Created by **Lindhoudt Harald** Date of Creation **May 12th, 2010**

Released by **Glatz Klaus** Date of Release **May 21st, 2010**

TABLE OF CONTENT

1. General Description

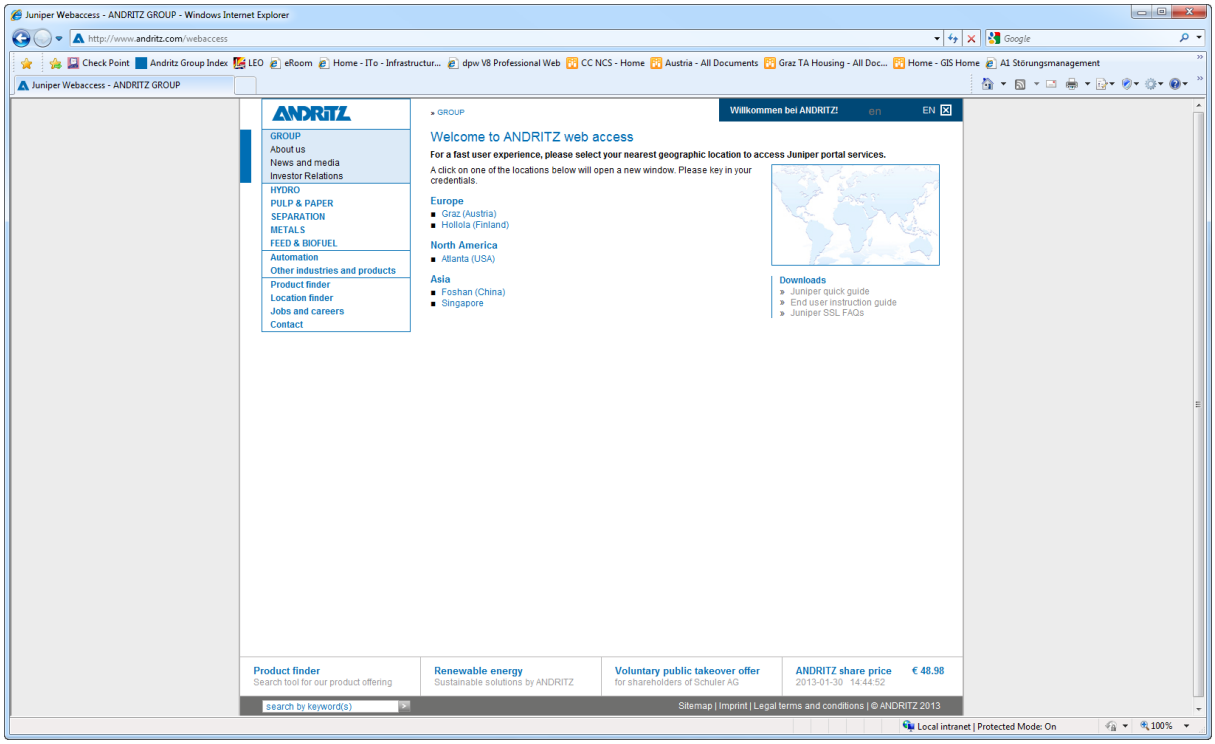
This instruction manual describes the use of Portal Services provided for the Andritz Group.
With the described methods it's possible to check your email or work with different applications from all around the world.
This solution replaces the "Check Point Secure Client" application and Microsoft VPN features.
To connect to the Portal Services you are only required to have internet connection, this can be either an internal or external connection.

Portal Services are meant to be used from external locations to provide you with a secure connection to internal IT Services and Applications.

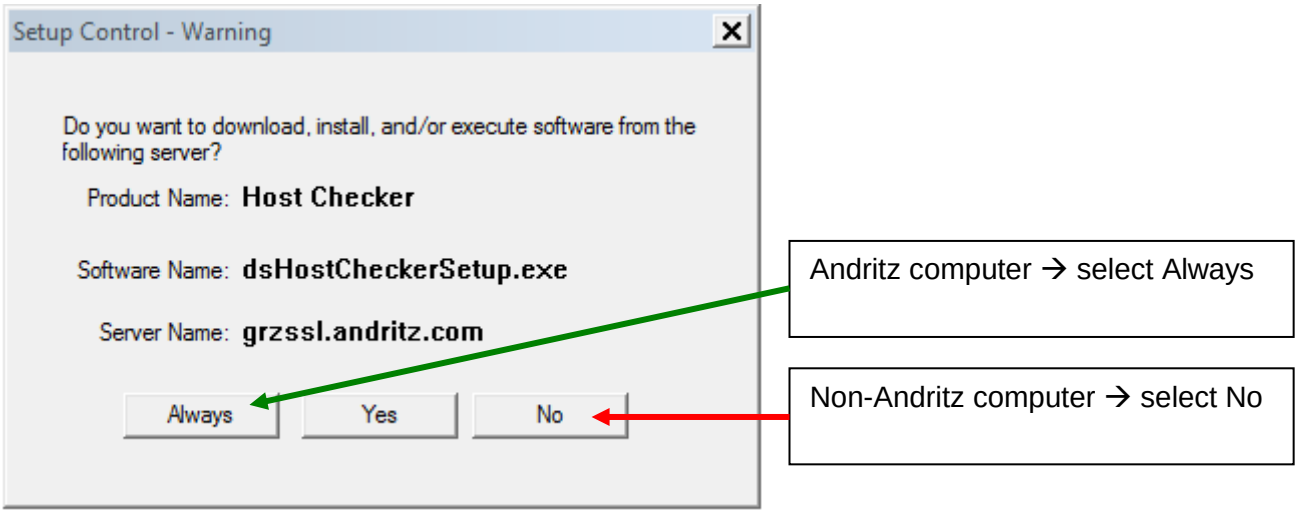
2. End-user Portal Services instructions

2.1 How to Log in to Portal Services

To log in to Portal Services use the following URL: http://www.andritz.com/webaccess. Please choose the geographically closest Portal (Graz, Hollola, Atlanta, Foshan or Singapore) to get the fastest connection and lowest latency.

