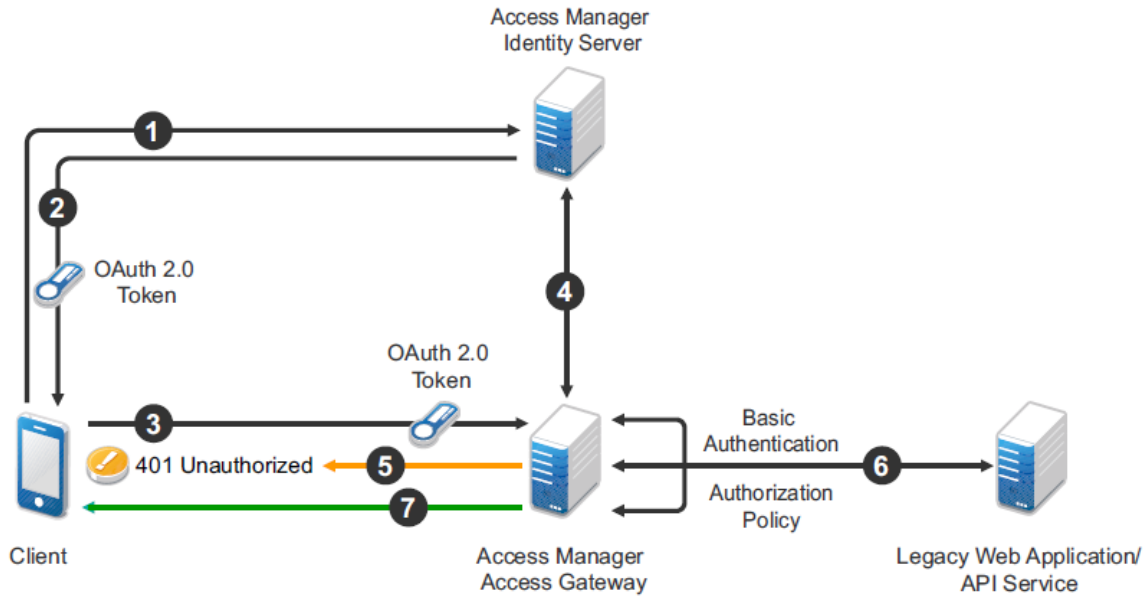




# INJECT OAUTH CLAIMS AND SCOPES TO WEBSERVR



Raja Manjit Singh



To inject OAuth Claims to web server do the below:

1. Create an Authorization Policy as below

Policies ▾

**Edit Policy: Oauth\_authorization**

Type: Access Gateway: Authorization  
 Description:

Rule List				
Rule	Priority	Enabled	Action	Description
<a href="#">1</a>	1	✓	Permit	
<a href="#">2</a>	10	✓	Deny	

**Edit Rule: Oauth\_authorization - Rule 1**

Type: Access Gateway: Authorization  
 Description:   
 Priority:

Conditions

Condition Group 1

If

Comparison: String : Equals  
 Mode: Case Sensitive  
 Value: OAuth Scopes email

Result on Condition Error: False

Actions

Do

Policies ▶ Edit Policy ▶

**Edit Rule: Oauth\_authorization - Rule 2**

Type: Access Gateway: Authorization

Description:

Priority: 10 ▼

**Conditions**

Condition Group 1

New ▼

No conditions in Rule 2. (Actions will always occur unconditionally.)

**Actions**

Do Deny ▼ Display Default Deny Page ▼

Changes made on this panel must be applied from the [Policies](#) Panel.

OK Cancel

The above authorization policy will allow the user only if Access Token contains the specified scope.

