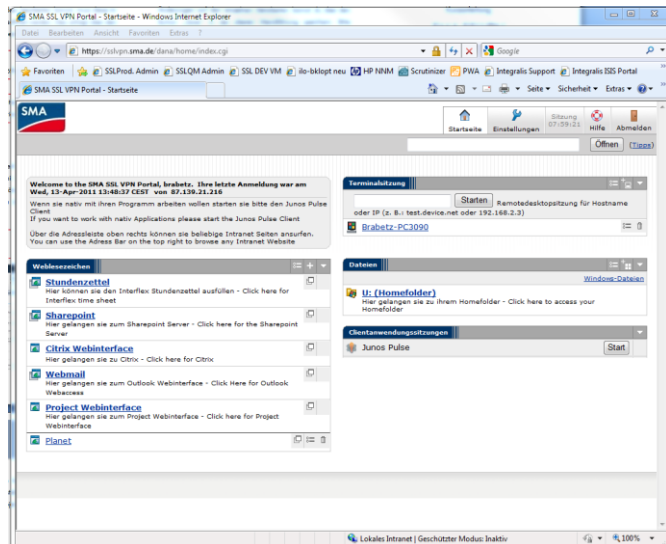


SMA SSL VPN



English version at page 8



Hallo SMA'lerinnen und SMA'ler,

für Dich wurde ein VPN-Zugang beantragt und eingerichtet. Dieser Zugang wird durch eine Zwei-Wege-Authentifizierung hergestellt, für den Du einen eToken (Code-Generator) und deine SMA-Anmeldedaten der Windows-Anmeldung benötigst.

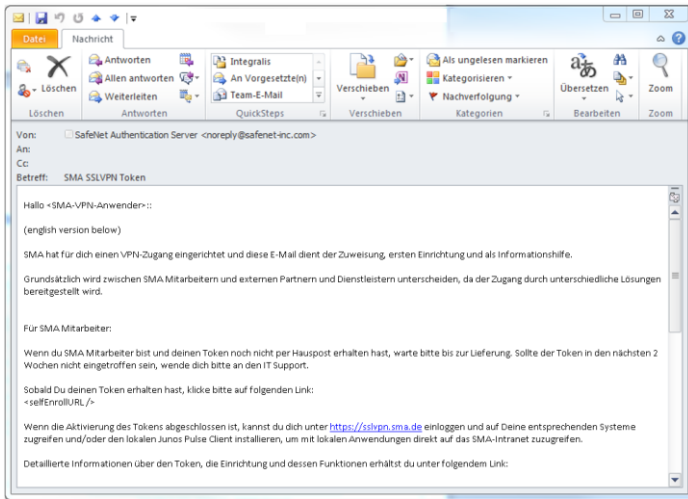
Mit Hilfe dieses eTokens wird es ermöglicht, das SMA Firmennetz, interne Applikationen und Services über externe Internetzugänge zu erreichen, ohne direkt mit dem Firmennetz verbunden zu sein.

Dieses Dokument leitet Dich durch die automatisierte Einrichtung und Installation der benötigten Software sowie die Möglichkeiten und Bedienung des VPN Portals.

Bei Fragen und Problemen wird Euch der SMA IT Support gerne weiterhelfen: IT.Support@SMA.de oder via Tel. +49 561 9522 2400.

Token Self-Assignment Prozess

Nach genehmigter Bestellung des VPN Zuganges und der Bearbeitung durch den IT Service, erhältst Du automatisiert eine Self-Assignment E-Mail.



Diese E-Mail beinhaltet weitere Informationen sowie den Aktivierungs- und Einrichtungslink für Deinen SSL VPN Token.

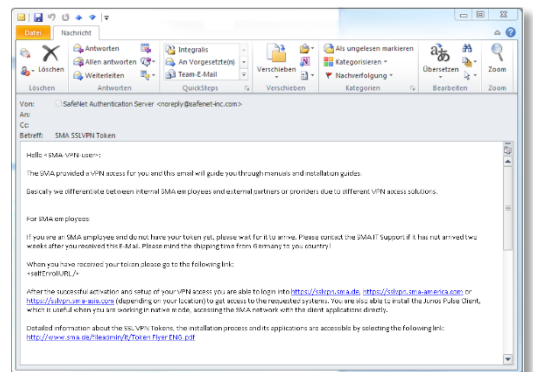
Bitte bedenke, dass es sich hierbei um eine automatisiert generierte und personalisierte E-Mail des eToken-Managements handelt.

Der angegebene Link zur Aktivierung wird nur für Dich nutzbar sein.

