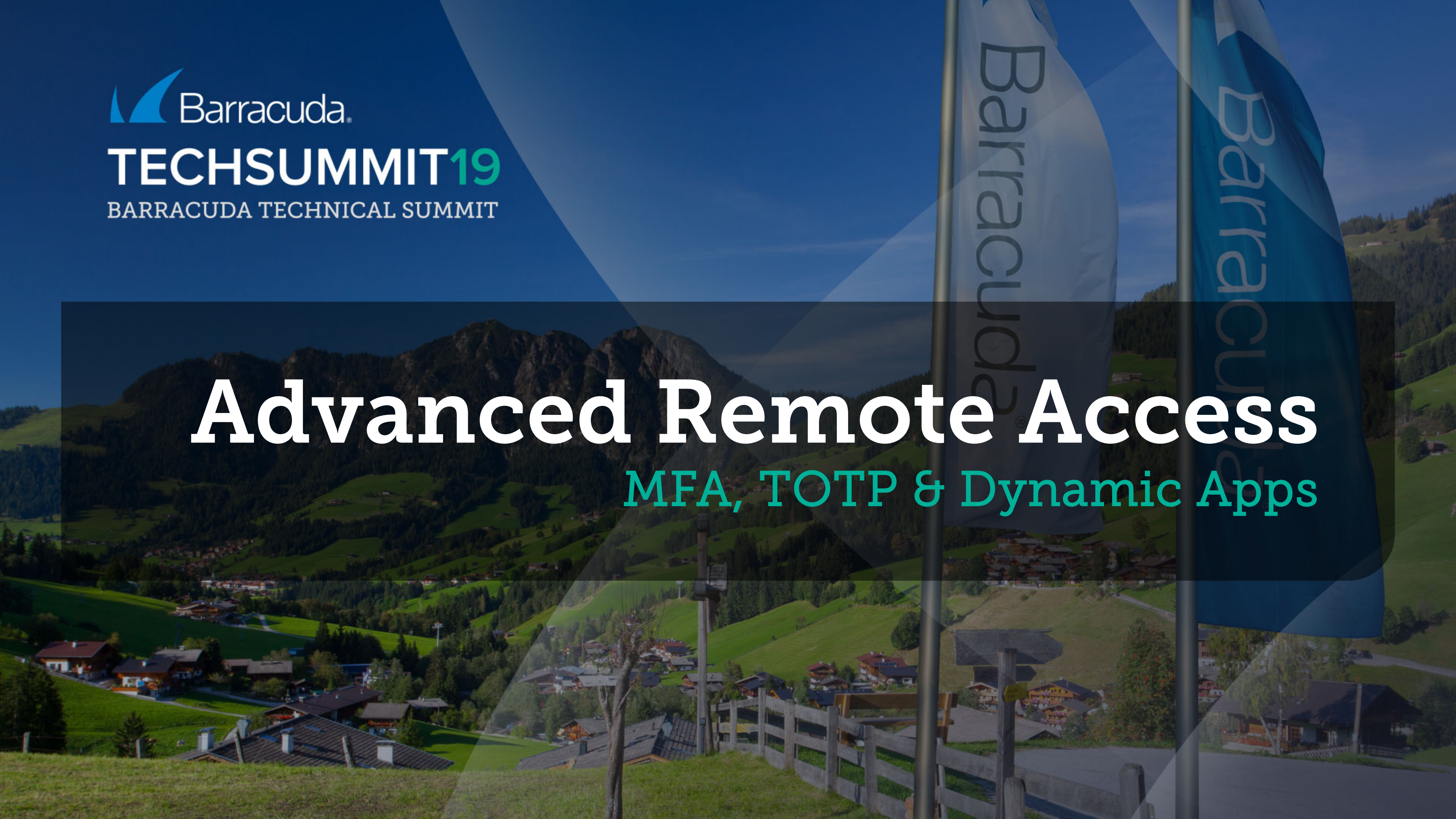


Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

Advanced Remote Access

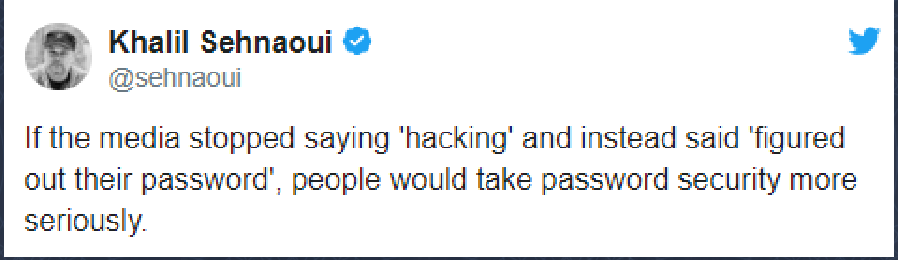
MFA, TOTP & Dynamic Apps

Agenda

- Introduction
  - Why - Tim
  - What the end-user sees – Tim
  - Licensing - Tim
- Setup
  - Self Enrollment - Jon
  - Bulk Enrollment - César
  - TINA VPN - Michael
  - VPN profiles - Michael
- SSL VPN dynamic apps – Jon
- What next?
- Q&A

Introduction

Why passwords suck



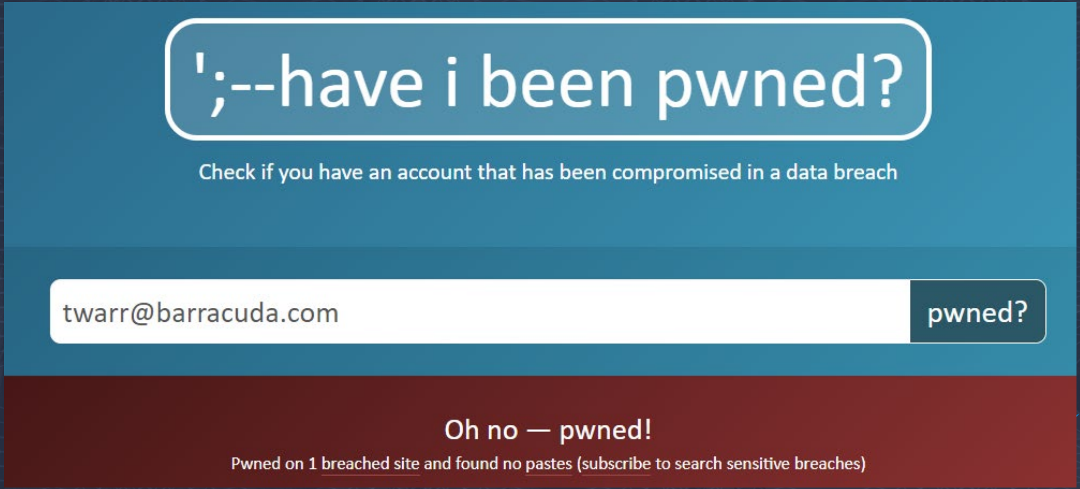
Khalil Sehnaoui
@sehnaoui

If the media stopped saying 'hacking' and instead said 'figured out their password', people would take password security more seriously.

Weak passwords

Phishing

Reused passwords



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

twarr@barracuda.com

Oh no — pwned!

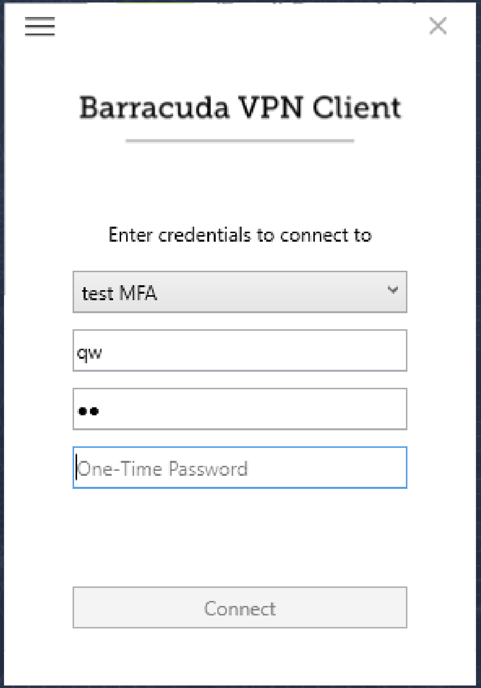
Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

Why MFA & TOTP

- Protect accounts and data
  - Re-used or weak passwords ∴ need extra protection layer
  - Something you know (e.g. password) + something you have (e.g. mobile app)
- Recommended by security experts
- Familiar consumer tech
  - e.g. online banking

Remote access clients with MFA/TOTP

VPN Client



Barracuda VPN Client

Enter credentials to connect to

test MFA

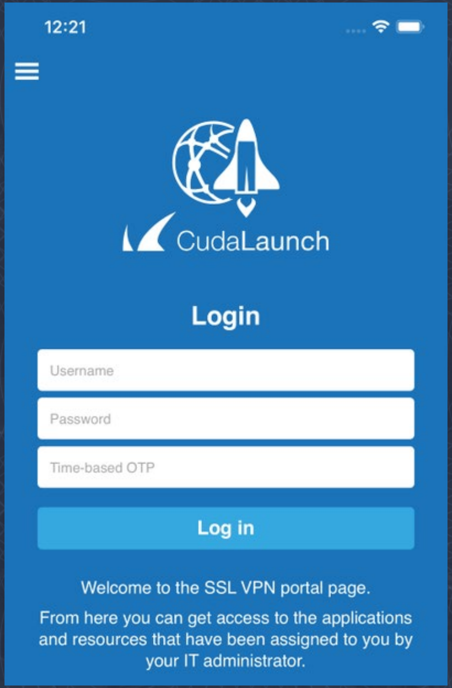
qw

••

One-Time Password

Connect

CudaLaunch



12:21

CudaLaunch

Login

Username

Password

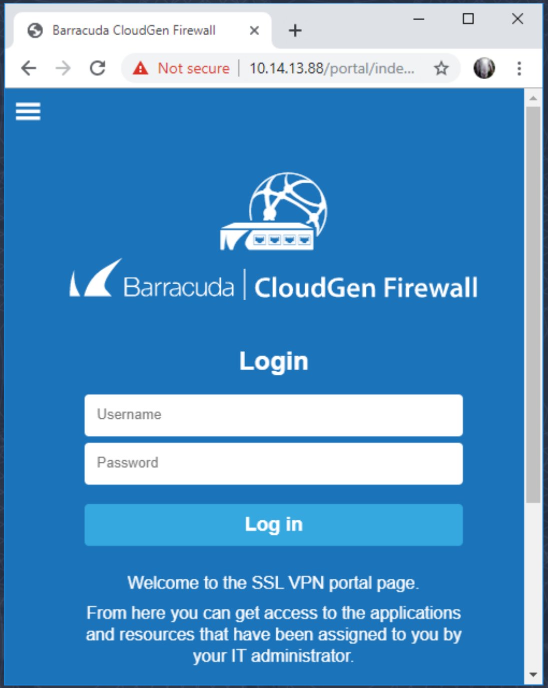
Time-based OTP

Log in

Welcome to the SSL VPN portal page.

