STEP 7 | (Optional) Define the set of user accounts that don't require IP address-to-username mappings, such as kiosk accounts.

> *Define the ignore user list on the firewall that is the User-ID agent, not the client. If you define the ignore user list on the client firewall, the users in the list are still mapped during redistribution.*

On the **Ignore User List** tab, **Add** each username you want to exclude from user mapping. You can also use the ignore user list to identify the users you want to force to use Captive Portal to authenticate. You can use an asterisk as a wildcard character to match multiple usernames but only as the last character in the entry. For example, **`corpdomain\it-admin*`** would match all administrators in the `corpdomain` domain whose usernames start with the string `it-admin`. You can add up to 5,000 entries to exclude from user mapping.

STEP 8 | Activate your configuration changes.

Click **OK** and **Commit**.

STEP 9 | Verify the configuration.

1. Access the firewall CLI.
2. Enter the following operational command:

```
> show user server-monitor state all
```

3. On the **Device** > **User Identification** > **User Mapping** tab in the web interface, verify that the Status of each server you configured for server monitoring is `Connected`.

Configure Server Monitoring Using WinRM

You can configure the PAN-OS integrated User-ID agent to monitor servers using Windows Remote Management (WinRM). Using the WinRM protocol improves speed, efficiency, and security when monitoring server events to map user events to IP addresses. The PAN-OS integrated User-ID agent supports the WinRM protocol on Windows Server 2008 Active Directory and Microsoft Exchange Server 2008 or later versions of both.

There are three ways to configure server monitoring using WinRM:

- Configure WinRM over HTTPS with Basic Authentication—The firewall authenticates to the monitored server using the username and password of the service account for the User-ID agent and the firewall authenticates the monitored server using the User-ID certificate profile.
- Configure WinRM over HTTP with Kerberos—The firewall and the monitored servers use Kerberos for mutual authentication and the monitored server encrypts the communication with the firewall using a negotiated Kerberos session key.
- Configure WinRM over HTTPS with Kerberos—The firewall and the monitored server use HTTPS to communicate and use Kerberos for mutual authentication.

Configure WinRM over HTTPS with Basic Authentication

When you configure WinRM to use HTTPS with basic authentication, the firewall transfers the credentials for the service account in a secure tunnel using SSL.

STEP 1 | Configure the service account with Remote Management User and CIMV2 privileges for the server you want to monitor.

STEP 2 | On the Windows server you are monitoring, obtain the thumbprint from the certificate for the Windows server to use with WinRM and enable WinRM.

> *Ensure that you use an account with administrator privileges to configure WinRM on the server you want to monitor. As a best practice for security, this account should not be the same account as the service account in Step 1.*

1. Verify the certificate is installed in the Local Computer certificate store (**Certificates (Local Computer)** > **Personal** > **Certificates**).

   If you do not see the Local Computer certificate store, launch the Microsoft Management Console (**Start** > **Run** > **MMC**) and add the Certificates snap-in (**File** > **Add/Remove Snap-in** > **Certificates** > **Add** > **Computer account** > **Next** > **Finish**).
2. Open the certificate and select **General** > **Details** > **Show: <All>**.
3. Select the **Thumbprint** and copy it.
4. To enable the firewall to connect to the Windows server using WinRM, enter the following command: **`winrm quickconfig`**.
5. Enter **`y`** to confirm the changes and then confirm the output displays `WinRM service started`.

   If WinRM is enabled, the output displays `WinRM service is already running on this machine.` You will be prompted to confirm any additional required configuration changes.
6. To verify that WinRM is communicating using HTTPS, enter the following command: **`winrm enumerate winrm/config/listener`** and confirm that the output displays `Transport = HTTPS`.

