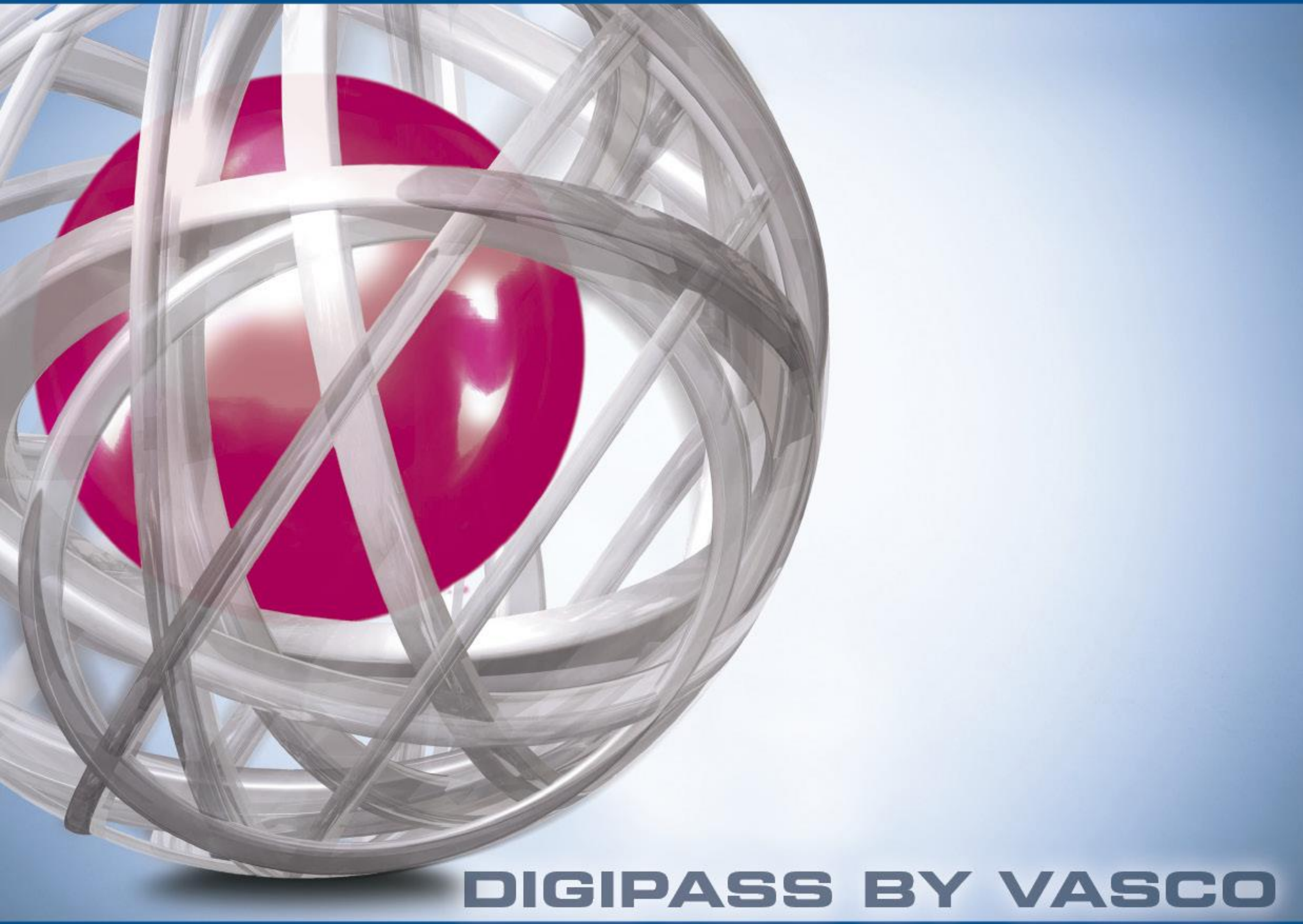
INTEGRATION GUIDE

DIGIPASS Authentication for Office 365 using IDENTIKEY Federation Server



VASCO

THE AUTHENTICATION COMPANY

The world's leading software company specializing in **Internet Security**

Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

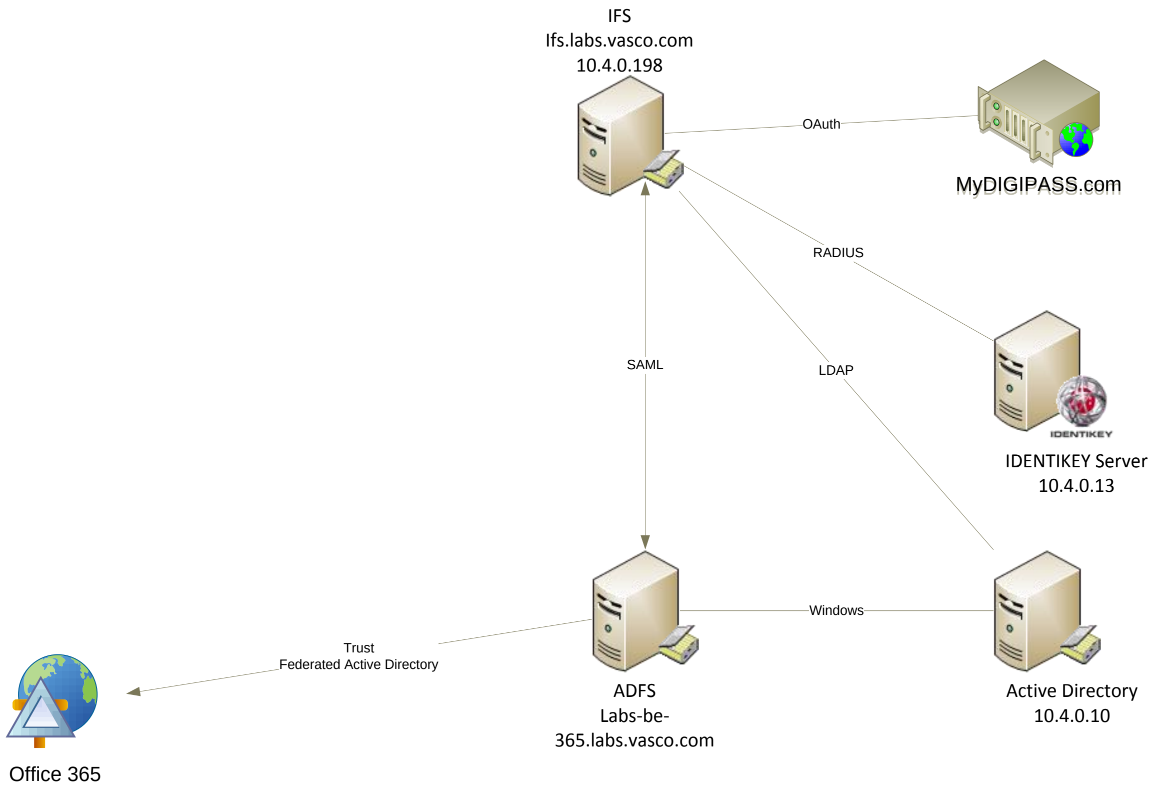
Copyright

Table of Contents

1 Overview

This setup was created in our LABS environment and can be tested on http://labs.vasco.com.

1.1 Architecture



1.2 Two factor authentication

Many organizations still rely on a username and password to protect their data or external access. However passwords are often very simple and very easy guessed, cracked or even stolen. Once it is compromised it can take quite a lot of time before anyone notices that it has been compromised. Recently a lot of services are being moved to the “cloud” where anyone can access the service from anywhere. This means that the users are often accessing it from outside the safe network, making protecting your password even more important and harder.

Two factor authentication of VASCO Data Security will add an additional factor, called DIGIPASS, to your password. The DIGIPASS will generate a One Time Password, or OTP, which you can use in combination with your password. This means that people will need a specific device and password if they want to gain access. Imagine if the device were to be stolen, this will be noticed quickly and that way access using that device can be denied, stopping any attacker quickly.

With this in mind you can secure your Office 365 accounts, granting you the freedom of Office 365 with the hardened security of two factor authentication.

2 Components

2.1 Microsoft

2.1.1 Office 365

Office 365 is Microsoft Office collaboration and productivity tools that are delivered to you through the Internet. This enables your work force to access and store documents, access email and even web conference from nearly any device that has an Internet connection.