2. Create Identity Injection Policy as below:

Type: Access Gateway: Identity Injection

Description:

Priority: 1 ▼

**Actions**

New ▼

Do Inject into Authentication Header

User Name: Selected OAuth Claims ▼ : Access Token: User ▼

Password: Selected OAuth Claims ▼ : Password ▼

Multi-Value Separator: , ▼

DN Format: LDAP (ex, cn=jsmith,ou=Sales,o=Novell) ▼

And Inject into Custom Header

Custom Header Name:

Value: Selected OAuth Claims ▼ : email ▼

Multi-Value Separator: , ▼

DN Format: LDAP (ex, cn=jsmith,ou=Sales,o=Novell) ▼

It will fetch the Username and password from the Access Token and send to web server as Authorization Header.



```
7qcRK9C0PA2OvarXApwJkSrmpoHUKLcLXQFLYRzNiOqgDO02j7M_kKozwWow6FrFrEiLk8pbd7zBEIDD2t0OusDv6
VJOaV9vTFGkR6OykdtJTLz4bj9Ka5kDgQKHZfGkjkLTQS5tHcM75xc59Tk-
5SvEanfXVcwtNB3j89TmLw_zW7ytVUV__1CBNquouWdZREDOjzyRZYbIF1chheiGDmbb-
WhWbesoKtfk38gfGAT9WFeorWi26oA-Rsf1Sv7MAXbEmZiUAzQWLMq6jLQC63MfcUJ-
gEd4E8xvwsLRMZZzod940ri8tc3JE4XASqD3Njfr9Iozaa1L1GzGYIWCg-
qcHJiV5E7kgTp8dNcJj_HB7sm6_gqCdU8q0v1pGo1f-
0FX98mBtU_tYkOagYDYlZApctGOnFZ8fOg9exylUxdMyxdqgwzGvTtO82Odo0uMQp65bZoxVuq8CYSXw-
mumSIOBVxH7jUmRLE7eX6mkfRAWr-NbGaQEwiCtqhie3TTdM6gA-
uFJprJog9yv8RCK4LdCk3cM2KtJyqsFVubexoQ5h4zElnRvhMLh68mMGFPgFTUovUr84F_ce5bzy3PIHtPf-
HVSIE2uqPbYSJ4P5zk9IB9mTwrFwybFaY3aZ97_pHpEJVzX83RBckzPmo-
q5mqHggC75bKNLnN_ngUSx2PioY84IRcLraOaPZnxuzbl3d5QBLI7dT5wdr9TktKFubaeOJm7b1y9W0G4xwVDI4Ev
WD8AmltWdDAhISJDI4yO54k-Ba8tN4AM-BJcrrEsNnG3ihir1SjmuKuBT-
dGxnLhhJpEGQBOmYZd2_Age6DYPXVFpOzTtK_KfGL55Y6sqwWQ7CTe7vAgmSsy-
YsYEj0w3_ex9VHHiwtM2XWtDHj3qX78vxO8HvjvJRALmByplCOUGhCaErQdzn5eaOz2m_YR9WmvRH7XxWj4uMV
a1OUOib-dcBOF5aBqsLMeyL8aYZecvScxvKgkUk_s2i7DHCyfsCPC1vVrGFLO6G-
WuePS9A1Z4e1fpsCE2tBrIFlMFTqZB2reoephUVV9n19D6IEhZujSY-
MjHaFeEGGL8KAPgFS_coih9RACtyi04ezadgw1Aclo5JYU7pLIXzZeJ0cCvBz93DQs4_cXqoWCJJ2hFEhAxAZ5ILAXmn
nrSR2Eze0.oRmzuPaT5I6Xdkcibq-OUG"
```

```
"scope": "email"
}
```