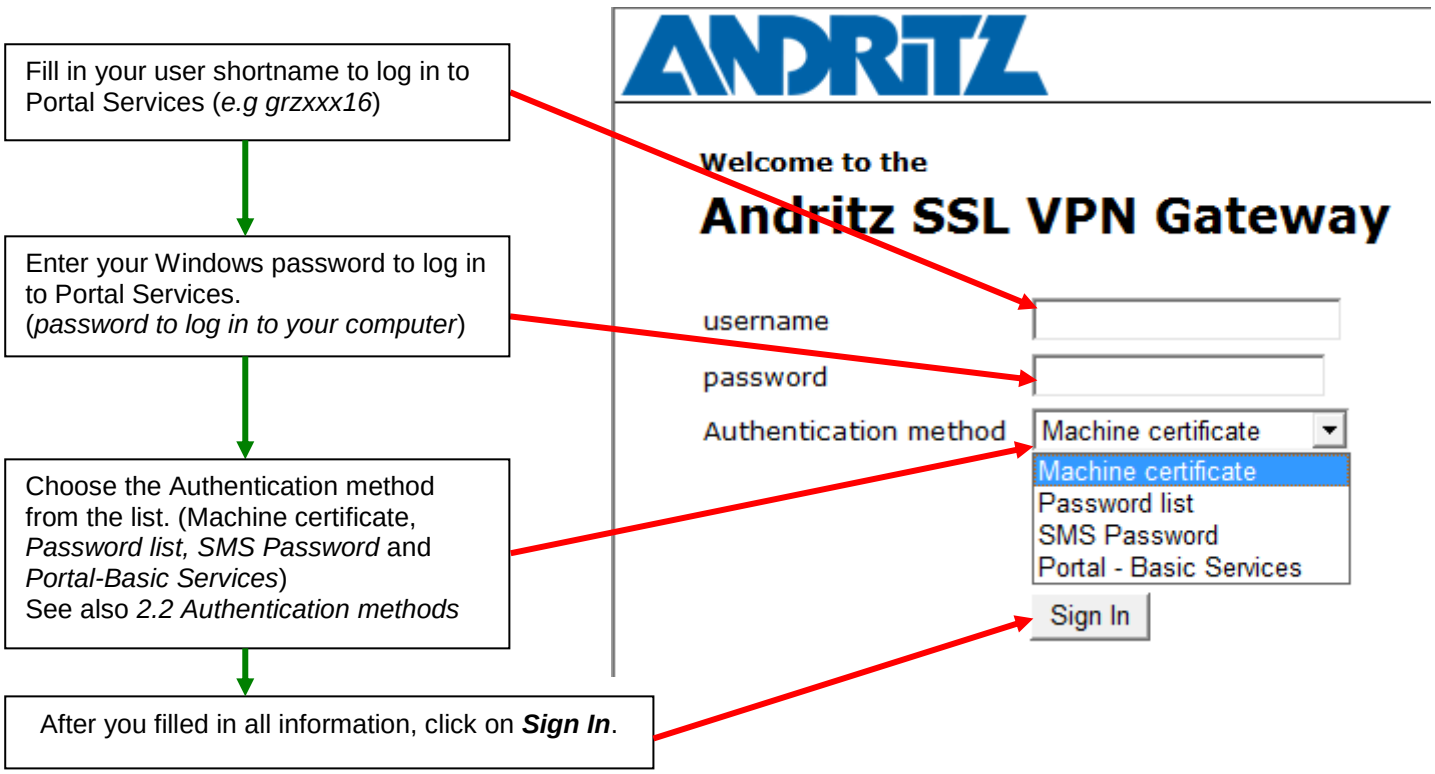


After the portal is chosen, the Host Checker will try to check the client machine. If the client machine is non-Andritz computer, it is suggested to select “No” to a following dialog (if Yes/Always is selected, it takes more time to download and install Host Checker and the result is still the same):



If the client is Andritz computer, Host Checker should be allowed to perform checks on the host. Then “Always” selection is the most suitable way to use, as this question will not be asked again if Juniper configuration is not changed. Host Checker is performed only once and it does not check the client machine again after the authentication.

On the following screen you have to fill in all information to log in to Portal Services Gateway:



2.2 Authentication methods

The portal offers two levels of access:

- **Strong authentication:**
  Machine certificate, Password List and SMS Password (*see the description below). This access works only by using computers integrated into the Andritz IT infrastructure.
  This Level gives you an access to all portal functions, this includes also a full network connect.
- **Portal - Basic Services:**
  This Level gives you only access to the standard portal services. In case you don't use an Andritz issued computer or network access fails; you can reach some services (e.g. Outlook Web Access).

Strong Authentication:
Andritz is enhancing the security of remote connections by using two-factor or "strong" authentication. Standard authentication is when you supply a user name and a password. Using standard authentication from public terminals, computers at home or while connected with unsecured wireless networks can easily expose this information and allow unauthorized access to the Andritz network.

Two-factor or strong authentication combines the standard user name and password with a one-time password generated by the system.
This can be either be from a password list that you keep with you, or the password is sent to you via mobile phone as a SMS message. This makes it much more difficult for someone who gets your user name and password to use that information to gain full access to the network. Machine certificate verifies that the computer that is used for signing in has a certificate that is provided by Andritz. This means the certificate is delivered only into the Andritz computers and certificate itself cannot be copied or moved to another computer. Machine certificate option is available only to Andritz computers that have passed the Host Checker certificate check before the login page is displayed. Machine certificate does not currently require any two-factor authentication (Passcode list or SMS Password); only username and password is enough for signing in.

