



NetIQ Advanced Authentication Framework- Web Service

Administrator's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
Strong Authentication	3
Strong Authentication Advantage	3
NetIQ Advanced Authentication Framework - Web Service Overview	4
How Does It Work?	4
Integrates with NetIQ Advanced Authentication Framework Edition	4
Getting started	5
What is Included	5
NetIQ Advanced Authentication Framework – Web Service	6
Terms	7
Checking State of NetIQ Web Service	7
Identifiers of Authentication Service Providers	7
Preparing Raw Authentication Data	9
Universal Card Authentication Service Provider	9
RADIUS Authentication Service Provider	9
Flash Drive + PIN Authentication Service Provider	10
OATH Authentication Service Provider	10
Error Codes Description	11
RPC Server Errors	11
SrvWrapper Errors	15
Password Filter Errors	15
Password Manager Errors	15
EventLog Errors	16
BioAPI Errors	16
Authenticore Server Errors	17
Authentication Providers Errors	19
Cryptography Errors	19
Manager Errors	20
Plugins Errors	20
Licensing Errors	20
Backup Provider Errors	21
Administration Tools Errors	21
GINA Errors	21
Data Errors	22
Troubleshooting	24
Authentication Failed	24
Index	25

Introduction

Strong Authentication

Compliance is important in a world where organizations have to adhere to increasingly complex rules and regulations. And information security is already vitally important for every business in our connected global society. No real solution for compliance or information security is possible without proper authentication of users. But authentication by user name and passwords is not reliable anymore. There are lots of stronger authentication methods on the market, but regrettably there is not the best solution in respect to cost, reliability and user convenience in every situation.

Strong Authentication Advantage

Many organizations are discovering that traditional password-based authentication systems frustrate users and administrators, while remaining costly to the organization. A recent study cites that password-related calls account for more than 30% of all Helpdesk calls. Unlike passwords, strong authentication systems do not require the hassle of memorizing a series of letters, numbers, and symbols, nor do they require periodic changing.

NetIQ connects to all leading authentication methods. Although there still is a lot of good old username password combination in use for authentication in the virtual world, there is general consensus that passwords are too vulnerable and not secure anymore. New, more stronger, authentication methods have been launched into the market. Authentication methods like contact cards, contactless cards, biometric technologies, one time password generators, hardware/software tokens and many more have all gained traction on the market. But regrettably none of these solutions is the best fit for every authentication requirement within a modern company. There is an urgent need for a more generic solution that enables companies to select a bundle of methods simultaneously, that serves specific and generic needs and is future proof. Adding new methods to NetIQ is a simple standardized and fast process.

NetIQ Advanced Authentication Framework - Web Service Overview

The NetIQ Advanced Authentication Framework - Web Service allows you to authenticate non-domain joined clients.

How Does It Work?

NetIQ Advanced Authentication Framework - Web Service enables users to authenticate in Active Directory/ Novell DSfW using their own authenticators on non-domain joined clients. It interacts with NetIQ Advanced Authentication Framework - Authenticore Server, which performs the actual authentication. The NetIQ Advanced Authentication Framework – Web Service acts as a proxy between the Authenticore server and for example a Linux based client.

The NetIQ Advanced Authentication Framework – Web Service is using [SOAP](#) version 1.1 for exchanging structured information and [WSDL](#) for describing network service.

Benefits:

- Authenticate users in Domain from the outside of the Domain.
- Users use authenticators of their domain accounts.
- You can use not only Microsoft Windows-based clients, but, for example, Linux-based client or browser on your cell phone or tablet.

Integrates with NetIQ Advanced Authentication Framework Edition

NetIQ Advanced Authentication Framework Edition is a strong authentication security solution that enables users to log on to their workstation and Windows domains. Designed and tested for enterprise-level deployments, NetIQ tightly integrates with Active Directory to allow administrators to secure network and workstation access. See NetIQ Advanced Authentication Framework Administrator Guide for detailed configuration information, or contact an NetIQ sales representative to learn more about this product.