## 5. Access the Protected Resource using above Access Token

Below html file can be used to inject token. (seeing some CORS issue, need to fix it )

```
<!DOCTYPE html>
<html>
<head>
<link rel="stylesheet" href="oauth.css">
</head>
<body>
<div class="form-style-6">
<h2>TokenInfo / UsernInfo</h2>
Access Token:<input type="text" id="access_token" name="access_token" placeholder="Enter the Access Token"
/><br>
<button type="button" onclick="loadDoc()">send token to AG </button>
<p id="demo"></p>
<script>
function loadDoc() {
var xhttp = new XMLHttpRequest();
xhttp.onreadystatechange = function() {
if (this.readyState == 4 && this.status == 200) {
document.getElementById("demo").innerHTML = this.responseText;
}
};
var token = 'Bearer ' + document.getElementById("access_token").value;
xhttp.open("GET", "https://msingh7.lab.novell.com/oauth.php", true);
xhttp.setRequestHeader('Authorization', token);
xhttp.send();
```



```
ExternalElementRef="PolicyID_xpemlPEP_AGIdentityInjection_1553668165322"  
UserInterfaceID="PolicyID_xpemlPEP_AGIdentityInjection_1553668165322"/>
```

```
</PolicyEnforcementList>
```

```
</Configure-ag>
```

```
</NXPES>
```

```
</SOAP-ENV:Body>
```

```
</SOAP-ENV:Envelope>
```

```
</amLogEntry>
```

ESP contacts the Admin Console to fetch policy information and cache it.

```
<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
```

```
Method: JNDILogEventListener.accept
```

```
Thread: ajp-nio-127.0.0.1-9009-exec-6
```

```
Connection: 4a3c15d3-5f92-4815-9e8f-f901c16e457c, Environment Parameters for InitialDirContext() method call:
```

```
Key: java.naming.factory.initial, Value: com.sun.jndi.ldap.LdapCtxFactory
```

```
Key: java.naming.security.principal, Value:
```

```
ou=nidsUser,ou=UsersContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_Root,ou=accessManagerContainer,o=novell
```

```
Key: com.sun.jndi.ldap.connect.timeout, Value: 10000
```

```
Key: com.sun.jndi.ldap.read.timeout, Value: 15000
```

```
Key: java.naming.provider.url, Value: ldaps://151.155.221.49:636
```

```
Key: java.naming.security.protocol, Value: ssl
```

```
Key: java.naming.ldap.factory.socket, Value: com.novell.nidp.common.util.net.client.NIDP_SSLSocketFactory
```

```
Key: java.naming.security.authentication, Value: simple
```

```
Key: java.naming.security.credentials, Value: *****
```

```
</amLogEntry>
```

```
<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
```

```
Method: JNDILogEventListener.accept
```

```
Thread: ajp-nio-127.0.0.1-9009-exec-6
```

```
Added property to DirContext Environment: Property Name: java.naming.ldap.attributes.binary, Value: GUID  
nDSPKITrustedRootCertificate </amLogEntry>
```

```
<amLogEntry> 2019-05-10T22:15:34Z VERBOSE NIDS Application: AM#501101030: AMDEVICEID#esp-
```

```
1ACD8C7C3D6413F8: Reading document at reference: ExternalDocRef -
```

```
ou=xpemlPEP,ou=mastercdn,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc
```

: romaName - xpemlPEP </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:

Method: JNDILogEventListener.accept

Thread: ajp-nio-127.0.0.1-9009-exec-6

Target object dn:

ou=AccessGateway,ou=3rqjtmelgk8305,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN\_Root,ou=accessManagerContainer,o=novell

Acting as:

ou=nidsUser,ou=UsersContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN\_Root,ou=accessManagerContainer,o=novell

Attr: romaContentCollectionXMLDoc

Attr: romaName

</amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:

Method: JNDILogEventListener.accept

Thread: ajp-nio-127.0.0.1-9009-exec-6

getNextConnection() attempting to get preferred replica from the IPreferredReplica interface </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z VERBOSE NIDS Application: AM#501101030: AMDEVICEID#esp-

1ACD8C7C3D6413F8: Reading document at reference: ExternalDocRef -

ou=AccessGateway,ou=3rqjtmelgk8305,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN\_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc

: romaName - AccessGateway-default </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z INFO NIDS Application: AM#501101030: AMDEVICEID#esp-

