

INTEGRASJONSGUIDE – BP CODE

Cisco ASA 8.3x – 9.1x

ÅPEN

Versjon: 1.1
Versjonsdato: 30.07.2013

Byypass AS

Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway

Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01

E-mail: kundeservice@buypass.no
VAT: NO 983 163 327

www.buypass.no

Endringshistorie

Versjon	Dato	Status	Beskrivelse/Endringer
1.0	30.05.2013	Final	Opprettelse og ferdigstillelse av dokument
1.1	30.07.2013	Final	Små justeringer

Bidragstere

Firmanavn	Navn
Bypass	Espen Sammerud

Innholdsfortegnelse

1	Konfigurere Cisco ASA med Bypass Code 2-faktor autentisering	4
1.1	Forutsetninger.....	4
1.2	Fremgangsmåte.....	4

1 Konfigurere Cisco ASA med Bypass Code 2-faktor autentisering.

1.1 Forutsetninger:

- BPC GW er installert i nettverket og kan kommunisere med LDAP server på TCP port 389 (ldap).
- Servicekonto som skal brukes for å lese AD er opprettet.
- Oversikt over ip-adresser for BPC GW, PoA (Point of Access).
- Velg LDAP stien. Skal man bruke hele AD, bestemt OU eller flere OU's?

1.2 Fremgangsmåte

- Logg på ditt brukersted med admin-bruker.

<https://www.bypass.no/bpcode/merchants/DINMERCHANTKODE/>

- Definer LDAP server og LDAP sti under LDAP.

LDAP sti(er).

URL	Brukernavn	Tel.nr. attribut	App.id. attribut	Beskrivelse
ldap://192.168.171.15	bpc_svc_ldap	mobile		LDAP BPLAB01
Prioritet LDAP sti				
1	basedn[ou=Users,ou=BPCode,dc=BPLAB01,dc=local(*)],filter[samAccountName=#USER#]			x slett
3	basedn[ou=Users2,ou=BPCode,dc=BPLAB01,dc=local(*)],filter[samAccountName=#USERS#]			x slett
2	basedn[ou=Users2,ou=BPCode,dc=BPLAB01,dc=local(*)],filter[samAccountName=#USER#]			x slett

Man kan definere en eller flere LDAP stier. Hvis man ønsker å liste alle undermapper så bruker man (*) bak siste DC= (i vårt eksempel ,dc=local(*)

- Definer RADIUS klient (Konfigurasjon → Radius → Ny konfigurasjon).
Skriv inn "inside" IP på Cisco ASA'n, shared secret og en beskrivelse.
Velg LDAP(er) som skal benyttes og deretter "lagre".

RADIUS konfigurasjon

IP-adresse:* 192.168.171.151

Shared secret:* ●●●●●●●●

NAS identifikator:

NAS IP:

Beskrivelse: Cisco ASA 5505 8.3(1)6

Tilgjengelige LDAPs
ldap://192.168.171.32

Valgt LDAPs
ldap://192.168.171.15

Tilbake Lagre

* betyr at feltet må være utfylt.

RADIUS konfigurasjon

Oversikten viser informasjon brukerstedet trenger for å sette opp en RADIUS-klient for autentisering med henhold til Bypass Code.

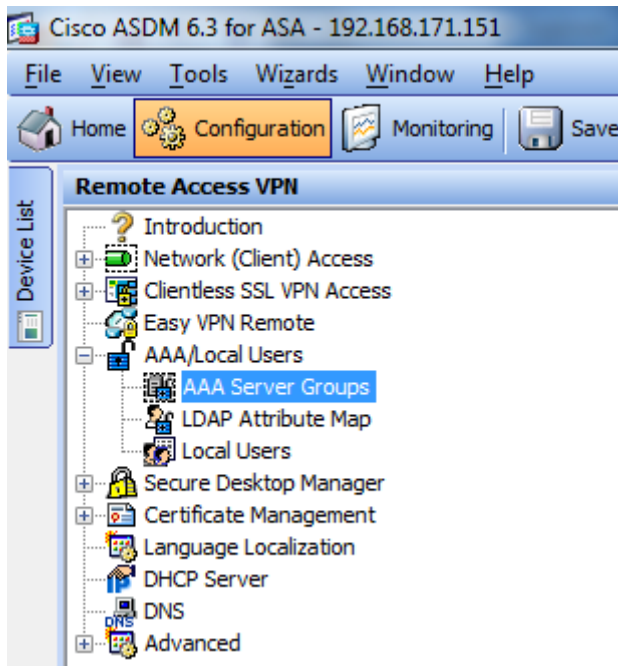
IP-adresse	NAS identifikator	NAS IP	Beskrivelse
192.168.171.24			Gw
192.168.171.35	httpstest		http
192.168.171.32	ldaptest		Tomcat
192.168.171.151			Cisco ASA 5505 8.3(1)6
LDAP URI		Beskrivelse	
ldap://192.168.171.15		LDAP BPLAB01	
192.168.171.37			MS UAG 2010
192.168.171.1			Check Point (SPLAT) R75.30
139.115.23.54			jeid test

