# How to Configure Captive Portal

Captive portal is one of the user identification methods available on the Palo Alto Networks firewall. Unknown users sending HTTP or HTTPS[1] traffic will be authenticated, as specified by the captive portal rulebase. There are four different captive portal scenarios, two of which involve the user being prompted for a username and password. The scenarios are:

Scenario 1: **Web form login page – transparent mode**

- The firewall temporarily hijacks the web session in order to present the login page
- Use cases: legacy method, so this should only be used for testing purposes
- Advantage: simplest to configure
- Disadvantage: the user will get a browser security warning, since the firewall's certificate is not the appropriate certificate for the destination web site

Scenario 2: **Web form login page- redirect mode**

- The user is redirected to an L3 interface on the firewall that presents the login page
- Use cases: to identify users in a guest network, kiosk environment, or on non-Windows machines
- Advantage: the user will not get a browser security warning

Scenario 3: **Client Certificate**

- A certificate is used to authenticate the client
- Use case: when the organization has a PKI infrastructure and all users are issued certificates, for example on a smartcard
- Advantage: the user is not prompted to type in a username/password
- Disadvantage: significant effort required to set up a PKI infrastructure

Scenario 4: **NTLM authentication**

- Windows users running IE or Firefox can authenticate via NTLM, without any user intervention. If the user's browser does not support NTLM, the device presents the web form login page.
- Use cases: Microsoft systems that are using cached credentials
- Advantage: the user is not prompted to login

[1] HTTPS when doing SSL decryption will trigger the captive portal login process as of PANOS 4.0.4.

- Disadvantage: only works on Windows clients using IE or Firefox

This document lists the steps to configure captive portal for these scenarios.

## Preparation steps

- The steps in this doc build upon previous scenarios: you must perform the scenario 1 steps first, and work your way through each successive scenario.

- The Palo Alto Networks firewall must be inline in the network, and configured to allow traffic to flow through the device. The interfaces can be in vwire, L2, or L3. This document discusses installation in an L3 network. For more information on installing in an L2 network, refer to this knowledge base article: https://live.paloaltonetworks.com/docs/DOC-1138

- Determine what authentication method you will be using. If querying an external server, it must be accessible by the Palo Alto Networks firewall. Possible authentication servers are: local database, RADIUS, LDAP, Kerberos, and Active Directory. User accounts must already be defined on the authentication server. New in PANOS 4.0, client certificates can be used to authenticate. If you choose this authentication method, a PKI infrastructure must be in place in your organization.

- For scenario 4 (NTLM Auth), you must have a PAN-agent running on the network.

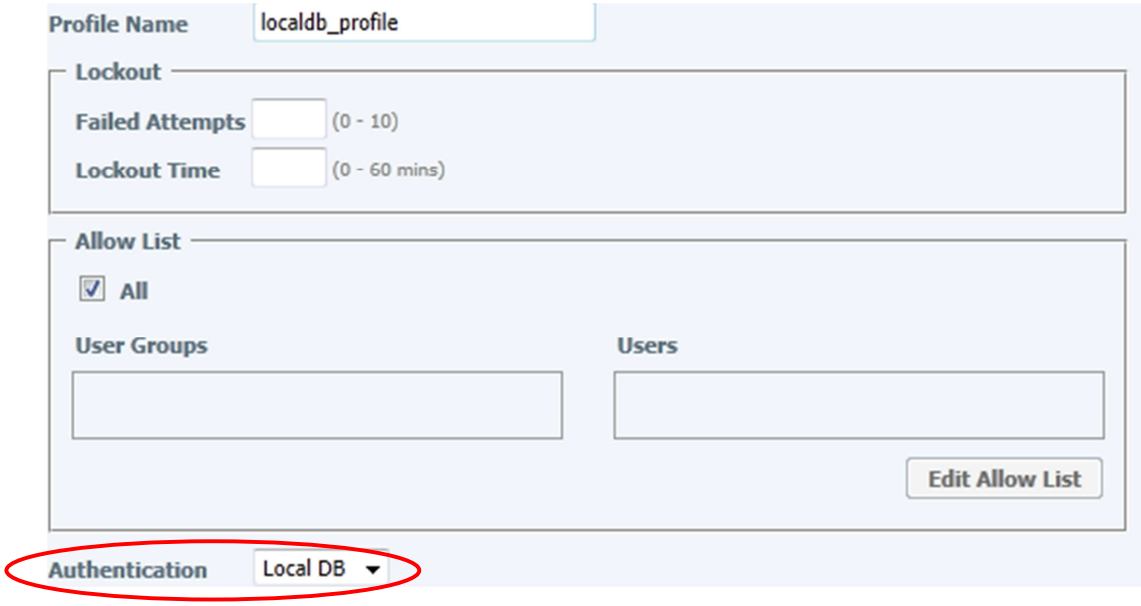
# Scenario 1: Web Form Login – Transparent Mode

In the example configurations shown in this document, the device has two interfaces in Layer3: one in the guest zone, one in the external zone. The goal is to attempt to authenticate users in the guest zone who are trying to access the external zone.