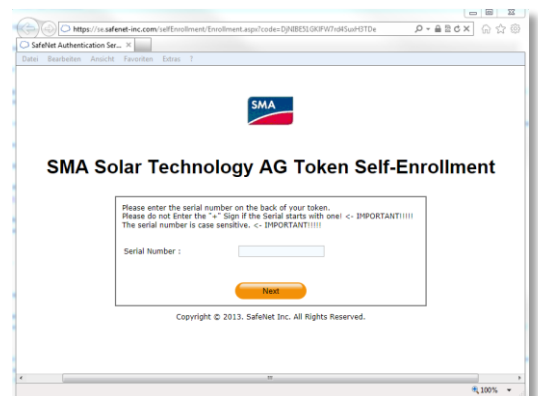
Wende Dich bei Problemen direkt an den IT Support.

Aktivierung und Einrichtung des eTokens

1. Bitte klicke innerhalb der Self-Enrollment Email auf den entsprechend hingewiesenen Link, sobald Du deinen Token erhalten hast.



2. Dieser Link leitet Dich zu einer Seite, auf der Du die Seriennummer deines Tokens eingeben musst. Diese befindet sich auf der Rückseite deines eTokens oberhalb des Strichcodes. Beachte bitte hierbei die Groß- und Kleinschreibung und darauf **keine** Sonderzeichen zu verwenden. Einige Token besitzen vor ihrer Seriennummer ein „+“. Dieses bitte nicht verwenden!

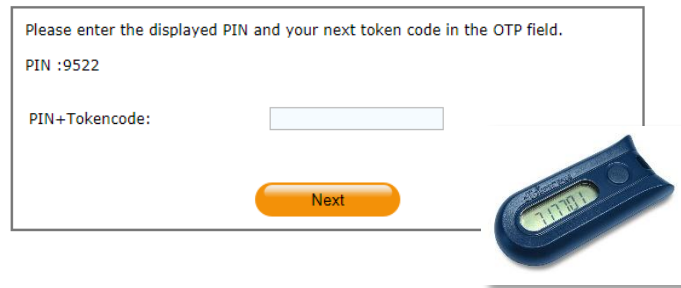


3. Im nächsten Schritt musst Du den PIN und folgend einen generierten eToken Code eingeben.

Der PIN ist immer **9522**.

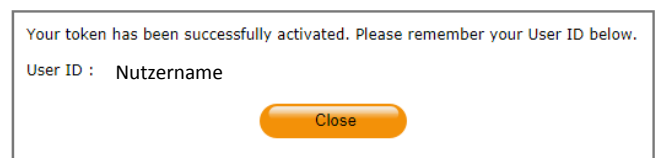
Der aus sechs Ziffern bestehende eToken Code wird durch kurzes Drücken des Knopfes generiert.

In diesem Beispiel muss somit Folgendes in das Feld „PIN + Tokencode“ eingegeben werden: **9522717701**



4. Die folgende Seite bestätigt Dir, dass die eToken-Zuweisung und Aktivierung erfolgreich war.

Der neue eToken kann nun für die Anmeldung am Pulse Client als auch an der SSL VPN Portal Webseite genutzt werden!



Login an der SSL VPN Portal Webseite

Das SSL VPN Portal erreichst Du unter folgender Adresse im Webbrowser: <https://sslvpn.sma.de>

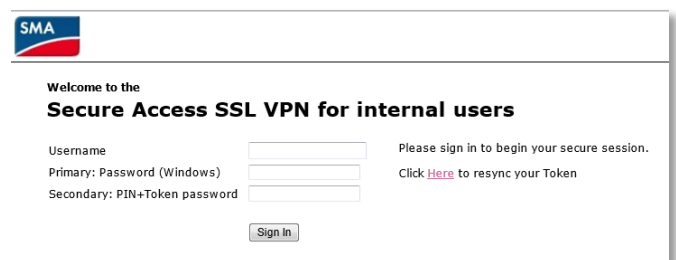
Bitte melde Dich hier mit deinen Windows Anmeldedaten und dem PIN inklusive des eToken Codes an.

Beispiel:

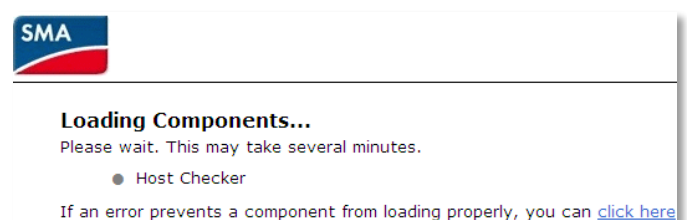
Username: mustermann

Password (Windows): s3cr3tPW!

PIN+Token password: 9522717701



Bei erfolgreicher Erst-Anmeldung wird der sog. Host-Checker installiert. Dieser dient dazu die SMA vor Viren und anderer Schadsoftware zu schützen. Bei der Einwahl am Portal und Aufbau eines VPN werden folgende Kriterien des PCs überprüft:



- Handelt es sich um einen SMA-PC/Notebook
- Ist die installierte Version des McAfee Antivirus Scanners aktuell

Bitte akzeptiere die Installation sowie Überprüfung und fahre fort.