From here you can get access to the applications and resources that have been assigned to you by your IT administrator.

SSL VPN



Barracuda CloudGen Firewall

Not secure | 10.14.13.88/portal/inde...

Barracuda | CloudGen Firewall

Login

Username

Password

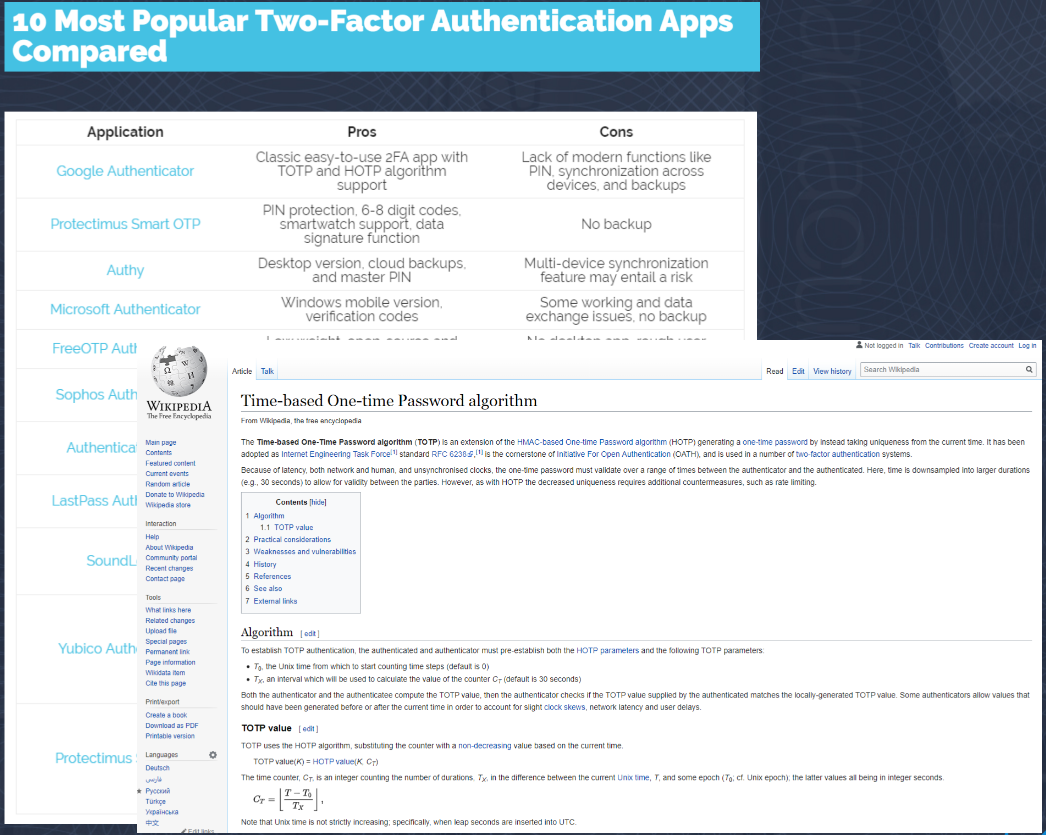
Log in

Welcome to the SSL VPN portal page.

From here you can get access to the applications and resources that have been assigned to you by your IT administrator.

We use TOTP standard RFC 6238

- Requested by customers
- Many $0 TOTP clients
- Consumer IT experience
- No expensive tokens
- Works offline
- No SMS or response wait
- No risk of phone porting



10 Most Popular Two-Factor Authentication Apps Compared

Application	Pros	Cons
Google Authenticator	Classic easy-to-use 2FA app with TOTP and HOTP algorithm support	Lack of modern functions like PIN, synchronization across devices, and backups
Protectimus Smart OTP	PIN protection, 6-8 digit codes, smartwatch support, data signature function	No backup
Authy	Desktop version, cloud backups, and master PIN	Multi-device synchronization feature may entail a risk
Microsoft Authenticator	Windows mobile version, verification codes	Some working and data exchange issues, no backup
FreeOTP Auth	Low weight, open source and	No desktop app, rough user
Sophos Auth		
Authentica		
LastPass Auth		
SoundL		
Yubico Auth		
Protectimus		

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Deutsch
فارسی
Русский
Türkçe
Українська
中文
Edit links

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

Time-based One-time Password algorithm

From Wikipedia, the free encyclopedia

The **Time-based One-Time Password algorithm** (**TOTP**) is an extension of the HMAC-based One-time Password algorithm (HOTP) generating a one-time password by instead taking uniqueness from the current time. It has been adopted as Internet Engineering Task Force[1] standard RFC 6238,[1] is the cornerstone of Initiative For Open Authentication (OATH), and is used in a number of two-factor authentication systems.

Because of latency, both network and human, and unsynchronised clocks, the one-time password must validate over a range of times between the authenticator and the authenticated. Here, time is downsampled into larger durations (e.g., 30 seconds) to allow for validity between the parties. However, as with HOTP the decreased uniqueness requires additional countermeasures, such as rate limiting.

Contents [hide]

Algorithm [edit]

To establish TOTP authentication, the authenticated and authenticator must pre-establish both the HOTP parameters and the following TOTP parameters:

- T_0, the Unix time from which to start counting time steps (default is 0)
- T_X, an interval which will be used to calculate the value of the counter C_T (default is 30 seconds)

Both the authenticator and the authenticatee compute the TOTP value, then the authenticator checks if the TOTP value supplied by the authenticated matches the locally-generated TOTP value. Some authenticators allow values that should have been generated before or after the current time in order to account for slight clock skews, network latency and user delays.

TOTP value [edit]

TOTP uses the HOTP algorithm, substituting the counter with a non-decreasing value based on the current time.

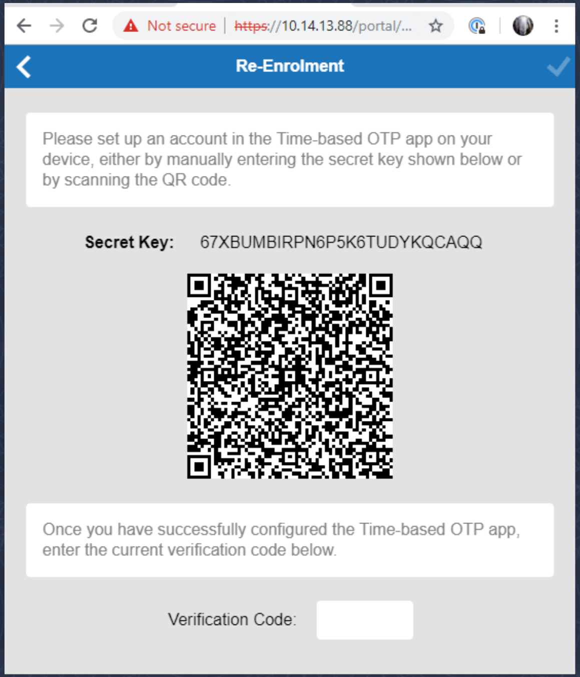
TOTP value(K) = HOTP value(K, C_T)

The time counter, C_T, is an integer counting the number of durations, T_X, in the difference between the current Unix time, T, and some epoch (T_0; cf. Unix epoch); the latter values all being in integer seconds.

$$C_T = \left\lfloor \frac{T - T_0}{T_X} \right\rfloor,$$

Note that Unix time is not strictly increasing; specifically, when leap seconds are inserted into UTC.

TOTP self enrollment or bulk enrollment



Re-Enrolment

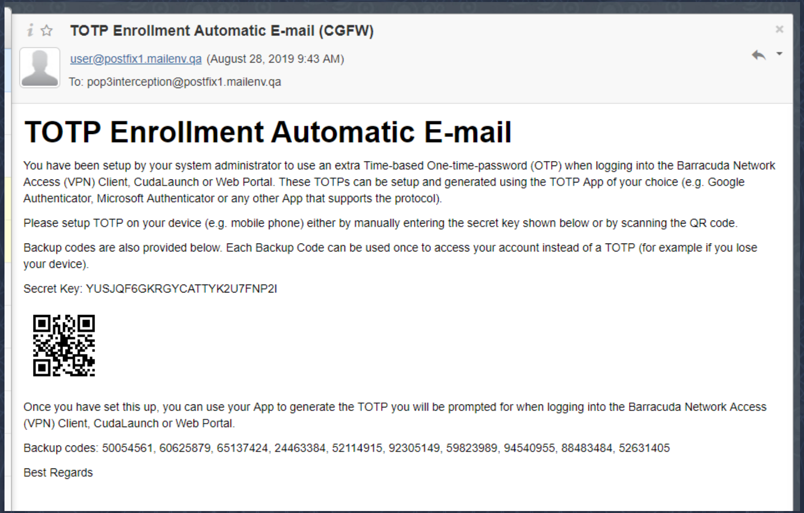
Please set up an account in the Time-based OTP app on your device, either by manually entering the secret key shown below or by scanning the QR code.