2.1.2 Active Directory Federation Server

Active Directory Federation Services (ADFS) is based on the emerging, industry-supported Web Services Architecture, which is defined in WS-* specifications. ADFS helps you use single sign-on (SSO) to authenticate users to multiple, related Web applications over the life of a single online session. ADFS accomplishes this by securely sharing digital identity and entitlement rights across security and enterprise boundaries.

2.2 VASCO

2.2.1 IDENTIKEY Federation Server

IDENTIKEY Federation Server is a virtual appliance providing you with the most powerful identity & access management platform. It is used to validate user credentials across multiple applications and disparate networks.

The solution validates users and creates an identity ticket enabling web single sign-on for different applications across organizational boundaries. As validated credentials can be reused, once a user's identity is confirmed, access to authorized services and applications is granted. Users can securely switch between the different applications and collaborate with colleagues, business partners, suppliers, customers and partners using one single identity.

IDENTIKEY Federation Server works as an Identity Provider within the local organization, but can also delegate authentication requests (for unknown users) to other Identity Providers. In a Federated Model, IDENTIKEY Federation Server does not only delegate but also receives authentication requests from other Identity Providers, when local users want to access applications from other organizations within the same federated infrastructure.

2.2.2 IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

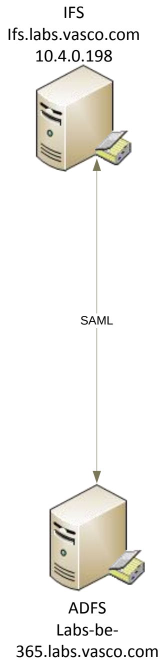
IDENTIKEY Authentication Server is supported on 32bit systems as well as on 64bit systems.

IDENTIKEY Appliance is a standalone authentication appliance that secures remote access to corporate networks and web-based applications.

⚠ The use and configuration of an IDENTIKEY Authentication Server and an IDENTIKEY Appliance is similar.

3 Configuration details

3.1 Architecture



3.2 Pre-requisites

This integration paper is written in the assumption that you already have a working Office 365 – Active Directory Federation Service connection in place. For that connection you will need to have an Active Directory Federation Service Server in place. If you do not yet have such a setup, this guide provided by Messageops.com is a good start for a demo environment (http://www.messageops.com/documentation/office-365-documentation/ad-fs-with-office-365-step-by-step-guide).

Following items are needed:

- Active Directory Federation Service
- Active Directory Federation Service – Office 365 connection
- IDENTIKEY Federation Server with basic setup

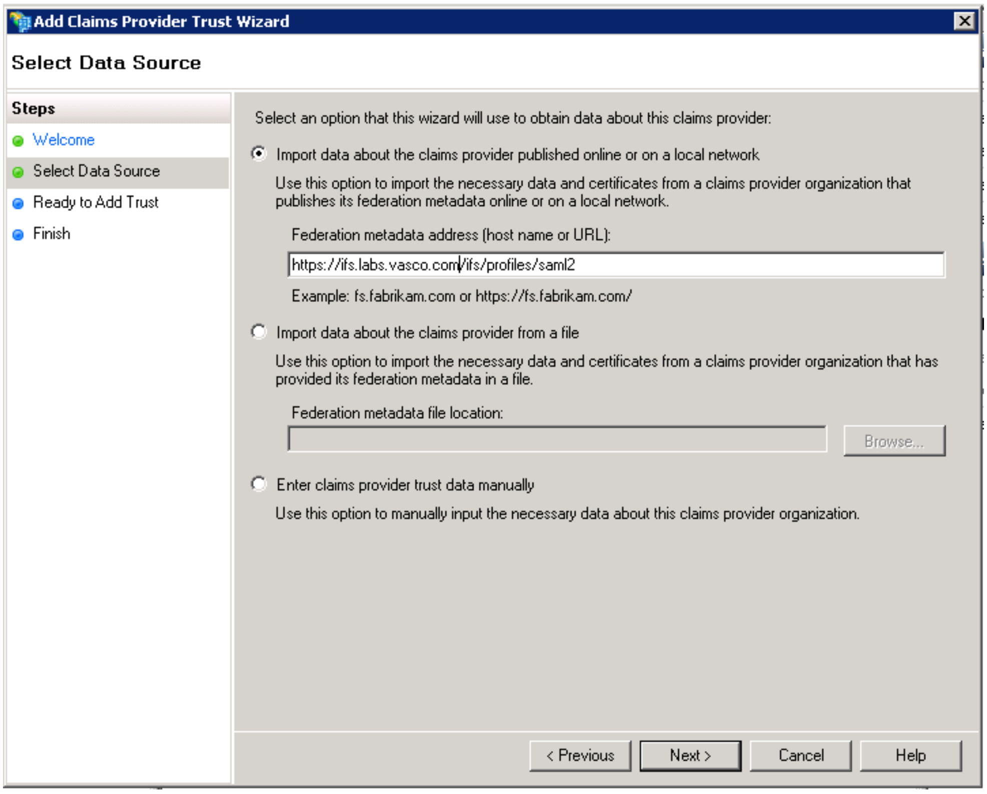
3.3 Active Directory Federation Service steps

3.3.1 Claims provider trust

Open the Active Directory Federation Service console. Once it is loaded expand **Trust Relationships** and select **Claims Provider Trust**. Now click **Add Claims Provider Trust**, this can be found in the menu on the right.

A wizard opens up.

Click **Start**.



Add Claims Provider Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this claims provider:

● Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

https://ifs.labs.vasco.com/ifs/profiles/saml2

Example: fs.fabrikam.com or https://fs.fabrikam.com/

○ Import data about the claims provider from a file

Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.

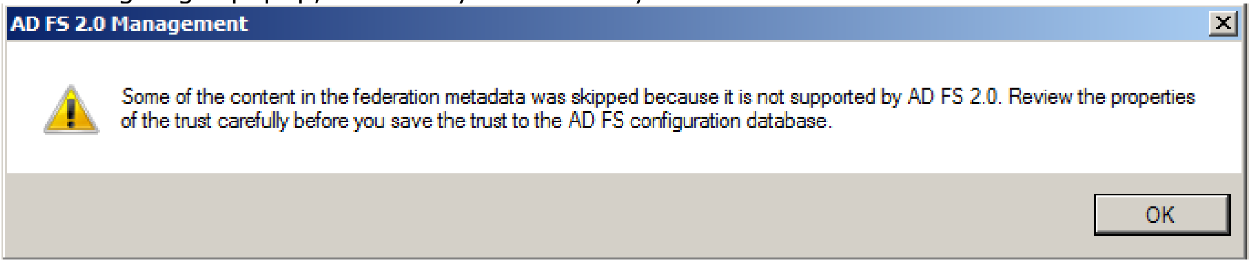
Federation metadata file location:

○ Enter claims provider trust data manually

Use this option to manually input the necessary data about this claims provider organization.

- Select Import Data about the claims provider published online or on local network
- Enter **https://<ifs-host>/ifs/profiles/saml2** (our example: https://ifs.labs.vasco.com/ifs/profiles/saml2)
- Click **Next**

A warning might popup, however you can safely dismiss this.



AD FS 2.0 Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS 2.0. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

Fill in a **Display name** (Example: ifs.labs.vasco.com) and click **Next**.

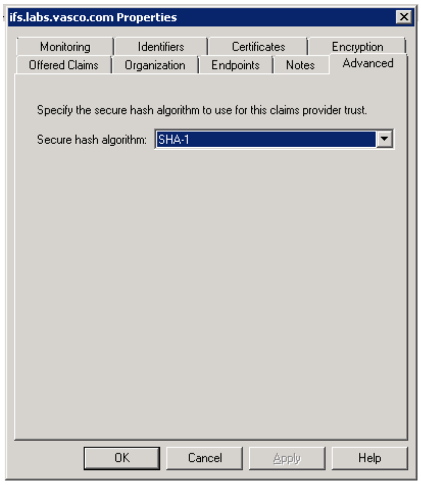
Review and click **Next**.

Click **Close**.

3.3.2 Hashing settings

Expand **Trust Relations** and open **Claims Provider Trusts**. Right-click the newly created Claims Provider (ifs.labs.vasco.com) and select **Properties**.

Go to the **Advanced** tab.



ifs.labs.vasco.com Properties

Specify the secure hash algorithm to use for this claims provider trust.

Secure hash algorithm: SHA-1

Select **SHA-1**.

