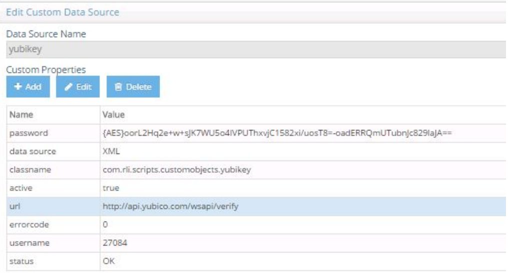
YUBICO

RadiantOne Configuration
Yubico Yubikey

- For Yubikey One Time Password (OTP), we include the script to call Yubicloud service
  - All that needs to be done is:
    1. Create a custom data source that points to Yubicloud URL, the classname we include in our install, the client ID and secret key associated with your Yubicloud service.



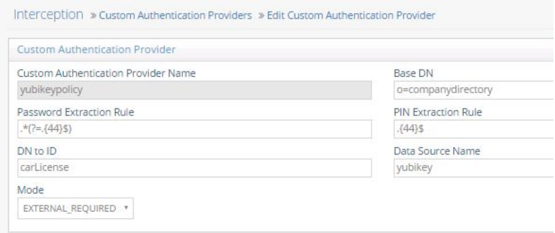
Edit Custom Data Source

Data Source Name: yubikey

Custom Properties

Name	Value
password	{AES}oorL2Hq2e+w+sJK7WU5o4IVPUThxvjC1582xi/uosT8=-oadERRQmUTubnJc829IaJA==
data source	XML
classname	com.rli.scripts.customobjects.yubikey
active	true
url	http://api.yubico.com/wsapi/verify
errorcode	0
username	27084
status	OK

    2. Configure a Custom Authentication Provider indicating the location in VDS where you want to invoke this logic, the password and pin extraction rule (from what came in the bind to VDS), the DN to ID attribute to retrieve the user's identifier, and the custom data source name created above.



Interception » Custom Authentication Providers » Edit Custom Authentication Provider

Custom Authentication Provider

Custom Authentication Provider Name: yubikeypolicy

Base DN: o=companydirectory

Password Extraction Rule: .*(?=.{44}$)

