voice Call AP Server	99
0094 Smart card or smart card reader doesn't work inside VMware Workstation	100
0095 Web Enrollment Wizard cannot be installed because of ASP.NET 4.5	101
0096 How to use ADMX on Windows Server 2003	102
0097 How to configure AuthenticoreService account with minimal permissions	103
0098 HTTP Error 500.19 while checking Voice Call Server	104
0099 Logon to Citrix via Microsoft Network Policy Server	105
0100 Delay before logon after hibernation	106
0101 Authenticore Server (NAAFRS) could not be installed during Authenticore Server upgrade ..	107
0102 Cannot install Authenticore Server on a domain controller	108
0103 RD Web is not protected by AWA	109
0104 Error "Could not register AuthenticoreService account. Either user data or the Enterprise Key is corrupt"	110
0105 Device is not registered in Apple Network Service	111
0106 Cannot log in to Web Enrollment Wizard using Internet Explorer	112
0107 Authentication fails while using VDA Shell in the Kiosk mode	113
0108 After 10 authentication attempts by YubiKey I am no longer able to logon	114
0109 Error "Could not load type 'System.ServiceModel.Activation.HttpModule'" after the Voice Call Server upgrade	115
0110 After swiping the finger there is delay about 3-4 seconds	116
0111 The request timed out on smartphone	117
0112 Push notification wasn't received on iOS device during authentication	118
0113 Client can authenticate to Authenticore Server from another AD site for the first time	119
0114 After the upgrade of Authenticore Server, Administrative Tools and other components are not upgraded	120
0115 Error "Failed to resolve user name. Check spelling and try again" while using VDA Shell	121
0116 NetIQ Group Policies are not displayed in Group Policy Management Console	122
0117 Error "You don't have rights for changing settings on this page. Please, ensure that these rights are delegated to you."	123
0118 How to change default logo in Web Enrollment Wizard	124
0119 Enterprise Key is damaged	125
0120 Device events don't work when presenting or removing a smartcard	126
0121 Error: "Value cannot be null. Parameter name: Waithandle array may not be empty."	127
0122 How to restore quick remote access after NetIQ Client installation	128
0123 Error 0xe06d7363 when using NPS plugin	129
0124 How to configure the Citrix USB redirection for BIO-key AP in case of XenDesktop	130
0125 How to configure FAR/FMR in BIO-key AP	131
0126 SecuGen Hamster IV does not work with BIO-key	132
0127 How to integrate RSA with Citrix Netscaler in the NetIQ framework	133


0128 How to prevent dual authentication request in case terminal mode is used	134
0129 Cannot log in using linked account	135
0130 How to make Yubikey OATH HOTP option invisible in WEW	136
0131 Error "Could not register AuthenticoreService account. Could not get access to ADAM server"	137
0132 How to configure Remote Desktop Services with NetIQ Advanced Authentication Framework	138
0133 How to create Security Groups and AuthenticoreService account manually	148
0134 OATH OTP AP installation rolls back without error message	149
0135 Smartphone Dispatcher service cannot be started	151
0136 How to enable visualization of Windows boot process	152
0137 Error "Incorrect username/password" when trying to authenticate to NetScaler	153
0138 BIO-key AP can't be installed/upgraded on Windows Server 2012 R2	155
0139 SecuGen Hamster doesn't work with the BIO-key AP	156
0140 Error "Windows could not start the Authasas Advanced Authentication - Authenticore Server on Local Computer"	157
0141 Low quality swipe fingerprint sensors	158
0142 Upgrading BIO-key Pin BSP v1.0.44 and earlier	159
0143 Fingerprint reader driver error (Subcode -101 -UFS_ERR_NO_LICENSE)	160

NetIQ Advanced Authentication Framework v4

The aim of this chapter is to provide you with complete and detailed solutions for the known issues of NetIQ Advanced Authentication Framework v4.


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.
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. Reboot your computer.
2. Ensure that your device is properly connected to your PC/notebook. Check that the device is working correctly using Device Manager.
3. 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.
4. 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.

5. 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.authasas.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?

Answer:

The server discovery flow is the following for NetIQ Advanced Authentication Framework v4.10 R3:

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](#).

For NetIQ Advanced Authentication Framework v4.11 the workflow is the following:

1. Client goes to the last Authenticore Server, if:
 - Client is in the same AD site as the Authenticore Server
 - Client has authenticated not less than 8 hours ago (it is configured using the [Last used server timeout](#) policy)
2. Otherwise Client connects to the random Authenticore Server from its AD site.
3. If there are no Authenticore Servers in the Client's AD Site or they are not available, Client goes to the Authenticore Server from the **Master server list** (if the [Master server](#) is enabled and Authenticore Servers are added to the **Master server list**). Master servers can used no matter in which AD site they are located.
4. If Master servers are not available, Client goes to other servers outside its AD site (if the **Forbid the client to go outside its AD site checkbox** is not selected in the [Master server](#) policy).

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 will NetIQ generate a random password for account

Description:

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

Solution:

The random password option is intended for the situation when a user should not know his/her password. When this option is enabled for the user and the user doesn't have enabled authenticators, a random password will not be generated. If the user enrolls a new authenticator, a random password will be generated by Authenticore Server during next user's login, if it doesn't contradict to system settings (the User cannot change password option of the Minimum password age policy).

Example 1: The administrator has created a user, enabled random password and enrolled authenticator for him, Minimum password age = 1. It means that the password will be changed the next day during logon. Also a random password will be re-generated the next time the user usually gets a system message about the necessity to change the password in several days.

Example 2: The policy settings are the following: Maximum password age = 42 days, Interactive logon: Prompt user to change password before expiration = 14 days. It means that the 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 password), 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, DN=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\Wow6432Node\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

Question:

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.

```
Idifde -i -f ExtendSchema.ldf -s DomainController.Domain.Com -c DC=X  
DC=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

Question:

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

Question:

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 do 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

Question:

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

Question:

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: `nlttest /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

Question:

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 NSLDAUTH 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: `msiexec /i "installname".msi /l*v "fullpaththellogfile"`.
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://<NAMServerPath>:<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://<NAMServerPath>:<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 uninstallation 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 smartcards 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
System.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 the error: *NetIQ Advanced Authentication Framework – Client is not licensed.*

Solution:

1. You should perform the installation under a domain user with local admins privileges.
2. Try to disable a firewall on the Authenticore Server and the client.
3. Check members of the Authenticore Servers group in AD. It should contain only Authenticore Servers.
4. Please ensure that Authenticore Servers are working (you should see a green tray icon), try to restart them via the tray icon.
5. Ensure that you have a valid license via Authenticore Server tray menu.

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\{C5F0DED2-4463-490D-9CBA-02BBE3402218} (x64) or HKEY_LOCAL_MACHINE\SOFTWARE\BSP\{C5F0DED2-4463-490D-9CBA-02BBE3402218} (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:

Domain Object Attributes


- **bioLicenses** - stores the list of licenses.
- **bioSchemes** - stores the information about server extensions.

Computer Object Attributes

- **bioCacheEnable** - indicates that authenticators caching is allowed on the computer.

User Object Attributes

- **bioAuthenticationSet** - stores the list of user authentication data. Encrypted.
- **bioBioUser** - indicates that the user is allowed to use NetIQ Advanced Authentication Framework. Equals to 1 for an NetIQ Advanced Authentication Framework user.
- **bioCustom** - stores additional user data (used in NetIQ Advanced Authentication Framework extensions and NetIQ Advanced Authentication Framework SDK).
- **bioHotpCounter** - stores the counter for HOTP. Is used only for OATH HOTP. Unencrypted.
- **bioSubsystemLicenses** - stores information about NetIQ Advanced Authentication Framework extensions.
- **bioUserPassword** - stores Active Directory user password. Encrypted.
- **bioUserSettings** - stores NetIQ Advanced Authentication Framework user settings. Signed.

 All encrypted attributes are encrypted with Enterprise Key. For more information, see Security and Encryption Guide.

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.

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
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. Open the following registry key on the workstation:
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework.
2. Specify the following parameters in the registry key:
 - IsWSLogon=1 to enable authentication via Web Service
 - WebAuthServer="https://<webserviceaddress>:<webserviceport>/Service.svc/bsc"
3. Restart the client.

-  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.

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.



If you deploy Advanced Authentication in parent domain and plan to use it for users in child domains, it's required to add AuthenticoreService account to members of Enterprise Admins group.

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.

0101 Authenticore Server (NAAFRS) could not be installed during Authenticore Server upgrade

Description:

Authenticore Server (NAAFRS) could not be installed during Authenticore Server upgrade.

Solution:

If during Authenticore Server upgrade there is displayed the dialog window notifying that authtray.exe is currently in use, please open **Task Manager** and end the process **authtray.exe** manually. Then click **Retry**.

If you select **Ignore**, in a few seconds you will get an error "Service 'NetIQ Advanced Authentication Framework - Authenticore Server' (NAAFRS) could not be installed. Verify that you have sufficient privileges to install system services.". Installation of Authenticore Server will be broken. To resolve the problem, just reboot, do Repair of installation and get an existing Enterprise key.

0102 Cannot install Authenticore Server on a domain controller

Description:

Cannot install Authenticore server on a domain controller.

Solution:

Installation of Authenticore Server on domain controller is no longer officially supported. You can use it only in case of demo at your own risk. In this case use the following command:
`msiexec /i authenticore.msi IGNOREDCCHECK=YES.`

0103 RD Web is not protected by AWA

Question:

I'm getting reports that some users can login without putting in their security token. Might this be some of the languages not being protected?

Solution:

AWA needs to replace a file in **rdweb/pages/en-us** folder. So during the first installation it was **rdweb/pages/en-us/login.aspx**. Apparently after a while there was installed another language: **rdweb/pages/<language-language>/login.aspx**, but **login.aspx** wasn't updated.

0104 Error "Could not register AuthenticoreService account. Either user data or the Enterprise Key is corrupt"

Description:

While restoring the Enterprise Key, the following error is displayed: *"Could not register AuthenticoreService account. Either user data or the Enterprise Key is corrupt"*.

Solution:

It is required to initialize restoring an Enterprise Key through Authenticore Tray Manager and reset a password for AuthenticoreServer account obligatory. You should have Domain Admins or delegated privileges in order to perform this operation.

0105 Device is not registered in Apple Network Service

Description:

While scanning the QR code containing the template data with NetIQ Smartphone Authenticator, the following error is displayed: *"Your device is not registered in Apple Network Service. Please turn ON internet access and restart the application"*.

Cause:

- a. The device cannot connect to Apple's Servers, which are used to register devices for further sending of push messages.
- b. NetIQ Smartphone Authenticator is installed on the device with the unsupported version of iOS.

Solution:

- a. Check the following article: <http://support.apple.com/kb/TS4264>.
- b. Check the version of your iOS device. Update your device to the latest version of iOS.

0106 Cannot log in to Web Enrollment Wizard using Internet Explorer

Description:

I cannot log in to NetIQ Web Enrollment Wizard using Internet Explorer. I go to `http://<domain name server or IP address>/WEW`, enter my user name and domain password, click OK. But the main menu of NetIQ Web Enrollment Wizard is not being loaded.

Solution:

The problem can be solved in the following way:

1. Open **Server Manager** -> **Local Server** -> **Properties**.
2. Set the **IE Enhanced Security Configuration** value to **Off**.
3. Repeat all required authorization steps.

0107 Authentication fails while using VDA Shell in the Kiosk mode

Description:

Authentication fails while using VDA Shell in the Kiosk mode. The authorization window is displayed once again.

Solution:

Before the start of VDA Shell, it is required to close Citrix Receiver and remove it from the Startup folder in the Start menu.

0108 After 10 authentication attempts by YubiKey I am no longer able to logon

Description:

After 10 authentication attempts by YubiKey I am no longer able to logon.

Solution:

In case of HOTP authentication, there is used the [HOTP policy](#) with 10 as default value of HOTP window. HOTP uses a secret and a counter. The counter is being incremented by YubiKey on each OTP request. The correct counter is being searched for on the server or cache side to match the OTP. The search is started from the current counter (stored in AD) and it is being incremented until there is found a correct one (entered by user) or until there is exceeded the HOTP windows value. The HOTP windows value can be changed in the HOTP policy settings.

0109 Error "Could not load type 'System.ServiceModel.Activation.HttpModule'" after the Voice Call Server upgrade

Description:

After the upgrade of the Voice Call Server, the following error is displayed after entering `http://<VoiceCallServerName>:<port>/` in the browser's navigation bar: *"Could not load type 'System.ServiceModel.Activation.HttpModule' from assembly 'System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089'"*.

Solution:

It is required to register the ASP.NET 4.5 and restart IIS. For more information, check the following article: [http://msdn.microsoft.com/en-us/library/hh169179\(v=nav.71\).aspx](http://msdn.microsoft.com/en-us/library/hh169179(v=nav.71).aspx).

0110 After swiping the finger there is delay about 3-4 seconds

Description:

There is delay about 3-4 seconds after scanning the fingerprint while using the inbuilt Broadcom reader (swipe method) on Dell laptops. The delay is about 1 second only while using the Lumidigm reader.

Solution:

The speed difference is 100% a result of what capabilities are available from the reader manufacturers SDK. The more capable is the SDK, the faster is the overall user experience. The difference in time comes from the reader interface logic, but not from the image processing time. The acquiring of the image and the creation of finger detect logic can add delays to the actual capture logic. Some readers do this and they can respond quickly to finger capture requests. Other readers can only return an image. In such case it will be required to look firstly at the image to see if it has a finger image there for finger detect. Then the image can be checked for quality and use if it passes quality check. All this image processing adds up to several seconds. The Lumidigm reader does it in the driver, that's why the finger is detected promptly, the image is of a good quality and the processing is performed quickly.

0111 The request timed out on smartphone

Description:

While scanning the QR code containing the template data with NetIQ Smartphone Authenticator, the following network error is displayed: "*The request timed out*".

Solution:

Please, open a registry key HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Policies\BioAPI\BSP\SaDispatcher on your Authenticore Server and check the value of the DispExternalMobileInterface parameter. The value should contain URL. The URL should be accessible on your iPhone. Open it (including port number) in Safari on your iPhone. The following message should be displayed: "*Smartphone dispatcher is running*".

0112 Push notification wasn't received on iOS device during authentication

Description:

Push notification wasn't received on my iOS device during authentication.

Solution:

Push messaging for iDevices works in the following way: Smartphone Authentication Dispatcher -> <https://proxy.athasas.com> -> Apple (APNS) servers -> iPhone/iPad. Try to authenticate once again within the certain period of time or try to authenticate using Android device. If push notification can be received on Android device, but cannot be received on iOS device, the issue is on Apple Servers side, not on the side of NetIQ.

0113 Client can authenticate to Authenticore Server from another AD site for the first time

Question:

Why can Client authenticate to Authenticore Server for the first time in case Authenticore Server and Client are not within one AD site?

Explanation:

The flow is the following:

1. The Client looks into the Authenticore Servers group.
2. The Client selects a random server from that group which belongs to the same AD site as the client PC.
3. The Client checks the Server2Sites (S2S) cache, asks whether it knows this Authenticore Server.
 - If it knows this Authenticore Server, the Client looks to which AD site this Authenticore Server belongs.
 - If it doesn't know this Authenticore Server, the Client asks S2S to find out in the background to which AD site this Authenticore Server belongs.
4. As the request may be delayed, the Client tries to find out through subnetworks whether it is the required AD site. If subnetworks overlap, there may occur errors for the first time and the Client will go to the wrong AD site.
5. During the second logon the Client gets an answer from S2S regarding the AD site to which Authenticore Server belongs.
6. If Authenticore Server is stopped, the request will be valid for 20 sec. (if there are several logons during this time, errors may occur).
7. S2S knows that Authenticore Servers can go from one AD site to another. That's why S2S cache is updated firstly in an hour since the start, and then - every 4 hours.

0114 After the upgrade of Authenticore Server, Administrative Tools and other components are not upgraded

Description:

After the upgrade of Authenticore Server, Administrative Tools and other components are not upgraded.

Solution:

After the upgrade of Authenticore Server, it is required to restore Enterprise Key as Authenticore Server is not started after the upgrade.

0115 Error "Failed to resolve user name. Check spelling and try again" while using VDA Shell

Description:

While using VDA Shell, the following error is displayed: "*Failed to resolve user name. Check spelling and try again*".

Solution:

1. Open the following registry key on the workstation:
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework.
2. Specify the following parameters in the registry key:
 - IsWSLogon=1 to enable authentication via Web Service
 - WebAuthServer="https://<webserviceaddress>:<webserviceport>/Service.svc/bsc"
3. Restart the client.

0116 NetIQ Group Policies are not displayed in Group Policy Management Console

Description:

NetIQ Group Policies are not displayed in Group Policy Management Console, even though NetIQ Administrative Tools and NetIQ Group Policy Templates are installed.

Solution:

NetIQ Group Policies should be displayed after adding NetIQ Administrative Tools and NetIQ Group Policy Templates manually on DC. If it doesn't help, follow these steps:

1. Open `\\<DCName>\SYSVOL\<DomainName>\Policies\`.
2. Create the PolicyDefinitions folder in it.
3. Copy NAAF.admx and UniversalCardBSP.admx from `C:\Windows\PolicyDefinitions\` folder on the Authenticore Server to the `\\<DCName>\SYSVOL\<DomainName>\Policies\PolicyDefinitions` folder.
4. Create the en-US folder in the PolicyDefinitions folder.
5. Copy NAAF.adml and UniversalCardBSP.adml from the en-US subfolder to the en-US in the shared folder.
6. Try again.
7. If it doesn't work, remove the PolicyDefinitions folder from `\\<DCName>\SYSVOL\<DomainName>\Policies\`. Check permissions on the files in the `C:\Windows\PolicyDefinitions\` folder on the Authenticore Server. Set Full control for local Administrators and SYSTEM on them.
8. Try again.

0117 Error "You don't have rights for changing settings on this page. Please, ensure that these rights are delegated to you."

Description:

After the upgrade of NetIQ to version 4.10 R3 in AD LDS configuration, the following error is displayed in the NetIQ Advanced Authentication Framework Users tab in ADUC: *"You don't have rights for changing settings on this page. Please, ensure that these rights are delegated to you"*. I have Domain Admins rights.

Solution:

It is required to delegate rights to the NetIQ Advanced Authentication Framework Admins group in the following way: DSACLs

