Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. For additional information, refer to the following resources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://docs.paloaltonetworks.com or search the documentation.

- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.

- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.

- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Authentication

Many of the services that Palo Alto Networks firewalls and Panorama provide require authentication, including administrator access to the web interface and end user access to Captive Portal, GlobalProtect portals, and GlobalProtect gateways. The authentication methods that you can configure vary by service, and can include Kerberos single sign-on (SSO), external authentication services, certificates and certificate profiles, local database accounts, RADIUS Vendor-Specific Attributes (VSAs), and NT LAN Manager (NTLM).

The following topics describe authentication methods that are common to most firewall and Panorama services, procedures to configure them, how to test authentication profiles, and how to troubleshoot authentication issues:

- Configure an Authentication Profile and Sequence
- Configure Kerberos Single Sign-On
- Configure Local Database Authentication
- Configure External Authentication
- Test Authentication Server Connectivity
- Troubleshoot Authentication Issues
Configure an Authentication Profile and Sequence

An authentication profile defines the authentication service that validates the login credentials of firewall or Panorama administrators and Captive Portal or GlobalProtect end users. The authentication service can be a local database (firewalls only), an external service (RADIUS, TACACS+, LDAP, or Kerberos server), or Kerberos single sign-on (SSO).

Some networks have multiple databases for different users and user groups (for example, TACACS+ and LDAP). To authenticate users in such cases, configure an authentication sequence, which is a ranked order of authentication profiles that the firewall or Panorama matches a user against during login. The firewall or Panorama checks against each profile in sequence until one successfully authenticates the user. A user is denied access only if authentication fails for all the profiles in the authentication sequence.

<table>
<thead>
<tr>
<th>Configure an Authentication Profile and Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Configure an Authentication Profile and Sequence (Continued)

Step 3  Configure an authentication profile. Define one or both of the following:
- Kerberos SSO—The firewall or Panorama first tries SSO authentication. If that fails, it falls back to the specified authentication Type.
- Local database or external authentication—The firewall or Panorama prompts the user to enter login credentials, and uses its local database (firewalls only) or an external service to authenticate the user.

1. Select Device > Authentication Profile and Add the authentication profile.
2. Enter a Name to identify the authentication profile.
3. If the firewall has more than one virtual system (vsys), select a Location (a vsys or Shared) where the profile is available.
4. Select the authentication Type. If you select RADIUS, TACACS+, LDAP, or Kerberos, select the authentication Server Profile from the drop-down.
   - If the Type is LDAP, define the Login Attribute. For Active Directory, enter sAMAccountName as the value.
5. (Optional) Select the User Domain and Username Modifier options as follows to modify the domain/username string that the user will enter during login. This is useful when the authentication service requires the string in a particular format and you don’t want to rely on users to correctly enter the domain.
   - To send only the unmodified user input, leave the User Domain blank (the default) and set the Username Modifier to the variable %USERINPUT% (the default).
   - To prepend a domain to the user input, enter a User Domain and set the Username Modifier to %USERDOMAIN%\%USERINPUT%.
   - To append a domain to the user input, enter a User Domain and set the Username Modifier to %USERINPUT%@%USERDOMAIN%.
6. If you want to enable Kerberos SSO, enter the Kerberos Realm (usually the DNS domain of the users, except that the realm is UPPERCASE) and Import the Kerberos Keytab that you created for the firewall or Panorama.
7. Select Advanced and Add the users and groups that can authenticate with this profile. You can select users and groups from the local database or, if you configured an LDAP server profile, from an LDAP-based directory service such as Active Directory. Selecting all allows every user to authenticate. By default, the list is empty, meaning no users can authenticate.
   - You can also create and allow custom groups based on LDAP filters: see Map Users to Groups.
8. Enter the number of Failed Attempts (0-10) to log in that the firewall or Panorama allows before locking out the user. The default value 0 means there is no limit.
9. Enter the Lockout Time (0-60), which is the number of minutes for which the firewall or Panorama locks out the user after reaching the Failed Attempts limit. The default value 0 means the lockout applies until an administrator unlocks the user account.
10. Click OK to save the authentication profile.
### Configure an Authentication Profile and Sequence

**Step 4** Configure an authentication sequence.
- Required if you want the firewall or Panorama to try multiple authentication profiles to authenticate users. The firewall or Panorama evaluates the profiles in top-to-bottom order until one profile successfully authenticates the user.

1. Select **Device > Authentication Sequence** and **Add** the authentication sequence.
2. Enter a **Name** to identify the authentication sequence.
3. If the firewall has more than one virtual system (vsys), select a **Location** (a vsys or **Shared**) where the sequence is available.
   
