SECURE APPLICATION LOGIN SERVICE ACCESS (SALSA)

END USER GUIDE

Version 1.7

14 June 2019

SITA

Create success. Together

1. INTRODUCTION 3

2. SECURE AUTHENTICATION END USER RULES 3

3. SALSA SOFTWARE AND TOOLS 4

A. Connectivity Software 4
B. Token Software tools 4
C. Self-Service Portal 4

4. USING SALSA 5

D. Start a connection 5
E. Stop a connection 8
F. Change your PIN Code after expiration (90 days) 9

5. FREQUENTLY ASKED QUESTIONS (FAQs) 10

G. What if I forget my PIN Code? 10
H. What if my Token is locked? 10
I. How long will my Token continue to operate? 10
J. What is the Idle Session Timeout? 10
K. What should I do if I can't logon using my Token? 10
L. How do I authenticate with my Token for self-service portal? 11
M. How do I change my PIN Code? 15
N. How do I resynchronize my Token? 16
O. How do I rename my Token? 18
P. How do I retrieve the "Token" application version? 18
Q. How do I retrieve my Token serial? 19
R. How do I remove my Token? 20
S. How do I remove completely SALSA? 21

1. INTRODUCTION

Thank you for choosing SALSA to get secured access to your applications.

This guide is intended for SALSA end-users and is valid for:

OS	Version
Windows	10 (32-bit & 64-bit) 8.1 (32-bit & 64-bit) 8 (32-bit & 64-bit) 7 (32-bit & 64-bit)
Mac	OSX v10.8 (Mountain Lion) or higher

The screenshots and details are based on Windows 10.
Some screenshots may vary using different version of Windows.

2. SECURE AUTHENTICATION END USER RULES

These rules apply to your use of the SALSA Token, and your secret Personal Identification Number (your PIN).

You should use your PIN and the Token software to identify yourself before accessing SITA applications.

- Your PIN must remain secret to you at all times. No other person ever needs to know this PIN and you should not disclose it to anyone. This includes your colleagues and systems administrators at your company and personnel who are, or claim to be representatives of SITA or a Partner of SITA. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code. You should be extremely suspicious of anyone who ever tells you at they need to know your PIN, and you should report any such incident to your Administrator or your usual help desk immediately.
- The privacy of your Token and the confidentiality of your PIN are crucial to the verification of your on-line identity and the security of your information and the networked system(s) that may be accessed using your identity. If you believe that the confidentiality of your Token or your PIN has been compromised in any way or that somebody is trying to use your on-line identity on your behalf (e.g. account locked when you did not try to login), you should report these incidents immediately to your Administrator or your usual help desk.

Important note: SALSA will require you to change your PIN Code **every 90 days**.

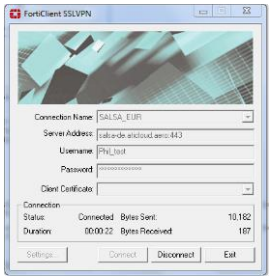
Please make sure you enter a new PIN Code as described in section F**. Change your PIN Code after expiration (90 days)**

PIN Code: Your PIN Code has to be **4 digits** long.
(example: 1234)

3. SALSA SOFTWARE AND TOOLS

A. Connectivity Software

FortiClient SSL VPN client software is used to establish a secured connection to the applications you want to use



B. Token Software tools

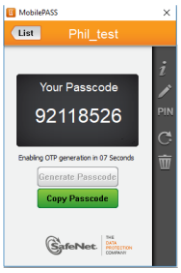
Software tools are a set of applications installed on your Windows PC as part of the SALSA pack and allow you to activate and manage your SALSA Token(s).

“Token” and “Token Manager” applications are part of these Software Tools.

The “Token” application is used to generate a Token Code required each time you need to establish a secured connection with FortiClient SSL VPN client software.

It also allows to:

- Select a Token when several are installed
- Rename a Token
- Resynchronize a Token
- Retrieve the version of the “Token” application



The “Token Manager” application is used for the administration of your token(s) and allows you to:

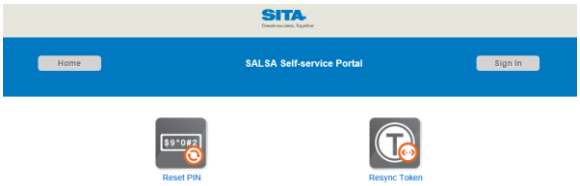
- Select a Token when several are installed
- Retrieve the serial number of a Token
- Remove a Token from your Windows PC

Note: Administrator rights are required to run the “Token Manager” application

C. Self-Service Portal

The self-service portal is dedicated web portal which allow you (in association with “Token” application) to:

- Reset your PIN
- Resync your PIN

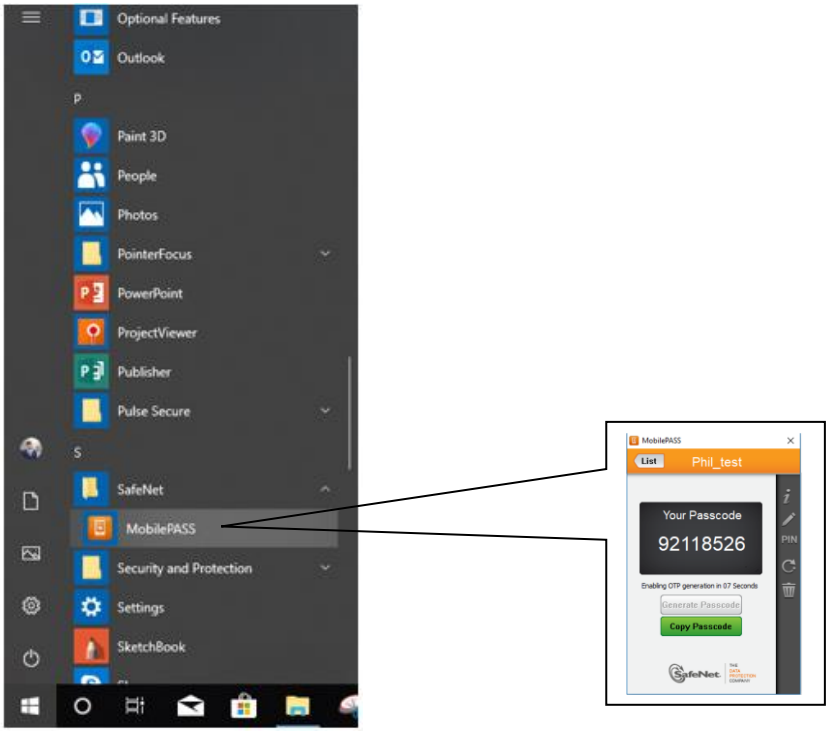


Self-service portal is available at:
https://ss.safenet-inc.com/blackshieldss/O/BVYSSIVWXI/index.aspx