Ny konfigurasjon

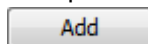
- Logg på Cisco ASA med Cisco ASDM

6. Opprett en ny AAA Server Group under meny "Configuration – Remote Access VPN"

[Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups](#)



Klikk på "add" på høyre side i "AAA Server Groups" oversikten.

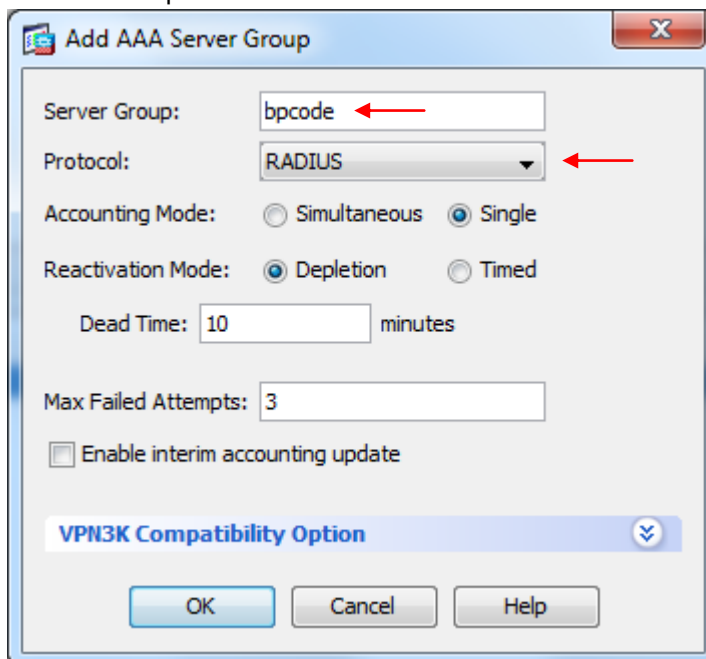


Gi gruppen et navn, for eksempel "bpcode".

Velg protokoll "RADIUS".

Resten av parameterne kan stå urørt.

Klikk deretter på "OK".



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
bpcode	RADIUS	Single	Depletion	10	3

- Legg til en server ("add" på høyre side) i den nylig opprettede gruppen (i feltet "Servers in the Selected Group").
Velg interface "inside".
Skriv inn ip-adressen til BP Code GW'n.
Endre "Server Authentication Port" til 1812.
Endre "Server Accounting Port" til 1813.
Skriv inn "Server Secret Key" (fra punkt 4).
Fjern haken fra "Microsoft CHAPv2 Capable".
Resten av parameterne kan stå urørt.
Klikk deretter på "OK".

Server Group: bpcode

Interface Name: inside

Server Name or IP Address: 192.168.171.24

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1812

Server Accounting Port: 1813

Retry Interval: 10 seconds

Server Secret Key: ●●●●

Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

OK Cancel Help

Servers in the Selected Group	
Server Name or IP Address	Interface
192.168.171.24	inside