Getting started

The following chapters will provide the details on how to get started using the NetIQ Advanced Authentication Framework – Web Service.

What is Included

The distributive of the NetIQ Advanced Authentication Framework - Web Service includes next files:

_webservice

- webservice.msi – NetIQ Advanced Authentication Framework - Web Service installer.

GUIDES

- NAAF_Web_Service_Administrator_Guide.pdf – NetIQ Advanced Authentication Framework - Web Service documentation in pdf format.

NetIQ Advanced Authentication Framework – Web Service

NetIQ Advanced Authentication Framework – Web Service performs the following challenges:

1. System.Guid Logon(string domain, string username, string subsystem, byte[] identifier)

The function provides authentication using domain name, username, subsystem name and identifier wrapped by BioAPI.

2. System.Guid Logon1N(string domain, string subsystem, byte[] identifier)

The function provides 1-N authentication using domain name, subsystem name and identifier wrapped by BioAPI. Can be used along with Flash Drive + PIN and Universal Card authentication service providers.

3. System.Guid LogonRaw(string domain, string username, byte[] bspId, string subsystem, byte[] rawIdentifier)

The function provides authentication using domain name, username, authentication service provider identifier, subsystem name and raw authentication data. See [Preparing raw authentication data](#).

4. System.Guid Logon1NRaw(string domain, byte[] bspId, string subsystem, byte[] rawIdentifier)

The function provides authentication using domain name, authentication service provider identifier, subsystem name and raw authentication data. Can be used along with FlashDrive+PIN and Universal Card authentication service providers. See [Preparing raw authentication data](#).

After successful authentication NetIQ Advanced Authentication Framework - Web Service can return user password and/or username if you need. These actions use the following functions:

- string GetPassword(System.Guid sessionId);
- string GetUserName(System.Guid sessionId).

Terms

1-N authentication – is an authentication mode when no need to input username. It will be detected automatically after authentication by NetIQ Advanced Authentication Framework - Authenticore Server.

Authentication service provider – is a component that implements communication between NetIQ Advanced Authentication Framework and authentication device.

BSP – see *Authentication service provider*.

One-Time Password – is a temporary password which is automatically generated at the current time in according to special algorithm.

OTP – see *One-Time Password*.

Subsystem – is an object of Active Directory that contains the data such as usernames, passwords, records, custom data and etc. These data are used by NetIQ Advanced Authentication Framework.

Checking State of NetIQ Web Service

You can check a state of NetIQ Advanced Authentication Framework – Web Service simple opening the following webpage in your browser: <https://<servername>/Service.svc?wsdl>, where <servername> is a name or IP-address of your IIS server. If you'll see XML-page containing AuthLogon definitions name, then the NetIQ Advanced Authentication Framework – Web Service works correctly. In case of any problems please follow the next instruction:

1. Open IIS Manager and check status of AuthWebService;
2. If AuthWebService site uses not default port, please try to use the next link: <https://<server-name>:<portnumber>/Service.svc?wsdl>, where <portnumber> - port number using by AuthWebService;
3. If you got Certificate Error please install required certificate.

Identifiers of Authentication Service Providers

You can use the following authentication service providers GUIDs for *bspld* parameter:

1. BIO-key Biometric Service Provider Version 1.9 – {EC4AC729-B969-6E46-BD2F-56B6055E18F8};
2. Universal Card Authentication Provider – {ED2D1872-4DAC-A84B-AF7C-188642267D56};
3. USB Flash Drive Authentication Provider – {1AF29AB5-0A30-0046-95DB-4FDA28989051};
4. OATH OTP Authentication Provider – {C7D6704E-F66A-4EF0-93A3-C5EF13F0C7A2};
5. RADIUS Authentication Provider – {E4828EC2-B520-46FC-9624-EB98487A7F2B}.

