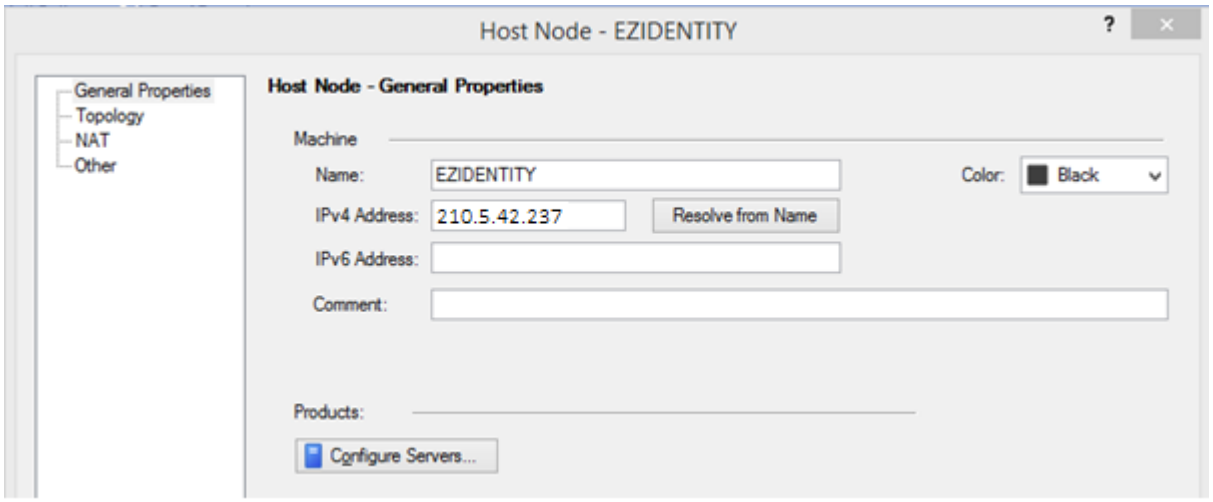
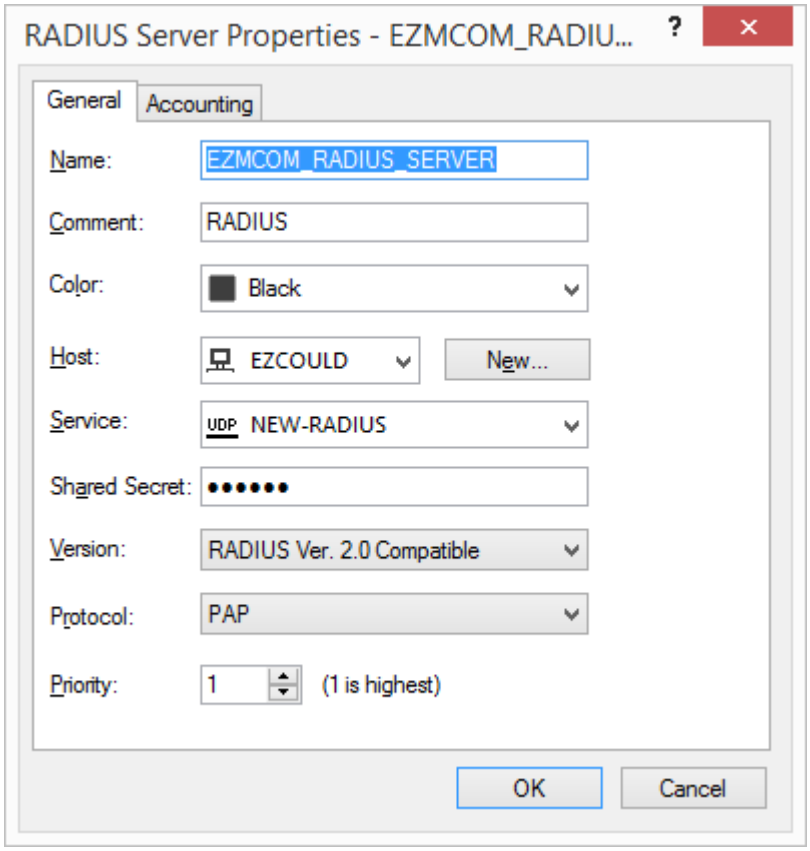