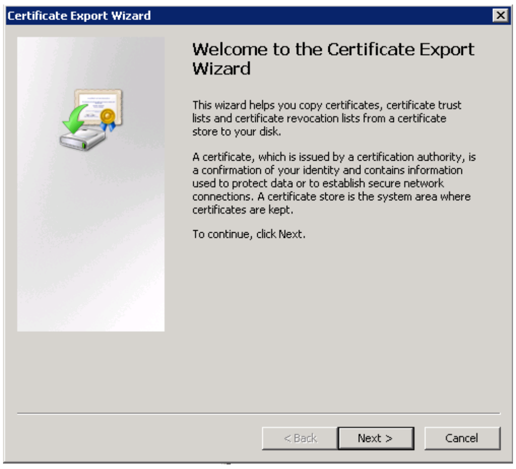
Click **OK**.

3.3.3 Certificate export

Expand **Service** and open **Certificates**.

Right-click the certificate under **Service communications** and select **View Certificate**.

Go to the **Details** tab and click **Copy to File...**



Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

An export wizard opens and click **Next**.

Select **No, do not export the private key** and click **Next**.

Select **Base-64 encoded X.509(.CER)** and click **Next**.

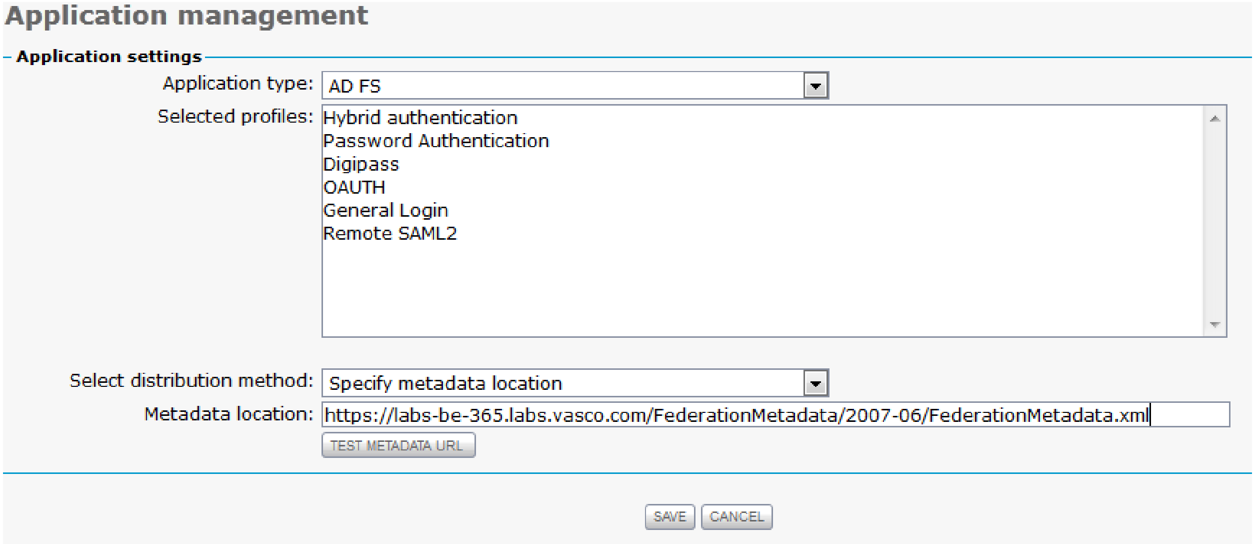
Enter a **<file name>.cer** and click **Next**.

Click **Finish**.

3.4 IDENTIKEY Federation Server

3.4.1 Application configuration

Open a browser and navigate to the IDENTIKEY Federation Server ‘s management console. Then go to **Applications**, **Add Application**.



Application management

Application settings

Application type: AD FS

Selected profiles: Hybrid authentication, Password Authentication, Digipass, OAUTH, General Login, Remote SAML2

Select distribution method: Specify metadata location

Metadata location: https://labs-be-365.labs.vasco.com/FederationMetadata/2007-06/FederationMetadata.xml

- Select **AD FS**
- Select an authentication profile
- Select **Specify metadata location**
- Fill in the location (**https://<adfs-host>/FederationMetadata/2007-06/FederationMetadata.xml** in our example: https://ifs.labs.vasco.com/FederationMetadata/2007-06/FederationMetadata.xml)
- Click **Save**

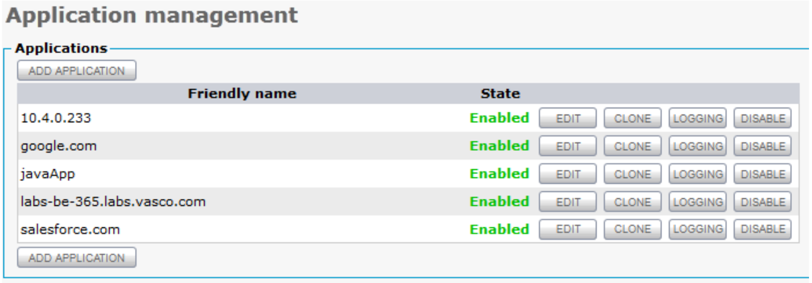
Authentication profiles are linked to authentication methods, for more information please view the IDENTIKEY Federation Server manual for more information.

3.4.2 Certificate import

The certificate should be installed together with the metadata. If this is not the case, follow these steps.

Edit the newly created application.

Click on Applications.

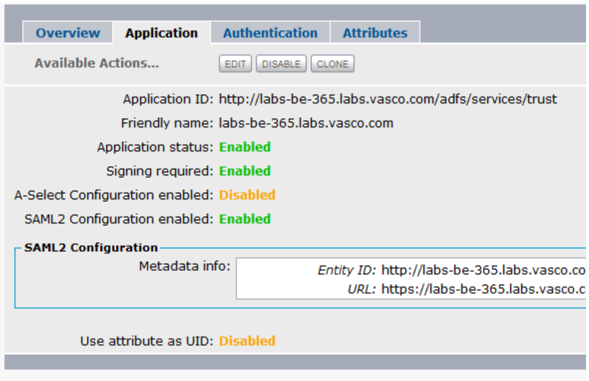


Application management

Applications

Friendly name	State
10.4.0.233	Enabled
google.com	Enabled
javaApp	Enabled
labs-be-365.labs.vasco.com	Enabled
salesforce.com	Enabled

Click **Edit** next to the name of the newly created application (holding the name of your server; here **labs-be-365.labs.vasco.com**).



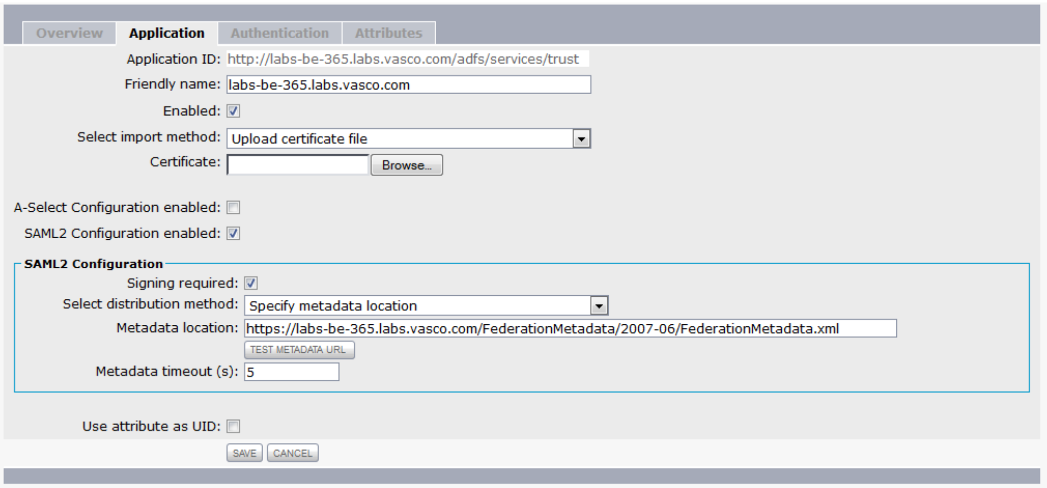
Application ID: http://labs-be-365.labs.vasco.com/adfs/services/trust
Friendly name: labs-be-365.labs.vasco.com
Application status: Enabled
Signing required: Enabled
A-Select Configuration enabled: Disabled
SAML2 Configuration enabled: Enabled

SAML2 Configuration
Metadata info: *Entity ID:* http://labs-be-365.labs.vasco.co
URL: https://labs-be-365.labs.vasco.c

Use attribute as UID: Disabled

Go to the **Application** tab and click **Edit**.