## Part 1: Define the Authentication Server Settings and Profile

1. You can use the local firewall database for authentication. If you want to define an external authentication server, go to **Device** tab-> **Server Profiles**. Select the type of authentication server that you have in your network: RADIUS, LDAP, or Kerberos, and add a new authentication server on that screen. The example configuration shown here will use the local database. You may want to start with the local database at first, and after successful testing, modify the authentication method to be an external server.

2. Go to **Device** tab-> **Authentication Profile** and add a new profile. At the bottom of the screen, select the authentication method and authentication server that you previously defined.

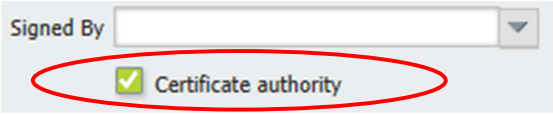



By default, all users on that server are allowed to authenticate. You can restrict that list via the Allow List in the middle of the screen.

## Part 2: Create Server Certificate and Enable Captive Portal

3. Go to the **Device** tab-> **Certificates** screen. You can choose to either **Import** a certificate or **Generate** a new certificate. For this first scenario, you will create two certificates:

   - **Generate** a CA certificate by completing the fields and checking the box at the bottom:

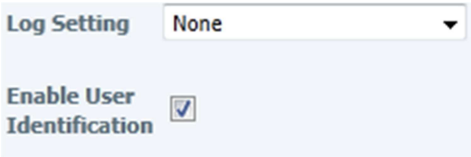
     
     

     No spaces are allowed in the certificate name.

   - **Generate** another certificate, making this one be signed by the CA you just created**.** For common name, enter in the IP address of the interface in the guest zone. Here are the two newly-created certificates:

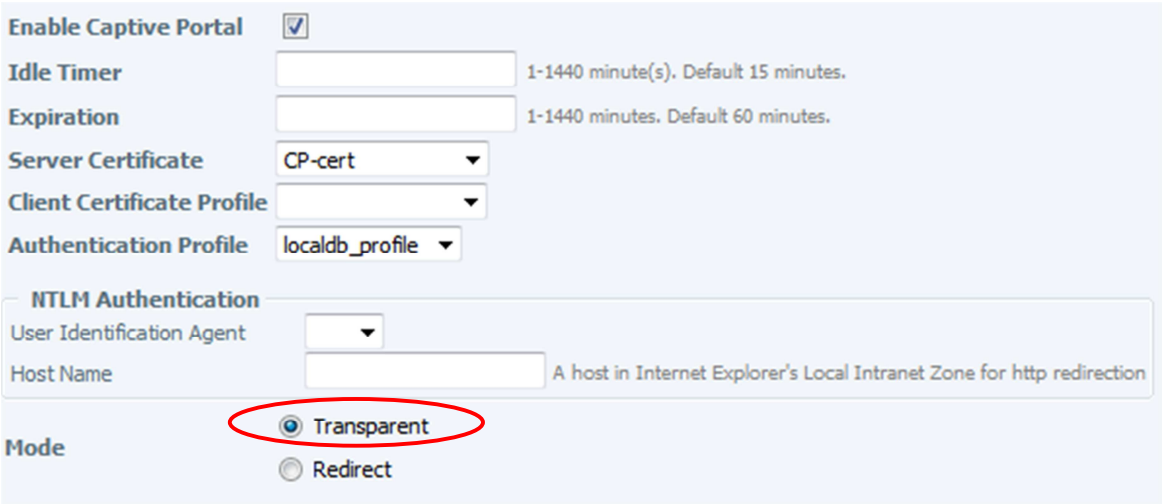
| | Name | Common Name | Certificate Authority | Private Key | Expires | Usage |
|---|---|---|---|---|---|---|
| | CP-cert | 192.168.1.1 | | ✔ | Jul 25 2021 | |
| | PA-CertAuthority | PA-CA | ✔ | ✔ | Jul 23 2021 | |

4. Go to **Network** tab -> **Zone** screen. On the zones that contain the users to be identified, enable user identification:

5. Go to the **Device** tab-> **User Identification** screen. **Edit** the Captive Portal settings. Configure the following settings:
    - Enable captive portal
    - Configure the timers as you see fit:
        - **Idle timer**- If there is no traffic going to/from the user's IP address, the idle timer will count down. Once it reaches zero, that user's entry will be removed from the authentication table, and the user will need to re-authenticate.
        - **Expiration timer**- Maximum amount of time the user is allowed to send traffic. This is an absolute time, starting at the time the user first authenticates. After this amount of time, the user must re-authenticate.
        - Note that users will not need to re-authenticate if session cookies are enabled. Session cookies supersedes the two timers above. Session cookies are discussed on page 11.
    - Pull down to select your captive portal certificate
    - Select your authentication profile as you defined previously
    - Choose the mode as follows:
        - **transparent** – legacy method, use this if you are doing your initial testing. The firewall presents a web form to the user.
        - **redirect**- recommended method, use this if you want to redirect the session to a dedicated web page on the firewall, or if you want to do NTLM authentication.

For this first scenario, here is an example configuration:



## Part 3: Configure Security Policies and Captive Portal Policies

6. Go to the **Policies** tab -> **Security** rulebase. Configure the policies to allow traffic to flow between appropriate zones. In this example, users on the guest zone are allowed to send DNS, ping, and HTTP traffic:

| | Source | | | Destination | | | | |
|---|---|---|---|---|---|---|---|---|
| Name | Zone | Address | User | Zone | Address | Application | Service | Action |
| allow ping DNS HTTP for guests | guest | any | any | external | any | dns<br>ping<br>web-browsing | any | |
| deny all other guest traffic | guest | any | any | any | any | any | any | |

We want to make sure those guest users login with an appropriate username/password however, so a captive portal policy must be configured.

7. Go to the **Policies** tab -> **Captive Portal** rulebase. Configure a rule that requires the users to authenticate. Note that possible actions/methods for these policies are:
   - **captive-portal** – this option presents a web form to the user (scenarios 1 & 2), or doesn't require any user prompting if using client certificates (scenario 3)
   - **ntlm-auth** – this option attempts to use NTLM to authenticate the user behind the scenes (scenario 4)

   Thus, in this example, we want users from the guest zone to authenticate using the method "captive portal":

| | Source | | Destination | | | |
|---|---|---|---|---|---|---|
| Name | Zone | Address | Zone | Address | Service | Action |
| guest must login for web access | guest | any | external | any | default | captive-portal |

8. Commit the configuration.

## Part 4: Testing Captive Portal

9. From a machine in the guest zone, try to ping to a machine in the external zone. The ping should work, even though the user is not authenticated yet.

10. (Optional) To confirm that the captive policy rule will be used for addresses from the guest network, login to the firewall via SSH, and perform the following command:

    ```
    test cp-policy-match source x.x.x.x destination y.y.y.y
    ```

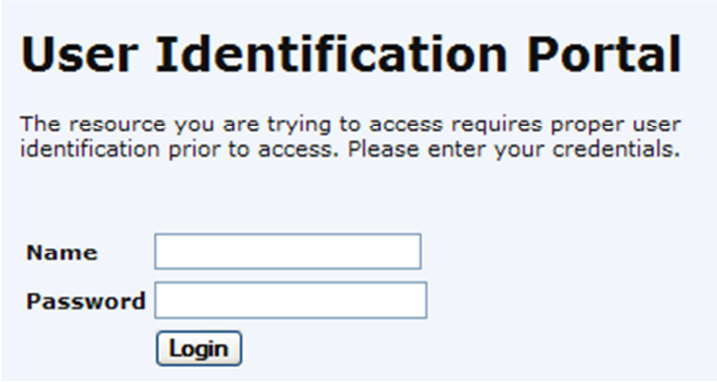
    where x.x.x.x is an IP of a machine in the guest zone, and y.y.y.y is some public IP address (an address found in the external zone). Here is an example of a success:

```
admin@PA-500> test cp-policy-match source 192.168.1.5 destination 4.2.2.2

Matched rule: 'guest must login for web access' action: captive-portal
```

11. You will now authenticate the user. From a machine in the guest zone, open a browser, and attempt to bring up an external web site using HTTP or HTTPS. (As of PANOS 4.0.4, HTTPS traffic is also intercepted, not just HTTP.) You will get a certificate error, go ahead and proceed with loading the web page.

12. You will see the captive portal login screen, as shown here:




    (Note that you can change the appearance of that page using **Device** tab -> **Response Pages**)

13. Login to the firewall with a valid username and password. Once authenticated, the originally-requested web page will be displayed. If you cannot authenticate, check the system log on the firewall, and check the authentication server and profile settings.

