Atostek ID Active Directory Registration Service 1.0 Installation Guide

for Windows

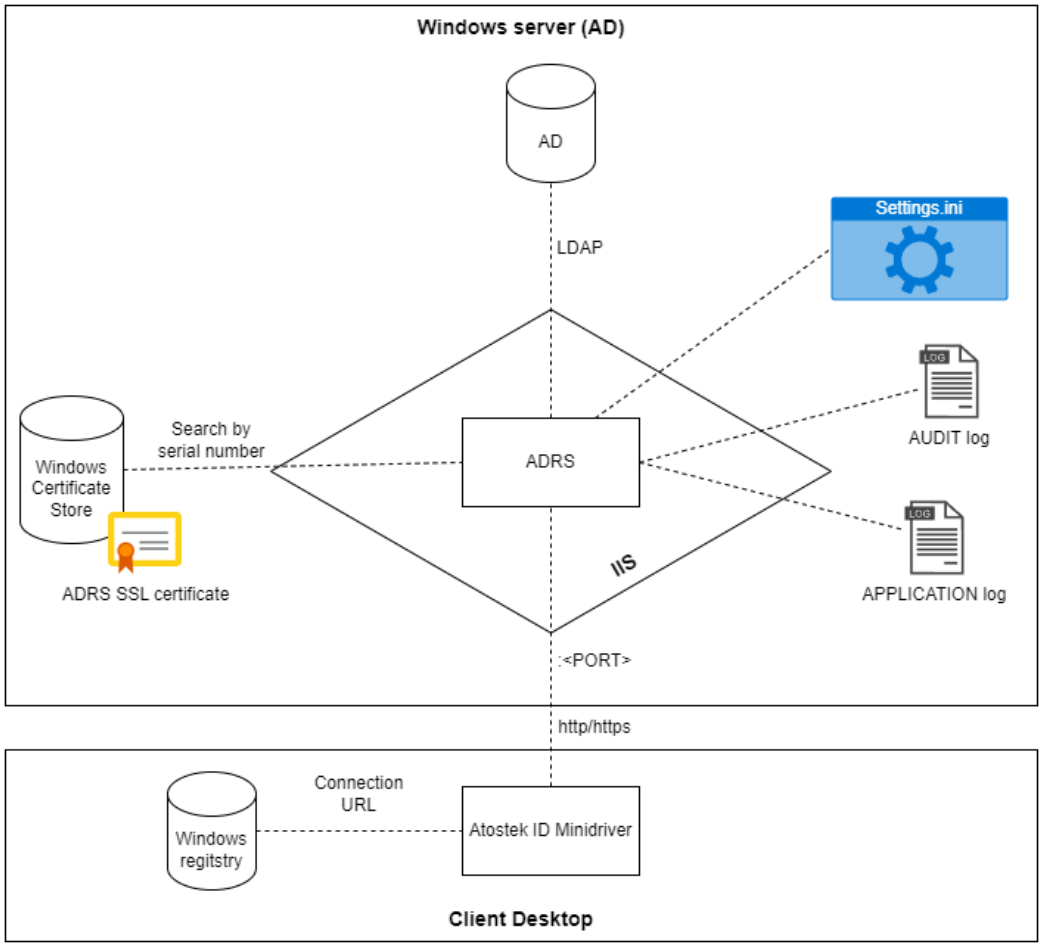
Atostek

Table of contents

1. What is Atostek ID ADRS?

Atostek ID ADRS is a separate active directory registration service (ADRS) that configures users' smart cards to match ad user identity. Microsoft is making changes to the certificate-based authentication and ADRS's responsibility is to match these new requirements (https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16). ADRS is a service that is installed to the organization's own environment and connected to the selected AD. Service configures each user altSecurityIdentity attribute to match new requirements. For each user X509IssuerSerialNumber mapping is added when the smart card is connected to the client device. ADRS finds the matching user from the AD and adds the corresponding X509IssuerSerialNumber mapping for the user. After that the user can log in to the device by using the smart card. Atostek ID also supports multiple installations of ADRS connected to same AD to enable higher availability. See more about the configuration of Atostek ID client from Atostek ID installation guide.

Atostek ID ADRS software runs on the Microsoft Windows operating system. The following diagram illustrates the ADRS system.



2. Installing the software using the installer

2.1. Before installing

Make sure that the firewall accepts TCP communication to the port the Active Directory is listening to and that the firewall accepts communication to the ADRS from client users. ADRS requires AD users to have the privileges to read and write data to AD user's “altSecurityIdentities” -attribute.

Example of giving right permissions:

1. Open the program "Active Directory Users and Computers".
2. If you want to create a new user for editing, please do so.
3. *View → Advanced Features* on.
4. Click domain root with the second mouse button and select *Delegate Control*.
5. Press *Add* and add the user you want to be able to edit altSecurityIdentities.
6. Select "Create a custom task to delegate".
7. Select "Only the following objects in the folder" and "User objects".
8. Permissions: In the Permissions dialog, select "Property-specific" and find and select "Read/Write altSecurityIdentities".

Install the TLS certificate that you will be using with the service to the system certificate store in the “Personal” -section. Install both private and public certificate keys. After the installation copy the certificate serial number that will be used at the ADRS installation to identify the correct certificate from the system store.

2.2. Installation

ADRS can be installed using the installation wizard or from the command line. For command line installation, you need to start a command prompt with administrator rights. If the installation package is in the current folder, it can be installed with e.g. the following command:

> msiexec /i ADRegistrationService_Setup.msi /qn ADRS_LDAP_URL="aid.atostek.com:5592" ADRS_LDAP_USERNAME="adrs" INSTALL_DESKTOP_SHORTCUT="true"

All parameters:

> msiexec /i ADRegistrationService_Setup.msi /qn CERTIFICATE_SERIALNUMBER="" ADRS_TRUSTED_CERTIFICATES="tc1,tc2" ADRS_LDAP_BASE_OBJECT="base" ADRS_LDAP_URL="aid.atostek.com:5592" ADRS_LDAP_USERNAME="adrs " ADRS_LDAP_PASSWORD="" INSTALL_DESKTOP_SHORTCUT="true" INSTALL_MENU_SHORTCUT="true" PORT=”9000”

A complete list of command line parameters can be found in the following table:

Parameter	Value type	Explanation
CERTIFICATE_SERIALNUMBER	string	Https certificate serial number which will be used for ADRS service.
ADRS_TRUSTED_CERTIFICATES	Comma separated list. eg. “tc1,tc2”	List of trusted smart card issuers
ADRS_LDAP_USERNAME	string	AD username which ADRS uses for attribute modification
INSTALL_DESKTOP_SHORTCUT	boolean (“true”/”false”)	If ADRS start icon is added to the desktop
INSTALL_MENU_SHORTCUT	boolean (“true”/”false”)	If ADRS start icon is added to the menu
PORT	int	Port number which the service starts listening

The program can be uninstalled from the Control Panel (Control Panel → Programs → Programs and Features) or from the command line (defaults as above):

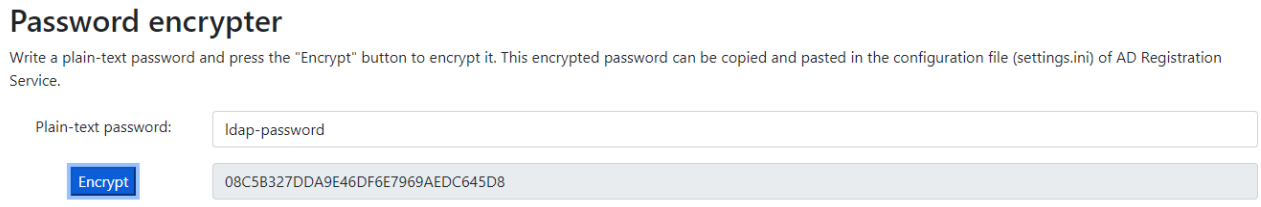
> msiexec /x ADRegistrationService_Setup.msi /qn

2.3. After installation

After starting the ADRS service at the host computer you can access the administration view by opening the browser navigating the URL and port that you have defined for the service and adding ”/administration” to the URL. For example:

https://localhost:9000/administration

From the admin view, you can see the service health check and the version and encrypt the password. Password encryptor is used for encrypting all passwords configured for ADRS service. For AD connection, you must encrypt the AD user password that you have defined to be used with the ADRS. Add the password to the plain-text field and click the ”encrypt” -button. After that, you will have the encrypted password which you can copy to the settings.ini file. Settings file can be found from the same folder where you installed the service. After updating the AD-user password start the ADRS again to achieve connection to the AD.



3. Service maintenance and usage

When the TLS certificate is updated, you must update the new certificate serial number to the settings.ini file and after that restart the service. After that, the new certificate is in use. By default, service logs two types of logs: Audit log and Application log. By default, both logs are written to the C:/logs -path. The audit log is written to file "C:\\logs\\ADRegistrationServiceLog_AUDIT_*.txt". The audit log contains the log of each configuration made to the AD. Application log is written to file "C:\\logs\\ADRegistrationServiceLog_APPLICATION_*.txt" and it contains more logs of the running service. A new log file is created for each day.