1ACD8C7C3D6413F8: Policy Configuration: PolicyEnforcementList - <PolicyEnforcementList

IncludedPolicyCategories="" LastModified="1553668498427" LastModifiedBy="cn=admin,o=novell"

RuleCombiningAlgorithm="DenyOverridesWithPriority" schemaVersion="2.0">

<PolicyRef ElementRefType="ExternalWithIDRef"

ExternalDocRef="ou=xpemlPEP,ou=mastercdn,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN\_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc"

ExternalElementRef="PolicyID\_xpemlPEP\_AGAAuthorization\_1553667840814"

UserInterfaceID="PolicyID\_xpemlPEP\_AGAAuthorization\_1553667840814"/>

<PolicyRef ElementRefType="ExternalWithIDRef"

ExternalDocRef="ou=xpemlPEP,ou=mastercdn,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN\_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc"

ExternalElementRef="PolicyID\_xpemlPEP\_AGIdentityInjection\_1553668165322"

UserInterfaceID="PolicyID\_xpemlPEP\_AGIdentityInjection\_1553668165322"/>

</PolicyEnforcementList>

</amLogEntry>



```
<amLogEntry> 2019-05-10T22:15:34Z INFO NIDS Application: AM#501101021: AMDEVICEID#esp-1ACD8C7C3D6413F8: PolicyID#1MK94LP4-71L9-P902-M9K0-M62PN7NO58K5: Response sent: Status - success
</amLogEntry>
```

## ESP sends response to AG

```
<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
Method: BaseHandler.sendSOAPResponse
Thread: ajp-nio-127.0.0.1-9009-exec-6
SOAP EndpointResponse:
  <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
      <NX PES Id="" Status="success">
        <ConfigureResponse PolicyId="1MK94LP4-71L9-P902-M9K0-M62PN7NO58K5">
          <ContextDataElement Enum="6666" ParameterValue="{ 'resourceServer': 'Identity
Provider', 'scope': 'email', 'claim': 'email' }"/>
          <ContextDataElement Enum="6666" ParameterValue="{ 'scope': '_Credential', 'claim':
'_password' }"/>
          <ContextDataElement Enum="6666" ParameterValue="{ 'scope': '_Credential', 'claim':
'_user' }"/>
          <ContextDataElement Enum="2551"/>
        </ConfigureResponse>
      </NX PES>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
</amLogEntry>
```

## AG sends policy configuration request for Authorization Policy:

```
<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
Method: BaseHandler.getSOAPDocument
Thread: ajp-nio-127.0.0.1-9009-exec-6
SOAP EndpointRequest
  <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
```

```

    <NX PES Id="">
      <Configure-ag LastUpdateTimestamp="3813500153" PEPName="AGAuthorization">
        <PolicyEnforcementList IncludedPolicyCategories="" LastModified="1553668498427"
LastModifiedBy="cn=admin,o=novell" RuleCombiningAlgorithm="DenyOverridesWithPriority" schemaVersion="2.0">
          <PolicyRef ElementRefType="ExternalWithIDRef"
ExternalDocRef="ou=xpemplPEP,ou=mastercdn,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou
=VCDN_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc"
ExternalElementRef="PolicyID_xpemplPEP_AGAuthorization_1553667840814"
UserInterfaceID="PolicyID_xpemplPEP_AGAuthorization_1553667840814"/>
          <PolicyRef ElementRefType="ExternalWithIDRef"
ExternalDocRef="ou=xpemplPEP,ou=mastercdn,ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou
=VCDN_Root,ou=accessManagerContainer,o=novell:romaContentCollectionXMLDoc"
ExternalElementRef="PolicyID_xpemplPEP_AGIdentityInjection_1553668165322"
UserInterfaceID="PolicyID_xpemplPEP_AGIdentityInjection_1553668165322"/>
        </PolicyEnforcementList>
      </Configure-ag>
    </NX PES>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
</amLogEntry>

