

DIGIPASS Authentication for Imprivata

With VASCO VACMAN Controller integrated

Disclaimer

Disclaimer of Warranties and Limitations of Liabilities

This Report is provided on an 'as is' basis, without any other warranties, or conditions.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security.

Trademarks

DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Copyright

© 2007 VASCO Data Security. All rights reserved.

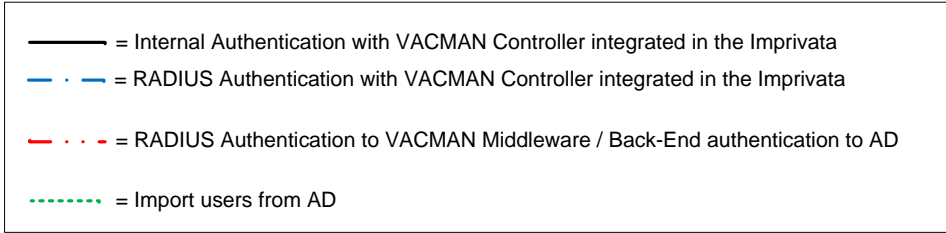
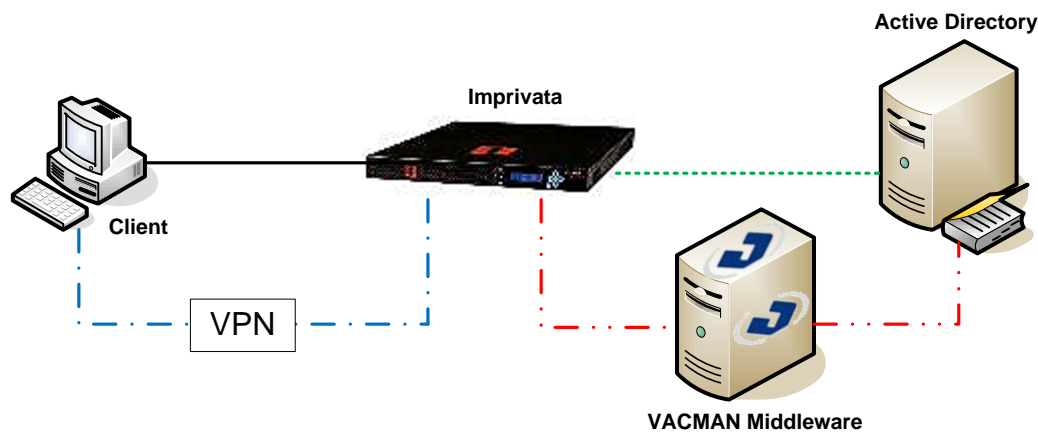
Table of Contents

DIGIPASS Authentication for Imprivata	1
Disclaimer	2
Table of Contents.....	3
1 Overview.....	4
2 Solution	4
2.1 LAN	4
2.2 RADIUS.....	4
2.3 ESSO	4
3 Imprivata configuration	5
3.1 Policies	6
3.2 DIGIPASS/DPX.....	8
3.3 User assignment	11
4 Imprivata test.....	13
4.1 LAN Logon.....	13
4.1.1 <i>Response Only</i>	13
4.1.2 <i>Challenge/Response</i>	14
4.1.3 <i>Static password</i>	15
4.2 Self-Assignment.....	16
4.3 PIN Unlocking	17
5 Features.....	19
5.1 Authentication Management	19
5.2 Single Sign-On.....	19
5.3 Physical Logical.....	19
6 About VASCO Data Security	20
7 About Imprivata.....	20

1 Overview

The purpose of this document is to demonstrate how to use an Imprivata appliance in combination with a DIGIPASS. We will show you how to import a DPX file and how to assign a DIGIPASS to a user.

2 Solution



2.1 LAN

The regular way of working with the Imprivata appliance is LAN authentication on a client computer. The Imprivata appliance has a VACMAN Controller integrated, so it can handle authentication requests on its own. It also has the possibility to synchronize it's user database with the Active Directory in your network.

2.2 RADIUS

The Imprivata appliance can act as a RADIUS client and server at the same time. Clients can request a RADIUS authentication to the Imprivata appliance or validate requests for instance coming from a VPN server. On the other hand, the Imprivata appliance can also act as a RADIUS proxy and transfer RADIUS requests to another RADIUS server.

2.3 ESSO

The Enterprise Single Sign-On (ESSO) feature enables users to use the already specified credentials to authenticate themselves to different kind of client activities. (Applications, websites, ...)

3 Imprivata configuration

Browse to the configuration page of the Imprivata appliance:
https://<Imprivata_ip_OR_hostname>. Through the **Imprivata OneSign Administrator** we are able to perform all required configuration changes.