The basic portal services do not require this stronger authentication. However, full VPN connections and other more sensitive portal applications will NOT be available unless you are using one of the strong authentication methods.

Please note that the recommended strong authentication method is the Machine certificate because it creates no costs. If the computer does not have an option of Machine certificate, Passcode list is preferred. Please use this method if available before the SMS Password method.

With these three strong authentication methods (Machine certificate, Password list and SMS Password) you can get full access to all Andritz resources that you have permission to use. This includes the network connect feature which is much like the Check Point and MS VPN clients being replaced.
With the Portal - Basic Services we just provide Web based Portal Services like Outlook Web Access, SPAM Quarantine and Intranet. These applications should work on any standard browser.

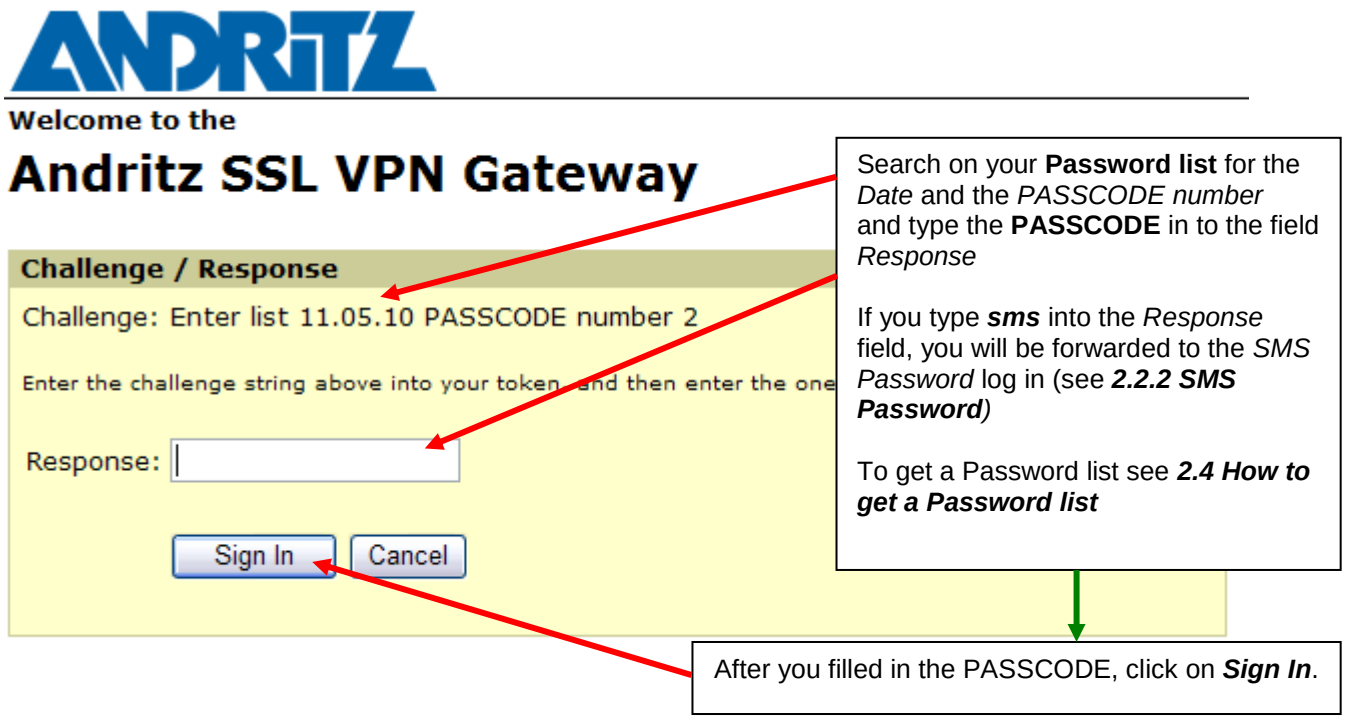
2.2.1 Machine certificate:

With this authentication method you have the all the same options that are also provided via Password list and SMS Password. Please notice that your computer must pass the required requirements such as McAfee virus scanner must be up-to-date.

Just log in with your company *shortname* (e.g. grzxxx12) and your *Windows password* (password to log in to your PC).