Preparing Raw Authentication Data

Universal Card Authentication Service Provider

This is the description of algorithm for forming raw authentication data for Universal Card authentication service provider:

1. Get MD5 hash of specified PIN code using Windows CryptoAPI (16 bytes);
2. Get MD5 hash of Card serial number (16 bytes);
3. Write array of the following data:
 - a. "REMOVABLE_BSP_SIGN" string;
 - b. Length of Card serial number;
 - c. MD5 hash of Card serial number;
 - d. MD5 hash of specified PIN code;
 - e. GUID of Card type (see Identifiers of card types);
 - f. Length of additional card information.

Identifiers of Card Types

You can use the following GUIDs for different supported card types:

1. RF IDEas cards: {2976548C-9797-450E-91D4-4CA4451A14D2};
2. OMNIKEY cards: {C91A345F-FDA9-4BC7-8F96-902B25E33011};
3. TMC Legic cards: {6BF122E4-695E-4589-8B29-E9C797F045D3}.

RADIUS Authentication Service Provider

RADIUS Authentication Service Provider can be used along with various RADIUS servers. Authentication data of the provider can be a domain password in the case when RADIUS server uses authentication by domain password or other passwords, or OTP depending on RADIUS server settings. These data are submitted in C String (i.e. ASCII string with terminal zero ('\0')).

Flash Drive + PIN Authentication Service Provider

Authenticator's File

When you enroll Flash Drive + PIN authenticator NetIQ Advanced Authentication Framework creates hidden file named FlashPinBspLogon.dat on enrolled USB flash drive. This file contains encrypted private key. Private key is generated via [RSA algorithm](#) with 1024 bit length. Encryption type is [DES](#). The encryption key is [SHA-1](#) hash of the specified PIN code.

Preparing Raw Authentication Data

This is the description of algorithm for forming raw authentication data for Flash Drive + PIN authentication service provider:

1. Generate 20 random bytes;
2. Get SHA-1 hash of 20 random bytes;
3. Get signature - sign hash by a private key from FlashPinBspLogon.dat file on enrolled USB Flash Drive using CryptoAPI;
4. Write array of the following data:
 - a. "REMOVABLE_BSP_SIGN" string in UTF-16 encoding with zero at the end;
 - b. Length of USB flash drive serial number (4 bytes, decimal);
 - c. USB flash drive serial number in UTF-16 encoding without zero at the end;
 - d. Length of 20 random bytes (4 bytes);
 - e. 20 random bytes;
 - f. Length of signature (4 bytes);
 - g. Signature.

OATH Authentication Service Provider

OATH TOTP (Time-based One-Time Password) is based on [TOTP algorithm](#). We use seed which contains 40-hex digits only when enrolling an authenticator. Later mobile application generates temporary code which contains 6 decimal digits depending on seed, generation interval and current time. User inputs this temporary code for authentication. OATH Authentication Service Provider generates few temporary codes for the situation if the time on mobile device and NetIQ Workstation and NetIQ Authentication Server differs from each other. The number of temporary codes depends on NetIQ *TOTP checking window* policy. Please read *NetIQ OATH Authentication Provider User Guide*.

Error Codes Description

Here you can find the description of possible NetIQ errors. Also you can use [MSDN website](#) for detailed description of Microsoft and Windows Script Host errors (such as 0x80070005 "Access is denied").