Secret Key: 67XBUMBIRPN6P5K6TUDYKQCAQQ

Once you have successfully configured the Time-based OTP app, enter the current verification code below.

Verification Code:

or



TOTP Enrollment Automatic E-mail (CGFW)

user@postfix1.mailenv.qa (August 28, 2019 9:43 AM)

To: pop3interception@postfix1.mailenv.qa

TOTP Enrollment Automatic E-mail

You have been setup by your system administrator to use an extra Time-based One-time-password (OTP) when logging into the Barracuda Network Access (VPN) Client, CudaLaunch or Web Portal. These TOTPs can be setup and generated using the TOTP App of your choice (e.g. Google Authenticator, Microsoft Authenticator or any other App that supports the protocol).

Please setup TOTP on your device (e.g. mobile phone) either by manually entering the secret key shown below or by scanning the QR code.

Backup codes are also provided below. Each Backup Code can be used once to access your account instead of a TOTP (for example if you lose your device).

Secret Key: YUSJQF6GKRGYCATTYK2U7FNP2I

Once you have set this up, you can use your App to generate the TOTP you will be prompted for when logging into the Barracuda Network Access (VPN) Client, CudaLaunch or Web Portal.

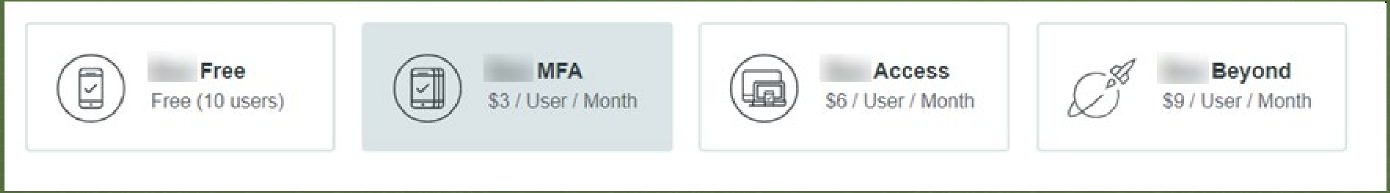
Backup codes: 50054561, 60625879, 65137424, 24463384, 52114915, 92305149, 59823989, 94540955, 88483484, 52631405

Best Regards

Licensing

Example: Specialised MFA provider

3US$ per user per month = 300 users $10800 year for just MFA



[redacted] Free Free (10 users)	[redacted] MFA $3 / User / Month	[redacted] Access $6 / User / Month	[redacted] Beyond $9 / User / Month

Barracuda: CloudGen Firewall

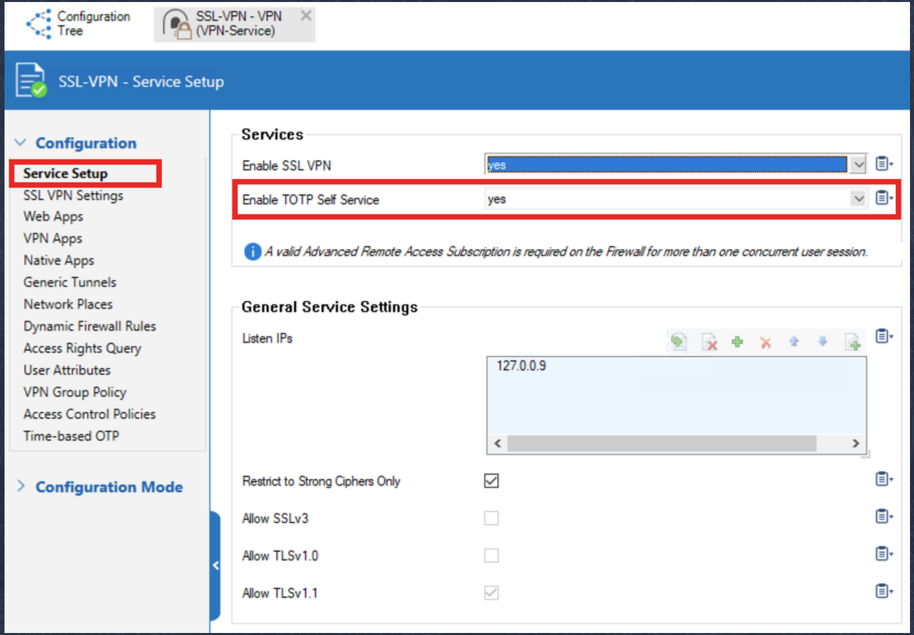
Requires **Advanced Remote Access** subscription

F400: add Advanced Remote Access 300+ users = <$1200 year.

Setup

Setup – self enrollment

Setting up the time-based OTP portal



Services

Enable SSL VPN: yes

Enable TOTP Self Service: yes

A valid Advanced Remote Access Subscription is required on the Firewall for more than one concurrent user session.

General Service Settings

Listen IPs: 127.0.0.9

Restrict to Strong Ciphers Only ☑

Allow SSLv3 □

Allow TLSv1.0 □

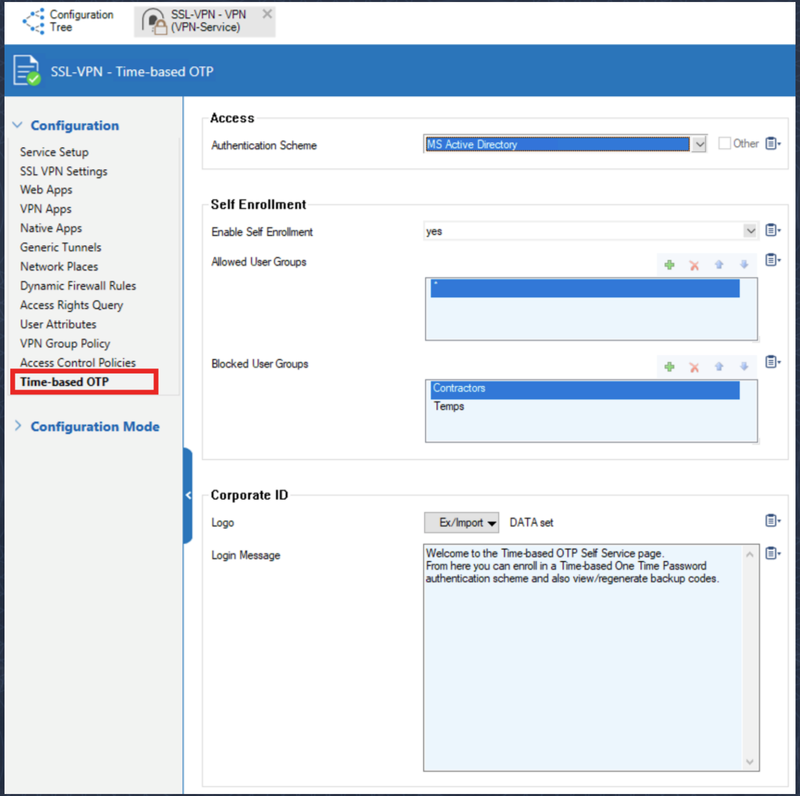
Allow TLSv1.1 ☑

The TOTP portal shares the same web service as the SSL VPN service.

They share the same IP, certificate, ciphers, etc.

You can run either service without the other.

Configuring the TOTP portal options



Access

Authentication Scheme: MS Active Directory □ Other

Self Enrollment

Enable Self Enrollment: yes

Allowed User Groups: *

Blocked User Groups: Contractors
Temps

Corporate ID

Logo: Ex/Import DATA set

Login Message: Welcome to the Time-based OTP Self Service page. From here you can enroll in a Time-based One Time Password authentication scheme and also view/regenerate backup codes.

Choose authentication scheme – independent of SSL VPN

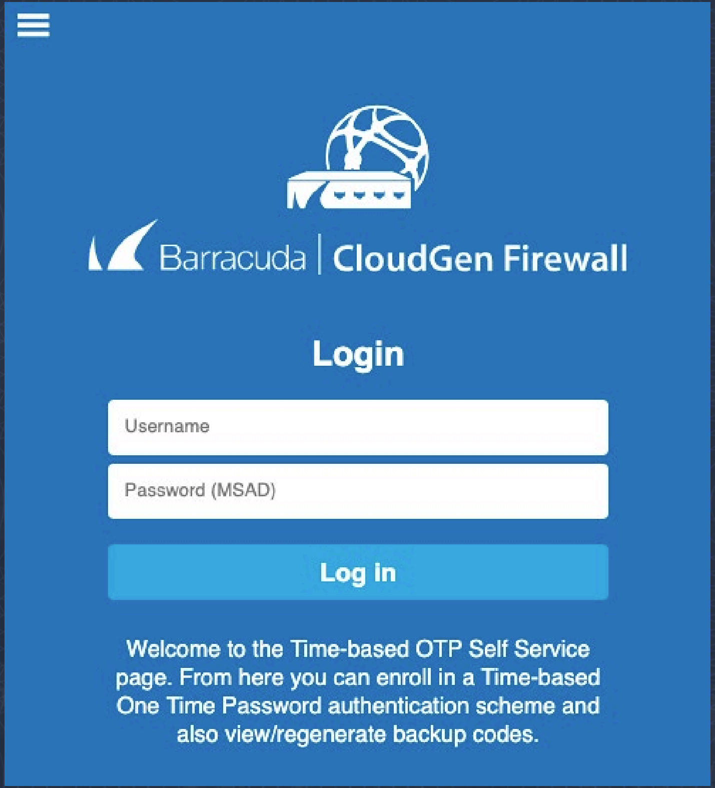
Allow self (re-)enrollment by user group

Or use the TOTP portal just for backup code management

Use your own corporate logo

Set your own welcome text

Using the TOTP portal



Barracuda | CloudGen Firewall

Login

Username

Password (MSAD)

Log in

Welcome to the Time-based OTP Self Service page. From here you can enroll in a Time-based One Time Password authentication scheme and also view/regenerate backup codes.

