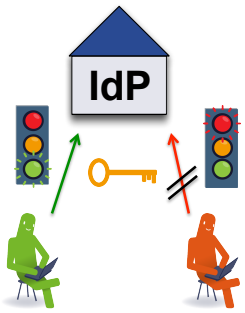
IdP User Authentication

How to do it the v3 way?



SWITCH

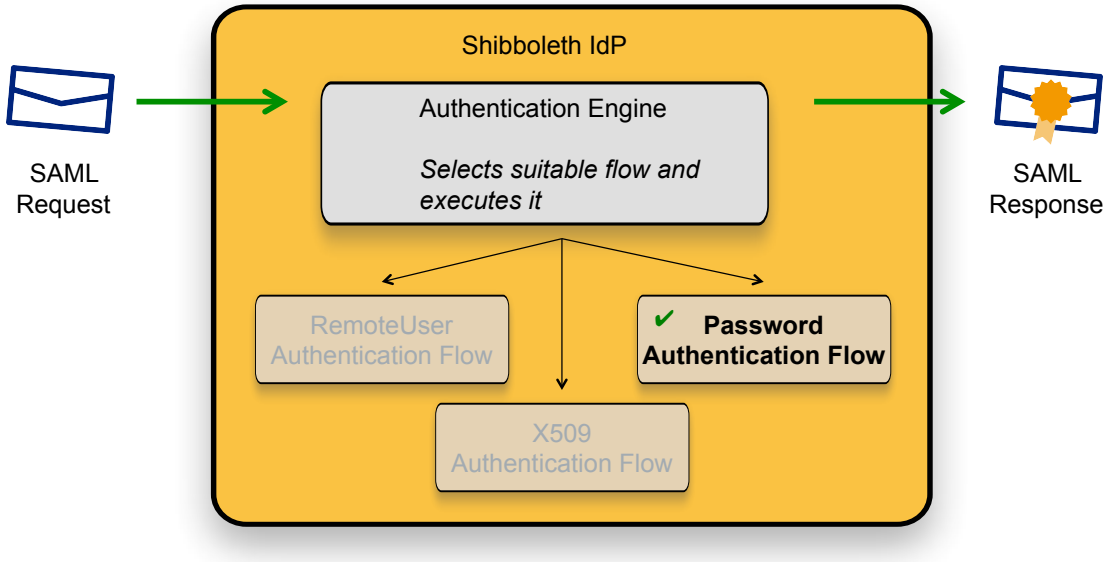
SWITCHaai Team
aai@switch.ch

From Login Handlers to Login Flows

- v2 uses "Login Handlers"
  - Typical/default setup: "UsernamePassword" login handler
    - Username/password login form
    - Authentication via JAAS and LDAP ("login.config")
  - Additional login handlers are available built-in (e.g. "RemoteUser") or as extension (e.g. "X.509", "Kerberos (SPNEGO)")

- v3 uses "Login Flows" (also called "Authentication Flows")
  - Typical/default setup: "Password" login flow
    - Username/password login form
    - Authentication via LDAP (natively), JAAS or Kerberos (username/password)
  - Additional login flows are available built-in (e.g. "RemoteUser", "X509"). A login flow for "SPNEGO/Kerberos" is in development.

Login Flows



Login Flows

- One or several flows can be activated.
- The authentication engine of the IdP selects a suitable flow depending on several criteria:
  - Does the SP request a specific authentication context type?
  - Does the SP request forced authentication?
  - Does the SP request passive authentication
- In practice, most deployments will use the "Password" login flow as the only one.
- ECP is supported out-of-the-box by the "Password" login flow. No special configuration is required.
  - But: Client must support ECP appropriately.