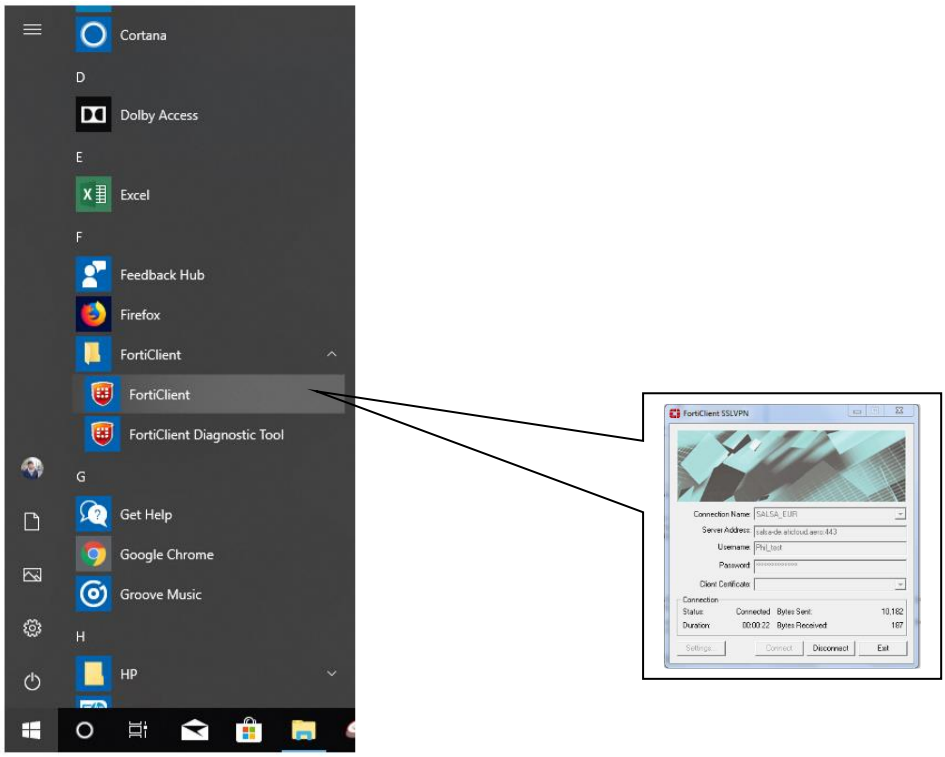
4. USING SALSA

D. Start a connection

Launch the Token application:
within the Windows taskbar, select “Start”, “All Programs”, “SafeNet”, “MobilePASS”.



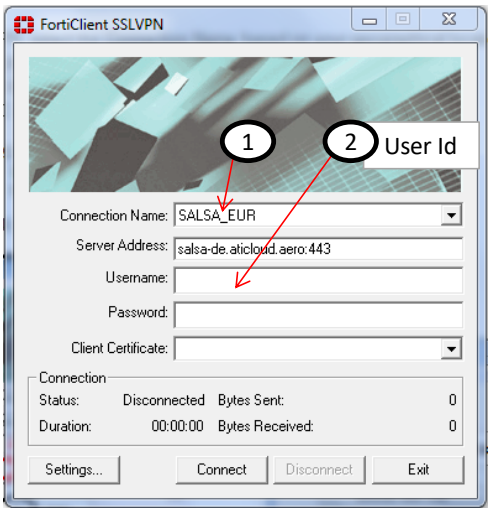
Launch FortiClient SSLVPN software:
within the Windows taskbar, select “Start”, “All Programs”, “FortiClient”, “FortiClient”.



On “FortiClient SSL VPN” window, select the Connection Name (1) based on your geographical location:

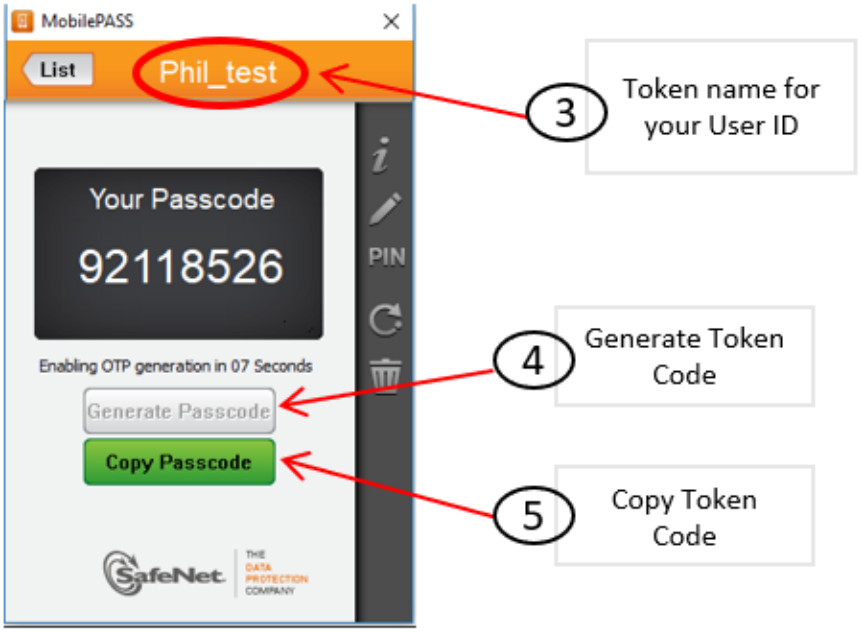
- **SALSA-EUR** if you are in Europe, Middle East or Africa
- **SALSA-NAM** if you are in the Americas
- **SALSA-APAC** if you are in Asia or Pacific region

Enter in Username (2) your **User Id** - as given initially for your Token



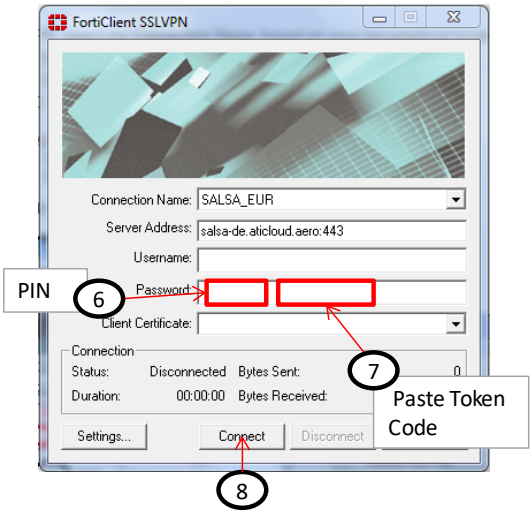
Go to “Token” window, and in Token (3) select the Token name associated to your User Id
(by default it is the same as your User Id)

Generate a new Token Code (4) and copy it (5)



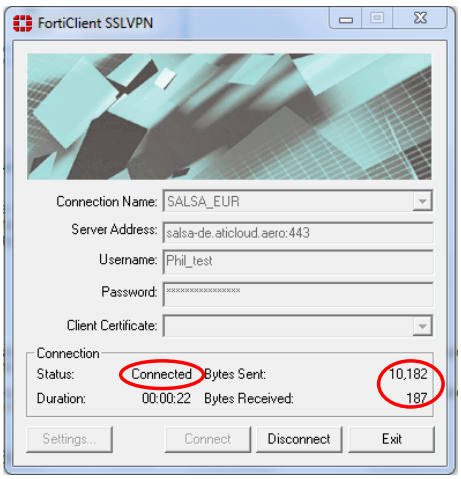
Go back to the “FortiClient SSL VPN” window, enter your PIN (6)
and paste (right click + Paste) the Token Code (7)

Press **Connect** (8)



Check that the connection is active:

- The status displayed is “**Connected**”
- The Bytes Sent and Received counters show increasing values



You have established a secured connection.