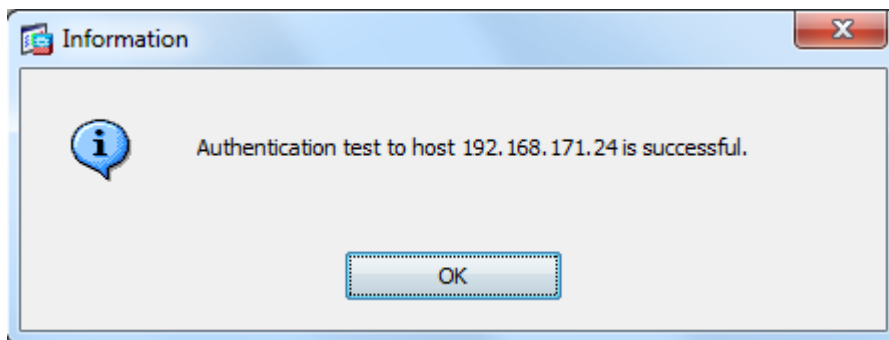
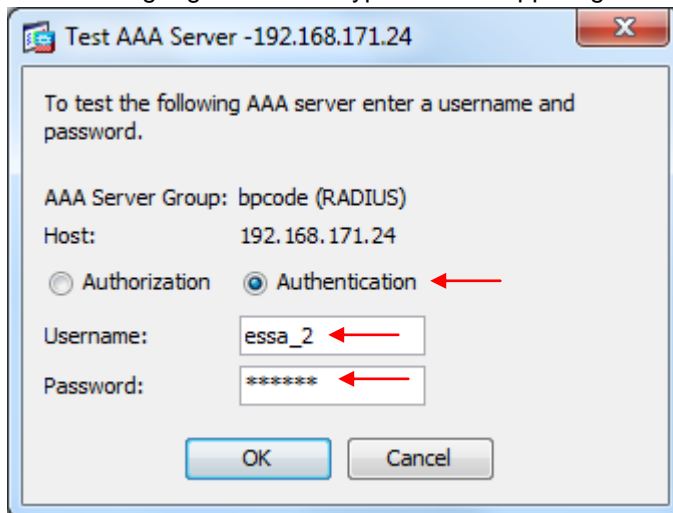
Klikk deretter på "Apply" nederst i konfigurasjonsvinduet.

Fra det samme vinduet kan man nå teste autentiseringen (klikk på knappen "Test" på høyre side) for å sjekke at oppsettet er korrekt.

Velg "Authentication".

Skriv inn brukernavn (må finnes i LDAP/AD).

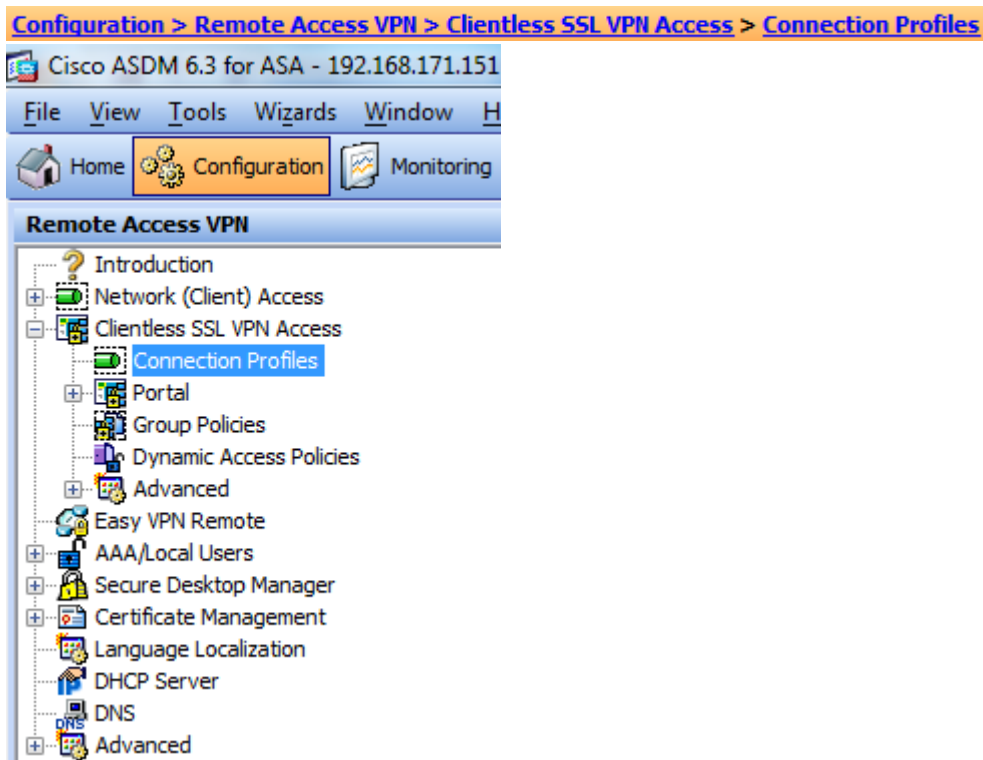
Skriv inn engangskode fra Buypass Code App'n og klikk deretter på "OK".