PIN Extraction Rule: .{44}$

DN to ID: carLicense

Data Source Name: yubikey

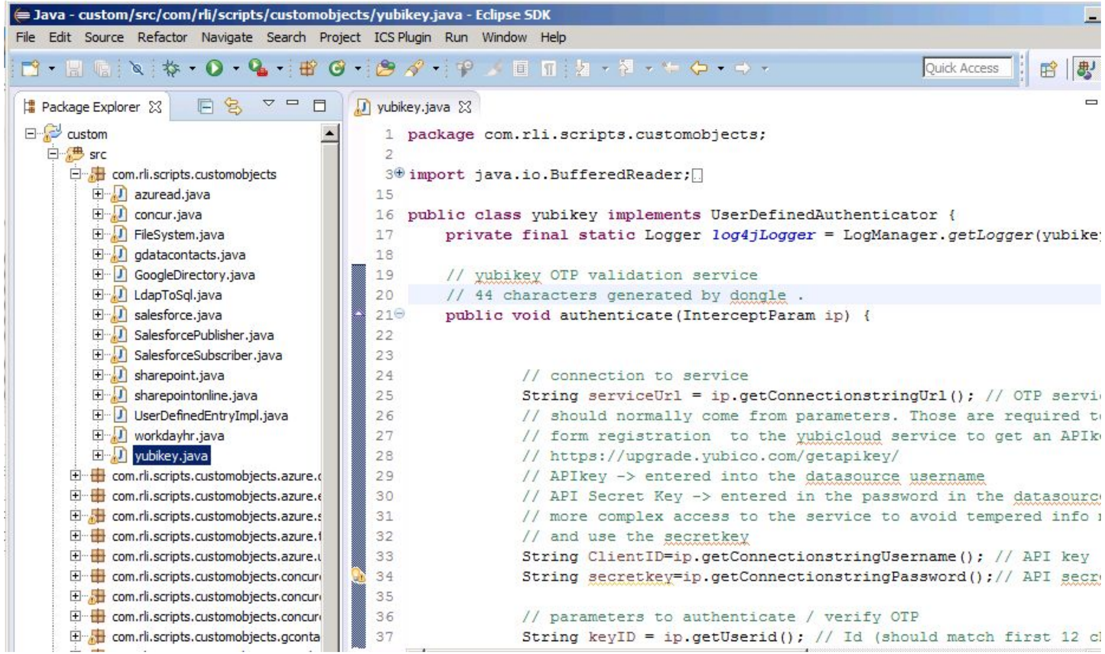
Mode: EXTERNAL_REQUIRED ▾

Note – The default Yubikey is 44 characters. The first 12 are the user's identity.

3. **RESTART VDS (every time you make changes to the custom authentication provider). If in a cluster, restart VDS on all nodes.**

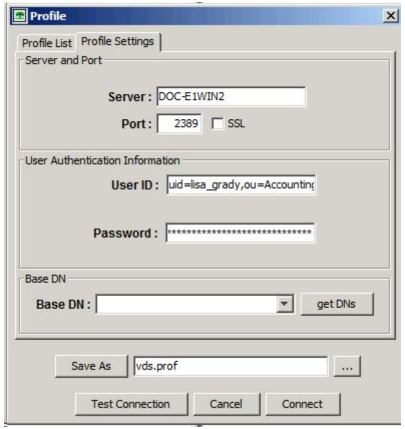
Yubikey Service Script

- Launch Eclipse for VDS and navigate to:
  custom -> src -> com -> rli -> scripts -> customobjects -> yubikey.java


Java - custom/src/com/rli/scripts/customobjects/yubikey.java - Eclipse SDK
File Edit Source Refactor Navigate Search Project ICS Plugin Run Window Help
Quick Access
Package Explorer
custom
src
com.rli.scripts.customobjects
azuread.java
concur.java
FileSystem.java
gdatacontacts.java
GoogleDirectory.java
LdapToSql.java
salesforce.java
SalesforcePublisher.java
SalesforceSubscriber.java
sharepoint.java
sharepointonline.java
UserDefinedEntryImpl.java
workdayhr.java
yubikey.java
com.rli.scripts.customobjects.azure.c
com.rli.scripts.customobjects.azure.e
com.rli.scripts.customobjects.azure.s
com.rli.scripts.customobjects.azure.f
com.rli.scripts.customobjects.azure.u
com.rli.scripts.customobjects.concur
com.rli.scripts.customobjects.concur
com.rli.scripts.customobjects.concur
com.rli.scripts.customobjects.gconta
yubikey.java

```java
package com.rli.scripts.customobjects;

import java.io.BufferedReader;

public class yubikey implements UserDefinedAuthenticator {
    private final static Logger log4jLogger = LogManager.getLogger(yubike

    // yubikey OTP validation service
    // 44 characters generated by dongle .
    public void authenticate(InterceptParam ip) {


            // connection to service
            String serviceUrl = ip.getConnectionstringUrl(); // OTP servi
            // should normally come from parameters. Those are required t
            // form registration  to the yubicloud service to get an APIk
            // https://upgrade.yubico.com/getapikey/
            // APIkey -> entered into the datasource username
            // API Secret Key -> entered in the password in the datasourc
            // more complex access to the service to avoid tempered info 
            // and use the secretkey
            String ClientID=ip.getConnectionstringUsername(); // API key
            String secretkey=ip.getConnectionstringPassword();// API secr

            // parameters to authenticate / verify OTP
            String keyID = ip.getUserid(); // Id (should match first 12 c
```