Authentication Configuration

- Login flow activation:
  - **`/opt/shibboleth-idp/conf/idp.properties`**:

    The active flows are specified via a regular expression (i.e. the order doesn't matter):

    ```
    idp.authn.flows = Password
    #idp.authn.flows = X509|Password
    ```

- Per login flow configuration:
  - **`/opt/shibboleth-idp/conf/authn/*-config.xml`**
- Side note: If multiple flows are activated, the order of the flows as defined in **`conf/authn/general-authn.xml`** might influence the flow selection process.

Configuration: Username/password with LDAP

- Most deployments use this authentication mechanism.
- Login flow for username/password authentication: "Password" (activated by default)
- Configuration is done in two properties files:
  - All LDAP parameters, except credentials: **`/opt/shibboleth-idp/conf/ldap.properties`**
  - Credentials are stored separately (for security reasons): **`/opt/shibboleth-idp/conf/credentials.properties`**
- The properties of the LDAP authentication can be re-used for the LDAP configuration of the attribute resolution (all defined in **`ldap.properties`**).

Example Configuration

- **/opt/shibboleth-idp/conf/ldap.properties**

```
idp.authn.LDAP.authenticator = bindSearchAuthenticator
idp.authn.LDAP.ldapURL       = ldaps://ldap-test2.aai.switch.ch:636
idp.authn.LDAP.useStartTLS   = false
idp.authn.LDAP.useSSL        = true
idp.authn.LDAP.sslConfig     = jvmTrust
idp.authn.LDAP.baseDN        = ou=People,dc=example,dc=org
idp.authn.LDAP.subtreeSearch = true
idp.authn.LDAP.userFilter    = (uid={user})
idp.authn.LDAP.bindDN        = cn=idp,dc=example,dc=org
```

- **/opt/shibboleth-idp/conf/credentials.properties**

```
[...]
idp.authn.LDAP.bindDNCredential = secret
[...]
```


Properties for LDAP authentication

- General options
  - **idp.authn.LDAP.authenticator**
    User lookup and authentication method. Must be set to "bindSearchAuthenticator".
- Connection options
  - **idp.authn.LDAP.ldapURL**
    URL of the LDAP server(s). Must start with ldap:// or ldaps://. (Multiple servers can be specified by listing multiple URLs, separated by spaces)
  - **idp.authn.LDAP.useStartTLS**
    Enable TLS encryption for ldap:// URLs (port 389) (if not enabled, the connection is not encrypted).
  - **idp.authn.LDAP.useSSL**:
    Enable TLS encryption for ldaps:// URLs (port 636). Must usually be set to "true".

Properties for LDAP authentication

- Connection options (continued)
  - **`idp.authn.LDAP.sslConfig`**
    Type of X.509 certificate verification method. Usually set to **`"jvmTrust"`**.
- User Directory options
  - **`idp.authn.LDAP.baseDN`**
    Entry point in user directory
  - **`idp.authn.LDAP.subtreeSearch`**
    Enable searching the whole tree. Usually set to "true".
  - **`idp.authn.LDAP.userFilter`**
    LDAP search filter. Takes the login name as input.

Properties for LDAP authentication

- LDAP service user options
  (The IdP connects to the LDAP server as this user to search for users.)
  - **`idp.authn.LDAP.bindDN`**
    Bind DN of the IdP service user
  - **`idp.authn.LDAP.bindDNCredential`**
    Password of the IdP service user

(Further properties for LDAP are available, but not described here. See the documentation for details.)

Hands-on 1: Explore the configuration

Get familiar with properties files:

- Which flows are enabled in **`/opt/shibboleth-idp/conf/idp.properties`**? (Hint: "idp.authn.flows")
- **`/opt/shibboleth-idp/conf/ldap.properties`**:
  - Which LDAP attribute holds the user's login name?
  - Which is the "Distinguished Name" (DN) of the service user the IdP uses for connecting to the LDAP server?
- Where is the password of the service user defined?