```
\\<LDSServerAddress>:<LDSPortNumber>\<InstanceName> /G
```

```
"<DomainName>\NetIQ Advanced Authentication Framework Admins:GA" /I:T
```

E.g., DSACLs \\localhost:50000\cn=NAAF /G "NetIQ\NetIQ Advanced Authentication Framework Admins:GA" /I:T

Afterwards re-log in for the configuration changes to take effect.

0118 How to change default logo in Web Enrollment Wizard

Question:

How can I change the default logo in Web Enrollment Wizard?

Answer:

To change the default logo, replace *logon_square.png* in C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW\Content\images with an applicable image in .png format.

0119 Enterprise Key is damaged

Question:

While generating a new Enterprise Key, its backup copy was protected with a password. It seems that now Enterprise Key is damaged. What should I do in such case?

Answer:

The problem can be solved using the following tool: <https://www.authasas.com/wp-content/uploads/2012/dist/BackupKeyFix.zip>.

Follow these steps:

1. Unpack the tool.
2. Place an old Enterprise Key file to the same folder with the tool.
3. Run "BackupKeyFix <old key file> <recovered key file>".
4. Import the recovered key file via Authenticore Server Tray app.

0120 Device events don't work when presenting or removing a smartcard

Description:

Device events, like automatic logoff or lock, don't work when presenting or removing a smartcard.

Solution:

The user logs in before the ClientHelper is started. It can happen when auto logon is enabled and the user (local user) logs in immediately . To solve this issue, it is required to make the User Profile Service dependent on the ClienthelperService. Follow these steps:

1. Open the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ProfSvc.
2. Add NAAFClientHlpService to the DependOnService registry value.
3. Restart the workstation.

0121 Error: "Value cannot be null. Parameter name: Waithandle array may not be empty."

Description:

While enrolling the Smartphone authentication provider with Web Enrollment Wizard, the following error is displayed: *"Value cannot be null. Parameter name: Waithandle array may not be empty."*

Solution:

The following error occurs only if the Smartphone Authentication Dispatcher policy is not configured or not applied on the server with the installed Web Enrollment Wizard. To configure the Smartphone Authentication Dispatcher, see the [Configuring Smartphone Authentication Dispatcher via Group Policy](#) chapter of the Smartphone Authentication Dispatcher - Installation Guide.

0122 How to restore quick remote access after NetIQ Client installation

Question:

Our finance department uses RDP-files for quick connection to some non-domain computers. After NetIQ Client installation the Windows Security dialog box appears every time when starting the RDP-file. Now our employees must select the Use another account option in the Windows Security dialog box and enter PC name/username and password manually. How is it possible to restore quick remote access?

Answer:

For more information on how to restore quick remote access, see the following article: <https://support.microsoft.com/kb/941641>.

0123 Error 0xe06d7363 when using NPS plugin

Description:

After the update of NetIQ, authentication through the NPS plugin has stopped working. In the NetIQ Advanced Authentication Framework Event Viewer the following error is displayed: *Could not authenticate the user by provided authenticator. Error: Unknown error. (0xe06d7363).*

Solution:

Ensure that the [NPS Logon Method Selection](#) policy is configured properly and applied on the Authenticore Servers, and the user that performs authentication is a member of an applicable group configured in the policy.

0124 How to configure the Citrix USB redirection for BIO-key AP in case of XenDesktop

Question:

How can we configure the Citrix USB redirection for BIO-key AP in case of XenDesktop? Currently we have the following error: "Error: VST error code = -152, msg = Cannot open virtual channel (Remote client: <name>)."

Answer:

To configure the Citrix USB redirection for BIO-key AP in case of XenDesktop:

1. Enable the [Credential provider filter settings](#) policy of the **Security** section on the workstation.
 - a. Select the **Enable Citrix credential provider (for pass-through)** checkbox to enable the **Show** button.
 - b. Click **Show** to add the following allowed credential provider in the **Show Contents** dialog box: {5B340FA8-5C3F-45de-87C8-487ABE91013E}.
 - c. Apply the changes.
 - d. To verify whether applicable parameters are added to the corresponding registry keys, open the registry:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\NetIQ\NetIQ Advanced Authentication Framework\Filter