Example – LDAP Bind Request



Server : DOC-E1WIN2

Port : 2389 ☐ SSL

User ID : uid=lisa_grady,ou=Accountinc

Password : ******************************

Base DN :

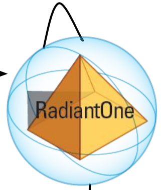
vds.prof

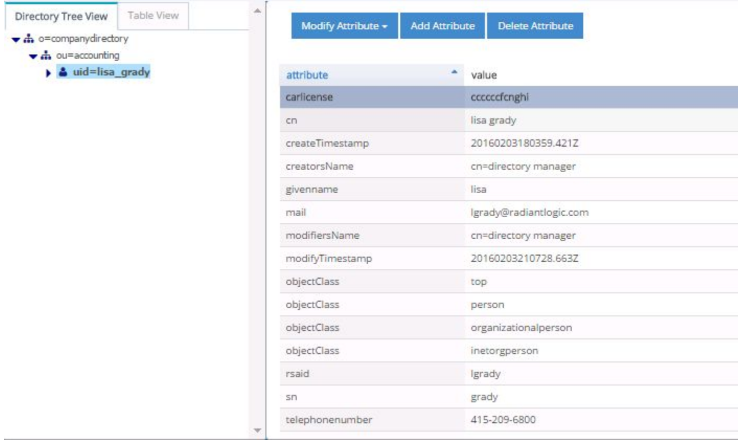
LDAP Client

1. **LDAP Bind:**
   uid=lisa_grady,ou=Accounting,o=companydirectory
   password = secret<YUBIKEY ONE TIME PWD>

Yubikey One Time Password Generator

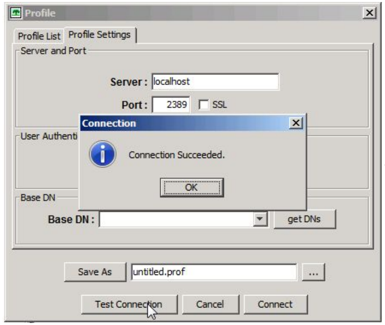
2. RadiantOne performs lookup (based on DN to ID setting) to retrieve the user identifier for external authentication service





attribute	value
carlicense	cccccfcnghi
cn	lisa grady
createTimestamp	20160203180359.421Z
creatorsName	cn=directory manager
givenname	lisa
mail	lgrady@radiantlogic.com
modifiersName	cn=directory manager
modifyTimestamp	20160203210728.663Z
objectClass	top
objectClass	person
objectClass	organizationalperson
objectClass	inetorgperson
rsaid	lgrady
sn	grady
telephonenumber	415-209-6800

Example – Call to External Authentication Service



Server : localhost

Port : 2389 □ SSL

Connection

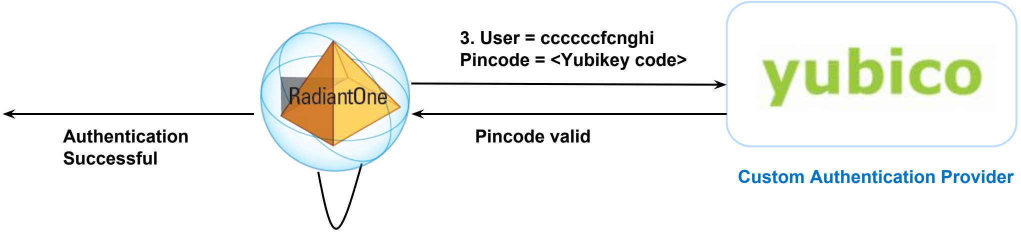
Connection Succeeded.

OK

Base DN :

untitled.prof

LDAP Client



3. User = ccccccfcnghi
Pincode = <Yubikey code>

Pincode valid

Authentication Successful

Custom Authentication Provider

4. RadiantOne validates the user's password :

User= uid=lisa_grady,ou=Accounting,o=companydirectory
password = secret