14. To see who is currently authenticated with the firewall, use this command:

```
show user ip-user-mapping
```

Here is example output:

```
admin@PA-500> show user ip-user-mapping

IP              Ident. By User                            Idle Timeout (s) Max. Timeout (s)
--------------- --------- ------------------------------- ---------------- ----------------
192.168.1.2     CP        guestuser                       86311            86311
```

Notice that in the "identified by" column, the value is "CP" for captive portal

15. After successfully authenticating with the firewall, the user should be able to browse to any web sites, and use any applications that are specifically permitted in the security policies.

16. For testing purposes, you can remove users from the authenticated user database using the following commands:

```
clear user-cache all
```

or

```
clear user-cache ip x.x.x.x
```

Here is an example:

```
admin@PA-500> clear user-cache ip 192.168.1.2

Entry in user cache removed!
```

If session cookies are enabled, the user's entry will be removed from the authentication table after the user closes the browser. If session cookies are not enabled, the entry will be aged out after the specified inactivity timer/expiration timer. These values are configured on the **Device** tab -> **User Identification** screen -> **Captive Portal** section.

17. Other useful troubleshooting commands:
    - To view the current captive portal policy:
      `> show running captive-portal-policy`
    - To view the captive portal config:
      `# show captive-portal`

## Scenario 2: Web Form Login – Redirect Mode

In order to configure scenario 2, you must first complete the steps in scenario 1. From that point, perform the following:

1. You must have an L3 interface on the firewall that will present the web form to the users. If the users are already in a zone that has an L3 interface, you can use that same interface to present the login page. In the example in this document, that is the case:

| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router | Tag | VLAN/ Virtual Wire | Security Zone |
|---|---|---|---|---|---|---|---|---|
| ethernet1/5 | L3 | ping and response pages | | 192.168.1.1/24 | routing_table | Untagged | | guest |

Notice that you must enable response pages on that interface via a management profile:

Note that the response pages reply on TCP ports 6080-6082, therefore the path between the unknown users and the L3 interface must allow those ports.

If the users are in a virtual-wire zone, you need to define a separate L3 interface, assign it an IP address on your network, and add the needed cabling to allow the unauthenticated users to access that IP address.

2. Go to the **Policies** tab -> **Security** screen, and make sure that there is a policy that allows the users to access the authentication IP address. In this example, a new policy was added to the top of the list:

| | Source | | | Destination | | | | |
|---|---|---|---|---|---|---|---|---|
| Name | Zone | Address | User | Zone | Address | Application | Service | Action |
| allow intra-zone traffic | guest | any | any | guest | any | any | any | |
| allow ping DNS HTTP for guests | guest | any | any | external | any | dns<br>ping<br>web-browsing | any | |
| deny all other guest traffic | guest | any | any | any | any | any | any | |

3. Obtain an SSL certificate that is signed by a CA that is trusted by the users' browsers. The certificate can be issued by a public CA, or from a CA for your organization. This certificate will be for the IP you specified in step 1. The file format for the certificate should be either:

   - Base64 encoded certificate (PEM)
   - Encrypted private key and certificate (PKCS12)

   Once you obtain the certificate, **Import** that SSL certificate on the **Device** tab -> **Certificates** page.

   Note: for testing purposes, we will use the certificate you created previously.

   Be careful! The common name on the certificate MUST MATCH EXACTLY the name or IP you specify in the address field of the Captive Portal configuration (see the next step). If it does not match, then the user will still see the security warning.