CitrixCPEnabled: type: DWORD; value: 0x00000001 (1).
 - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\NetIQ\NetIQ Advanced Authentication Framework\Filter\AllowedCPs
1: type: REG_SZ; value: {5B340FA8-5C3F-45de-87C8-487ABE91013E}.
2. Allow the **Client USB device redirection** policy in the **Policies** section of **Citrix Studio**. Click **OK**.
3. Open the registry key
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\NetIQ\NetIQ Advanced Authentication Framework\ and specify the following parameter:
LocalBspForced: type: DWORD; value: 1.
4. The drivers of an applicable device should be obligatory installed on the workstation.
5. Open the registry key
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BIO-key\Common\Settings and specify the following parameter:
DisableVirtualChannel: type: REG_DWORD; value: 0x00000001 (1).

0125 How to configure FAR/FMR in BIO-key AP

Question:

How can we configure FAR/FMR in BIO-key AP?

Answer:

Open the registry key `HKEY_LOCAL_MACHINE\Software\BIO-key\Biometric Service Provider\Threshold\` and specify the following parameters:

- **EnrollmentInitialMaxDistanceFromTarget:** type: DWORD.
Initial maximum distance (as a percentage of the display area's width) between the fingerprint center and the target before the enrollment process will accept an image. If the enrolled finger is further from the target, the user will be prompted to move his/her finger towards the center of the target.
- **EnrollmentFinalMaxDistanceFromTarget:** type: DWORD.
Final maximum distance (as a percentage of the display area's width) between the print center and the target before the enrollment process will accept an image. If the Final Max value is bigger than the Initial Max value, then the guidance circle in the display area will gently grow over time to accommodate errant behavior. If they are the same, then the size will be locked. It is not permitted for Final Max to be less than Initial Max distances.

i The percentage is the percentage of the Radius (or half the width). So a 300 pixel wide reader has a 150 pixel radius, but that is just represented as percentage, so 20% is 30 pixels from the center, 50% is 75 pixels, given the example of 300 pixel width. Range is 0-50 (it is not recommended to set anything less than 15%).

- **IdentificationMinCompareScore:** type: DWORD.
During enrollment multiple images of the same finger are captured. This is the minimum comparison score that must be present between the images before they are accepted. Values range from 0 (no match) to 99 (very good match). A default value of 50 is good. Anything below 50 is a miss or a false hit and should not be used.

i If you change the IdentificationMinCompareScore parameter (ranges from 1 to 100 with default of 50), you will be moved on the range of score distribution of the True Accepts and True Rejects. The True Reject curve is a sharp curve that centers around 35-40, with a strong tail into the mid to upper 40's. So, as you drop into the 40's the False Accepts increase as you pierce more of the True Reject curve. Essentially what you are shifting is the False Accept Rate, with benefit of the False Reject Rate. It is not recommended to go any lower than 48, except for special needs.

0126 SecuGen Hamster IV does not work with BIO-key

Question:

During either testing or actual enrollment of fingerprints using a SecuGen Hamster IV reader, the finger is not recognized/read. The SecuGen HAMSTER IV reader is connected to the PC, Windows detects and recognizes the device. When I place my finger on the reader, the red light turns on for 1 second and then stays off, and my fingerprint is not read. When I use this or another reader on a test PC (Windows 7 Pro x64), it works without problems. The current PC has Windows 8.1 PRO and USB 3.0 ports.

Answer:

To solve the problem, follow the steps:

1. When the SecuGen Hamster reader is plugged in, go to the **Device Manager** and remove the current driver making sure you have selected the **Delete the driver software for this device** option.
2. Disconnect your computer from the network (wired and wireless). Now **Windows Update** will not search for a WBF driver on-line.
3. Run the BIO-key BSP 1.0.30 installer and install the SecuGen Hamster reader drivers. Select **Manual Reader Install**, clear all reader checkboxes. The black check on the white background will be displayed. If applicable, select it to force the install of the SecuGen Hamster drivers.
4. Complete the BIO-key BSP installation.
5. The reader operation can be checked in the test point during installation, or in the **BIO-key Control Panel** app.