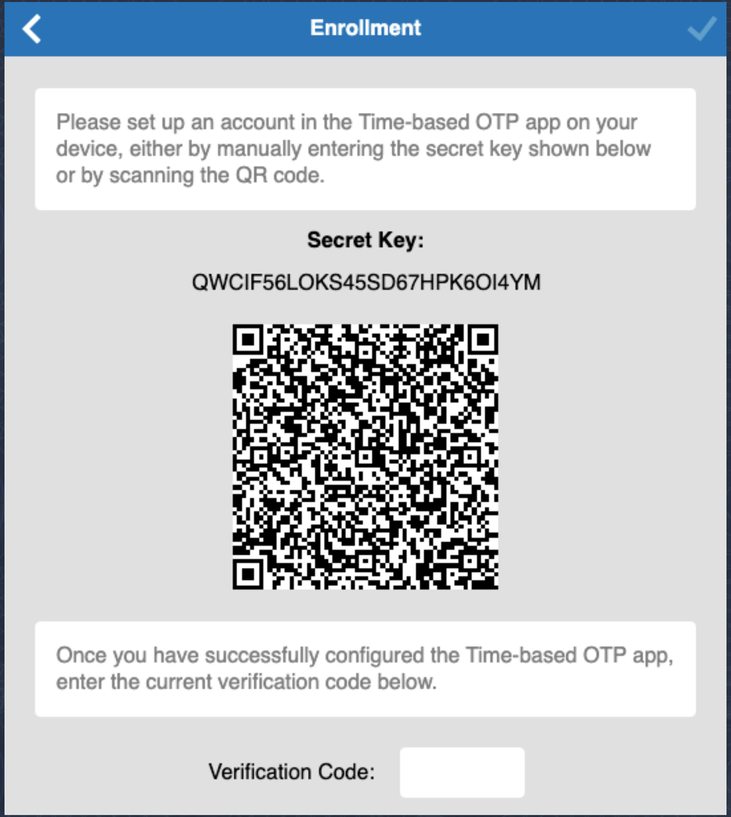
If no SSL VPN just go to the root URL.

If you have an SSL VPN setup you can use the CudaLaunch app or direct your browser to

https://sslvpn.company.com/portal/totp.html

Log in with the authentication scheme you selected.

TOTP portal: enrollment



Please set up an account in the Time-based OTP app on your device, either by manually entering the secret key shown below or by scanning the QR code.

Secret Key:

QWCIF56LOKS45SD67HPK6OI4YM

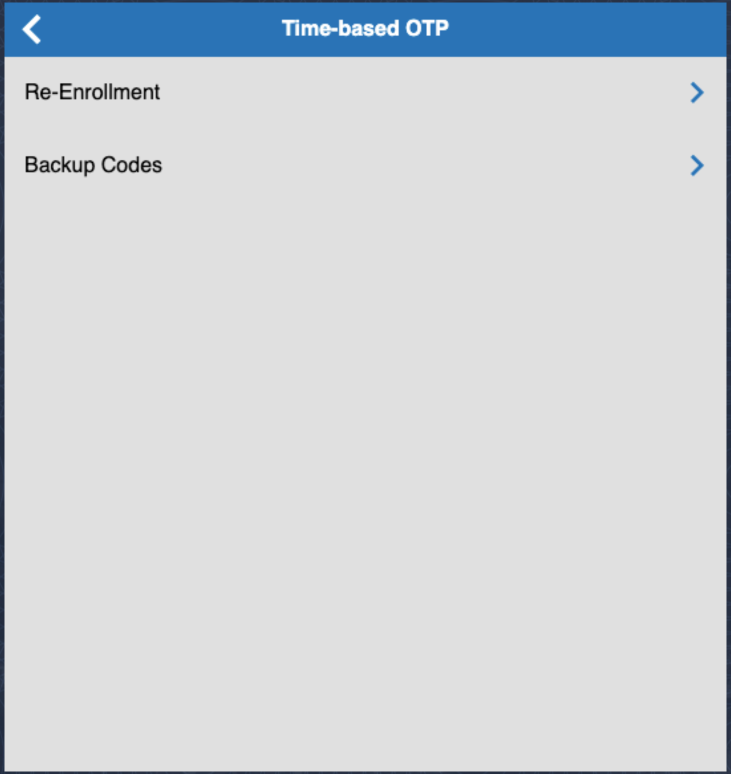
Once you have successfully configured the Time-based OTP app, enter the current verification code below.

Verification Code:

Scan or click the QR code or copy and paste the key into the TOTP authenticator app of your choice.

Enter the token generated by the app to enroll.

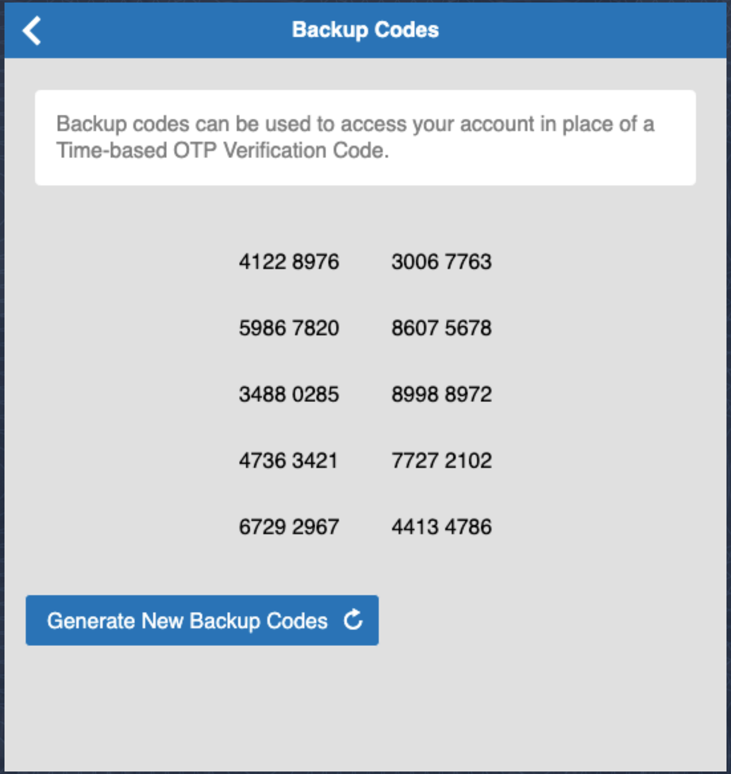
TOTP portal: Backup codes



Time-based OTP

Re-Enrollment

Backup Codes



Backup Codes

Backup codes can be used to access your account in place of a Time-based OTP Verification Code.

4122 8976	3006 7763
5986 7820	8607 5678
3488 0285	8998 8972
4736 3421	7727 2102
6729 2967	4413 4786

Generate New Backup Codes

TOTP self service and CudaLaunch

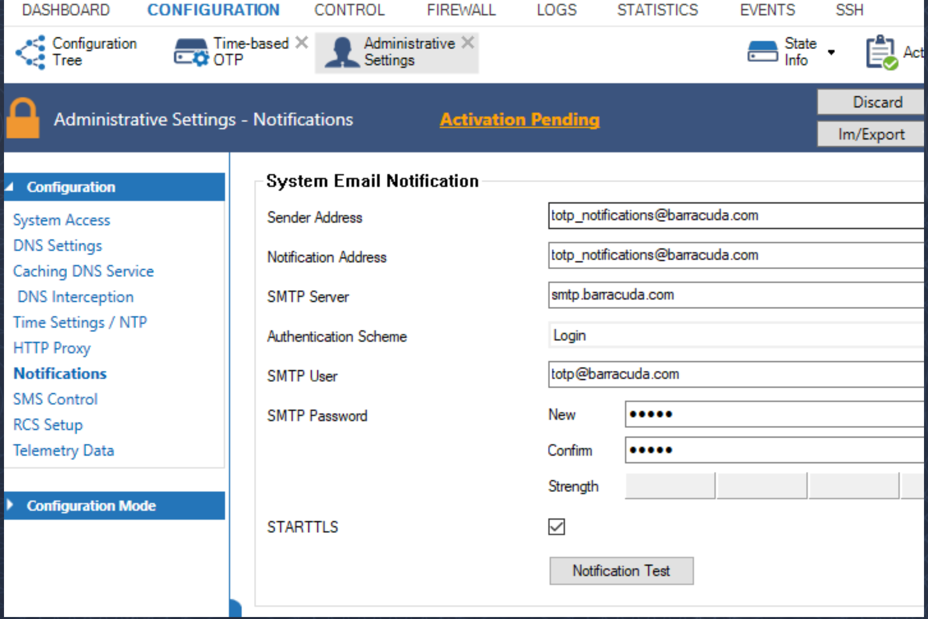
All the features in the TOTP portal are available through CudaLaunch and the SSL VPN web portal.

Go to menu

- Settings
  - Time-based OTP
    - Enrollment
    - Re-Enrollment
    - View backup codes
    - Generate new backup codes

Setup – bulk Enrollment

Requirement: – Setting up email notifications



Administrative Settings - Notifications Activation Pending

System Email Notification

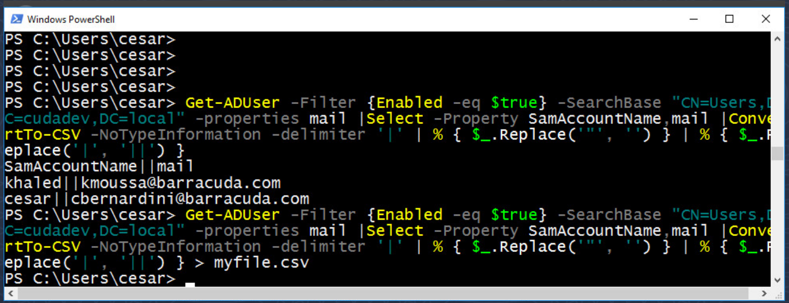
Sender Address	totp_notifications@barracuda.com
Notification Address	totp_notifications@barracuda.com
SMTP Server	smtp.barracuda.com
Authentication Scheme	Login
SMTP User	totp@barracuda.com
SMTP Password	New ●●●●● Confirm ●●●●● Strength
STARTTLS	☑

Notification Test

Setup the system email notifications

- After configuration, ensure that emails are being sent by using the **Notification Test** button.