   To expedite the authentication process, the best practice is to use domain to determine authentication profile: the firewall or Panorama will match the domain name that a user enters during login with the **User Domain** or **Kerberos Realm** of an authentication profile in the sequence, and then use that profile to authenticate the user. If the firewall or Panorama doesn’t find a match, or if you clear the check box, it tries the profiles in the top-to-bottom sequence.

4. **Add** each authentication profile. To change the evaluation order of the profiles, select a profile and **Move Up** or **Move Down**.
5. Click **OK** to save the authentication sequence.

**Step 5** Assign the authentication profile or sequence.

Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.

- Test **Authentication Server Connectivity** to verify that an authentication profile can communicate with the back-end authentication server and that the authentication request succeeded.
Configure Kerberos Single Sign-On

Palo Alto Networks firewalls and Panorama support Kerberos V5 single sign-on (SSO) to authenticate administrators to the web interface and end users to Captive Portal. A network that supports Kerberos SSO prompts a user to log in only for initial access to the network (for example, logging in to Microsoft Windows). After this initial login, the user can access any browser-based service in the network (for example, the firewall web interface) without having to log in again until the SSO session expires. (Your Kerberos administrator sets the duration of SSO sessions.) If you enable both Kerberos SSO and external authentication services (for example, a RADIUS server), the firewall or Panorama first tries SSO and, only if that fails, falls back to the external service for authentication.

To support Kerberos SSO, your network requires:
- A Kerberos infrastructure, including a key distribution center (KDC) with an authentication server (AS) and ticket-granting service (TGS).
- A Kerberos account for the firewall or Panorama that will authenticate users. An account is required to create a Kerberos keytab, which is a file that contains the principal name and hashed password of the firewall or Panorama. The SSO process requires the keytab.

### Configure Kerberos Single Sign-On

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Create a Kerberos keytab. The keytab is a file that contains the principal name and password of the firewall, and is required for the SSO process. When you configure Kerberos in your Authentication Profile and Sequence, the firewall first checks for a Kerberos SSO hostname. If you provide a hostname, the firewall searches the keytabs for a service principal name that matches the hostname and uses only that keytab for decryption. If you do not provide a hostname, the firewall tries each keytab in the authentication sequence until it is able to successfully authenticate using Kerberos.</td>
</tr>
<tr>
<td>7</td>
<td>Import the keytab into an authentication profile.</td>
</tr>
<tr>
<td>8</td>
<td>Assign the authentication profile to the administrator account or to the Captive Portal settings.</td>
</tr>
</tbody>
</table>

Configure an Authentication Profile and Sequence:
- Enter the Kerberos Realm (usually the DNS domain of the users, except that the realm is uppercase).
- Import the Kerberos Keytab that you created for the firewall or Panorama.

If the firewall is in FIPS/CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. Otherwise, you can also use des3-cbc-sha1 or arcfour-hmac. To use an Advanced Encryption Standard (AES) algorithm, the functional level of the KDC must be Windows Server 2008 or later and you must enable AES encryption for the firewall or Panorama account.

The algorithm in the keytab must match the algorithm in the service ticket that the TGS issues to clients. Your Kerberos administrator determines which algorithms the service tickets use.
Configure Local Database Authentication

You can use a local firewall database instead of an external service to manage user account credentials and authentication. For example, you might create a local database of users and user groups for specialized purposes if you don't have permission to add them to the directory servers that your organization uses to manage regular accounts and groups. Local database authentication is available for firewall administrators and for Captive Portal and GlobalProtect end users.

If your network supports Kerberos single sign-on (SSO), you can configure local authentication as a fall-back in case SSO fails. For details, see Configure Kerberos SSO and External or Local Authentication for Administrators. You can also Configure an Administrative Account to use local account management and authentication without a local database, but only for firewall administrators.

<table>
<thead>
<tr>
<th>Configure Local Database Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>4.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td>Set the authentication Type to Local Database.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td>- Administrators—Configure an Administrative Account:</td>
</tr>
<tr>
<td>- Specify the Name of a user you defined in Step 1.</td>
</tr>
<tr>
<td>- Assign the Authentication Profile that you configured for the account.</td>
</tr>
<tr>
<td>- End users—For all services, you must assign the Authentication Profile that you configured for the accounts:</td>
</tr>
<tr>
<td>- Configure Captive Portal.</td>
</tr>
<tr>
<td>- Configure the GlobalProtect portal.</td>
</tr>
<tr>
<td>- Configure the GlobalProtect gateway.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td>Test a Local Database Authentication Profile.</td>
</tr>
</tbody>
</table>
Configure External Authentication

Palo Alto Networks firewalls and Panorama can use external servers for many services that require authentication, including administrator access to the web interface and end user access to Captive Portal, GlobalProtect portals and GlobalProtect gateways. The server protocols that firewalls and Panorama support include Lightweight Directory Access Protocol (LDAP), Kerberos, Terminal Access Controller Access-Control System Plus (TACACS+), and Remote Authentication Dial-In User Service (RADIUS). If you enable both external authentication and Kerberos single sign-on (SSO), the firewall or Panorama first tries SSO and, only if that fails, falls back to the external server for authentication. To configure external authentication, you create an authentication server profile, assign it to an authentication profile, and then enable authentication for an administrator account or firewall/Panorama service by assigning the authentication profile to it.

