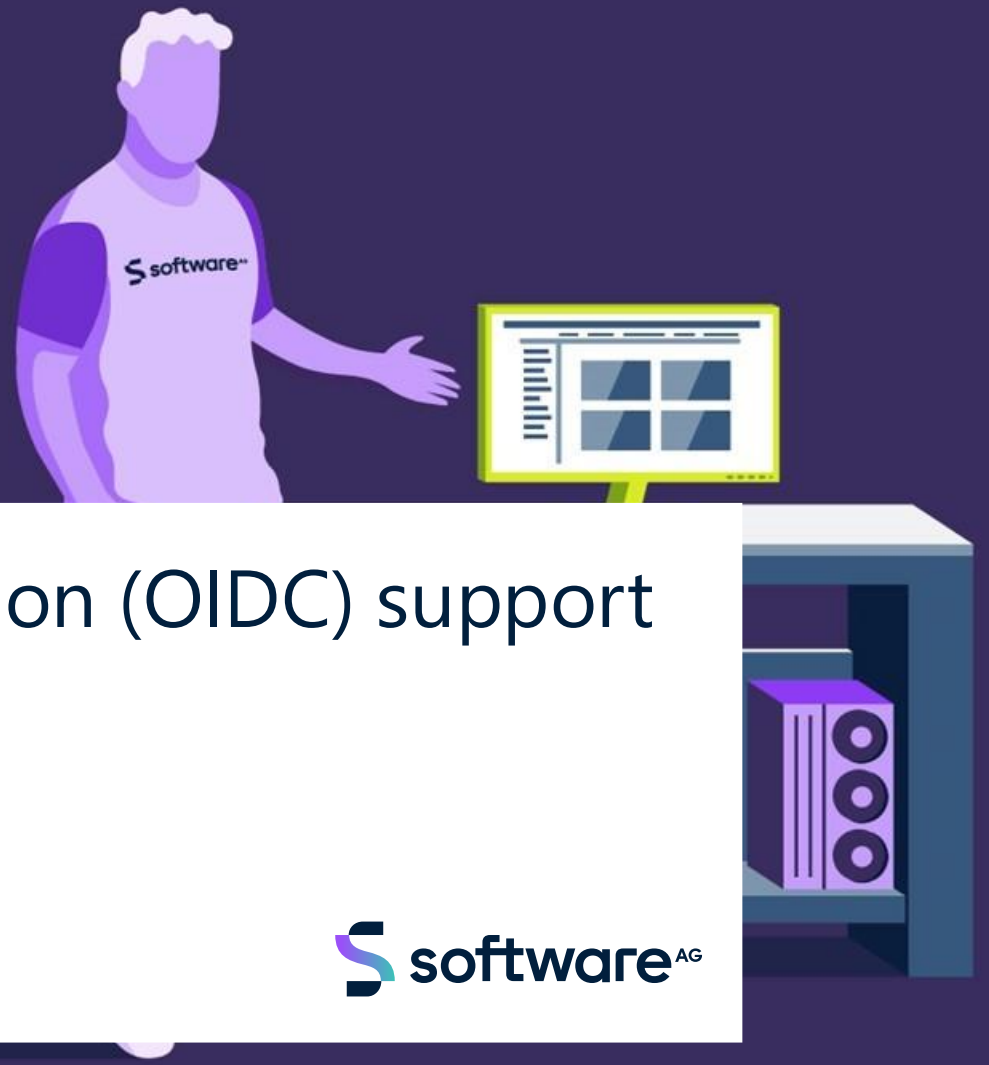


Ask R&D: Token-based Authentication (OIDC) support with Natural for Linux and Cloud

A&N Virtual User Group Event, May 19th, 2026

Marcel Schmall, Senior Software Engineer, A&N R&D
Zvonimir Ivanetic, Director A&N R&D Natural Open Systems, A&N R&D

What is the Requirement for Token-Based-Authentication?

A modern Enterprise authentication should offer

- **Single-Sign-On**
  Users expect to login only once, usually just on their notebook.

  Users should not additionally be prompted for username/password in applications.