You can now access the SITA application(s) through the related client:

SITA Smart Front End Basic (SFEB)
SITA Reservations Desktop (SRDT)
Horizon Weight and Balance

Please refer to the corresponding installation guide if the client/application is not yet installed on your PC.

E. Stop a connection

The connection is stopped under the following conditions:

- “Log off” from Windows session
- “Shut down” from Windows
- “Restart” from Windows
- Manual disconnection (from FortiClient SSLVPN)

Important note: “Switch User” from Windows will **not stop the connection**.

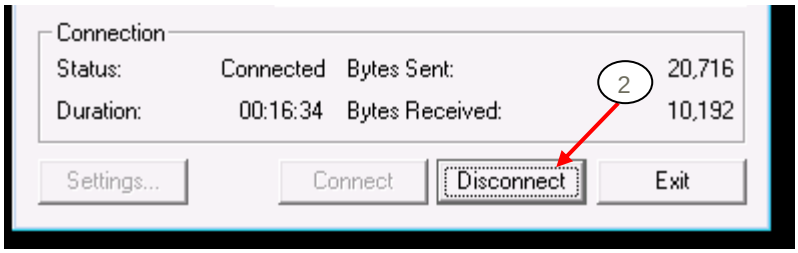
It is recommended in this case to manually disconnect the connection, as described below, before switching user if you do not want the connection to be available for the other user.

Manual disconnection (from FortiClient SSLVPN):

To manually perform a disconnection:

- Reopen FortiClient SSLVPN by clicking on the icon (1)
- Click on “Disconnect” (2)

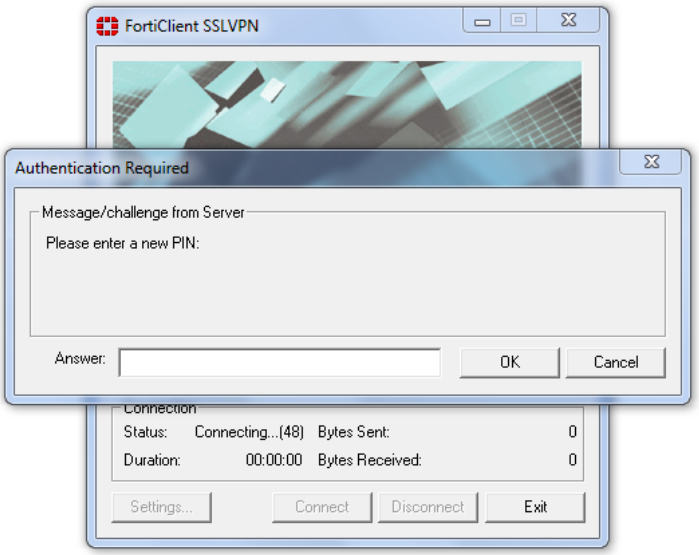
  or “Exit” (Exit will disconnect and close the SSL-VPN client software)



F. Change your PIN Code after expiration (90 days)

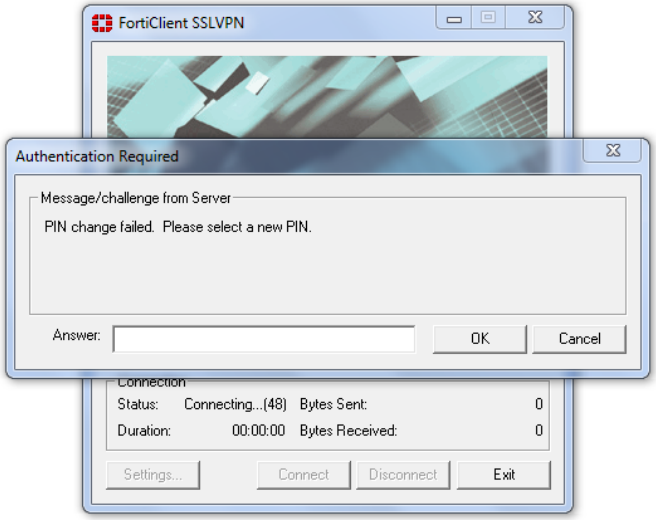
Every 90 days your PIN Code will expire and you will be requested to change it.

When trying to connect using the Forticlient SSLVPN, and after the PIN Code expiration (90 days), you will be prompted to enter a new PIN:



Enter a new PIN Code
has to be **4 digits** long
(example: 1234)

If the PIN Code is not in the correct format or if you enter the previous PIN Code without changing it, you will see an error message as per below and you will have to enter a new PIN:



After the change of your PIN code you can use it to start a SALSA connection as described in section D

5. FREQUENTLY ASKED QUESTIONS (FAQS)

G. What if I forget my PIN Code?

Contact your administrator or your usual help desk. Upon verifying your identity they will be able to request a reset of your PIN Code or you can use the Self-Service Portal Password via email option.

H. What if my Token is locked?

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock.
If Not contact your administrator or your usual help desk. Upon verifying your identity they will be able to request your Token to be unlocked and/or resolve logon problems.

I. How long will my Token continue to operate?

Your Token does not have any expiry date. It will be available to you to generate Token Codes until it is revoked under administrator's decision.

J. What is the Idle Session Timeout?

Session timeout represents an event occurring when a user does not perform any actions or continuously inactive for 15 minutes and it prevents users from leaving application open when they away from their workstation. In case of session timeout, user should stat connection again.

K. What should I do if I can't logon using my Token?

The most common cause of failed logon is entering an incorrect Token Code or an incorrect PIN.
Generate a new Token Code each time you establish a new connection and never attempt to reuse a Token Code from a previous connection.
Ensure that you enter the Token Code exactly as displayed on the Token application.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your administrator or your usual help desk to resolve logon problems.