- Configure Authentication Server Profiles
- Enable External Authentication for Users and Services

Configure Authentication Server Profiles

- Configure a RADIUS Server Profile
- Set CHAP or PAP Authentication for RADIUS Servers
- RADIUS Vendor-Specific Attributes Support
- Configure a TACACS+ Server Profile
- Configure an LDAP Server Profile
- Configure a Kerberos Server Profile

Configure a RADIUS Server Profile

You can configure the firewall or Panorama to use a RADIUS server for managing administrator accounts. You can also configure the firewall to use a RADIUS server for authenticating end users and collecting RADIUS Vendor-Specific Attributes (VSAs) from GlobalProtect clients.

When you predefine dynamic administrator roles on the server, use lower-case to specify the role (for example, enter `superuser`, not `SuperUser`).

To use a RADIUS server for managing administrator accounts or collecting GlobalProtect clients VSAs, you must define VSAs on the RADIUS server. For details, see the list of supported RADIUS Vendor-Specific Attributes Support.
Configure External Authentication

Authentication

Configure a RADIUS Server Profile

Step 1  Add a RADIUS server profile.

1. Select Device > Server Profiles > RADIUS and click Add.
2. Enter a Profile Name to identify the server profile.
3. For a firewall with more than one virtual system (vsys), select the Location (vsys or Shared) where the profile is available.
4. For the Timeout, enter an interval in seconds after which an authentication request times out (range is 1-30, default is 3).
5. Enter the number of automatic Retries following a Timeout before the request fails (range is 1-5, default is 3).
6. For each RADIUS server, click Add and enter a Name (to identify the server), server IP address or FQDN (RADIUS Server field), Secret/Confirm Secret (a key to encrypt passwords), and server Port for authentication requests (default is 1812).
   If you use an FQDN address object to identify the server and you subsequently change the address, you must commit the change for the new server address to take effect.
7. Click OK.

Step 2  Implement the RADIUS server profile.

1. Assign the RADIUS server profile to an authentication profile or sequence.
2. Test a RADIUS Authentication Profile to verify that the firewall or Panorama can connect to the RADIUS server.
3. Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.
4. Commit your changes.

Set CHAP or PAP Authentication for RADIUS Servers

When you configure the firewall to use RADIUS server authentication for a particular service (such as Captive Portal), it first tries Challenge-Handshake Authentication Protocol (CHAP) and falls back to Password Authentication Protocol (PAP) under certain conditions. Optionally, you can override this automatic protocol selection and configure the firewall or Panorama to always use a specific protocol. For details, see Set CHAP or PAP Authentication for RADIUS Servers.

When sending authentication requests to a RADIUS server, the firewall and Panorama use the authentication profile name as the network access server (NAS) identifier, even if the profile is assigned to an authentication sequence for the service that initiates the authentication process.
If you want the firewall to always use a specific protocol for authenticating to the RADIUS server, enter the following operational CLI command (the `auto` option reverts to the default automatic selection):

```
set authentication radius-auth-type [ auto | chap | pap ]
```

When configuring a RADIUS server for CHAP, you must define user accounts with reversibly encrypted passwords. Otherwise, CHAP authentication will fail.

### RADIUS Vendor-Specific Attributes Support

Palo Alto Networks firewalls and Panorama support the following RADIUS Vendor-Specific Attributes (VSAs). To define VSAs on a RADIUS server, you must specify the vendor code (25461 for Palo Alto Networks firewalls or Panorama) and the VSA name and number. Some VSAs also require a value.

