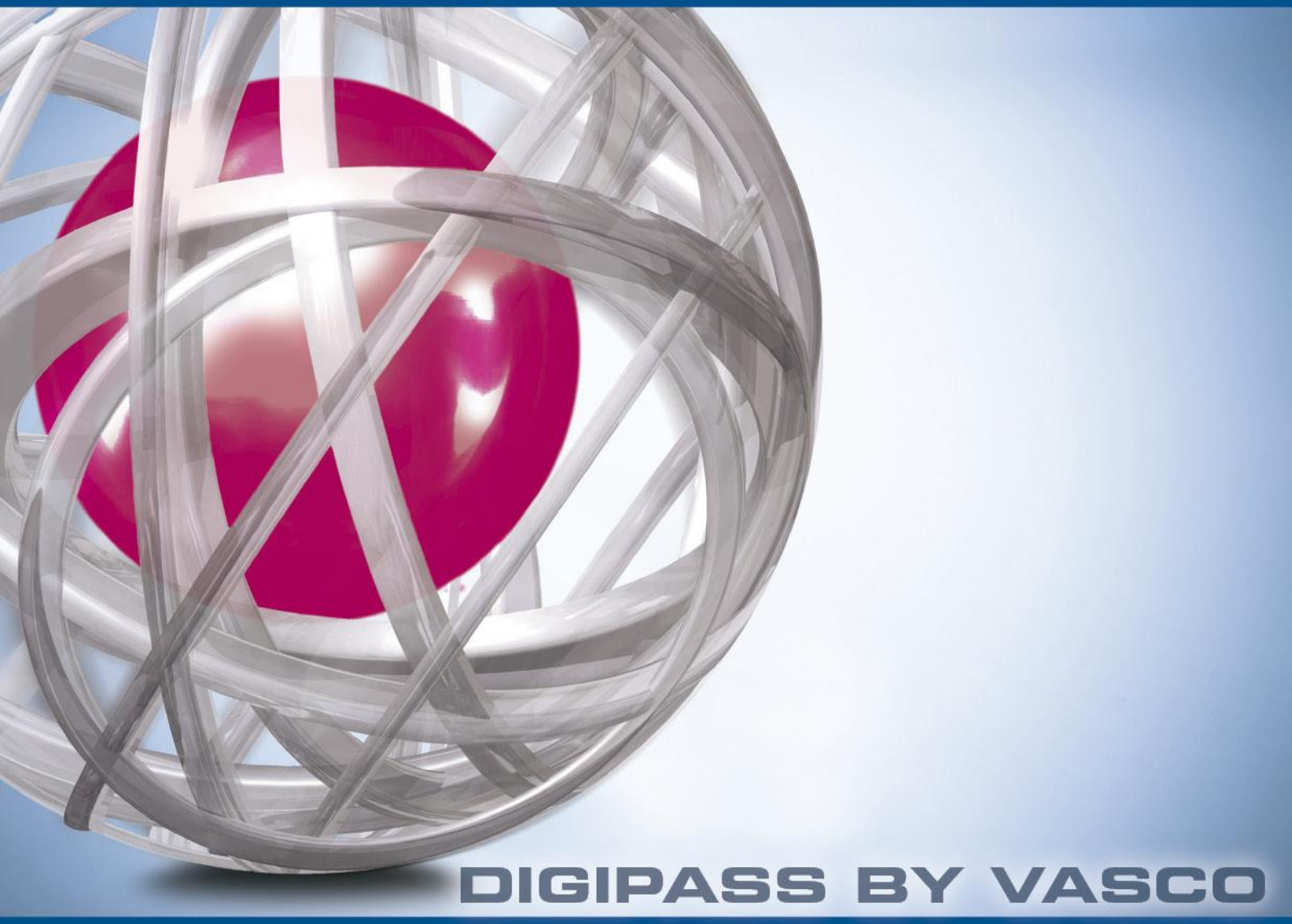
INTEGRATION GUIDE

DIGIPASS Authentication for Office 365 using IDENTIKEY Authentication Server with Forms based Web Filter



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.

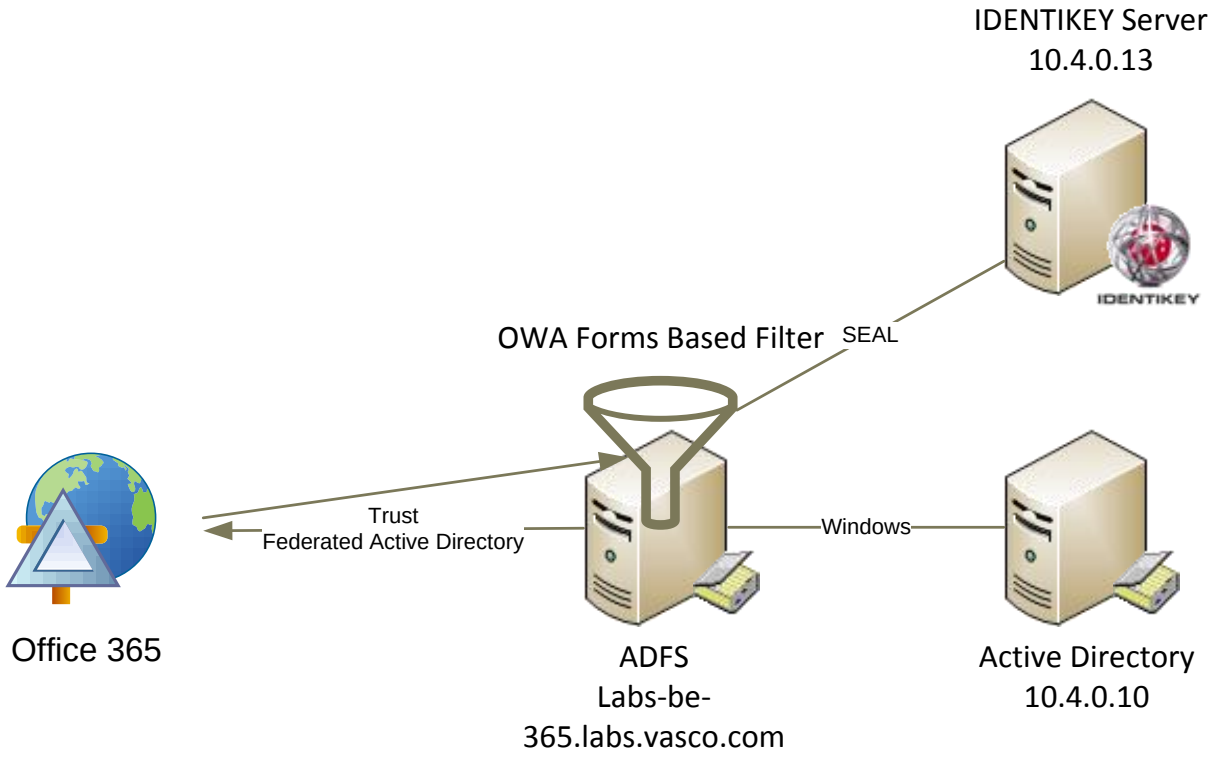
In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

Copyright

Table of Contents

1 Overview

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 Technical Concepts

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 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.