Requirements: Import users from AD



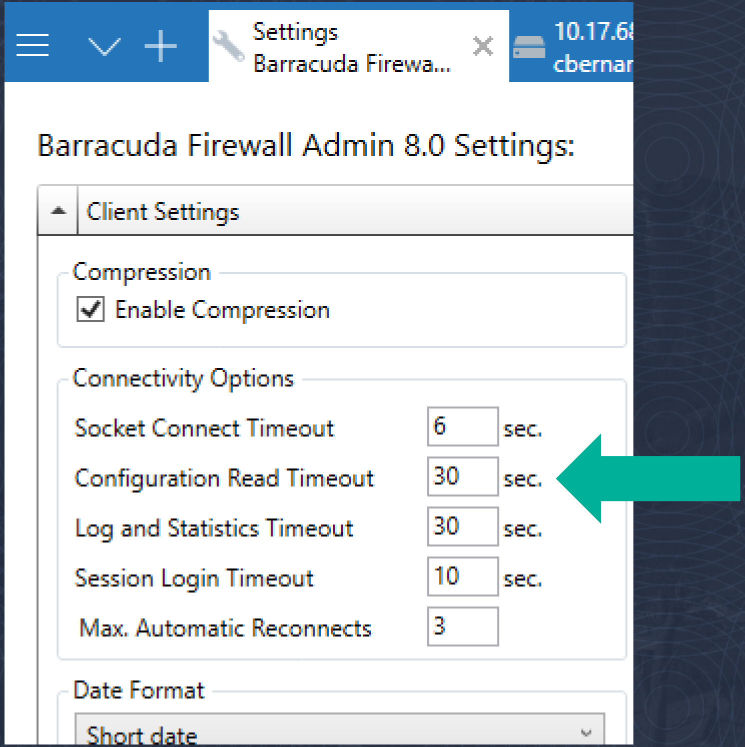
```
PS C:\Users\cesar>
PS C:\Users\cesar>
PS C:\Users\cesar>
PS C:\Users\cesar>
PS C:\Users\cesar> Get-ADUser -Filter {Enabled -eq $true} -SearchBase "CN=Users,D
C=cudadev,DC=local" -properties mail |Select -Property SamAccountName,mail |Conve
rtTo-CSV -NoTypeInformation -delimiter '|' | % { $_.Replace('"', '') } | % { $_.R
eplace('|', '||') }
SamAccountName||mail
khaled||kmoussa@barracuda.com
cesar||cbernardini@barracuda.com
PS C:\Users\cesar> Get-ADUser -Filter {Enabled -eq $true} -SearchBase "CN=Users,D
C=cudadev,DC=local" -properties mail |Select -Property SamAccountName,mail |Conve
rtTo-CSV -NoTypeInformation -delimiter '|' | % { $_.Replace('"', '') } | % { $_.R
eplace('|', '||') } > myfile.csv
PS C:\Users\cesar>
```

Extract users with PowerShell:

- `Get-ADUser –Filter * –SearchBase “CN=Sales,DC=barracuda,DC=com –properties mail | where { $_.Enabled –eq $True} | Select –Property SamAccountName,mail | Convert-ToCSV –NoTypeInformation –delimiter ‘|’ | %{$_.Replace(‘”’, ‘’) } | %{$_.Replace(‘|’, ‘||’) }`

Copy the list of users in the clipboard.

Requirements: Change connection timeout



Barracuda Firewall Admin 8.0 Settings:

Client Settings

Compression

☑ Enable Compression

Connectivity Options

Socket Connect Timeout 6 sec.

Configuration Read Timeout 30 sec.

Log and Statistics Timeout 30 sec.

Session Login Timeout 10 sec.

Max. Automatic Reconnects 3

Date Format

Short date

Firewall Admin settings

Client settings

Connection read timeout:

- NUMBER_OF_USERS x 3s
- For instance, to enrol 100 users: 100 x 3 sec. = 300 sec.

Restart your Firewall Admin session

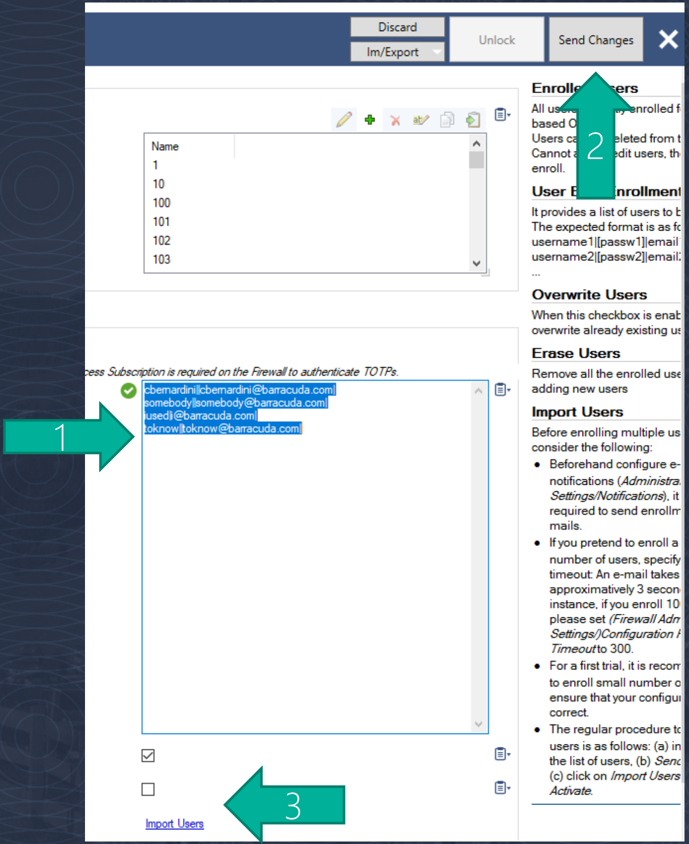
Bulk Enrollment: How To 1/2

Location

- CC: [Range]/[Cluster]/[FW]/Infrastructure Service/Time-based OTP bulk Enrollment
- Firewall: Infrastructure Service/Time-based OTP bulk Enrollment

Steps

- Lock
- Paste the list of users (1)
- Send changes (2)
- Import users (3)
- Activate



cess Subscription is required on the Firewall to authenticate TOTPs.

```
cbernardini||cbernardini@barracuda.com|
somebody||somebody@barracuda.com|
iused|i@barracuda.com|
toknow||toknow@barracuda.com|
```

Enrolle ers

All use enrolled f
based O
Users ca eleted from t
Cannot a edit users, th
enroll.

User E nrollment

It provides a list of users to b
The expected format is as fo
username1|[passw1]|email
username2|[passw2]|email
...

Overwrite Users

When this checkbox is enab
overwrite already existing us

Erase Users

Remove all the enrolled use
adding new users

Import Users

Before enrolling multiple us
consider the following:

- Beforehand configure e-notifications (*Administra Settings/Notifications*), it required to send enrollm mails.
- If you pretend to enroll a number of users, specify timeout: An e-mail takes approximatively 3 secon instance, if you enroll 10 please set *(Firewall Adm Settings/)Configuration I Timeout* to 300.
- For a first trial, it is recom to enroll small number o ensure that your configu correct.
- The regular procedure to users is as follows: (a) in the list of users, (b) *Send* (c) click on *Import Users* *Activate*.

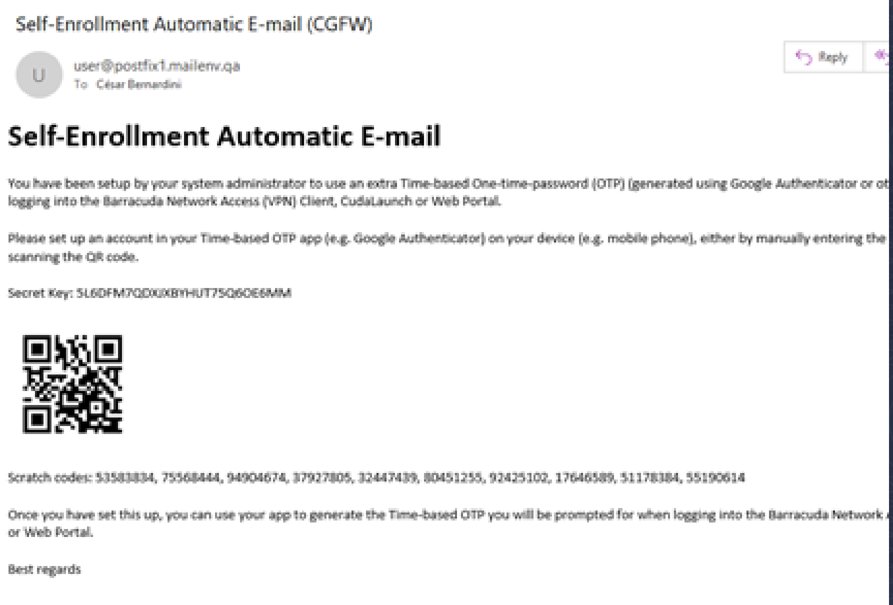
Bulk Enrollment: How To 2/2

Every user receives an email w/

- QR code
- Backup codes
  - These codes can be used once, when we don't have access to the physical device.

Design your own template

- Available in the advanced settings
- HTML



Self-Enrollment Automatic E-mail (CGFW)

user@postfix1.mailenv.qa
To: César Bernardini

Self-Enrollment Automatic E-mail

You have been setup by your system administrator to use an extra Time-based One-time-password (OTP) (generated using Google Authenticator or ot
logging into the Barracuda Network Access (VPN) Client, CudaLaunch or Web Portal.

Please set up an account in your Time-based OTP app (e.g. Google Authenticator) on your device (e.g. mobile phone), either by manually entering the
scanning the QR code.

