Berry Remote Operating Instructions

Doc. Version 1.03

2014-08-01

FIIN1 dept.

Important Informations:

- **Before using the software for the first time**
  - **You need a valid BerryRemote account**
  - **The CryptoCard Hardware Token must be personalized.**
  - **A internet connection is available**
- **Please close all programs, if you have data from the Berry network or another network in progress, if you establish or terminate a connection with Berry Remote! Warning: Please note, otherwise data may be lost!**
- **If the VPN connection is established local devices in your network are not usable.**

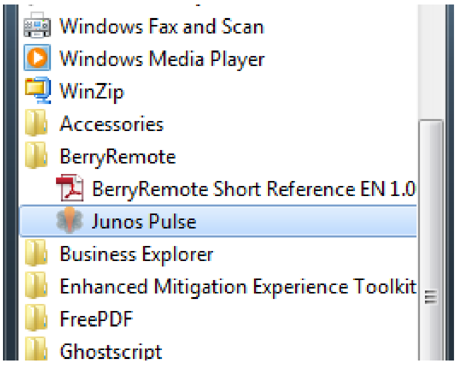
1. Introduction and important information

The Berry Remote software package is used for connecting mobile computers to the Berry company network (Berry Net).

The software package includes one program and a short reference.

- **Junos Pulse:** This program is a VPN client and provides encrypted and secure connectivity to the Berry company network worldwide.

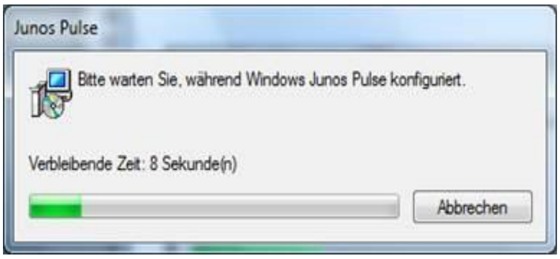
In the standard installation on a Berry laptop, the software package is located at Start-> Programs -> BerryRemote



1.1. Important: First Use of the software (automatically installed only)

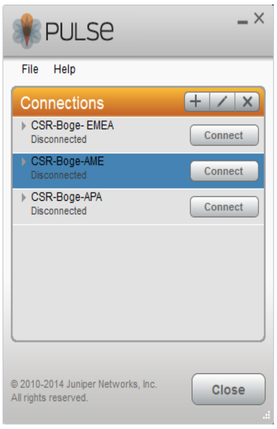
This chapter is for Berry employees only. Users from e.g. ZF Friedrichshafen AG or other companies with non Fujitsu managed computer installations are asked to skip the chapter 1.1 and go ahead with chapter 2.

Berry employees with Fujitsu managed computers:
Please start your Software once as your computer is connected to the Berry- Network e.g. in your office or in one of the Berry locations.
Click one file (e.g. Junos Pulse) listed below the BerryRemote register and the process starts. If the installation is finalized the selected program or the selected information appears.


Junos Pulse

Bitte warten Sie, während Windows Junos Pulse konfiguriert.

Verbleibende Zeit: 8 Sekunde(n)



© 2010-2014 Juniper Networks, Inc.
All rights reserved.