Es gibt zwei Gründe wodurch der Host Checker fehlschlägt:

- Virenschanner nicht aktuell
 - ➔ Kein Zugriff auf die VPN Portal Webseite
 - ➔ Kein Aufbau eines vollständigen VPN Tunnels möglich
 - Host-Checker versucht den McAfee Client zu aktualisieren
- Kein SMA-PC/Notebook
 - ➔ Eingeschränkter Zugriff auf die VPN Portal Webseite
 - ➔ Zugriff auf Citrix möglich
 - ➔ Kein Aufbau eines vollständigen VPN Tunnels möglich

You have logged in from a computer that does **not** comply to the SMA security requirements. Please note that your access is **restricted!**

Aus Sicherheitsgründen ist ein vollwertiger Zugriff nur mit SMA Geräten möglich. Anderweitig stehen nur wenige Applikationen, wie z.B. Citrix, zur Verfügung. Wir bitten darüber hinaus um Verständnis, dass die SMA IT keine privaten Geräte betreuen kann.

Ein vollwertiger Zugriff sowie Support durch die IT kann nur über SMA-eigene Geräte gewährleistet werden

Wenn die geforderten Kriterien **zutreffen** und der genutzte Computer somit akzeptiert wird, erscheint die Startseite des SSL VPN Portals.

Links und Applikationen des VPN Web Portals

Auf der Portalseite kannst Du nun zwischen folgenden Links und Applikationen wählen:

(je nach Berechtigungen können einige der aufgelisteten Möglichkeiten bei dir nicht sichtbar sein)

HR-Self Services

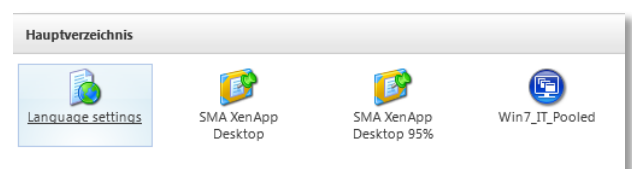
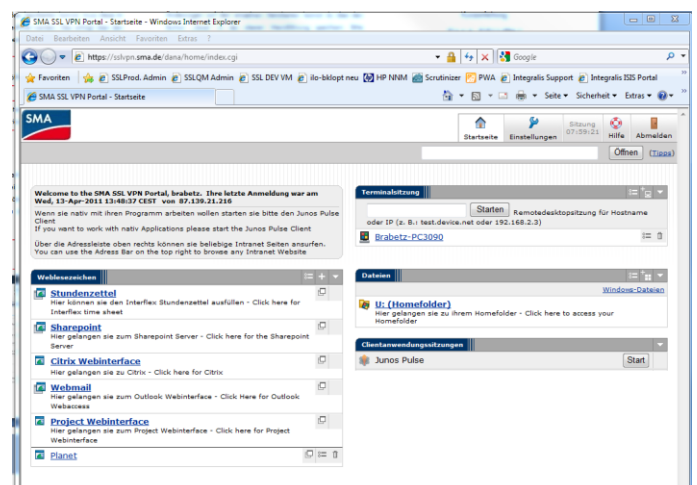
- Hier gelangst Du zum HR-Selfservice Portal

Sharepoint

- Hier gelangst Du zum Sharepoint-Server

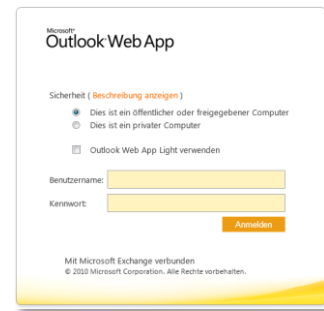
Citrix Webinterface

- Hier gelangst Du zum Citrix Webinterface mit dessen Hilfe Du nach der Installation einen virtuellen Desktop zur Verfügung gestellt bekommst. Mit diesem ist es dir möglich, Citrix Applikationen (z.B. SAP CRM) zu nutzen.



Webmail

- Hier gelangst Du zur Outlook Web App um auf dein Outlook zuzugreifen

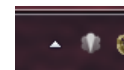


Terminalsitzung und Dateien

- Hiermit kannst Du per Remote Client auf freigegebene PCs, Server und Ordner zugreifen

Junos Pulse Client

- Der Pulse Client ermöglicht dir einen vollwertigen Zugriff auf das SMA Netzwerk.
Das Wählen des Start-Buttons leitet die Installation ein.
Diese verläuft automatisch und lässt anschließend in der Taskleiste das Pulse Client Symbol erscheinen. Bei aktiver VPN Verbindung pulsiert dieses farbig.