Secret Key: 5L6DFM7QDXJXBYHUT75Q6OE6MM

Scratch codes: 53583834, 75568444, 94904674, 37927805, 32447439, 80451255, 92425102, 17646589, 51178384, 55190614

Once you have set this up, you can use your app to generate the Time-based OTP you will be prompted for when logging into the Barracuda Network
or Web Portal.

Best regards

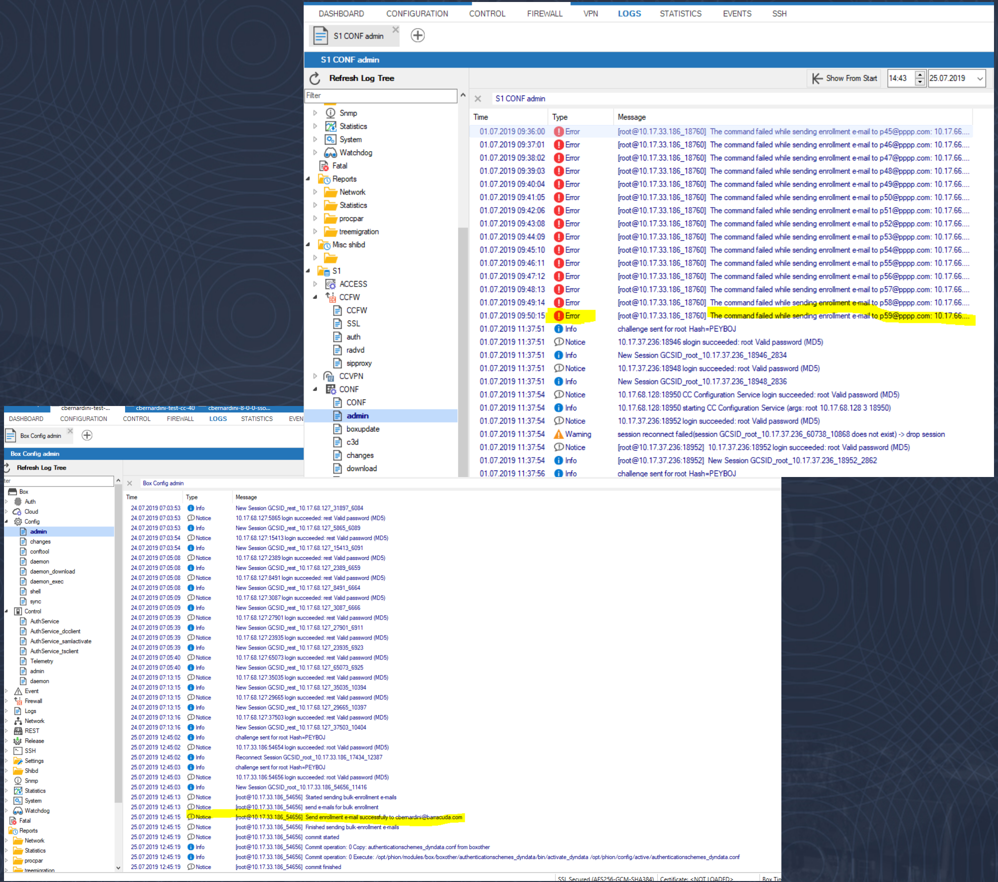
Troubleshooting

In the logs, we report:

- Successfully/Unsuccessfully sent enrollment emails

Location

- In a Firewall:
    - Box/Config/Admin
- In a Control Center:
    - [Server]/CONF/admin



S1 CONF admin

```
Time                 Type     Message
01.07.2019 09:36:00  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p45@pppp.com: 10.17.66....
01.07.2019 09:37:01  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p46@pppp.com: 10.17.66....
01.07.2019 09:38:02  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p47@pppp.com: 10.17.66....
01.07.2019 09:39:03  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p48@pppp.com: 10.17.66....
01.07.2019 09:40:04  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p49@pppp.com: 10.17.66....
01.07.2019 09:41:05  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p50@pppp.com: 10.17.66....
01.07.2019 09:42:06  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p51@pppp.com: 10.17.66....
01.07.2019 09:43:08  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p52@pppp.com: 10.17.66....
01.07.2019 09:44:09  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p53@pppp.com: 10.17.66....
01.07.2019 09:45:10  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p54@pppp.com: 10.17.66....
01.07.2019 09:46:11  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p55@pppp.com: 10.17.66....
01.07.2019 09:47:12  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p56@pppp.com: 10.17.66....
01.07.2019 09:48:13  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p57@pppp.com: 10.17.66....
01.07.2019 09:49:14  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p58@pppp.com: 10.17.66....
01.07.2019 09:50:15  Error    [root@10.17.33.186_18760]  The command failed while sending enrollment e-mail to p59@pppp.com: 10.17.66....
01.07.2019 11:37:51  Info     challenge sent for root Hash=PEYBOJ
01.07.2019 11:37:51  Notice   10.17.37.236:18946 slogin succeeded: root Valid password (MD5)
01.07.2019 11:37:51  Info     New Session GCSID_root_10.17.37.236_18946_2834
01.07.2019 11:37:51  Notice   10.17.37.236:18948 login succeeded: root Valid password (MD5)
01.07.2019 11:37:51  Info     New Session GCSID_root_10.17.37.236_18948_2836
01.07.2019 11:37:54  Notice   10.17.68.128:18950 CC Configuration Service login succeeded: root Valid password (MD5)
01.07.2019 11:37:54  Info     10.17.68.128:18950 starting CC Configuration Service (args: root 10.17.68.128 3 18950)
01.07.2019 11:37:54  Notice   10.17.37.236:18952 login succeeded: root Valid password (MD5)
01.07.2019 11:37:54  Warning  session reconnect failed(session GCSID_root_10.17.37.236_60738_10868 does not exist) -> drop session
01.07.2019 11:37:54  Notice   [root@10.17.37.236:18952]  10.17.37.236:18952 login succeeded: root Valid password (MD5)
01.07.2019 11:37:54  Info     [root@10.17.37.236:18952]  New Session GCSID_root_10.17.37.236_18952_2862
01.07.2019 11:37:56  Info     challenge sent for root Hash=PEYBOJ
```

Box Config admin

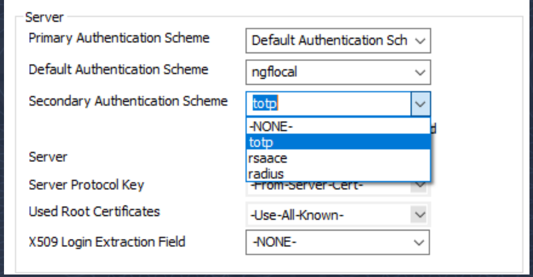
```
Time                 Type    Message
24.07.2019 07:03:53  Info    New Session GCSID_rest_10.17.68.127_31897_6084
24.07.2019 07:03:53  Notice  10.17.68.127:5865 login succeeded: rest Valid password (MD5)
24.07.2019 07:03:53  Info    New Session GCSID_rest_10.17.68.127_5865_6089
24.07.2019 07:03:54  Notice  10.17.68.127:15413 login succeeded: rest Valid password (MD5)
24.07.2019 07:03:54  Info    New Session GCSID_rest_10.17.68.127_15413_6091
24.07.2019 07:05:08  Notice  10.17.68.127:2389 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:08  Info    New Session GCSID_rest_10.17.68.127_2389_6659
24.07.2019 07:05:08  Notice  10.17.68.127:8491 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:08  Info    New Session GCSID_rest_10.17.68.127_8491_6664
24.07.2019 07:05:09  Notice  10.17.68.127:3087 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:09  Info    New Session GCSID_rest_10.17.68.127_3087_6666
24.07.2019 07:05:39  Notice  10.17.68.127:27901 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:39  Info    New Session GCSID_rest_10.17.68.127_27901_6911
24.07.2019 07:05:39  Notice  10.17.68.127:23935 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:39  Info    New Session GCSID_rest_10.17.68.127_23935_6923
24.07.2019 07:05:40  Notice  10.17.68.127:65073 login succeeded: rest Valid password (MD5)
24.07.2019 07:05:40  Info    New Session GCSID_rest_10.17.68.127_65073_6925
24.07.2019 07:13:15  Notice  10.17.68.127:35035 login succeeded: rest Valid password (MD5)
24.07.2019 07:13:15  Info    New Session GCSID_rest_10.17.68.127_35035_10394
24.07.2019 07:13:15  Notice  10.17.68.127:29665 login succeeded: rest Valid password (MD5)
24.07.2019 07:13:15  Info    New Session GCSID_rest_10.17.68.127_29665_10397
24.07.2019 07:13:16  Notice  10.17.68.127:37503 login succeeded: rest Valid password (MD5)
24.07.2019 07:13:16  Info    New Session GCSID_rest_10.17.68.127_37503_10404
25.07.2019 12:45:02  Info    challenge sent for root Hash=PEYBOJ
25.07.2019 12:45:02  Notice  10.17.33.186:54654 login succeeded: root Valid password (MD5)
25.07.2019 12:45:02  Info    Reconnect Session GCSID_root_10.17.33.186_17434_12387
25.07.2019 12:45:03  Info    challenge sent for root Hash=PEYBOJ
25.07.2019 12:45:03  Notice  10.17.33.186:54656 login succeeded: root Valid password (MD5)
25.07.2019 12:45:03  Info    New Session GCSID_root_10.17.33.186_54656_11416
25.07.2019 12:45:13  Notice  [root@10.17.33.186_54656]  Started sending bulk-enrollment e-mails
25.07.2019 12:45:13  Notice  [root@10.17.33.186_54656]  send e-mails for bulk enrollment
25.07.2019 12:45:15  Notice  [root@10.17.33.186_54656]  Send enrollment e-mail successfully to cbernardini@barracuda.com
25.07.2019 12:45:15  Notice  [root@10.17.33.186_54656]  Finished sending bulk-enrollment e-mails
25.07.2019 12:45:19  Notice  [root@10.17.33.186_54656]  commit started
25.07.2019 12:45:19  Info    [root@10.17.33.186_54656]  Commit operation: 0 Copy: authenticationschemes_dyndata.conf from boxother
25.07.2019 12:45:19  Info    [root@10.17.33.186_54656]  Commit operation: 0 Execute: /opt/phion/modules/box/boxother/authenticationschemes_dyndata/bin/activate_dyndata /opt/phion/config/active/authenticationschemes_dyndata.conf
25.07.2019 12:45:19  Notice  [root@10.17.33.186_54656]  commit finished
```