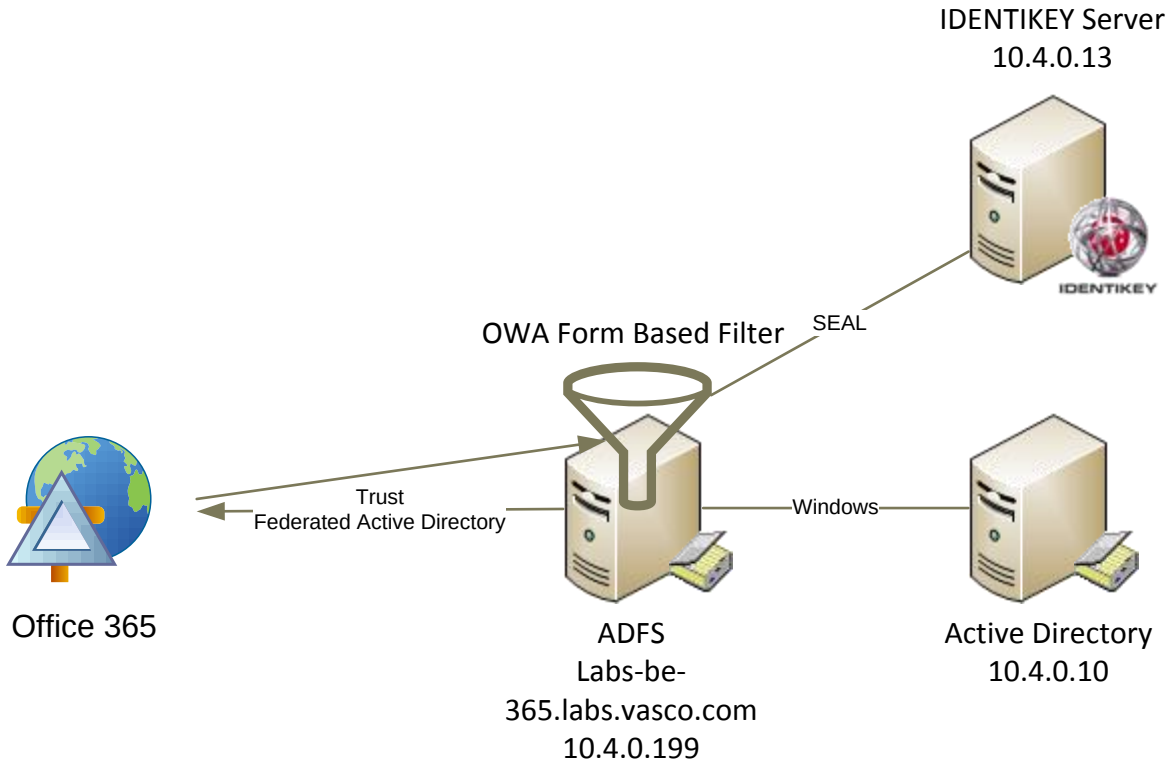
The use and configuration of an IDENTIKEY Authentication Server and an IDENTIKEY Authentication Appliance is similar.

2.2.2 DIGIPASS Authentication for OWA – Forms

The DIGIPASS Authentication Plug-In is an add-on for Internet Information Services (IIS) and can be configured to intercept authentication requests to Web sites using the HTTP forms authentication mechanism. It allows users to use one-time passwords (OTPs) instead of static passwords. The plug-in intercepts authentication requests, validates the OTP, and replaces it with the static password expected by the back-end. The OTPs are validated using an IDENTIKEY Authentication Server or IDENTIKEY Authentication Appliance.

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).

In addition you will need to have installed the DIGIPASS Authentication for IIS – forms based filter. This installation is easily done by following the documentation provided with the package.

Following items are needed:

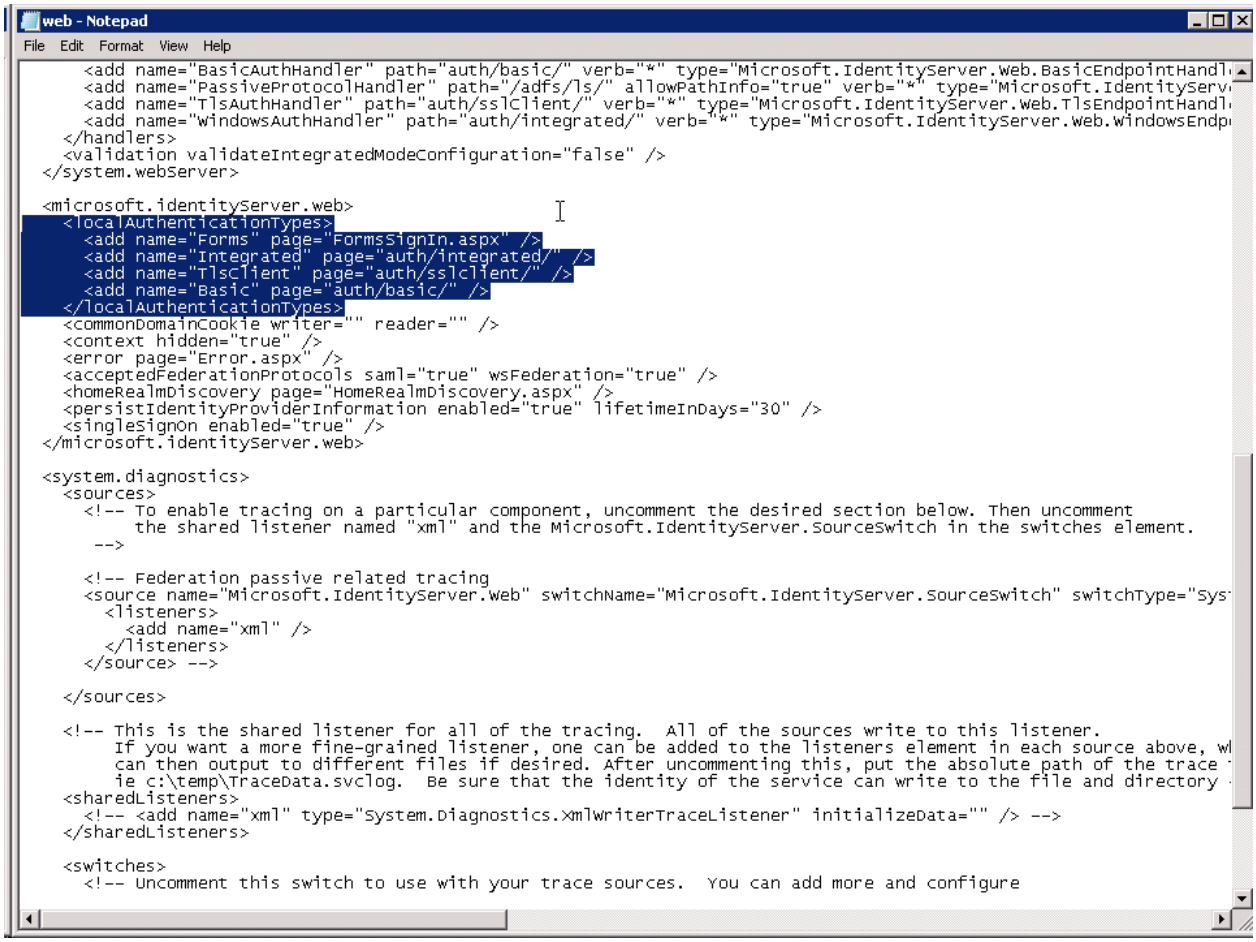
- Active Directory Federation Service
- Active Directory Federation Service – Office 365 connection
- VASCO OWA Forms based Filter
- IDENTIKEY Authentication Server running
- Message Delivery Component (optional)
- SMS-Gateway (optional)