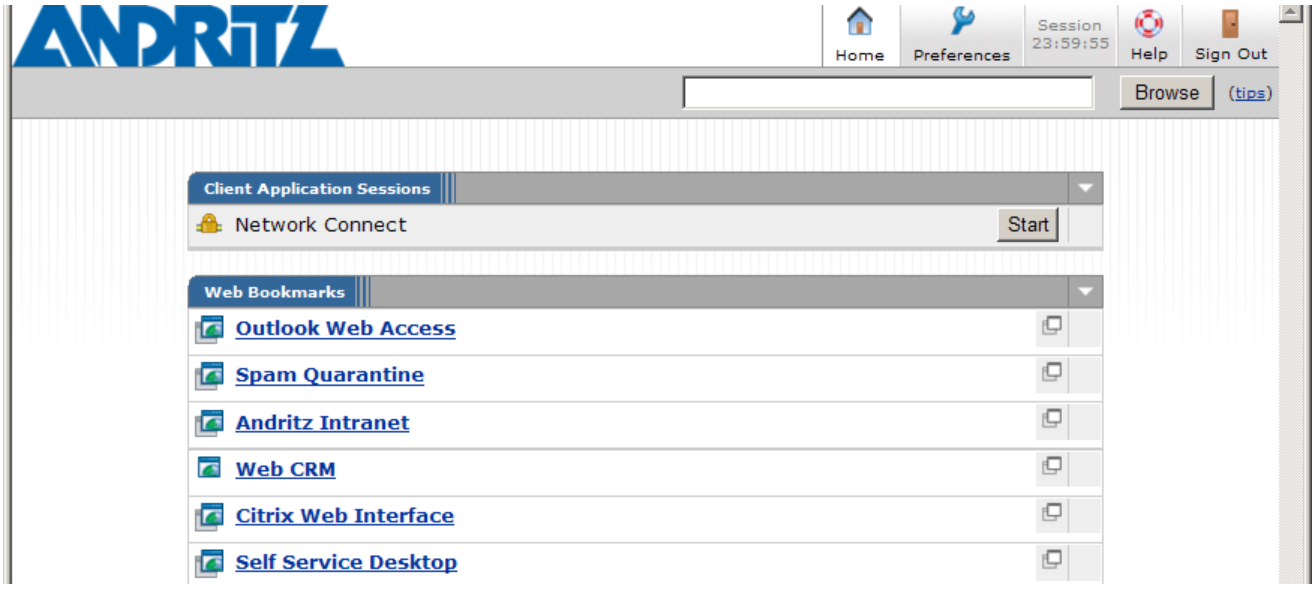
2.2.2 Password list:

After signing in you will be forwarded to this site



After the sign in your computer will be checked to assure it meets our security standards. This may take a few minutes the first time you connect. If all requirements are fulfilled you can use all features. If the PC does not meet the requirements (Home PC, public terminal) Network Connect will not be provided to you.

After your PC was checked and proven secure, you will be directed to this site:



2.2.3 SMS Password:

After signing in you will be forwarded to this site:

After the sign in your computer will be checked to assure it meets our security standards. This may take a few minutes the first time you connect. If all requirements are fulfilled you can use all features. If the PC does not meet the requirements (Home PC, public terminal) Network Connect will not be provided to you.

2.2.4 Portal – Basic Services:

With this authentication method you have the option for basic services (*Outlook Web Access, Spam Quarantine, Intranet and Citrix Web Interface*).

Just log in with your company *shortname* (e.g. grzxxx12) and your *Windows password* (password to log in to your PC).

2.3 Using the Portal Services Interface

If you are opening Portal – Basic Services with non-Andritz computer, it is suggested to skip the Host Checker installation by clicking “No” to download dialog. If “Yes or Always” is selected, download and installation process will take a while and the result is the same as clicking “No”. This is because the Host Checker will notice if the computer is part of Andritz or not.

If you are authenticated you are able to reach the services offered by the Portal:

The Applications listed are:

Network Connect (only with strong authentication)

Outlook Web Access
Spam Quarantine
New Password List
Andritz Intranet
Web CRM
Citrix Web Interface

Network Connect: Network Connect will replace the current VPN solutions (Check Point Secure Client and MS VPN) used to connect to the Andritz Network. To use Network Connect see *2.3.1 How to use Network Connect*

Outlook Web Access: To reach Outlook Web Access to check email please click this link.

Spam Quarantine: You can open your Spam quarantine by clicking the Spam Quarantine link to manage your blocked E-Mails.

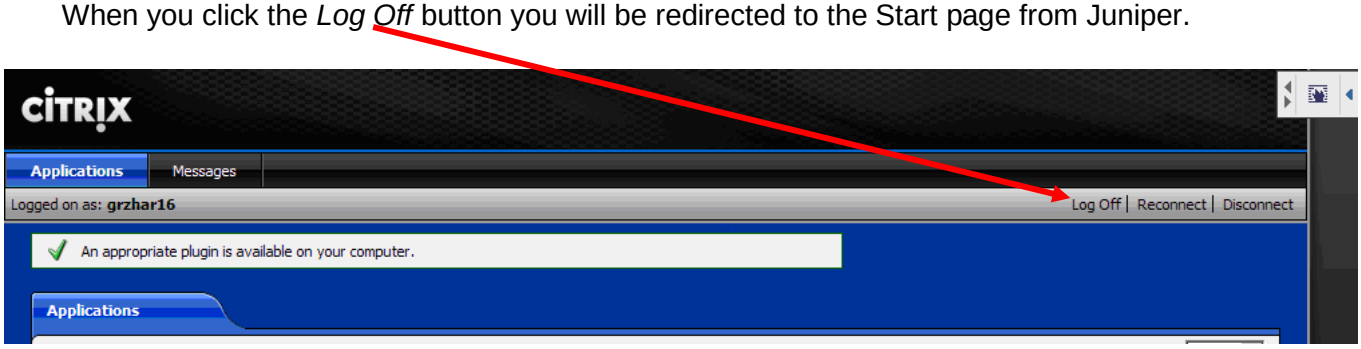
New Password List: You can generate a new password list (See also section *2.4 How to get a Password list*)

Andritz Intranet: The Andritz Intranet is available with this link.

Web CRM: By clicking this link you get access to the CRM System.