Setup – TINA VPN

Setting up MFA in CGF

e.g. add secondary auth to TINA client-to-site VPN:

- Either TOTP, RSA or RADIUS
- Add Group Policy Conditions
  - e.g. Require for Sales and not Engineering



Server

Primary Authentication Scheme: Default Authentication Sch

Default Authentication Scheme: ngflocal

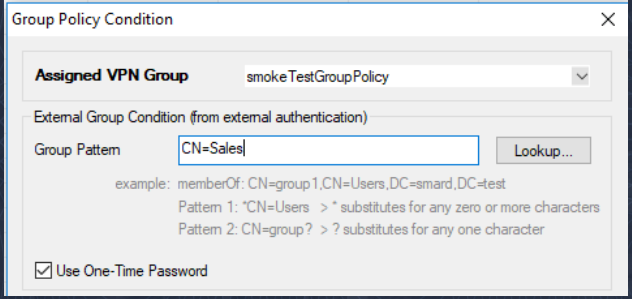
Secondary Authentication Scheme: totp

Server

Server Protocol Key: -From-Server-Cert-

Used Root Certificates: -Use-All-Known-

X509 Login Extraction Field: -NONE-



Group Policy Condition

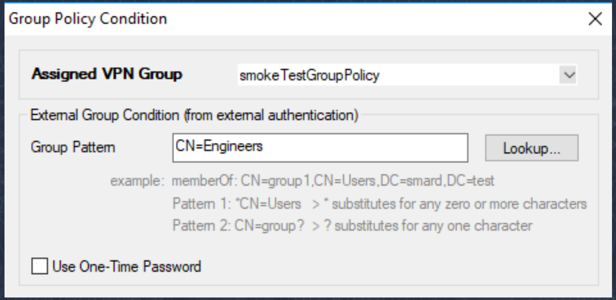
Assigned VPN Group: smokeTestGroupPolicy

External Group Condition (from external authentication)

Group Pattern: CN=Sales

example: memberOf: CN=group1,CN=Users,DC=smard,DC=test
Pattern 1: *CN=Users > * substitutes for any zero or more characters
Pattern 2: CN=group? > ? substitutes for any one character

☑ Use One-Time Password



Group Policy Condition

Assigned VPN Group: smokeTestGroupPolicy

External Group Condition (from external authentication)

Group Pattern: CN=Engineers

example: memberOf: CN=group1,CN=Users,DC=smard,DC=test
Pattern 1: *CN=Users > * substitutes for any zero or more characters
Pattern 2: CN=group? > ? substitutes for any one character

☐ Use One-Time Password

Setup – VPN client profiles

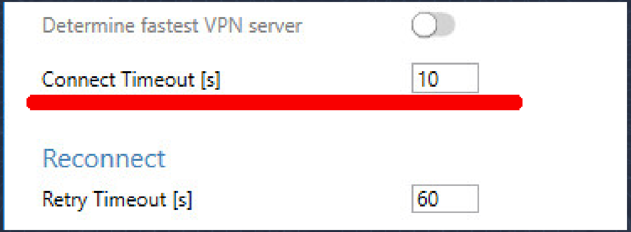
Setting up Client Profile

Choose TOTP Mode:

- Off, Static, Dynamic

Connection Timeouts:

- Increase timeout

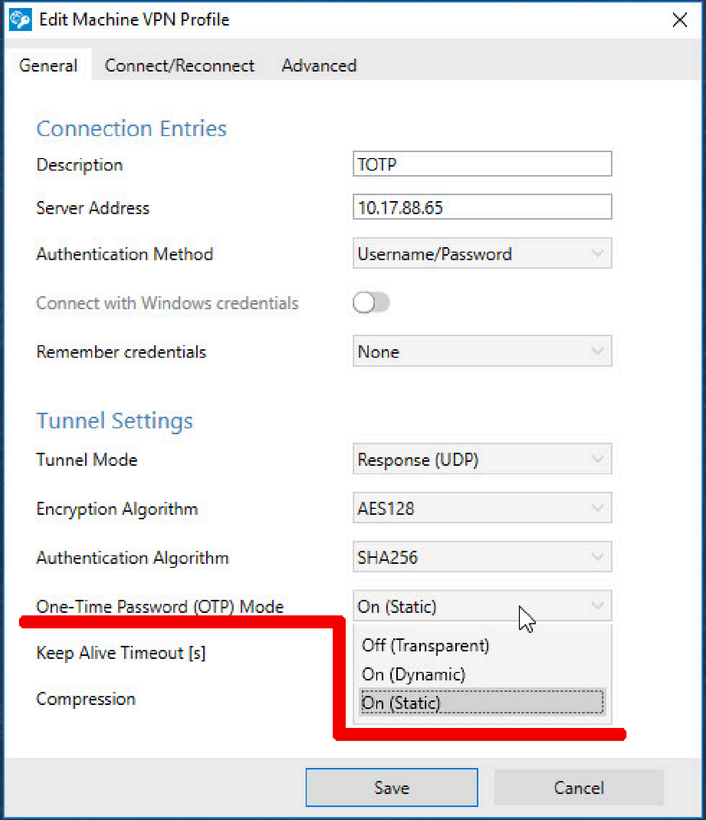


Determine fastest VPN server ○

Connect Timeout [s] 10

Reconnect

Retry Timeout [s] 60



Edit Machine VPN Profile

Connection Entries

Description: TOTP

Server Address: 10.17.88.65

Authentication Method: Username/Password

Connect with Windows credentials ○

Remember credentials: None

Tunnel Settings

Tunnel Mode: Response (UDP)

Encryption Algorithm: AES128

Authentication Algorithm: SHA256

One-Time Password (OTP) Mode: On (Static)

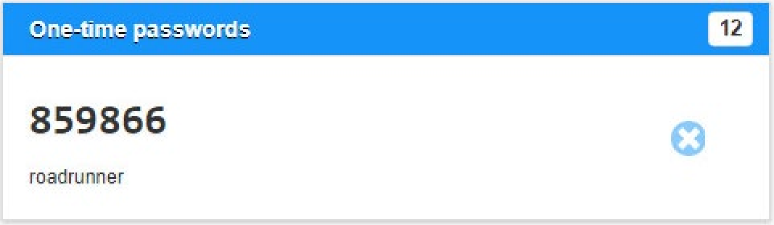
Keep Alive Timeout [s]

Compression

VPN Connector

Static:

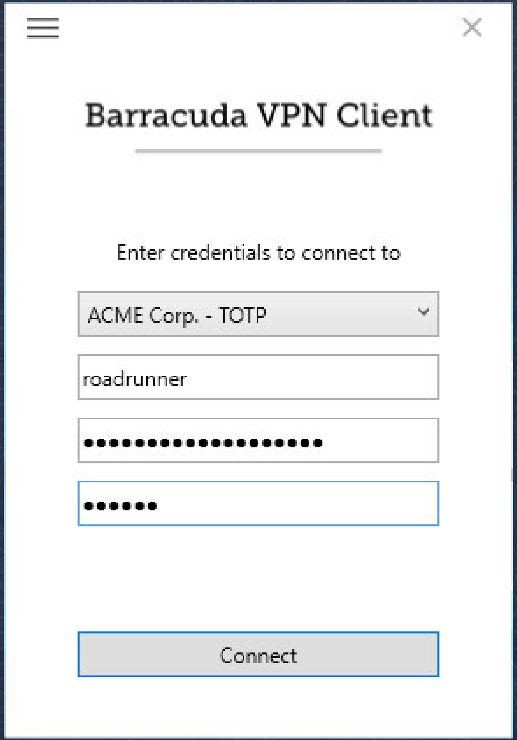
- always use OTP to connect



One-time passwords 12

859866

roadrunner



Barracuda VPN Client

Enter credentials to connect to

ACME Corp. - TOTP

roadrunner

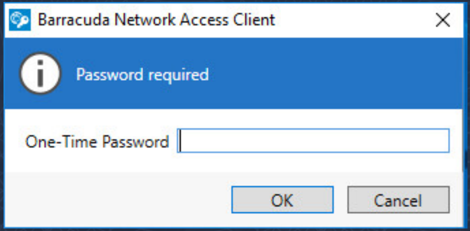
••••••••••••••••••

••••••

VPN Connector

Dynamic:

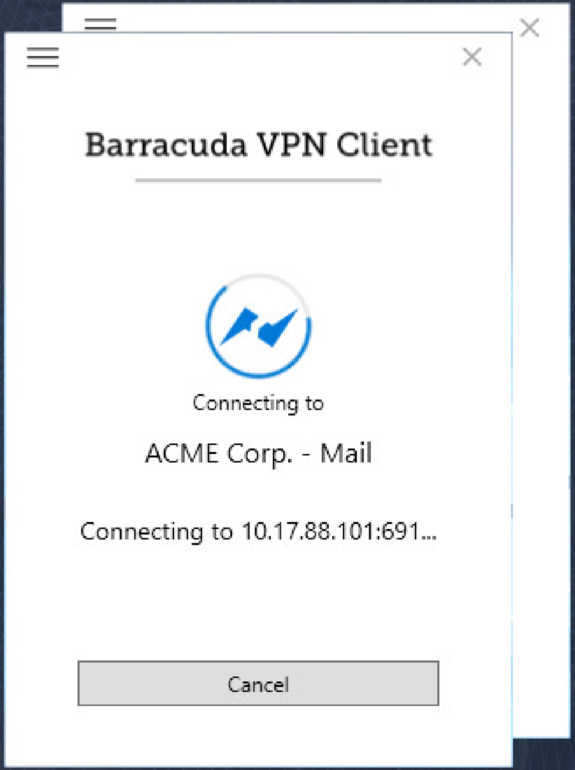
- OTP is being used, but not known at initial connect