```

## ESP sends response to AG

```

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
Method: BaseHandler.sendSOAPResponse
Thread: ajp-nio-127.0.0.1-9009-exec-6
SOAP EndpointResponse:
  <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
      <NX PES Id="" Status="success">
        <ConfigureResponse PolicyId="71L06K90-30N0-8ML5-PNP1-N64N84O5LLP7">
          <ContextDataElement Enum="6663"/>
        </ConfigureResponse>
      </NX PES>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
</amLogEntry>

```



SLqzI5Or4H0VPwerp8\_iyzz\_f2YhRlqxjlec0neLFwyUUT6jtk\_IF8I3qmlGkRDs4MXsoeJKNWkK0XmhMrglfgEsIzqC9--  
yY3ml8jMLWZLLRZdsP4oxa0yoF6HBNutKBZ-xigiqM1Y3E-ry-  
U3p9G6YAKDNA591H6Pc4QRuqaKipECFjZCmekQnOX9JOUkSEXLFJUhrnwp93MWMh\_r\_9evUtYsAF\_-  
iCGt2GTfMoVgn2Fu5S5cVivlOOzmi4oDzHZZIWhoUvGS3rOYCExDRFvEM82oWfBxBsME-Z3WNIPL-  
FcG2REbRwcUFkvRbgda6rt33qKC\_P8gg

11 > connection: keep-alive

11 > host: msingh5.lab.novell.com:8443

11 > user-agent: Java/1.8.0\_192

</amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Session Logger:  
com.novell.nam.nidp.oauth.core.grants.OAuth2ClientGrant: Token found in user's issued token list. </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Session Logger:  
com.novell.nam.nidp.oauth.nidp.servlets.NIDPLoginService: The token is valid. </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z INFO NIDS Session Logger:  
com.novell.nam.nidp.oauth.core.helpers.OAuth2TokenInfoResponse: Token info response success </amLogEntry>

<amLogEntry> 2019-05-10T22:15:34Z INFO NIDS Session Logger:  
com.novell.nam.nidp.oauth.nidp.servlets.OAuthApplication: 12 \* Server responded with a response on thread https-  
jsse-nio-151.155.221.50-8443-exec-2

12 < 200

12 < Content-Type: application/json

</amLogEntry>

## ESP sends NRLLoginResponse to AG

<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:

Method: BaseHandler.sendSOAPResponse

Thread: ajp-nio-127.0.0.1-9009-exec-8

SOAP EndpointResponse:

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">

<SOAP-ENV:Body>

<NRLLoginResponse correlationId="">

<Status code="success" processingState="complete"/>

<Authentication hardExpire="3252" softExpire="3252">

<Store>

<dn>

**admin**

```
</dn>
</Store>
</Authentication>
</NRLoginResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
</amLogEntry>
```