2. Personalizing the Token before the First Connection (selfenrollment)

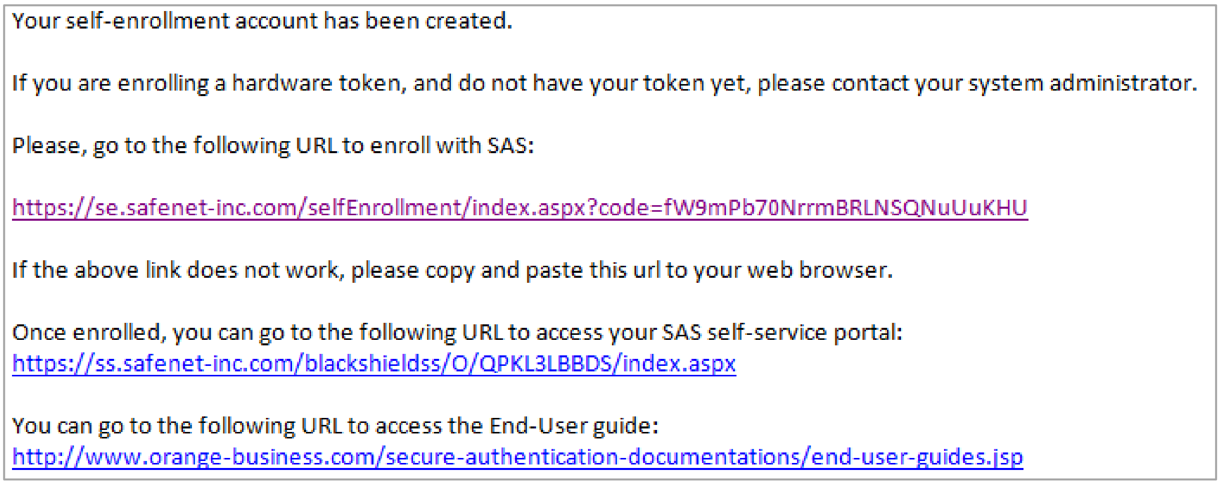
2.1. Start of self-enrollment

Required:

1. Cryptocard Hard Token
2. Enrollrollment message as shown below
3. User ID
4. Internet Access (best unrestricted, if not please check with chapter 6.2)

All three of these requirements are urgently required.
If you do not receive 1+2 then go in touch with the Berry Usermanagement.

The self-enrollment process starts with the following e-mail. Click on the first link to enroll a hardware token. A new window will pop up.
Important: You have max. 10 days to enroll your token.



Your self-enrollment account has been created.

If you are enrolling a hardware token, and do not have your token yet, please contact your system administrator.

Please, go to the following URL to enroll with SAS:

https://se.safenet-inc.com/selfEnrollment/index.aspx?code=fW9mPb70NrrmBRLNSQNuUuKHU

If the above link does not work, please copy and paste this url to your web browser.

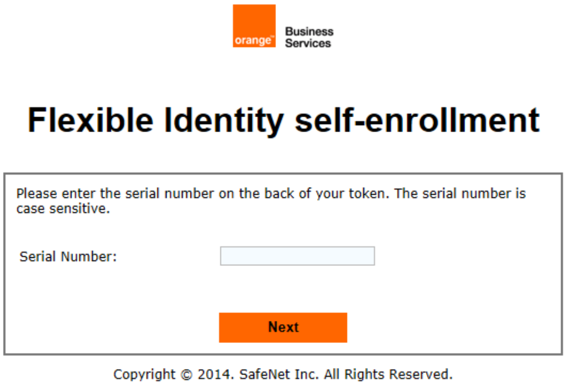
Once enrolled, you can go to the following URL to access your SAS self-service portal:
https://ss.safenet-inc.com/blackshieldss/O/QPKL3LBBDS/index.aspx

You can go to the following URL to access the End-User guide:
http://www.orange-business.com/secure-authentication-documentations/end-user-guides.jsp

>>> Please safe this email because of the further need of the two described links !!!

Important: You have max. 30 days to enroll your token.

3. Register the hardware token



Flexible Identity self-enrollment

Please enter the serial number on the back of your token. The serial number is case sensitive.

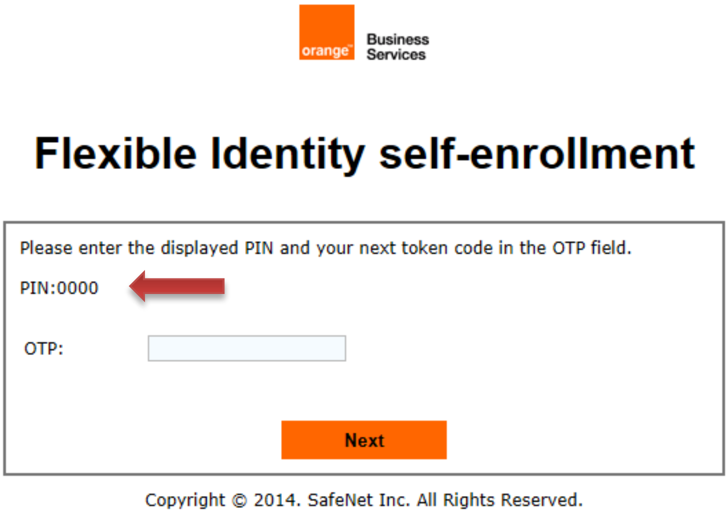
Serial Number:

Copyright © 2014. SafeNet Inc. All Rights Reserved.