- **Multi-Factor Authentication support**
  Solutions should leverage existing Multi-Factor-Authentication mechanism.

- **No need to maintain passwords in applications**
  For security reasons no application should cache or maintain user passwords additionally.

Preferred Protocol is OpenID Connect

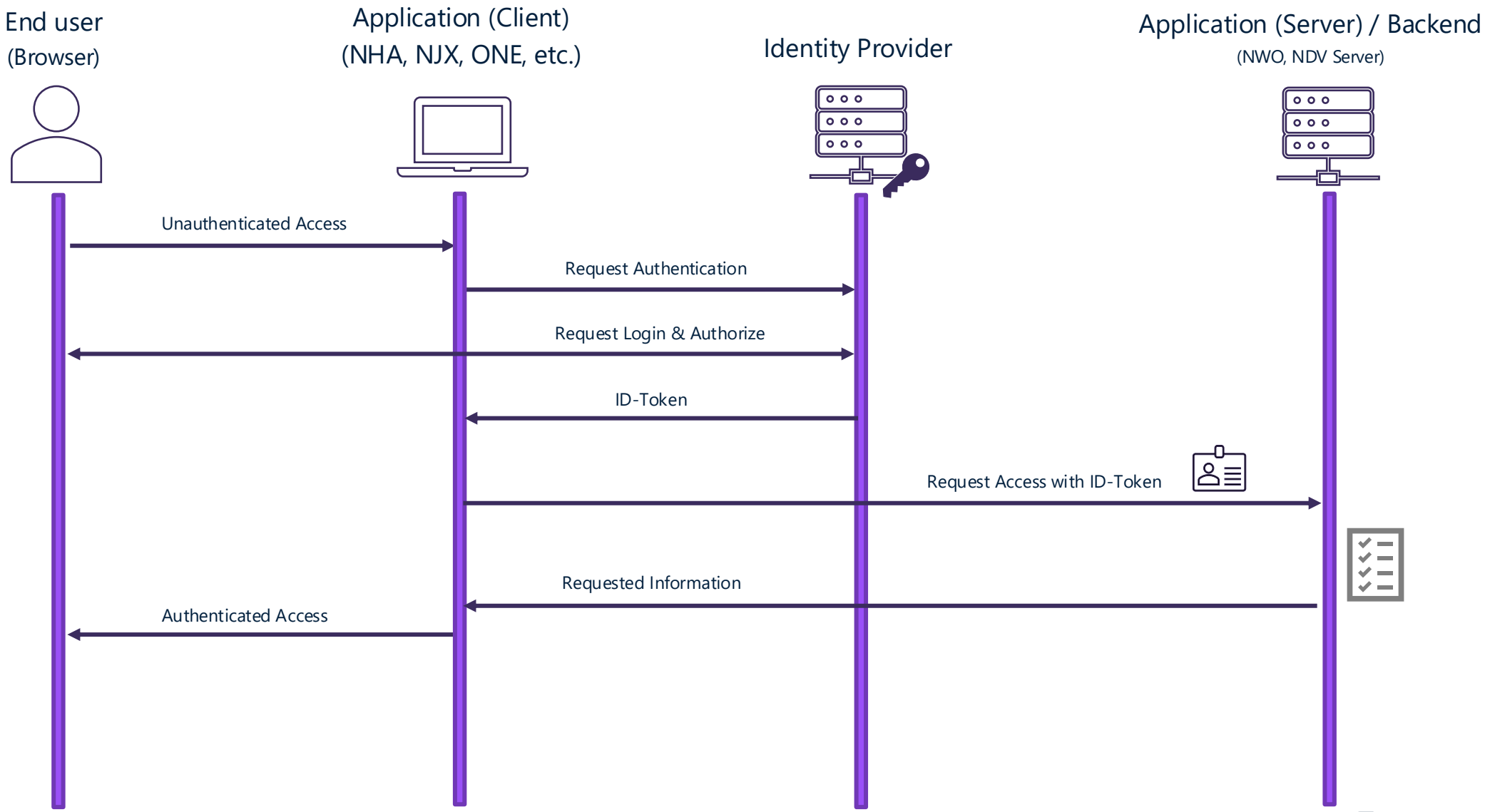
Why is OpenID Connect the right choice?