<table>
<thead>
<tr>
<th>Name</th>
<th>Number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VSAs for administrator account management and authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaloAlto-Admin-Role</td>
<td>1</td>
<td>A default (dynamic) administrative role name or a custom administrative role name on the firewall.</td>
</tr>
<tr>
<td>PaloAlto-Admin-Access-Domain</td>
<td>2</td>
<td>The name of an access domain for firewall administrators (configured in the <strong>Device &gt; Access Domains</strong> page). Define this VSA if the firewall has multiple virtual systems.</td>
</tr>
<tr>
<td>PaloAlto-Panorama-Admin-Role</td>
<td>3</td>
<td>A default (dynamic) administrative role name or a custom administrative role name on Panorama.</td>
</tr>
<tr>
<td>PaloAlto-Panorama-Admin-Access-Domain</td>
<td>4</td>
<td>The name of an access domain for Device Group and Template administrators (configured in the <strong>Panorama &gt; Access Domains</strong> page).</td>
</tr>
<tr>
<td>PaloAlto-User-Group</td>
<td>5</td>
<td>The name of a user group that an authentication profile references.</td>
</tr>
<tr>
<td><strong>VSAs forwarded from GlobalProtect clients to the RADIUS server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaloAlto-User-Domain</td>
<td>6</td>
<td>Don't specify a value when you define these VSAs.</td>
</tr>
<tr>
<td>PaloAlto-Client-Source-IP</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>PaloAlto-Client-OS</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>PaloAlto-Client-Hostname</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>PaloAlto-GlobalProtect-Client-Version</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>
Configure a TACACS+ Server Profile

Terminal Access Controller Access-Control System Plus (TACACS+) protocol provides better Authentication security than RADIUS because it encrypts usernames and passwords (instead of just passwords), and is also more reliable (it uses TCP instead of UDP).

When authenticating to the TACACS+ server, the firewall first tries Challenge-Handshake Authentication Protocol (CHAP) and falls back to Password Authentication Protocol (PAP) if the server rejects the CHAP request. This will happen if, for example, the server doesn’t support CHAP or isn’t configured for CHAP. CHAP is the preferred protocol because it is more secure than PAP. After falling back to PAP for a particular TACACS+ server, the firewall uses only PAP in subsequent attempts to authenticate to that server. The firewall records a fall back to PAP as a medium severity event in the System logs. If you modify any fields in the TACACS+ server profile and then commit the changes, the firewall reverts to first trying CHAP for that server.

When you predefine dynamic administrator roles on the server, use lower-case to specify the role (for example, enter superuser, not SuperUser).

Configure a TACACS+ Server Profile

**Configure a TACACS+ Server Profile**

**Step 1**  Add a TACACS+ server profile.

1. Select **Device > Server Profiles > TACACS+** and click **Add**.
2. Enter a **Profile Name** to identify the server profile.
3. For a firewall with more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.
4. For the **Timeout**, enter an interval in seconds after which an authentication request times out (range is 1-20, default is 3).
5. Select the **Use single connection for all authentication** check box to use the same TCP session for all authentications that use this profile. This option improves performance by avoiding the need to start and end a separate TCP session for each authentication. The check box is cleared by default.
6. For each TACACS+ server, click **Add** and enter a **Name** (to identify the server), server IP address or FQDN (TACACS+ **Server** field), **Secret/Confirm Secret** (a key to encrypt usernames and passwords), and server **Port** for authentication requests (default is 49).

   If you use an FQDN address object to identify the server and you subsequently change the address, you must commit the change for the new server address to take effect.

7. Click **OK**.

**Step 2**  Implement the TACACS+ server profile.

1. Assign the TACACS+ server profile to an authentication profile or sequence.
2. Test a TACACS+ Authentication Profile to verify that the firewall or Panorama can connect to the TACACS+ server.
3. Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.
4. **Commit** your changes.
Configure an LDAP Server Profile

An LDAP server profile enables you to:

- Authenticate administrators and end users of Palo Alto Networks firewalls and Panorama.
- Define security rules based on user or user group. The LDAP server profile instructs the firewall how to connect and authenticate to the server and how to search the directory for user and group information. You must also configure User-ID to Map Users to Groups. Then you can select users or groups when defining policy rules.
Configure an LDAP Server Profile

**Step 1** Add an LDAP server profile.

1. Select Device > Server Profiles > LDAP and click Add.
2. Enter a Profile Name to identify the server profile.
3. For a firewall with more than one virtual system (vsys), select the Location (vsys or Shared) where the profile is available.
4. For each LDAP server (up to four), click Add and enter a Name (to identify the server), server IP address (LDAP Server field), and server Port (default 389).
5. Select the server Type from the drop-down: active-directory, e-directory, sun, or other.
6. If you want the firewall or Panorama to use SSL or TLS for a more secure connection with the directory server, select the Require SSL/TLS secured connection check box (it is selected by default). The protocol that the firewall or Panorama uses depends on the server Port:
   - 389 (default)—TLS (Specifically, the firewall or Panorama uses the Start TLS operation, which upgrades the initial plaintext connection to TLS.)
   - 636—SSL
   - Any other port—The firewall or Panorama first tries to use TLS. If the directory server doesn't support TLS, the firewall or Panorama falls back to SSL.
7. To improve security, you can select the Verify Server Certificate for SSL sessions check box (it is cleared by default) so that the firewall or Panorama verifies the certificate that the directory server presents for SSL/TLS connections. If the verification fails, the connection fails. To enable verification, you must also select the Require SSL/TLS secured connection check box. The firewall or Panorama verifies the certificate in two respects:
   - The certificate is trusted and valid. For the firewall or Panorama to trust the certificate, its root certificate authority (CA) and any intermediate certificates must be in the certificate store under Device > Certificate Management > Certificates > Device Certificates. Import the certificate if necessary: see Import a Certificate and Private Key.
   - The certificate name must match the host Name of the LDAP server. The firewall or Panorama first checks the certificate attribute Subject AltName for matching, then tries the attribute Subject DN. If the certificate uses the FQDN of the directory server, you must enter that FQDN in the LDAP Server field for the name matching to succeed.
8. Click OK.
## Configure an LDAP Server Profile (Continued)