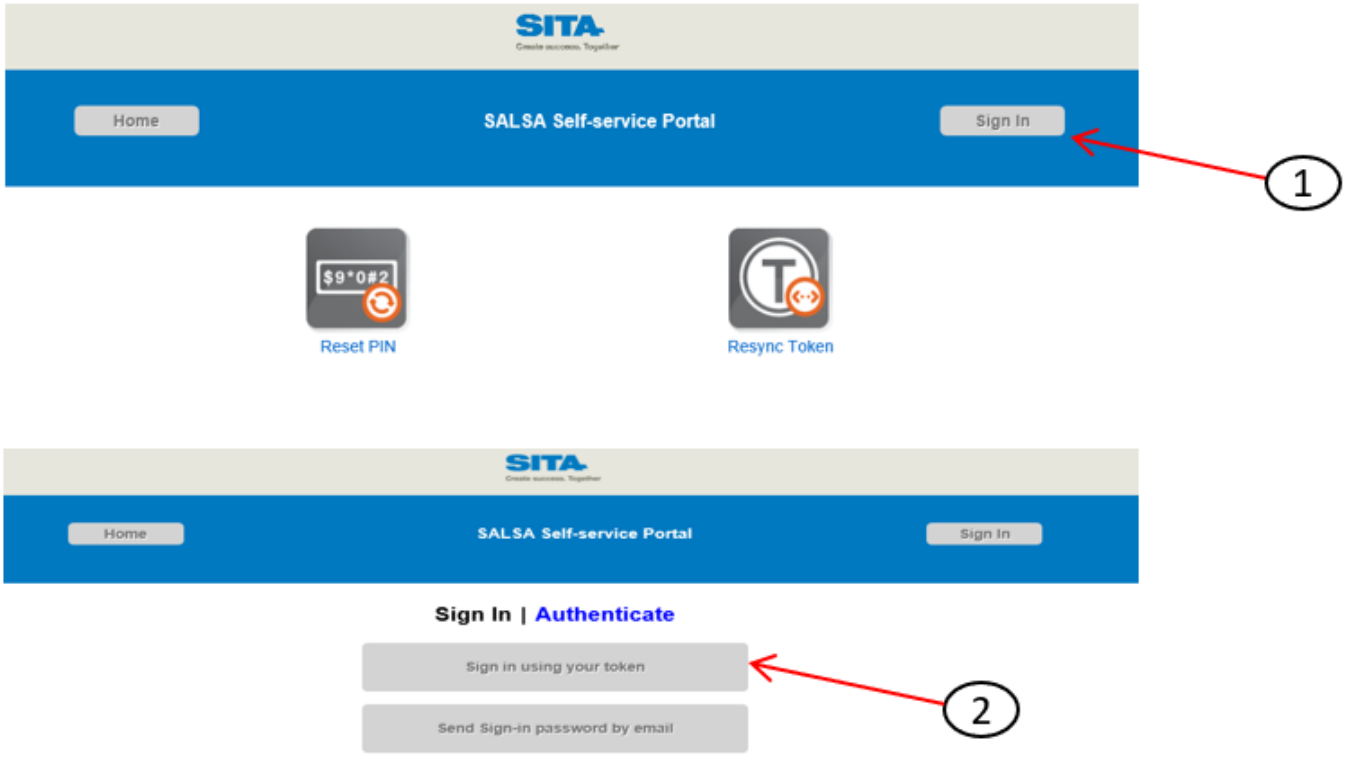
L. How do I authenticate with my Token for self-service portal?

You have the ability to test authentication with your Token thanks to the self-service portal.

If you received a “self-enrolment” message, the link is included in the message.
Otherwise you go to:
https://ss.safenet-inc.com/blackshieldss/O/BVYSSIVWXI/index.aspx

Option 1. Sing in using your token

In the self-service portal “Home” page click on “Sign In” (1)
and click on “Sign in using your Token”(2) on the next page.

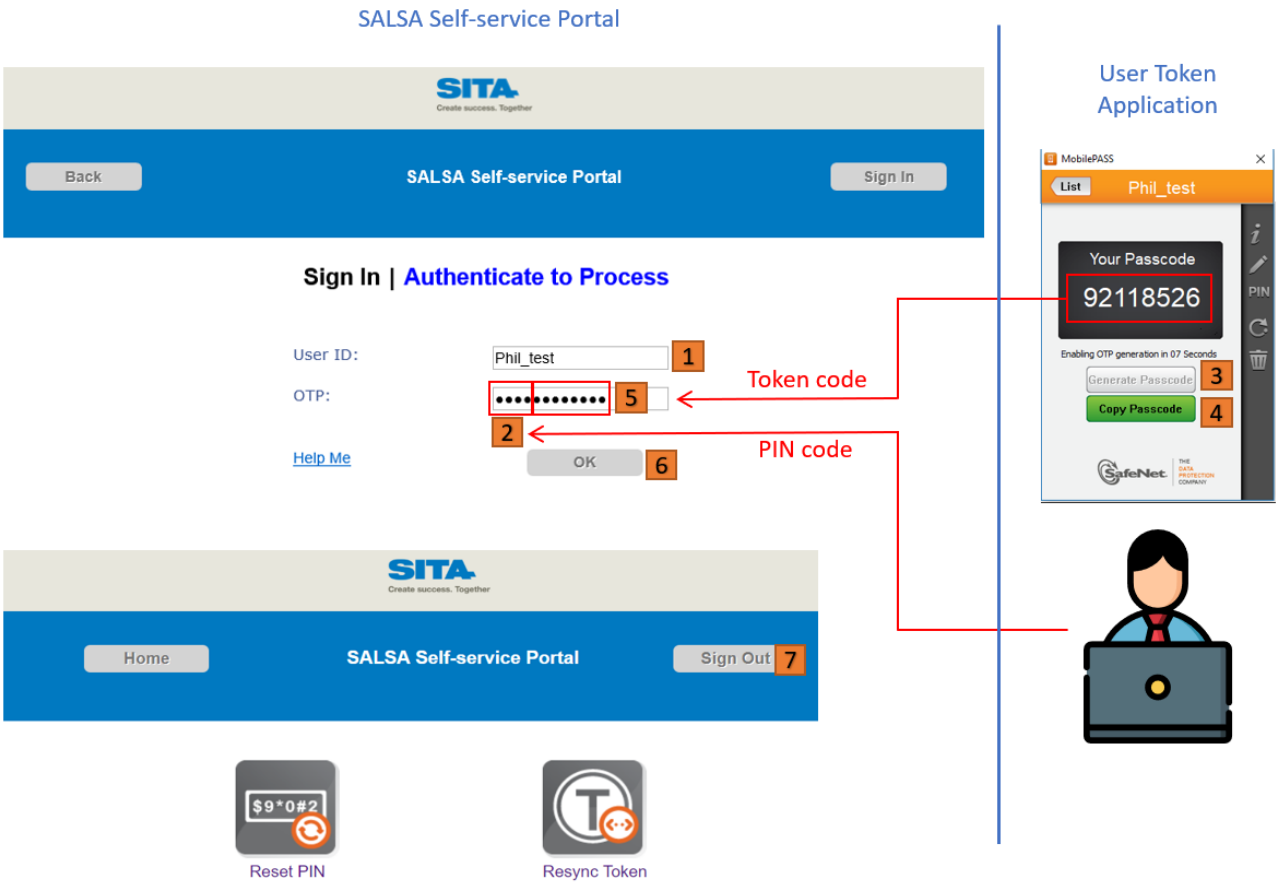


In the next page enter your user ID in the “User ID” field (1)
and your PIN Code in the “OTP” field (2) .

Go to the “Token” application, and click on “Generate Token Code” (3),
and “Copy” the Token Code (4).