## 8. AG sends Policy Evaluation Request to ESP for Authorization Policy and II Policy with Access Token value.

ESP sends a userinfo request to IDP server and cache the user info.

```
<amLogEntry> 2019-05-10T22:15:35Z INFO NIDS Session Logger:
com.novell.nam.nidp.oauth.nidp.servlets.OAuthApplication: 13 * Server has received a request on thread https-jse-
nio-151.155.221.50-8443-exec-1
```

```
13 > GET https://msingh5.lab.novell.com:8443/nidp/oauth/nam/userinfo?sp-
id=https://msingh7.lab.novell.com:443/nesp/idff/metadata
```

```
13 > accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
```

```
13 > authorization: bearer
```

```
eyJraWQiOiJ0TU5MzQ3NzY5ODAxMTg1ODM0NDUyMDQ3MzE0NTc3MTUxMzQ4Mzk1NzE5NDYiLCJ0eXAiOiJK
V1QiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwczovL21zaW5naDUubGFmLm5vdmVsbC5jb206ODQ0My9uaWRwL29h
dXRoL25hbSIsImp0aSI6IjlmZWQyMTM5MDQ0NTM3NC1hM2RkLWVjMDljZjA1ODg4Mm5mImF1ZCI6IjE1NzBmZTFkL
TUyZjgtNDBkOC1hZDFILTk4OTY2NWRkNThiNCIsImV4cCI6IjE1NzUyOTc0NywiYWV0IjoxNTU3NTI2MTg3LzJmYmYiO
jE1NTc1MjYxNTesInN1YiI6IjVhMGZmNW5NzAxYmY4NDhhMjQ3NWVhZmY1Yzk3MDFiIiwiaXNzIjE1NzUyOTc0Nywi
SXIldk9IN2NkeiJoVGJTa1BJdWJeenFMTHk4Tlk3dkJRK0poVXVIVHFMzRjUkp3NIRJbjJYV1NwNUhlnVIEa1Fjak1oO
HBiZwXpWkg1MS9IWngyQkFmd3FCMUyxWWQ0a3BLLmFjcy9CMXlvd0hxMThxMC9lK0ZnNmtQZWVndmpvai92Wi9G
VE9NM1R4TkRkQVJYeHRFUGM1Q1pwOHp3c0N2MjYxcllSYyt2MzY0V0VmlRU0hvS3V6VWVxTFJNUXlORzJCV2hEdFJ0
SExEYU50UVNzSXRCeHhDbXdh0hEhE1ZVZW3bVBGVGdab1N0Y1RkK3hHL29lbi9hN0QzZ2tweDdTdU9KaWI3alhV
FiM1pCdXlpY1U2ZHZVRnJQS0pzd0ZjOENOTy9PMWtuVjRlK1hLWmxQL0l3Ym5mOHZYUWhPzZl0aE10Y0pLM1hnbW
NFWDFLNUV3OHhKY2k5bUR6UkNiekNXQ3l0Vm1LSXZidndOeks1elVCUII3Rm1HNUxjRDY1amJGaTVaMFRmekdpTF
R5Nk52UWE0Ym95V3ltMXNsSINjZTB1WFhHdmFWam5yRW1qZ2pmQXFibFBkRVNXTUI0TnBqRkdQOVQ0Nm1DT1Jp
MDhhQnlqdJWZFPsanhIMmdwQ0xqYUdvdNddRbmZETDBPaThmYk1MzcwYkMxRUtBWXNEQWZCNCt2ell6ajdYdW9z
UDUzUXZTRWovZ3MyVFBPd3BoYS9GdjRtdDFHK21UcUFzeVhFb2djcjZVY3ZzSUJINHIQWepYaHlZbkRtYmRvYm5vRW
dZL015VfNWHJUYXhxTHZqZW4yM2IHNOFuUkZjU0JGYzEzNlpaVgvd1VUZWhBMmZHSjFwbHh5bnBBams0c2ttbkJ
KeXBMaEJuOVgwPS4yIiwic2NvcGU0IjE1NzUyOTc0NywiYWV0IjoxNTU3NTI2MTg3LzJmYmYiOjE1NTc1MjYxNT
SLzI5Or4H0VPwper8_izyx_f2YhRlqxjlec0neLFwyUUT6jtk_IF8I3qmlGkRDs4MXsoeJKNWkK0XmhMrglfgEsIzqC9-
yY3ml8jMLWZLLRzdsP4oxa0yoF6HBNutKBZ-xigiqM1Y3E-ry-
U3p9G6YAKDNA591H6Pc4QRuqaKipECFjZCmekQnOX9JOUkSEXLFJUhrnwpx93MWMh_r_9evUtYsAF_-
iCGt2GTfMoVgn2Fu5S5cVivlOOzmi4oDzHZZIWhoUvGS3rOYCEvDRFvEM82oWfBXBsME-Z3WNIPL-
FcG2REbRwcUFkvRbgda6rt33qKC_P8gg
```

```
13 > connection: keep-alive
```

```
13 > host: msingh5.lab.novell.com:8443
```

```
13 > user-agent: Java/1.8.0_192
```

```
</amLogEntry>
```

```
<amLogEntry> 2019-05-10T22:15:35Z INFO NIDS Session Logger:
com.novell.nam.nidp.oauth.core.OAuth2ClaimsResponse: OAuth2 Claim response success </amLogEntry>
```

```
<amLogEntry> 2019-05-10T22:15:35Z INFO NIDS Session Logger:  
com.novell.nam.nidp.oauth.nidp.servlets.OAuthApplication: 14 * Server responded with a response on thread https-  
jsse-nio-151.155.221.50-8443-exec-1
```

```
14 < 200
```

```
14 < Content-Type: application/json
```

```
</amLogEntry>
```