Fill in the serial number from the back side of the token into the system and click on next.

3.1. Enter a passcode

For the identification a passcode is needed. You can create this passcode by using the given PIN (e.g. 0000) and the generated code displayed on the token. Insert the passcode into the OTP field below.



Flexible Identity self-enrollment

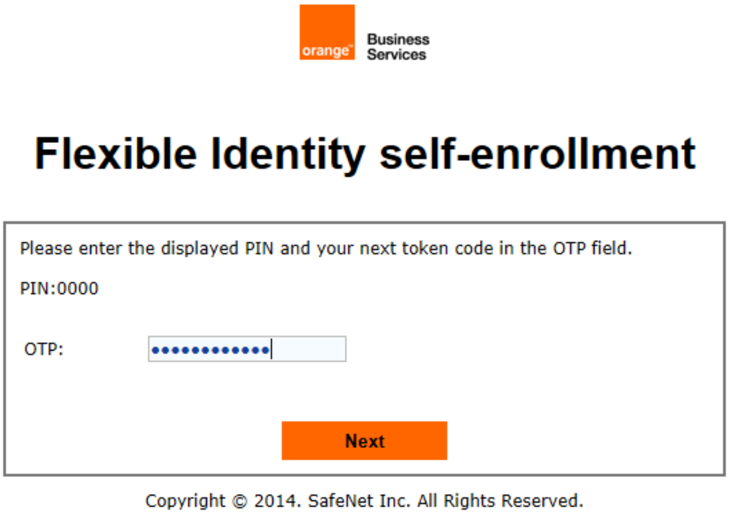
Please enter the displayed PIN and your next token code in the OTP field.

PIN:0000

OTP:

Copyright © 2014. SafeNet Inc. All Rights Reserved.

Enter **Passcode = PIN (XXXX) + token code (XXXXXXXXXX)**



Flexible Identity self-enrollment

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

PIN:0000

OTP: ••••••••••••

Copyright © 2014. SafeNet Inc. All Rights Reserved.

Click on next.

Register the hardware token

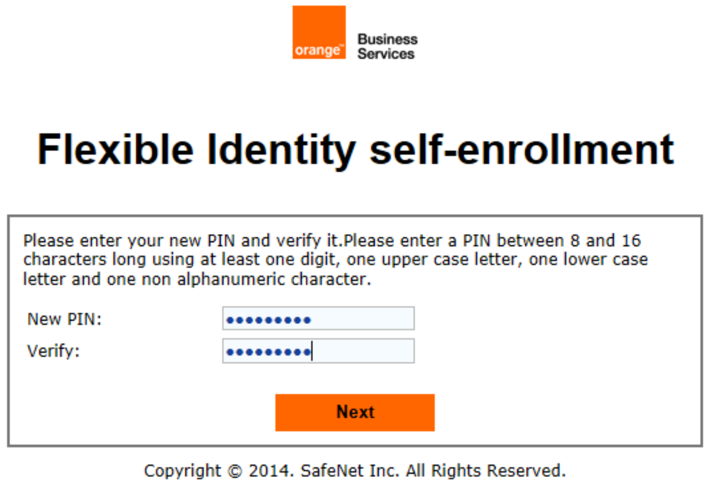
3.2. Create your own PIN (Complexe Alphanumeric)

You have now the possibility to choose a new PIN.

3.2.1. PIN rules

• Between 8 – 16 characters	
• Minimum one capital letter	aA – zZ exclude il or IL or oO
• Context sensitive	
• Minimum one number	0-9
• Minimum one special character	. , ; : ! “ § $ % & / ( ) = ? * + - _ #
• Old PIN is reusable	
• No change frequency	

Insert your own PIN twice.