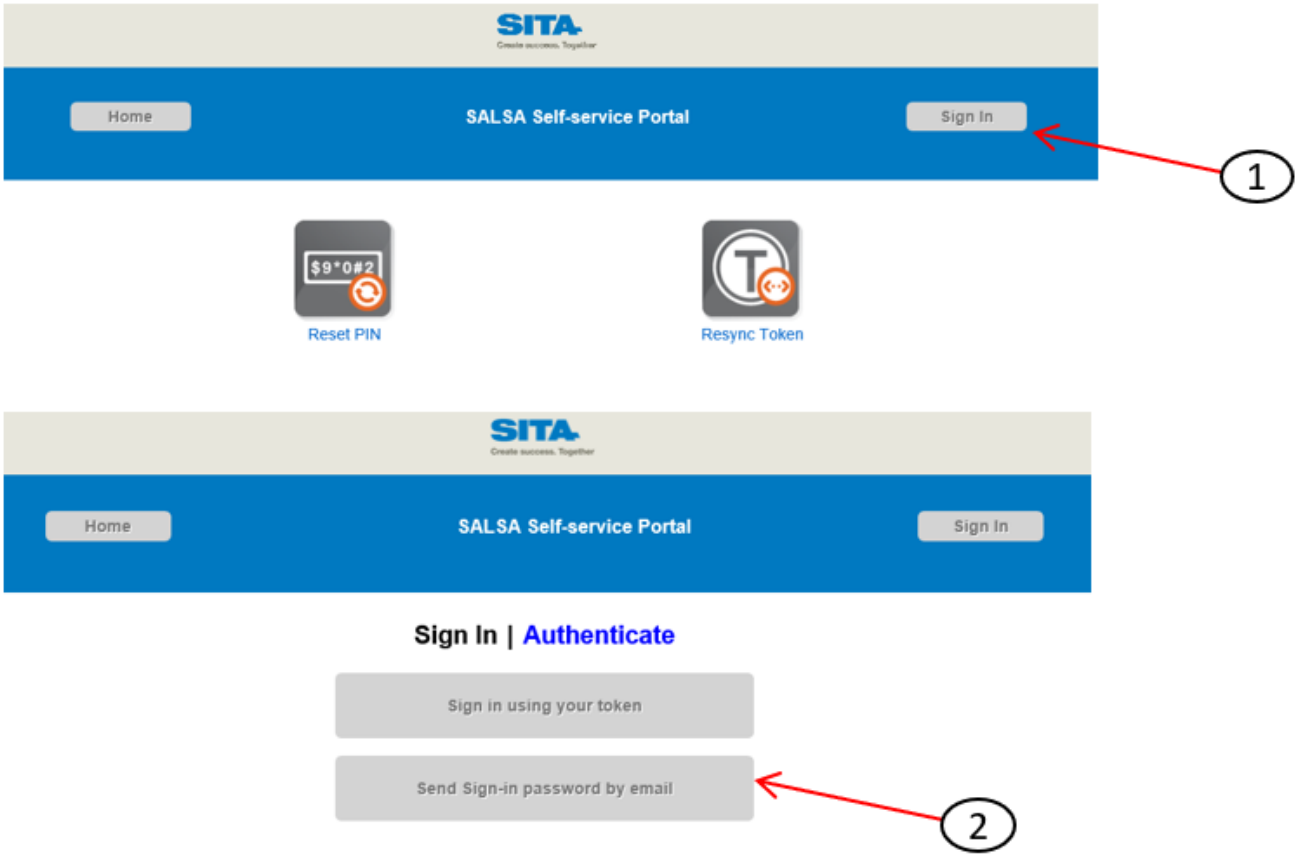
Go back to the self-service portal, and paste the Token Code value next to the PIN Code in the “OTP” field (5),
click on “OK” (6)

The “Sign Out” button (7) displayed within the “Home” page indicates that your authentication is successful.

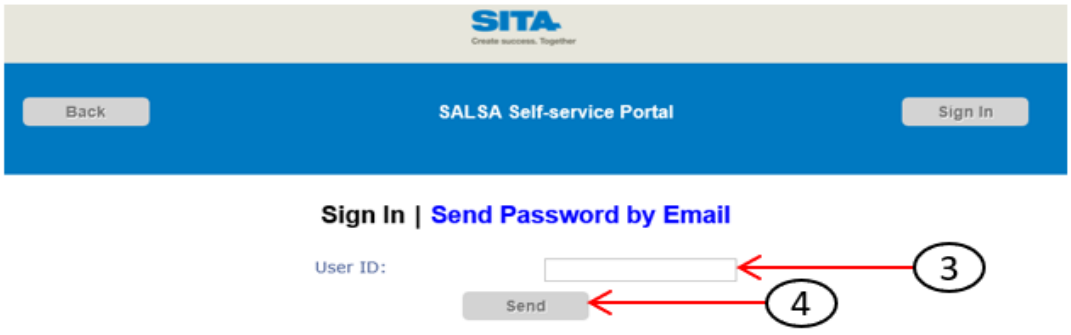


Option 2. Send Sign in password by email

In the self-service portal "Home" page click on "Sign In" (1)
and click on "Send Sign-in password by email" (2) on the next page.



This feature will send a Password to the email address of the User ID entered and this password can be used within 10 minutes to enter the self-service portal.



After the Password being received on the email, repeat the same steps on **Sign in Using your Token** section and use the Password received on the email.

M. How do I change my PIN Code?

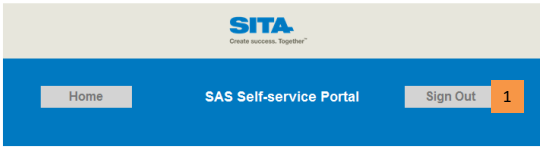
Within the self-service portal “Home” page,

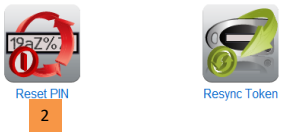
once authenticated - “Sign Out” button must be displayed (1),

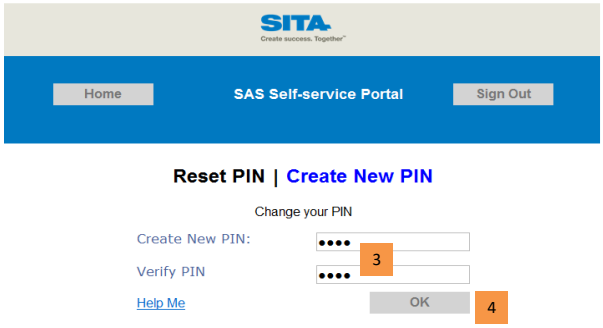
click on “Reset PIN”(2)

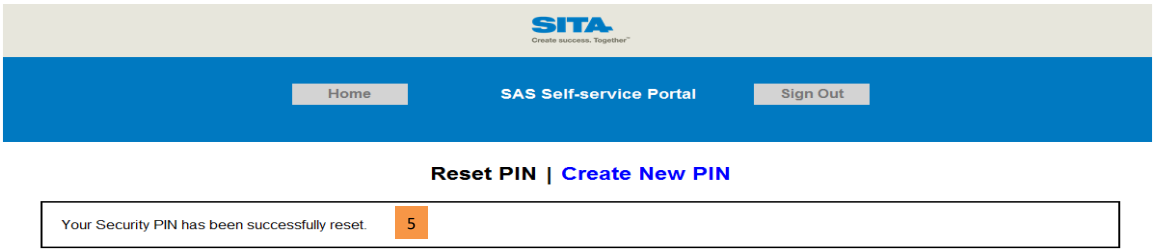
In the next page choose a new PIN Code and enter it in the “Create New PIN” and “Verify PIN” fields (3), then click on “OK” (4)

In the next page a message should indicate that your PIN Code change is successful (5).