RPC Server Errors

0xC0FF000FL	RPCS_E_LOGON_USER	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
0xC0FF0010L	RPCS_E_READ_USER_NAME	Server could not read the name of user account under which the server must work
0xC0FF0011L	RPCS_E_REGISTER_INTERFACE	Server could not register RPC-interface
0xC0FF0012L	RPCS_E_WRITE_USER_NAME	Server could not save user account name under which it must work
0xC0FF0013L	RPCSKEY_E_WRONG_CLIENT	Server requested the Enterprise Key, is not the domain member or its request is incorrect
0xC0FF0014L	RPCSKEY_E_GET_TICKET	Could not get Kerberos Ticket of the Authenticore server which requested the Enterprise Key
0xC0FF0015L	RPCSKEY_E_NOT_LOCAL_CALL	This function is intended for the local call only
0xC0FF0016L	RPCSKEY_E_CONNECT_SERVER	Could not find Authenticore server or establish connection with it
0xC0FF0017L	RPCSKEY_E_REGISTER_SPN	Could not register Service Provider Name (SPN)
0xC0FF0018L	RPCSKEY_E_CREATE_TIKET	Could not get Kerberos Ticket using data received from Authenticore server
0xC0FF0019L	RPCSKEY_E_GET_TICKET_NO_SPN	Could not get Kerberos Ticket from Authenticore server, which had requested Enterprise Key: SPN is not registered. Most likely, the error occurred because Active Directory data replication had not been completed. In this case, please wait until replication is completed and then click Retry button

0xC0FF001AL	RPCSKEY_E_CLIENT_NOT_MEMBER_OF_GROUP	Authenticore server, which has requested Enterprise Key, is not included into the Authenticore Servers group. Most likely, the error occurred because Active Directory data replication had not been completed. In this case, please wait until replication is completed and then click Retry button
0xC0FF001BL	RPCS_E_NO_DELEGATE	The level of impersonalization, allowed by the requested side, is lower than "Delegate" level.
0xC0FF001CL	RPCS_E_WAIT_FOR_LICENSE	Server installation has not been completed. Currently the server is in progress of adding license.
0xC0FF001DL	RPCS_E_DELEGATION_DISABLED	Computer account is not trusted for delegation
0xC0FF001EL	RPCS_E_SENSITIVE_ACCOUNT	Cannot connect to the Authenticore server. Please, ensure that for your account the "Account is sensitive and cannot be delegated" option is turned off
0xC0FF0463L	RPCS_E_LOGON_LOGON_FAILED	Could not authenticate the user by provided authenticator
0xC0FF044FL	RPCS_E_LOGON_LOGON_BY_PASSWORD_FAILED	Could not authenticate the user by the entered password. The error could also occur if the entered account was invalid.
0xC0FF0451L	RPCS_E_ENUM_TEMPLATES_PUT_ITEM_FAILED	User could not re-enroll the authenticator
0xC0FF0453L	RPCS_E_ENUM_TEMPLATES_ADD_FAILED	User could not add new authenticator
0xC0FF0455L	RPCS_E_ENUM_TEMPLATES_REMOVE_FAILED	User could not remove the authenticator
0xC0FF045BL	RPCS_E_FIND_SERVER	Could not find Authenticore server
0xC0FF045EL	RPCS_E_FIND_LICENSED_SERVER	Could not find Authenticore server with active license.
0xC0FF0461L	RPCS_E_ADD_LICENSE	Could not add license
0xC0FF0463L	RPCS_E_LOGON_LOGON_FAILED_EX	Could not authenticate the user by provided authenticator
0xC0FF0465L	RPCS_E_ADD_LICENSE_EX	Could not add license
0xC0FF04BBL	RPCS_E_MANAGER_CREATE_FAILED	Could not permit User to use authenticators