Flexible Identity self-enrollment

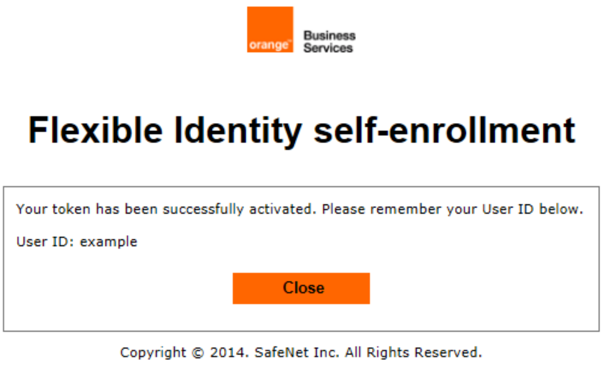
Please enter your new PIN and verify it.Please enter a PIN between 8 and 16 characters long using at least one digit, one upper case letter, one lower case letter and one non alphanumeric character.

New PIN: ●●●●●●●●●

Verify: ●●●●●●●●●

Copyright © 2014. SafeNet Inc. All Rights Reserved.

3.3. Successful enrollment



Flexible Identity self-enrollment

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

User ID: example

Copyright © 2014. SafeNet Inc. All Rights Reserved.

The enrollment was successful if this window will show up. Please remember your given User ID.

Register the hardware token

4. PIN setup

4.1. PIN change with selfservice portal

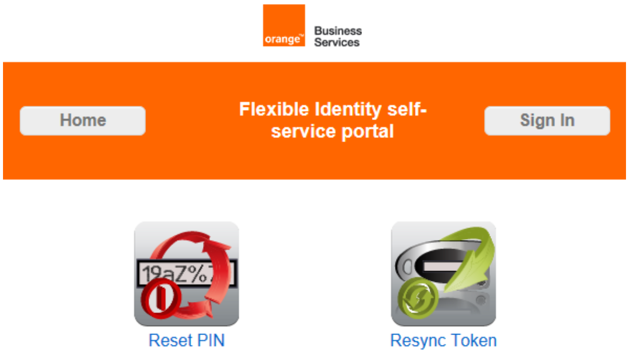
If you want to change your chosen PIN, you can log in the flexible identity self-service portal and reset the PIN.

Link to the selfservice portal:

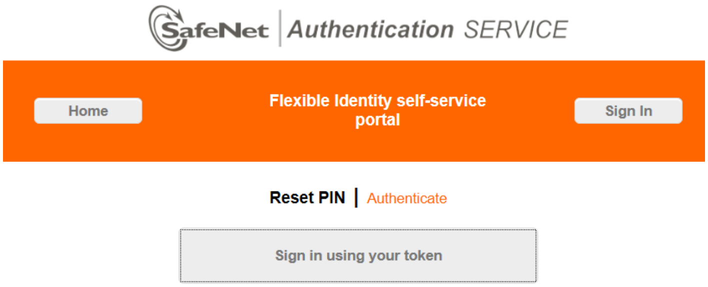
https://ss.safenet-inc.com/blackshieldss/O/QPKL3LBBDS/index.aspx

or written in your personal enrollment mail (Chapter 2.1)

⇨ Then click to “Reset Pin”



⇨ Then click to “Sign in using your token”

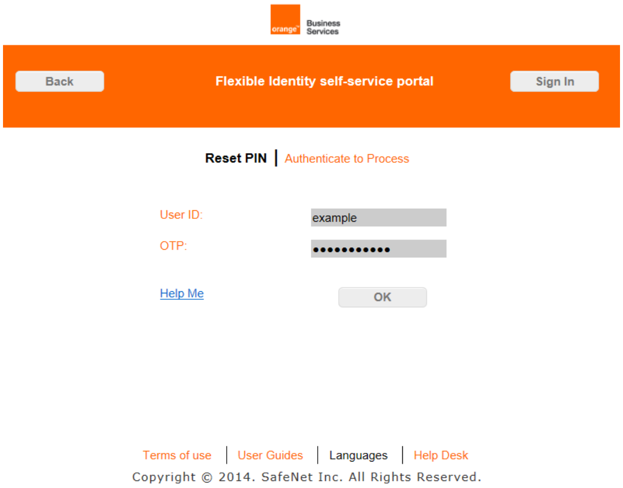

SafeNet | Authentication SERVICE
Home
Flexible Identity self-service portal
Sign In
Reset PIN | Authenticate
Sign in using your token

⇨ Then type in your user ID and OTP = actual **PIN** + **Tokencode** from CRYPTOCARD

