

Using Username and/or Password

- Apache's htpasswd
- Authenticate with RACF
- Enabling Web Service Authorization

Apache's htpasswd

A password file can be created using Apache's htpasswd program. It is very important that this file is not placed in an area which is accessible to the web via the web server. It is recommended that the password file should be named "htpasswd". We recommend that the file is placed in the following locations

Linux	[SOAG_INSTALL_DIR]/apache2/bin/htpasswd
Windows	[SOAG_INSTALL_DIR]\Apache22\bin\htpasswd.exe

See Apache 2.0 documentation for more information about htpasswd.

Authenticate with RACF

There are a number of prerequisites to authenticating with RACF, ACF2 or Top Secret:

1. If you wish the SOA Gateway to check directly with using the SAF interface, the SOA Gateway address space must be APF authorized.
2. If you have ADABAS installed and are using the ADABAS SAF Server, the SOA Gateway can communicate with the SAF Gateway to authorize userids and passwords and to ensure that your ADABAS database is fully protected. In order to do this, you must make the ADABAS WAL Library available in the SOA Gateway STEPLIB on z/OS and relink the current SAFASG module as follows. Please ensure that the newly linked SAFASG is higher in the STEPLIB chain than the WAL library you are using.

```
//LINK EXEC PGM=IEWL,
// PARM='MAP,LET,LIST,XREF,NCAL,REUS,RENT'
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD UNIT=VIO,SPACE=(CYL,(1,1))
//SYSLMOD DD DSN=<target load librart>,DISP=SHR
//ADALIB DD DSN=<root>.ADAvrm.MVSLOAD,DISP=SHR
//WALLIB DD DSN=<root>.WALvrm.MVSLOAD,DISP=SHR
//SYSLIN DD *
INCLUDE WALLIB(SAFASG)
INCLUDE ADALIB(ADALNKR)
ENTRY SAFASG
MODE AMODE(31),RMODE(24)
NAME SAFASG(R)
/*
```

Please refer to the Adabas SAF Security documentation for more information and configuration options.

The SOA Gateway must be configured to run with its security level at the “User” or above. Note that with “User” level, only userids will be checked which can be useful if all requests come from a trusted source but under normal circumstances, you should run with level “Password”.

Once the SOA Gateway is running at Security Level = Password, then all requests must provide a password.

To pass security credentials from the SOA Gateway Control Centre, use the "Set Credentials For Server" option.

If you wish to use HTTP Headers to provide the credentials:

- Edit the HT\$CONF file
- Enter

```
<IfModule mod_xmiddle.c>
  <Location /configurationService>
    AuthType Basic
    AuthName "Username and password required"
    Require valid-user
  </Location>
</IfModule>
```

- Submit the JCL which copies this HT\$CONF to the SOA Gateway file system and restart the server.

If you wish to provide the credentials on the SOAP headers, there is no need to modify HT\$CONF

Enabling Web Service Authorization

Important:

The AuthUserFile is not required on z/OS.

There are 2 methods to pass the credentials to the SOA Gateway server

1. Using the SOAP Headers: Once the WSDL has been imported into your chosen SOAP client, you can add your credentials to the `<soap:Header>` section. No additional changes are required on the server side, and your request is processed using these credentials.
2. Using HTTP Headers: The Apache configuration file must be modified to include a `<Location ... >` directive. Now when a client requests this location, the server will "challenge" for the credentials. Examples for the `<Location ...>` directive are provided below.

Example 1

To request authorization on the configuration web service, perform the following steps, ensuring the `<<filename>>` is filled into the password file appropriate to your system.

- Edit the SOA Gateway Apache configuration file
- Enter the following directives:

```

<IfModule mod_xmiddle.c>
  <Location /configurationService>
    AuthType Basic
    AuthName "Username and password required"
    AuthUserFile <<filename>>
    Require valid-user
  </Location>
</IfModule>

```

- Restart your SOA Gateway Server.
- Open a web browser, and enter the URL `http://<host>:<port>/configurationService?WSDL` where `<host>` and `<port>` are the host and port (if required) where your SOA Gateway server is running.
- You will not be granted access to the WSDL unless you enter the correct credentials.

Example 2

To request authorization on the web service for a resource “adabas_Employees”, perform the following steps, ensuring the `<<filename>>` is filled into the `htpasswd` file appropriate to your system.

- Edit the SOA Gateway Apache configuration file
- Enter the following directives:

```

<IfModule mod_xmiddle.c>
  <Location /adabas_Employees>
    AuthType Basic
    AuthName "Username and password required"
    AuthUserFile <<filename>>
    Require valid-user
  </Location>
</IfModule>

```

- Restart your SOA Gateway Server.
- Open a web browser, and enter the URL `http://<host>:<port>/adabas_Employees?WSDL` where `<host>` and `<port>` are the host and port (if required) where your SOA Gateway server is running.
- You will not be granted access to the WSDL unless you enter the correct credentials.

Example 3

The following example will demonstrate how to access the `adabas_Employees` web service from PHP. This resource should be set up to only allow access when the client has the correct user name and password. You should change this program to use the host and port that your SOA Gateway server is running on.

Important:

This program assumes that `personnel_id` field of the “adabas_Employees” resource has been set up to be the one and only primary key.

```

<?php

ini_set( "soap.wsdl_cache_enabled", 0);

$soapClient = new SoapClient(

```

```

        "http://localhost:8080/adabas_QE_Employees?WSDL",
        array( 'login'="asg", 'password'=>"boston1" ) );

$adabasEmployeeGetKey = array( 'personnel_id'=>50005000 );

try{
    $results = $soapClient->get( $adabasEmployeeGetKey );
}
catch( Exception $e){

    print "An exception occurred!\n";
    print "Code : ";
    print_r( $e->faultcode);

    print "\nString : ";
    print_r( $e->faultstring);

    print "\n ";

    exit;
}
?>

```

If the PHP request works, then the results of the get operation will be printed using PHP print_r function.

Or in the case of an error:

```
X-Powered-By: PHP/5.1.2 Content-type: text/html
```

```
An exception occurred!
```

```
Code : HTTP
```

```
String : Unauthorized Request
```

The Apache error_log should have more information about why this request was rejected

Example 4

It is also possible to add a username and password to a SOAP Request.

On z/OS, the username and password will be authenticated against RACF. This allows request to be not only authenticated, but also authorized to run with the required credentials.

Important:

It is recommended that the SOA Gateway's security level should be set to "Password".

Important:

On z/OS, the SOA Gateway dataset must be authorized.

Consider the following SOAP Request:

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:xmid="http://www.risaris.com/namespaces/xmiddle"
                  xmlns:sec="http://schemas.xmlsoap.org/ws/2002/04/secext">
  <soapenv:Header>
    <sec:Security>
      <UsernameToken>

```

```
        <Username>ASG</Username>
        <Password>BOSTON1</Password>
    </UsernameToken>
</sec:Security>
</soapenv:Header>
<soapenv:Body>
    <xmid:adabasEmployeeListElement>
        <personnel_id>400001*</personnel_id>
    </xmid:adabasEmployeeListElement>
</soapenv:Body>
</soapenv:Envelope>
```

If this SOAP request is sent to z/OS, the SOA Gateway will attempt to authenticate this user with RACF, providing the username “ASG” and the password “BOSTON1”.