3.3 Enabling forms

3.3.1 Active Directory Federation Service

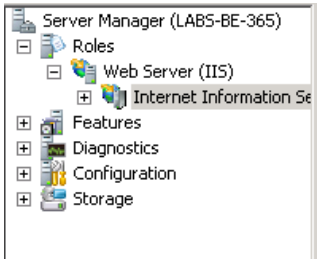
To enable forms based sign-on in your domain, you must **edit** the **web.xml** file. This file can be found in **<ADFS-web-folder>/web.xml** (by default: C:\inetpub\adfs\ls\web.xml).

In this file search for **localAuthenticationTypes**. In the localAuthenticationTypes element make sure to place forms authentication first in line.

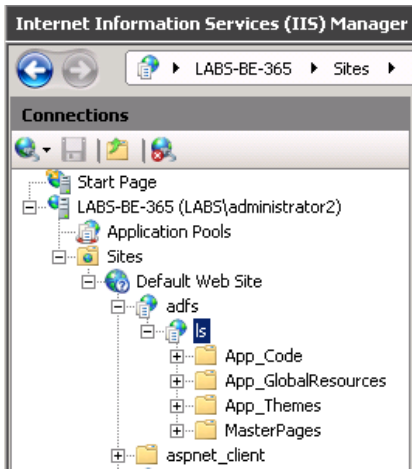


3.3.2 Internet Information Service

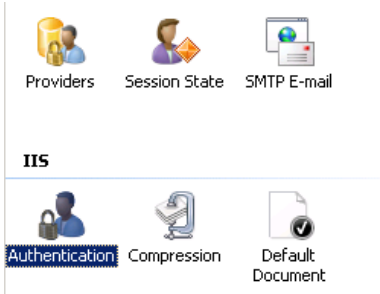
In the Server Manager, select your **Internet Information Service.**



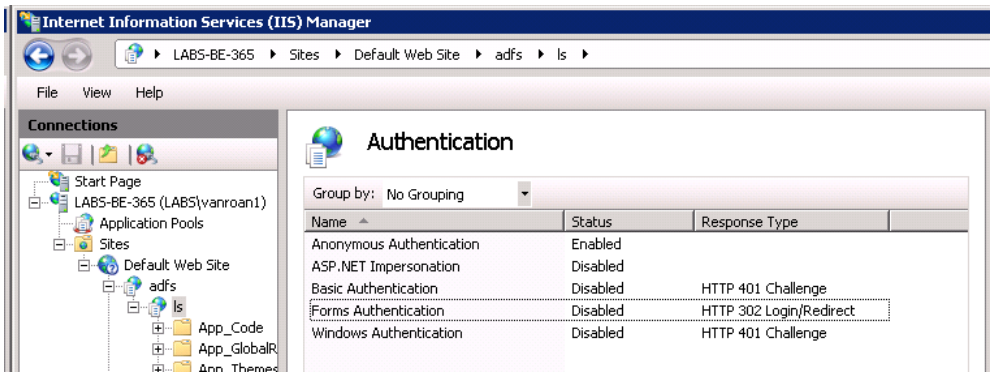
Under Connections, expand **<IIS-host>** (in our example: labs-be-365), **Sites**, **Default Web Site**, **adfs**. Select **ls**.



In the pane next to it a lot of options for that website will appear. Under **IIS**, double click on **Authentication**.



Enable Anonymous Authentication and disable all other authentication methods.



With this completed, forms based authentication will function properly.

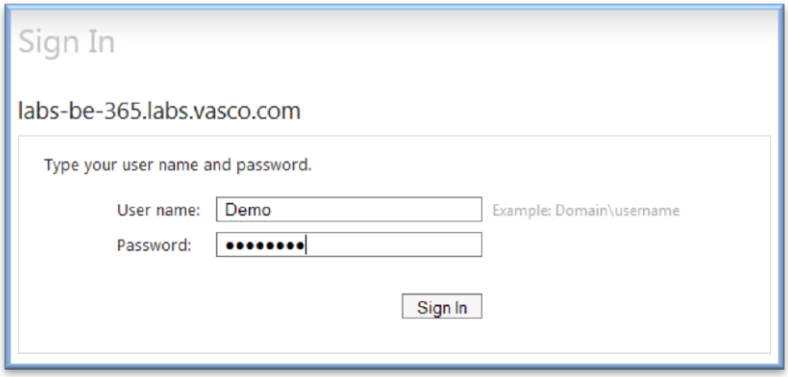
The reason why you have to make sure that even "Forms Authentication" is set to disabled is because the Active Directory Federation Service server will implement its own authentication ways.

As seen in 3.3.1 Active Directory Federation Service, the server will decide to take the first authentication method, and associated web page, declared in the web.xml file.