- **Most comprehensive**
  Well-established protocol for authentication for internet and enterprise environments, with huge offering on frameworks, covering all client scenarios (Web/Desktop/Mobile).

- **Simple and Developer-Friendly**
  Uses JSON/REST and widely adopted formats like JWT (JSON Web Tokens), making it much easier to implement and integrate compared to older protocols such as SAML.

- **Variety of Identity Provider (with Broker also SAML supported)**
  Microsoft Entra ID (Azure AD), Google Identity, Okta, Keycloak, etc.

How it works - OIDC Authentication Flow (Simplified)



What is the Id-Token?

- The ID-Token is a JSON Web Token (JWT)

  https://tools.ietf.org/html/rfc7519

- It is a security token that contains claims about the Authentication of an End-User.

- The claims are a set of name/value pairs defined by the OpenID Connect standard.

- The token is cryptographically signed by a trusted identity provider.

What is the Id-Token?

The Id-Token is a JSON-Web-Token (JWT.IO)

Login Information (ID-Token, encoded):


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjkzNDFhYmM
0MDkyYjZmYzAzOGU0MDNjOTEwMjJkZDNlNDQ1Mz
liNTYiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodH
RwczovL2FjY291bnRzLmdvb2dsZS5jb20iLCJhe
nAiOiI5MDk4OTQ3OTY2OTAtNm1udGhxbWltcDNv
ZG0yNnY4dTRrZDNmcW81NTFpN3EuYXBwcy5nb29
nbGV1c2VyY29udGVudC5jb20iLCJhdWQiOiI5MD
k4OTQ3OTY2OTAtNm1udGhxbWltcDNvZG0yNnY4d
TRrZDNmcW81NTFpN3EuYXBwcy5nb29nbGV1c2Vy
Y29udGVudC5jb20iLCJzdWIiOiIxMTM5OTY2NDk
yMTIyNjMyNDc0NzkiLCJoZCI6InNvZnR3YXJlYW
cuY29tIiwiZW1haWwiOiJ6aXZAc29mdHdhcmVhZ
y5jb20iLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwi
YXRfaGFzaCI6ImRiN1htS3o3Q01zSDhLQXhkMk5
oTHciLCJub25jZSI6ImVlNDcxZmU5ODM5ZTQ5Mm
NhNjcxNTdjZmYzNTY3ZjgzIiwiaWF0IjoxNjM4O
Tk4Njc3LCJleHAiOjE2MzkwMDIyNzd9.Fn_j9fL
1Ve8wug7e720BtPZXzLWQ0vuZSqgO9lMPlBwZOC
FkR17vOlkh7n0FegvIqLXArq5d-
7B37N6EmvwWrJUiEFwGc0CibLwAdTn3O4G4kYoE
uU5qsQBkv70iSri2hp-0FeBH3VXfEwm4Ct-
qrc2RuA7Eyjh4MUA8Uc6EXFgk0jfGste4jOKMh_
NC00TaQaBGzDI7INGLqq7Ii7tmJ2MDk2rgefYqg
IZ3cCXGFODTP7tQiUggzH0oFBSfgmdXFpExE0MB
mVSvuYyYJQu38k0GALG6OivCaSBXF_C8vzD_4nK
Z6qusZEUginP0uA8I3YG9CSf4iTeKyRH7cG90Ew
```


ID-Token (decoded):

Header:


```
{
 "alg":"RS256",
 "kid":"9341abc4092b6fc038e403c91022dd3e44539b56",
 "typ":"JWT"
}
```


Payload:


```
{
 "iss":"https://accounts.google.com",

 "aud":"909894796690-
6mnthqmimp3odm26v8u4kd3fqo551i7q.apps.googleusercontent.com",

 "sub":"113996649212263247479",

 "hd":"softwareag.com",
 "email":"ziv@softwareag.com",
 "email_verified":true,
 "at_hash":"db7XmKz7CMsH8KAxd2NhLw",
 "nonce":"ee471fe9839e492ca67157cff3567f83",
 "iat":1638998677,

 "exp":1639002277
}
```


Signature:


```
Fn_j9fL1Ve8wug7e720BtPZXzLWQ0vuZSqgO9lMPlBwZOCFkR17vOlkh7n0FegvIqLXArq
5d-7B37N6EmvwWrJUiEFwGc0CibLwAdTn3O4G4kYoEuU5qsQBkv70iSri2hp-
0FeBH3VXfEwm4Ct-
qrc2RuA7Eyjh4MUA8Uc6EXFgk0jfGste4jOKMh_NC00TaQaBGzDI7INGLqq7Ii7tmJ2MDk
2rgefYqgIZ3cCXGFODTP7tQiUggzH0oFBSfgmdXFpExE0MBmVSvuYyYJQu38k0GALG6O
ivCaSBXF_C8vzD_4nKZ6qusZEUginP0uA8I3YG9CSf4iTeKyRH7cG90Ew
```

Id-Token Validation

What needs to be considered?

- **Validate Signature**

  Verify that the ID-Token signature is valid, using a certificate which is stored in the JSON Web Key Store (JWKS).

  Applications can store certificates locally to improve performance, as they are not changed frequently.

- **Verify Issuer and Audience**

  Verify that the value of the “issuer” claim in the ID-Token is equal to expected issuer

  and the value of “audience” claim is equal to your applications client-Id.

- **Verify the expiry time**

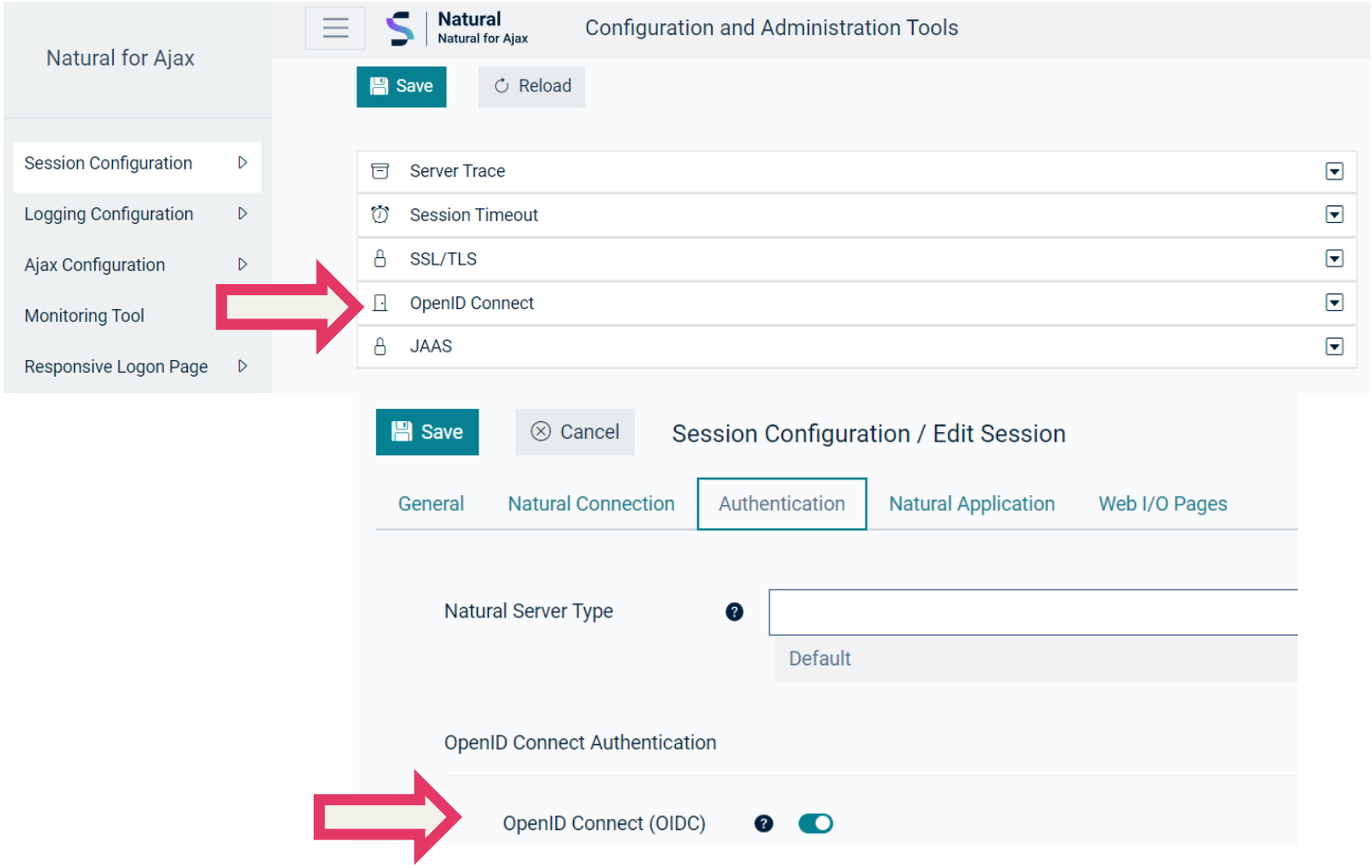
  Verify that the value of the “expiry” claim of the ID-Token has not passed.

How did we apply this to our products?