0xC0FF04BDL	RPCS_E_MANAGER_REMOVE_FAILED	Could not forbid authenticators for User
0xC0FF04CCL	RPCS_E_USER_PUT_SETTINGS_FAILED	Could not initialize settings for User
0xC0FF04CEL	RPCS_E_USER_CLEAN_AUTHENTICATORS_FAILED	Could not clear the list of enrolled authenticators of user
0xC00004CFL	RPCS_E_COMPUTER_CANTWRITEOBJECT	Could not initialize settings for computer
0xC0FF04D2L	RPCS_E_USER_GET_SETTINGS_FAILED	Could not obtain settings for User
0xC0FF04D3L	RPCS_E_USER_GET_TEMPLATES_FAILED	Could not get the list of enrolled authenticators of user
0xC0FF04D4L	RPCS_E_USER_CHANGE_PASSWORD_FAILED	Could not change password for user
0xC0FF04D5L	RPCS_E_USER_PUT_PASSWORD_FAILED	Could not set password for user
0xC0FF0516L	RPCS_E_SERVER_CAN_NOT_START	Could not start Authenticore Server service
0xC0FF0517L	RPCS_E_SERVER_CAN_NOT_READ	Authenticore Server service could not read data from Active Directory
0xC0FF0518L	RPCS_E_SERVER_CAN_NOT_WRITE	Authenticore Server service could not write data into Active Directory
0xC0FF0519L	RPCS_E_SERVER_CAN_NOT_DECODE	Authenticore Server service could not decrypt data retrieved from Active Directory. Either data was corrupted or the Enterprise Key has been changed
0xC0FF051BL	RPCS_E_GETKEYS_FAILED	Could not transfer Enterprise Key to server
0xC0FF051CL	RPCS_E_GETKEYS_FROM_FAILED	Could not get Enterprise Key from server
0xC0FF051FL	RPCS_E_EXPORT_KEYS_FAILED	Could not export Enterprise Key
0xC0FF0521L	RPCS_E_IMPORT_KEYS_FAILED	Could not import Enterprise Key
0xC0FF0523L	RPCS_E_GENERATION_KEYS_FAILED	Could not generate Enterprise Key
0xC0FF0524L	RPCS_E_AD_IS_OFFLINE	Active Directory is offline
0xC0FF06BCL	RPCS_E_LOGON_REFUSED_BY_RULES	Logon refused by security rules.
0xC0FF06BDL	RPCS_E_RULESERVER_CALL_FAILED	Error occurred while checking security rules

SrvWrapper Errors

0xC1050457L	SRVWRAPPER_E_SERVER_NOT_FOUND	The user could not be authenticated. The error could occur due to 1. Authenticore server was not found 2. The authentication method is not supported by available Authenticore servers (required BSP module is missing on server) 3. Lost communication with Domain Controller 4. The required subsystem was not installed
0xC1050458L	SRVWRAPPER_LOG_E_SERVER_NOT_FOUND	The user could not be authenticated. The error could occur due to: 1. Authenticore server was not found 2. The authentication method is not supported by available Authenticore servers (there is no required BSP module on server) 3. Lost communication with Domain Controller. 4. The required subsystem was not installed.
0xC105045CL	SRVWRAPPER_E_LOCAL_USER	Either user account or authenticator is invalid.
0xC105045DL	SRVWRAPPER_E_NOT_BIOUSER	Authentication Failed. Press OK to try again.
0xC1050466L	SRVWRAPPER_E_CACHE_USED	Authenticore server not found. User could not be logged in using authenticator from cache

Password Filter Errors

0xC104057AL	PWDFILT_E_PASSWORD_SET_FAILED	Error while resetting password for user
0xC104058AL	PWDFILT_E_PASSWORD_CHANGE_FAILED	Error while changing password for user

Password Manager Errors

0xC1080585L	PWDMGR_E_ERROR_OCCURED	An error occurred during Password Manager work
0xC1080586L	PWDMGR_E_CHANGE_PASSWORD_FAILED	Could not change password for user It is recommended to check "Minimal password age" domain setting. In case its value differs from 0, it is possible that password change can be denied because the password has been already changed within the specified time interval. Also, password cannot be changed in case "User cannot change password" account setting is enabled
0xC1080587L	PWDMGR_E_BAD_START_TIME	The time period specified using command prompt had expired before Password Manager was started. The service has been stopped

EventLog Errors

0xC10705DCL	LOG_E_CANT_WRITE_REMOTE_LOG	Could not get access to remote Log Server There is either no Log Server, it was turned off, or being reloaded. In case the error persists, it is recommended to check Firewall settings and the correctness of the domain names permission.
-------------	-----------------------------	--