**Step 2** Implement the LDAP server profile.

1. Assign the LDAP server profile to an authentication profile or sequence.
2. Test an LDAP Authentication Profile to verify that the firewall or Panorama can connect to the LDAP server.
3. Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.
4. Commit your changes.

---

### Configure a Kerberos Server Profile

A Kerberos server profile enables users to natively authenticate to an Active Directory domain controller or a Kerberos V5-compliant authentication server. This authentication method is interactive, requiring users to enter usernames and passwords, in contrast with Kerberos single sign-on (SSO), which involves transparent authentication.

To use a Kerberos server for authentication, the server must be accessible over an IPv4 address. IPv6 addresses are not supported.

---

### Configure a Kerberos Server Profile

**Step 1** Add a Kerberos server profile.

1. Select Device > Server Profiles > Kerberos and click Add.
2. Enter a Profile Name to identify the server profile.
3. For a firewall with more than one virtual system (vsys), select the Location (vsys or Shared) where the profile is available.
4. For each Kerberos server, click Add and enter a Name (to identify the server), server IPv4 address or FQDN (Kerberos Server field), and an optional Port number for communication with the server (default 88).
   
   If you use an FQDN address object to identify the server and you subsequently change the address, you must commit the change for the new server address to take effect.

5. Click OK.

**Step 2** Implement the Kerberos server profile.

1. Assign the Kerberos server profile to an authentication profile or sequence.
2. Test a Kerberos Authentication Profile to verify that the firewall or Panorama can connect to the Kerberos server.
3. Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.
4. Commit your changes.
Enable External Authentication for Users and Services

Palo Alto Networks firewalls and Panorama can use external services to authenticate administrators and end users.

<table>
<thead>
<tr>
<th>Enable External Authentication</th>
</tr>
</thead>
</table>
| **Step 1** Configure an external server profile. | • Configure a RADIUS Server Profile.  
• Configure a TACACS+ Server Profile.  
• Configure an LDAP Server Profile.  
• Configure a Kerberos Server Profile. |
| **Step 2** Assign the server profile to an authentication profile.  
Optionally, you can assign multiple authentication profiles to an authentication sequence. | 1. Configure an Authentication Profile and Sequence.  
2. Test Authentication Server Connectivity. |
| **Step 3** Assign the authentication profile or sequence to an administrator account or to a firewall service for end users. | • Administrators: Configure an Administrative Account.  
• End user services:  
  • Configure Captive Portal.  
  • Configure the GlobalProtect portal.  
  • Configure the GlobalProtect gateway. |
Test Authentication Server Connectivity

After you configure an authentication profile on a Palo Alto Networks firewall or Panorama, you can use the test authentication feature to determine if it can communicate with the back-end authentication server and if the authentication request succeeded. You can additionally test authentication profiles used for GlobalProtect and Captive Portal authentication. You can perform authentication tests on the candidate configuration, so that you know the configuration is correct before committing.

Authentication server connectivity testing is supported for local database, RADIUS, TACACS+, LDAP, and Kerberos authentication.

The following topics describe how to use the test authentication command and provides examples:

- Run the Test Authentication Command
- Test a Local Database Authentication Profile
- Test a RADIUS Authentication Profile
- Test a TACACS+ Authentication Profile
- Test an LDAP Authentication Profile
- Test a Kerberos Authentication Profile

Run the Test Authentication Command

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the PAN-OS firewall or Panorama server, <a href="#">Configure an authentication profile</a>. You do not need to commit the authentication or server profile configuration prior to testing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys. To define the target vsys: <code>admin@PA-3060&gt; set system setting target-vsys &lt;vsys-name&gt;</code> For example, if the user is defined in vsys2, run the following command: <code>admin@PA-3060&gt; set system setting target-vsys vsys2</code> The target-vsys command is per-login session, so the system clears the option when you log off.</td>
</tr>
</tbody>
</table>
Run the Test Authentication Command

**Step 4** Test an authentication profile by entering the following command:

```
admin@PA-3060> test authentication authentication-profile <authentication-profile-name> username <username> password
```

For example, to test an authentication profile named my-profile for a user named bsimpson, run the following command:

```
admin@PA-3060> test authentication authentication-profile my-profile username bsimpson password
```

When entering authentication profile names and server profile names in the test command, the names are case sensitive. Also, if the authentication profile has a username modifier defined, you must enter the modifier with the username. For example, if you add the username modifier `%USERINPUT%@%USERDOMAIN%` for a user named bsimpson and the domain name is mydomain.com, enter bsimpson@mydomain.com as the username. This will ensure that the correct credentials are sent to the authentication server. In this example, mydomain.com is the domain that you define in the User Domain field in the Authentication profile.