Natural for Ajax – Supports OIDC

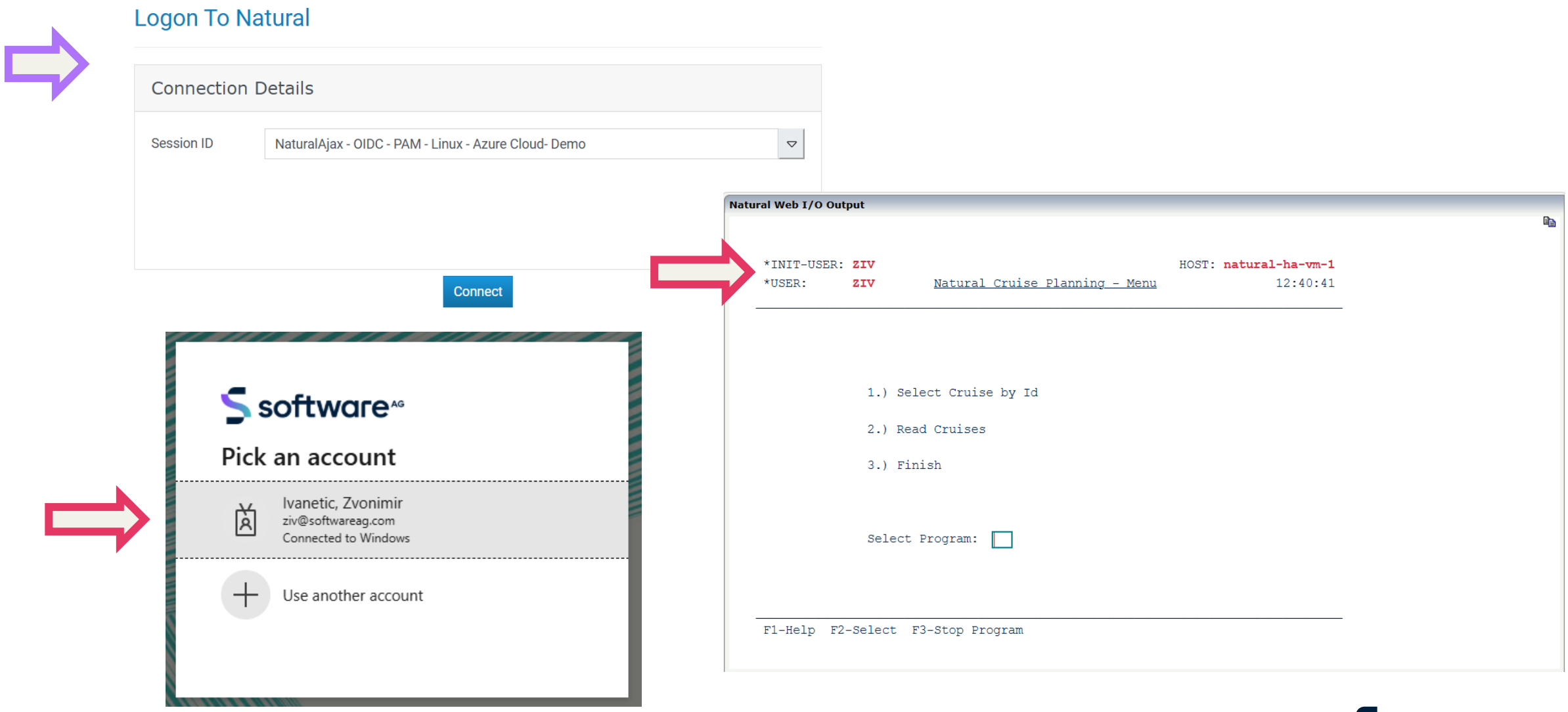
Single Sign On (SSO) with OpenID Connect (OIDC) – Natural for Linux and Cloud (only)

- User authentication is delegated to an OIDC Identity Provider.
- Prerequisite is WebIO server, which supports SSO with OIDC.
- Configuration and Administration tool supports corresponding OIDC settings.
- OIDC can be activated per session definition.



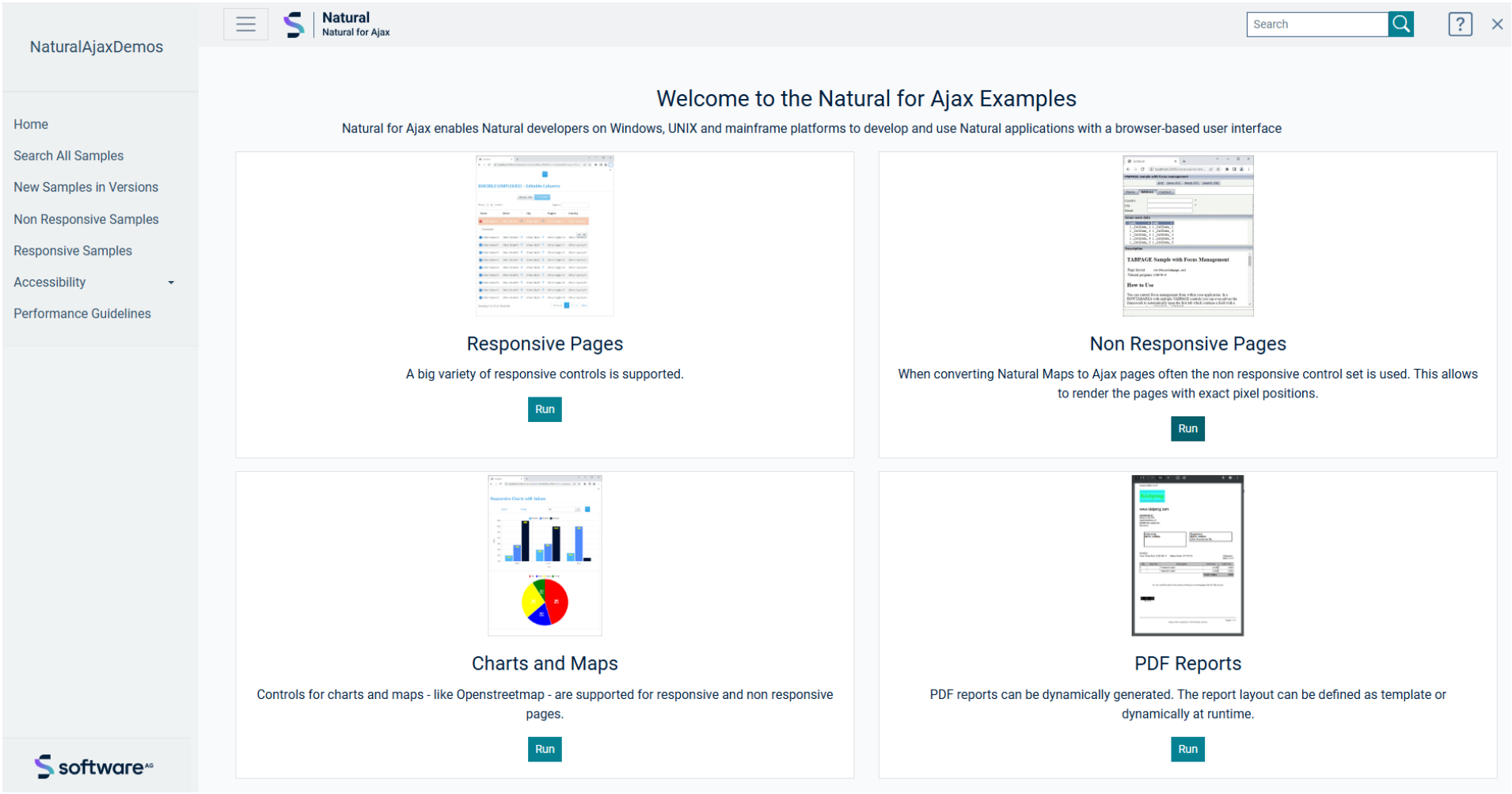
Natural for Ajax