Enable signing and upload the certificate from the Active Directory Federation Server (gained in step 3.3.3 Certificate export).



Application ID: http://labs-be-365.labs.vasco.com/adfs/services/trust
Friendly name: labs-be-365.labs.vasco.com
Enabled: ☑
Select import method: Upload certificate file
Certificate:

A-Select Configuration enabled: □
SAML2 Configuration enabled: ☑

SAML2 Configuration
Signing required: ☑
Select distribution method: Specify metadata location
Metadata location: https://labs-be-365.labs.vasco.com/FederationMetadata/2007-06/FederationMetadata.xml
Metadata timeout (s): 5

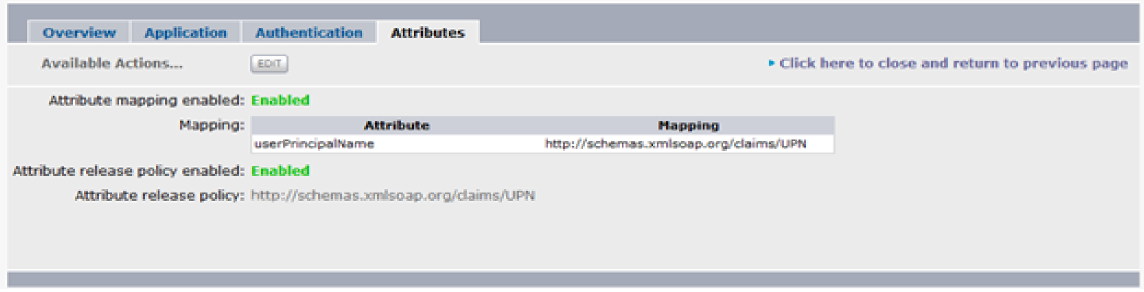
Use attribute as UID: □

- Check **Signing required**
- Select import method **Upload certificate file**
- Click **Browse** and select the IDENTIKEY Federation Server Certificate
- Click **Save**

3.4.3 Application attributes

When the application is created it also creates some attributes and mappings by default. These attributes are later needed by the Active Directory Federation Service server. If these values are not set, the connection between Office 365 and your Active Directory Federation Service server using the IDENTIKEY Federation Server as sign-on medium will fail.

The default values are shown here:



Attribute mapping enabled: Enabled

Mapping:

Attribute	Mapping
userPrincipalName	http://schemas.xmlsoap.org/claims/UPN

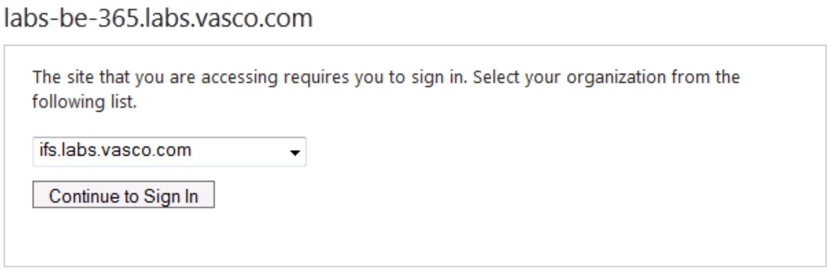
Attribute release policy enabled: Enabled

Attribute release policy: http://schemas.xmlsoap.org/claims/UPN

- Mapping
  - Attribute
    - userPrincipalName
  - Mapping
    - http://schemas.xmlsoap.org/claims/UPN
- Attribute Release Policy
  - http://schemas.xmlsoap.org/claims/UPN

3.5 Connection test

By now you should be able to test the connection using a test application in the Active Directory Federation Service. Open the browser and navigate to https://<adfs-host>/adfs/ls/IdpInitiatedSignon.aspx (in our application: https://ifs.labs.vasco.com/adfs/ls/IdpInitiatedSignon.aspx). On this page you can now select your new Claims Provider.


labs-be-365.labs.vasco.com

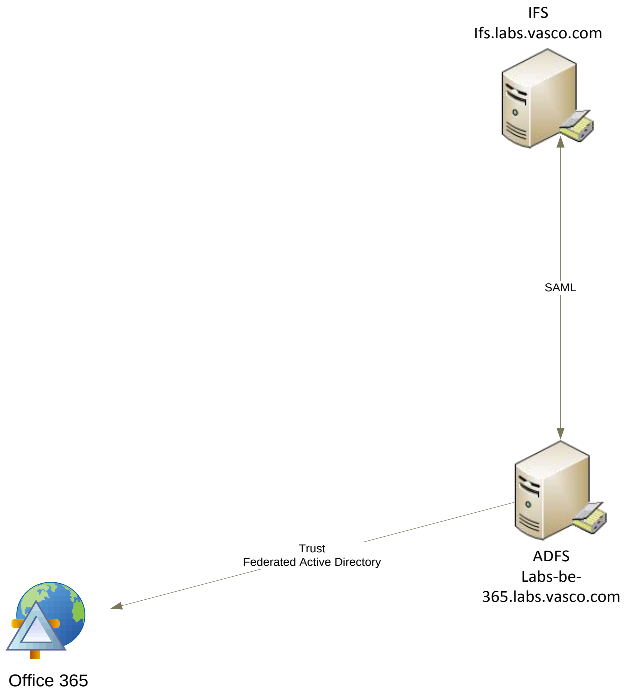
The site that you are accessing requires you to sign in. Select your organization from the following list.

ifs.labs.vasco.com

Click on **Continue to Sign In** and you will be redirected to the login page of your IDENTIKEY Federation Server. Once Logged in you will be redirected to your Active Directory Federation Service login page stating you are logged in.

4 Office 365 and IDENTIKEY Federation Server

4.1 Architecture



4.2 Pre-requisites

To connect Office 365 to IDENTIKEY Federation Server via Active Directory Federation Service you will need to add a small tool used for name translation between the IDENTIKEY Federation Server and Office 365. This tool needs to be installed on the Active Directory Federation Service server.

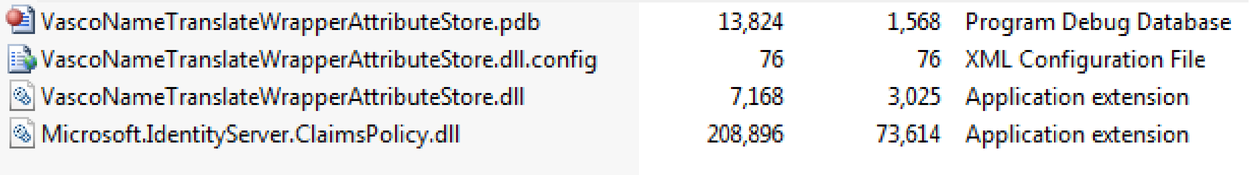
The tool itself requires .NET 4.0 and in most cases you will be running .NET 3.5. When this is the case you will need to install .NET 4.0 and edit a configuration file:

Edit the file Microsoft.IdentityServer.Servicehost.exe.config, which is located in **<ADFS installation home>/** (by default: “C:\Program Files\Active Directory Federation Services 2.0”). Here, add the following lines:

```
<configuration>
      (...)
      <startup>
      <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
      </startup>
</configuration>
```

Now **Restart** the Active Directory Federation Service and it will support .NET 4.0.

You can find this tool on the installation disk of the IDENTIKEY Federation Server under: **Office 365/bin**. Copy all the contents from this file to **<ADFS installation home>/** (by default: “C:\Program Files\Active Directory Federation Services 2.0”) and restart the service.



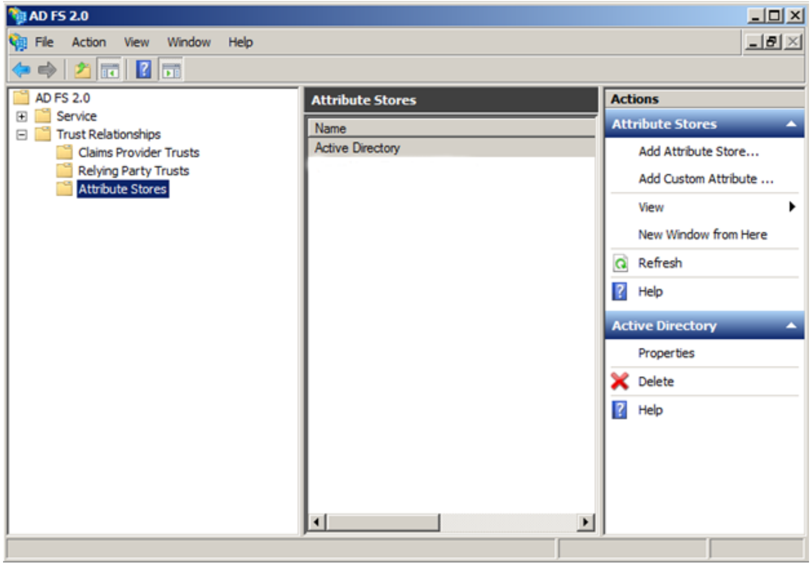
VascoNameTranslateWrapperAttributeStore.pdb	13,824	1,568	Program Debug Database
VascoNameTranslateWrapperAttributeStore.dll.config	76	76	XML Configuration File
VascoNameTranslateWrapperAttributeStore.dll	7,168	3,025	Application extension
Microsoft.IdentityServer.ClaimsPolicy.dll	208,896	73,614	Application extension

The tool is now installed.