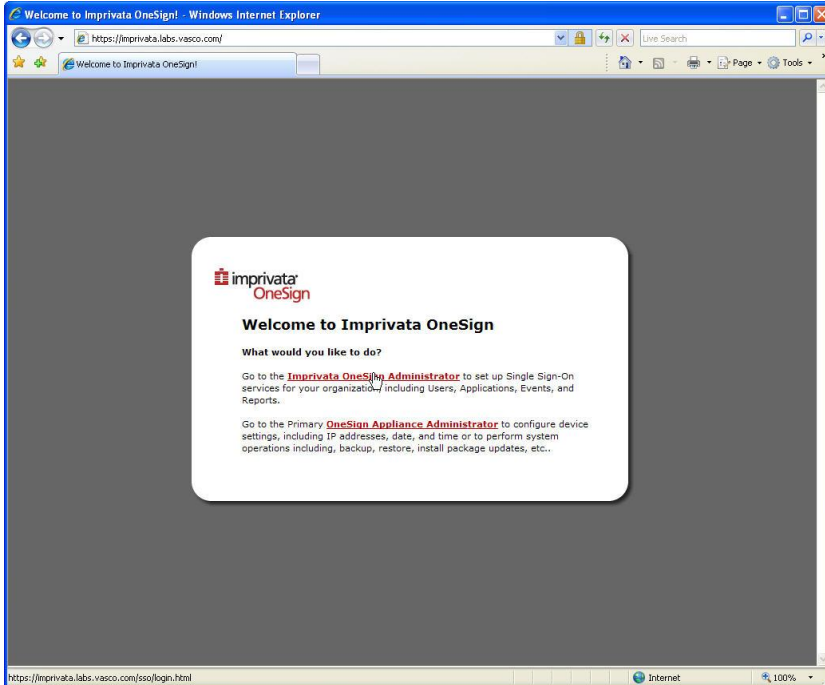


Figure 1: Imprivata configuration (1)

Use a **OneSign administrative user** to authenticate with the OneSign Administrator. These accounts were chosen when installing the OneSign application for the first time.

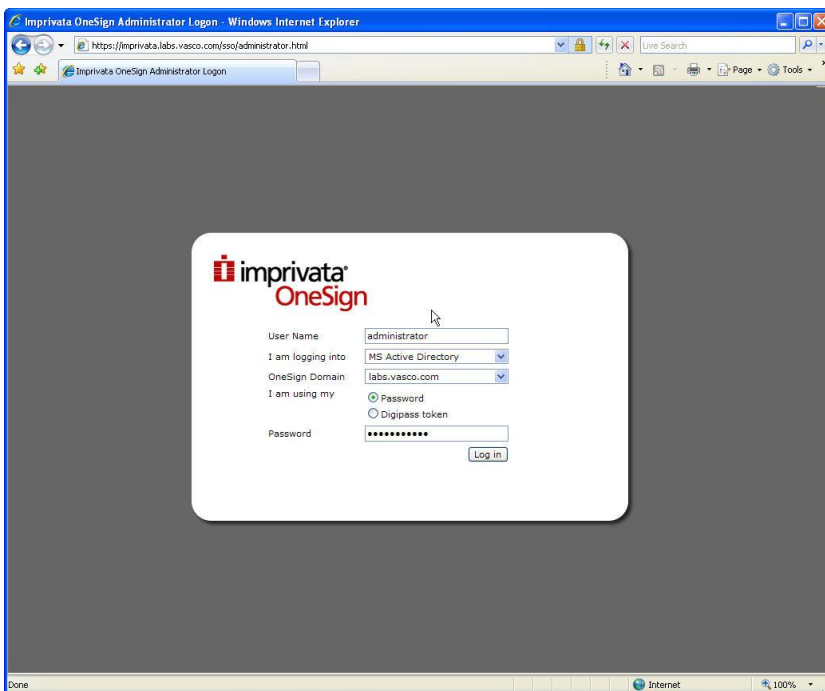


Figure 2 Imprivata configuration (2)

3.1 Policies

Add or Change a policy to allow only access to users who will use a DIGIPASS to authenticate.

Click the **Add** button to create a new policy, **or click a policy** to change the settings from an existing policy.