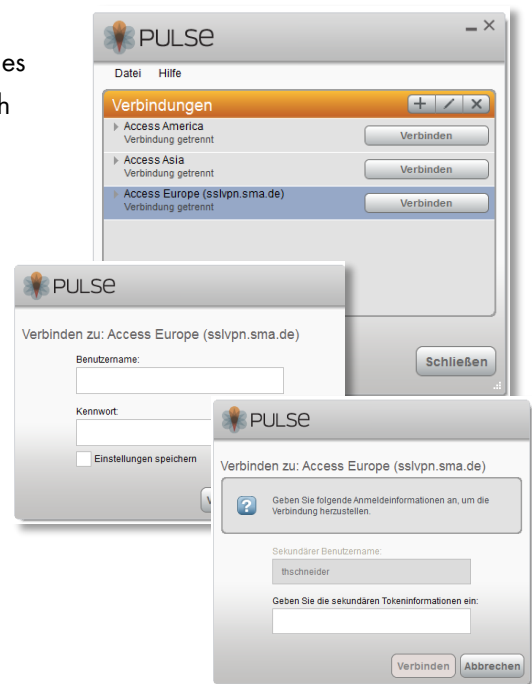
Aufbau eines VPN Tunnels mit dem Junos Pulse Client

Nach der Installation kann der Pulse Client direkt gestartet werden, ohne das VPN Web Portal zu nutzen. Bei Auswahl des Pulse Symbols oder über das Start Menü kann somit – je nach Standort – eine Verbindung aufgebaut werden.

Sobald „Verbinden“ gewählt wird, erscheinen aufeinander folgend zwei Anmelde-fenster. Das erste benötigt die Windows Anmeldedaten, das zweite den eToken Code.

Beispiel:

1. Eingabe der SMA-Windows Anmeldedaten
Benutzername: mustermann
Kennwort (Windows): s3cr3tPW!
2. Eingabe des eToken Codes
PIN+Token Code: 9522123456



Wichtig

Bei Eingabe des eToken Codes muss der PIN 9522 vor dem generierten Token Code gesetzt werden!

Sobald alle eingegebenen Daten korrekt sind, wird über den Pulse Client ein VPN Tunnel aufgebaut, das Symbol pulsiert farbig. Dir ist es nun möglich auf das SMA Netz zuzugreifen.

SSL VPN – eToken self service



Dieses Dokument leitet Dich kurz durch den Synchronisationsprozess deines SSL VPN eTokens.

Es kann vorkommen, dass ein eToken asynchron wird und somit keine gültigen Codes generiert. Dabei erscheint folgende Meldung auf der Anmeldeseite des VPN Web Portals:

Welcome to the
Secure Access SSL VPN for internal users

Primärer Benutzername oder Kennwort ungültig. Geben Sie Ihre Benutzerinformationen erneut ein.

Username Please sign in to begin your secure session.
Primary: Password (Windows) Click [Here](#) to resync your Token
Secondary: PIN+Token password

Diese Login Seite verfügt über einen Link, der Dich zum Self-Service Portal deines Accounts führt.

Bei Anklicken des Links erscheint die Startseite des Self-Service.

Hier kann unter anderem auf diese Anleitung zugegriffen werden sowie der Prozess zur Token-Synchronisierung gestartet werden.

SMA VPN
Token
Self-service
Portal

[VPN Token Setup and Synchronization Guide](#) | [Grid Code Setup and Resetting Guide](#) | | [Contact SMA IT-Support](#)
Copyright © 2014. SafeNet Inc. All Rights Reserved.

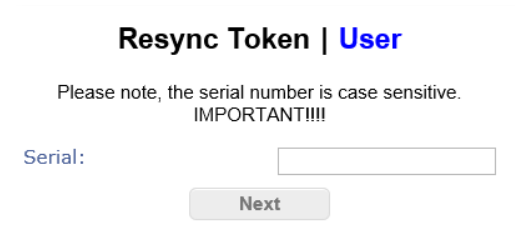
Wenn „Resync Token“ gewählt wird, erscheint die Aufforderung zur Eingabe des Windows Benutzernamens.

Resync Token | User

User ID:

Beim nächsten Schritt muss die Seriennummer des eTokens eingegeben werden. Diese befindet sich auf der Rückseite deines eTokens oberhalb des Strichcodes.

Beachte bitte hierbei die Groß- und Kleinschreibung und darauf **keine** Sonderzeichen zu verwenden.



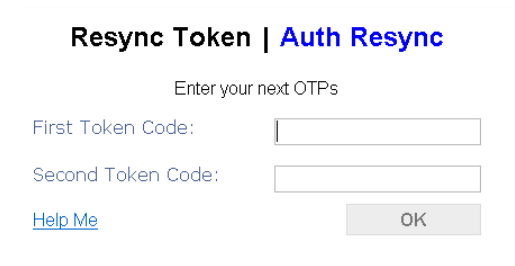
Resync Token | User

Please note, the serial number is case sensitive.
IMPORTANT!!!!