---

**Step 5** View the output of the test results.

If the authentication profile is configured correctly, the output displays `Authentication succeeded`. If there is a configuration issue, the output displays information to help you troubleshoot the configuration.

For example use cases on the supported authentication profile types, see [Test Authentication Server Connectivity](#).

The output results vary based on several factors related to the authentication type that you are testing as well as the type of issue. For example, RADIUS and TACACS+ use different underlying libraries, so the same issue that exists for both of these types will produce different errors. Also, if there is a network problem, such as using an incorrect port or IP address in the authentication server profile, the output error is not specific. This is because the test command cannot perform the initial handshake between the firewall and the authentication server to determine details about the issue.

---

Test a Local Database Authentication Profile

The following example shows how to test a Local Database authentication profile named LocalDB for a user named User1-LocalDB and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

**Local Database Authentication Profile Test Example**

**Step 1** On the PAN-OS firewall, ensure that you have an administrator configured with the type Local Database. For information on administrator accounts, refer to [Manage Firewall Administrators](#).

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.
Step 3 (Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys. To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```
The `target-vsys` command is per-login session, so the system clears the option when you log off.

Step 4 Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile LocalDB-Profile username User1-LocalDB password
```

Step 5 When prompted, enter the password for the User1-LocalDB account. The following output shows that the test failed:

```
Allow list check error:
Do allow list check before sending out authentication request...
User User1-LocalDB is not allowed with authentication profile LocalDB-Profile
```
In this case, the last line of the output shows that the user is not allowed, which indicates a configuration problem in the authentication profile.

Step 6 To resolve this issue, modify the authentication profile and add the user to the Allow List.

1. On the firewall, select **Device > Authentication Profile** and modify the profile named LocalDB-Profile.
2. Click the **Advanced** tab and add User1-LocalDB to the Allow List.
3. Click **OK** to save the change.

Step 7 Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
nname "User1-LocalDB" has an exact match in allow list
Authentication by Local User Database for user "User1-LocalDB"
Authentication succeeded for Local User Database user "User1-LocalDB"
```

Test a RADIUS Authentication Profile

The following example shows how to test a RADIUS profile named RADIUS-Profile for a user named User2-RADIUS and how to troubleshoot error conditions that arise. For details on using the test authentication command, see **Run the Test Authentication Command**.

RADIUS Authentication Profile Test Example

Step 1 On the PAN-OS firewall, **Configure a RADIUS Server Profile** and **Configure an authentication profile**. In the authentication profile, you select the new RADIUS server profile in the **Server Profile** drop-down.

Step 2 Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.
**RADIUS Authentication Profile Test Example**

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys. To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```

The `target-vsys` command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile RADIUS-Profile username User2-RADIUS password
```

**Step 5** When prompted, enter the password for the User2-RADIUS account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User2-RADIUS" is in group "all"
Authentication to RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"
Egress: 10.5.104.98
Authentication type: CHAP
Now send request to remote server ...
RADIUS error: Invalid RADIUS response received - Bad MD5
Authentication failed against RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"
```

In this case, the output shows Bad MD5, which indicates that there may be an issue with the secret defined in the RADIUS server profile.

**Step 6** To resolve this issue, modify the RADIUS server profile and ensure that the secret defined on the RADIUS server matches the secret in the server profile.

1. On the firewall, select Device > Server Profiles > RADIUS and modify the profile named RADIUS-Profile.
2. In the Servers section, locate the RADIUS server and modify the Secret field.
3. Type in the correct secret and then retype to confirm.
4. Click OK to save the change.