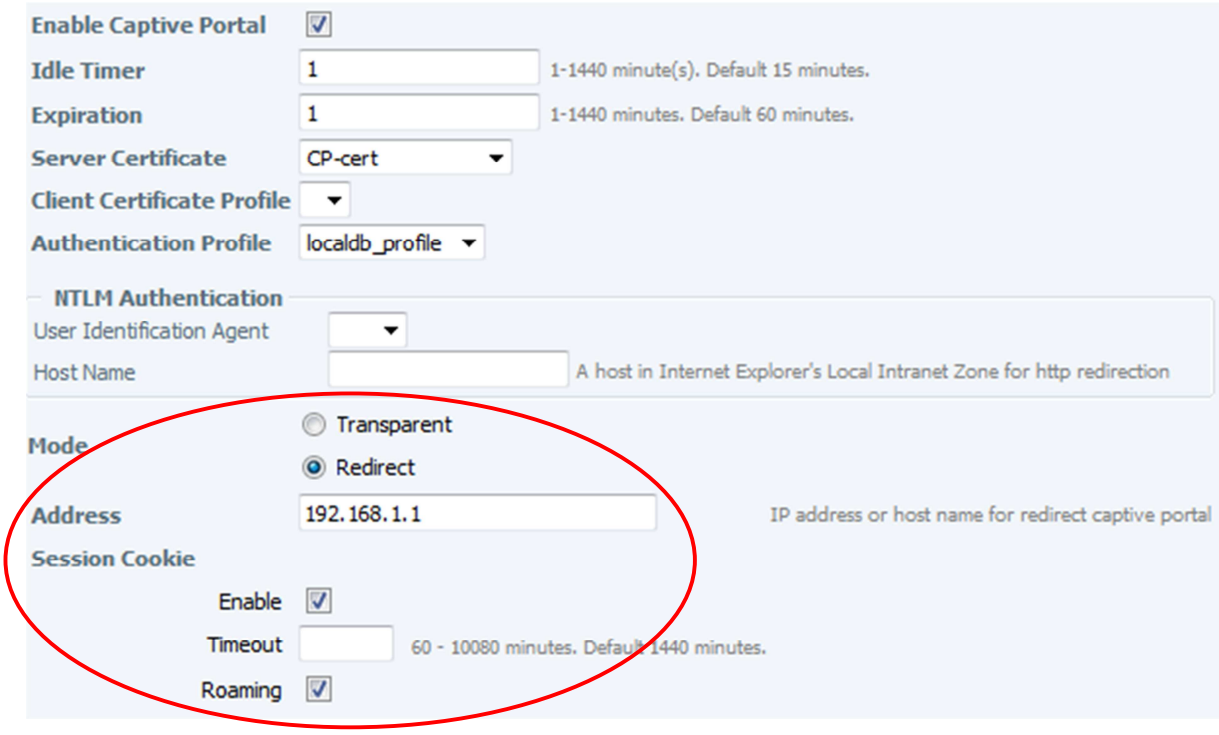
| Name | Common Name | Certificate Authority | Private Key | Expires |
|---|---|---|---|---|
| CP-cert | 192.168.1.1 | | ✔ | Jul 25 2021 |

4. On the **Device** tab -> **User Identification** page, **Edit** the captive portal configuration.
    - Server certificate: select the captive portal certificate
    - authentication profile will be the same as in the last scenario
    - mode: **redirect**
    - address: specify the IP address of the L3 interface you defined in step 1, or the hostname that resolves to that IP. Again, whatever you enter here must match the common name in the certificate you selected above
    - A **session cookie** is stored within the browser itself and is sent within each HTTP request packet. Session cookies are removed when the browser is closed. Enabling session cookie has two advantages:
        - The user will not need to re-authenticate when the idle or expiration timers trigger.
        - When **roaming** is enabled, if the machine's IP address changes, the user will be re-mapped to the new IP. Re-authentication is not required.

      The **session cookie timeout** is an absolute time value. After this period of time has passed, the user will be prompted to login again.

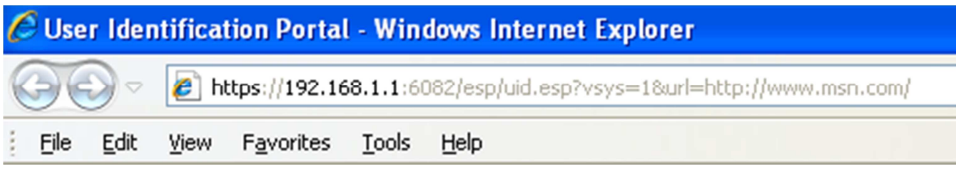
      Best practice is to enable session cookies, and to configure the idle and expiration timer to be 1 minute. That way, once the browser is closed, the association will timeout in 60 seconds.

Here is the configuration for this example:



5. Commit the configuration.

6. Test your configuration. From a machine in the guest zone, open a browser, and attempt to bring up an external web site using HTTP. You should NOT get a certificate error, the web form login page should appear immediately. At this point, you should be able to login and access web pages, as you did in scenario 1.




Notice the port number in the URL above: port 6082.

## Scenario 3: Client Certificate

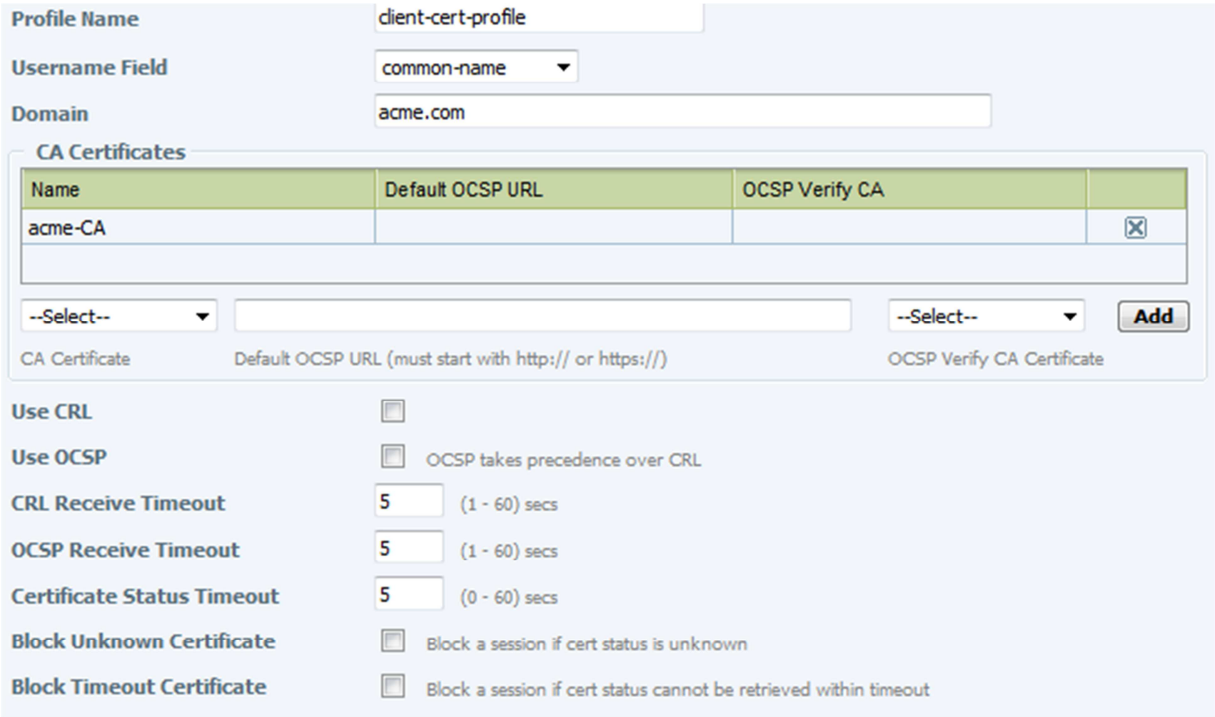
In this scenario, you cannot use the PA firewall to create certificates, you must use your organization's PKI infrastructure. Therefore, make sure the following are set up:

- the user's browser trusts the CA of the organization
- the user has a client certificate, either loaded into the browser, or on a smartcard
- the PA has loaded onto it the CA certificate of the organization

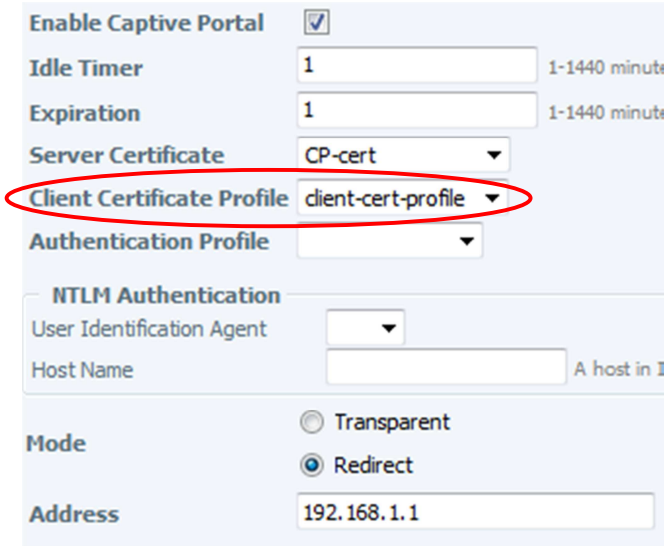
In order to configure this scenario, you must complete the steps for scenario 2. From that point, do the following:

1. On the **Device** tab -> **Client Certificate Profile** screen, create a new profile. At a minimum, complete the following fields:
    - username field: select which field in the user certificate contains the username.
    - domain: domain for the CA
    - CA certificate: add the CA certificate for the organization

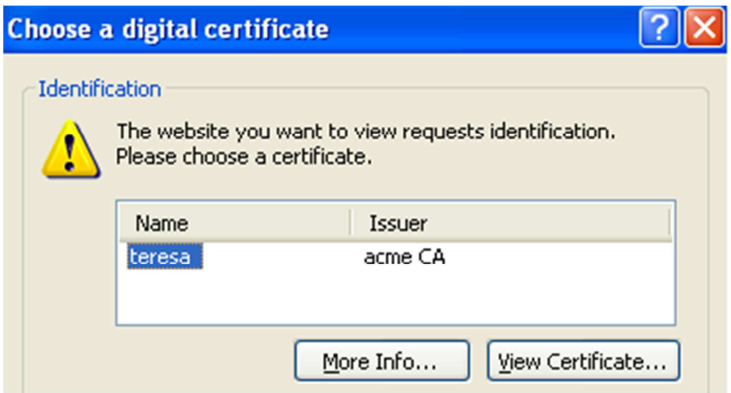
    Here is an example:



2. On the **Device** tab -> **User Identification** page, **Edit** the captive portal configuration.
   - client certificate profile: select the one you just created
   - authentication profile: leave blank if you want only certificates to be used for authentication. If you want two levels of authentication, select an authentication profile. Thus the user will be prompted for a certificate, and then presented with the web form login page.
   - Mode: **redirect**, as the user is still being redirected to a different IP address—that IP address will prompt the user for the certificate
   - Redirect address: use the same L3 interface as in previous scenarios.
   - Enable session cookies and roaming if desired




3. Confirm there is a captive portal policy in place with action “captive-portal”.
4. Commit the configuration.
5. Test your configuration. From a machine in the guest zone, open a browser, and attempt to bring up an external web site using HTTP. You should be prompted to select what certificate you want to use:




After you select a certificate, the target web site should appear.

## Scenario 4: NTLM Authentication

In this scenario, the goal is to allow the firewall to retrieve user information from the browser using NTLM, and no user intervention is required. Requirements:

- The network must be running an Active Directory domain
- The user's browser must be IE or Firefox

In order to configure this scenario, you must first complete the steps in scenario 2. From that point, perform the following:

1. Make sure there is an operational PAN-agent in the network, and the PA firewall is communicating with the PAN agent.

2. One of the configuration parameters to be specified on the PA firewall is a NetBIOS name that will resolve to the firewall's L3 interface that is serving up redirect pages. This parameter is called "host name", found on the Captive Portal configuration screen. For purposes of this discussion, let's use the string "PA_NetBIOS" as the hostname, and let's map that to 192.168.1.1.

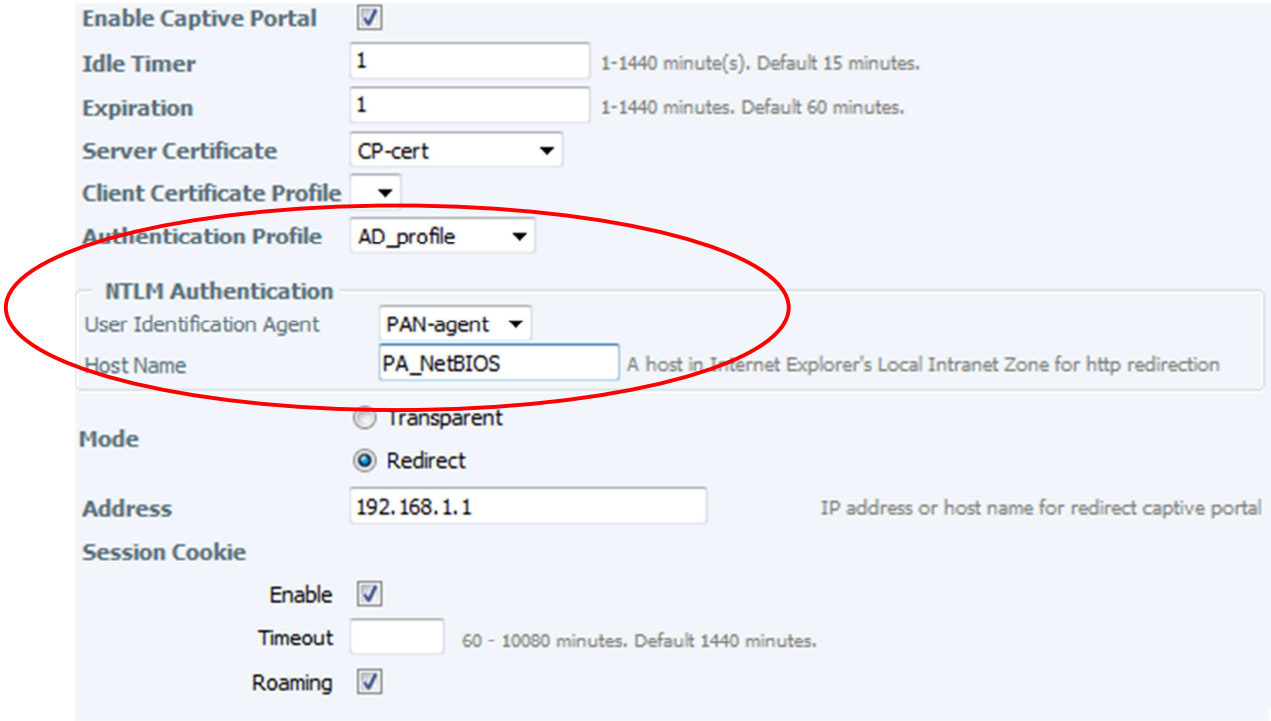
   a) My NTLM authentication host name: _____
   b) IP of the firewall's L3 interface serving redirect pages: _____

3. You must now specify how this name will be resolved by the clients. Add an entry in your DNS server that maps the hostname specified in step 2a to the IP specified in step 2b. For this example, we will map "PA_NetBIOS" to 192.168.1.1. The DNS suffix will be the same domain as the other client machines on the network.

   Thus for this example, all client machines should now be able to resolve "PA_NetBIOS" to 192.168.1.1.

4. Edit the captive portal configuration. Make the following changes:
   - Authentication profile: select an auth profile that points to the Active Directory domain controllers
   - NTLM authentication-> User Identification Agent: pull down to select the PAN agent
   - NTLM authentication -> Host Name: name you wrote in step 2a
   - Redirect address: IP you wrote in step 2b
   - Enable session cookies and roaming as you see fit

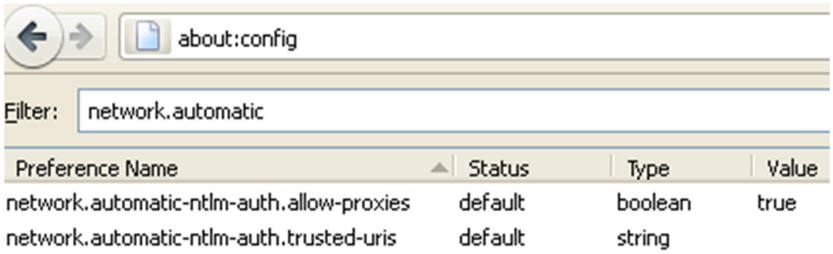
Here is an example:



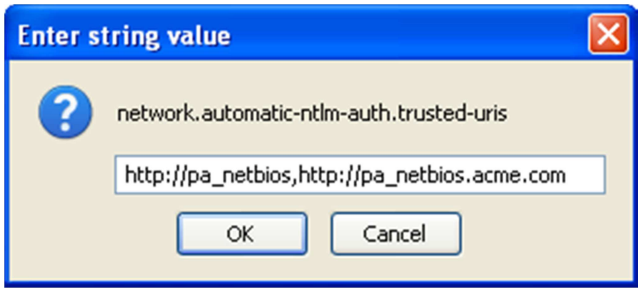

5. Edit the captive portal policy, and change the action to "NTLM-auth"

| | Source | | Destination | | | |
|---|---|---|---|---|---|---|
| Name | Zone | Address | Zone | Address | Service | Action |
| guest must login for web access | guest | any | external | any | default | ntlm-auth |

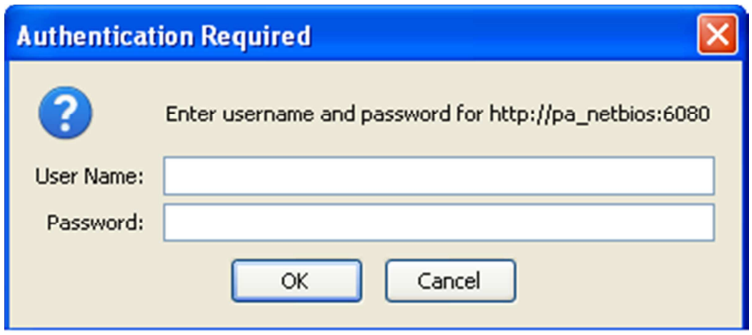
6. Commit the configuration.
7. Login to the client machine as a user in the domain. Make sure that PC can ping the NetBios hostname ("PA_NetBIOS").
8. Configure the browser (Firefox or IE) to answer NTLM authentication queries. To do so, google "enable NTLM authentication" for the particular browser you will be using. Configure the appropriate settings in the browser. For example, to configure Firefox, browse to "about:configure", and filter on "network.automatic":



Edit network.automatic-ntlm-auth.trusted-uris, and add the following URLs (the example domain here is acme.com):




9. Within the browser, attempt to bring up a web page on the Internet. The browser will receive an NTLM challenge. If everything is configured properly, the browser will reply with the username/password of the person logged in, and the requested web page will appear without the user being prompted. If you get prompted for a username/password:




Then your browser is not configured to answer the NTLM requests—go back to the previous step and confirm you configured the browser settings appropriately.

10. Once you get the web page to appear with no login prompts, you can confirm that NTLM was used for authentication by viewing the user mapping database. Run the command `show user ip-user-mapping`. You will see the method used to identify the particular client IP is NTLM:

```
admin@PA-500> show user ip-user-mapping
IP              Ident. By User                            Idle Timeout (s) Max. Timeout (s)
--------------- --------- ------------------------------- ---------------- ----------------
192.168.1.2     NTLM      teresa                          809              3168
```