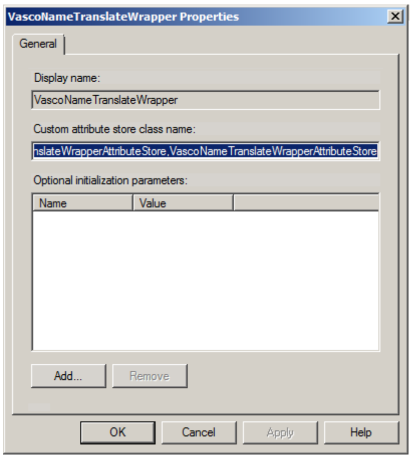
4.3 Configuration

4.3.1 Adding Attribute Store

Start the Active Directory Federation Service Management Console.



Expand **Trust Relationships** and click on **Attribute Stores**. In the actions pane, click on **Add Custom Attribute Store**.



VascoNameTranslateWrapper Properties

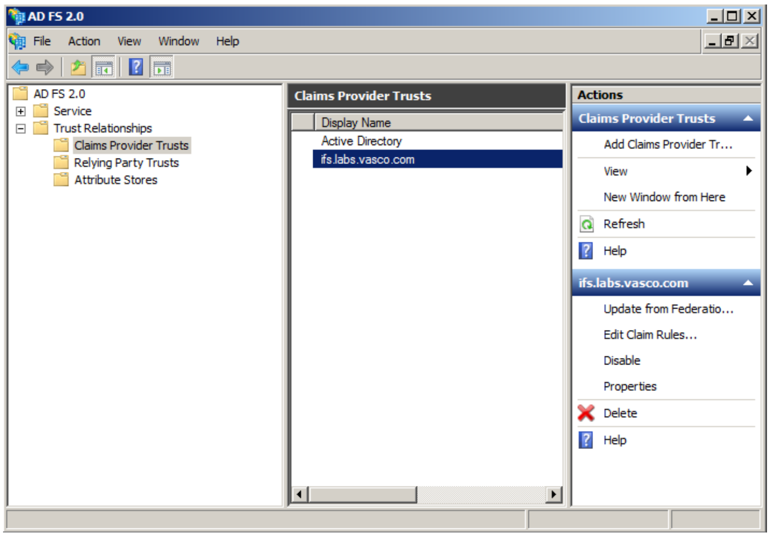
Display name: VascoNameTranslateWrapper

Custom attribute store class name: nslateWrapperAttributeStore,VascoNameTranslateWrapperAttributeStore

Optional initialization parameters:

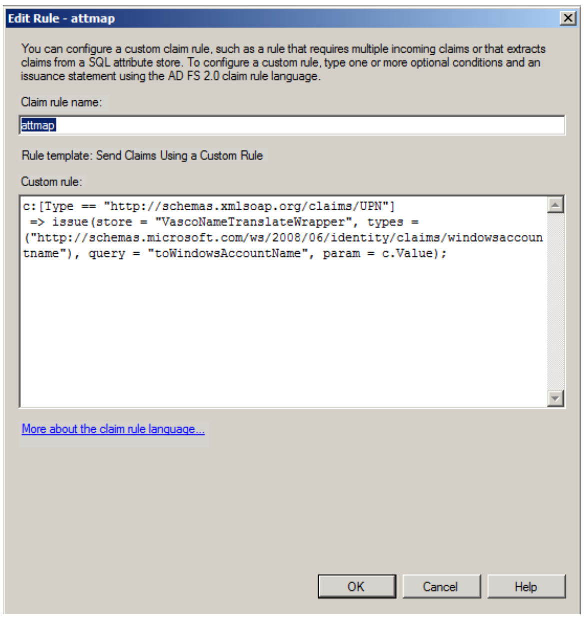
Name	Value

- Display name: **VascoNameTranslateWrapper**
- Custom attribute store class name: **VascoNameTranslateWrapperAttributeStore.VascoNameTranslateWrapperAttributeStore, VascoNameTranslateWrapperAttributeStore**
- Click **OK**



Click on **Claims Provider Trust** and select your IDENTIKEY Federation Server (in our example: **ifs.labs.vasco.com**). In the actions pane, click on **Edit Claim Rules**.

A new window pops up and click on **Add Rule**.


Edit Rule - attmap

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name: attmap

Rule template: Send Claims Using a Custom Rule

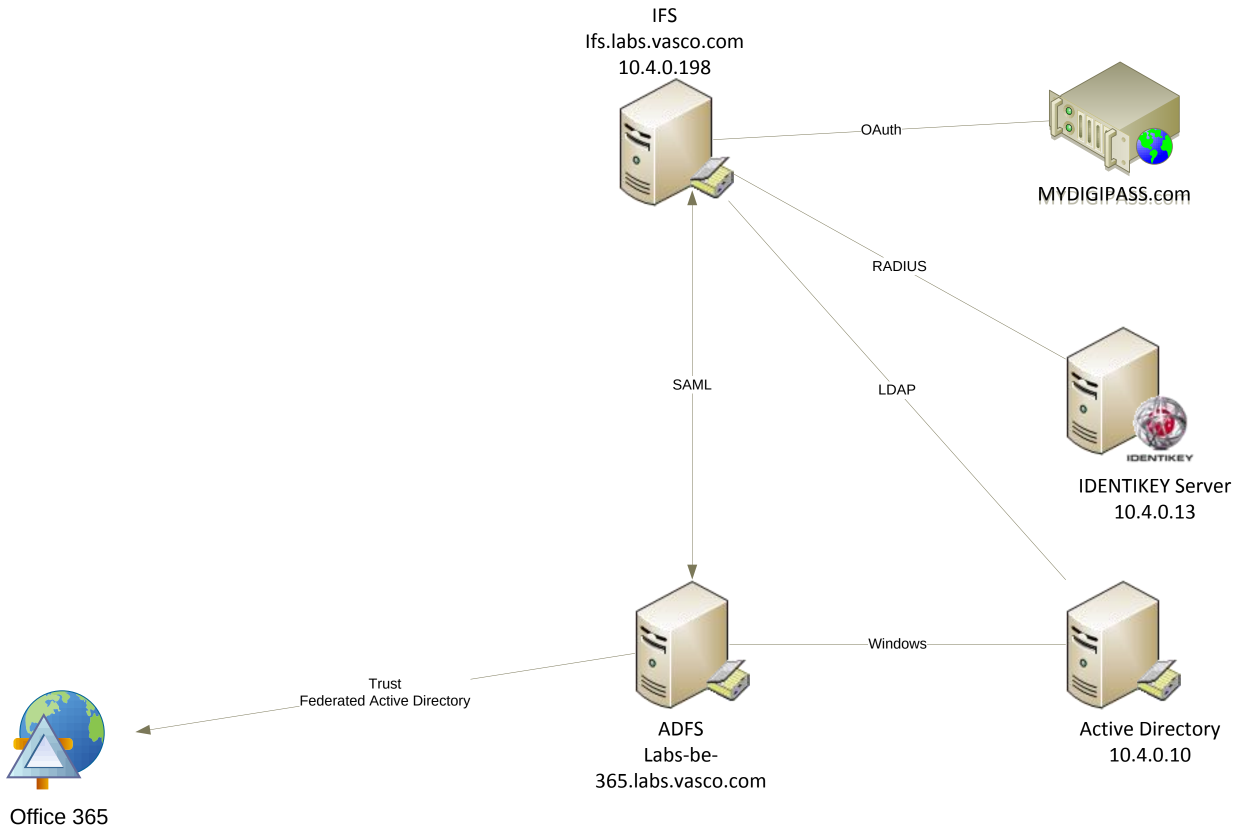
Custom rule:

```
c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]
 => issue(store = "VascoNameTranslateWrapper", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccoun
tname"), query = "toWindowsAccountName", param = c.Value);
```

- Claim rule name: **attmap**
- Custom rule: **c:[Type == "http://schemas.xmlsoap.org/claims/UPN"] => issue(store = "VascoNameTranslateWrapper", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"), query = "toWindowsAccountName", param = c.Value);**
- Click **OK**

5 Basic IDENTIKEY Federation Setup

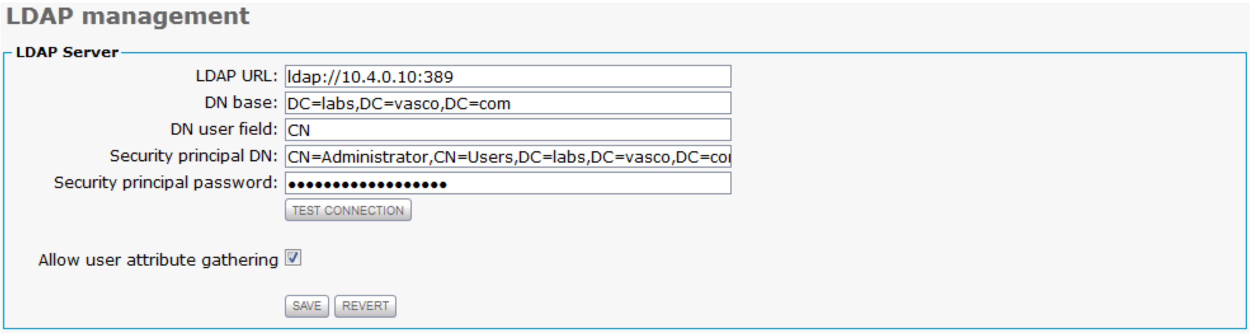
5.1 Setup



5.2 Back-ends

5.2.1 LDAP

Log into IDENTIKEY Federation Server's management web console and navigate to **Authentication**, **LDAP**.



LDAP management

LDAP Server

LDAP URL:	ldap://10.4.0.10:389
DN base:	DC=labs,DC=vasco,DC=com
DN user field:	CN
Security principal DN:	CN=Administrator,CN=Users,DC=labs,DC=vasco,DC=co
Security principal password:	●●●●●●●●●●●●●●●●●●

Allow user attribute gathering ☑

- LDAP URL: **ldap://10.4.0.10:389**

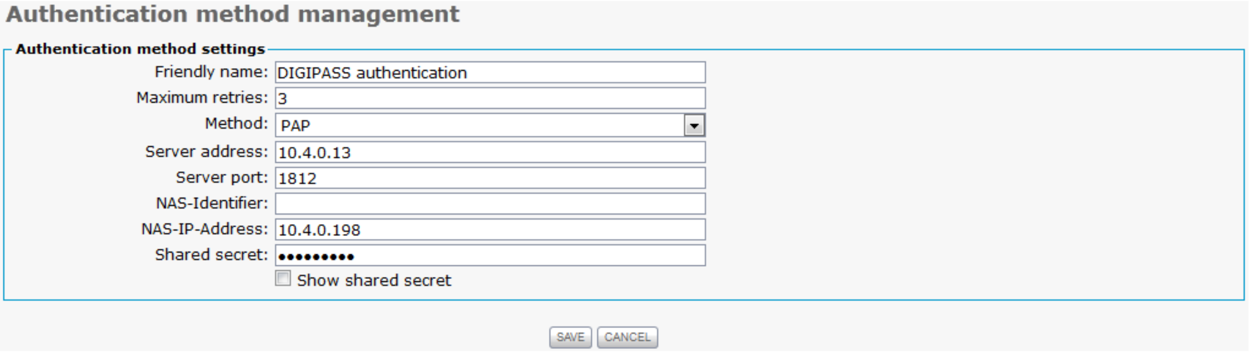
- DN base: **DC=labs,DC=vasco,DC=com**
- DN user field: **CN**
- Security principal DN: **CN=Administrator,CN=Users,DC=labs,DC=vasco,DC=com**
- Security principal password: **<administrator password>**
- Check **Allow user attribute gathering**
- Click **Save**

By clicking on **Test Connection** you can verify if the data you set is correct.

5.2.2 IDENTIKEY Authentication Server

Log into IDENTIKEY Federation Server's management web console and navigate to **Authentication**, **Manage methods**.

Edit DIGIPASS authentication.



Authentication method management

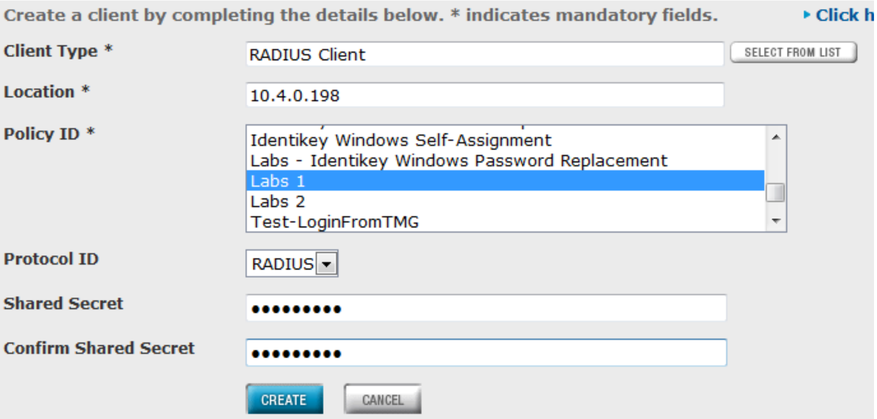
Authentication method settings

Friendly name: DIGIPASS authentication
Maximum retries: 3
Method: PAP
Server address: 10.4.0.13
Server port: 1812
NAS-Identifier:
NAS-IP-Address: 10.4.0.198
Shared secret: •••••••••
□ Show shared secret

- Friendly name: **DIGIPASS authentication**
- Maximum retries: **3**
- Method: **PAP**
- Server address: **10.4.0.13**
- Server port: **1812**
- NAS-IP-Address: **10.4.0.198**
- Shared secret: **<RADIUS secret>** (can be chosen)
- Click **Save**

5.2.2.1 IDENTIKEY Authentication Server Client

Log into your IDENTIKEY Authentication Server and go to **Clients**, **Register**.



Create a client by completing the details below. * indicates mandatory fields.

Client Type * RADIUS Client
Location * 10.4.0.198
Policy ID * Identikey Windows Self-Assignment
Labs - Identikey Windows Password Replacement
Labs 1
Labs 2
Test-LoginFromTMG
Protocol ID RADIUS
Shared Secret •••••••••
Confirm Shared Secret •••••••••

- Client Type : select **Radius Client** from "**select from list**"
- Location : **10.4.0.198**

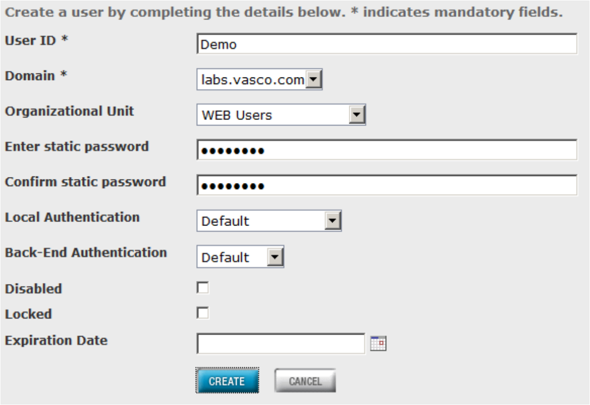
- Policy ID : Select a policy
- Protocol ID: **RADIUS**
- Shared Secret: **<RADIUS secret>**
- Confirm Shared Secret: reenter the **<RADIUS secret>**
- Click **Create**

Make sure that the **<RADIUS secret>** is the same on both IDENTIKEY Federation Server and IDENTIKEY Authentication Server.

5.2.2.2 Creating a demo user

The user created in the IDENTIKEY Authentication Server has to exist in the Active Directory.

Log into your IDENTIKEY Authentication Server and go to **Users**, **Create**.



Create a user by completing the details below. * indicates mandatory fields.

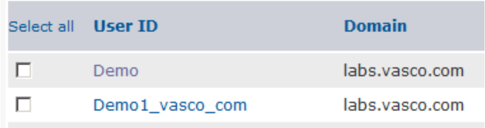
User ID *	Demo
Domain *	labs.vasco.com
Organizational Unit	WEB Users
Enter static password	••••••••
Confirm static password	••••••••
Local Authentication	Default
Back-End Authentication	Default
Disabled	□
Locked	□
Expiration Date	

- User ID: **<your-user>** (in our setup: **Demo**)
- Domain: **<your-domain>** (in our setup: **labs.vasco.com**)
- Organizational unit: **<your-OU>** (OPTIONAL, in our setup: **WEB Users**)
- Enter static password: **<your-password>**
- Confirm static password: **<your-password>**
- Local Authentication: **Default**
- Back-end Authentication: **Default**
- Click on **Create**

You have now added a user in your IDENTIKEY Authentication Server.

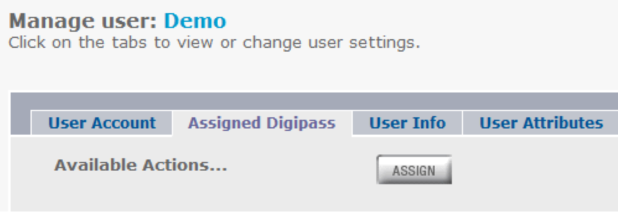
5.2.2.3 Attaching a DIGIPASS

Log into your IDENTIKEY Authentication Server and type the name of a user in the **FIND** field then click **SEARCH**.



Select all	User ID	Domain
□	Demo	labs.vasco.com
□	Demo1_vasco_com	labs.vasco.com

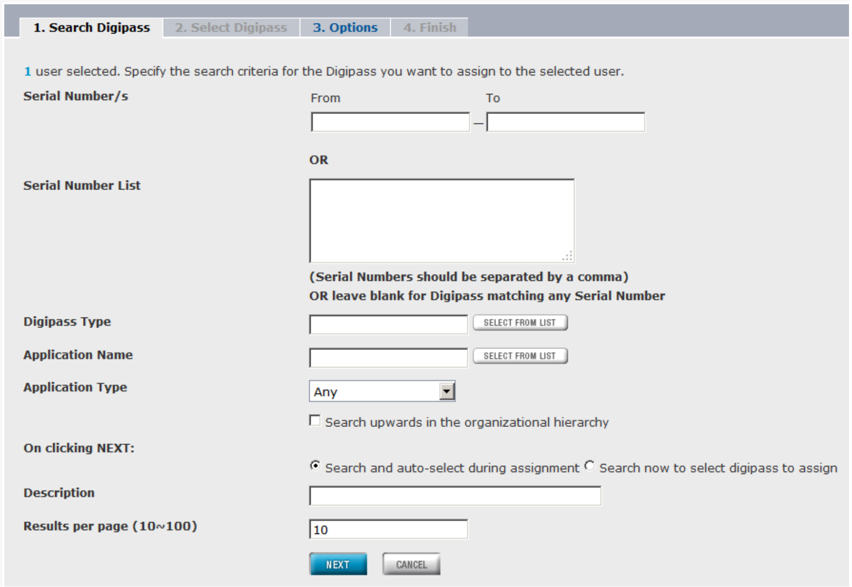
Click on the **User ID** and navigate to **Assigned DIGIPASS**.



Manage user: Demo

Click on the tabs to view or change user settings.

Click on **ASSIGN**.



1 user selected. Specify the search criteria for the Digipass you want to assign to the selected user.

Serial Number/s — From: ______ – To: ______

OR

Serial Number List: ______

(Serial Numbers should be separated by a comma)
OR leave blank for Digipass matching any Serial Number

Digipass Type: ______ SELECT FROM LIST

Application Name: ______ SELECT FROM LIST

Application Type: Any

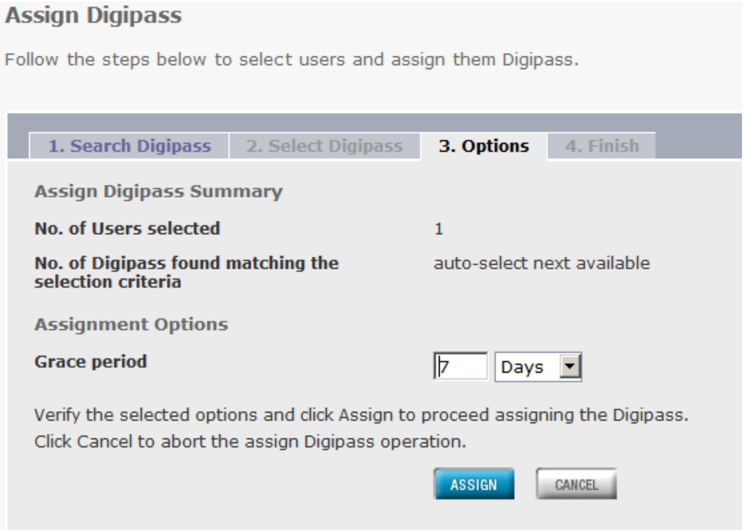
□ Search upwards in the organizational hierarchy

On clicking NEXT: ● Search and auto-select during assignment ○ Search now to select digipass to assign

Description: ______

Results per page (10~100): 10

Click **NEXT**.



Assign Digipass

Follow the steps below to select users and assign them Digipass.

Assign Digipass Summary

No. of Users selected	1
No. of Digipass found matching the selection criteria	auto-select next available

Assignment Options

Grace period: 7 Days

Verify the selected options and click Assign to proceed assigning the Digipass.
Click Cancel to abort the assign Digipass operation.

Click **ASSIGN**.

Click **FINISH**.

With the DIGIPASS assigned, the user is now ready for testing.

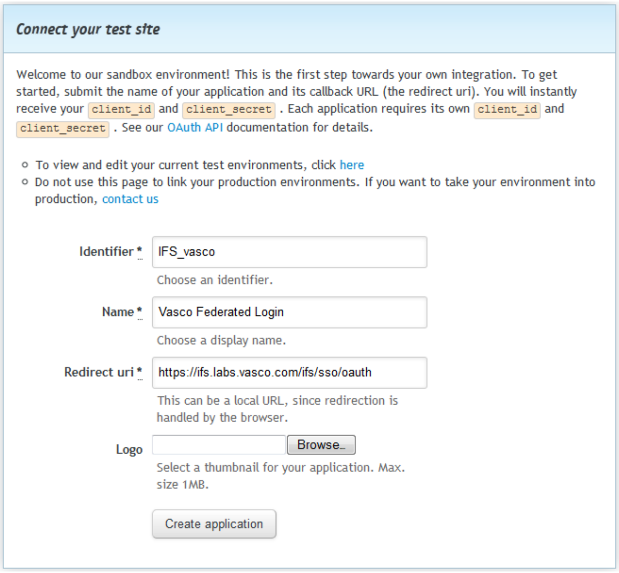
5.3 Additional authentication methods

5.3.1 MYDIGIPASS.com

To illustrate adding an OAuth provider, MYDIGIPASS.com's sandbox environment will be used as example. If you do not have a MYDIGIPASS developer account, you can create one for free on https://developer.mydigipass.com/.

Log into your MYDIGIPASS.com developer account and go to **Sandbox**.

Click on **Connect your test site**.



Connect your test site

Welcome to our sandbox environment! This is the first step towards your own integration. To get started, submit the name of your application and its callback URL (the redirect uri). You will instantly receive your `client_id` and `client_secret` . Each application requires its own `client_id` and `client_secret` . See our OAuth API documentation for details.

- To view and edit your current test environments, click here
- Do not use this page to link your production environments. If you want to take your environment into production, contact us

Identifier * IFS_vasco
Choose an identifier.

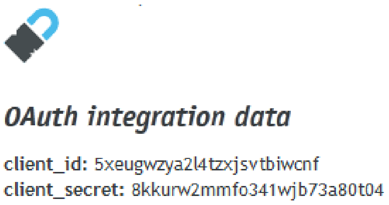
Name * Vasco Federated Login
Choose a display name.

Redirect uri * https://ifs.labs.vasco.com/ifs/sso/oauth
This can be a local URL, since redirection is handled by the browser.

Logo
Select a thumbnail for your application. Max. size 1MB.

- Identifier: **IFS_vasco** (this must be a unique identifier)
- Name: **Vasco Federated Login**
- Redirect uri: **https://<ifs-host>/ifs/sso/oauth** (in our application: https://ifs.labs.vasco.com/ifs/sso/oauth)
- Click on **Create application**

Go to **Sandbox** and click on your newly generated test site.

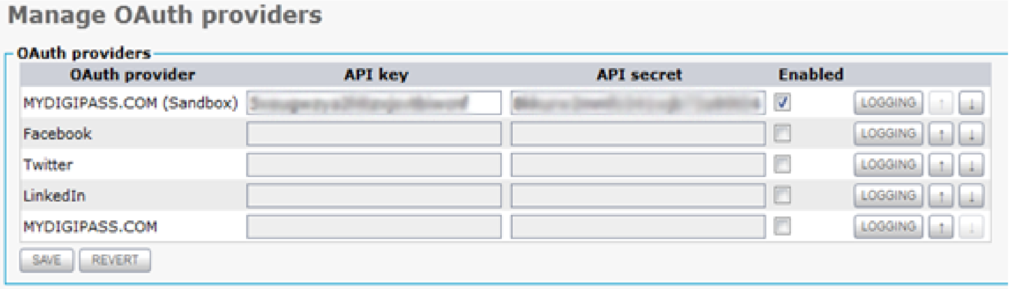


OAuth integration data

client_id: 5xeugwzya2l4tzxjsvtbiwcnf
client_secret: 8kkurw2mmfo341wjb73a80t04

Take note of the **client_id** and the **client_secret**.

Log into your IDENTIKEY Federation Server's management web console and go to **Federated authentication**, **Manage OAuth providers**.



Manage OAuth providers

OAuth providers

OAuth provider	API key	API secret	Enabled			
MYDIGIPASS.COM (Sandbox)	[redacted]	[redacted]	☑	LOGGING	↑	↓
Facebook			□	LOGGING	↑	↓
Twitter			□	LOGGING	↑	↓
LinkedIn			□	LOGGING	↑	↓
MYDIGIPASS.COM			□	LOGGING	↑	↓

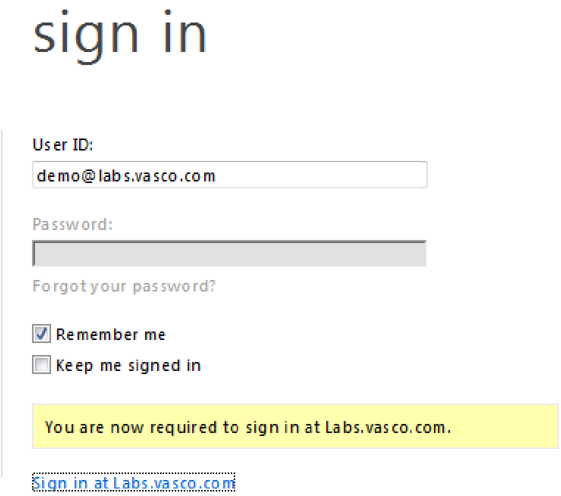
- Check **Enabled** for MYDIGIPASS.COM (Sandbox)
- Fill in the **client_id** of your OAuth provider
- Fill in the **client_secret** of your OAuth provider
- Click **Save**

6 Test the solution

6.1 IDENTIKEY Authentication Server

6.1.1 Response only

Open a browser and navigate to https://portal.microsoftonline.com. Enter your user@yourdomain and press tab. The password field will grey out and you will be asked to log in using your domain.



sign in

User ID:
demo@labs.vasco.com

Password:

Forgot your password?

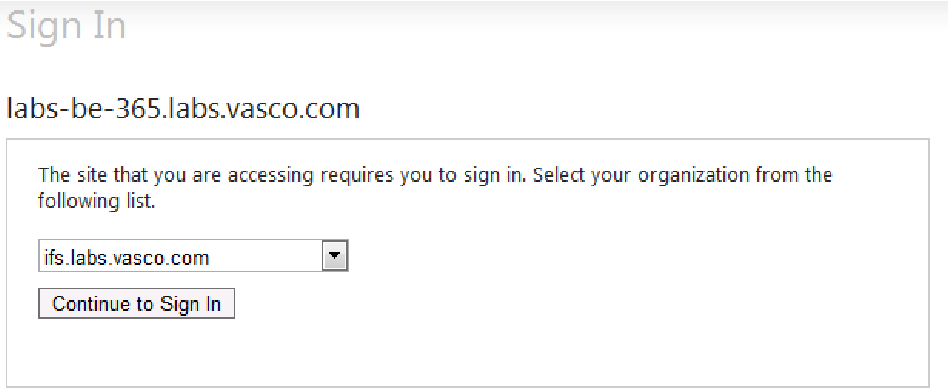
☑ Remember me

□ Keep me signed in

You are now required to sign in at Labs.vasco.com.

Sign in at Labs.vasco.com

When clicking on the link **Sign in at <your-domain>**, you will be redirected to the Active Directory Federation Server’s realm page. Here you can choose which Identity Provider you wish to use (the choice of the claims provider will be saved once a successful login occurred).



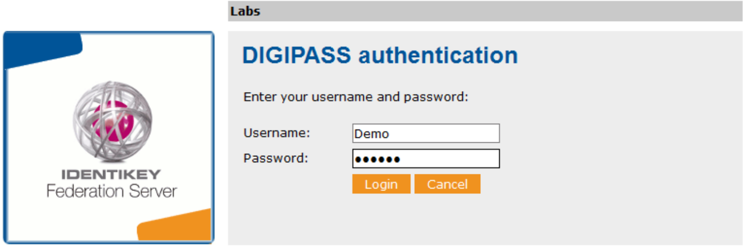
Sign In

labs-be-365.labs.vasco.com

The site that you are accessing requires you to sign in. Select your organization from the following list.

ifs.labs.vasco.com

Select your IDENTIKEY Federation Server and continue. Now you are redirected to the login page on the IDENTIKEY Federation Server using the authentication method selected in the application.



DIGIPASS authentication

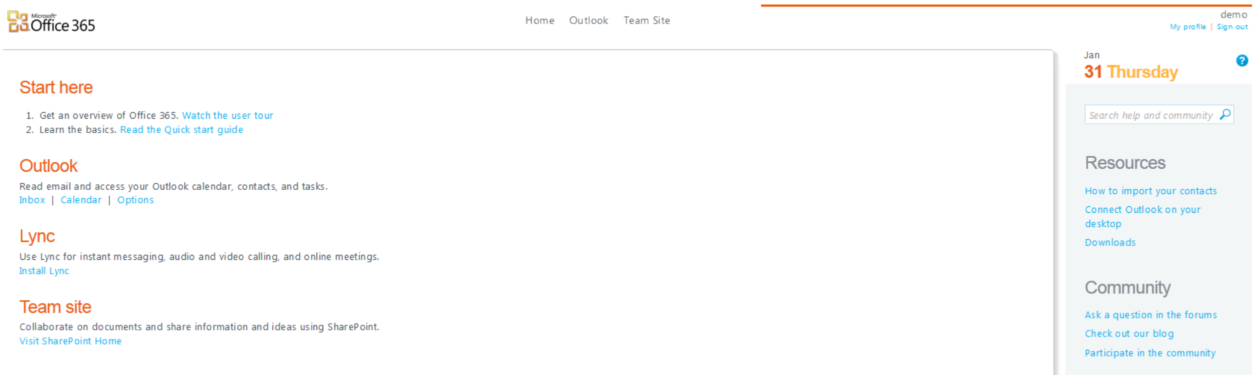
Enter your username and password:

Username: Demo

Password: ••••••

- Username: **Demo** (this is the user we added in 5.2.2.2 Creating a demo user)
- Password: **One Time Password** (this is an OTP received from the device assigned to the user in 5.2.2.3 Attaching a DIGIPASS)

Once you have logged in you will be redirected to your Office 365 account.



Start here

1. Get an overview of Office 365. Watch the user tour
2. Learn the basics. Read the Quick start guide

Outlook

Read email and access your Outlook calendar, contacts, and tasks.
Inbox | Calendar | Options

Lync

Use Lync for instant messaging, audio and video calling, and online meetings.
Install Lync

Team site

Collaborate on documents and share information and ideas using SharePoint.
Visit SharePoint Home

Jan
31 Thursday

Resources

How to import your contacts
Connect Outlook on your desktop
Downloads

Community

Ask a question in the forums
Check out our blog
Participate in the community

6.1.2 Challenge response and Backup Virtual DIGIPASS

The IDENTIKEY Federation Server version 1.2 does not yet support challenge response and Backup Virtual DIGIPASS.