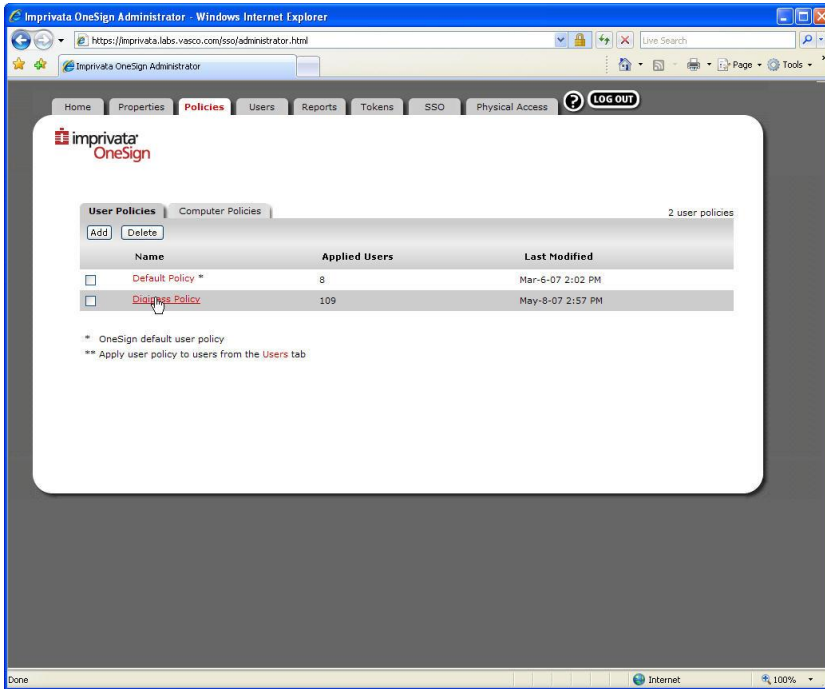


Figure 3: Policies (1)

The **Local Network Authentication Method** can be found under the authentication tab in the page. Make sure **only "Digipass token"** is selected here. You could, if preferred, enable the Emergency Access. This allows the users to answer some security questions and be granted access afterwards in case they forget or lost their DIGIPASS.

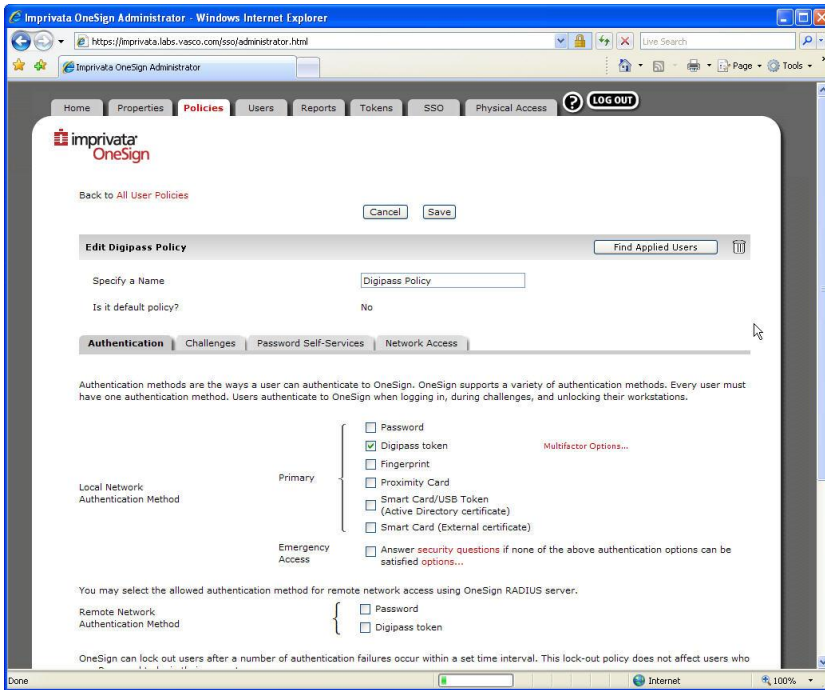


Figure 4: Policies (2)

At the bottom of the same page, you can find different lockout parameters when authentication has failed.

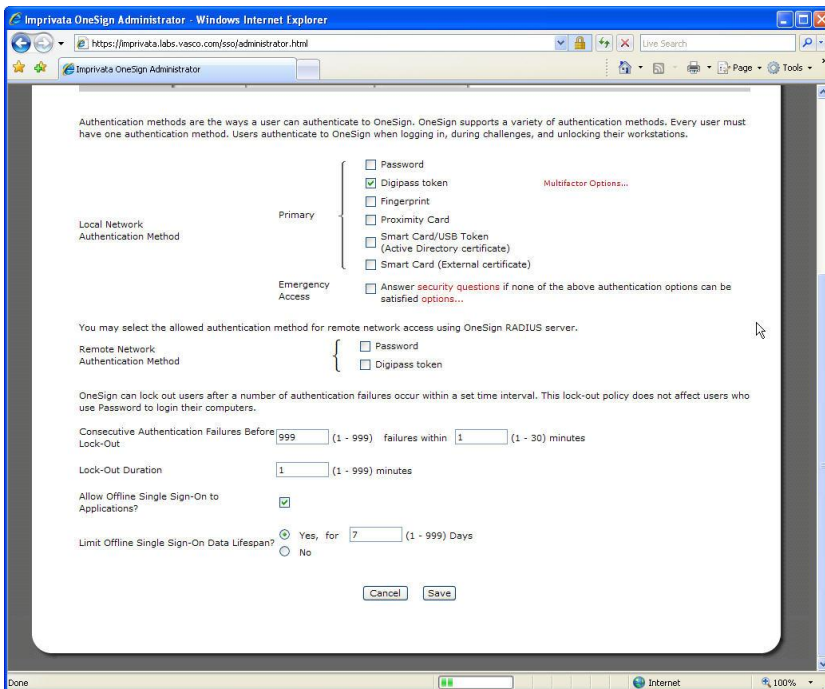


Figure 5: Policies (3)

3.2 DIGIPASS/DPX

In case you would like to use the internal validation method for the DIGIPASS, you will have to upload your DPX file and enter the transportation key. Using this method, you will eliminate the need to install an external DIGIPASS validation tool (VACMAN Controller, VACMAN Middleware,...).

To insert a DPX file on the Imprivata appliance, go to the **Tokens** tab and click the **Import** button.

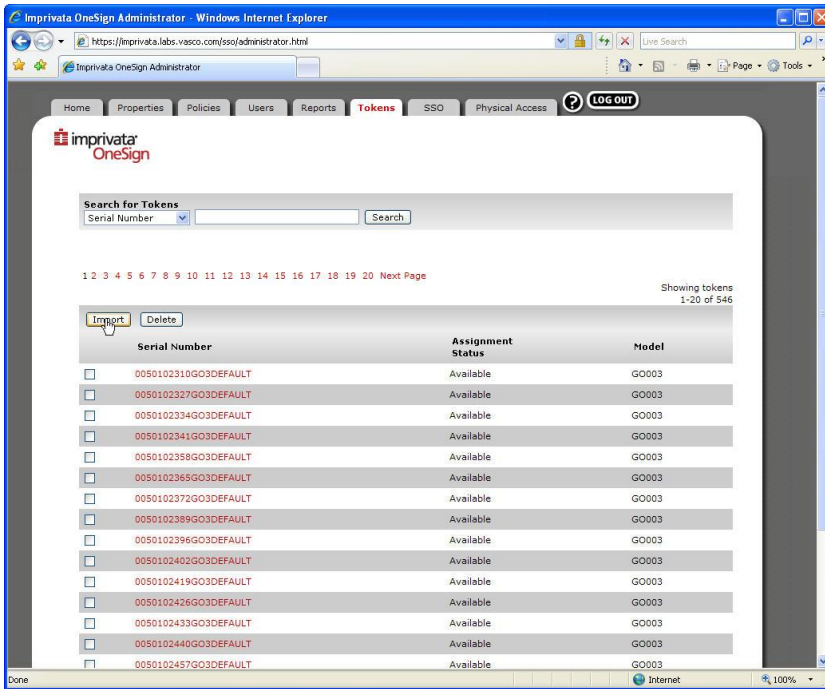


Figure 6: DIGIPASS/DPX (1)

Fill in the DPX transport key in the **shipping code** field. Select **Yes or No** if there is only one application in your DPX file. (If you don't know, select Yes, you will receive a message box with the values of more than one application is found.) Click **Browse** to select your DPX file and afterwards click **Upload**.

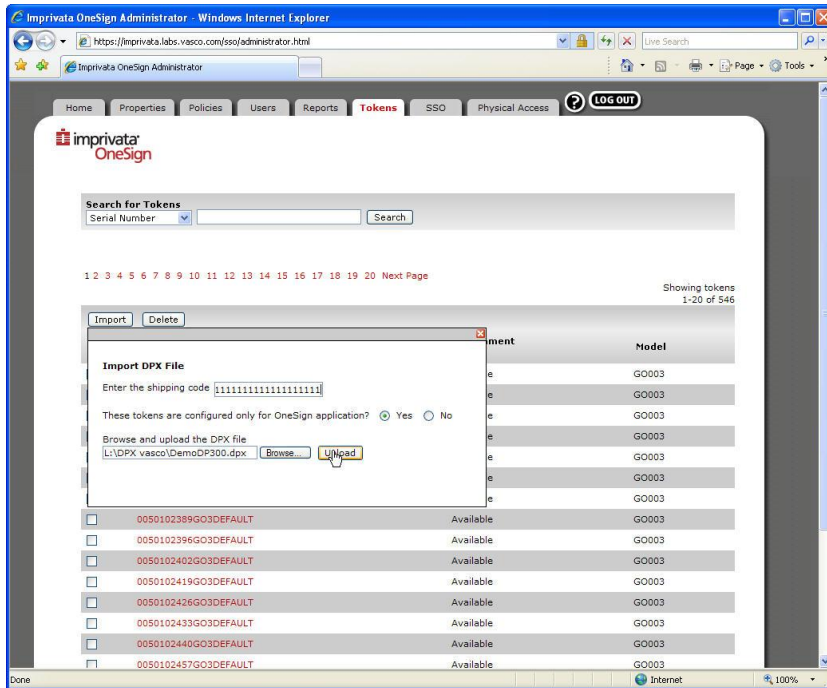


Figure 7: DIGIPASS/DPX (2)

The following message boxes show you what kind of errors you could receive. The first one is when you entered the wrong transport key or shipping code.



Figure 8: DIGIPASS/DPX (3)

The second one is when there is more than one application found in the DPX file while you selected YES in the previous step. In this box you can see the applications that it found, so you can easily choose the correct application to import.

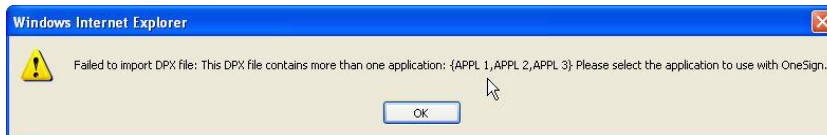


Figure 9: DIGIPASS/DPX (4)

When the DPX file is successfully imported, you will see how many DIGIPASS were added to database.

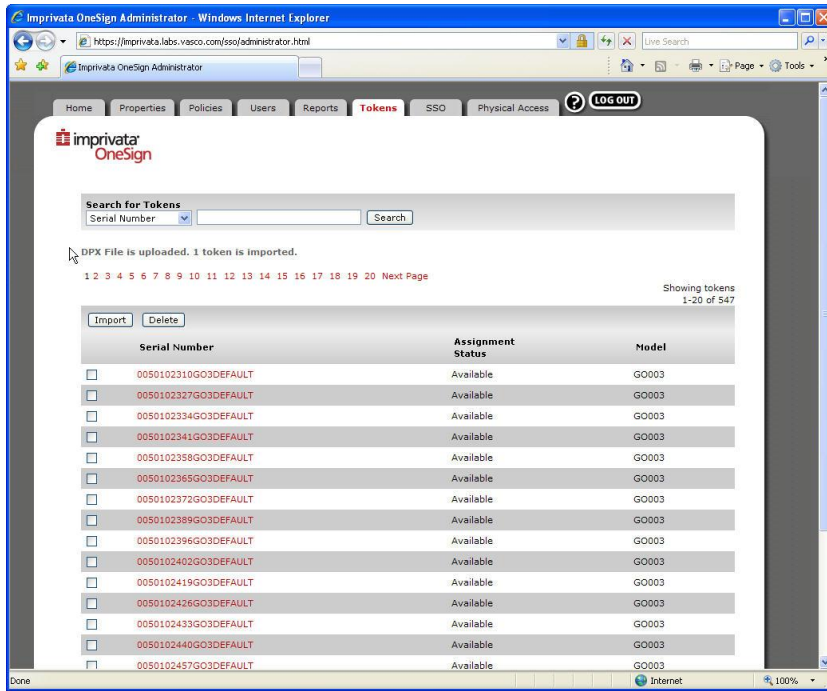


Figure 10: DIGIPASS/DPX (5)

3.3 User assignment

To assign a DIGIPASS to a user, you first have to select the desired DIGIPASS. Search for your desired DIGIPASS or select one from the list. **Click on the DIGIPASS Serial Number to see the details.**

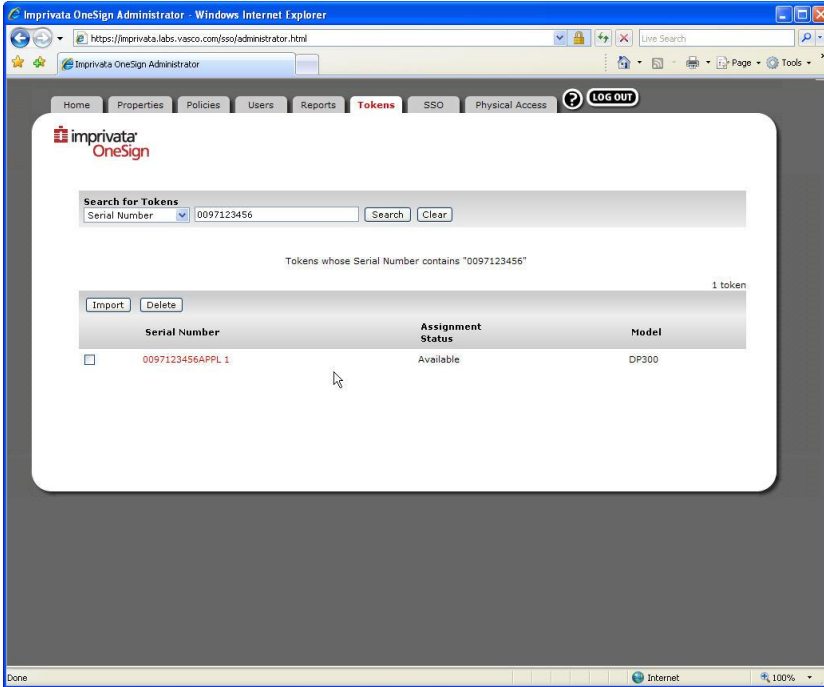


Figure 11: User assignment (1)

If the Assignment Status is Available, you can click the **Change Status** button. Here you select the **“Assign Token to User”** option. Fill in the **username** and select the correct **domain**. Click OK to save the changes.

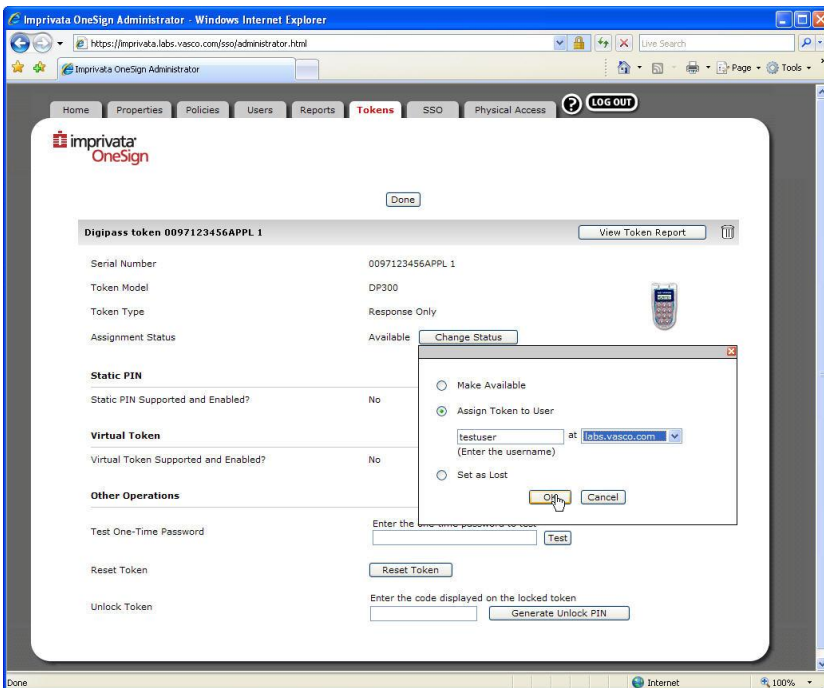


Figure 12: User assignment (2)

You will now see that the user is assigned to this DIGIPASS. To see if everything works correct, you can enter a **One Time Password (OTP)** in the bottom of the page in the Test One-Time Password field and click the **Test** button.

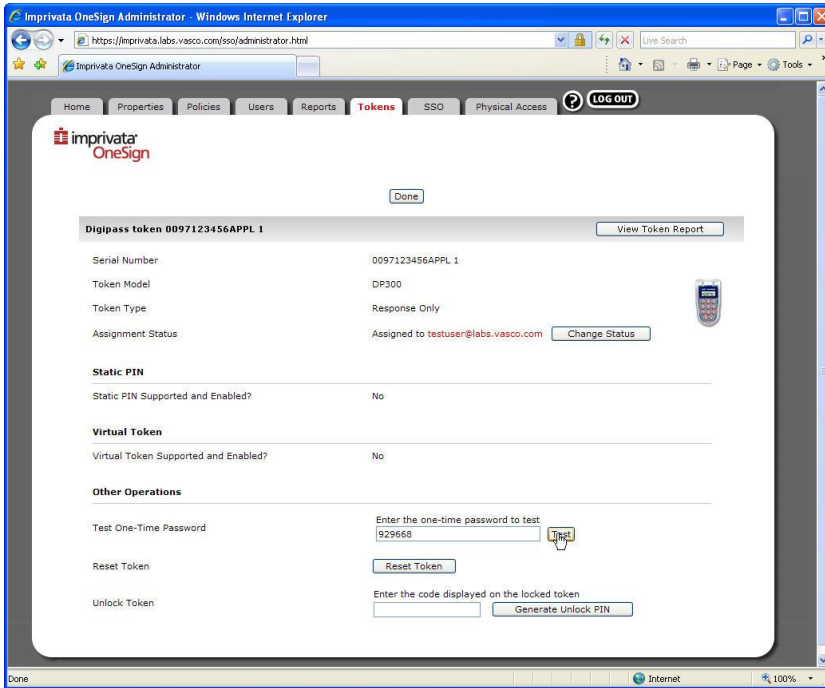


Figure 13: User assignment (3)

You will receive a successful test message if the OTP is validated correctly for this DIGIPASS.



Figure 14: User assignment (4)

4 Imprivata test

4.1 LAN Logon

4.1.1 Response Only

Once the Imprivata software is installed on the client machine, you will see an extra option field in the logon screen of the client.

The **Username** and **Domain** remain unchanged and have to be filled in like before. Only if you select the **ID Token** option in the OneSign Logon field, the password field will change to **Passcode** . Here you have to fill in a One Time Password (OTP) generated by the DIGIPASS assigned to your username.



Figure 15: LAN Logon – Response Only

You will be granted access to your client when the OTP is validated on the Imprivata appliance.

4.1.2 Challenge/Response

When you want to make use of a challenge/response DIGIPASS, you enter your credentials like before. This means, enter your **Username**, **Password** and **Domain**. Make sure you selected **ID Token** in the OneSign Logon box.



Figure 16: LAN Logon – Challenge/Response (1)

Afterwards, you will be shown a **Challenge code**, which you will have to enter on your DIGIPASS (with numeric keypad) to calculate the **Response** code.



Figure 17: LAN Logon – Challenge/Response (2)

You will be granted access to your client once the Response code is validated on the Imprivata appliance.

4.1.3 Static password

Once your DIGIPASS is assigned to your account, you can no longer use your static password to get access to your client.



Figure 18: Static password (1)

If you try, you will receive the following alert message.



Figure 19: Static password (2)

4.2 Self-Assignment

Once the Imprivata software is installed on a client machine, you will be prompted to specify your "Digipass token serial" as long as there is no DIGIPASS assigned to the user that was logged on to Windows.

To self-assign a DIGIPASS, enter the **DIGIPASS token serial**, which you can find on the back of the DIGIPASS. Generate an OTP with the same DIGIPASS and enter it in the **Passcode** field. By doing this, the software instantly knows if the correct DIGIPASS was specified by the user.

The next time you logon with this username, you will have to use your DIGIPASS.



Figure 20: Self-Assignment

4.3 PIN Unlocking

In the DIGIPASS family there exist some models with a numeric keypad. These models may be protected with a user PIN. After entering 3 wrong user PIN's, the DIGIPASS will be locked. If a DIGIPASS gets locked, there will appear an unlock code on the screen.

The Imprivata appliance has a built-in function to unlock a DIGIPASS. Go to the details of that specific DIGIPASS. At the bottom of the page, you will find an unlock function for a locked DIGIPASS.

Enter the **code** that is shown on the **screen of the locked DIGIPASS** and click the **Generate Unlock PIN** button.

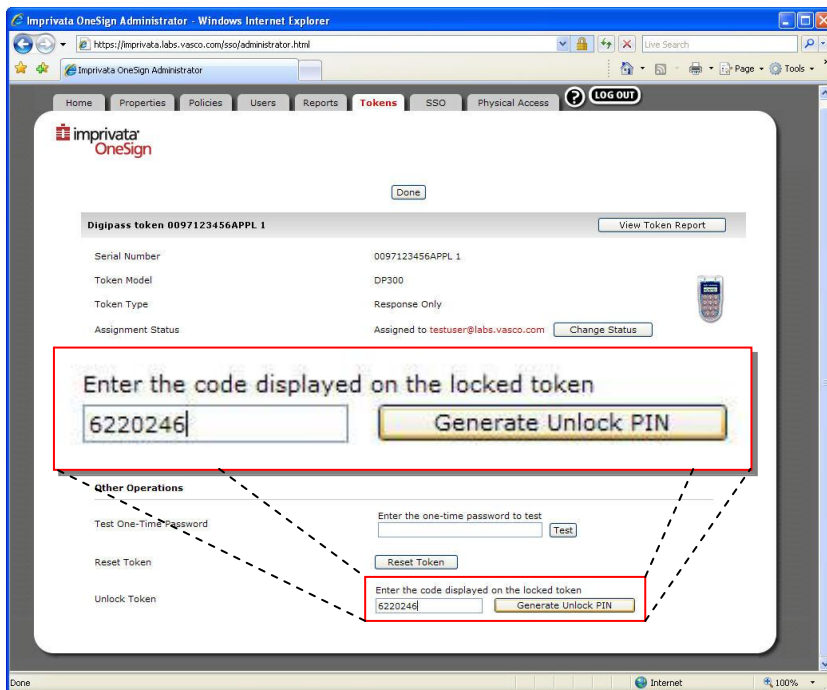


Figure 21: PIN Unlocking (1)

You unlock the DIGIPASS by entering the unlock PIN on your DIGIPASS. The user is then allowed to choose a new PIN code, which has to be confirmed by entering the PIN a second time.