How to get the Tokencode:

Click the button at your Cryptocard and readout the displayed tokencode

Use the last valid and known PIN. If you do not know the PIN please read chapter 3.2


Business Services
Back
Flexible Identity self-service portal
Sign In
Help Me
OK
Terms of use | User Guides | Languages | Help Desk

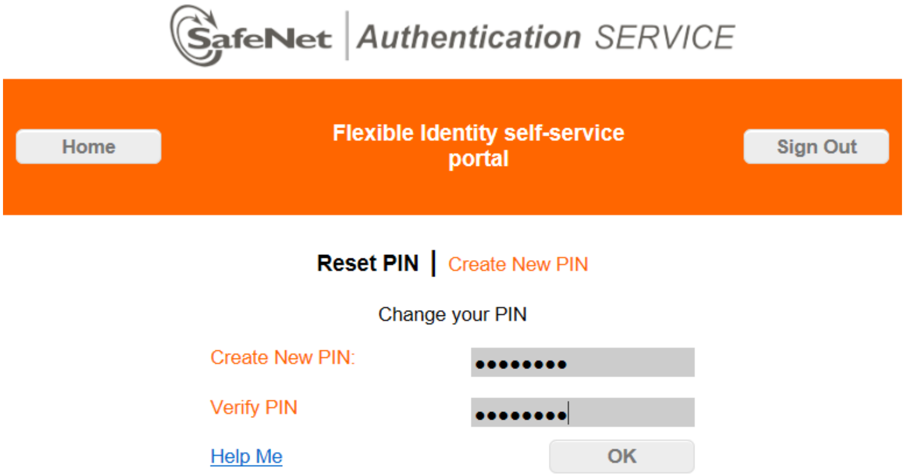
Reset PIN | Authenticate to Process

User ID: example

OTP: ●●●●●●●●●●●

Copyright © 2014. SafeNet Inc. All Rights Reserved.

⇨ Choose your PIN under use of the PIN rules in chapter 2.4.1 and click ok


SafeNet Authentication SERVICE
Home
Flexible Identity self-service portal
Sign Out
Help Me
OK

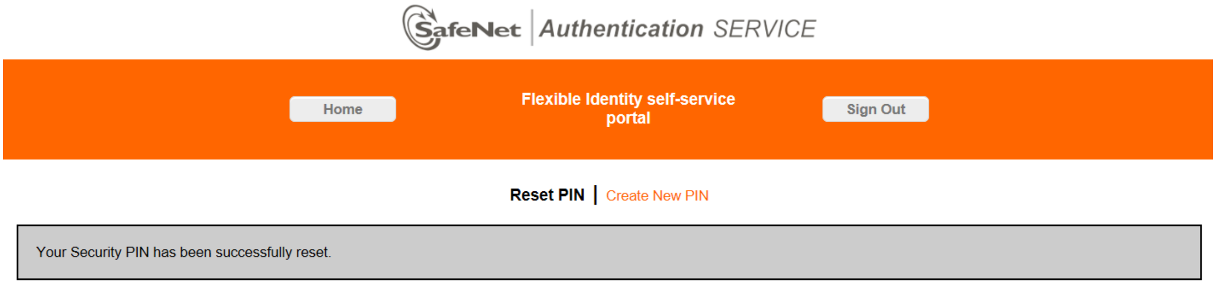
Reset PIN | Create New PIN

Change your PIN

Create New PIN: ●●●●●●●●

Verify PIN ●●●●●●●●

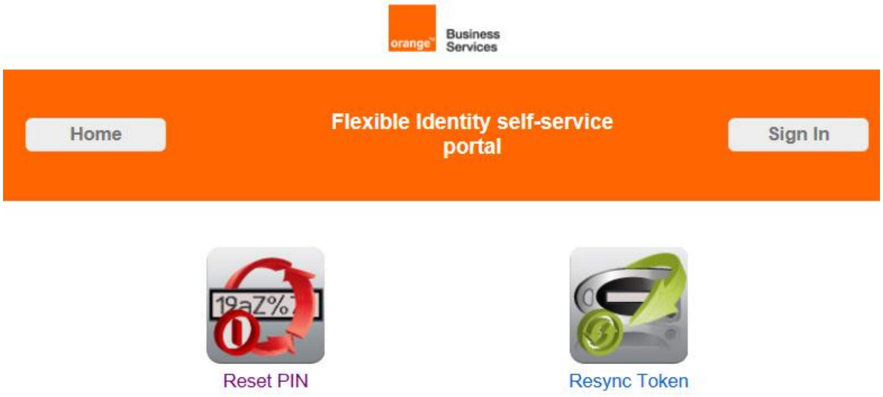
⇨ In case of correct setup the system confirmed the success