Hands-on 1: Solutions

- Enabled flows: "Password"
  `idp.authn.flows = Password`
- LDAP attribute holding the login name: "uid"
  `idp.authn.LDAP.userFilter = (uid={user})`
- DN of the service user the IdP searches users with:
  `cn=idp,dc=example,dc=org`
- In the file
  `/opt/shibboleth-idp/conf/credentials.properties`
  `(idp.authn.LDAP.bindDNCredential = secret)`

Hands-on 2: Migrate LDAP configuration from IdPv2

From IdPv2:

File **`/opt/shibboleth-idp/conf/login.config`**:

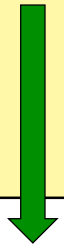
```
ShibUserPassAuth {
  edu.vt.middleware.ldap.jaas.LdapLoginModule required
    ldapUrl="ldaps://ldap-test1.aai.switch.ch:636 ldaps://ldap-test2.aai.switch.ch:636"
    baseDn="ou=People,dc=example,dc=org"
    bindDn="cn=idp,dc=example,dc=org"
    bindCredential="secret"
    userField="uid"
    subtreeSearch="true";
};
```

PS: Common and equivalent alternative to *userField*: *userFilter*

`userField="uid"` ⇔ `userFilter="uid={0}"`

Hands-on 2: Migrate LDAP configuration from IdPv2 (Hints)

```
ShibUserPassAuth {
  edu.vt.middleware.ldap.jaas.LdapLoginModule required
    ldapUrl="ldaps://ldap-test1.aai.switch.ch:636 ldaps://ldap-test2.aai.switch.ch:636"
    baseDn="ou=People,dc=example,dc=org"
    bindDn="cn=idp,dc=example,dc=org"
    bindCredential="secret"
    userField="uid"
    subtreeSearch="true";
};
```



- Edit **`/opt/shibboleth-idp/conf/ldap.properties`** and modify the property **`idp.authn.LDAP.ldapURL`**
- Restart Tomcat:

  `service tomcat7 restart`
- Test in browser

Hands-on 2: Solution

To IdPv3:

File **/opt/shibboleth-idp/conf/ldap.properties**:

```
[...]
idp.authn.LDAP.authenticator = bindSearchAuthenticator
idp.authn.LDAP.ldapURL       = ldaps://ldap-test1.aai.switch.ch:636 \
                               ldaps://ldap-test2.aai.switch.ch:636
idp.authn.LDAP.useStartTLS   = false
idp.authn.LDAP.useSSL        = true
idp.authn.LDAP.sslConfig     = jvmTrust
idp.authn.LDAP.baseDN        = ou=People,dc=example,dc=org
idp.authn.LDAP.subtreeSearch = true
idp.authn.LDAP.userFilter    = (uid={user})
idp.authn.LDAP.bindDN        = cn=idp,dc=example,dc=org
[...]
```

File **/opt/shibboleth-idp/conf/credentials.properties**:

```
[...]
idp.authn.LDAP.bindDNCredential = secret
[...]
```


Advanced Topics

- JAAS authentication, as used in v2, is still supported in v3
  - Supported by the "Password" login flow. Needs to be activated in **/opt/shibboleth-idp/conf/authn/password-authn-config.xml**
  - JAAS configuration file (corresponds to login.config): **/opt/shibboleth-idp/conf/authn/jaas.config**
  - JAAS authentication is recommended for:
    - Connecting to multiple LDAP trees with different user bases
      - Might be done with native LDAP authentication, but requires complex configuration.
    - Connecting to other user directories like RDBMs (using specific JAAS module)
  - See the documentation on the Shibboleth wiki for details.

References

Documentation

- **Authentication Configuration**
  https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationConfiguration
- **Password Authentication Configuration**
  https://wiki.shibboleth.net/confluence/display/IDP30/PasswordAuthnConfiguration
- **Password / LDAP Authentication Configuration**
  https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration
- **Advanced LDAP Configuration**
  http://www.ldaptive.org/docs/guide/authentication
- **Password / JAAS Authentication Configuration**
  https://wiki.shibboleth.net/confluence/display/IDP30/JAASAuthnConfiguration