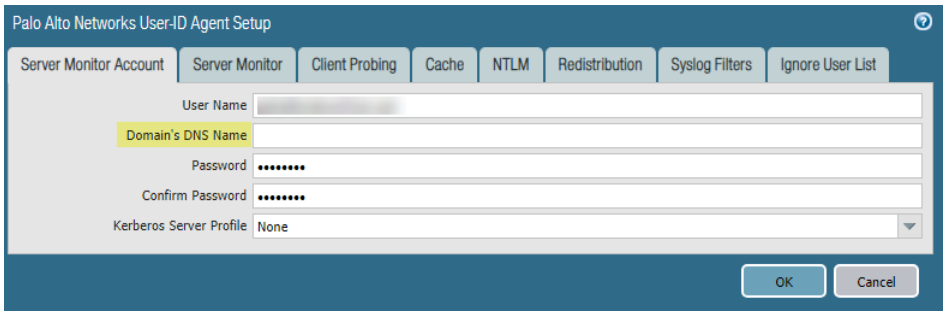
   By default, WinRM/HTTPS uses port 5986.
7. From the Windows server command prompt, enter the following command: **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**, where *hostname* is the hostname of the Windows server and *Certificate Thumbprint* is the value you copied from the certificate.

   > *Use the command prompt (not Powershell) and remove any spaces in the Certificate Thumbprint to ensure that WinRM can validate the certificate.*
8. From the Windows server command prompt, enter the following command:

   ```
   c:\> winrm set winrm/config/client/auth @{Basic="true"}
   ```
9. Enter the following command: **`winrm get winrm/config/service/Auth`** and confirm that `Basic = true`.

STEP 3 | Enable Basic Authentication between the PAN-OS integrated User-ID agent and the monitored servers.

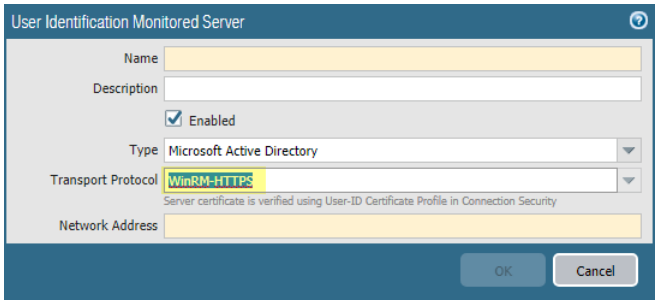
1. Select **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor Account**.
2. In **`domain\username`** format, enter the **User Name** for the service account that the User-ID agent will use to monitor servers.
3. Enter the **Domain's DNS Name** of the server monitor account.
4. Enter the **Password** and **Confirm Password** for the service account.



5. Click **OK**

STEP 4 | Configure server monitoring for the PAN-OS integrated User-ID agent.

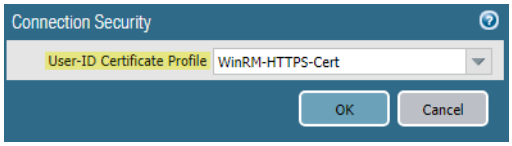
1. Select the Microsoft server **Type** (**Microsoft Active Directory** or **Microsoft Exchange**).
2. Select **Win-RM-HTTPS** as the **Transport Protocol** to use Windows Remote Management (WinRM) over HTTPS to monitor the server security logs and session information.
3. Enter the IP address or FQDN **Network Address** of the server.



STEP 5 | To enable the PAN-OS integrated User-ID agent to communicate with the monitored servers using WinRM-HTTPS, verify that you successfully imported the root certificate for the

service certificates that the Windows server uses for WinRM on to the firewall and associate the certificate with the User-ID Certificate Profile.

1. Select **Device** > **User Identification** > **Connection Security**.
2. Click **Edit**.
3. Select the Windows server certificate to use for the **User-ID Certificate Profile**.



4. Click **OK**.

STEP 6 | **Commit** your changes.

STEP 7 | Verify that the status of each monitored server is Connected (**Device** > **User Identification** > **User Mapping**).

Configure WinRM over HTTP with Kerberos

When you configure WinRM over HTTP with Kerberos, the firewall and the monitored servers use Kerberos for mutual authentication and the monitored server encrypts the communication with the firewall using a negotiated Kerberos session key.

WinRM with Kerberos supports the aes128-cts-hmac-sha1-96 and aes256-cts-hmac-sha1-96 ciphers. If the server you want to monitor uses RC4, you must download the Windows update and disable RC4 for Kerberos in the registry settings of the server you want to monitor.

STEP 1 | Configure the service account with Remote Management User and CIMV2 privileges for the server you want to monitor.

STEP 2 | Confirm that WinRM is enabled on the Windows server you are monitoring.

Ensure that you use an account with administrator privileges to configure WinRM on the server you want to monitor. As a best practice for security, this account should not be the same account as the service account in Step 1.