SafeNet Authentication SERVICE
Home
Flexible Identity self-service portal
Sign Out

Reset PIN | Create New PIN

Your Security PIN has been successfully reset.

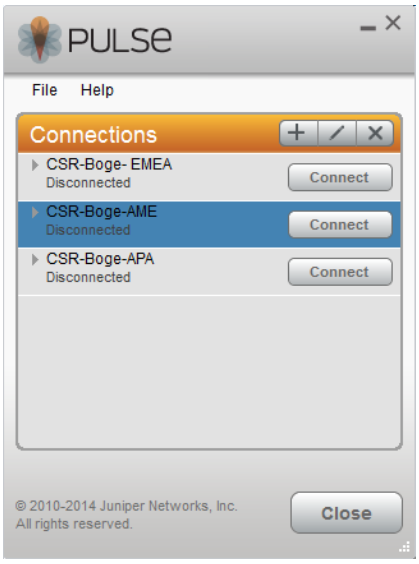
⇨ Click sign out to leave the selfservice portal

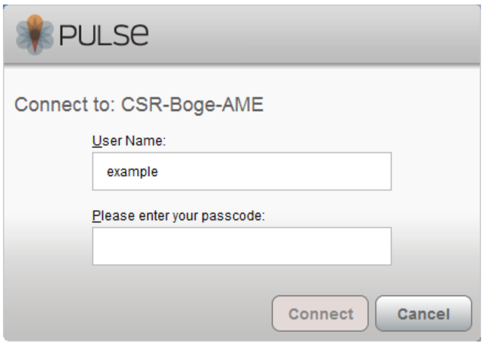


4.2. New Pin mode

If you do not know your PIN your are pleased to go in touch with your Berry Helpdesk . The helpdesk set your account in new PIN mode and tells you a four digit and temporarily PIN.Start the Junos Pulse using all programs > BerryRemote > Junos Pulse and choose the link to your home gateway e.g. "CSR-Boge- AME" and press connect.

Type in your Username and then the passcode.



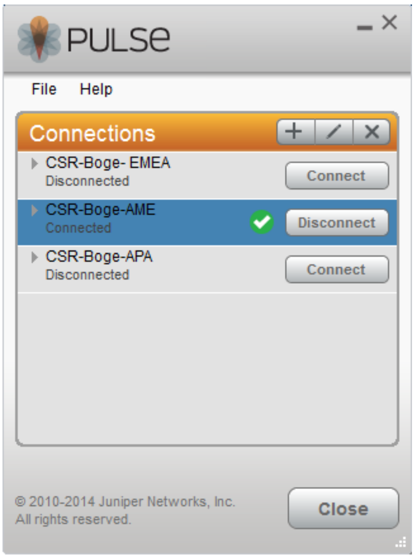


Connect to: CSR-Boge-AME

User Name: example

Please enter your passcode:

Passcode= temporarily PIN + Tokencode without any blank between.



CSR-Boge- EMEA
Disconnected

CSR-Boge-AME
Connected

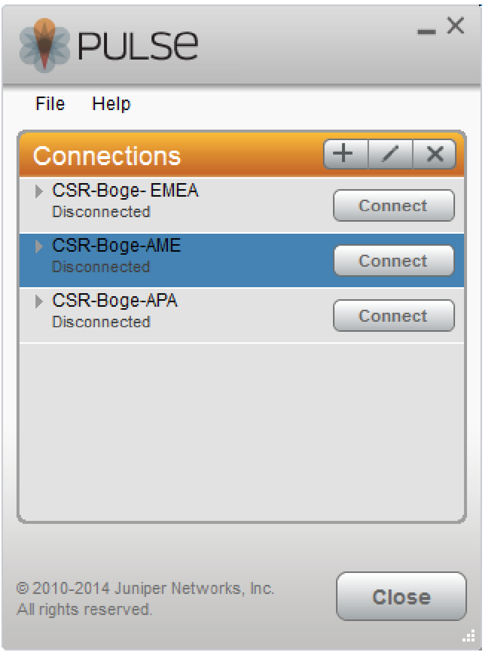
CSR-Boge-APA
Disconnected

© 2010-2014 Juniper Networks, Inc.
All rights reserved.

