AD FS eParaksts mobile Authentication Module - Administrator's Guide

Prepared by

LVRTC

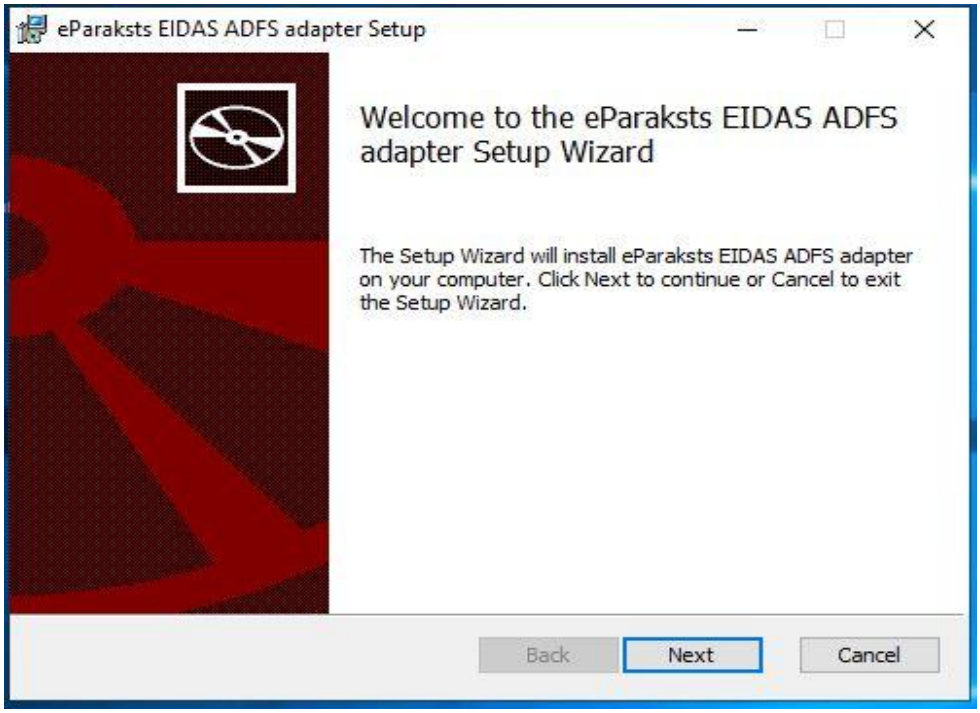
13.07.2023

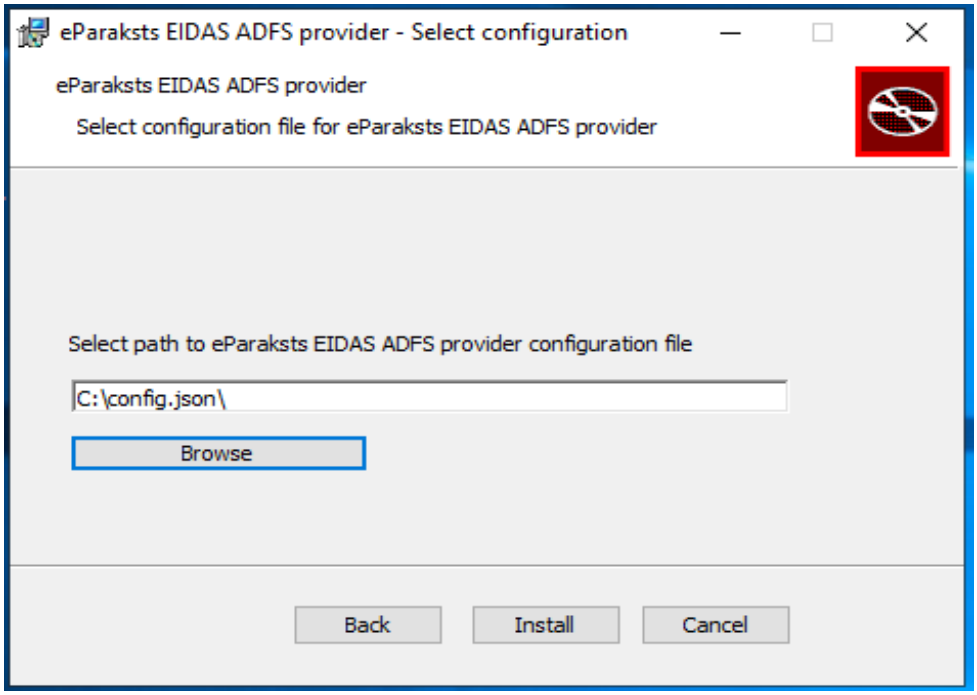
Table of Contents

Installation Instructions

The AD FS eParaksts mobile authentication module is designed to be installed on Windows Server 2019 (also tested on Server 2016) with the AD FS service installed and configured according to the INSTAL_ADFS guidelines.

The installation is performed by running the installation msi file: **eParaksts-ADFS-Adapter-{version}.msi** and specifying the path to the configuration file, which contains the necessary configuration parameters in JSON format.





For a successful installation, a running AD FS service is required, as it will be restarted during the installation process. The installation must be executed with Administrator privileges.

The module requires network access from the AD FS server to either:

- **https://eidas.eparaksts.lv/** (production environment)
- **https://eidas-demo.eparaksts.lv/** (test environment).