1. To enable the firewall to connect to the Windows server using WinRM, enter the following command: **`winrm quickconfig`**.
2. Enter **`y`** to confirm the changes and then confirm the output displays `WinRM service started`.

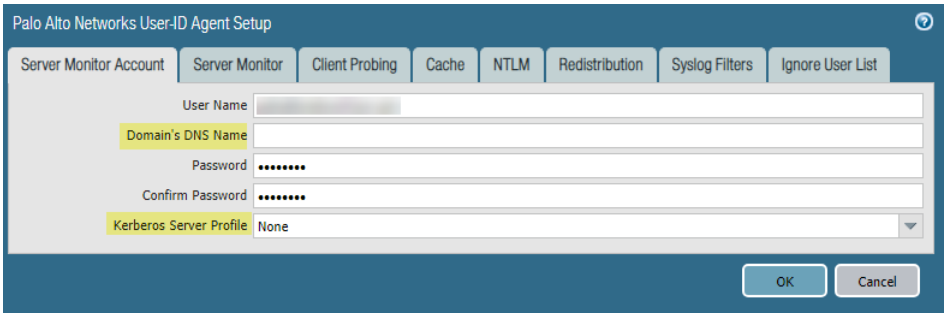
   If WinRM is enabled, the output displays `WinRM service is already running on this machine.` You will be prompted to confirm any additional required configuration changes.
3. To verify that WinRM is communicating using HTTP, enter the following command: **`winrm enumerate winrm/config/listener`** and confirm that the output displays `Transport = HTTP`.

   By default, WinRM/HTTP uses port 5985.
4. Enter the following command: **`winrm get winrm/config/service/Auth`** and confirm that `Kerberos = true`.

STEP 3 | Enable the PAN-OS integrated User-ID agent and the monitored servers to authenticate using Kerberos.

1. If you did not do so during the initial configuration, configure date and time (NTP) settings to ensure successful Kerberos negotiation.
2. Configure a Kerberos server profile on the firewall to authenticate with the server to monitor the security logs and session information.
3. Select **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor Account**.
4. In **`domain\username`** format, enter the **User Name** for the service account that the User-ID agent will use to monitor servers.
5. Enter the **Domain's DNS Name** of the server monitor account.

   Kerberos uses the domain name to locate the service account.
6. Enter the **Password** and **Confirm Password** for the service account.
7. Select the **Kerberos Server Profile** you configured in Step 3.2.

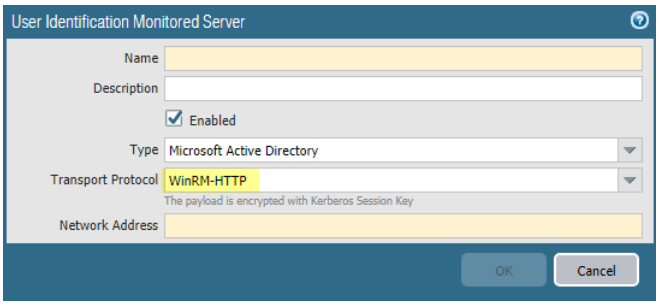


8. Click **OK**.

STEP 4 | Configure server monitoring for the PAN-OS integrated User-ID agent.

1. Configure the Microsoft server type (**Microsoft Active Directory** or **Microsoft Exchange**).
2. Select **WinRM-HTTP** as the **Transport Protocol** to use Windows Remote Management (WinRM) over HTTP to monitor the server security logs and session information.
3. Enter the FQDN **Network Address** of the server.

   If you are using Kerberos, the network address must be a fully qualified domain name (FDQN).



STEP 5 | **Commit** your changes.

STEP 6 | Verify that the status of each monitored server is Connected (**Device** > **User Identification** > **User Mapping**).

Configure WinRM over HTTPS with Kerberos

When you configure WinRM over HTTPS with Kerberos, the firewall and the monitored server use HTTPS to communicate and use Kerberos for mutual authentication.

WinRM with Kerberos supports the aes128-cts-hmac-sha1-96 and aes256-cts-hmac-sha1-96 ciphers. If the server you want to monitor uses RC4, you must download the Windows update and disable RC4 for Kerberos in the registry settings of the server you want to monitor.

STEP 1 | Configure the service account with Remote Management User and CIMV2 privileges for the server you want to monitor.