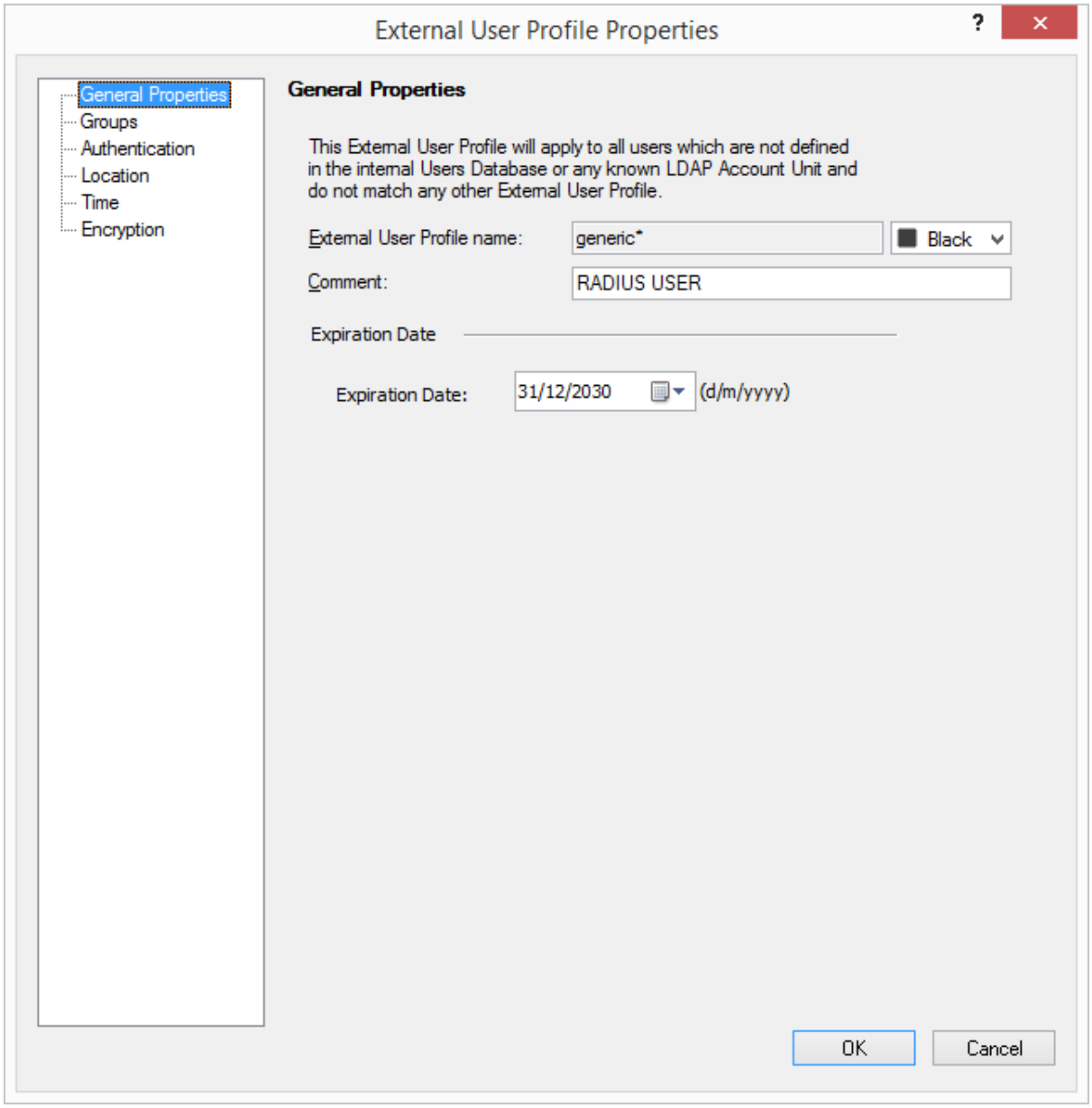