Barracuda Network Access Client

Password required

One-Time Password



Barracuda VPN Client

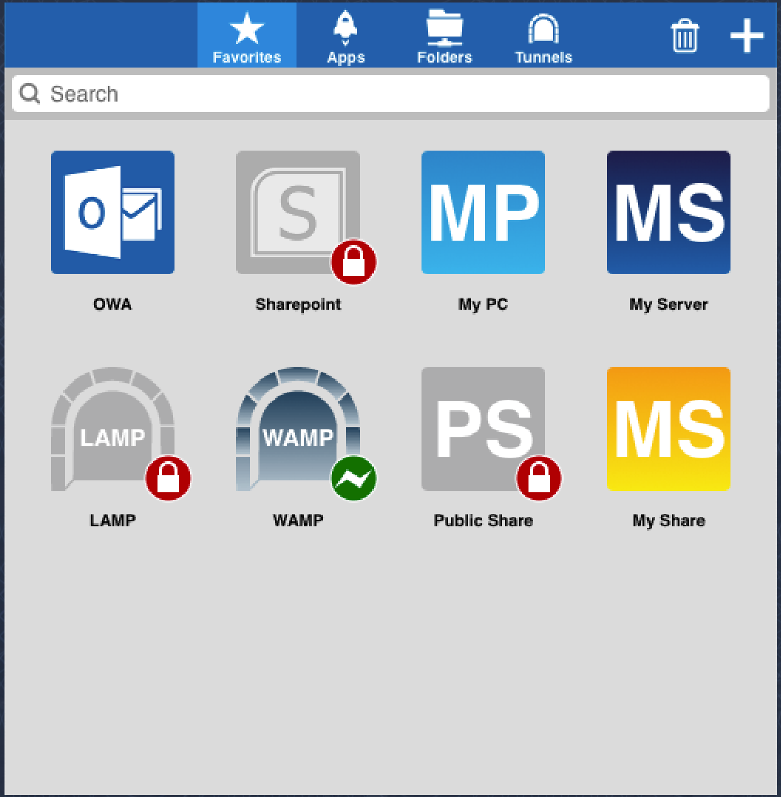
Connecting to

ACME Corp. - Mail

Connecting to 10.17.88.101:691...

SSL VPN dynamic apps

Dynamic Apps: User View



Can see all resources that they have/could have access to.

Resources that are dynamic are decorated with a padlock while disabled.

Dynamic apps

Ability for designated ‘Super-Users’ to control resource access in CudaLaunch.

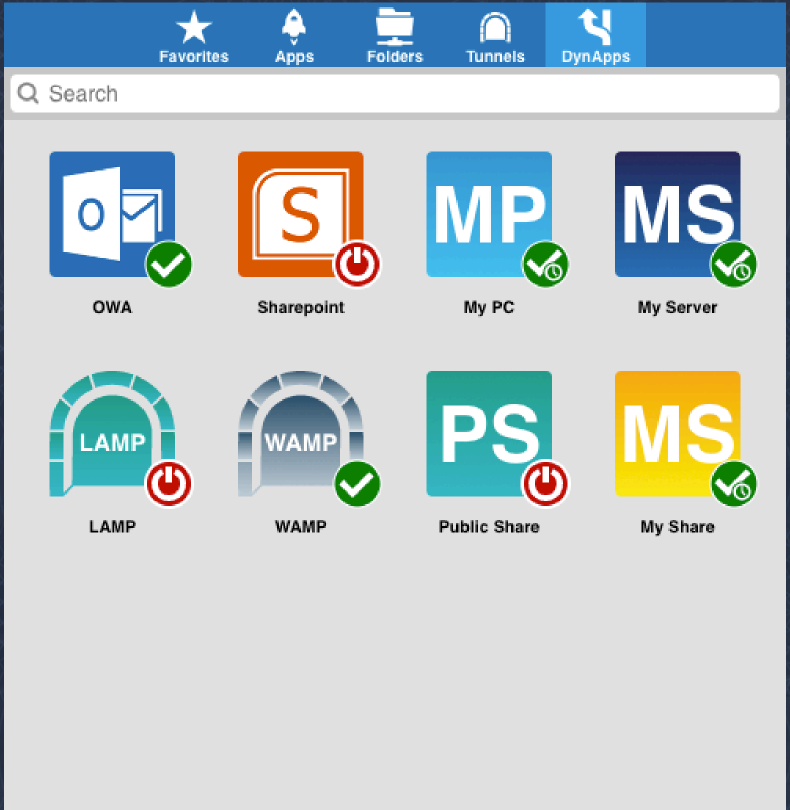
Global ‘Super-Users’

Per-Resource ‘Super-Users’

Available on proxied web apps, tunneled web apps, RDP apps, generic tunneled apps and network places.

Requires Advanced Remote Access.

Dynamic apps: 'Super-User' view



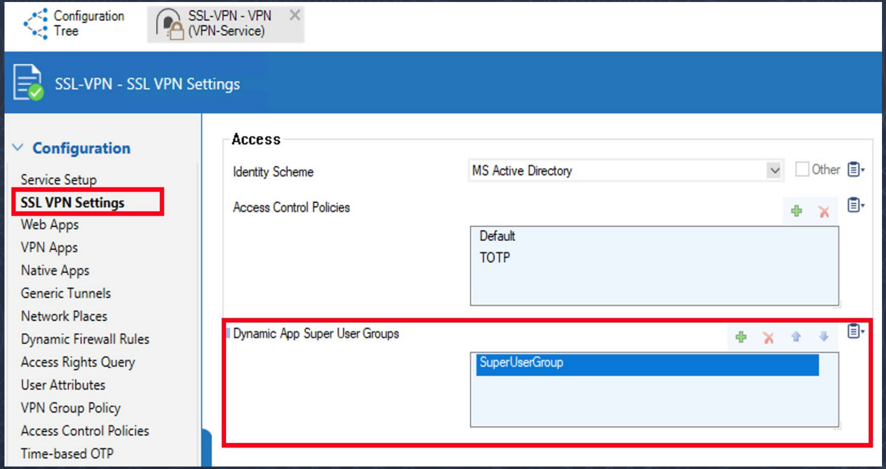
New 'DynApps' resource tab in CudaLaunch and SSL VPN web portal

Click the 'DynApp' to enable, time enable or disable

See current state of all 'DynApps'

Search and Favorite

Dynamic apps: Global ‘Super-Users’



Access

Identity Scheme: MS Active Directory □ Other

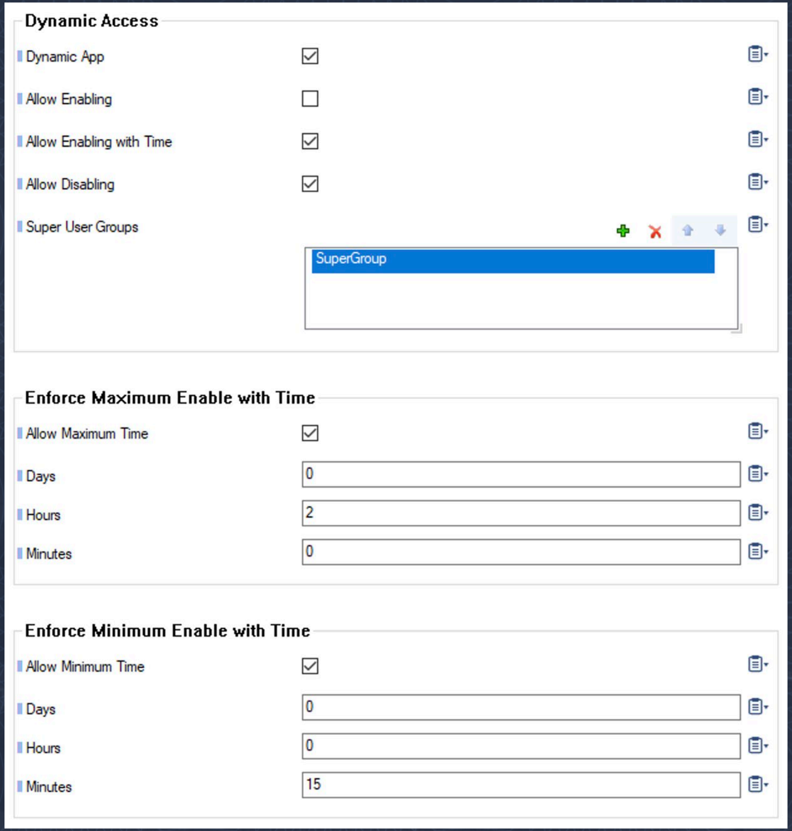
Access Control Policies: Default, TOTP

Dynamic App Super User Groups: SuperUserGroup

Defined by group

Can control all resources set as dynamic apps

Dynamic Apps: Resource Setup



Dynamic Access

Dynamic App	☑
Allow Enabling	□
Allow Enabling with Time	☑
Allow Disabling	☑
Super User Groups	SuperGroup

Enforce Maximum Enable with Time

Allow Maximum Time	☑
Days	0
Hours	2
Minutes	0

Enforce Minimum Enable with Time

Allow Minimum Time	☑
Days	0
Hours	0
Minutes	15

For each resource type

- Make Dynamic
- Choose Allowable Actions
- Define Super User Groups just for this resource
- Limit Time

What next?

Potential MFA / TOTP Improvements

- In progress - Add Linux and macOS VPN client support
- Auto-reconnect & TOTPs = Anti-pattern
  - Configurable 'Remember Me'
    - Designing what dimensions to cover. E.g. time, device, user/group?
- Add MFA/TOTP to Firewall Admin

Thank you

Barracuda.

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT