Authentication in D2000

Authentication is a process of verification of the user's identity, i.e. the verification that the user is who he says he is. The authentication of the user is performed based on something the user knows (user's name and password), what he owns (USB token, personal chip card with encryption and identification PKI key), or user's measurable biometric characteristic (fingerprint, iris scan).

The D2000 Server verifies the name and password of the user in D2000. In some cases it is better to delegate verification of user's identity to Windows domain which enables:

- to use the same password to log into D2000 and Windows (NTLM authentication),
- to use the same name and password to log into several D2000 systems; the password can be changed in one system and is valid for all systems - the password into Windows (NTLM authentication),
- automatic logon into D2000 without entering the name and password based on user's logon to Windows (Kerberos authentication),
- to secure the logon of the user into D2000 by hardware means (USB token, personal chip card with encryption and identification PKI key) in such a way that these hardware means are used to log the user into Windows and then the Kerberos authentication is used for logon into D2000,
- to disable to logon of the user into D2000 by Windows user management tools,
- to set policies and parameters for D2000 password by Windows user management tools.

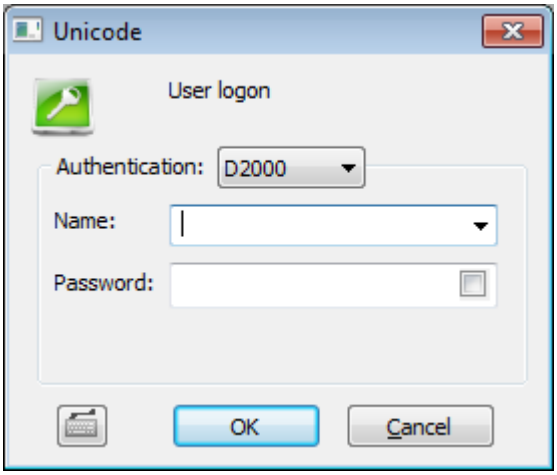
Note for Linux and Raspberry PI platforms: as of D2000 version 12.2.65 (patches from 27.5.2020 and later), Kerberos authentication is also available on Linux x64 and Raspberry PI platforms. The following steps must be performed to make it work:

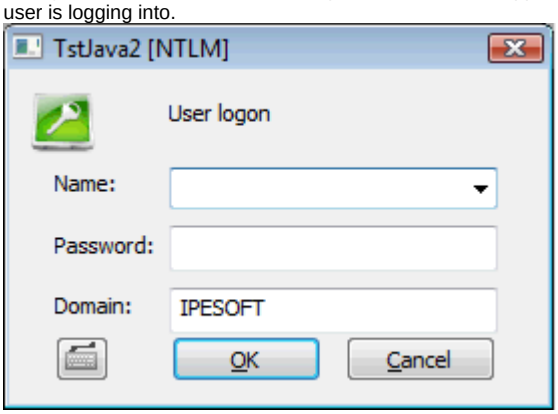
- joining of Linux/Raspberry PI server to Windows domain
  (with the command *realm join domain_name*, e.g. *realm join IPSTEST.SK*)
- enabling access of the D2000 Server (kernel) to the */etc/krb5.keytab* file. One option is to configure the D2000 Server to run as root, another - less dramatic - is to configure access rights for the group under which the D2000 Server is running. For example, if the d2users group is used, you need to run:
  chgrp d2users /etc/krb5.keytab
  chmod 640 /etc/krb5.keytab

On the Linux platform, authentication within one domain (*IPSTEST.SK*) and between two domains was tested (hi.exe run under a user in the *IPESOFT.SK* domain, D2000 server on a Linux server in the *IPSTEST.SK* domain. In both cases, the value of the AuthSecPrinc parameter was set to *SRVAPP$@IPSTEST.SK*, where *SRVAPP* is the name of a Linux computer joined in the Windows domain.

Authentication method

The following authentication methods are supported in D2000 System from version 7.02.008:

Authentication method	Meaning
D2000	The authentication of the user's name and password is performed by the process D2000 Server. This is the standard authentication method. It uses name and password which are saved in configuration of object User. Logon dialog displays user's name and password: 

NTLM	The authentication subsystem Windows NTLM (NT LAN Manager) verifies the user's name and password. This subsystem is available from the Windows NT 4.0 version and the authentication is done in the domain defined by configuration parameter Domain . After the authentication D2000 Server will obtain the information about successful / unsuccessful verification of user's name and password in the domain. If the authentication is successful it will look for the object of User type with the same user name and check whether the NTLM authentication (parameter Authentication methods) is allowed, the domain name is the same and the logon is enabled. Dialog box contains: user name and password, name of application, text *[NTLM]* in the title and the name of Windows domain the user is logging into.  **Note:** NTLM authentication is available on standalone computer with locally defined users (in this case Domain is computer's name) as well as in Windows domain (Domain is the name of domain). If the connection to an authentication authority failed, the user is not logged on. The NTLM authentication will change to D2000 authentication and this warning occurs: "NTLM authentication has failed. Enter your login name and password from D2000."
Kerberos	The authentication of the user's identity is made by the authentication subsystem Windows Kerberos (available from the version Windows 2000). It verifies the identity of the user which is logged into Windows so that the logon into D2000 System is automatic without Logon dialog or entering name and password. D2000 Server will obtain the information about user's name and domain from Windows Kerberos authentication subsystem. If the domain name matches the user's configuration parameter Domain then it will look for the object of User type with the same user name and check whether the Kerberos authentication (parameter Authentication methods) is allowed and the logon is enabled. **Note:** Using Kerberos authentication method is almost as risky as using the start parameters /AN and /AP which allow to start HI process and perform auto logon without entering user's name and password if the user leaves the workstation and does not lock the desktop (usage of the start parameters /AN and /AP is even more hazardous because they allow to steal the password for later misuse, while Kerberos permits only immediate misuse but not stealing of the password). Therefore we recommend: • instruct the users to lock the desktop or log off when they leave the workstation • use the Kerberos authentication only in secure places • use the hardware key to logon into Windows (USB token, security card etc), which automatically lock the desktop if the user removes the hardware key **Note:** Kerberos authentication is available only in Windows domain, not on standalone computer, because it requires a software infrastructure which is installed only as a part of Windows domain controller.
SPNEGO	Authentication method available for D2000 versions above 12.00.061. The authentication of the user's identity is performed by the Windows Kerberos authentication subsystem (available from the version Windows 2000). It verifies the identity of the user who is logged into Windows so that the logon into D2000 System is automatic without Logon dialog and without entering name and password. D2000 Server will obtain the information about user's name and domain from Windows Kerberos authentication subsystem. If the domain name matches the user's configuration parameter Domain then it will look for the object of User type with the same user name and check whether the SPNEGO authentication (parameter Authentication methods) is allowed and the logon is enabled. **Note:** SPNEGO authentication is available only in Windows domain, not on standalone computer, because it requires a software infrastructure which is installed only as a part of Windows domain controller.
RFID	This method is available from D2000 version 9.1.30. The user is identified by scanning the RFID card. RFID authentication works if RFID tag is installed on the client work station on some of serial COM ports, D2000 HI is running with the parameters (parameters of console) that ensure the handling of the RFID tag (see Console preferences - RFID parameters). After scanning the RFID card, there can occur two situations: 1. Any picture that implements <ENTRY OnRFID> is not opened in D2000 HI - it means that HI logs on the user with particular RFID card automatically. 2. At least one picture that implements <ENTRY OnRFID> is opened in D2000 HI - it means that HI does not log the user but calls OnRFID entry to the all pictures, which implement this entry, and lets the application script handle this entry.