BioAPI Errors

0xC1010000L	BIO_E_INITIALIZE	Could not initialize BioAPI framework
0xC1010001L	BIO_E_LOAD_MODULE	Could not load the required BioAPI BSP module
0xC1010002L	BIO_E_ENROLL	Could not get enrolled authenticator
0xC1010003L	BIO_E_IDENTIFY	Could not get authenticator
0xC1010004L	BIO_E_VERIFY	Could not compare user's authenticators
0xC1010005L	BIO_E_DATA_CORRUPTED	Could not load authenticators from the memory. Data is corrupt
0xC1010006L	BIO_E_COMPARE_BSP_MISMATCH	The type of enrolled authenticator does not correspond to the type of the given authenticator
0xC1010007L	BIO_E_COMPARE_DATA_MISMATCH	Authenticator does not correspond to the enrolled authenticator

Authenticore Server Errors

0xC1000000L	LOGON_E_CREATE_TEMPLATE	Could not create authenticator. The list of user authenticators may be corrupt
0xC1000001L	LOGON_E_LOAD_TEMPLATE	Could not load the authenticator. The list of user authenticators may be corrupt
0xC1000002L	LOGON_E_READ_COLLECTION	Could not read user authenticators list
0xC1000003L	LOGON_E_WRONG_PASSWORD	Either user account or password value is invalid
0xC1000004L	LOGON_E_WRONG_AUTHENTICATOR	Authentication Failed. Press OK to try again.
0xC1000005L	LOGON_E_CANNOT_LOGON	Authentication Failed. Press OK to try again.
0xC1000006L	LOGON_E_OPERATION_DENIED	This operation is forbidden by administrator
0xC1000007L	LOGON_E_TOO_MANY_AUTHENTICATORS	The allowed amount of authenticators is exceeded
0xC1000008L	LOGON_E_SERVER_NOT_FOUND	Could not set connection with the Authenticore server. Check network connection and try again. If the error persists please contact your system administrator
0xC1000009L	USER_E_CHANGE_PASSWORD_INVALID	The passwords were unsynchronized
0xC100000AL	USER_E_CHANGE_PASSWORD_POLICY	Could not change password for the user. The generated value does not satisfy the security policies. It is recommended to check "Minimal password age" domain setting. In case its value differs from 0, the password change can be denied because the password has been already changed within the specified time interval
0xC100000BL	USER_E_CHANGE_PASSWORD_ACCESS_DENIED	Could not change user password. The current security settings forbid the user to change his/her password
0xC100000CL	USER_E_CHANGE_PASSWORD	Could not change password for the user. The reason is unknown

0xC100000DL	LOGON_E_WRONG_DATE	Time interval from the moment the user authenticator was obtained and the moment it was delivered to the Authenticore server exceeds the value of the settings, which regulates authenticator validity period (5 minutes by default). This error can occur as a result of either system time desynchronization between user computer and Authenticore server or criminal attempt to use authenticator intercepted over network
0xC100000EL	LOGON_E_LOAD_BSP	Could not load BioAPI BSP module. Either the required BSP module is not installed on the Authenticore server or it failed to load. The system will attempt to authenticate on another Authenticore server.
0xC100000FL	CHANGEPWD_OUT_OF_RESOURCES	System resources are not enough to change password for the user
0xC10006BEL	LOGON_E_LOGON_REFUSED_BY_RULES	Logon refused by security rules.
0xC10006BFL	LOGON_E_DENY_LOGON_BY_PASSWORD	Logon by password was denied.

Authentication Providers Errors

0xC1020000L	PROV_E_NO_USER	The user was not found
0xC1020001L	PROV_E_ACCESS_DATA	Could not get access to user data
0xC1020002L	PROV_E_PROPERTY_NOT_FOUND	The property was not found. Perhaps the Active Directory scheme is not extended by additional attributes
0xC1020003L	PROV_E_ALREADY_CREATED	User is already allowed to use authenticators
0xC1020004L	PROV_E_CREATE_ENUMERATOR	Could not create users sorting object
0xC1020005L	PROV_E_SEARCH_USER	Could not start user search
0xC1020006L	PROV_E_ACCESS_DENIED	Access is denied. Not enough permissions
0xC1020009L	PROV_E_AD_OBJECT_NOT_BIND	Unable to get object data in AD.
0xC102000AL	PROV_E_ADAM_OBJECT_NOT_BIND	Unable to get object data in ADAM.
0xC102000BL	PROV_E_ADAM_NOT_OPERATIONAL	Could not get access to ADAM server