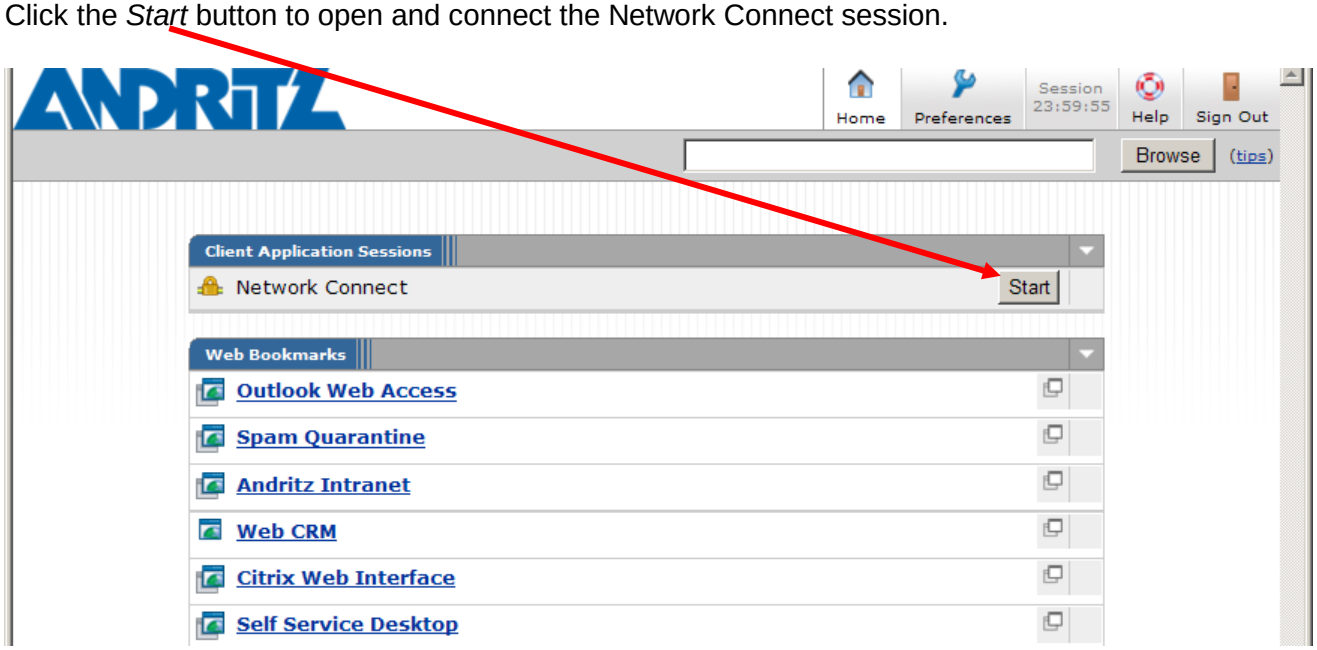
Citrix Web Interface: By clicking Citrix Web Interface link you will be redirected to your Citrix listed Applications.

When you click the *Log Off* button you will be redirected to the Start page from Juniper.

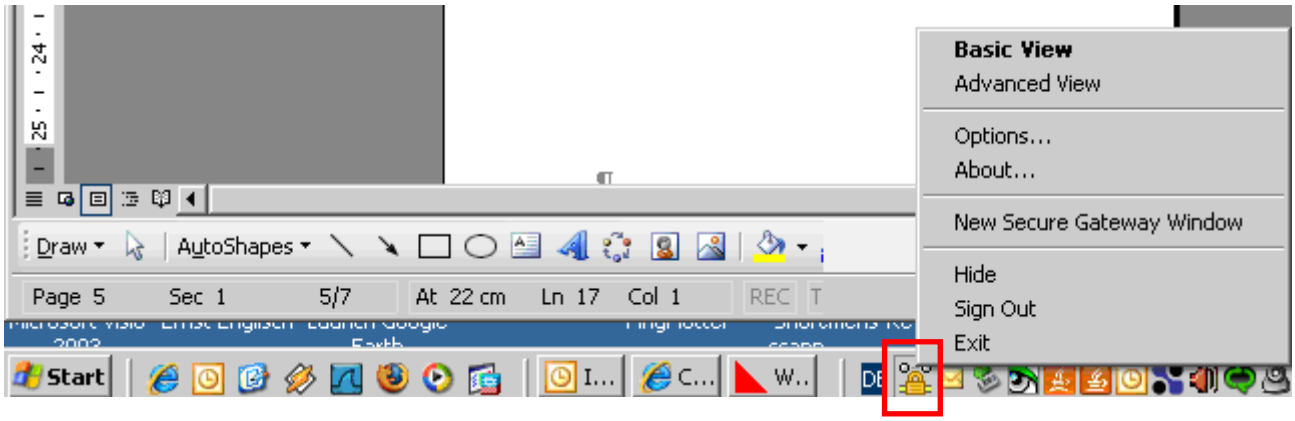


2.3.1 How to use Network Connect

Click the *Start* button to open and connect the Network Connect session.



To disconnect from the Network Connect click *right* mouse button on top of the ***Network Connect Icon*** on the taskbar (inside the **red box**) and select *Sign Out* from the appearing list.