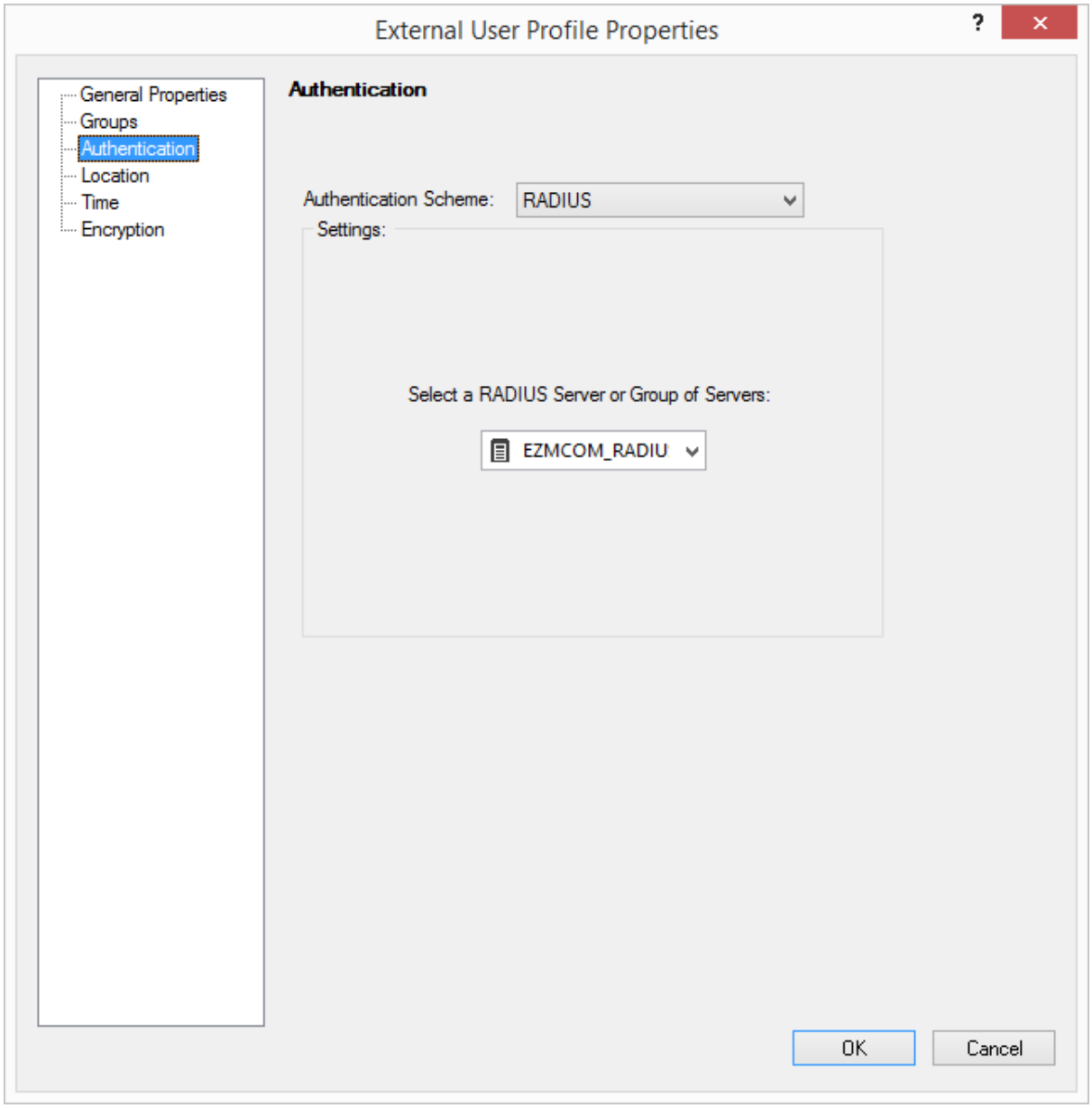
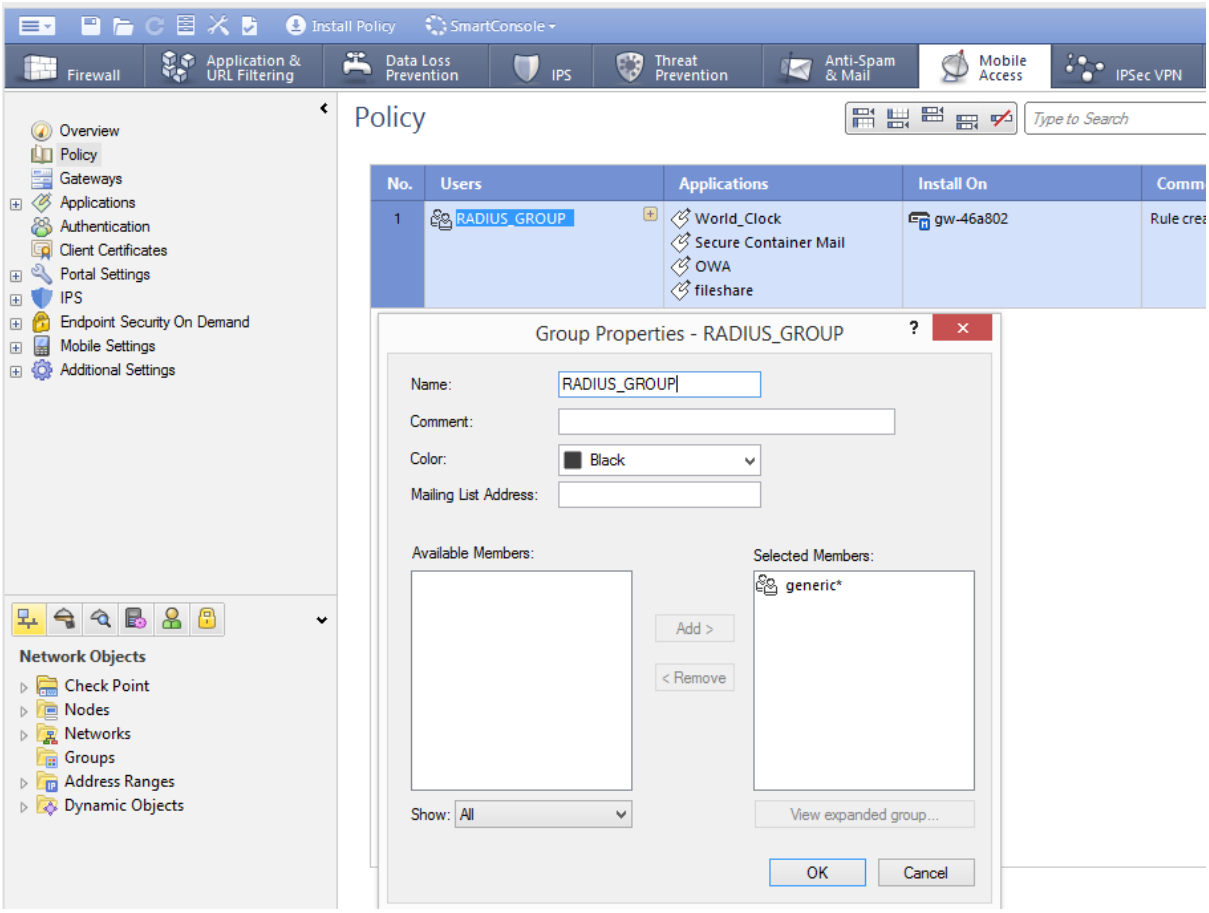
Checkpoint Integration with EZMCOM's EzIdentity.