Cryptography Errors

0xC1030001L	CRYPT_E_USER_DATA_CORRUPTED	User data corrupted
0xC1030002L	CRYPT_E_VERIFY_SIGNATURE	Either user data or the Enterprise Key is corrupt
0xC1030003L	CRYPT_E_INIT_PROVIDER	Could not initialize required Crypto Service Provider (CSP)
0xC1030004L	CRYPT_E_GENERATE_OR_EXPORT_KEYS	Could not generate or export cryptographic keys
0xC1030005L	CRYPT_E_IMPORT_KEYS	Could not import cryptographic keys
0xC1030006L	CRYPT_E_DATA_CORRUPTED	Data is corrupted

Manager Errors

0x01060001L	MGR_S_LAST_TEMPLATES_REMOVED	Several authenticators were deleted because the allowed amount of authenticators was reduced
0xC1060002L	MGR_E_LOGON_DOMAIN_REDIRECTION_OP_UNSUPPORTED	The operation is not supported while the domain redirection policy is enabled

Plugins Errors

0xC1090000L	PLUGIN_E_NOT_REGISTERED	The specified Plug-in is not registered on the server.
0xC1090001L	PLUGIN_E_CANNOT_CREATE	Could not create registered Addon.
0xC1090002L	PLUGIN_E_USER_NOT_TRUSTED	The user was authenticated by password.
0xC1090003L	PLUGIN_E_OPERATION_DENIED	The operation is forbidden.

Licensing Errors

0xC10A0001L	LIC_E_INVALID_FORMAT	Invalid format of license data.
0xC10A0002L	LIC_E_LICENSE_NOT_FOUND	License not found.
0xC10A0003L	LIC_E_LICENSE_STORAGE_CORRUPTED	License storage data is corrupted.
0xC10A0004L	LIC_E_LICENSE_CORRUPTED	License data was changed or corrupted.
0xC10A0005L	LIC_E_RESTRICTIONS_ERROR	Your license does not match the time period restriction, the product version restriction or the domain name is wrong
0xC10A0006L	LIC_E_PUBLICKEY_CORRUPTED	Cannot validate digital signature of the license. Certificate may be missing or corrupt.
0xC10A0007L	LIC_E_PLUGIN_DOESNT_SUPPORT_LICENSING	This Addon does not support licensing.
0xC10A0008L	LIC_E_START_LIMIT_ERROR	The actual number of installed Authenticore Servers exceeds the number allowed by the License.
0xC10A0009L	LIC_E_USERS_LIMIT_ERROR	Actual number of Authasas-enabled accounts exceeds the number allowed by the License.
0xC10A000AL	LIC_E_DOWNGRADE	The license you are trying to add allows fewer number of licensed objects than you have now

Backup Provider Errors

0xC10C0001L	BACKUPPROV_E_BAD_PASSWORD_OR_DATA	Bad password or data corrupted.
-------------	-----------------------------------	---------------------------------

Administration Tools Errors

0xC10D0001L	ADMTOOLS_E_NOT_MLADMIN	You don't have rights for changing settings on this page. Please, ensure that you are the member of the Authasas Admins group and these rights are delegated to the Authasas Admins group.
0xC10D0002L	ADMTOOLS_E_NO_RIGHTS	You don't have rights for changing settings on this page. Please, ensure that these rights are delegated to you.