Serial:

[Next](#)

Um den eToken nun zu synchronisieren, müssen beim letzten Schritt zwei generierte eToken Codes **ohne PIN (9522)** eingegeben werden.



Resync Token | Auth Resync

Enter your next OTPs

First Token Code:

Second Token Code:

[Help Me](#) [OK](#)

Sobald alle Eingaben korrekt sind, erscheint abschließend die Bestätigung der erfolgreichen eToken Synchronisierung.



Resync Token | Confirmation

Token successfully synchronized.

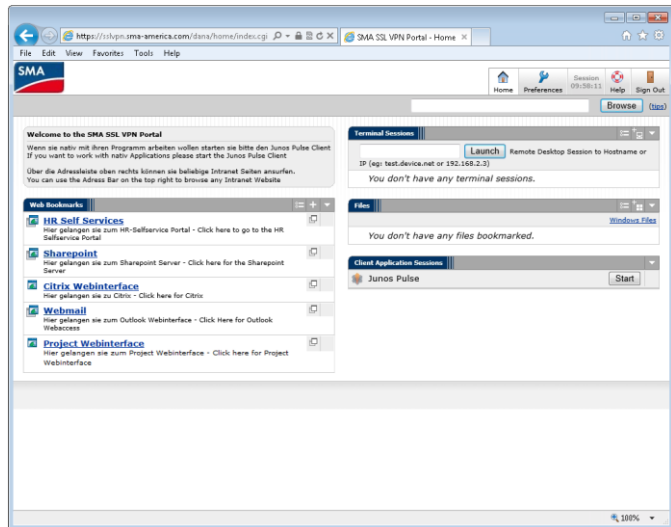
Weitere Fragen oder Probleme?

Bei weiteren Fragen oder Problemen wende Dich bitte an den IT Support:

Tel: +49 561 9522 2400

Email: IT.Support@sma.de





Dear SMA colleagues,

A new VPN access was requested for you. This access is provided by using a two way authentication. The requirements for this authentication are an eToken (code generator) and your SMA login credentials for Windows.

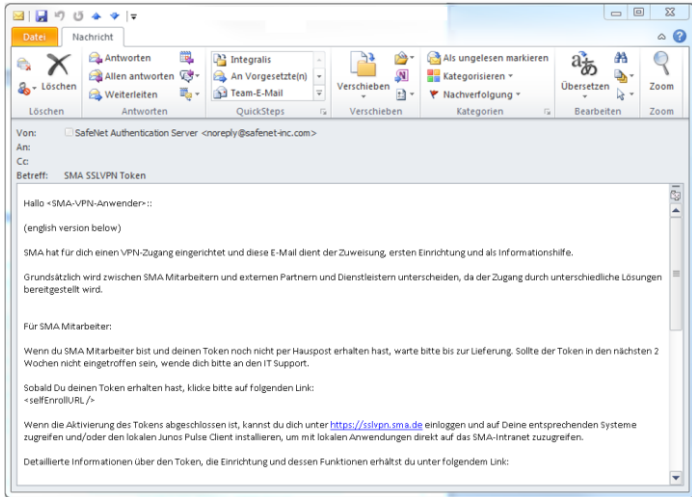
With this eToken you are able to access the company's network, internal applications and services from any external internet access point.

This document will guide you through the setup and installation process of needed software and will show you the possibilities of the VPN access.

Please contact the IT support if you have problems or further questions via email at IT.Support@SMA.com or by phone +49 561 9522 2400.

Token Self-Assignment Process

According to your resolved request of the VPN access you'll receive an automatically generated self-assignment email.



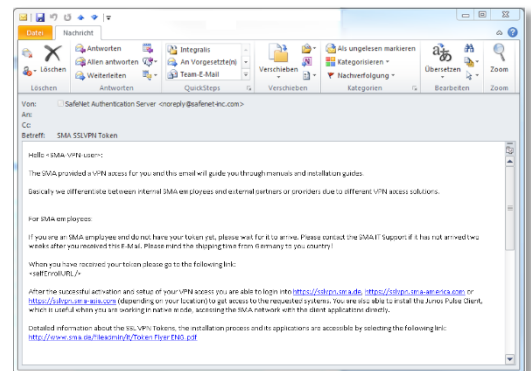
This email contains further information about the VPN access and a link to your SSL VPN eToken setup.

Please keep in mind that this mail is an automatically generated and personalized email. All links for the activation and setup will just work for you.