N. How do I resynchronize my Token?

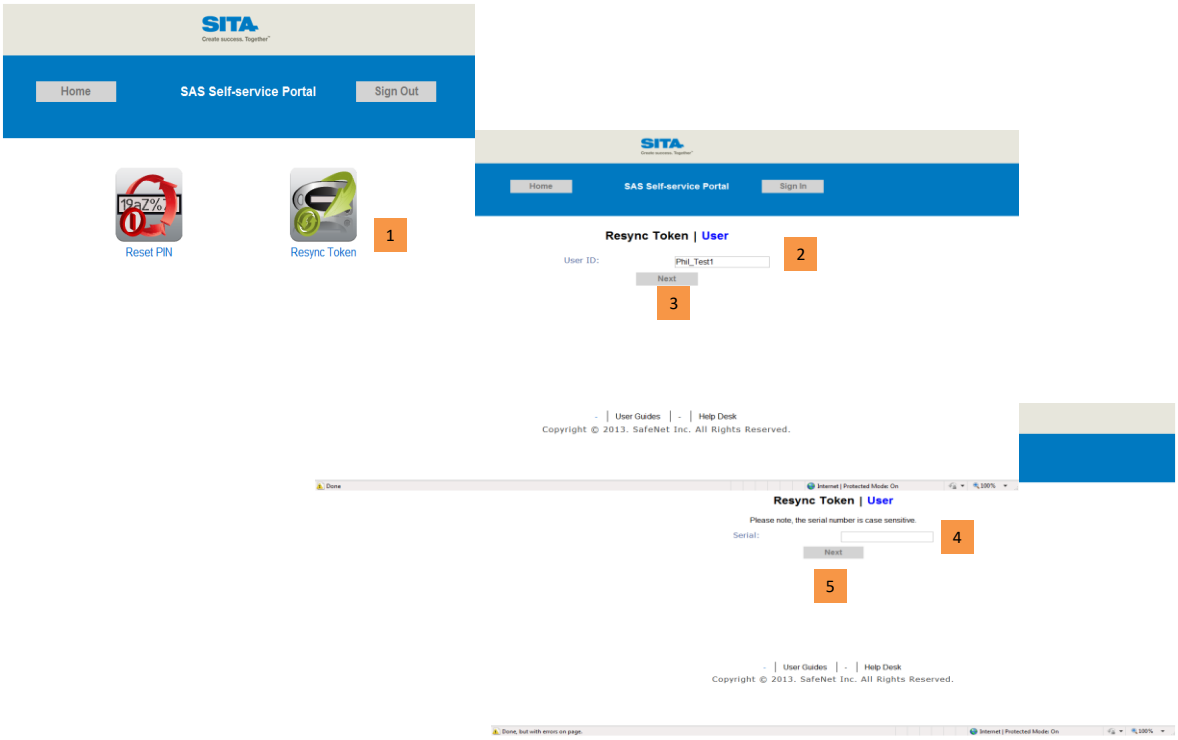
The resynchronization of your Token should never be required, but in case you have to resynchronize it, please follow the steps below:

In the self-service portal “Home” page,
click on “Resync Token” (1)

In the next page enter your user ID in the “User ID” field (2),
and click on “Next” (3)

Enter the serial of your Token in the “Serial” field (4),
then click on “Next” (5).

Serial of your Token can be found in section Q**. How do I retrieve my Token serial?**



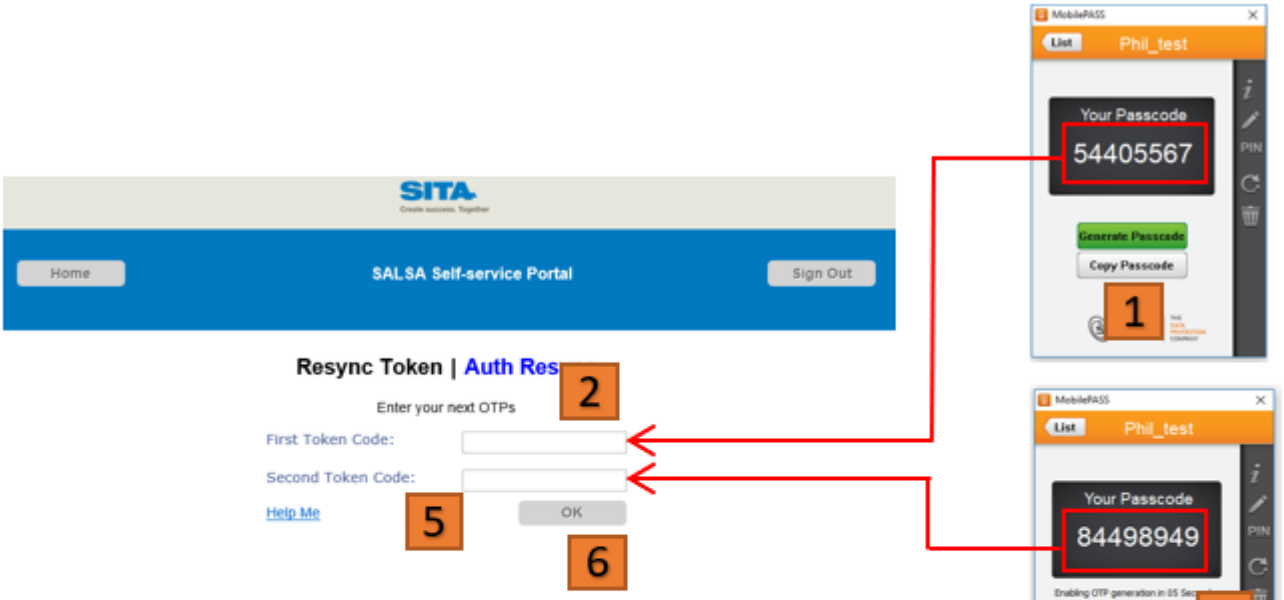
Then proceed as follows:

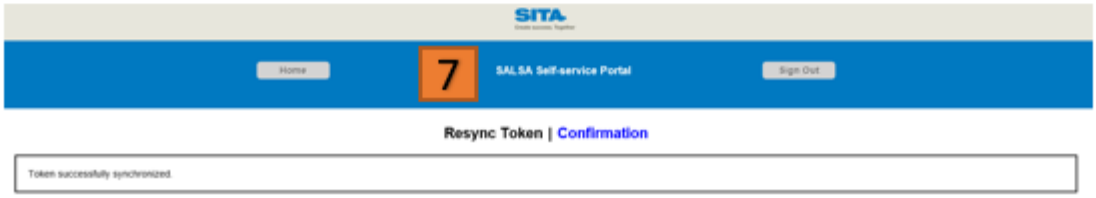
In the self-service portal “Auth Resync” page enter your next OTPs as per below:

Go to your “Token” application, “Copy” the Token Code (1)
then “Paste” (2) to “First Token Code” section.