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
name "User2-RADIUS" is in group "all"
Authentication to RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"
Egress: 10.5.104.98
Authentication type: CHAP
Now send request to remote server ...
RADIUS CHAP auth request is NOT accepted, try PAP next
Authentication type: PAP
Now send request to remote server ...
Authentication succeeded against RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"
Authentication succeeded for user "User2-RADIUS"
```
Test a TACACS+ Authentication Profile

The following example shows how to test a TACACS+ profile named TACACS-Profile for a user named User3-TACACS and how to troubleshoot error conditions that arise. For details on using the test authentication command, see Run the Test Authentication Command.

### TACACS+ Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, Configure a TACACS+ Server Profile and Configure an authentication profile. In the authentication profile, you select the new TACACS+ server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```

The `target-vsys` command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile TACACS-Profile username User3-TACACS password
```

**Step 5** When prompted, enter the password for the User3-TACASC account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User2-TACACS" is in group "all"
Authentication to TACACS+ server at '10.5.196.62' for user 'User2-TACACS'
Server port: 49, timeout: 30, flag: 0
Egress: 10.5.104.98
Attempting CHAP authentication ...
CHAP authentication request is created
Sending credential: xxxxxx
Failed to send CHAP authentication request: Network read timed out
Attempting PAP authentication ...
PAP authentication request is created
Failed to send PAP authentication request: Network read timed out
Returned status: -1
Authentication failed against TACACS+ server at 10.5.196.62:49 for user User2-TACACS
Authentication failed for user "User2-TACACS"
The output shows error Network read timed out, which indicates that the TACACS+ server could not decrypt the authentication request. In this case, there may be an issue with the secret defined in the TACACS+ server profile.

**Step 6** To resolve this issue, modify the TACACS+ server profile and ensure that the secret defined on the TACACS+ server matches the secret in the server profile.

1. On the firewall, select **Device > Server Profiles > TACACS** and modify the profile named TACACS-Profile.
2. In the Servers section, locate the TACACS+ server and modify the **Secret** field.
3. Type in the correct secret and then retyping to confirm.
4. Click **OK** to save the change.
Test Authentication Server Connectivity

**TACACS+ Authentication Profile Test Example**

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
name "User2-TACACS" is in group "all"
Authentication to TACACS+ server at '10.5.196.62' for user 'User2-TACACS'
Server port: 49, timeout: 30, flag: 0
Egress: 10.5.104.98
Attempting CHAP authentication ...
CHAP authentication request is created
Sending credential: xxxxxx
CHAP authentication request is sent
Authentication succeeded!
Authentication succeeded for user "User2-TACACS"
```

**Test an LDAP Authentication Profile**

The following example shows how to test a LDAP authentication profile named LDAP-Profile for a user named User4-LDAP and how to troubleshoot error conditions that arise. For details on using the test authentication command, see Run the Test Authentication Command.

**LDAP Authentication Profile Test Example**

**Step 1** On the PAN-OS firewall, **Configure an LDAP Server Profile** and **Configure an authentication profile**. In the authentication profile, you select the new LDAP server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```

The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile LDAP-Profile username User4-LDAP password
```
**Authentication Test Authentication Server Connectivity**

**Kerberos Authentication Profile Test Example**

**Step 5** When prompted, enter the password for the User4-LDAP account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User4-LDAP" is in group "all"
Authentication to LDAP server at 10.5.104.99 for user "User4-LDAP"
Egress: 10.5.104.98
Type of authentication: plaintext
Starting LDAP connection...
Succeeded to create a session with LDAP server
parse error of dn and attributes for user "User4-LDAP"
Authentication failed against LDAP server at 10.5.104.99:389 for user "User4-LDAP"
Authentication failed for user "User4-LDAP"
The output shows parse error of dn and attributes for user User4-LDAP, which indicates a BIND DN value issues in the LDAP server profile. In this case, a Domain Component (DC) value is incorrect.
```

**Step 6** To resolve this issue, modify the LDAP server profile and ensure that the Bind DN DC value is correct by comparing the DC value with the DC value of the LDAP server.
1. On the firewall, select Device > Server Profiles > LDAP and modify the profile named LDAP-Profile.
2. In the Server settings section, enter the correct value for the DC in the Bind DN field. In this case, the correct value for the DC is MGMT-GROUP.
3. Click OK to save the change.

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
name "User4-LDAP" is in group "all"
Authentication to LDAP server at 10.5.104.99 for user "User4-LDAP"
Egress: 10.5.104.98
Type of authentication: plaintext
Starting LDAP connection...
Succeeded to create a session with LDAP server
DN sent to LDAP server: CN=User4-LDAP,CN=Users,DC=MGMT-GROUP,DC=local
User expires in days: never
Authentication succeeded for user "User4-LDAP"
```

**LDAP Authentication Profile Test Example**

**Step 5** When prompted, enter the password for the User4-LDAP account. The following output shows the test failed:

```
Do allow list check before sending out authentication request...
name "User4-LDAP" is in group "all"
Authentication to LDAP server at 10.5.104.99 for user "User4-LDAP"
Egress: 10.5.104.98
Type of authentication: plaintext
Starting LDAP connection...
Succeeded to create a session with LDAP server
parse error of dn and attributes for user "User4-LDAP"
Authentication failed against LDAP server at 10.5.104.99:389 for user "User4-LDAP"
Authentication failed for user "User4-LDAP"
The output shows parse error of dn and attributes for user User4-LDAP, which indicates a BIND DN value issues in the LDAP server profile. In this case, a Domain Component (DC) value is incorrect.
```

**Test a Kerberos Authentication Profile**

The following example shows how to test a Kerberos profile named Kerberos-Profile for a user named User5-Kerberos and how to troubleshoot error conditions that arise. For details on using the test authentication command, see Run the Test Authentication Command.