Note 1: For other operating systems than Windows only the D2000 authentication is supported.
Note 2: For other authentication methods than D2000 authentication a dynamic library d2auth.dll is required (it is located in the directory D2000.EXE\bin).
Note 3: Other authentication methods than D2000 authentication are implemented in following D2000 processes and modules: D2000 HI, D2000 GrEditor, D2000 CNF, D2000 Application Manager, D2000 DDE Server, D2000 System Console, D2000 Tell, D2000 Browser, D2000 ODBC Driver

Configuration parameters of authentication

Following configuration parameters are used to configure the authentication methods:

Parameter	Meaning
AuthMethod	Default method of authentication the process D2000 Server requires from all users. Possible values of parameter are: • D2000 • NTLM • Kerberos • SPNEGO (Only for Thin client and Smart Web)
AuthSecPrinc	Security principal of authentication. Parameter is mandatory for Kerberos and SPNEGO authentication. Security principal can be the name of account which the process D2000 Server runs under. By default (kernel.exe runs as service under account *Local System)*, the *Security principal* is the computer account in domain. Its name is the same as the name of computer and at the end is the symbol $. If the process kernel.exe has been run manually (from a command line) the *Security principal* is the account of the user in domain. **Example:** Domain is *MyCompany*, server is *SrvApp1*, process kernel.exe runs as service on account *LocalSystem*. Parameter AuthSecPrinc can be *srvapp1$* or *srvapp1$@MyCompany*. If users belongin to a different domain OtherCompany want to be authenticated, AuthSecPrinc must be *srvapp1$@MyCompany* and moreover the domain MyCompany must trust the domain OtherCompany. **Note:** inter-domain autentication was tested on server srvapp114v belonging to domain ipstest.sk, AuthSecPrinc=*srvapp114v$@ipstest.sk*. HI was run on a computer belonging to domain IPESOFT, domain ipstest.sk trusted the domain IPESOFT. **Example:** Domain is MyCompany, process kernel.exe has been started from the command line by user D2User. Parameter AuthSecPrinc can be *d2user* or *d2user@MyCompany.* **Note:** Security principal can be defined also by the tools for Active Directory management so that it is independent from user name under which the process kernel.exe runs. More information can be obtained from Active Directory documentation and the instructions for the utility ktpass.exe on Microsoft web site.

Parallel usage of several authentication methods

During NTLM/Kerberos authentication the user name and password are not transferred between the computer with the process D2000 Server and computer with the user process (HI, Cnf, GrEditor etc). Instead only so called tokens are exchanged between the authentication subsystems Window NTLM /Kerberos on these computers and transferred via network. That is why the NTLM/Kerberos authentication will not work if the domain controller is not available (a breakdown/switch-off the domain controller, an access of client from behind the firewall etc.).

For these reasons as well as for the sake of configuration flexibility, the client process (HI, Cnf, GrEditor etc.) can use other authentication method than the default configured by parameter AuthMethod provided that:

- all mandatory configuration parameters are configured (i.e. Domain for NTLM/Kerberos and AuthSecPrinc for Kerberos)
- the authentication method is enabled in user's Authentication methods

Selection of non-default authentication method is possible via start parameter of client process /AF<Method>. In case of D2000 ODBC Driver, the authentication method is configured in DSN configuration.

Note: The process D2000 Server loads the configuration parameters of authentication from Windows registry during every connect of a process that supports logon of the user (HI, Cnf, GrEditor etc.) and sends these parameters to this process. The reason is to change dynamically the default authentication method (e.g. during domain controller's failure) and allow to users to restart HI and logon to application by different authentication method (D2000) without the necessity to modify the start-up parameters of HI on all computers. This scenario requires that the D2000 authentication method is enabled for every user and every user knows his "backup" password to D2000, which is saved in the configuration of user.

Debugging the authentication

The Debug category **DBG.Authentication** is intended for debugging the authentication. It can be activated at start-up of the process by the start parameter **/E+DBG.Authentication** or dynamically by D2000 System Console.
When the debugging is activated, the log of process D2000 Server or log of the client process (HI, Cnf, GrEditor etc) will contain detailed information about the phases of authentication (for NTLM and Kerberos authentication), which are intended for technical support.

Related pages:

Application configuration