Go back to “Token” application again and click “Generate Passcode” (3) and click “Copy” (4)
then “Paste” (5) to “Second Token Code” section
Click on “OK” (6)

In the “Confirmation” page a message indicates that your Token resynchronization is successful (7).





O. How do I rename my Token?

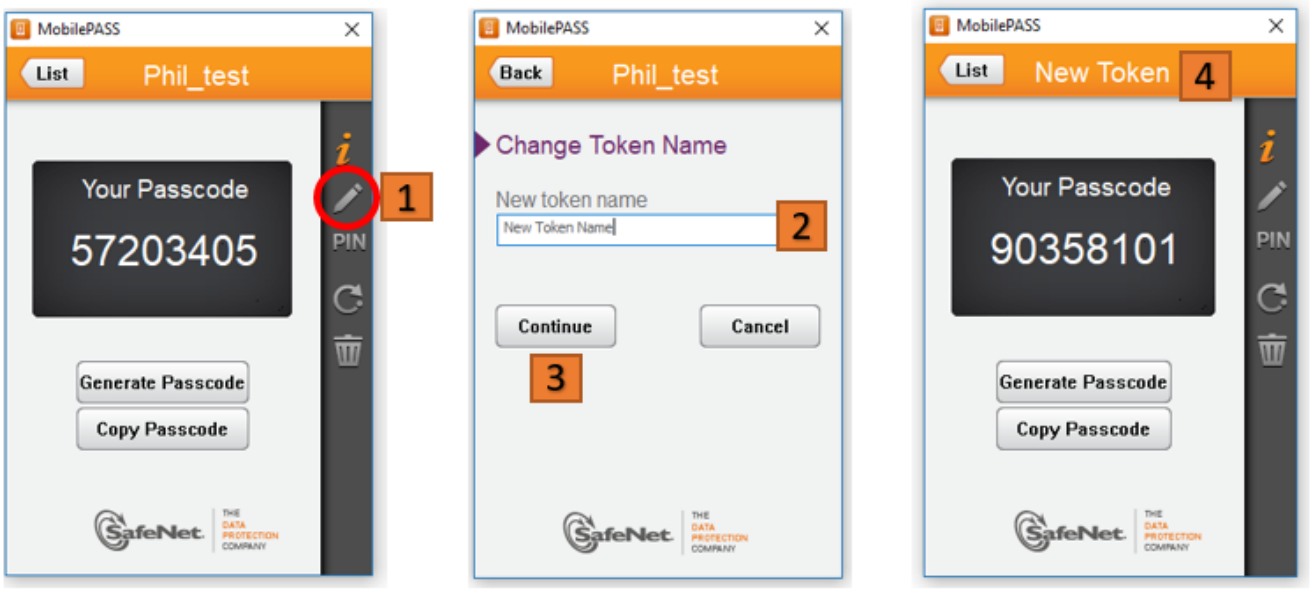
By default, Token name is based on your user ID.

It is recommended not to change the name of your Token but if needed to better identify it, please proceed as follows:

In your “Token” application’
select “Pen”, to rename token (1),

In the pop-up window enter the new Token name in the “New Name” field (2),
then click on “Continue” (3)

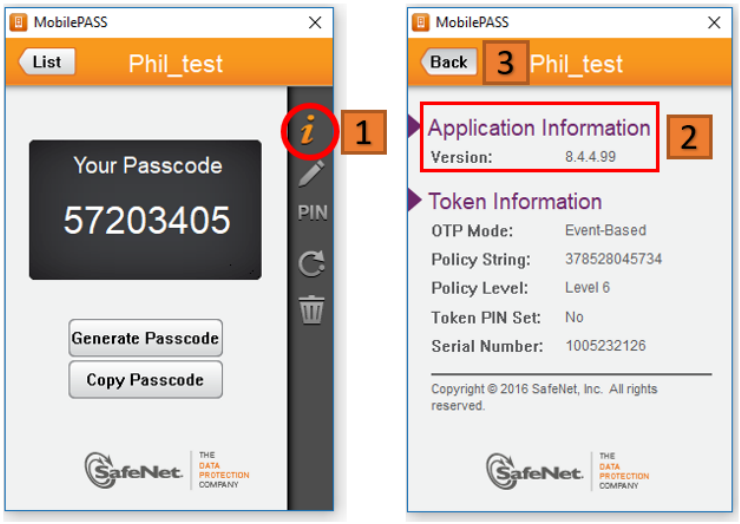
Your Token is now referenced with the new name (4).



P. How do I retrieve the “Token” application version?

For maintenance or troubleshooting purposes, your administrator may ask you the version of your Token application. To retrieve the version, please proceed as follows:

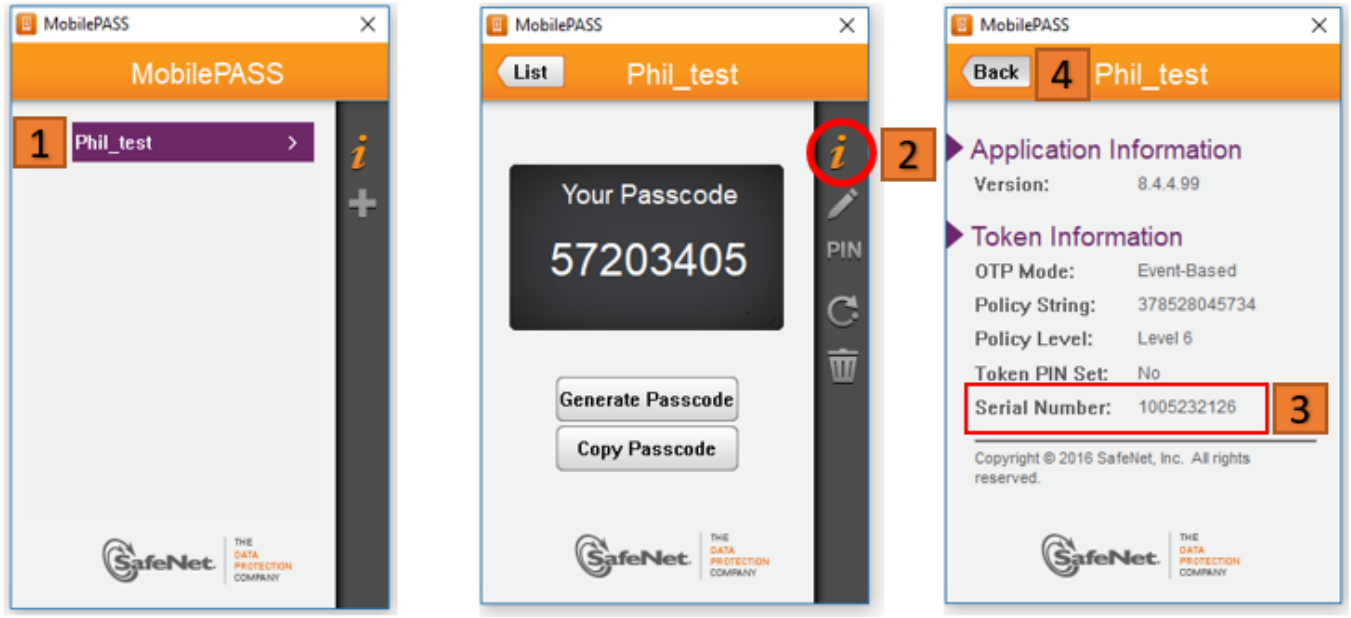
In your “Token” application:
select “Information” button (1),
memorize the “Token” application version (2),
then click on “Back” (3).