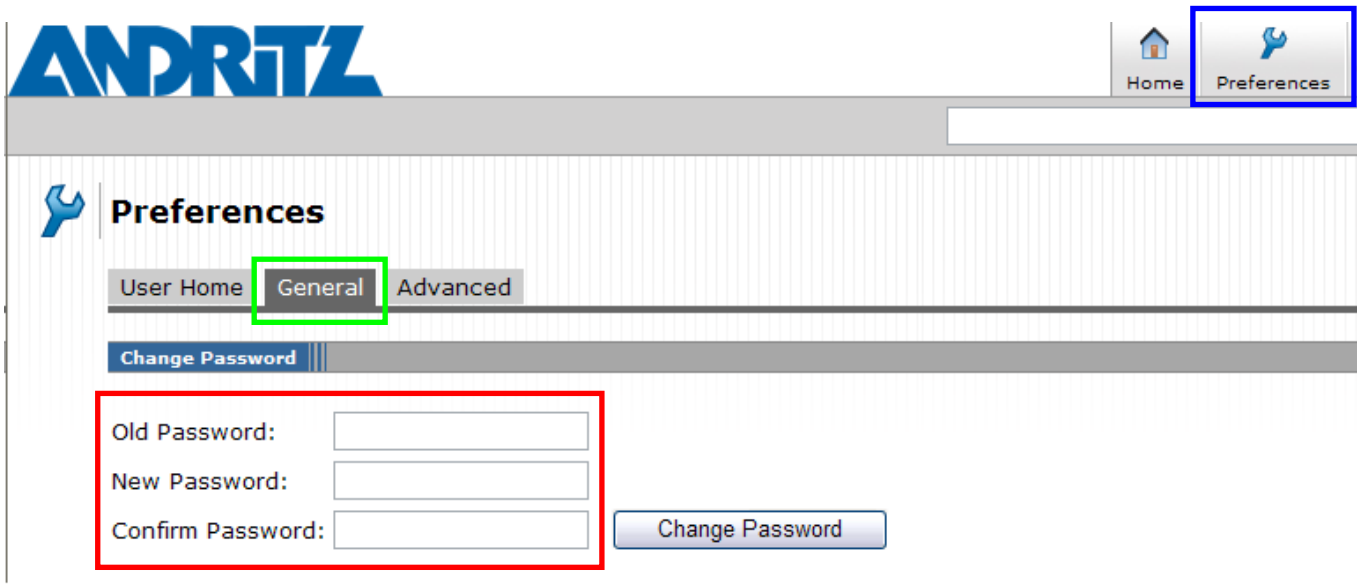
2.3.2 How to change the Windows password via Portal Services

To change the Windows password click on Preferences on the Toolbar (**blue box**).

Then choose the register General (**green box**)

You will get to the page below. Fill in your old and your new password twice **(red box)** and click on *Change Password*, to change your Windows password.

Please consider the existing password Policy:
Enforce password history: 24 passwords remembered
Maximum password age: 60 days
Minimum password age: 1 day
Minimum password length: 10 characters
Password must meet complexity requirements: Enabled
Complexity requirements:
Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least 10 characters in length
Contain characters from three of the following four categories:
1. English uppercase characters (A through Z)
2. English lowercase characters (a through z)
3. Base 10 digits (0 through 9)
4. Non-alphabetic characters (for example !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.



2.4 How to get a Password list

2.4.1 How to get the first Password list

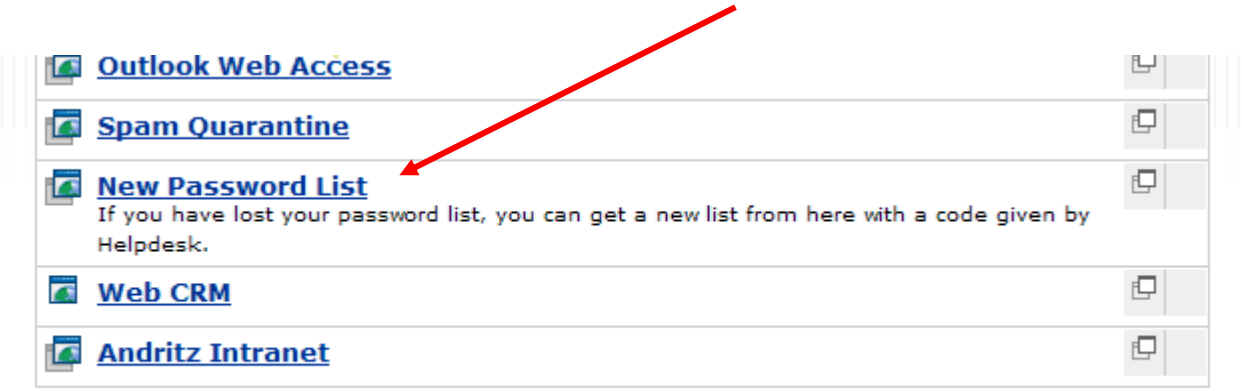
You will receive the first password list to your mobile phone and email when you are authenticating to Portal Services with *SMS Password* or *Password list*.
If you don't have a mobile phone, you can cancel the sign out after the response page; sign in to *Portal – Basic Services* (with your *shortname* (e.g. grzxxx12) and download the password list from Outlook Web Access.

If you have lost your Password list, then you have to contact your regional Help Desk.
Ask them to generate a new list for you.

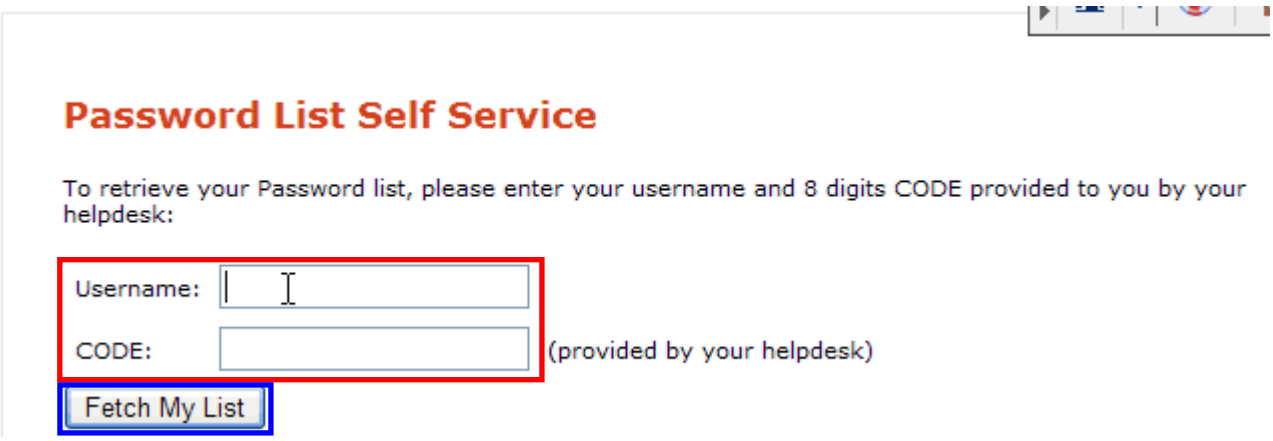
The new list can be sent to
- your email and/or
- your company mobile phone and/or
- use a code to download the list to your PC as a PDF.