If the PIN is accepted you are connected to the Berry Network

5. Connecting the Berry Network

5.1. Connecting to the VPN gateway



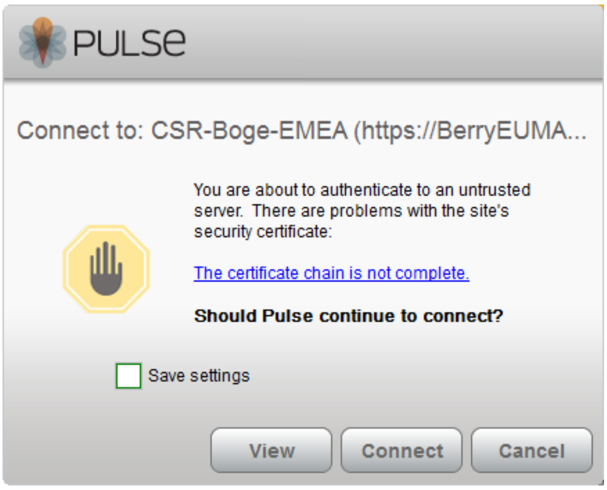
CSR-Boge- EMEA
Disconnected

CSR-Boge-AME
Disconnected

CSR-Boge-APA
Disconnected

© 2010-2014 Juniper Networks, Inc.
All rights reserved.

Now open the connection to your CSR-Boge region (EMEA, AMERICA, APA). Contact the helpdesk if you are not sure to which region you must log in.



Connect to: CSR-Boge-EMEA (https://BerryEUMA...

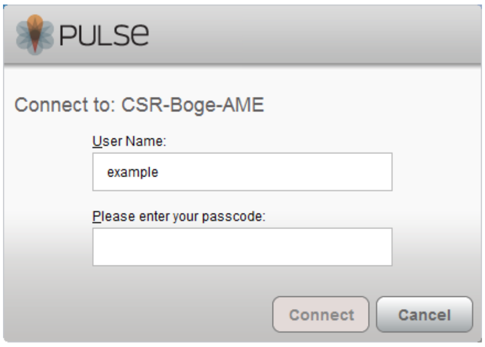
You are about to authenticate to an untrusted server. There are problems with the site's security certificate:

The certificate chain is not complete.

Should Pulse continue to connect?

□ Save settings

If this screen appear choose your domain and click on connect to go further on.



Connect to: CSR-Boge-AME

User Name: example

Please enter your passcode:

Fill in your credentials to complete the connection.

User Name: Use your user name which was given in the enrollment.

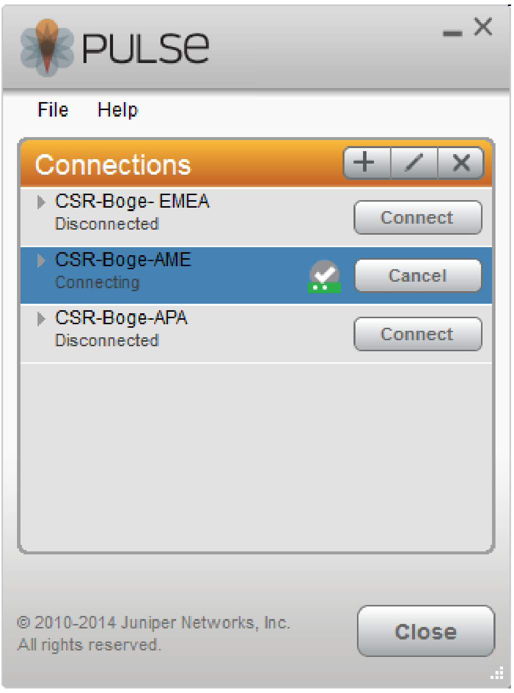
Passcode= PIN + Tokencode without any blank between

- **Tokencode** – how to get it:

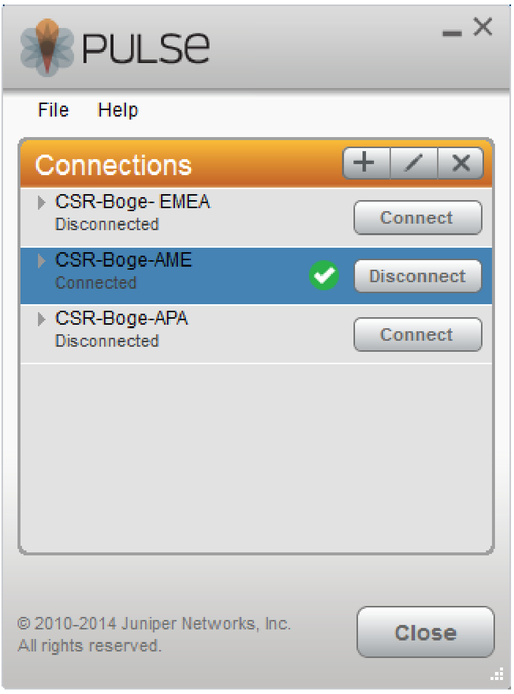
Click the button at your Cryptocard and readout the displayed tokencode

- **PIN**

as defined in the enrollment phase.

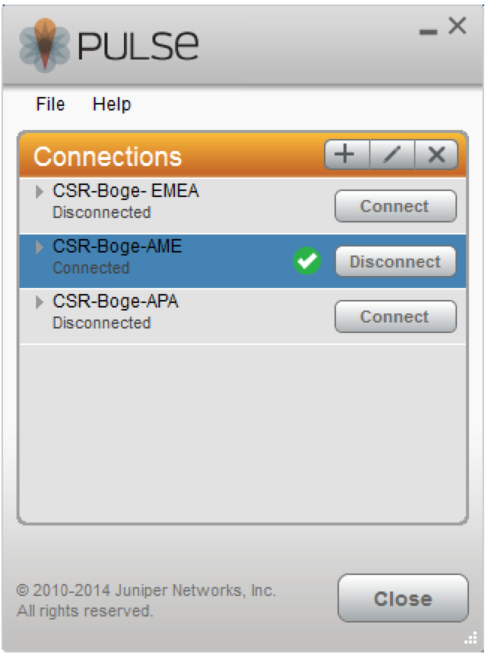


If Username and the passcode correct the Junos Pulse try to connect the gateway visible with “running dots”. In case of issues read chapter 5.2.



Green symbol shows the successful connection to the network.

5.2. Disconnecting from VPN gateway



You can disconnect from the Remote once you have finished your work or no longer require Remote VPN connection. In the "Junos Pulse" program, click "Disconnect".

5.3. Connection rules

5.3.1. Idle Time (Non activity timer) = 60 minutes

The system interrupt if there is no data traffic via the remote connection. 5 minutes before a reminder appears. The session can extend to a further period.

5.3.2. Max Session length = 24 hours

A session is interrupted after 24 hours. 5 minutes before a reminder appears. The session can extend to a further period

5.3.3. Reauthentication after break within 5 minutes not neccessary

When a connection is interrupted or the computer is used by e.g. connecting LAN to a wireless network, the maximum interrupt time without authentication is 5 minutes.

6. Troubleshooting and Assistance

6.1. Helpdesk (IT hotline)

All locations

Phone extension: 3600

6.2. Gateway does not response

- Check if your computer have access to the Internet using www.google.com, etc.
- Check if your gateway is reachable with a Ping command. The destination IP’s are shown in chapter 7
- Check the information in chapter 7

7. VPN connections via firewall systems

Before you can connect to the Berry network, the following ports and/or IP addresses must be enabled:

53	DNS (name resolution)
443	SSL (also referred to as https)

DNS name	Gateway IP	Domain
https://BerryEUMA.flexiblessl.com/core	194.3.138.20	EMEA
https://berryAME.flexiblessl.com/core	57.77.24.131	AMERICA
https://BerryAPA.flexiblessl.com/core	57.73.40.134	APA

If you are in a non-Berry network, you may encounter connection problems caused by disabled network ports. In this case, please contact the responsible network administration.