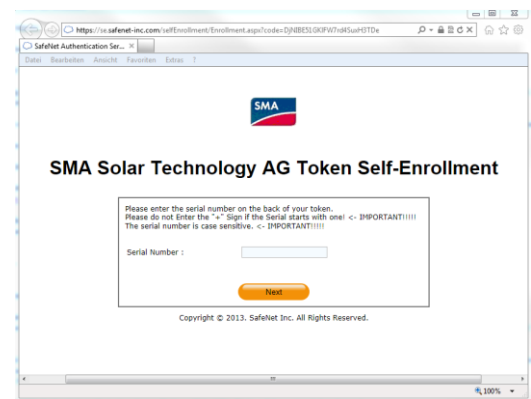
Please contact the IT support if you have problems or further questions.

Setup of the VPN access and the eToken

1. Please click at the activation and setup link for internal users and SMA employees.



2. This link will pass you to a website where you have to enter the serial number (**without** special characters) that is on the backside of the eToken above the barcode.
Please pay attention to small and capital letters!
Confirm the serial number with the "next" button.

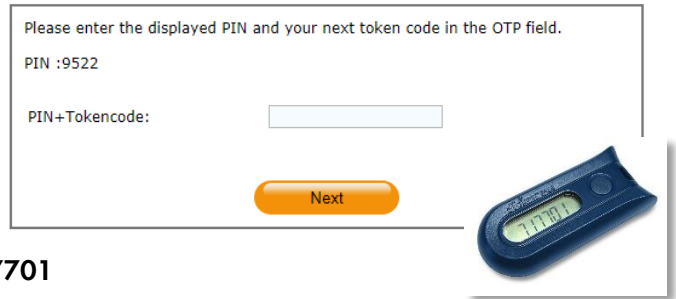


- Now you have to enter the PIN code and a generated eToken code.

The PIN code is always **9522**.

You generate an eToken code by briefly pressing the eTokens button.

In this example the user has to enter: **9522717701**



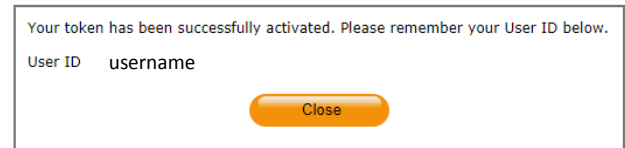
Please enter the displayed PIN and your next token code in the OTP field.

PIN :9522

PIN+Tokencode:

Next

- The next page will confirm your successfully activated eToken. You are now able to use this eToken for access at the SSL VPN webportal or the Junos Pulse Client.



Your token has been successfully activated. Please remember your User ID below.

User ID username

Close

Login at the SSL VPN portal website

The SSL VPN web portal is accessible by your web browser at <https://sslvpn.sma.de>, <https://sslvpn.sma-america.com> or <https://sslvpn.sma-asia.com>.

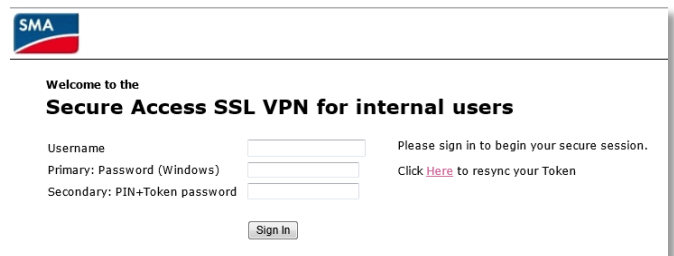
Please login by using your SMA login credentials and the PIN with your generated eToken code.

Example:

Username: smith

Password (Windows): s3cr3tPW!

PIN+Token password: 9522717701



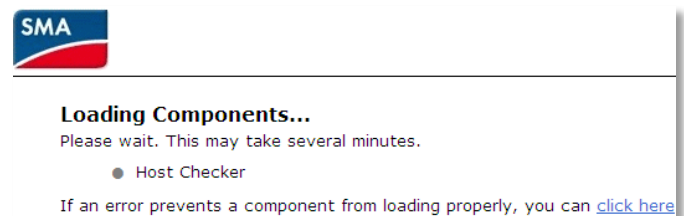
SMA

Welcome to the
Secure Access SSL VPN for internal users

Username Please sign in to begin your secure session.
Primary: Password (Windows) Click [Here](#) to resync your Token
Secondary: PIN+Token password

Sign In

Once the credentials have been successfully entered an installation process of the so-called Host Checker will start at the first login. This host checker protects the SMA network against any digital threats and will always active for every VPN session.



SMA

Loading Components...
Please wait. This may take several minutes.

● Host Checker

If an error prevents a component from loading properly, you can [click here](#)

Additionally the host checker will verify if

- the used Computer is property of the SMA
- the installed version of McAfee Anti-Virus software is up to date

Please confirm every permission and additional installation of further plugins.

There are two reasons that will cause the host check to fail:

- McAfee not up to date
 - ➔ No access to the VPN web portal
 - ➔ No active VPN tunnel

- No SMA hardware
 - ➔ Limited access to VPN web portal applications
 - ➔ Only Citrix available
 - ➔ No active VPN tunnel

You have logged in from a computer that does **not** comply to the SMA security requirements. Please note that your access is **restricted!**

For security reasons full functional range will only be available from SMA hardware. However it will be possible to use certain applications from private hardware e.g. Citrix.

Please understand that we cannot give support for all private computer installations. If you rely on constant access to the SMA network a SMA notebook is advised. For that we can guarantee full compatibility.

If the host checker scan is completed **successfully** and there are now further problems you will get access to the SSL VPN web portal.

Links and applications of the VPN portal

Depending on your requested permissions there are several links and applications available.

HR-Self Services

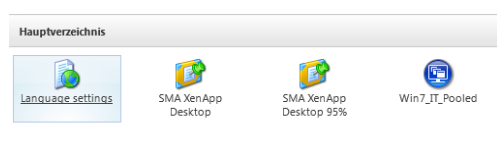
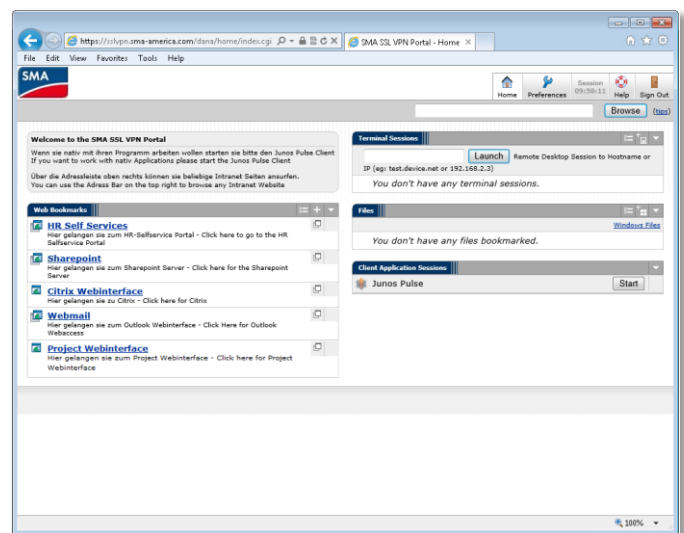
- This link provides a direct access to your HR-Self Service

Sharepoint

- This link will launch the SMA SharePoint start page in your web browser

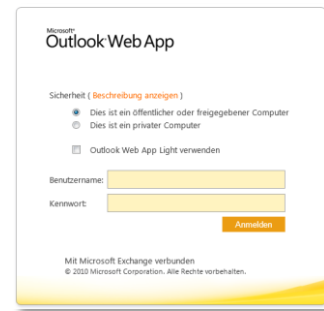
Citrix Webinterface

- This link will activate the Citrix web interface to launch virtual desktops. After the installation of needed browser plugins these desktops provide access to internal SAP systems and applications



Webmail

- This link will give you access to your SMA email account



Terminal sessions and files

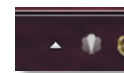
- Experienced users can directly connect to remote desktop sessions or file shares using these application

Junos Pulse Client

- The Junos Pulse client will provide full access to the SMA network. Pressing Start will initiate the Pulse client



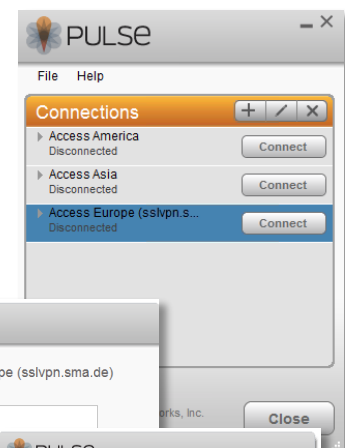
Installation process. At the first time it will ask to install the client automatically. The client should then appear and be also visible in your taskbar. When the client is connected the client logo will pulse in the system tray near the Windows clock. That means it is connected and will grant full access to the SMA network.



Establishing a VPN connection with Junos Pulse Client

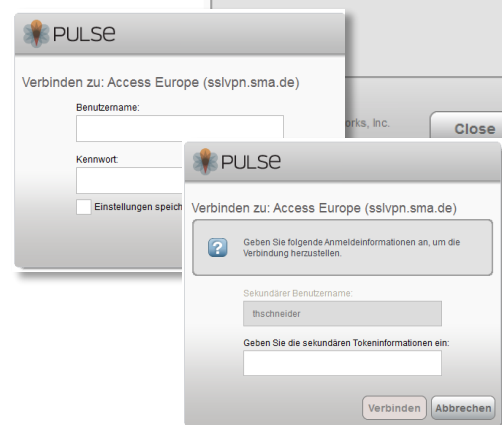
After the first installation the pulse client can be started directly via the Windows Start menu without logging into the SSL VPN Portal page. Then please choose the access point depending on you actual location.