ESP sends the Policy Evaluation Response to AG Server.

```
<amLogEntry> 2019-05-10T22:15:34Z DEBUG NIDS Application:
```

```
Method: BaseHandler.sendSOAPResponse
```

```
Thread: ajp-nio-127.0.0.1-9009-exec-8
```

```
SOAP EndpointResponse:
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">  
  <SOAP-ENV:Body>  
    <NX PES Id="" Status="success">  
      <EvaluateResponse>  
        <DoAction ActionName="Permit" ActionTTL="-1" Enum="2610"/>  
      </EvaluateResponse>  
    </NX PES>  
  </SOAP-ENV:Body>  
</SOAP-ENV:Envelope>  
</amLogEntry>
```

```
<amLogEntry> 2019-05-10T22:15:35Z DEBUG NIDS Application:
```

```
Method: BaseHandler.sendSOAPResponse
```

```
Thread: ajp-nio-127.0.0.1-9009-exec-8
```

```
SOAP EndpointResponse:
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">  
  <SOAP-ENV:Body>  
    <NX PES Id="" Status="success">  
      <EvaluateResponse>  
        <DoAction ActionName="InjectAuthHeaderData" ActionTTL="-1" Enum="2710">  
          <Parameter Enum="10" Name="Uid" Value="XX"/>  
          <Parameter Enum="20" Name="Pwd" Value="XX"/>  
        </DoAction>
```

```

<DoAction ActionName="InjectCustomHeader" ActionTTL="-1" Enum="2720">
  <Parameter Enum="10" Name="HeaderName" Value="XX"/>
  <Parameter Enum="20" Name="Text" Value="XX"/>
</DoAction>
</EvaluateResponse>
</NXPES>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
</amLogEntry>

```

9. AG will use the response to take authorization decision and to inject II values to the web server.

The screenshot displays a network traffic analysis tool interface. On the left, a list of network events shows a series of HTTP requests and responses between 'www.googleapis.com' and 'msingh5.lab.novell.com'. The selected request is highlighted in blue. On the right, the 'HTTP Headers Information' panel is open, showing the details of the selected request. The 'Authorization' header is highlighted in yellow and contains the value 'Basic YWRtaW46'. The 'OAUTHCLAIMS' header is also highlighted in yellow and contains the value '151.155.223.132'. Other headers include 'Host', 'Origin', 'User-Agent', 'Referer', 'Accept-Encoding', and 'Accept-Language'.

HTTP Request Headers	
HTTP Request	GET /oauth.php HTTP/1.1
Host	msingh7.lab.novell.com
Authorization	Basic YWRtaW46
Origin	https://151.155.223.132
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
Accept	*/*
Referer	https://151.155.223.132/bootcamp/msingh5/OAUTHAPP/html/AG.html
Accept-Encoding	gzip, br
Accept-Language	en-US,en;q=0.9
OAUTHCLAIMS	151.155.223.132
Via	1.1 msingh7.lab.novell.com (Access Gateway-ag-1ACD8C7C3D6413FB-)
X-Forwarded-For	137.65.220.220
X-Forwarded-Host	msingh7.lab.novell.com
X-Forwarded-Server	msingh7.lab.novell.com
Connection	Keep-Alive