Q. How do I retrieve my Token serial?

In your “Token” application,
select the Token you need (1),
click on “Information” button (2)

In the pop-up window memorize the Token serial (3),
then click on “Back” (4)



R. How do I remove my Token?

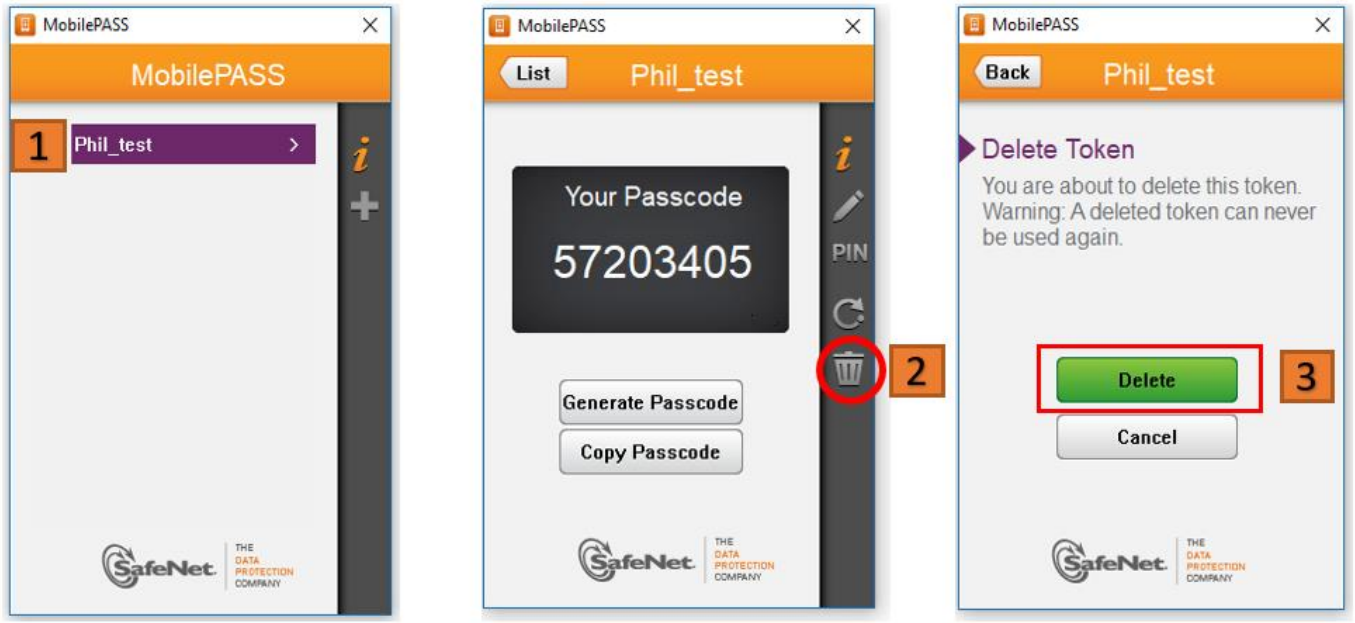
For maintenance or troubleshooting purposes, your administrator may ask you to remove a Token from your device. To remove a Token, please proceed as follows:

In your “Token” application,

select the Token you want to remove (1),
click on “Trash” button (2)

In the pop-up window click on “Delete” (3)

Check that the Token has been successfully removed.



S. How do I remove completely SALSA?

To remove SALSA software and tools from your Windows PC, please proceed as follows:

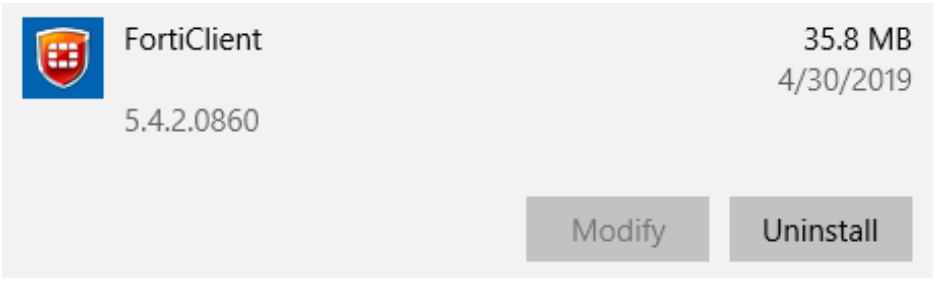
First you have to remove the Token(s) as described in section **How do I remove my Token?**

Make sure all Tokens are removed.

With Windows 10:
In the Windows Start menu, go to “Settings” and “Apps and Features” and remove the SALSA software and tools:

FortiClient

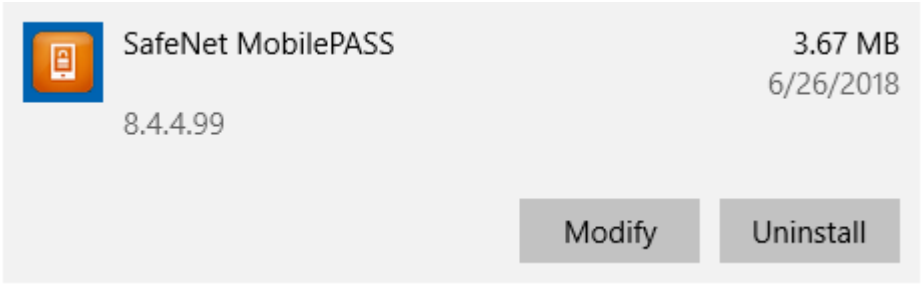
Select



And Click “Uninstall”

SafeNet

Select



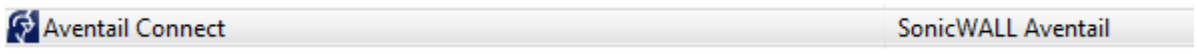
And Click “Uninstall”

If you have former version of SALSA (based on RSA), you can remove the corresponding software as described below:

With Windows 7:
In the Windows Start menu, go to “Control Panel” and “Programs and Features” and remove the SALSA software:

Aventail

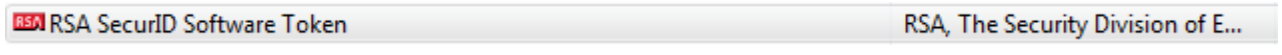
Select



And Click “Uninstall”

RSA

Select



And Click “Uninstall”