1 Installation Configuration Description

Parameter Name	Parameter Name	Parameter Name
authorization_server	Authorization server corresponding to the EIPS connection	lvrtc-eipssign-as
authorization_scope	Authorization scope corresponding to the EIPS connection	urn:lvrtc:fpeil:aa
client_id	Client identifier corresponding to the EIPS connection	test
client_secret	Client password corresponding to the EIPS connection	demodemo
acr_values	Authentication flow identifier Supported values: • urn:eparaksts:authentication:flow:mobileid	urn:eparaksts:authentication:flow:mobileid
userinfo_givenname_field	Field for the user's first name in the EIPS authentication response	given_name
userinfo_identity_field	User identifier from the EIPS platform, which must be compared to the ldap_trustedx_identity_attribute attribute Possible values: serial_number (Personal Code in the format PNOLV-123456-12345), email, username The attribute will be stored in the AD field specified by ldap_trustedx_identity_attribute. If the parameter is not set, the comparison is performed only based on the identity_linking_policy.	serial_number
userinfo_familyname_field	Field for the user's last name in the EIPS authentication response	family_name

ldap_trustedx_identity_attribute	AD field for the user identifier to be compared with userinfo_identity_field. If the parameter is not set, the comparison is performed only based on the identity_linking_policy. Possible values: Any AD user attribute, e.g., eParakstsIdentity	eParakstsIdentity
identity_linking_policy	Identity verification policy: Possible values: link_identity_by_fullname - compares userinfo_givenname_field with AD givenName and userinfo_familyname_field with AD sn. If ldap_trustedx_identity_attribute and userinfo_identity_field are specified, their attribute values are also compared.	link_identity_by_fullname
ldap_trustedx_login_hint_attribute	AD field for the user's login name, used to avoid requiring the user to enter their username every time they authenticate	eparakstsLoginHint

2 Configuration Example

To apply this configuration, you must have access as an "Identity Platform Client" in the production or test environment.

{

"host": "eidas-demo.eparaksts.lv",

"client_id": "test",

"client_secret": "password",

"authorization_server": "lvrtc-eipsign-as",

"authorization_scope": "urn:lvrtc:fpeil:aa",

"userinfo_givenname_field": "given_name",

"userinfo_familyname_field": "family_name",

"userinfo_identity_field": "serial_number",

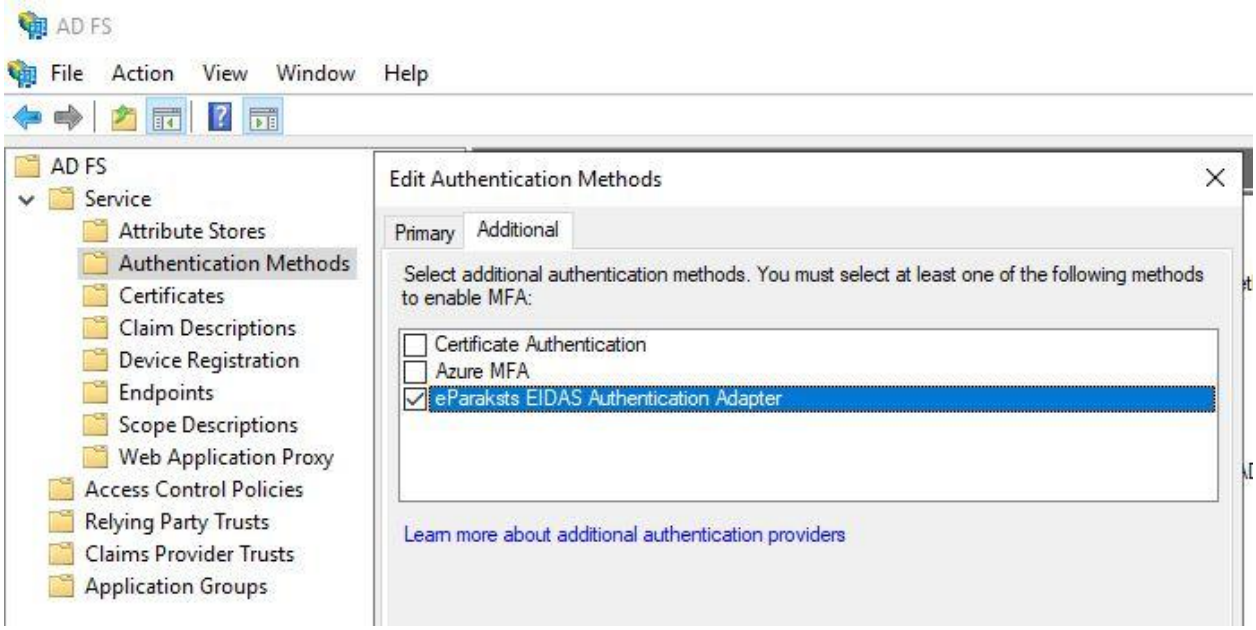
"acr_values": "urn:eparaksts:authentication:flow:mobileid",
"ldap_trustedx_identity_attribute": "eParakstsADFSIdentity",
"ldap_trustedx_login_hint_attribute": "eParakstsADFSUserName", "identity_linking_policy": "link_identity_by_fullname"

}

3 Enabling the AD FS eParaksts Module

To enable the AD FS eParaksts module, open the "AD FS Management" tool:

- Navigate to Services > Authentication Methods > Edit Multi-factor Authentication methods and select the eParaksts EIDAS Authentication Adapter checkbox.



4 Creating AD Attributes

If the necessary AD attributes required for configuring ldap_trustedx_login_hint_attribute and ldap_trustedx_identity_attribute are not available, these attributes can be created by executing the attached script (Create_EparakstsProvider_AD_attributes.ps1).

The script can be customized as needed by modifying parameter names, descriptions, counts, etc.

The script should be executed on the AD server from which AD FS retrieves Windows identities.Code Block 1 Add Atributes

5 Testing

Microsoft provides a tool to test ADFS. Configuration should be performed according to the instructions available at:
https://adfshelp.microsoft.com/ClaimsXray/TokenRequest

AD FS eParaksts Mobile Authentication Module - Administrator's Guide