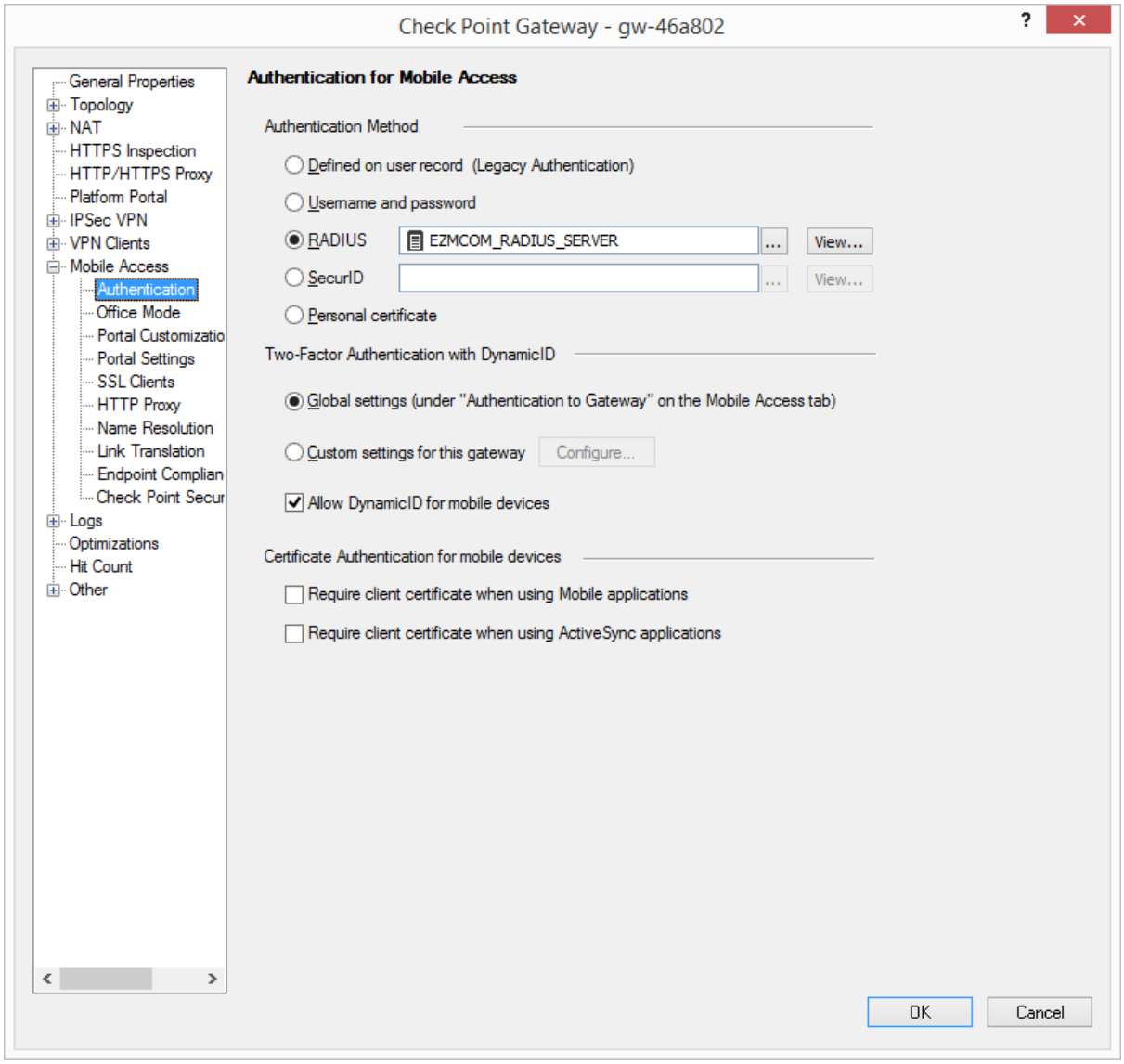


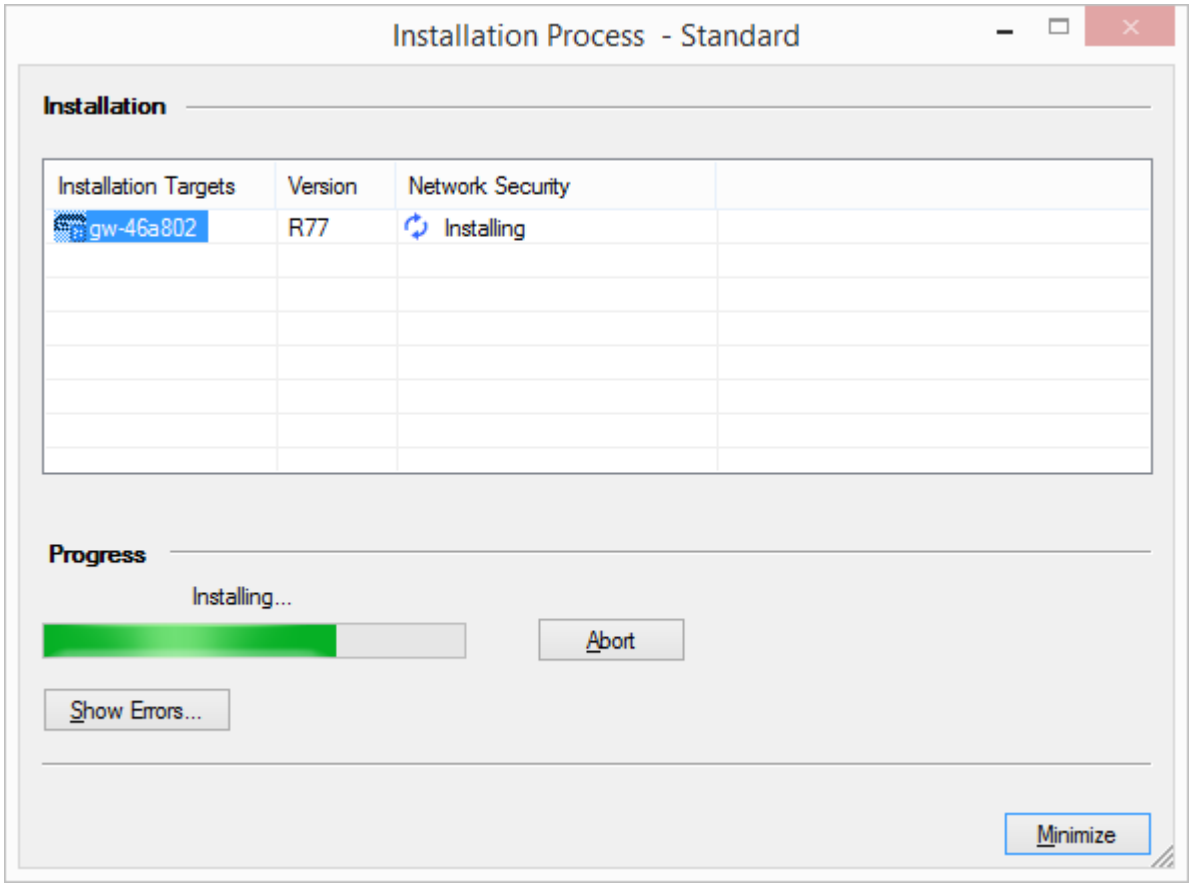



External User Profile Properties
General Properties
Groups
Authentication
Location
Time
Encryption
General Properties
This External User Profile will apply to all users which are not defined in the internal Users Database or any known LDAP Account Unit and do not match any other External User Profile.
External User Profile name:
generic*
Black
Comment:
RADIUS USER
Expiration Date
Expiration Date:
31/12/2030
(d/m/yyyy)
OK
Cancel


External User Profile Properties
General Properties
Groups
Authentication
Location
Time
Encryption
Authentication
Authentication Scheme:
RADIUS
Settings:
Select a RADIUS Server or Group of Servers:
EZMCOM_RADIU
OK
Cancel


Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Mobile Settings
Additional Settings
Network Objects
Check Point
Nodes
Networks
Groups
Address Ranges
Dynamic Objects
Policy
Type to Search
No.
Users
Applications
Install On
Comm
1
RADIUS_GROUP
World_Clock
Secure Container Mail
OWA
fileshare
gw-46a802
Rule cre
Group Properties - RADIUS_GROUP
Name:
RADIUS_GROUP
Comment:
Color:
Black
Mailing List Address:
Available Members:
Selected Members:
generic*
Add >
< Remove
Show:
All
View expanded group...
OK
Cancel


Check Point Gateway - gw-46a802
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
IPSec VPN
VPN Clients
Mobile Access
Authentication
Office Mode
Portal Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Access