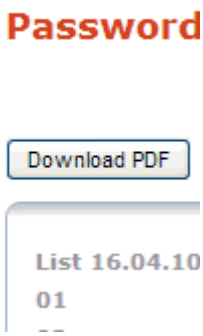
If you choose to download the list as a PDF you will get a code from the Help Desk.
Please log in with your company *shortname* (e.g. grzxxx12), your *Windows password* and the Authentication method *Portal-Basic Services*.

On the Juniper SSL interface click on *New Password List* to download the PDF file.



You will be forwarded to the page below.
Please fill in your company *shortname* (e.g. grzxxx12) and the *CODE* provided by your helpdesk. (**Red box**)
Then Click on *Fetch My List (**Blue box**)*





Click on *Download PDF* to save the Password list on your PC.

When finished, select Logout and close the browser window

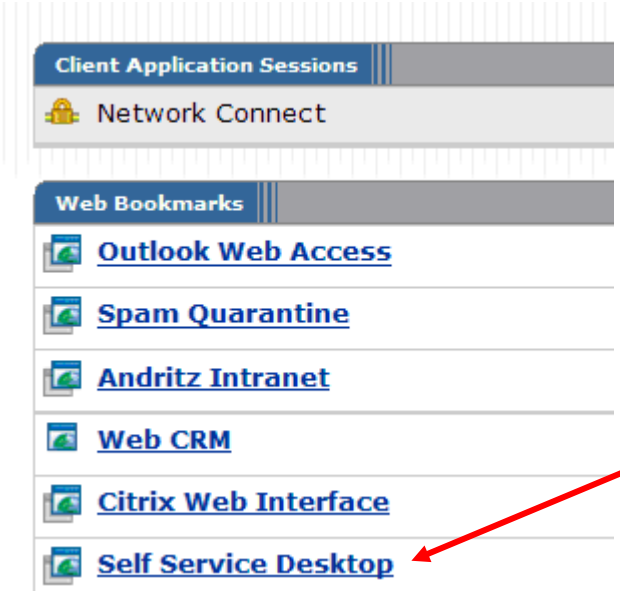
2.4.2 How to generate a <u>new</u> Password list

Normally, as soon as you use your last password from the list, a new list will be generated and sent to your mobile phone and email.
Note: If you create a new password list, the previous list is invalid and not usable.

If you need to generate a new list manually for some reason, there are two possibilities.

The first possibility is to generate the new Password list by yourself if you think your list has been compromised or misused.

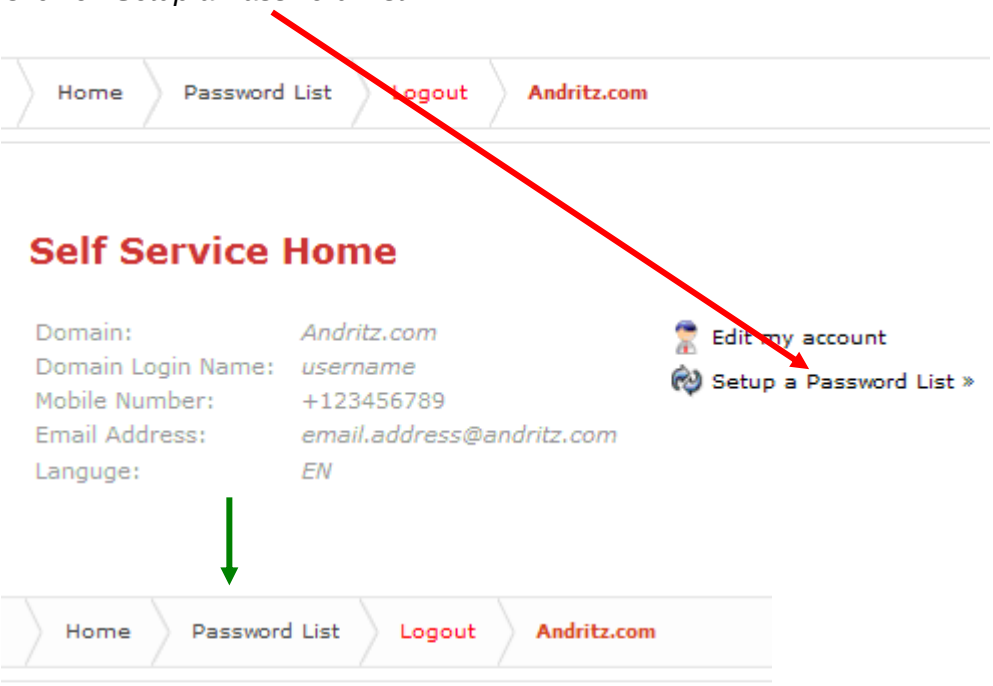
To generate the new Password list by yourself; once you are logged into the Juniper SSL Gateway with your company *shortname* (e.g. grzxxx12) and *Windows password* with the Authentication method *Password list* or *SMS Password*.