As soon as the access point was selected the Pulse Client first asks for the windows credentials and then for the PIN with eToken credentials. You will see two separate login screens one after another.



Example:

1. Please enter your windows credentials
Username: smith
Password (Windows): s3cr3tPW!
2. Please enter your eToken code
PIN+eToken coide: 9522717701



Important

When entering the generated eToken code add the PIN 9522 in front of it!

As soon as all credentials were entered correctly the client logo will pulse in the system tray near the Windows clock. That means it is connected and will grant full access to the SMA network.

SSL VPN – eToken self service



This manual will quickly guide you through the resynchronization process of your SSL VPN eToken.

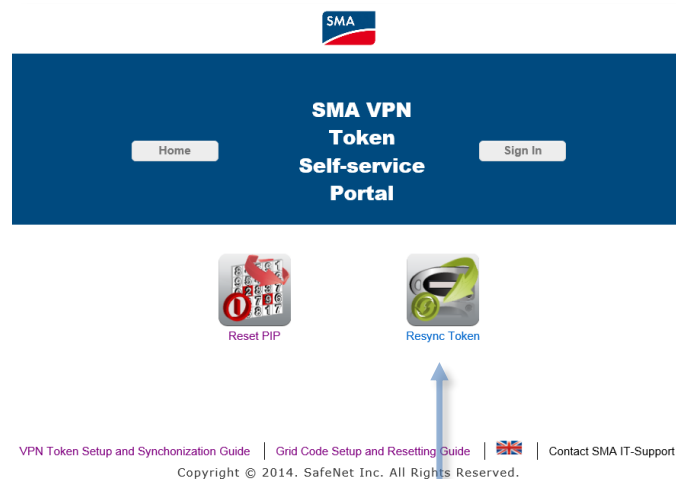
It can happen that an eToken gets out of sync and this will result in the following login message:



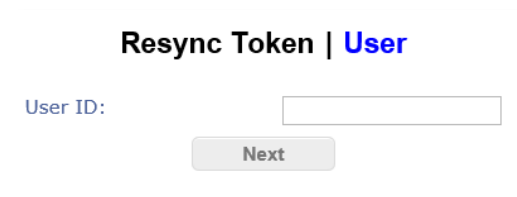
The SSL VPN login page also contains a link to the self-service page for token users.

By clicking the link you will be presented with the following self-service page.

Here you are able to get access to the troubleshooting guides and to start the eToken resynchronization process.

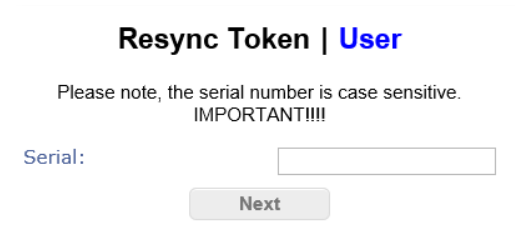


By choosing "Resync Token" you will be asked to enter your user ID (Windows username):



In the next step you have to provide your eToken serial number (without special characters) that is on the backside of the eToken above the barcode.

Please pay attention to small and capital letters!



Resync Token | User

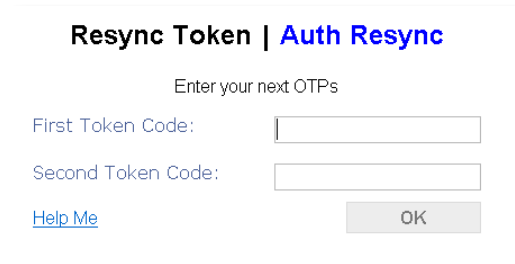
Please note, the serial number is case sensitive.
IMPORTANT!!!!

Serial:

Next

To finally resync your eToken you need to enter 2 following eToken codes **without the PIN code**.

Do not enter 9522 in front of your eToken code!



Resync Token | Auth Resync

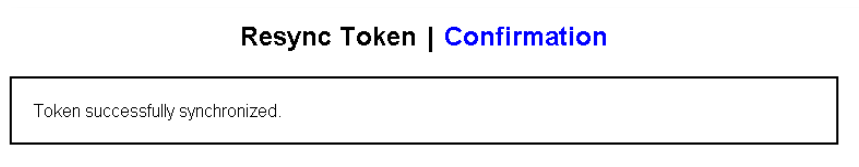
Enter your next OTPs

First Token Code:

Second Token Code:

[Help Me](#) OK

As soon as everything was entered correctly you will be verified that your eToken was successfully synchronized.



Resync Token | Confirmation

Token successfully synchronized.

Further questions or problems?

For further questions feel free to contact the IT Support:

Fon: +49 561 9522 2400
Email: IT.Support@sma.de