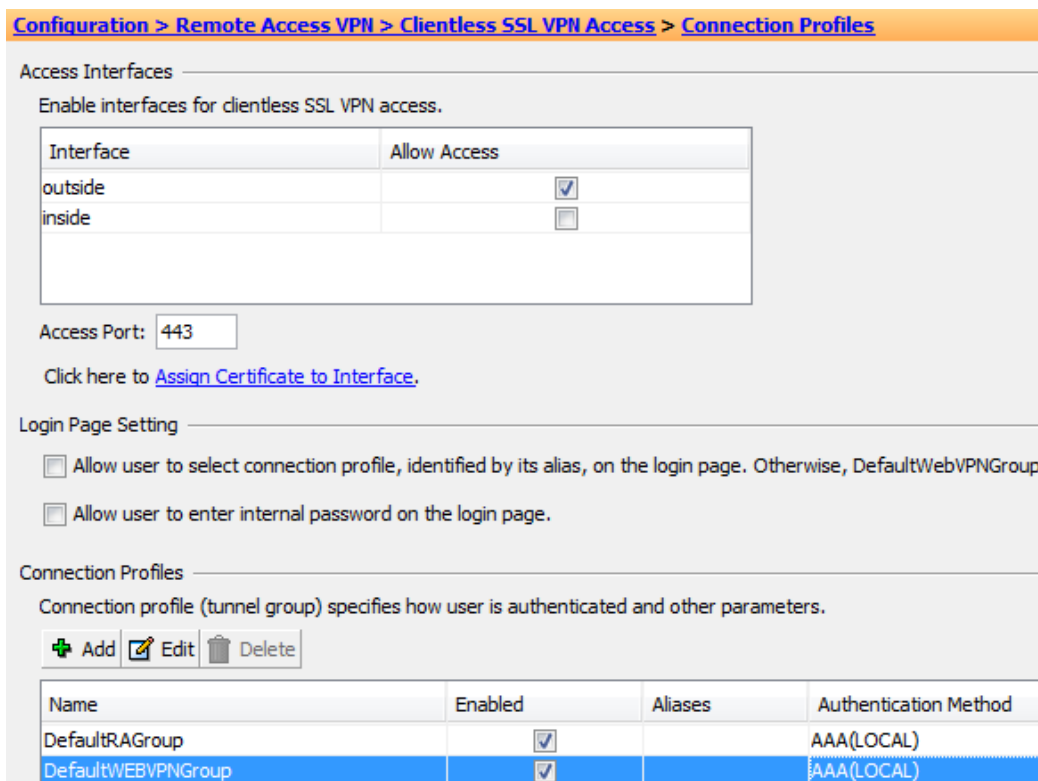
Den samme konfigurasjonen kan gjøres fra CLI og ser da slik ut:

```
aaa-server bpcode protocol radius
aaa-server bpcode (inside) host 192.168.171.24
key *****
authentication-port 1812
accounting-port 1813
no mschap2-capable
```