Authentication Method
Defined on user record (Legacy Authentication)
Username and password
RADIUS
EZMCOM_RADIUS_SERVER
View...
SecurID
View...
Personal certificate
Two-Factor Authentication with DynamicID
Global settings (under "Authentication to Gateway" on the Mobile Access tab)
Custom settings for this gateway
Configure...
Allow DynamicID for mobile devices
Certificate Authentication for mobile devices
Require client certificate when using Mobile applications
Require client certificate when using ActiveSync applications
OK
Cancel



Step x: Modify the Checkpoint page to include the EzIdentity URL.

SSH to the Checkpoint as admin

You will get

```
gw-46a802>
```

Type **expert** to enter into expert mode

```
gw-46a802> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@gw-46a802:0]#
```

cd to /opt/CPcvpn-R77/htdocs/Login

```
[Expert@gw-46a802:0]# cd /opt/CPcvpn-R77/htdocs/Login/
[Expert@gw-46a802:0]#
```

Edit the **MultiChallenge** page to add the EzIdentity URL.

Search for <\HTML> and add the EzIdentity URL just above the <\HTML>.

Before:

```
<!-- End Main Table -->
  </body>
</HTML>
```

After:

```
<!-- End Main Table -->
  </body>
<!-- EZMCOM INTEGRATION START -->
<script type="text/javascript" src="https://XXXX/ezauthservice/js/ezidentity/auth/challengeinc-
min.js"></script>
<!-- EZMCOM INTEGRATION END -->
</HTML>
```

Whereas the XXXX is the domain name of the EzIdentity server exposed to internet.