Single Sign On (SSO) with OpenID Connect (OIDC) – Natural for Linux and Cloud (only)



Natural for Ajax

Single Sign On (SSO) with OpenID Connect (OIDC) – Responsive Pages

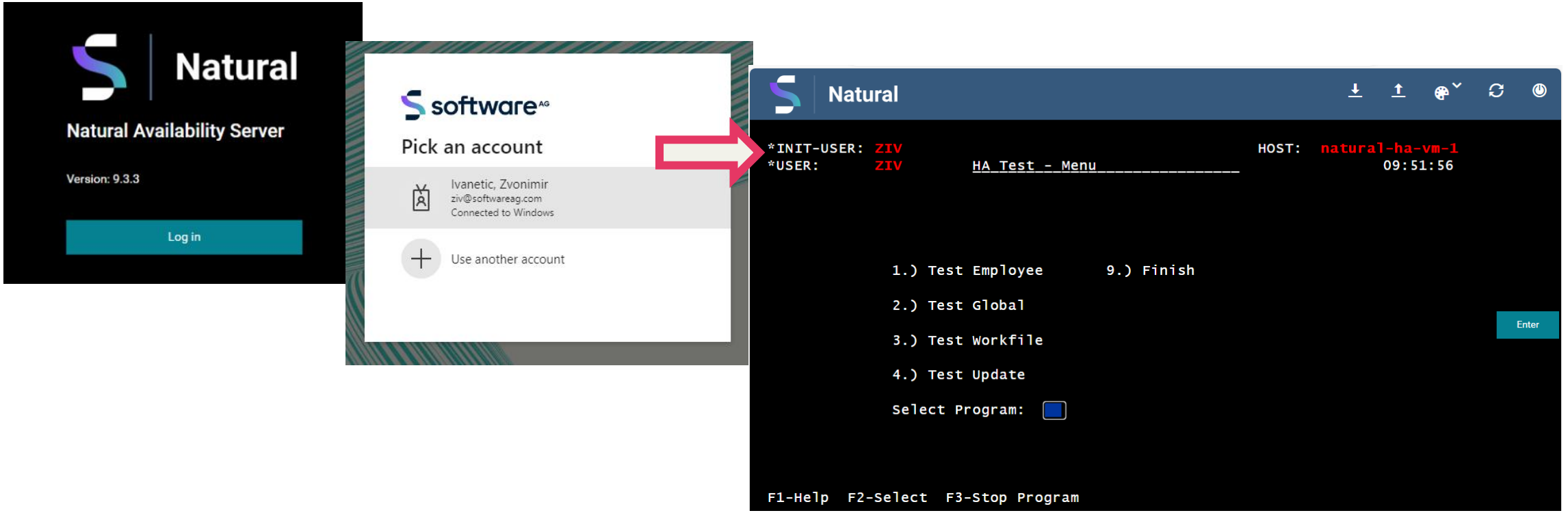


Natural Availability Server (NHA) - Supports OIDC

Single Sign On (SSO) with OpenID Connect (OIDC) – Natural for Linux and Cloud (only)

Open Id Connect Authentication

- Configured in “application.properties” file (see Online Documentation)



Token-based authentication support (OIDC with NHA)

It´s show time

software AG

Q&A