**Kerberos Authentication Profile Test Example**

**Step 1** On the PAN-OS firewall, Configure a Kerberos Server Profile and Configure an authentication profile. In the authentication profile, you select the new Kerberos server profile in the Server Profile drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.
Test Authentication Server Connectivity

Authentication

Kerberos Authentication Profile Test Example

Step 3  (Firewalls with virtual systems configured) Define the target virtual system that the test command will access. This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```

The target-vsys command is per-login session, so the system clears the option when you log off.

Step 4  Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile Kerberos-Profile username User5-Kerberos password
```

Step 5  When prompted, enter the password for the User5-Kerberos account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User5-Kerberos" is in group "all"
Authentication to KERBEROS server at '10.5.104.99' for user 'User5-Kerberos'
Realm: 'Bad-MGMT-GROUP.LOCAL'
Egress: 10.5.104.98
KERBEROS configuration file is created
KERBEROS authcontext is created. Now authenticating ...
Kerberos principal is created
Sending authentication request to KDC...
Authentication failure: Wrong realm: 'Bad-MGMT-GROUP.LOCAL' (code: -1765328316)
Authentication failed against KERBEROS server at 10.5.104.99:88 for user "User5-Kerberos"
Authentication failed for user "User5-Kerberos"
```

In this case, the output shows **Wrong realm**, which indicates that the Kerberos realm has an incorrect value.

Step 6  To resolve this issue, modify the Kerberos server profile and ensure that the Realm value is correct by comparing the realm name on the Kerberos server.

1. On the firewall, select Device > Authentication Profiles and modify the profile named Kerberos-Profile.
2. In the Kerberos Realm field, enter the correct value. In this case, the correct realm is mgmt-group.local.
3. Click **OK** to save the change.

Step 7  Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
name "User5-Kerberos" is in group "all"
Authentication to KERBEROS server at '10.5.104.99' for user 'User5-Kerberos'
Realm: 'MGMT-GROUP.LOCAL'
Egress: 10.5.104.98
KERBEROS configuration file is created
KERBEROS authcontext is created. Now authenticating ...
Kerberos principal is created
Sending authentication request to KDC...
Authentication succeeded!
Authentication succeeded for user "User5-Kerberos"
```
Troubleshoot Authentication Issues

When users fail to authenticate to a Palo Alto Networks firewall or Panorama, or the Authentication process takes longer than expected, analyzing authentication-related information can help you determine whether the failure or delay resulted from:

- **User behavior**—For example, users are locked out after entering the wrong credentials or a high volume of users are simultaneously attempting access.
- **System or network issues**—For example, an authentication server is inaccessible.
- **Configuration issues**—For example, the Allow List of an authentication profile doesn't have all the users it should have.

The following CLI commands display information that can help you troubleshoot these issues:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the number of locked user accounts associated with the authentication profile (auth-profile), authentication sequence (is-seq), or virtual system (vsys). To unlock users, use the following operational command:</td>
<td>show authentication locked-users</td>
</tr>
<tr>
<td>request authentication [unlock-admin</td>
<td>unlock-user]</td>
</tr>
<tr>
<td>Use the debug authentication command to troubleshoot authentication events. Use the show options to display authentication request statistics and the current debugging level:</td>
<td>debug authentication</td>
</tr>
<tr>
<td>• show displays the current debugging level for the authentication service (authd).</td>
<td></td>
</tr>
<tr>
<td>• show-active-requests displays the number of active checks for authentication requests, allow lists, and locked user accounts.</td>
<td></td>
</tr>
<tr>
<td>• show-pending-requests displays the number of pending checks for authentication requests, allow lists, and locked user accounts.</td>
<td></td>
</tr>
<tr>
<td>• connection-show displays authentication request and response statistics for all authentication servers or for a specific protocol type.</td>
<td></td>
</tr>
<tr>
<td>Use the connection-debug options to enable or disable authentication debugging:</td>
<td></td>
</tr>
<tr>
<td>• Use the on option to enable or the off option to disable debugging for authd.</td>
<td></td>
</tr>
<tr>
<td>• Use the connection-debug-on option to enable or the connection-debug-off option to disable debugging for all authentication servers or for a specific protocol type.</td>
<td></td>
</tr>
</tbody>
</table>