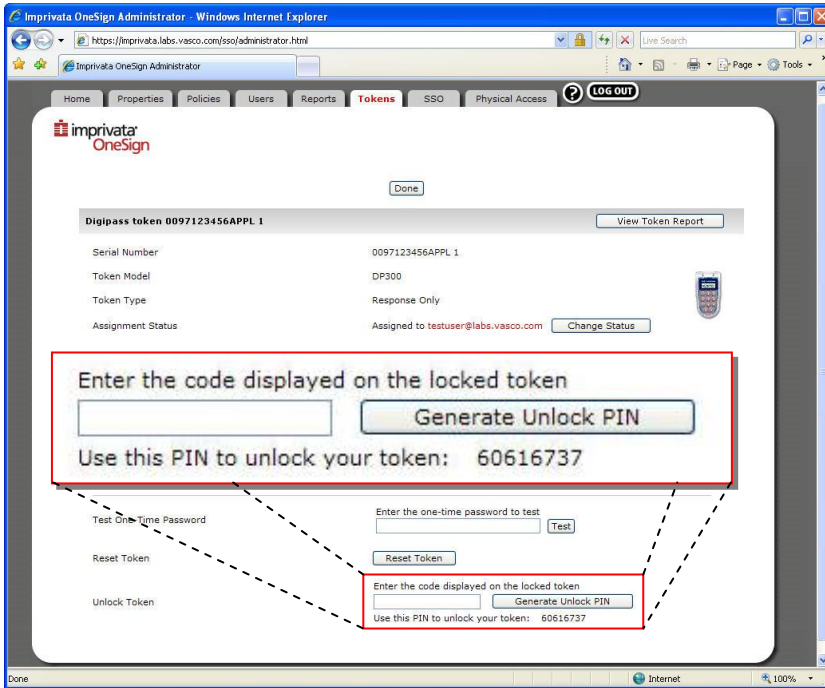


Figure 22: PIN Unlocking (2)

5 Features

5.1 Authentication Management

- Appliance-based
- Easy to Use, Easy to Manage
- Tightly Integrated Two-Factor Authentication
- Upgrade to Single Sign-On and/or Physical | Logical

5.2 Single Sign-On

- Automate Application Password Changes
- Self-Service Password Management
- Broad Support for Strong Authentication
- Application Profile Generator™ (APG)
- Point-and-Click instead of expensive scripting
- Monitoring and Reporting
- Provisioning Support
- OneSign Extension Objects
- Roaming Desktops, Drive-Mapping, and More

5.3 Physical & Logical Access

Maps identities between physical access systems and IT directories to enable one converged policy for allowing or denying network access based on a user's:

- *Physical location, organizational role, and/or employee status*
- *Includes both local and remote network access*

Provides integrated and centralized user access monitoring and reporting in order to better demonstrate regulatory compliance

- *Who is accessing what, from where and when?*

Enables a single point for *Instant User Lockout* from access to both buildings and IT networks

- *Eliminates latency between badge revocation and IT de-provisioning*

Non-intrusive, interoperable with companies' existing physical access system infrastructure

- *Maximizes existing security investments*
- *Building access card agnostic, works with all current and future card types*

6 About Imprivata

Today, the Imprivata OneSign platform offers distinct license modules to address specific enterprise needs:

The power of Imprivata OneSign is that it's **ALL** in the box. Regardless of your initial start point, you can seamlessly enable additional capabilities as your needs evolve - all with a simple license key.

Imprivata OneSign is shipped as a hardware appliance pair - there is nothing else to buy, install or maintain. OneSign's scalable web service-based architecture and built-in failover for system reliability gets you up and running quickly and easily, without the complexity and costs associated with buying, implementing, and managing independent and non-integrated alternatives.

Imprivata continues to deliver on its vision of delivering breakthrough appliance-based authentication and access management solutions that provide out-of-the-box functionality and ease-of-use to our customers and partners worldwide.

More information: www.imprivata.com

7 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO's User Authentication software is carried by the end user on its DIGIPASS products which are small "calculator" hardware devices, or in a software format on mobile phones, other portable devices, and PC's.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO's target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO's time-based system generates a "one-time" password that changes with every use, and is virtually impossible to hack or break.

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO's user authentication software is delivered via its DIGIPASS hardware and software security products. With over 25 million DIGIPASS products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 500 international financial institutions and almost 3000 blue-chip corporations and governments located in more than 100 countries.