GINA Errors

0xC10B0645L	GINA_E_LOGON_BY_PASSWORD_FAILED	Could not authenticate the user by the entered password. The error could also occur if the entered account was invalid.
-------------	---------------------------------	--

Data Errors

0xC10E0001L	DATA_E_FIELD_NOT_SET	The field value is not set.
0xC10E0002L	DATA_E_VALUE_NOT_SET	The subfield value is not set.
0xC10E0003L	DATA_E_SUBSYSTEM_NOT_FOUND	Subsystem is not found.
0xC10E0004L	DATA_E_ACCESS_DENIED	Data access denied.
0xC10E0005L	DATA_E_RECORD_NOT_FOUND	Record is not found.
0xC10E0006L	DATA_E_USER_NOT_TRUSTED	The user was authenticated by password.
0xC10E0007L	DATA_E_INVALID_FIELD_NAME	Invalid field name.
0xC10E0008L	DATA_E_BAD_SCHEME_SIGNATURE	Bad schema signature
0xC10E0009L	DATA_E_USERS_LICENSE_NOT_FOUND	Subsystem users license is not found.
0xC10E000AL	DATA_E_BASE_LICENSE_NOT_FOUND	Subsystem servers license is not found.
0xC10E000BL	DATA_E_NOT_SUBSYSTEM_USER	User is not using given subsystem.
0xC10E000CL	DATA_E_USERS_LICENSE_LIMIT_ERROR	Actual number of the subsystem-enabled accounts exceeds the number allowed by the License.
0xC10E06A5L	DATA_E_ADMIN_GET_DATA_FAILED	Unable to get the subsystem data for the user
0xC10E06A6L	DATA_E_USER_GET_DATA_FAILED	User is unable to get the subsystem data
0xC10E06A7L	DATA_E_ADMIN_FAILED_TO_ALLOW_TO_USE_SS	Unable to make user the client of the subsystem
0xC10E06A9L	DATA_E_USER_FAILED_TO_BE_SS_CLIENT	User failed to be a client of the subsystem
0xC10E06ADL	DATA_E_ADMIN_CHANGE_DATA_FAILED	Unable to change the subsystem data for the user
0xC10E06AFL	DATA_E_USER_CHANGE_DATA_FAILED	User is unable to change the subsystem data
0xC10E06B1L	DATA_E_RESET_PASSWORD	The password was reset for user. Could not reset special data for subsystem
0xC10E06B3L	DATA_E_ADMIN_REMOVE_SS_DATA	Unable to deny user to use the subsystem
0xC10E06B5L	DATA_E_USER_REMOVE_SS_DATA	User was unable to quite using the subsystem
0xC10E06B7L	DATA_E_RESET_DATA	The password was reset for user. Could not reset special data for subsystem

0xC10E06B8L	DATA_E_RESET_DATA_FULL_RESET	The password was reset for user. Could not reset special data for subsystem. The subsystem data was reset completely
0xC10E06BAL	DATA_E_SUBSYSTEM_LIST_INVALID_COMMON	The subsystems list for user is invalid and was cleared.
0xC10E06BBL	DATA_E_SUBSYSTEM_LIST_INVALID_SS	The subsystems list for user is invalid and was cleared.
0xC10E06C0L	DATA_E_CONTAINER_NOT_FOUND	Data container is not defined in the schema.

Troubleshooting

 This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

Authentication Failed

Description:

Authentication using Web Service has failed.

Cause:

Web Service is installed separately from Authenticore Server and authentication providers are not installed on Web Service.

Solution:

In the case if Web Service is installed separately from Authenticore Server, it is necessary to install authentication providers on Web Service.

Index

A

Active Directory 4, 7
Administrator 1, 4-5
Authentication 1, 3-7, 9-10, 19, 24
Authenticator 10
Authenticore server 4

B

BIO-key 8

C

Card 6, 8-9

D

Data 10, 22
Domain 4

E

Error 7, 11

G

Generate 10
GINA 21

O

OATH 8, 10
OTP 7

P

Password 7, 15
PIN 6, 9-10

R

RADIUS 8-9

S

Server 4, 7, 11, 17, 24

System 6

T

TOTP 10

U

User 10

W

Windows 4, 11

Workstation 10