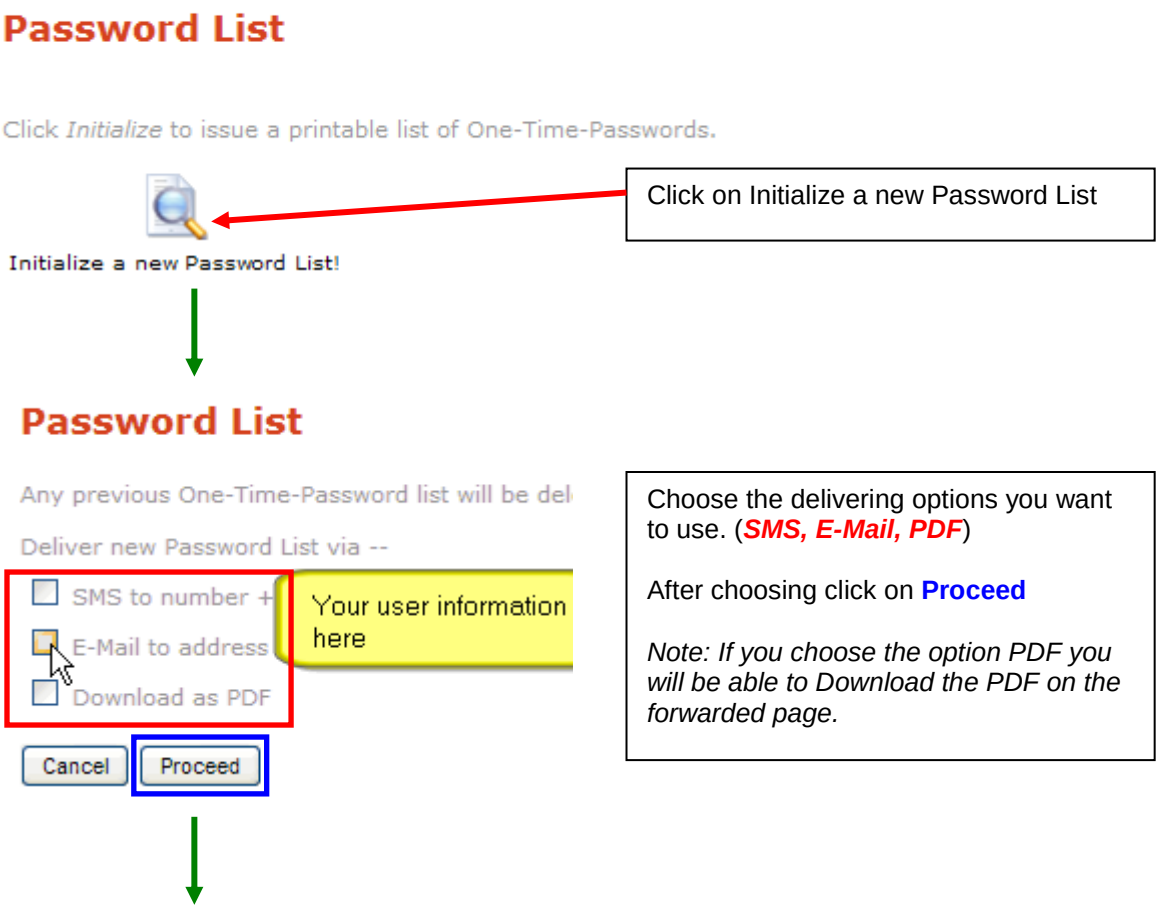


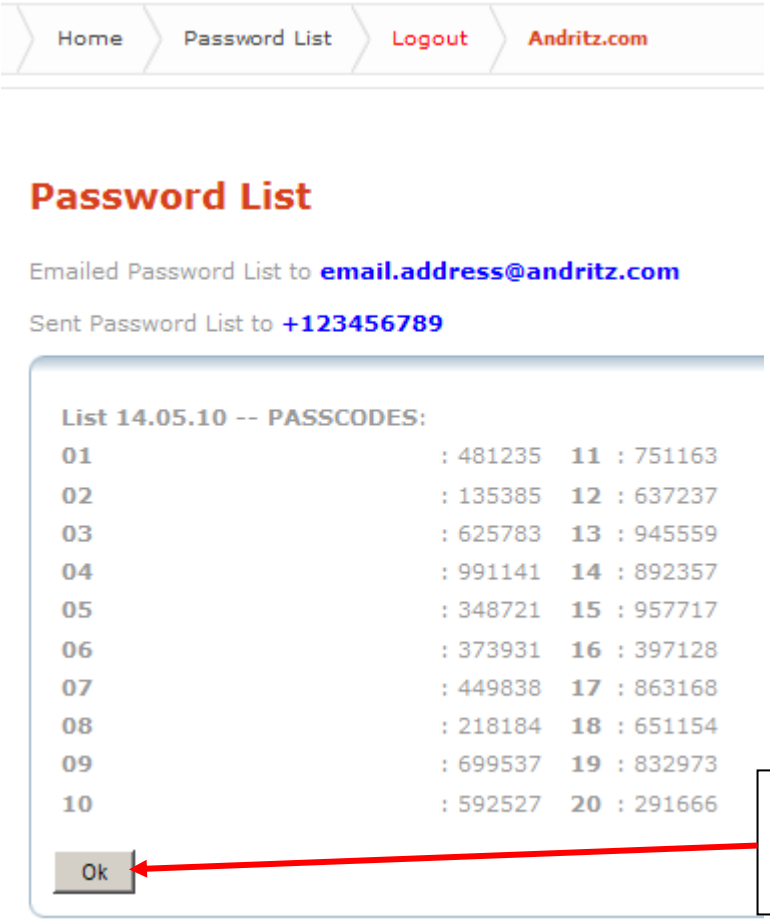
On the Interface click on *Self Service Desktop*.

A new window will open.

Click on *Setup a Password List*







Click Ok to return back to the main page of Self Service Desktop.

The second possibility is to contact Help Desk and ask them to renew your password list. See more information from [2.4.1 How to get the first Password list]