6. Connect your computer to the network.
7. Run **Windows Update** and review the list of **Optional Updates**. If one of them is SecuGen Drivers, set is as **Hidden/Disabled** for future update notifications. Do not install it.

0127 How to integrate RSA with Citrix Netscaler in the NetIQ framework

Question:

How is it possible to integrate RSA with Citrix Netscaler in the NetIQ framework?

Answer:

There are 2 ways to integrate RSA in the NetIQ framework:

- **Replace RSA by NetIQ** (e.g., with the NetIQ Smartphone Authentication app)
Let Netscaler point to the RSA Radius server and set up a proxy that points to the NetIQ Radius server when authentication fails. Configure RSA in a two field screen mode, one for the username and one for RSA-code plus password. For more information, see the RSA configuration guide.
- **Add RSA authentication as an extra authentication option**
Configure an extra logon point in Netscaler that points to the RSA setup. The user now may select an applicable authentication option (e.g., the NetIQ Smartphone Authentication app or RSA by selecting the appropriate URL).

0128 How to prevent dual authentication request in case terminal mode is used

Description:

We would like to use RDP to connect to the broker which load balances our terminal server sessions. We have a thin client in the domain and NetIQ Client with the installed Universal Card authentication provider. We can connect to the terminal servers directly using RDP and it passes through the credentials without issue. But when we are connecting to the session farm, it prompts for credentials again.

Solution:

You need to use NetIQ VDA Shell. It allows performing pre-session authentication instead of in-session. As a result you will be required to authenticate only once before the RDP session is initiated. Then you will get a pass-through authentication inside the session. For more information, see our [online documentation](#) about NetIQ VDA Profile Editor and NetIQ VDA Shell.

Please perform the following steps:

1. Create RDP profile using the VDA Profile Editor tool.
2. Install NetIQ VDA Shell on the thin client and add the configured profile.
3. Remove NetIQ Client software from the terminal server to avoid the repeated authentication request.
4. Run NetIQ VDA Shell and authenticate using your credentials.

0129 Cannot log in using linked account

Question:

My account is linked to a common account which was never used to authorize my computer. I try to log in using my account and an authenticator of the common account, but I'm not able to do it.

Answer:

1. Ensure that you use a valid authenticator.
2. Ensure that you are connected to the corporate network. Offline logon using linked accounts is not supported.

0130 How to make Yubikey OATH HOTP option invisible in WEW

Question:

We have upgraded our Authenticore Server last week. Since the upgrade we have a capability to enroll Yubikey OATH HOTP token in the web interface of Web Enrollment Wizard. We are not going to use it in the nearest future. How can we make this option invisible?

Answer:

To make this option invisible, follow the steps:

1. Browse C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW on the server with Web Enrollment Wizard installed.
2. Open the web.config file in Notepad.
3. Find the following line: `<add key="c7d6704e-f66a-4ef0-93a3-c5ef13f0c7a2:0" value="Yubikey HOTP"/>`
4. Remove it or comment it:
`<!--
<add key="c7d6704e-f66a-4ef0-93a3-c5ef13f0c7a2:0" value="Yubikey HOTP"/>
-->`
5. Save changes.

0131 Error "Could not register AuthenticoreService account. Could not get access to ADAM server"

Description:

While generating Enterprise Key, the following error is displayed: "*Could not register AuthenticoreService account. Could not get access to ADAM server*".

Solution:

Please remove an AD LDS instance and install it again. Follow the instructions of the [Deployment Guide](#).

0132 How to configure Remote Desktop Services with NetIQ Advanced Authentication Framework

Question:

How can I configure Remote Desktop Services with NetIQ Advanced Authentication Framework?

Answer:

Before proceeding to RDS configuration, make sure that the following requirements are fulfilled:

- DC is installed.
- Domain network is configured.
- All servers are joined to the domain.

Operating System	Windows Server 2012	Windows Server 2012	Windows Server 2012	Windows 7
Hostname, IP	192.168.179.197, win-dc	192.168.179.198, win-rdshost01	192.168.179.199, win-rdshost02	192.168.179.200, vmware-PC
Installed Roles	DC	Connection Broker, Session Host, Web Access	Session Host	
Installed NetIQ Components	NetIQ Password Filter	NetIQ Authenticore Server, Client	Authenticore Server	

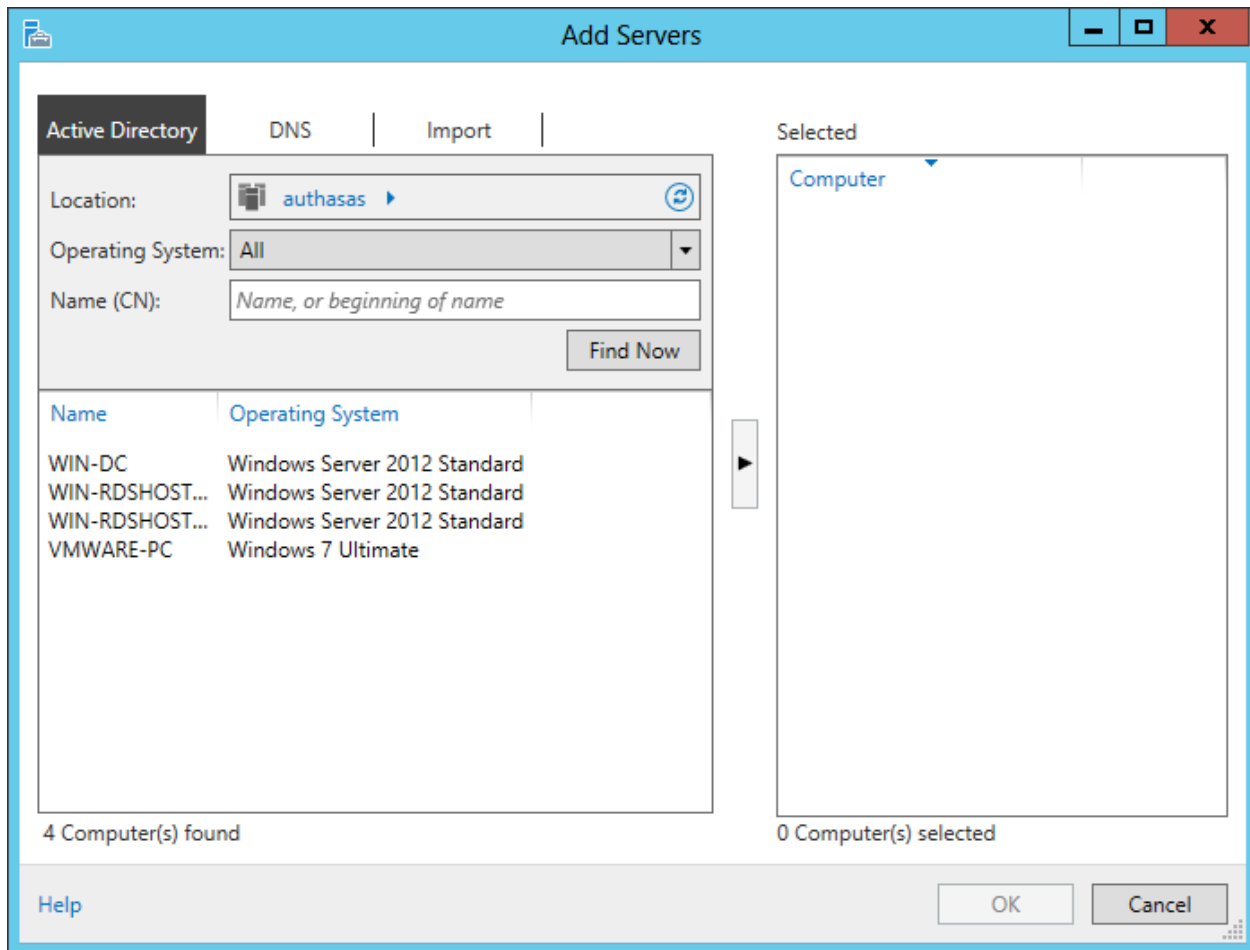
To configure Remote Desktop Services with NetIQ Advanced Authentication Framework, it is required:

- [to configure server pool](#)
- [to create RDS farm](#)
- [to configure Session Host connection](#)
- [to install NetIQ components](#)

Configuring Server Pool

To configure server pool, follow the steps:

1. Open Server Manager.
2. On the **Manage** menu, click **Add Servers**.
3. Select an applicable location and click **Find Now**. Click **OK**.



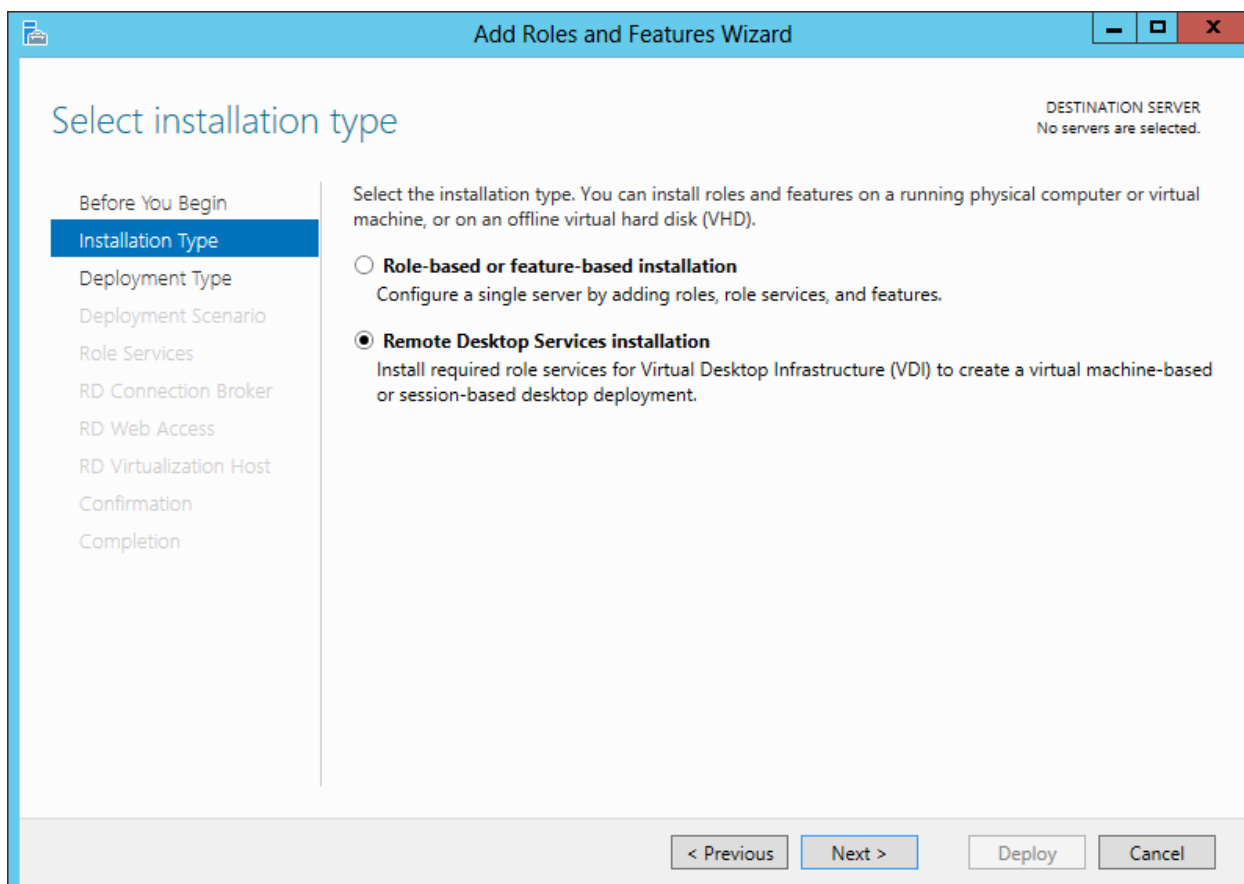
4. Select servers that will be included to the pool.
5. To view server that are included to the pool, open the **All Servers** page in Server Manager.

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-DC	192.168.179.197	Online - Performance counters not started	3/6/2015 5:18:41 AM	Not activated
WIN-RDSHOST01	-	Target computer not accessible	3/6/2015 5:19:21 AM	-
WIN-RDSHOST02	-	Target computer not accessible	3/6/2015 5:19:20 AM	-

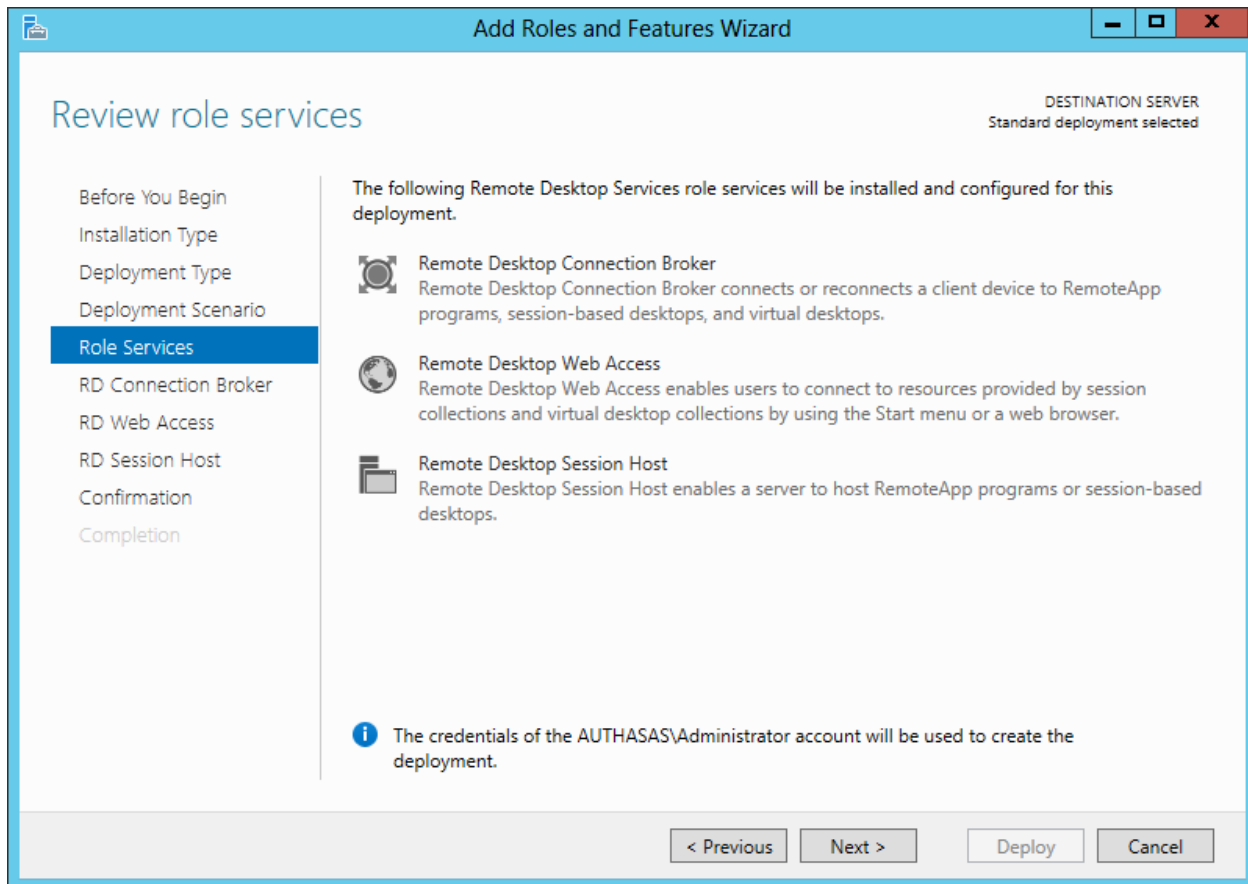
Creating RDS Farm

To create RDS farm, follow the steps:

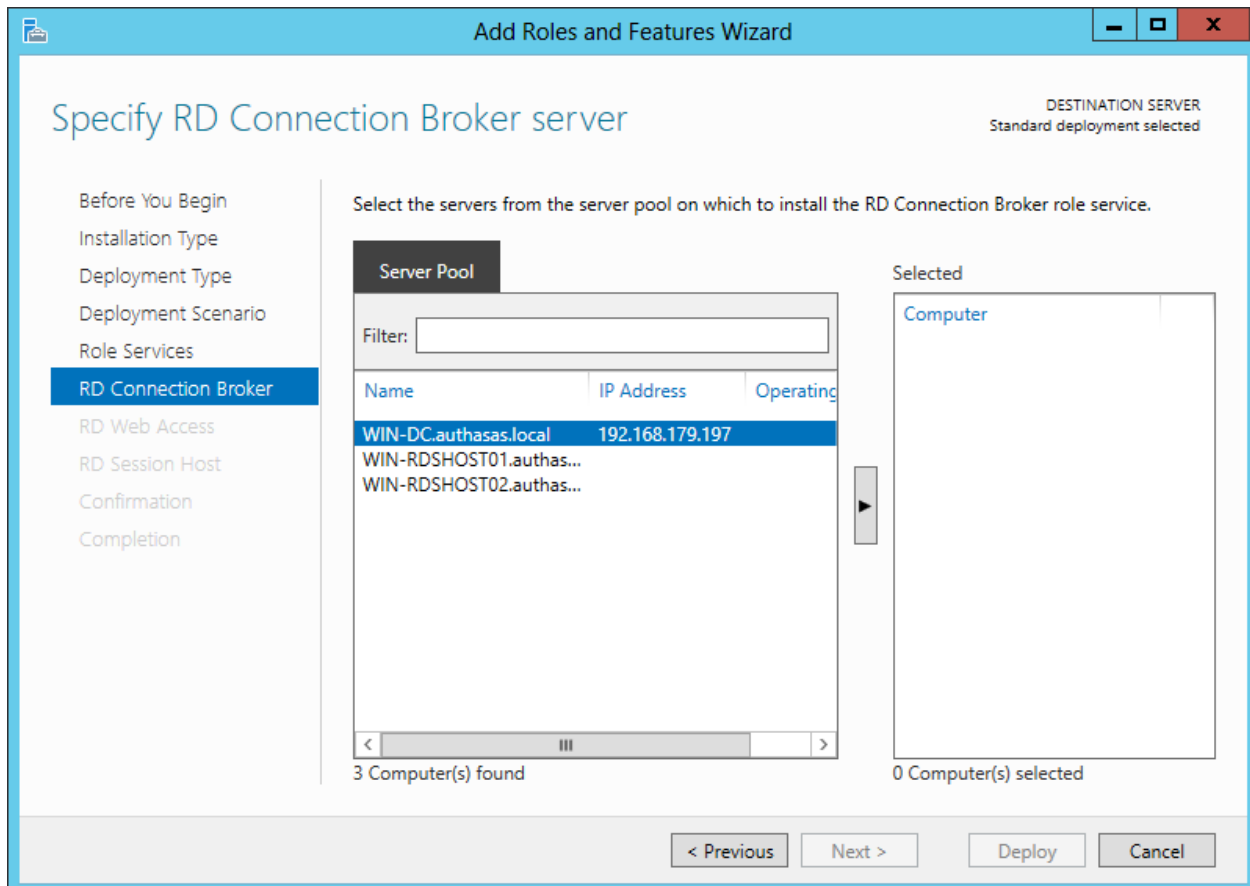
1. Open Server Manager.
2. On the **Manage** menu, click **Add Roles and Features**.
3. Select **Remote Desktop Services installation** type. Click **Next**.



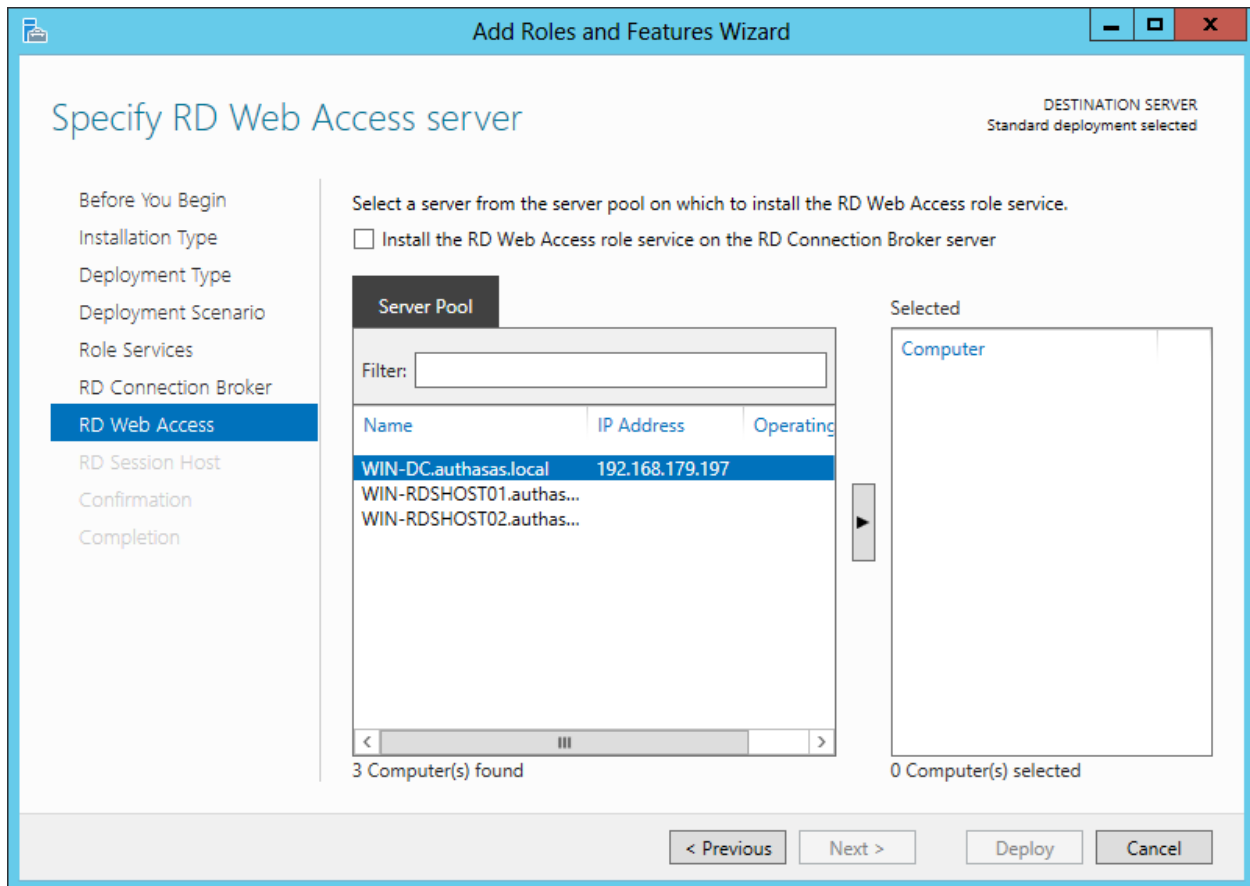
4. Select **Standard** deployment type. Click **Next**.
5. Select **Session-based desktop** deployment scenario. Click **Next**.
6. The wizard notifies about roles that will be installed. Click **Next**.



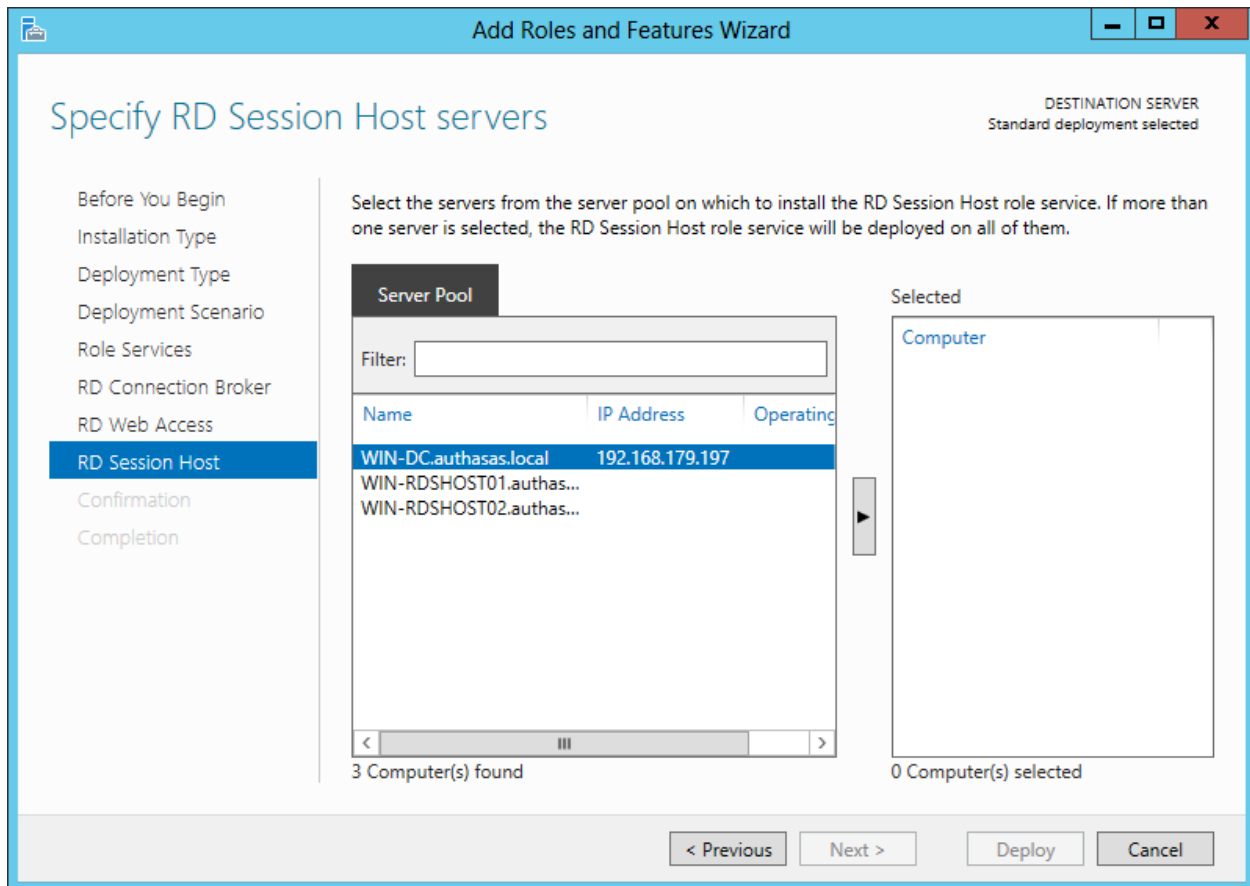
7. Select servers from the server pool on which the RD Connection Broker role service will be installed. Click **Next**.



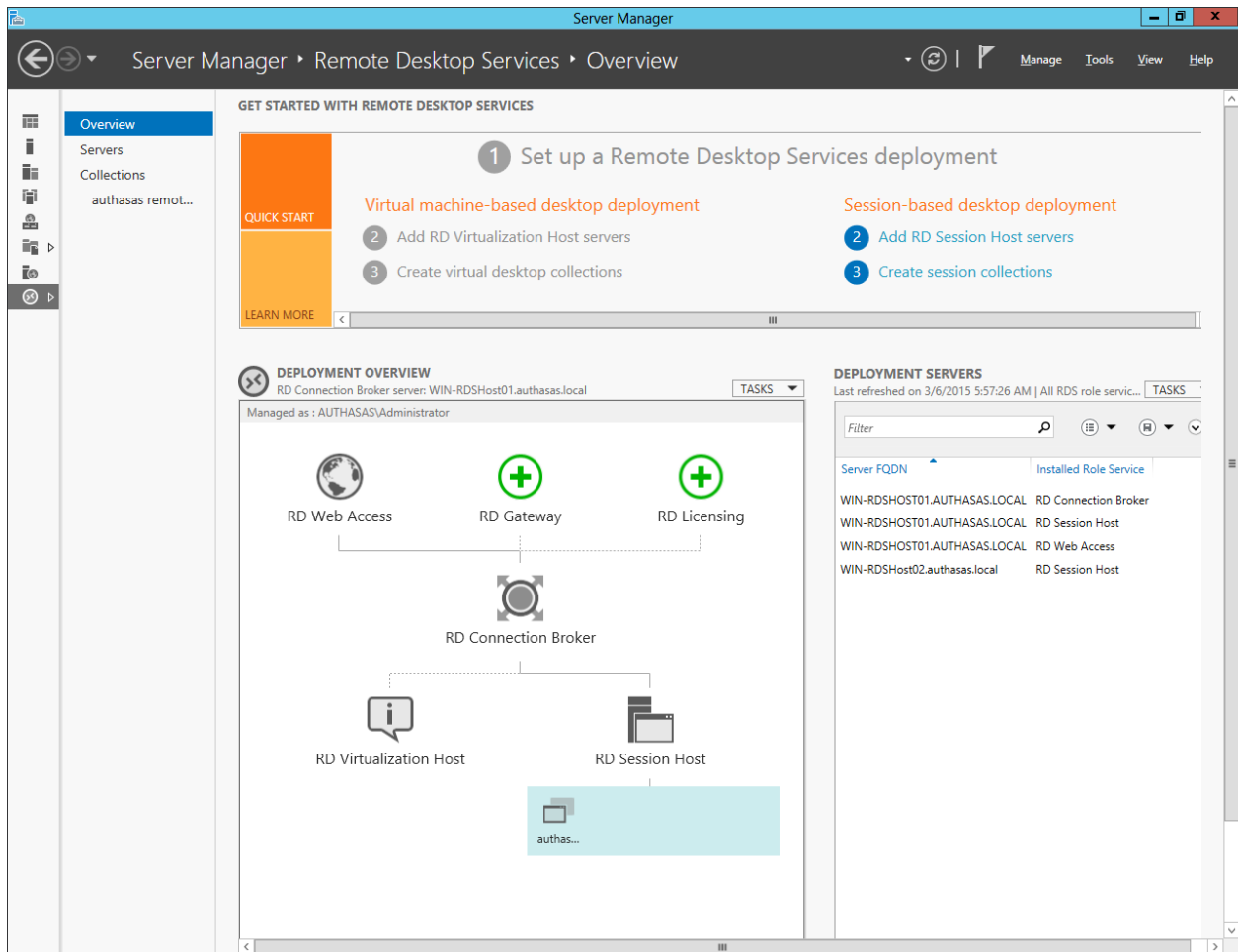
8. Select servers from the server pool on which RD Web Access role server should be installed. Click **Next**.



9. Select servers from the server pool on which RD Session Host role service should be installed. Click **Next**.



10. Confirm deployment parameters and click **Deploy**.
11. After deployment is performed and servers are rebooted, open Service Manager, go to the **Remote Desktop Services** page and open the **Overview** section.



Configuring Session Host Connection

To configure session-host collection, follow the steps:

1. Open Server Manager.
2. In the left pane, click Remote Desktop Services.
3. Select **Collections**.
4. Specify collection's name and its description. Click **Next**.

Before You Begin

Collection Name

RD Session Host

User Groups

User Profile Disks

Confirmation

Progress

A session collection name is displayed to users when they log on to a Remote Desktop Web Access server.

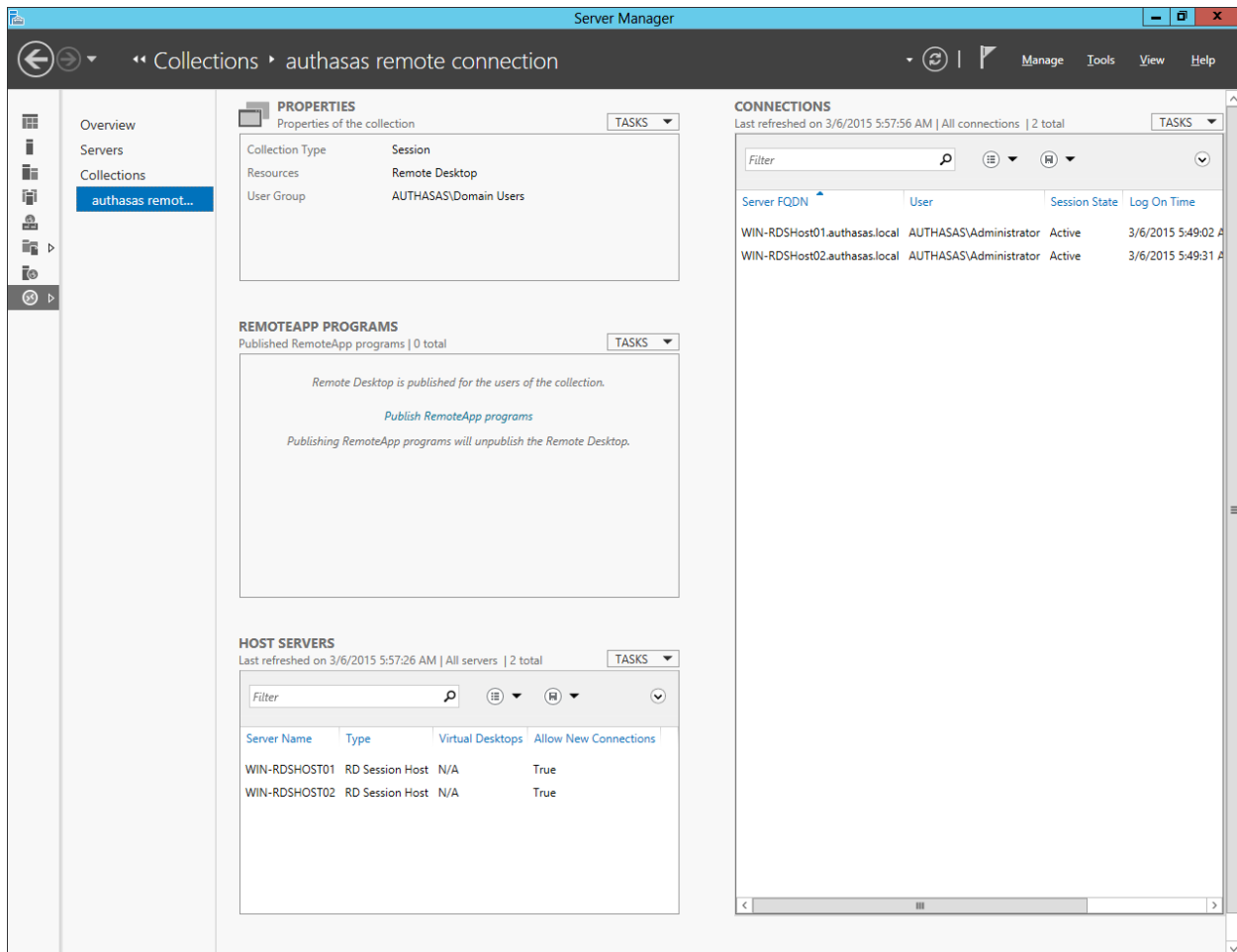
Name:
test

Description (optional):
test

< Previous Next > Create Cancel

5. Specify RD Session Host servers. Click **Next**.
6. Specify user groups available for remote connection. Click **Next**.
7. On the **Confirm selections** page, click **Create**.

After collection is created, open Service Manager, go to the **Remote Desktop Services** page and open the **Collection** section.



Installing NetIQ Components

After server pool configuration and RDS farm creation, it is required to install NetIQ Advanced Authentication Framework Components:

- NetIQ Authenticore Server should be installed on win-rdshost01 and win-rdshost02. For more information, see the [NetIQ Authenticore Server Configuration](#) chapter.
- NetIQ Password Filter should be installed on win-dc. For more information, see [Password Filter - Installation Guide](#).

0133 How to create Security Groups and AuthenticoreService account manually

Question:

How can I create Security Groups and AuthenticoreService account manually?

Answer:

To create Security Groups and assign Group membership, complete the following steps:

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 Servers, ensuring that your user account is a member of this group.
5. Create a Global Security Group named **Authasas Advanced Authentication Admins**.
6. Assign users and groups to administer/enroll Authasas users, ensuring that your user account is a member of this group.
7. Create an account named **AuthenticoreService**, set the **Password never expires** option, follow the article: [0097 How to configure AuthenticoreService account with minimal permissions](#).
8. Create a Global Security Group named **Authenticore Servers**.
9. Create a Global Security Group named **Authasas Advanced Authentication ADAM Servers**.

0134 OATH OTP AP installation rolls back without error message


Description:

Roll-back without error message occurred during OATH OTP AP installation. The installation log contains the following errors:

```
CAQuietExec: OSS Nokalva BioFoundry BioAPI2.0 Adapter for BioAPI1.1 BSPs
Installation utility 1.0
CAQuietExec: Copyright (C) 1997-2015 OSS Nokalva, Inc. All rights reserved.
CAQuietExec:
CAQuietExec: ***** Reading records from the BioAPI 1.1 Registry
'C:\Windows\system32\OSSBioAPIFFDB\OSSBioAPIRegistry' ...
CAQuietExec: ***** Using BioAPI 1.1 registry at
C:\Windows\system32\OSSBioAPIFFDB\OSSBioAPIRegistry ...
CAQuietExec: ***** BioAPI 1.1 BSP module source path C:\Program Files (x86)
\BSP\OATH BSP\OathBSP.dll ...
CAQuietExec: Error: Could not load BSP library at "C:\Program Files (x86)\BSP\OATH
BSP\OathBSP.dll"
CAQuietExec: Error: BioAPI 1.1 BSP installation failed.
CAQuietExec: Error 0x80070001: Command line returned an error.
CAQuietExec: Error 0x80070001: CAQuietExec Failed
CustomAction RegBsp returned actual error code 1603 (note this may not be 100%
accurate if translation happened inside sandbox)
```

Solution:

1. Go to the directory **C:\Windows\SysWOW64** and take a backup of the following files:
 - *iconv.dll*
 - *libpskc-0.dll*
 - *libxml2-2.dll*
 - *zlib1.dll*
2. Replace them with new files.

 You can request these libraries at techsupport@authasas.com or take from another workstation with the installed OATH OTP AP.

3. Request BioApi utilities at techsupport@authasas.com.
4. Open **cmd**, go to directory **..\BioAPI\v11** and install bioapi with the following command:
bio_reg_create.exe -F. E.g.:

```
C:\Users\Administrator\Downloads\BioAPI\v11>bio_reg_create.exe -F
OSS Nokalva BioFoundry BioAPI Registry Create utility 1.0
Copyright (C) 1997-2015 OSS Nokalva, Inc. All rights reserved.
***** Creating BioAPI registry at  $\pm$ %g ...
***** Reading records from the BioAPI Registry 'C:\Windows\system32\OSSBioAPIFFD
B\OSSBioAPIRegistry' ...
***** The BioAPI registry 'C:\Windows\system32\OSSBioAPIFFDB\OSSBioAPIRegistry'
does not exist and will be created.
***** Creating the BioAPI Registry ...
***** BioAPI Registry create completed succesfully.
```

5. Go to directory **..\BioAPI\v20** and install framework with the following command:
framework_install -f. E.g.,

```
C:\Users\Administrator\Downloads\BioAPI\v20>framework_install -f
OSS Nokalva BioFoundry BioAPI 2.0 Framework Installation utility
Copyright (C) 1997-2015 OSS Nokalva, Inc. All rights reserved.
***** Step 1. Processing .inf file.
The target path is not specified. System default DLL directory will be used.
***** Step 2. Verifying the installation.
***** Step 3. Copying files to the target.
Source: C:\Users\Administrator\Downloads\BioAPI\v20
Target: C:\Windows\system32
Error: The target file 'C:\Windows\system32\bioapi20.dll' already exists and -f
is not specified.
```



Please note that framework is already installed in this example.

6. Go to directory **..\BioAPI\Adapter11** and execute the following command:
RegBSP11c.exe -s %systemroot%\system32\adapter110.dll.
7. Move to directory **..\BioAPI** and execute the following command:
EnableBioAPIForAll.exe /oss.
8. To install bsp library, move to **..\BioAPI** and execute the following command: **asd_bsp_install.exe -s "C:\Program Files (x86)\BSP\OathBSP\OathBSP.dll"**. Create appropriate directories and copy library before executing the command. You can take this library from the workstation with the installed OATH OTP AP or require it at techsupport@authasas.com.
9. Run the OATH OTP AP installer.

0135 Smartphone Dispatcher service cannot be started

Description:

After upgrade of the Smartphone Dispatcher from v1.1.108 to the latest version, the Smartphone Dispatcher service cannot be started.

Solution:

A new parameter in Smartphone Dispatcher's policy may not be applied. Please check HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\BioAPI\BSP\SaDispatcher on the Smartphone Dispatcher server. Verify whether the DispDataPort parameter is added.

If the parameter is not added, please go to the policies on the Smartphone Dispatcher server, open the [Smartphone Authentication Dispatcher policy](#). Ensure that you have filled in all the fields.

Please verify also whether 'rpc' is switched to 'http' (or 'https') in the policy settings. Then apply the group policy changes. Try to run the Smartphone Dispatcher service again.

0136 How to enable visualization of Windows boot process

Question:

Sometimes it takes a long time to log in to the system. How can I analyze a slow boot?

Answer:

It is recommended to enable the **Verbose vs normal status messages** policy on the client PC. The policy allows to you examine what exact step of the boot process takes a long time. With this policy enabled, each step in the process of starting, shutting down, logging on, or logging off the system will be reflected. To enable the **Verbose vs normal status messages** policy:

1. Open **Group Policy Editor Object**.
2. Navigate to **Computer Configuration -> Administrative Templates -> System**. Double-click the **Verbose vs normal status messages** policy and enable it.
3. Check registry to make sure that policy is enabled. Open the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\, the **verbosestatus** option should be set to **1**.

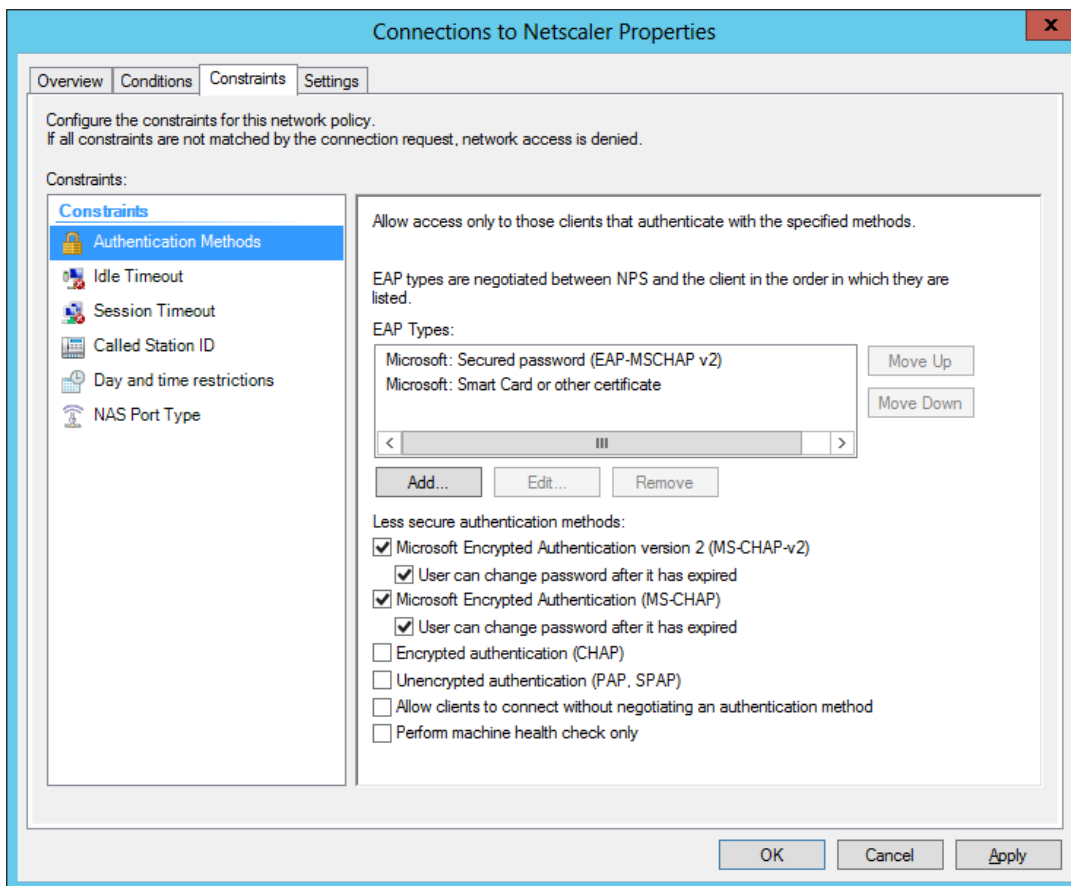
0137 Error "Incorrect username/password" when trying to authenticate to NetScaler


Description:


I try to authenticate to NetScaler with Smartphone authentication provider. After tapping the **Accept** button of NetIQ application, the following error is displayed in NetScaler: "*Incorrect username/password*". When I try to authenticate with SMS authentication provider, text messages are not received on my smartphone.

Solution:

In most cases such issues can be caused by incorrect authentication protocol configuration. E.g., NetScaler is configured to use PAP and NPS is configured to use MSCHAP. Please make sure that the correct Radius authentication protocol is used. On Windows side, go to NPS. Open properties of an appropriate network policy, and verify methods of the **Constraints** tab.



 MSCHAPv2 protocol is supported by all authentication providers except for SMS AP. SMS AP requires PAP protocol.

 CHAP protocol requires reversible encryption. Reversible encryption is a user class attribute and is not enabled by default in the Active Directory. You must enable this setting manually for each account by selecting the **Store password using reversible** checkbox in the **Account** tab, or through Group Policy Objects Editor by enabling the **Store passwords using reversible encryption** policy which is located in the **Account Policies** section.

0138 BIO-key AP can't be installed/upgraded on Windows Server 2012 R2

Question:

Cannot upgrade the BIO-key AP to v1.0.45 on Windows Server 2012 R2. Even if I remove a previously installed version and try to do a clean installation, it doesn't work. Sometimes the installation hangs or I get an error "*Unable to create file C:\Windows\system32\WinBioPlugins\BKEngineAdapterx64.dll*".

Answer:

Please add the **Windows Biometric Framework** feature and try again.

0139 SecuGen Hamster doesn't work with the BIO-key AP

Question:

I got the following error *"The reader cannot be initialized. Error code: -4, Message: Fingerprint reader DLL failed to load"* when trying to use SecuGen Hamster with BIO-key AP 1.0.45

Answer:

Please open **C:\Program Files\BIO-key\Drivers\6.5\SecuGen** and copy **sgfplib.dll** from subfolder **x64** to **C:\Windows\system32** and from subfolder **x86** to **C:\Windows\SysWOW64**. Reboot and try again.

0140 Error "Windows could not start the Authasas Advanced Authentication - Authenticore Server on Local Computer"

Description:

When trying to start the Authenticore Server, the following error is displayed: *"Windows could not start the Authasas Advanced Authentication - Authenticore Server on Local Computer. For more information, review the System Event Log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code - 1057030129."*

Solution:

This error occurs when the Authenticore Server doesn't have an Enterprise Key. Please try to restore an Enterprise key (**Authenticore Server tray icon -> Enterprise Key -> Restore key**). If it doesn't help, please reinstall the Authenticore Server.

0141 Low quality swipe fingerprint sensors

Question:

When using a swipe sensor I need to provide my fingerprint 3-7 times for authentication. When using a touch sensor it works fine with first touch as magic. Why?

Answer:

Images from two different technologies differ because of the following reasons:

- Elastic deformation - skin on the finger stretches differently when pulled across a surface rather than flattening out when pushed down on a touch sensor.
- Hardware - touch sensor has all the data available for the finger and can simply read it directly. The swipe sensor only has a narrow slice of the finger and software then has to reassemble the fingerprint image into a usable format. Some manufacturers stitching algorithms work better than others.

Select one of the following options to improve enrollment process:

- Enroll the person with the technology he/she will use the most
- Enroll using both swipe sensor and touch sensor (it may not be supported due to aliases, depends on the application)
- Enroll a second finger using the other technology (one finger for touch and one finger for swipe)

In general, sweeping is less intuitive and natural than using a touch-based device. So, a novice user may encounter some difficulties in performing the sweeping properly (i.e., without sharp speed changes, or discontinuities). This is supported by a noticeable failure to acquire rate of 37.9% for the sweeping sensor during FVC2004 database collection. For more information, check the [following source](#).

0142 Upgrading BIO-key Pin BSP v1.0.44 and earlier

Question:

Do I need to perform some preliminary actions before upgrading BIO-key Pin BSP v1.0.44 to the later version?

Answer:

If you are upgrading BIO-key Pin BSP v1.0.44 and earlier to BIO-key Pin BSP v1.0.45 and later on the server, then add the Windows Biometric Framework feature on it. If you are upgrading BIO-key Pin BSP v1.0.44 and earlier to BIO-key Pin BSP v1.0.45 and later on the computer, then start the Windows Biometric Service manually.

0143 Fingerprint reader driver error (Subcode -101 -UFS_ERR_NO_LICENSE)

Question:

I use Suprema BioMini readers with BIO-key AP. When I try to enroll an authenticator, I get an error: *"Your fingerprint reader could not be initialized. Error: VST error code = -17, msg = Fingerprint reader driver error (Subcode -101 -UFS_ERR_NO_LICENSE)"*.

Answer:

Please copy the **UFLicense.dat** from the **c:\windows\system32** to the **c:\windows\sysWOW64** directory.