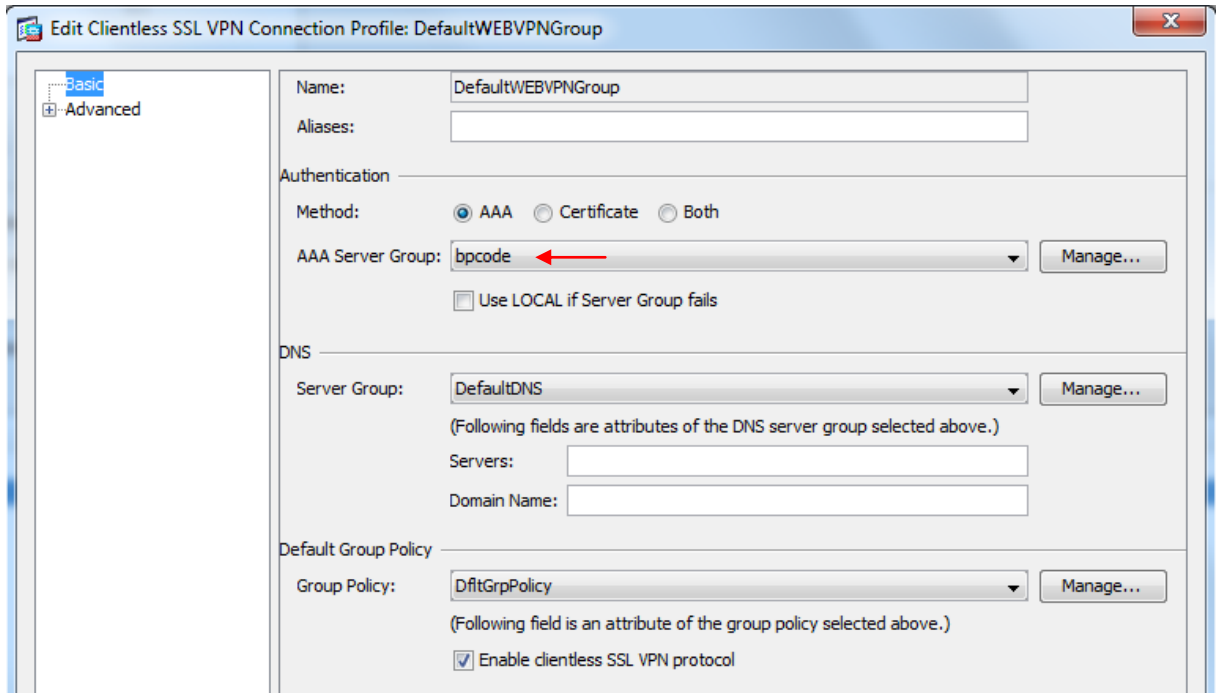

8. Konfigurer "Clientless SSL VPN Access" til å bruke BP Code (RADIUS).
I dette tilfellet benyttes standardprofilen (DefaultWEBVPNGroup)



Dobbelklikk på "DefaultWEBVPNGroup".



Velg "Authentication Method" AAA og deretter AAA Server Group fra pkt.6
Fjern eventuelt hake fra "Use LOCAL if Server Group fails"



Klikk OK

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

+ Add Edit Delete

Name	Enabled	Aliases	Authentication Method
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>		AAA(bpcode)

Klikk deretter "Apply" nederst i vinduet.

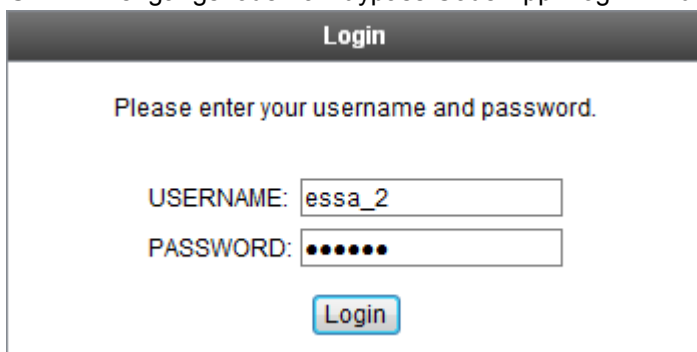
Den samme konfigurasjonen kan gjøres fra CLI og ser da slik ut:

```
tunnel-group DefaultWEBVPNGroup general-attributes
authentication-server-group bpcode
```

9. Pålogging på Clientless SSL VPN Access (browser-based VPN access)

Skriv inn brukernavn (må finnes i LDAP/AD).

Skriv inn engangskode fra Bypass Code App'n og klikk deretter på "Login".



The screenshot shows a web-based login form with a dark header bar containing the word "Login". Below the header, the text "Please enter your username and password." is displayed. There are two input fields: the first is labeled "USERNAME:" and contains the text "essa_2"; the second is labeled "PASSWORD:" and contains six black dots. Below the password field is a blue "Login" button.