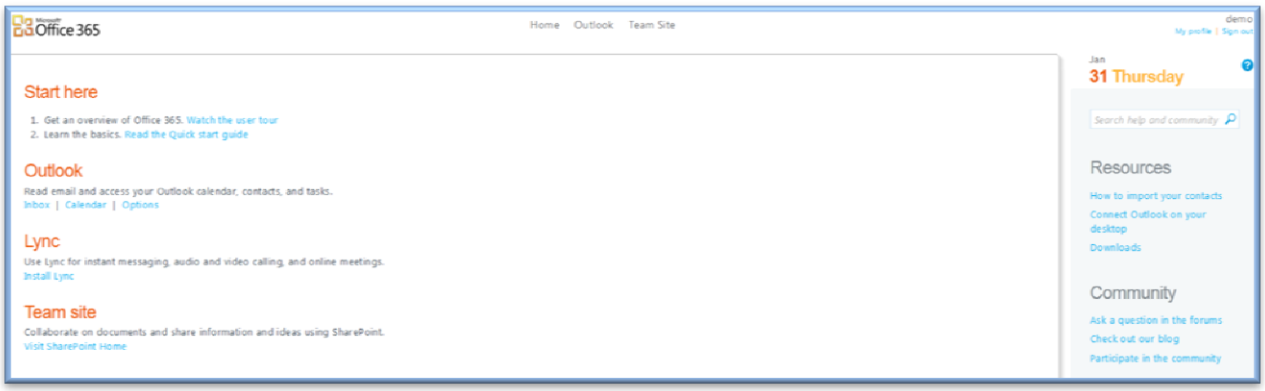
3.3.3 Test Forms based logon

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

When clicking on the link **Sign in at <your-domain>**, you will be redirected to the logon form of your Active Directory Federation Service.



Use your username and Active Directory credentials.



3.4 Installation of the web filter

The installer for this package can be found on the IDENTIKEY Authentication Server installation DVD.

Select the installer for the correct architecture of your server (x86/x64). When selecting the wrong architecture, the installer will inform you with an error and quit the installation.

Run the installer package **DIGIPASS Authentication for OWA Forms** on your Active Directory Federation Service server.

A wizard will open. Click **Next**.

I accept the terms in the license agreement and click **Next**.

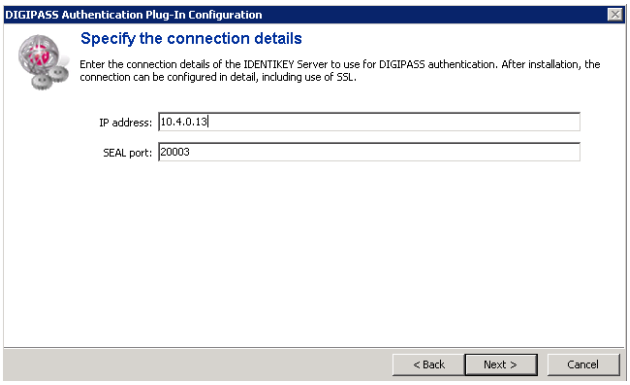
Keep the default destination folder and click **Next**.

Click **Install**.

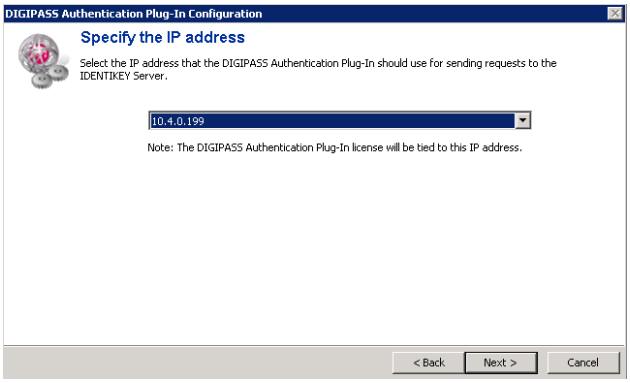
Now an installer will run and complete the installation process. Once it's done click **Finish** and a new wizard will open.

If no wizard opens after the installation go to: **Start**, **All programs**, **Vasco**, **DIGIPASS Authentication for IIS Basic**, **Configuration Wizard**.

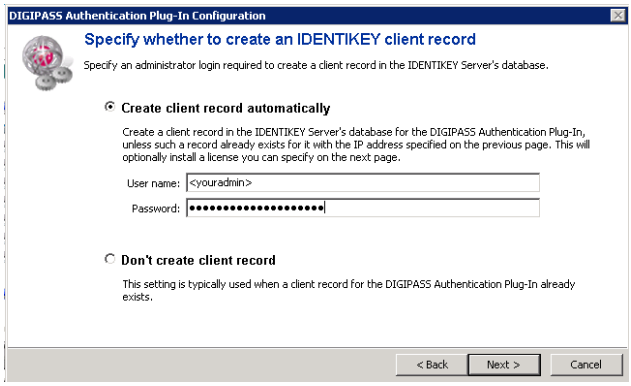
Click **Next**.



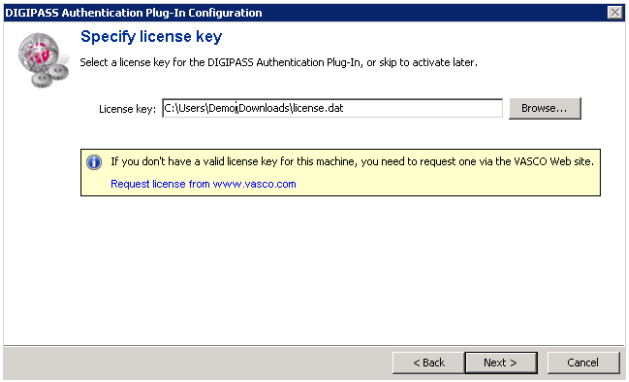
- IP address: **<your IDENTIKEY Authentication Server>**
- SEAL port: **20003** (default)



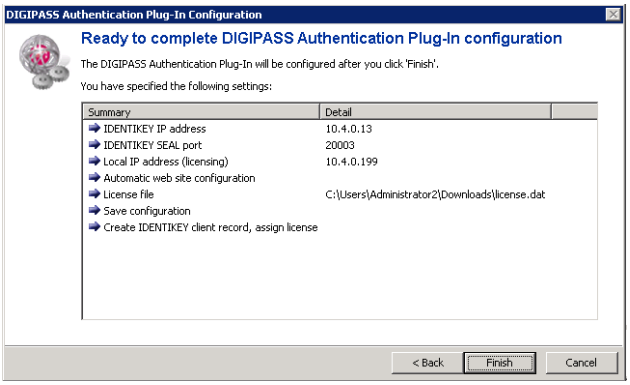
The IP address of your Active Directory Federation Server should be displayed here. Click **Next**.



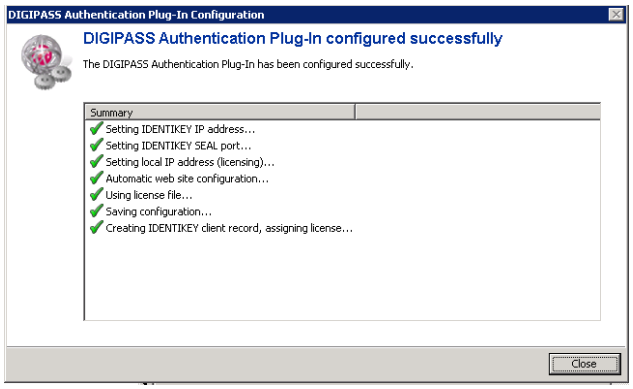
- Select **Create client record automatically**
- User name: **<your-admin>** (IDENTIKEY Authentication Server Admin username)
- Password: **<your-password>** (IDENTIKEY Authentication Server Admin password)
- Click **Next**



Click **Browse** and select your license for the web filter. Click **Next**.



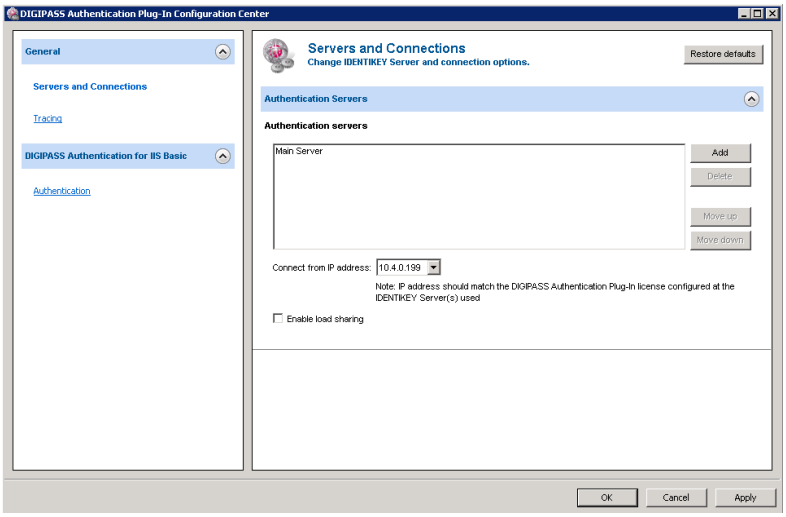
Click **Finish**.



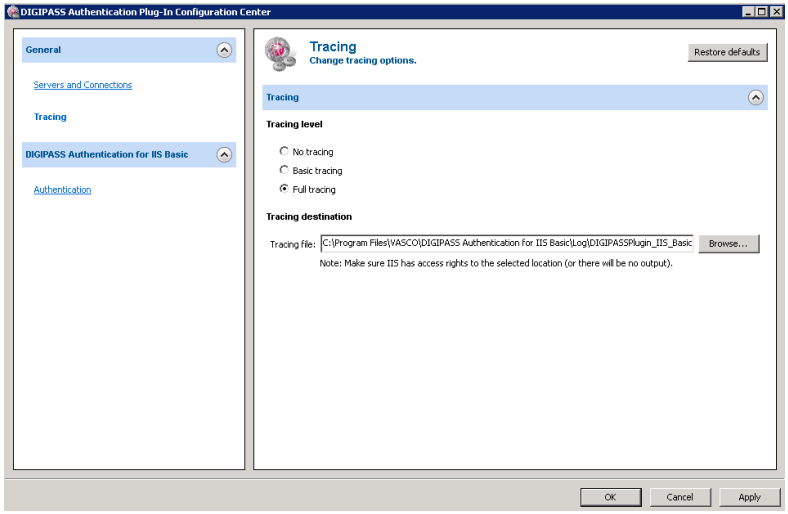
Click **Close**. The web filter is now installed.

3.5 Additional configuration of the web filter

Go to **Start**, **All programs**, **Vasco**, **DIGIPASS Authentication for IIS Basic**, **Configuration Center**.

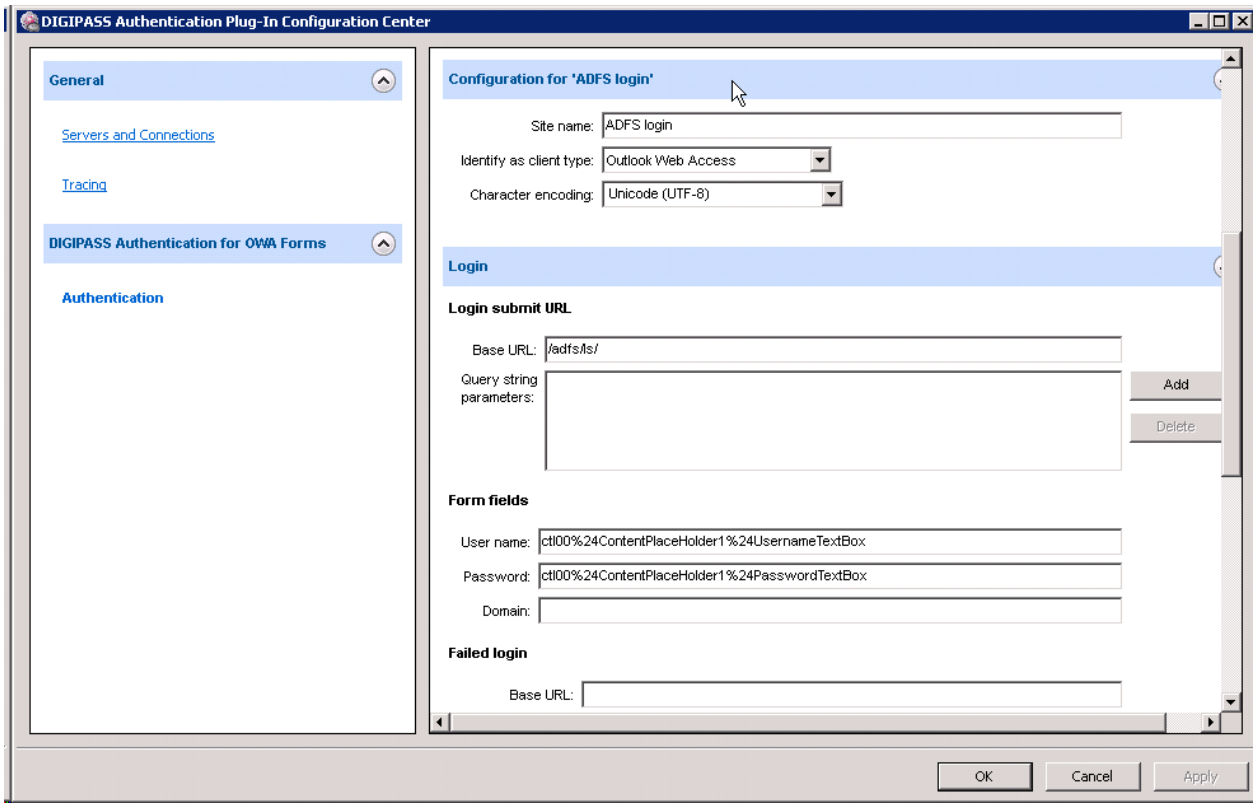


Click on **Tracing**.



Set the Tracing level to **Full tracing**.

Click on **Authentication**.



- Site name: **ADFS login**
- Base URL: **/adfs/ls/**
- Form fields
  - |User name: **ctl00%24ContentPlaceHolder1%24UsernameTextBox**
  - |Password: **ctl00%24ContentPlaceHolder1%24PasswordTextBox**
    └>(see below for more information)
- Click **OK**

To get the form fields you must go to the Active Directory Federation Service logon form page and view the source. The "name" attribute will then be used by the web filter.

```
<table class="UsernamePasswordTable">
    <tr>
        <td>
            <span class="Label"><span>User name: </span></span>
        </td>
        <td>
            <input name="ctl00$ContentPlaceHolder1$UsernameTextBox" type="text" id="ctl00_ContentPlaceHolder1_UsernameTextBox" />
        </td>
        <td class="TextColorSecondary TextSizeSmall">
            <span>Example: Domain\username</span>
        </td>
    </tr>
    <tr>
        <td>
            <span class="Label"><span>Password: </span></span>
        </td>
        <td>
            <input name="ctl00$ContentPlaceHolder1$PasswordTextBox" type="password" id="ctl00_ContentPlaceHolder1_PasswordTextBox" />
        </td>
        <td> </td>
    </tr>
```

Note that the names are: **ctl00$ContentPlaceHolder1$UsernameTextBox** and **ctl00$ContentPlaceHolder1$PasswordTextBox**. The filter will search for the URL encoded names. The URL encoding for the "$" character is: "%24".

The web filter is now fully configured and will start capturing.

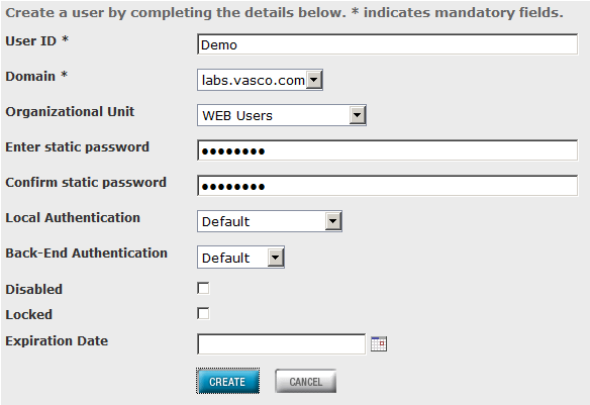
4 IDENTIKEY Authentication Server configuration

4.1 Creating a demo user

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

4.1.1 Registering a user

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



- 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**

For existing users you can use the Password Synchronization tool or the password auto-learn function. For more information on the Password Synchronization Manager please read the manual (can be found on the VASCO website: www.vasco.com). More information on the password auto-learn can be found in 4.3.3 Configuring the policy for password auto-learn.

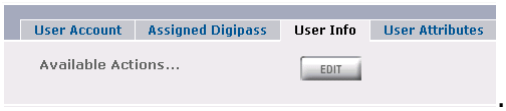
You have now added a user in your IDENTIKEY Authentication Server.

4.1.2 Adding additional user information

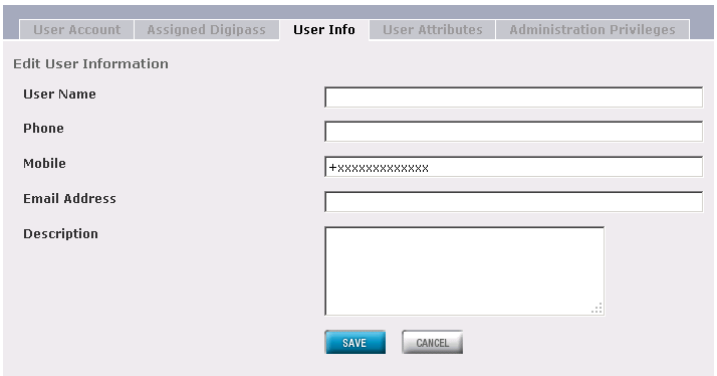
Log into your IDENTIKEY Authentication Server and type the name of a user in the **FIND** field then click **SEARCH**.

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

Click on the **User ID** and navigate to **User Info**



Click on **Edit**.

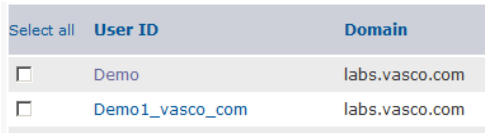


Fill in the **Mobile** and click **Save**.

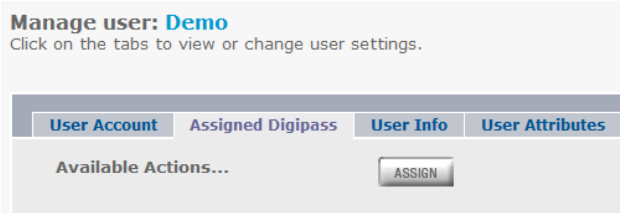
We will need a mobile phone number to use Backup Virtual DIGIPASS (explained later in this paper).

4.2 Attaching a DIGIPASS

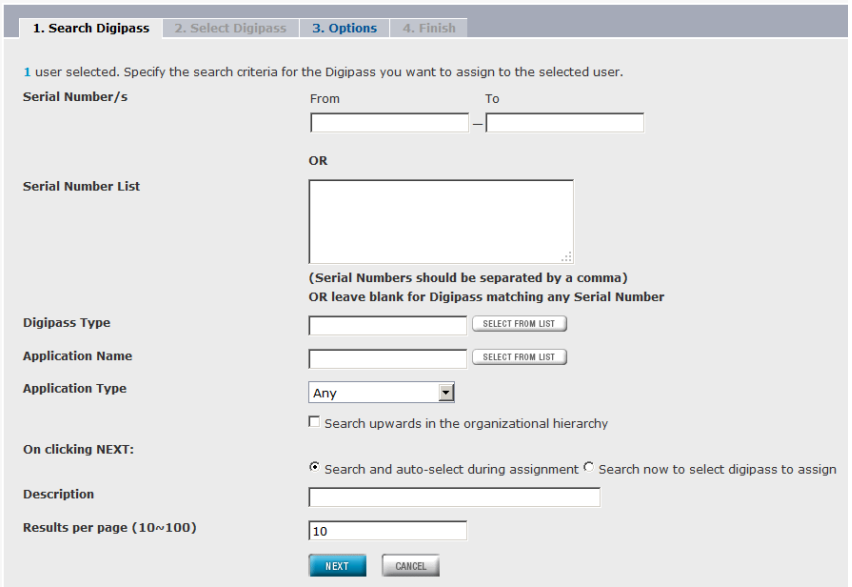
Log into your IDENTIKEY Authentication Server and type the name of a user in the **FIND** field then click **SEARCH**.



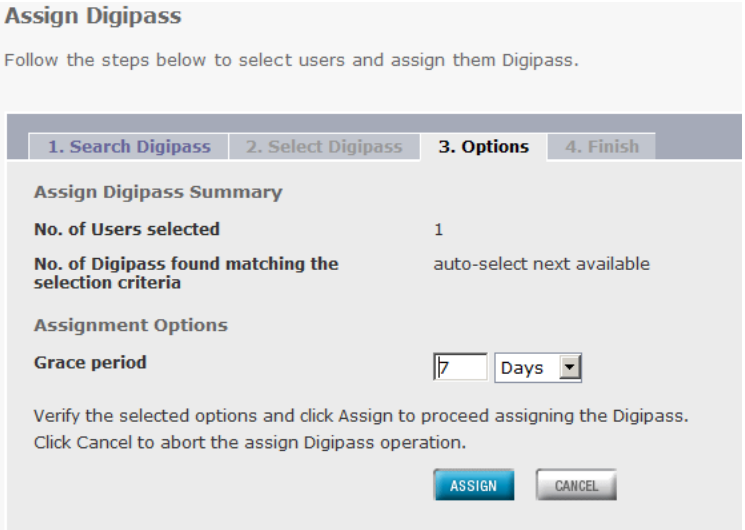
Click on the **User ID** and navigate to **Assigned DIGIPASS**.



Click on **ASSIGN**.



Click **NEXT**.



Click **ASSIGN**.

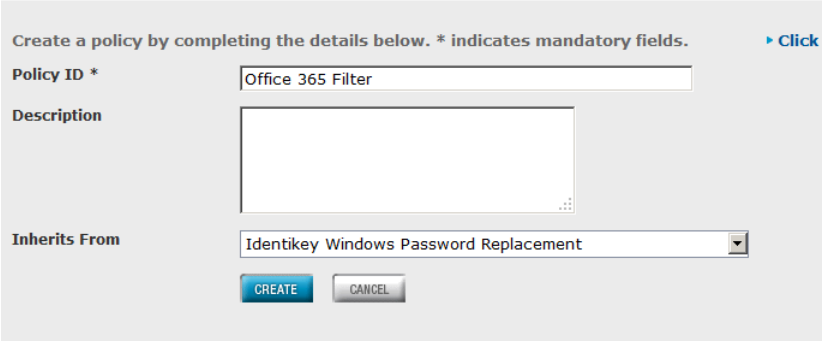
Click **FINISH**.

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

4.3 Policy

4.3.1 Creating the policy

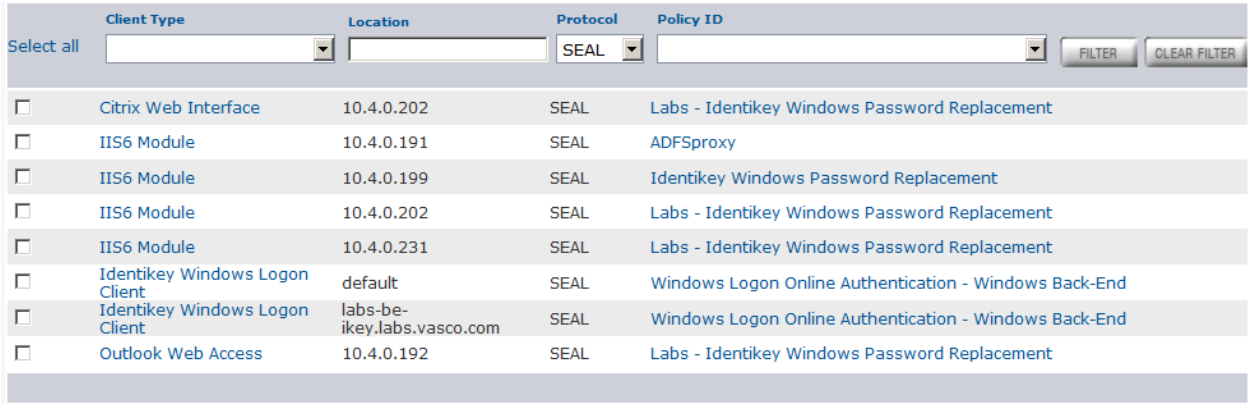
Log into your IDENTIKEY Authentication Server and go to **Policies**, **Create**.



- Policy ID: **Office 365 Filter**
- Inherits from: **Identikey Windows Password Replacement**
- Click **Create**

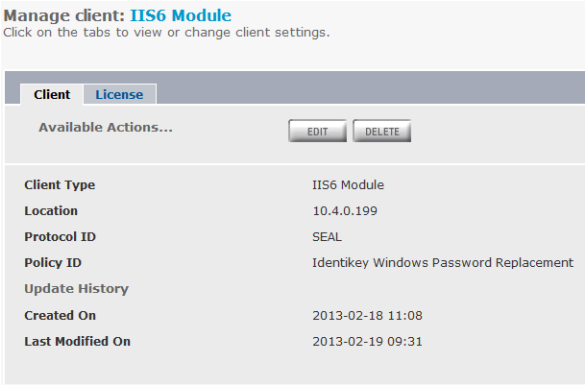
4.3.2 Attaching the policy

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

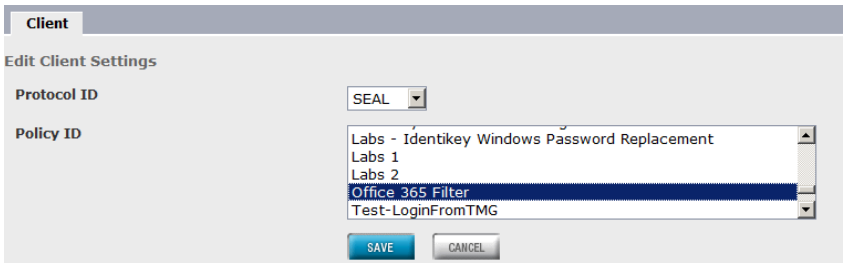


Select **SEAL** as protocol and click **Filter**.

Click on **IIS6 Module** where the location matches the IP-address of your **<ADFS-host>**.



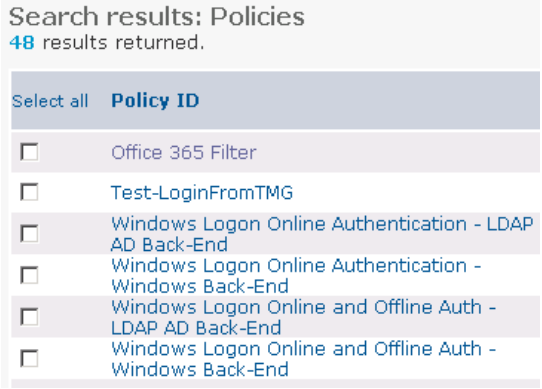
Click on **Edit**.



- Policy ID: **Office 365 Filter**
- Click **Save**

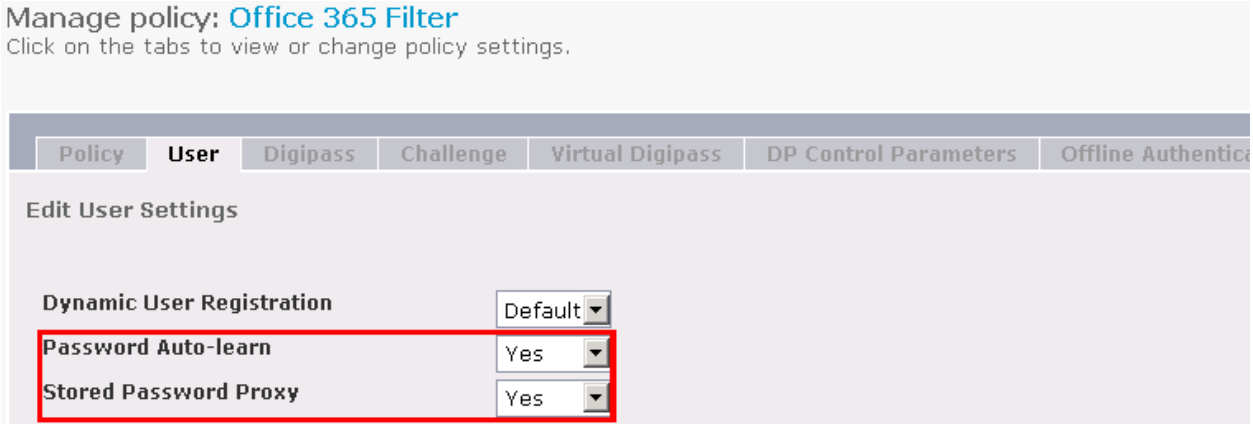
4.3.3 Configuring the policy for password auto-learn

Log into your IDENTIKEY Authentication Server and go to **Policy**, **List**.



Navigate the pages and look for the recently created policy (in our example: **Office 365 Filter**) and **click** on it.

Go to the **User** tab and click on **Edit**.



Make sure that Password Auto-learn and Stored Password Proxy are set to **Yes**.

Click **Save**.

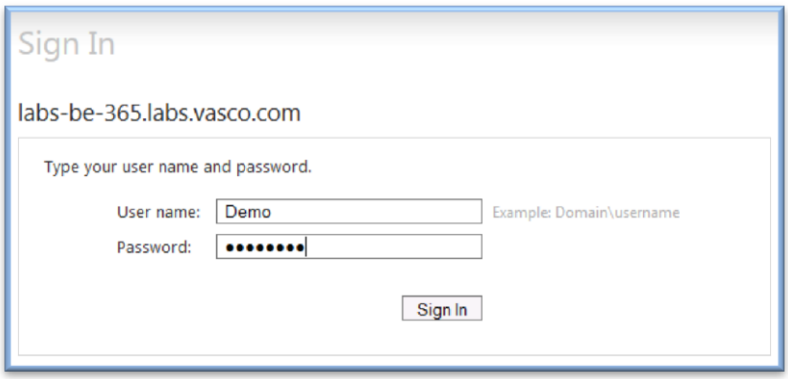
Now the IDENTIKEY Authentication Server can learn the password of users through a successful login. Your users' first login using a DIGIPASS should be in the following format: Static Password + One Time Password (example: User = Test; Password = Test123; OTP = 654123; First login: Username: Test; Password: Test123654123).

5 Test the setup

5.1 Response only

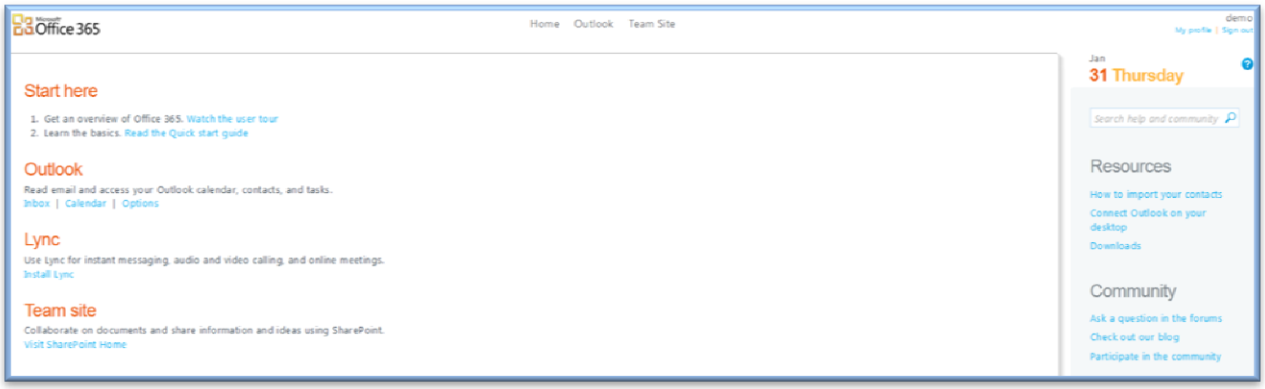
Open a browser and navigate to https://portal.microsoftonline.com. Enter your user@yourdomain and press tab. The password field will gray out and you will be asked to log in using your domain.

When clicking on the link **Sign in at <your-domain>**, you will be redirected to the logon form of your Active Directory Federation Service. Use your username and Active Directory credentials.



When you use password learning, your first login must contain your Active Directory password (password + OTP). Example: User = Test; Password = Test123; OTP = 654123; First login: Username: Test; Password: Test123654123.

Click **OK** and you will be logged into Office 365.



5.2 Backup virtual DIGIPASS

The DIGIPASS Authentication for OWA – Forms version 3.4.0 does not yet support backup virtual DIGIPASS and Office 365 login using Active Directory Federation Service.